celonis

Built-In Security Features of the EMS

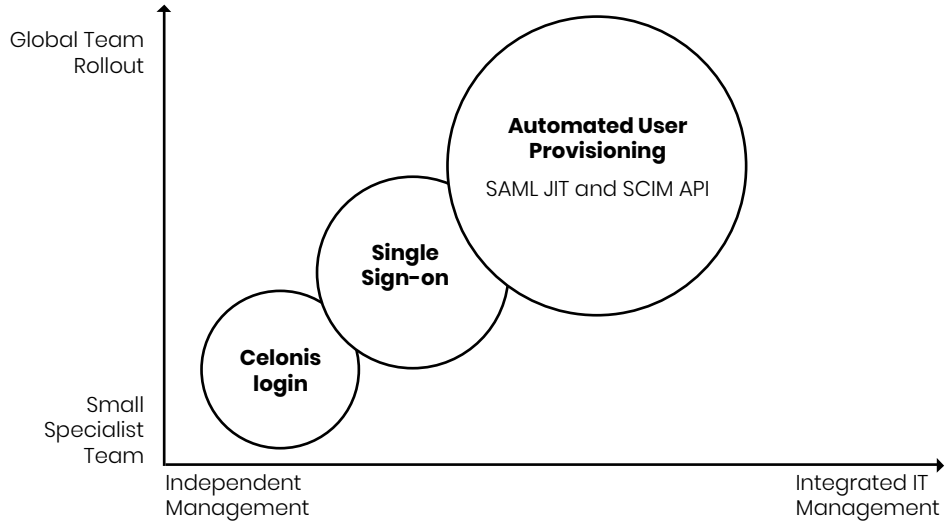
Introduction

Data is fundamental to Celonis' ability to sense execution gaps and act upon insights, therefore the Execution Management System (EMS) is built and operated using advanced data security measures and default settings. Customers also have the ability to control additional configuration to ensure compliance with organizational security policies. This document provides guidance on some of the main areas which should be considered.

After purchasing an EMS license, you are provided with a Team. A Team is a space that allows you to use your data with the applications provided by the EMS, such as Business Views, Studio or Event Collection. Each Team includes members. One member role is that of the administrator, who controls team configuration including user access privileges and data security.

Access Controls

Managing the users that can access your Team is a key part of managing and maintaining security. Celonis customers come in all sizes, therefore we provide multiple options for balancing the effort of Team management, including: single sign-on via SAML and OpenId, SAML JIT and SCIM API.



No coupling of user management:
Users are provisioned manually and authenticate via Celonis login, using username and password and optionally 2FA.

- All user management takes place within the EMS.
- No additional effort is required — this is the default scenario within the EMS.
- This is appropriate for small teams without complex governance structures.

Image 1: User management options exist for all Team sizes and complexity. Recommendations above are based on team size.

Light coupling of user management:
Users are invited via email and the account is created on first login. Authentication takes place via Single Sign-on. The use of Single Sign-on decouples user login from EMS and gives admins an extra security layer where they can define their own password policies, 2FA strategy and user management. and provides an extra layer of security.

- The one-time effort of linking your identity provider to Celonis via metadata files is required.
- This scenario is appropriate for medium-sized teams without complex governance structures.
- EMS supports three types of certificates for SSO: self signed, let's encrypt and user provided

Tight coupling of user management: Users and groups are automatically provisioned and users are assigned to groups according to access information provided by the identity provider. This is often combined with Single Sign-on to increase ease of access. This scenario is appropriate for larger teams with complex governance structures. Celonis supports Users and groups are automatically provisioned and users are assigned to groups:

1. SAML Just-in-Time:

- Users authenticate via SAML Single Sign-on and accounts are created automatically upon their first login.
- The one-time effort of linking your identity provider to Celonis via metadata files is required.
- Identity providers must have a group structure in place.

By default, users cannot access any Celonis capabilities or team data. After creating user groups, administrators can assign user permissions and data permissions. These topics are covered later in this whitepaper.

*The EMS supports SSO via SAML 2.0 and OIDC.

Login Security

Organizations can further reduce the risk of improper information access by restricting access using IP restrictions and two-factor authentication.

IP restrictions limit the IP addresses that can access the Celonis web application. Administrators can easily add a list of IP addresses which should have access. Updating the list is also helpful, especially if there is a need to provide or remove access to external partners, such as 3rd-party implementation partners. IP restrictions can be set within Team Settings. By default, IP restrictions are disabled.

Two-factor authentication requires users to enter a temporary token upon login. This ensures that login credentials cannot be misused by non-authorized users. It can be easily implemented by flipping a switch within Team Settings.

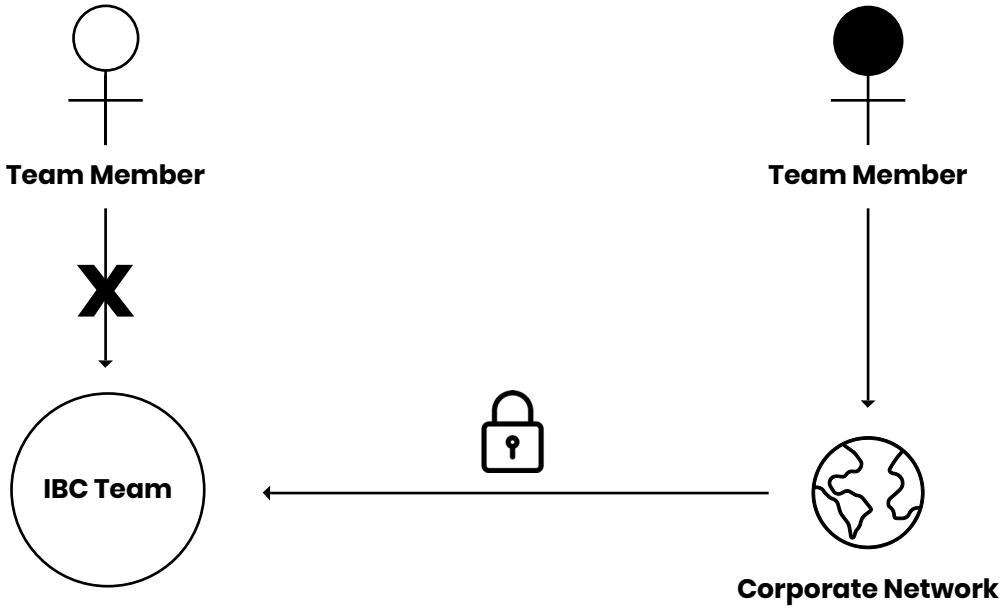


Image 2: IP Restrictions only allow employees that go through approved IP addresses, such as the Corporate Network IP address to access the system.

User Permissions

Once you have established control over who can login, you can customize each user's access and permissions. Access permissions provide guidelines as to how a user can interact with objects within Celonis.

There are three roles that a user can be assigned to. These control the set of permissions s/he may have:

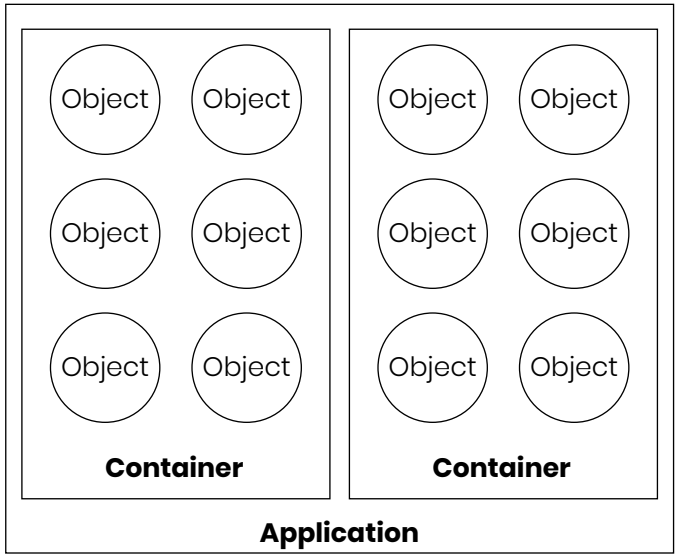
- **Member** - view content depending on permissions
- **Analyst** - create / view / edit / delete content depending on permissions
- **Admin** - create / view / edit / delete content AND team administration

User permissions are never assumed — every new user is initially assigned to the member role and is not assigned any permissions. This means that they are not able to view anything.

The EMS supports role-based access control (RBAC) via groups. This functionality allows admins to create named groups, assign permissions to a group and assign users to a group. For example, an admin might create a group named "Data Engineers" to provide required access permissions to analysts that work on the data pipeline. The admin would assign access permissions to Celonis' Event Collection capability so that members of the "Data Engineers" group can set up data connections and create data models. Once configured, the admin would assign specific users to the group.

Access is separately configured for each of the Celonis capabilities and can be configured granularly. If access is provided to a capability, the user can equally access the more granular container and object. For example, if analyst access is provided to Event Collection, that user can also view/edit data pools and data models. Alternatively, if access is provided to an object, the user cannot access the broader container or capability. For example, if view/edit permissions are provided for an Analysis, the user does not have view/edit access for the entire workspace or Process Analytics.

Diagram 2: The deployment architecture of the EMS



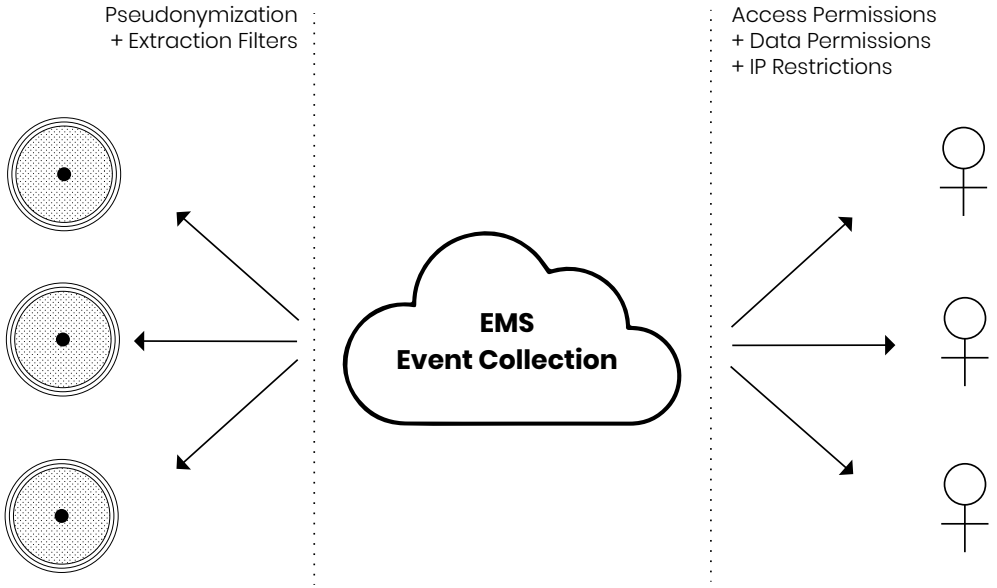
Permissions can be viewed within Celonis or exported for audit via the CSV export capability within Team Settings.

Additional information on Role-Based Access Controls:
https://help.celonis.cloud/help/display/CEMS/Permission+Management+Overview

CAPABILITY	CONTAINER	OBJECT
Event Collection	Data Pool	Data Model
Process Analytics	Workspace	Analysis
Action Engine	Project	Skill
Machine Learning	--	App
Business Views		View
Process Repository		Process Model
Actions Flows	--	Scenario
Studio		

Data Permissions

Data protection is extremely important to Celonis. We've implemented data protection methods across the entire data lifecycle.



Data Permissions: What data can a user see in a public analysis?
Access Permissions: What objects can a user interact with?

1. Before Data is Extracted:

- **A** Pseudonymization: Remain GDPR compliant by de-identifying personally identifiable information. Pseudonymization is configured within the data extractor.
- **B** Extraction Filters: Extract only the needed data fields. Filters are configured within the data extractor.

Image 3: Data protection measures take place before data enters the EMS and when data is visualized to individual users

2. During Data Extraction and Transformation:

A Limit access to only data engineers via user permissions.

3. At All Times:

A Data permissions enforce what specific data a user can see within Analyses and Views. While two users may look at the same analysis, the data visualized may be different depending on their access rights. By default, all users are provided no data permissions. Data permissions are assigned within the Data Model.

B At All Times: Data is encrypted both in-transit and at-rest.

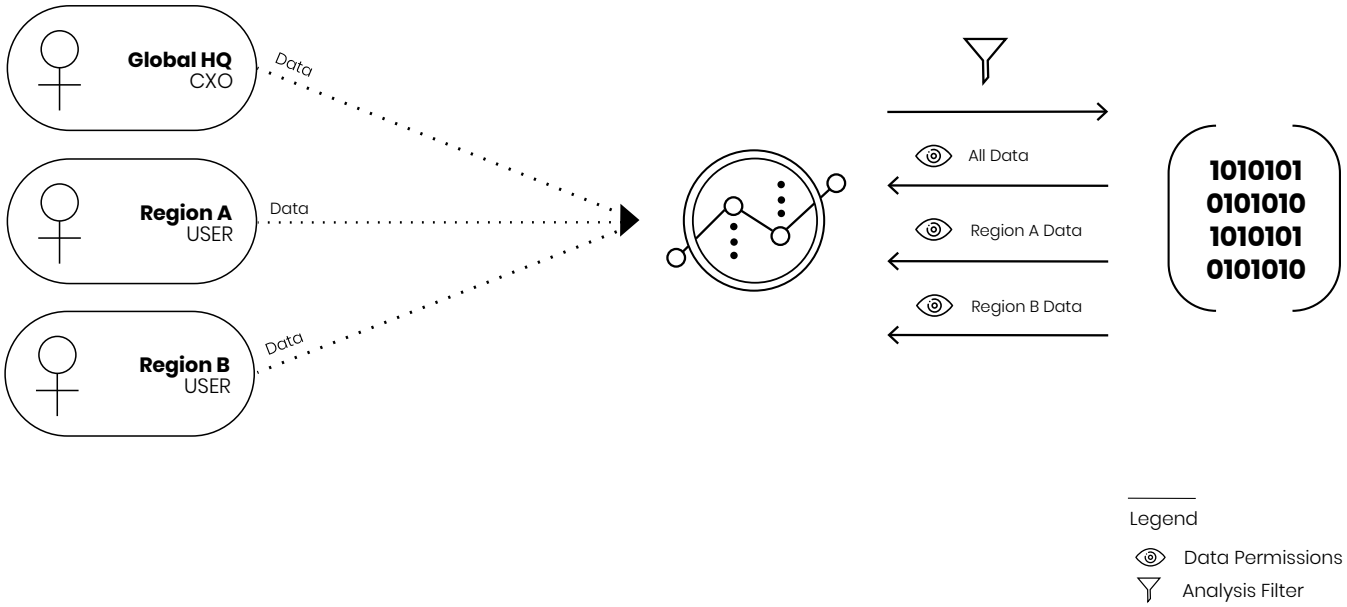


Image 4: Using data permissions, one analysis can service multiple users. The CXO has all data permissions and will see all data, while regional users will see the same analysis structure with regional data. Additional analysis filters can be applied to further drill into data.

Monitoring and Auditing

Security is not robust without active monitoring, therefore the EMS offers a comprehensive, tamper-proof audit log and an optional login history log.
Audit Logging records changes to every level of the application, for example changing the visibility of an analysis, user permissions or a bulk import of users. This provides a reliable source for data auditing and compliance exercises. The audit log is automatically recorded and includes the following information:

- User ID - who changed permissions within the system, e.g. 60433993-4ce4-4c93-9a88-421cdf2e57e5 (a.smith@exampledomain.com)
- Event - what was done, e.g. TEAM_MEMBERSHIP_CREATED
- Date - when the event took place, e.g 04/29/2020, 12:17:11 PM GMT+2
- Message - additional event-specific information, e.g. which users were created or removed, or which analyses were updated. {“userId”:”caafd466-2d62-4e3d-8170-ad964094af71”,”email”:”a.smith@exampledomain.com”}

Login history records who logged into the team and how often. To comply with regional regulations, login history is not automatically recorded. Both logs can be downloaded in CSV format for additional analysis.

- **Additional information on Audit Logs, including all logged events**
- **Additional information on Login History Logs**

Image XYZ: The built-in Celonis Audit Log functionality.

Security Responsibilities

This document covers the built-in functionality that customers can use to further their data security, however security is a much broader topic. Security across the Celonis Execution Management System application and infrastructure stack is a true partnership between customers, Celonis and our hosting providers.
Customers can implement the measures outlined in this document and take additional measures outside of the EMS to increase security, such as vetting employees. Celonis and our hosting providers work to provide the most up-to-date platform and infrastructure security measures, including penetration testing, physical security measures and software development processes that prioritize data security.
Data security is a continuous process and all partners — customers, Celonis and infrastructure partners — must remain diligent about implementing and monitoring data security measures.
The below table outlines the distribution of security measures.

	OWNER		
RESPONSIBILITY	**CUSTOMER**	**CELONIS**	**HOSTING PROVIDER**
Customer data management (classification, retention)	○		
Backup and restore	●	○	●
Authentication and authorization	○		
Data encryption at rest		○	
Encryption key management		○	●
Security logging and monitoring	○	○	●
Vulnerability management	○	○	
Business continuity and disaster recovery		○	○
Secure SDLC processes	○	○	
Penetration testing		○	
Privacy	○	○	
Compliance: regulatory and legal	○	○	○
Infrastructure management		○	●
Secure configuration of team	○		
Employee vetting or screening	○	○	○
Physical security			○
Audit logging		○	

Disclaimer

This document is provided for informational purposes only. It represents Celonis' current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of Celonis' products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances. The responsibilities and liabilities of Celonis to its customers are controlled by Celonis agreements, and this document is not part of, nor does it modify, any agreement between Celonis and its customers.

celonis.com