Enhanced User Security In TEOSM

Ms. Selvi Jayaraman (TATA ELXSI)

Ecosystem Day (March 2023)
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.
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.
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.
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](https://osm.etsi.org/gitlab/osm/features/-/issues/10941)
- Design: [https://osm.etsi.org/pad/p/feature10941](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
Thank You!