Celonis 4 - Secure Configuration Guide

Overview

This guide provides instructions and recommendations for securely configuring the Celonis Process Mining 4 (CPM4) application. It is intended to be used in conjunction with the publicly available end-user documentation and FedRAMP-specific annotations. This guide specifically details the management of top-level administrative accounts and the security-related settings that those top-level administrators may configure.

Secure Configuration

1. General Best Practices

The following are best practice guidelines for managing access to your CPM4 instance.

- Document internal processes for granting, adjusting, and revoking managing access to CPM4.
- Grant permissions to users based on the principle of least privilege.
- Do not share accounts. Ensure each account is associated with an individual.
- Regularly review access rights to ensure that they are appropriate.

2. Managing Top-Level Administrative Accounts

Celonis Process Mining 4 (CPM4) uses roles and permissions to grant administrative access to user accounts. In CPM4, a top-level administrative account is defined as a single user possessing all three of the following administrative roles: System Administrator, Global Content Administrator, and User Administrator. These accounts control enterprise access to the entire cloud service offering.

Initial Setup

- **Access Control:** All accounts are provisioned with no access by default. Customers are responsible for provisioning all non-top-level administrative accounts and appropriately granting roles and permissions to users.
- **Top-level Admin Initial Setup:** During customer onboarding, Celonis will guide you through integration of Celonis Process Mining with your chosen customer-owned Identity Provider (IdP). The customer should ensure that the chosen IdP supports FIPS-validated Multi-Factor Authentication (MFA). Once the integration is complete, customers are responsible for provisioning a single top-level administrative account, which will be granted initial permissions by Celonis.
- **Best Practices:**
  - Do not provision additional top-level administrative accounts.
  - Do not grant a top-level administrative account direct content permissions.
  - Only enable the top-level administrative account when required.

Secure Operation

Utilize the top-level administrative account only when performing the following actions:

1. Granting the "User Administrator" role to the appropriate number of user accounts (configured in the application frontend, either via the User Profile or through Groups).
2. Setting up Authorizations (setting up Authorizations is the only administrative action that explicitly requires all three top-level administrative roles).

The top-level administrative account should be managed directly via your IdP. We recommend one of the following two options:

- **Option 1 (Suspension):** The top-level administrative account is suspended/locked on the customer IdP side by default. It is only activated temporarily upon reasonable, written request.
- **Option 2 (Deletion & Recreation):** The top-level administrative account is deleted after the initial setup. A new top-level administrative account is temporarily provisioned upon reasonable written request. Top-level administrative privileges are then granted by a User Administrator editing the User Profile or by provisioning the account into a Group with all three roles assigned.

A procedure for managing the activation and deletion/deactivation should be documented by the customer.

Application level audit logs, including privileged actions are collected, monitored, and retained by Celonis. Application audit logs may be provided upon written request to support the investigation of a security incident.

3. Top-Level Administrative Security Settings

Authorizations are the only security-related setting that can solely be operated by the top-level administrative account, as configuration requires access to manage users, content, and system settings (source). All other security-related settings can be operated by privileged accounts.

Authorizations are used to further restrict the data visible to individual users or groups within a Data Model (e.g., based on criteria like country or department). Configuration requires access to manage users, content, and system settings and is performed via the application frontend.

Recommended defaults:

- It is recommended to add a dedicated Authorization object to every Data Model in the Celonis application. The target table and column depend on the use case and data structure
- It is recommended to apply the Data Model-specific Authorizations objects to every user in the application.
- It is recommended to implement a “Zero Trust” baseline by not adding any permitted values to any user by default.

Use Case Example: If users from the US are only allowed to see US purchasing data, and the Data Model contains global purchasing data, Authorizations *must* be configured to ensure users are restricted to their respective countries. (Note: If the Data Model *only* contains US data, Authorizations are not required, as standard content permissions can enforce this).

Security Implications: Improper use or misconfiguration can result in users viewing data they are not authorized to see.

4. Privileged Account Security Settings

The following security-related settings can be operated by privileged accounts within the application frontend (e.g., users holding specific administrative roles rather than all three top-level roles).

Setting	**Required role**	**Description**	**Implications**
User management	User Administrator	Managing user accounts, e.g. granting additional elevated privileges	Assigning improper roles and permissions can result in users being able to view data they are not authorized to
Group management	User Administrator	Managing groups, e.g. granting additional elevated privileges	Assigning improper roles and permissions can result in users being able to view data they are not authorized to
Source configurations	System Administrator	Required for setting up LDAP sources and Database Sources for Authorizations, User Providers and Group Providers	Improper configuration can lead to dysfunctional user provisioning, SSO, Authorizations, including non-authorized application access. **Note**: Additional securities are applied for FedRAMP customers
User Provider	System Administrator	Required to provision individual users via LDAP or Database	
Group provider	System Administrator	Required to provision groups via LDAP or Database	
Authentication	System Administrator	Required to specify authentication systems such as LDAP and HTTP-Header	
Compute Node Management	System Administrator	Required to register additional compute nodes	Improper configuration can lead to process data being processed outside the authorized boundary. **Note**: Additional securities are applied for FedRAMP customers

Security Configuration Exports and Evaluation

To verify your Celonis Process Mining 4 environment aligns with the Secure Configuration Guide, administrators should routinely evaluate both system-level configurations and user access privileges. Start by reviewing the System Settings to manually confirm that your Authentication parameters and Identity Provider integrations are strictly enforcing SSO and any required MFA policies. Next, to audit access and detect drift from the secure defaults, utilize the system's export capabilities. You can generate the User Management and Permission Report to extract a comprehensive, point-in-time view of all user roles, group memberships, and specific content permissions. Cross-referencing these detailed exports and your authentication settings against the baseline recommendations in this guide will allow you to quickly identify overly permissive accounts or unauthorized configuration drift.

It should be noted that security configurations outside of those explicitly listed within this guide are managed by Celonis and set within the config-custom.properties file. The contents of your specific config-custom.properties file may be made available to you via submission of a customer support request.

Appendix I: Revision History

Version	**Date**	**Application Version**	**Summary**
1.0	Feb 24, 2026	4.7.4	Initial creation

Appendix II: Control References

- SCG-CSO-RSC: Secure Configuration
- SCG-CSO-SDF: Secure Configuration
- SCG-ENH-CMP: Security Configuration Exports and Evaluation
- SCG-ENH-EXP: Security Configuration Exports and Evaluation
- SCG-ENH-VRH: Appendix I: Revision History
- SCG-ENH-MRG: Excluded. Not supported by CPM4.
- SCG-ENH-API: Excluded. Not supported by CPM4.