



EUROPEAN CENTRAL BANK

EUROSYSTEM

CASPER

FREQUENTLY ASKED QUESTIONS (FAQ)

CASPER – Centralised Submission Platform

EUROPEAN CENTRAL BANK



Contents

1.	About this guide	4
2.	ECB Identity Portal FAQ	4
Q 2.1	<i>I do not have an ECB Identity Portal account. How do I get one?</i>	4
Q 2.2	<i>How do I activate my ECB Identity Portal account?</i>	4
Q 2.3	<i>How do I log in to the ECB Identity Portal?</i>	4
Q 2.4	<i>I am experiencing issues with my account. Who should I contact for support?</i>	4
Q 2.5	<i>How do I update my personal details in the ECB Identity Portal?</i>	4
3.	CASPER FAQ	5
3.1	Access	5
Q 3.1.1	<i>How do I access CASPER?</i>	5
Q 3.1.2	<i>The CASPER tiles are missing from “My Apps”. How do I add them?</i>	6
Q 3.1.3	<i>I can log in to CASPER but I cannot access any data collections.</i>	6
Q 3.1.4	<i>Are roles granted separately for each data collection?</i>	6
Q 3.1.5	<i>How long does it take to gain access to CASPER?</i>	6
Q 3.1.6	<i>Can generic or shared email addresses such as info@... be used to register in CASPER?</i>	7
Q 3.1.7	<i>What is the password policy for CASPER users?</i>	7
Q 3.1.8	<i>Does two-factor authentication apply each time CASPER is accessed?</i>	7
Q 3.1.9	<i>Does CASPER use third-party services? If so, what is the authentication mechanism?</i>	7
Q 3.1.10	<i>What exactly are the services provided by OneWelcome? What security certifications do CASPER service providers have?</i>	7
Q 3.1.11	<i>What is CASPER’s average response time?</i>	7
Q 3.1.12	<i>Do external software providers for CASPER have access to any information stored in the system?</i>	8
3.2	Administration	8
Q 3.2.1	<i>Can a CASPER web data submitter be assigned to parts of a data collection only? Or are collection and entity the only limitations?</i>	8
Q 3.2.2	<i>What policies and procedures govern the change management and configuration management process for CASPER? What is the change management process?</i>	8
Q 3.2.3	<i>What can external participants do or control in the software development lifecycle and configuration change lifecycle?</i>	8
3.3	Audit and compliance	8



EUROPEAN CENTRAL BANK
EUROSYSTEM

Q 3.3.1	<i>Can participating external parties audit CASPER?</i>	8
Q 3.3.2	<i>Is a log kept of all actions performed on an item saved in CASPER?</i>	8
Q 3.3.3	<i>Which logs are made available to CASPER users and how?</i>	8
Q 3.3.4	<i>Are IT security requirements passed on to fourth and fifth parties?</i>	8
Q 3.3.5	<i>Can banks be provided with a copy of the security audit/due diligence/penetration tests performed by the ECB and any other relevant documentation on security?</i>	9
3.4	Business continuity and risk management	9
Q 3.4.1	<i>What is the procedure for detecting, evaluating and managing incidents?</i>	9
Q 3.4.2	<i>What is the process for monitoring events and communicating when incidents such as anomalous use or access abuse occur?</i>	9
Q 3.4.3	<i>Are risk analyses conducted on CASPER services?</i>	9
3.5	Confidentiality	9
Q 3.5.1	<i>What confidentiality regime applies to CASPER?</i>	9
3.6	Data security	10
Q 3.6.1	<i>What safeguards are in place to prevent social engineering?</i>	10



1. About this guide

This document provides answers to general questions on the use of CASPER. The questions have been collected in previous exercises and are organised by the following topics:

- ECB Identity Portal FAQ;
- CASPER FAQ.

It does not provide a step-by-step description of how to use the system and its functionalities. This can be found in the [CASPER web user manual](#).

2. ECB Identity Portal FAQ

Q 2.1 I do not have an ECB Identity Portal account. How do I get one?

Please contact the local delegated user administrator in your organisation or your ECB business counterpart.

Q 2.2 How do I activate my ECB Identity Portal account?

Upon registration you should have received an email containing an account activation link. If you cannot find the email or the link has expired, please follow this link to receive a new activation email: <https://id.ecb.europa.eu/login/help-menu>.

Q 2.3 How do I log in to the ECB Identity Portal?

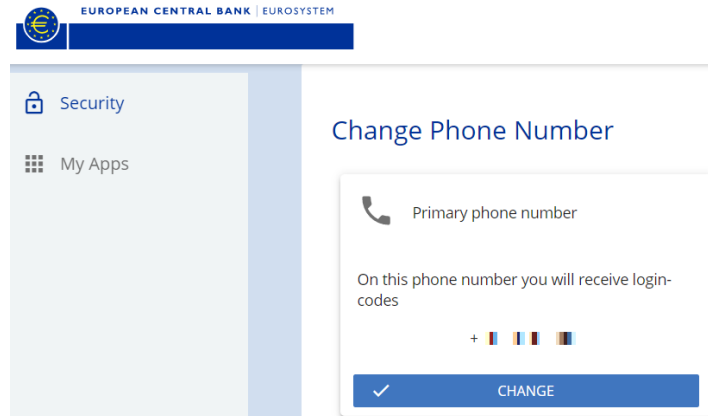
The ECB Identity Portal can be accessed via this link: <https://id.ecb.europa.eu>. The supported browsers are Google Chrome and Microsoft Edge. If you have difficulties accessing this URL, please clear your browsing history and try again.

Q 2.4 I am experiencing issues with my account. Who should I contact for support?

Please contact the ECB Support Centre by email at supportcentre@ecb.europa.eu or by phone on +49 69 1344 7766.

Q 2.5 How do I update my personal details in the ECB Identity Portal?

You can update your phone number by logging in to your profile page in the ECB Identity Portal and navigating to the “Security” tab.



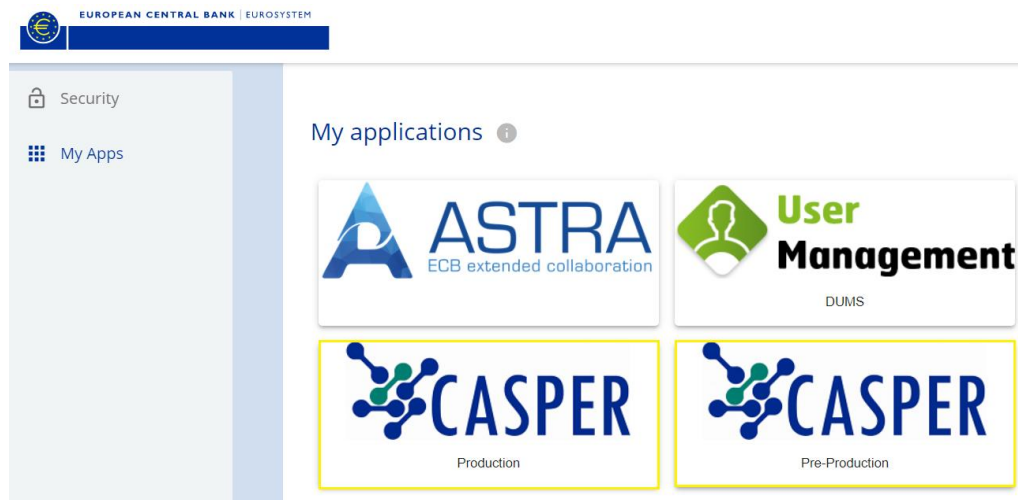
If you cannot log in, or you need to change other details like your email address, please get in touch with your relevant contact person. If access was provided by a local department in your organisation, you will need to contact your delegated user administrator; if access was provided by the ECB, please reach out to your ECB counterpart.

3. CASPER FAQ

3.1 Access

Q 3.1.1 How do I access CASPER?

CASPER can be accessed through the “My Apps” tab by clicking on the CASPER Production or Pre-Production tile (depending on the working environment), as shown below.





EUROPEAN CENTRAL BANK
EUROSYSTEM

Q 3.1.2 The CASPER tiles are missing from “My Apps”. How do I add them?

The delegated access administrator needs to add group memberships. Please contact the local access administrator in your organisation or your ECB business counterpart. Detailed information can be found in the [ECB Identity Portal user manual \(CASPER-specific\)](#).

Q 3.1.3 I can log in to CASPER but I cannot access any data collections.

If you log in to CASPER without having any CASPER roles assigned to a data collection, you will see the message “*The user does not have any CASPER roles assigned*”.

To have access a data collection, a CASPER administrator first needs to assign you a role as web user administrator and/or web data submitter for that collection. Please contact a user administrator or the business counterpart at your central bank or the ECB to have them assign you to the data collection. More information about the responsibilities of each role and for the assignment process can be found in the [CASPER web user manual](#).

Q 3.1.4 I can access a data collection in CASPER through the “Submission tab”, but I do not see any reporting obligations in the submission list.

To view reporting obligations within a data collection, you must be assigned to both the relevant collection and the appropriate reporting entity or entities. If you can access the data collection using the submission tab, but do not see any reporting obligations, please check with your CASPER web user administrator that your entity assignment is correctly configured.

Q 3.1.5 Are roles granted separately for each data collection?

From the moment CASPER roles are granted in the ECB Identity Portal, users appear in CASPER with the associated roles. However, to be able to carry out their tasks, users need to be assigned separately to each data collection required as a web user administrator or/and web data submitter. The effect of the roles is applied at data collection level. More information about roles and the process for assigning and removing data collection users can be found in the [CASPER web user manual](#).

Q 3.1.6 How long does it take to gain access to CASPER?

Typically, it takes several working days to go through the necessary steps. However, in exceptional cases and with good coordination, access for a single user can be obtained within a matter of hours.

The steps involved in granting access to CASPER are as follows:

1. The user provides their credentials (name, phone number and email address) to their delegated user administrator.
2. The delegated user administrator creates the user account.
3. The delegated access administrator assigns the necessary roles to the new user.
4. The user connects to <https://id.ecb.europa.eu/login/> to activate the account, making the account visible in CASPER so that roles can be assigned.
5. The administrator assigns the user to both a data collection and the respective reporting entity. The user now has access to the assigned data collection for the designated reporting entity.



For more information, please refer to the user manual for account activation in the [Banking supervision portal](#).

Q 3.1.7 Can generic or shared email addresses such as “info@...” be used to register in CASPER?

Generic or shared email addresses must not be used, as they prevent access tracing. The email address serves as the unique identifier for the user, so the same address cannot be assigned to more than one user.

Q 3.1.8 What is the password policy for CASPER users?

1. Passwords remain valid for 215 days.
2. Passwords must have at least ten characters.
3. Passwords must include at least three of the following:
 - a) at least one uppercase letter (ABC...);
 - b) at least one lowercase letter (abc...);
 - c) at least one number (12345...);
 - d) at least one special character (!@#\$\$%^&*).
4. Passwords must not contain the first name or surname of the user.
5. Passwords cannot be reused (a history of ten passwords is stored).

Q 3.1.9 Does two-factor authentication apply each time CASPER is accessed?

Yes, two-factor authentication is required for each login.

Q 3.1.10 Does CASPER use third-party services? If so, what is the authentication mechanism?

CASPER consists of the ECB Identity Portal as external authentication mechanism, plus a set of internal ECB services. Authentication between the different components uses secure state-of-the-art protocols. Beyond that, CASPER is not integrated with any other third-party services.

Q 3.1.11 What exactly are the services provided by OneWelcome? What security certifications do CASPER service providers have?

OneWelcome is the identity provider of the ECB Identity Portal.

They are ISO/IEC 27001 certified. Please see [OneWelcome website](#).

IBM Germany (Europe) built the user interfaces. Their certification can be found on their [website](#).

Q 3.1.12 What is CASPER's average response time?

CASPER is designed to ensure a smooth user experience. Browsing usually returns new pages in less than a second. Uploading or downloading large files is normally limited by the bandwidth of the user rather than the performance of the platform.

Q 3.1.13 Do external software providers for CASPER have access to any information stored in the system?

Contractual, technical and operational safeguards have been put in place to prevent external providers from accessing the information stored in CASPER. Only ECB-authorised persons have access to the content in the system.

3.2 Administration

Q 3.2.1 Can a CASPER web data submitter be assigned to parts of a data collection only? Or are collection and entity the only limitations?

Web data submitter(s) can be assigned by data collection and entity level, but not to sub-sections of a data collection. More information about roles and the process of data collection user assignment can be found in the [CASPER web user manual](#).

Q 3.2.2 What policies and procedures govern the change management and configuration management process for CASPER? What is the change management process?

The change management and configuration management processes are the standard ones applied across all solutions used by the ECB. The change management process is in line with industry best practices, which include proper up-front testing and minimising business disruptions.

Q 3.2.3 What can external participants do or control in the software development lifecycle and configuration change lifecycle?

External participants are not involved in these.

3.3 Audit and compliance

Q 3.3.1 Can participating external parties audit CASPER?

External entities are not allowed to audit internal ECB systems.

Q 3.3.2 Is a log kept of all actions performed on an item saved in CASPER?

All security-relevant actions affecting information in CASPER are logged, providing full traceability. Tracked actions for each individual document currently include additions and modifications. Access, downloading, copying, moving, deletions, etc. will be added at a future date.

Q 3.3.3 Which logs are made available to CASPER users and how?

External users of the system do not have access to low-level audit logs/databases.

Q 3.3.4 Are IT security requirements passed on to fourth and fifth parties?

The ECB takes the utmost care to ensure that its IT systems are secure and that the controls protecting the information shared via CASPER are effective, in view of its potentially high sensitivity. This includes comprehensive security assessments before commencing service, contractual agreements stipulating adequate technical and operational security controls for services from the provider, including any sub-



contractors, regular security reviews, audit rights and a suitable exit strategy. However, the ECB does not share details about the security measures it has in place.

Q 3.3.5 Can banks be provided with a copy of the security audit/due diligence/penetration tests performed by the ECB and any other relevant documentation on security?

The ECB takes the utmost care to ensure that its IT systems are secure and that the controls protecting the information shared via CASPER are effective, in view of its potentially high sensitivity. This includes comprehensive security assessments before commencing service, contractual agreements stipulating adequate technical and operational security controls for services from the provider, including any sub-contractors, regular security reviews, audit rights and a suitable exit strategy. However, the ECB does not share details about the security measures it has in place.

3.4 Business continuity and risk management

Q 3.4.1 What is the procedure for detecting, evaluating and managing incidents?

Incident management is a standard operational process built into the ECB's IT and information security processes. The system is closely monitored for security breaches and other operational incidents. Incident management processes are in place to detect and respond to incidents, including investigation, containment and remediation. Service providers are obliged to report any incidents affecting the service to the ECB in a timely manner, and to coordinate their response with the ECB.

Q 3.4.2 What is the process for monitoring events and communicating when incidents such as anomalous use or access abuse occur?

If a security incident occurs, the ECB will contact the relevant stakeholders as part of the incident response process. Stakeholders are informed in a timely manner based on the ECB's incident management procedures.

Q 3.4.3 Are risk analyses conducted on CASPER services?

Yes, the ECB conducts risk assessments at IT and business levels before commencing service and at regular intervals thereafter.

The ECB constantly monitors the risks associated with its IT services, including CASPER. Mitigation measures are proposed and introduced where necessary, with prioritisation based on likelihood and impact of risks if they were to materialise.

One of the main motivations for introducing CASPER is to reduce existing risks inherent in the solutions it replaces. The system significantly reduces risks from the ECB's relationships with its external counterparts, on both a technical level (integrity, confidentiality and availability of information) and an operational level (the automation and approval processes remove a range of potential human mistakes and delays).

3.5 Confidentiality

Q 3.5.1 What confidentiality regime applies to CASPER?

ECB-PUBLIC, ECB-UNRESTRICTED, ECB-RESTRICTED and ECB-CONFIDENTIAL information may be shared via CASPER.



3.6 Data security

Q 3.6.1 What safeguards are in place to prevent social engineering?

The ECB has implemented two-factor authentication to make social engineering harder and provides regular IT security awareness training for all staff. User awareness in external organisations is also essential to avoid falling victim to social engineering.