Enhanced User Security In TEOSM

Ms. Selvi Jayaraman (TATA ELXSI)

Ecosystem Day (March 2023)

16/06/2022

Agenda

- User Management Overview
- User Management - TEOSM
- Security Implementation
- Advantages
- Demo

User Management Overview

- User Management is an important security requirement for any orchestrator application.
- It allows administrators to control and manage access to the application and its resources while ensuring security and compliance with industry best practices.
- Administrators need powerful user management capabilities to maintain user status and also define policies.

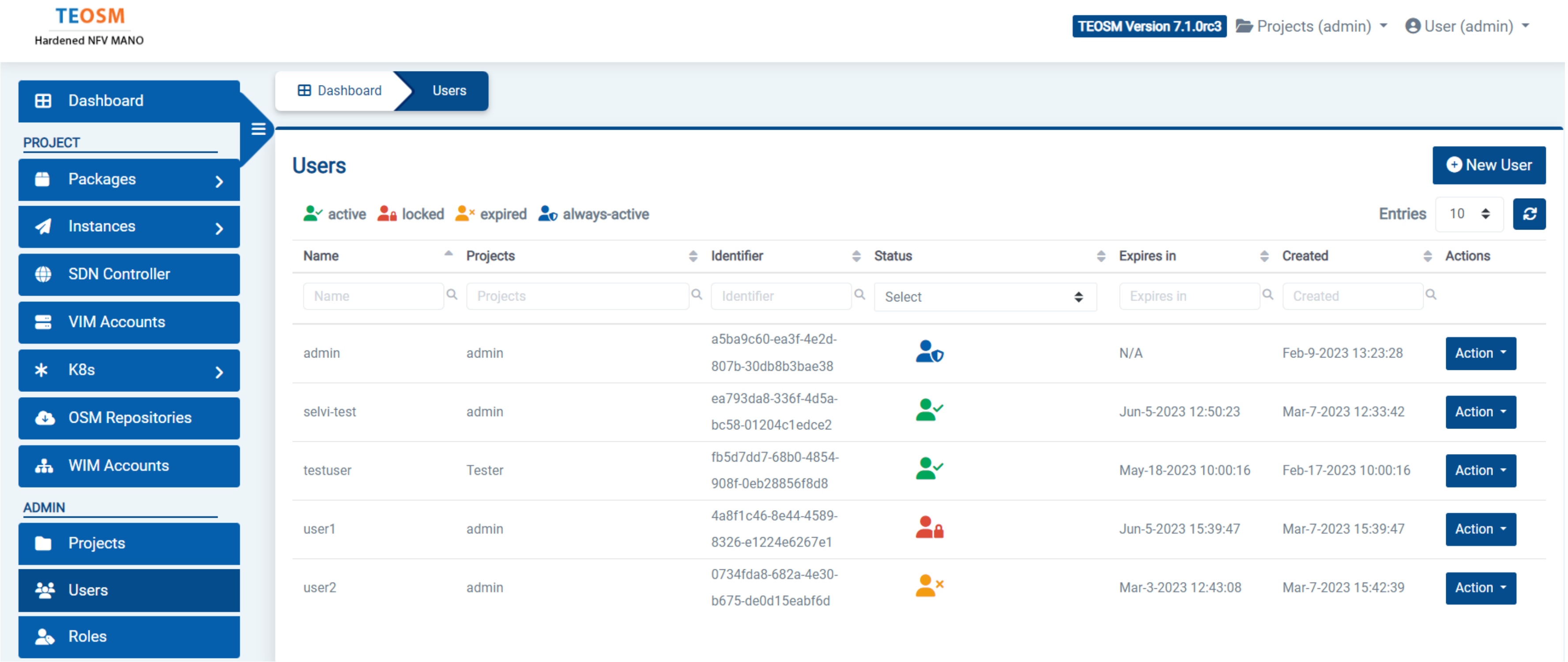
User Management in TEOSM Orchestrator

Some of the key considerations for user management are:

- **Authentication**: The first step in user management is to ensure that only authenticated users can access the application.
- **Authorization**: Once users are authenticated, the next step is to ensure that they have access to the appropriate resources within the application. Authorization is the process of defining what users can and cannot do within the application based on their roles, permissions, and privileges.
- **User Roles and Permissions**: User roles are used to define a set of permissions that a user has within the application. This can range from basic read-only access to full administrative privileges.
- **User Creation and Management**: The ability to create and manage users is an essential aspect of user management. Administrators should be able to create new users, modify existing user accounts, and delete users as necessary. Additionally, user accounts should be managed in a way that ensures security and prevents unauthorized access.

Security Implementation

- **User Activity**: User activity is important for tracking user behavior and detecting potential security breaches. Application administrators should be able to review user status to identify suspicious activity and take appropriate action as needed.



Users

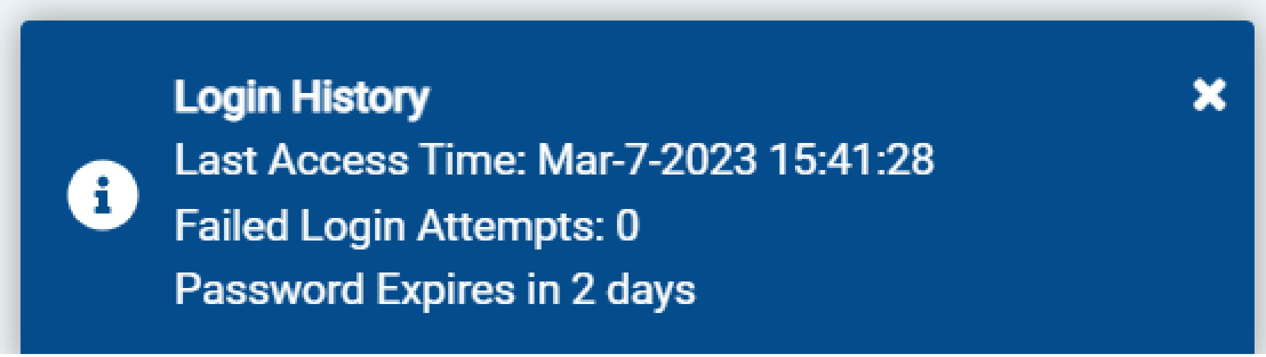
✓ active 🔒 locked × expired 🛡 always-active

Name	Projects	Identifier	Status	Expires in	Created	Actions
admin	admin	a5ba9c60-ea3f-4e2d-807b-30db8b3bae38	🛡	N/A	Feb-9-2023 13:23:28	Action
selvi-test	admin	ea793da8-336f-4d5a-bc58-01204c1edce2	✓	Jun-5-2023 12:50:23	Mar-7-2023 12:33:42	Action
testuser	Tester	fb5d7dd7-68b0-4854-908f-0eb28856f8d8	✓	May-18-2023 10:00:16	Feb-17-2023 10:00:16	Action
user1	admin	4a8f1c46-8e44-4589-8326-e1224e6267e1	🔒	Jun-5-2023 15:39:47	Mar-7-2023 15:39:47	Action
user2	admin	0734fda8-682a-4e30-b675-de0d15eabf6d	×	Mar-3-2023 12:43:08	Mar-7-2023 15:42:39	Action

Security Implementation

- **Password Policies**: Strong password policies can help prevent unauthorized access to the application. Password policies should include requirements for password length, complexity, and expiration. Additionally, users should be prompted to reset their passwords periodically to ensure continued security, and users should not be able to reuse the last 3 passwords.

- **Password Notification**: Password notification is a process of notifying users to change their passwords after a specified period.



Login History
Last Access Time: Mar-7-2023 15:41:28
Failed Login Attempts: 0
Password Expires in 2 days

Security Implementation

- **Account Renewal**: It is an important aspect of user management that ensures only authorized users have access to an application's resources. It is a process of extending the validity of a user account.

- **User Support**: User management should include support for users who experience issues with their accounts. This can include features such as password reset or account renewal.

Advantages

- **Improved Security:** Enforcing user login and password notifications helps to improve the security of an application by reducing the risk of unauthorized access.
- **Account Management:** Account expiration policies allow administrators to manage user accounts efficiently.
- **Centralized Management:** Enforcing these policies in user management provides a centralized approach to managing user accounts, making it easier for administrators to manage large numbers of users.
- Reduced Risk of Data Breaches.
- Password notifications remind users to update their passwords regularly, making it harder for attackers to crack weak or old passwords.

References

- Feature: https://osm.etsi.org/gitlab/osm/features/-/issues/10941
- Design: https://osm.etsi.org/pad/p/feature10941

Demo

- Enforcing password change
- Locking user account on exceeding failed login attempts and performing unlock action
- Expiring the user account and performing renewal action
- Displaying the login history information in NGUI

Open Source MANO

by ETSI

Thank You!