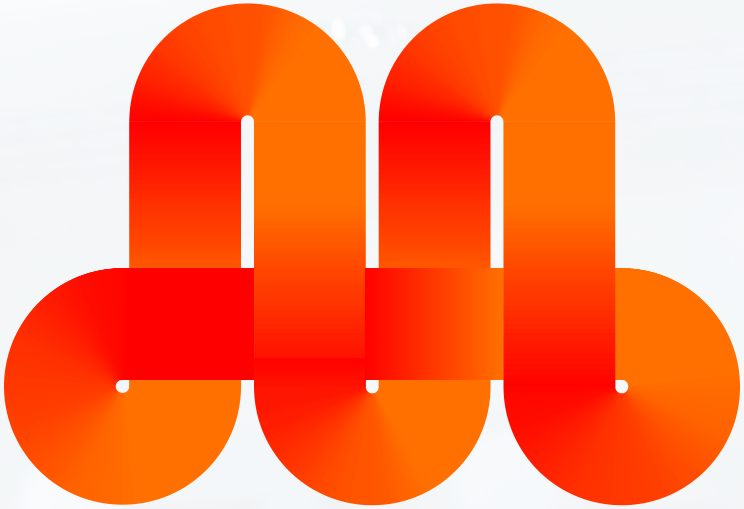


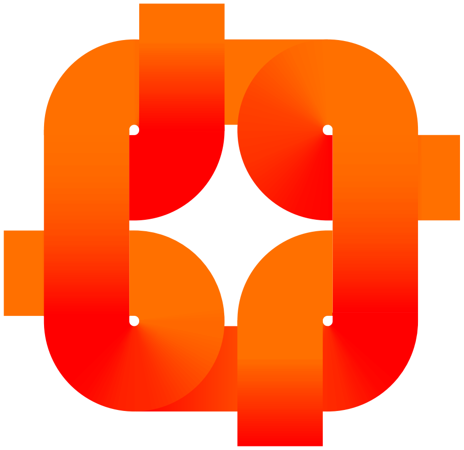
Built-In Security Features of the IBC

celonis

Introduction

Data is fundamental to Celonis' ability to sense friction and act upon insights, therefore the Intelligent Business Cloud (IBC) 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 IBC 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 IBC, such as Boards, Process Analytics or Action Engine. 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
Login Security
User Permissions
Data Permissions
Monitoring and Auditing
Security Responsibilities

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, LDAP and Active Directory integrations.

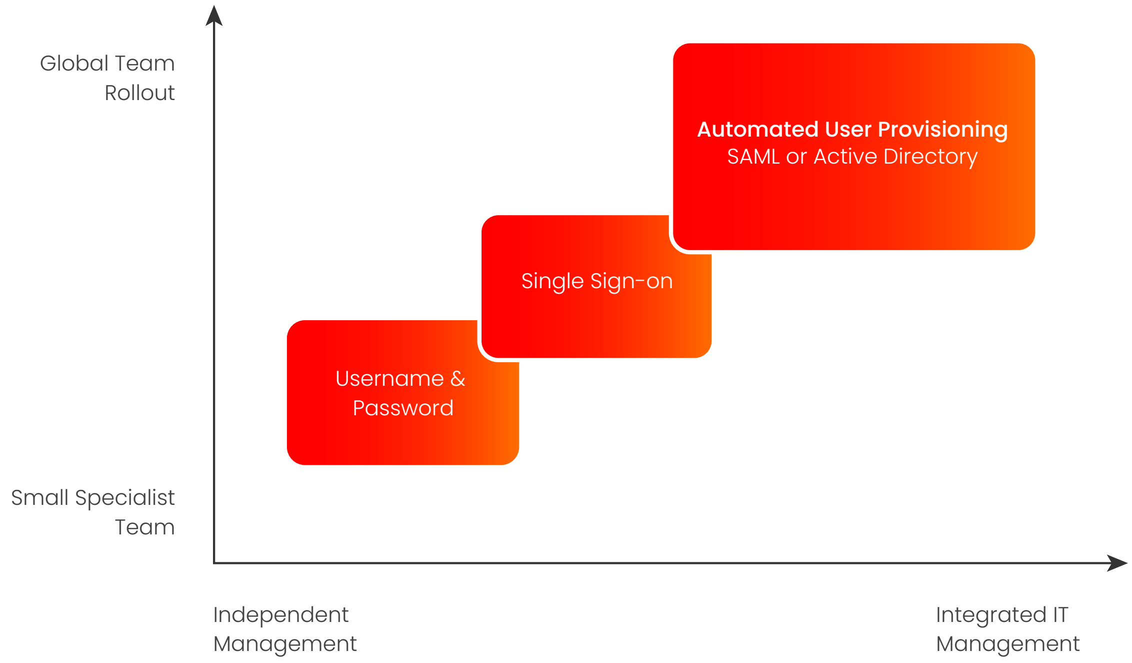


Figure 1: User management options exist for all team sizes and complexity. Recommendations above are based on team size.

No coupling of user management: Users are provisioned manually and authenticate via username and password.

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

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 simplifies username and password management and provides an extra layer of security.

- All user management takes place within the IBC.
- 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.

Tight coupling of user management: User accounts are automatically provisioned, assigned groups and deleted 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 two options:

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.

2 **Active Directory:**

- Users and groups are synchronized with the IBC via an LDAP-capable source.
- This requires adding a Celonis application to your infrastructure and writing LDAP queries that select the appropriate users for your team.

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 IBC 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 code 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.

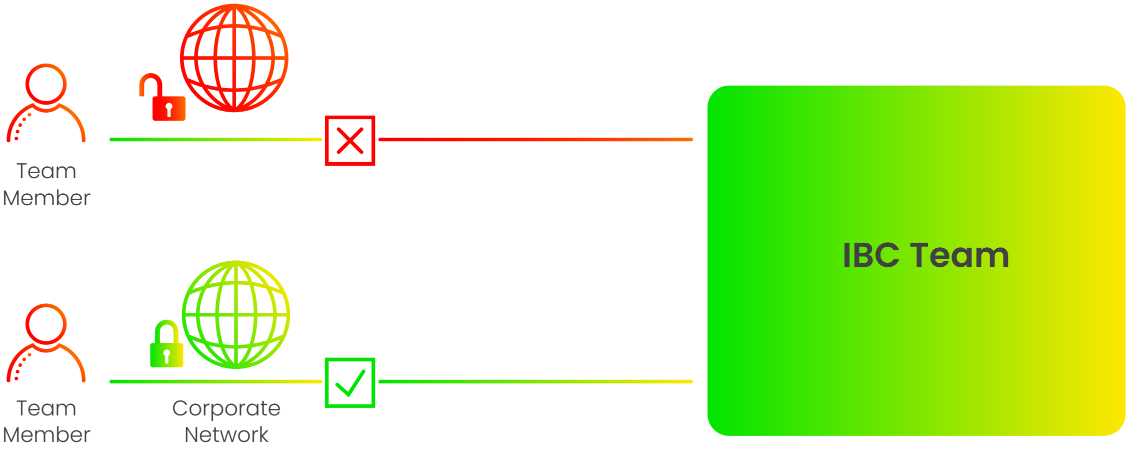


Figure 2: IP Restrictions only allow employees that go through approved IP addresses, such as the Corporate Network IP address to access the system.

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 interacts 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:

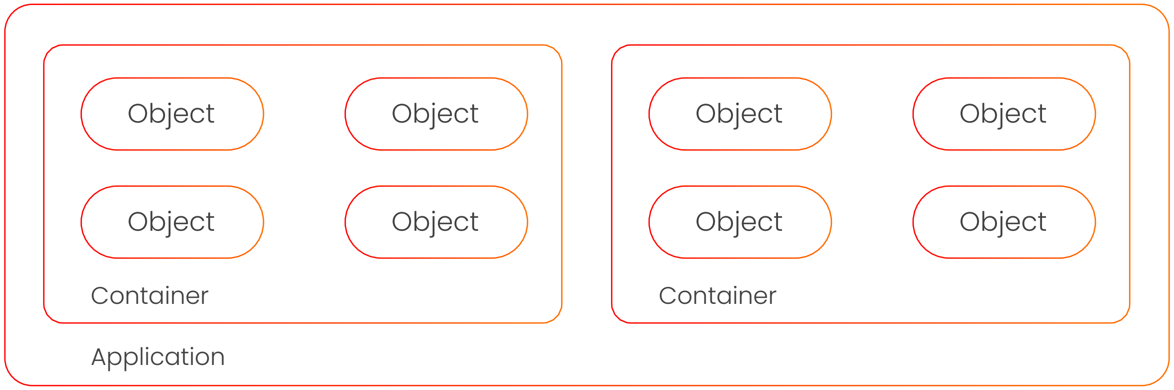
1. **Member** - view content depending on permissions
2. **Analyst** - create / view / edit / delete content depending on permissions
3. **Admin** - create / view / edit / delete content AND team administration

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 IBC 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.

Access Controls
Login Security
User Permissions
Data Permissions
Monitoring and Auditing
Security Responsibilities



Capability	Container	Object
Event Collection	Data Pool	Data Model
Process Analytics	Workspace	Analysis
Action Engine	Project	Skill
Machine Learning	--	App
Process Automation	--	Workflow

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/CIBC/Permission+Management+Overview

Data Permissions

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

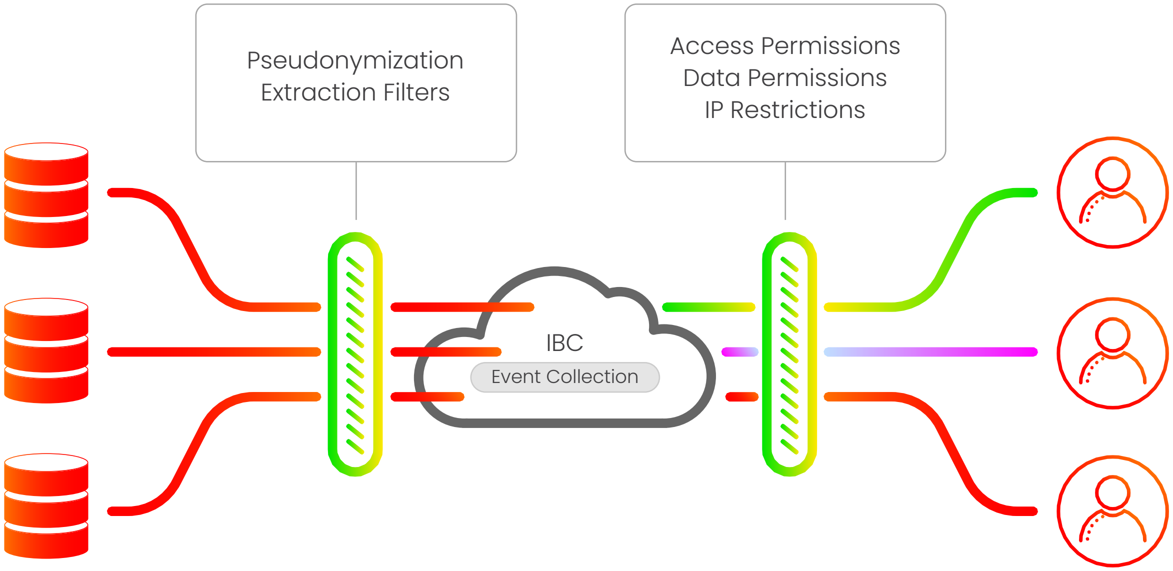


Figure 3: Data protection measures take place before data enters the IBC and when data is visualized to individual users

1 **Before Data is Extracted:**

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

2 **During Data Extraction and Transformation:**

- Limit access to only data engineers via user permissions.

3 **At All Times:**

- Data permissions enforce what specific data a user can see within the Celonis system. 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.
- At All Times: Data is encrypted both in-transit and at-rest.

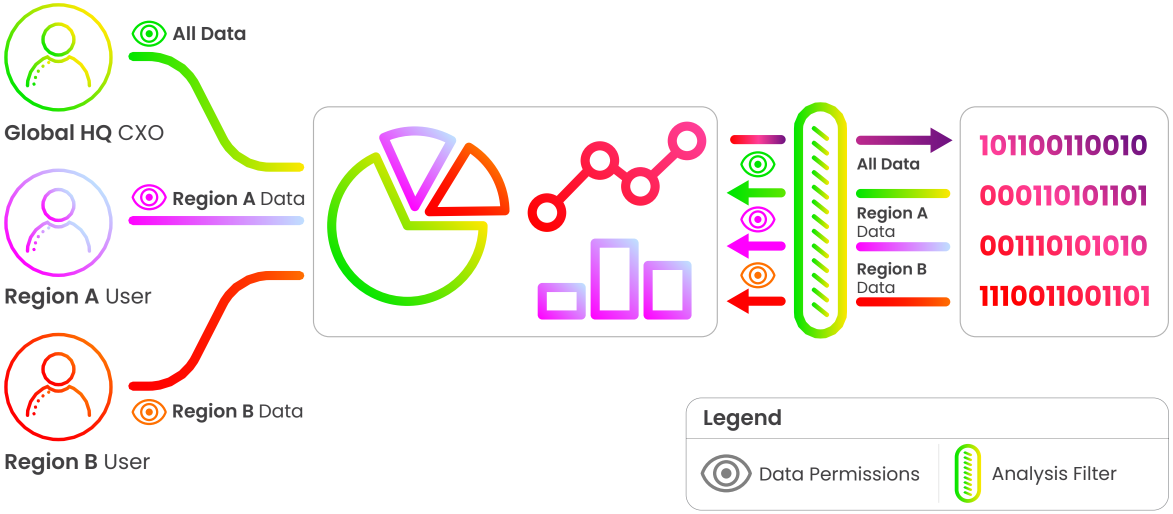
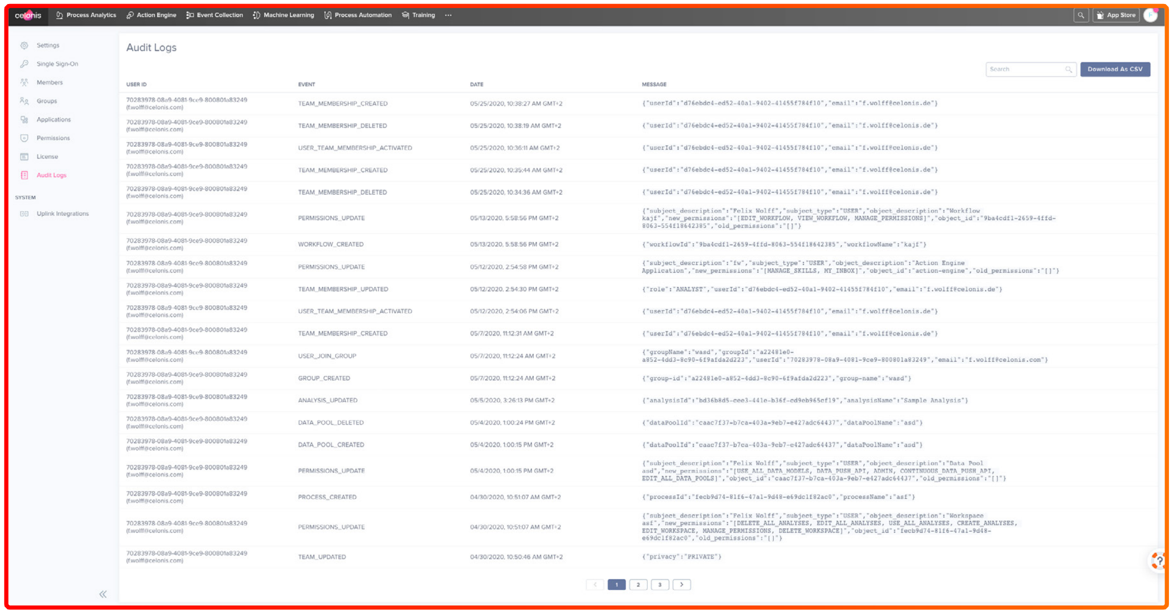


Figure 4: Using data permissions, one analysis can service multiple users. The CXO has all data permissions and will see all data, while regional users will see the same analysis structure with regional data. Additional analysis filters can be applied to further drill into data.

Monitoring and Auditing



Audit Logs

USER ID	EVENT	DATE	MESSAGE
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	TEAM_MEMBERSHIP_CREATED	05/25/2020, 10:38:27 AM GMT+2	{"userId":"d76ebdc4-ed52-40a1-9402-41455f784f10","email":"f.wolff@celonis.de"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	TEAM_MEMBERSHIP_DELETED	05/25/2020, 10:38:19 AM GMT+2	{"userId":"d76ebdc4-ed52-40a1-9402-41455f784f10","email":"f.wolff@celonis.de"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	USER_TEAM_MEMBERSHIP_ACTIVATED	05/25/2020, 10:36:11 AM GMT+2	{"userId":"d76ebdc4-ed52-40a1-9402-41455f784f10","email":"f.wolff@celonis.de"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	TEAM_MEMBERSHIP_CREATED	05/25/2020, 10:35:44 AM GMT+2	{"userId":"d76ebdc4-ed52-40a1-9402-41455f784f10","email":"f.wolff@celonis.de"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	TEAM_MEMBERSHIP_DELETED	05/25/2020, 10:34:36 AM GMT+2	{"userId":"d76ebdc4-ed52-40a1-9402-41455f784f10","email":"f.wolff@celonis.de"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	PERMISSIONS_UPDATE	05/13/2020, 5:58:56 PM GMT+2	{"subject_description":"Felix Wolff","subject_type":"USER","object_description":"Workflow kajf","new_permissions":"[EDIT_WORKFLOW, VIEW_WORKFLOW, MANAGE_PERMISSIONS]","object_id":"9ba4cdf1-2659-4ffd-8063-554f18642385","old_permissions":"[]"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	WORKFLOW_CREATED	05/13/2020, 5:58:56 PM GMT+2	{"workflowId":"9ba4cdf1-2659-4ffd-8063-554f18642385","workflowName":"kajf"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	PERMISSIONS_UPDATE	05/12/2020, 2:54:58 PM GMT+2	{"subject_description":"fw","subject_type":"USER","object_description":"Action Engine Application","new_permissions":"[MANAGE_SKILLS, MY_INBOX]","object_id":"action-engine","old_permissions":"[]"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	TEAM_MEMBERSHIP_UPDATED	05/12/2020, 2:54:30 PM GMT+2	{"role":"ANALYST","userId":"d76ebdc4-ed52-40a1-9402-41455f784f10","email":"f.wolff@celonis.de"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	USER_TEAM_MEMBERSHIP_ACTIVATED	05/12/2020, 2:54:06 PM GMT+2	{"userId":"d76ebdc4-ed52-40a1-9402-41455f784f10","email":"f.wolff@celonis.de"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	TEAM_MEMBERSHIP_CREATED	05/7/2020, 11:12:31 AM GMT+2	{"userId":"d76ebdc4-ed52-40a1-9402-41455f784f10","email":"f.wolff@celonis.de"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	USER_JOIN_GROUP	05/7/2020, 11:12:24 AM GMT+2	{"groupName":"wasd","groupId":"a22481e0-a852-4dd3-8c90-6f9afda2d223","userId":"70283978-08a9-4081-9ce9-800801a83249","email":"f.wolff@celonis.com"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	GROUP_CREATED	05/7/2020, 11:12:24 AM GMT+2	{"group-id":"a22481e0-a852-4dd3-8c90-6f9afda2d223","group-name":"wasd"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	ANALYSIS_UPDATED	05/5/2020, 3:26:13 PM GMT+2	{"analysisId":"bd36b8d5-cee3-441e-b36f-cd9eb965cf19","analysisName":"Sample Analysis"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	DATA_POOL_DELETED	05/4/2020, 1:00:24 PM GMT+2	{"dataPoolId":"caac7f37-b7ca-403a-9eb7-e427adc64437","dataPoolName":"asd"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	DATA_POOL_CREATED	05/4/2020, 1:00:15 PM GMT+2	{"dataPoolId":"caac7f37-b7ca-403a-9eb7-e427adc64437","dataPoolName":"asd"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	PERMISSIONS_UPDATE	05/4/2020, 1:00:15 PM GMT+2	{"subject_description":"Felix Wolff","subject_type":"USER","object_description":"Data Pool asd","new_permissions":"[USE_ALL_DATA_MODELS, DATA_PUSH_API, ADMIN, CONTINUOUS_DATA_PUSH_API, EDIT_ALL_DATA_POOLS]","object_id":"caac7f37-b7ca-403a-9eb7-e427adc64437","old_permissions":"[]"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	PROCESS_CREATED	04/30/2020, 10:51:07 AM GMT+2	{"processId":"fecb9d74-81f6-47a1-9d48-e69dc1f82ac0","processName":"asf"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	PERMISSIONS_UPDATE	04/30/2020, 10:51:07 AM GMT+2	{"subject_description":"Felix Wolff","subject_type":"USER","object_description":"Workspace asf","new_permissions":"[DELETE_ALL_ANALYSES, EDIT_ALL_ANALYSES, USE_ALL_ANALYSES, CREATE_ANALYSES, EDIT_WORKSPACE, MANAGE_PERMISSIONS, DELETE_WORKSPACE]","object_id":"fecb9d74-81f6-47a1-9d48-e69dc1f82ac0","old_permissions":"[]"}
70283978-08a9-4081-9ce9-800801a83249 (f.wolff@celonis.com)	TEAM_UPDATED	04/30/2020, 10:50:46 AM GMT+2	{"privacy":"PRIVATE"}

Figure 5: The built-in Celonis Audit Log functionality.

Access Controls

Login Security

User Permissions

Data Permissions

Monitoring and Auditing

Security Responsibilities

Security is not robust without active monitoring, therefore the IBC 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 (f.wolff@celonis.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":"f.wolff+1@celonis.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:
https://help.celonis.cloud/help/display/CIBC/Audit+Logs

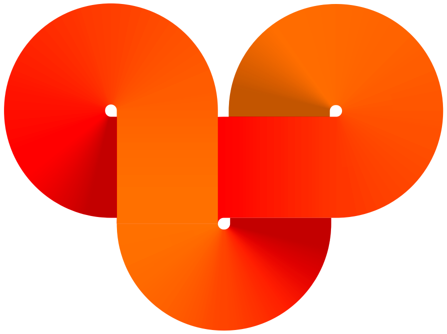
Additional information on Login History Logs:
https://help.celonis.cloud/help/display/CIBC/Login+history

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 Intelligent Business Cloud 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 IBC 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.



Access Controls

Login Security

User Permissions

Data Permissions

Monitoring and Auditing

Security Responsibilities

The below table outlines the distribution of security measures.

Responsibility	Owner		
	Customer	Celonis	Hosting Provider
Customer data management (classification and 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 instance	●		
Employee vetting or screening	●	●	●
Physical security			●

Disclaimer:

This document is protected by copyright laws and contains material proprietary to Celonis SE, its affiliates (jointly "Celonis") and its licensors. The receipt or possession of this document does not convey any rights to reproduce, disclose or distribute its contents, or to manufacture, use or sell anything that it may describe, in whole or in part.

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