

ClearstreamXact

Security Guide

ClearstreamXact Security Guide

March 2026

Document number: 6209

Information in this document is subject to change without notice and does not represent a commitment on the part of Clearstream Banking S.A. (referred to hereinafter as Clearstream Banking or CBL), or any other entity belonging to Clearstream International, S.A. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written consent of Clearstream International, S.A.

© Copyright Clearstream International, S.A., (2026). All rights reserved.

Clearstream and Xact File Transfer are registered trademarks of Clearstream International, S.A. S.W.I.F.T. is a registered trademark of the Society for Worldwide Interbank Financial Telecommunication. Windows is a registered trademark of Microsoft Corporation in the United States and other countries. All other trademarks are the property of their respective owners.

Clearstream International, S.A. is a Deutsche Börse Group company.

Security Guide

ClearstreamXact is a suite of connectivity products that gives Clearstream clients real-time access to enhanced information, instruction input, transaction and position reporting.

ClearstreamXact offers secure multi-channel connectivity to Clearstream with a choice of connection via web-browser, file transfer and the Swift network. Whatever your operating or technical environment, ClearstreamXact provides seamless, direct access, giving you adaptable connectivity for your growing business.

About this guide

The purpose of this guide is to assist ClearstreamXact client technical staff to understand the security details with regard to the different options for connectivity.

This guide is organised into chapters dedicated to the individual connectivity channels, as follows:

- [“1. Xact Web Portal”](#) on page 1-1;
- [“2. Xact File Transfer via Internet”](#) on page 2-1.

Each chapter may be further subdivided into areas of general and/or specific subject matter within the respective channel.

Note: For details of the Swift network, please refer to Swift’s proprietary documentation.

Contact details

For technical assistance with ClearstreamXact, please contact Client Service Connectivity Support as follows:

	Luxembourg	Frankfurt	London
Tel:	+352-243-38110	+49-(0) 69-2 11-1 15 90	+44-(0)20-786 27100
Fax:	+352-243-638110	+49-(0) 69-2 11-6 1 15 90	+44 (0) 20-786 27254
Email:	connectlux@clearstream.com	connectfrankfurt@clearstream.com	connectlondon@clearstream.com

You can also consult our website www.clearstream.com under Products and Services/Connectivity for the latest information on ClearstreamXact.

Before contacting Clearstream Banking, please ensure that you have the following information to hand:

- Your organisation name and account number with Clearstream Banking.
- Your telephone number, fax number and email address.
- Details of the problem (please have full details available).
- If you have received an error message, full details of the error, with the error message number.

Clients should note that, as is normal practice within financial organisations, Clearstream Banking has implemented telephone line recording to ensure that the interests of Clearstream Banking and of its clients are protected against misunderstandings or miscommunications.

Areas subject to telephone line recording include Client Services, the Treasury Dealing Room and back office operations. The recorded lines are the subject of an ongoing formal maintenance and quality control programme to ensure their continued effective and appropriate deployment and operation.

Security Guide	i
About this guide	i
Contact details	ii
1. Xact Web Portal	1-1
Registration and initial administrator activation	1-1
Certificate import and user login	1-1
User credentials	1-1
Certificate storage for Xact Web Portal	1-2
Mobile ForgeRock-Authenticator-App	1-2
Certificates	1-2
Password expiry	1-2
Password changes	1-2
Password attempts / blocked	1-3
Network	1-3
OU security settings	1-4
Audit log	1-6
Digital signatures	1-7
Additional client-side recommended security measures	1-7
Penetration test reports	1-7
Data encryption	1-7
2. Xact File Transfer via Internet	2-1
Network	2-1
Integrating with firewalls	2-1

Security Guide

This page has intentionally been left blank.

1. Xact Web Portal

The Xact Web Portal is the interface for the Clearstream Banking online platform to access instruction input, query, reporting and exception handling services.

The application and all associated data is hosted in Luxembourg, Europe.

It is under the oversight of the Commission de Surveillance du Secteur Financier (CSSF -www.cssf.lu), the Luxembourg financial regulator.

Registration and initial administrator activation

Please refer to the [Xact Web Portal User Manual](#).

Certificate import and user login

Please refer to the [Xact Web Portal User Manual](#).

User credentials

Each Xact Web Portal user has the following personal credentials:

- A user password.
- Software certificates to digitally sign operations and transactions when working in Xact Web Portal.
- Mobile App Authenticator if configured.

The certificates are issued by Clearstream Banking's Certification Authority (CA) and certify the two private keys that users generate on their local PC.

ClearstreamXact Security Guide

Certificate storage for Xact Web Portal

Your Xact Web Portal certificates and private keys are safely stored in your browsers IndexedDB. This database is only accessible by xact.clearstream.com and the keys cannot be extracted.

You will have to re-import the backup .p12 with the .p12 password in order to login if:

- Your browser profile is not stored centrally or synchronised after log-off;
- Your browser profile is reset or deleted.

Supported browsers are recent versions of Google Chrome, Microsoft Edge and Mozilla Firefox.

Mobile ForgeRock-Authenticator-App

By default, ClearstreamXact requires 2-factor authentication based on passwords and software certificates. For additional security, a third factor can be added to achieve 3-factor authentication. The third factor relies on an authenticator app (ForgeRock Authenticator) to additionally integrate a shared TOTP secret secured via biometric features (if configured).

For more information about mobile app authentication, please refer to the [Xact web Portal User Manual](#).

Certificates

The certificates received from Clearstream or from the OU Administrator are always temporary certificates, this means they are:

- Only valid for six (6) weeks
- Must be regenerated upon login

When the temporary certificates are regenerated by the user, permanent certificates are received that are valid for two (2) years.

All digital certificates have an expiry date. Before the expiry date is reached the user will be prompted at login to regenerate the certificates, and the new certificates will have an expiry date of two (2) years in the future.

If the certificates are not regenerated before the expiry date the user cannot use the certificates anymore and must contact the OU Administrator to receive new certificates.

Password expiry

The password of the user expires according to the password rules defined in the Xact Web Portal OU properties of the user. When the password has or is going to expire users are prompted at login to change their user password.

Password changes

The user can change their Xact Web Portal user password once per day.

This applies only to permanent passwords, not to temporary passwords, which must be changed at the first login.

Password attempts / blocked

After 10 wrong password attempts, the user's password is blocked and the OU Administrator has to reset the password.

Network

Via Internet the Xact Web Portal is available at <https://xact.clearstream.com>.

The IP address is 194.36.230.129 and the only port used is 443 (the regular SSL port).

The Xact Web Portal web server supports TLS 1.2 and TLS 1.3.

The traffic is regular https and you can use a network proxy server.

OU security settings

My properties					
Service name	Property name	Category	Propagation	Updatable by	Value
User Management					
User Management	Preferred Language	Session	User	All Types of Admin Users	English
User Management	Mobile App Registration	Credentials Types	User	All Types of Admin Users	Optional
User Management	Skip Mobile App Registration	Credentials Types	User	All Types of Users	No

41 Rows | 10 Rows per page

There are a number of configurable security settings on the Organisation Unit level.

- 1. Minimum Password Length**
the minimum number of characters a user password must have.
Possible values:
 - 8 characters
 - 10 characters
 - 12 characters
 - 16 characters
 - 24 characters
 - 35 characters
- 2. Minimum Password Complexity**
The number of character categories from which a user password must be composed, categories are: lower case; upper case; numbers and special characters.
Allowed values are:
 - 3 of 4 constraints
 - 4 of 4 constraints
- 3. Maximum Password Validity Period**
This time is used to calculate how long before users have to change their password.
Allowed values are:
 - 1 month
 - 2 months
 - 3 months
 - 6 months
 - 9 months
 - 12 months

4. Minimum Password History Length

This is the number of previous passwords that users cannot reuse when changing their user password.

Allowed values are:

- 1 password
- 3 passwords
- 5 passwords
- 10 passwords
- 12 passwords
- 15 passwords
- 20 passwords
- 24 passwords

5. Maximum Session Time (screenlock)

This is the time of inactivity after which users are taken back to the login screen to enter their user password to get back into the Xact Web Portal.

Allowed values are:

- 5 minutes
- 10 minutes
- 20 minutes
- 40 minutes
- 60 minutes

6. Risk Based Re-Authentication

If this setting is ON, users must re-enter their user password when performing sensitive operations, for example, releasing an instructions.

- ON
- OFF

7. Mobile App Registration Property

Allowed values are:

- Not Allowed
- Optional
- Required

8. Skip Mobile App Registration Property

Allowed values are:

- Yes
- No

ClearstreamXact Security Guide

9. User Mgt N-eyes principle

If this setting is 4-eyes then all actions in User Management must be confirmed by a second user before they become active.

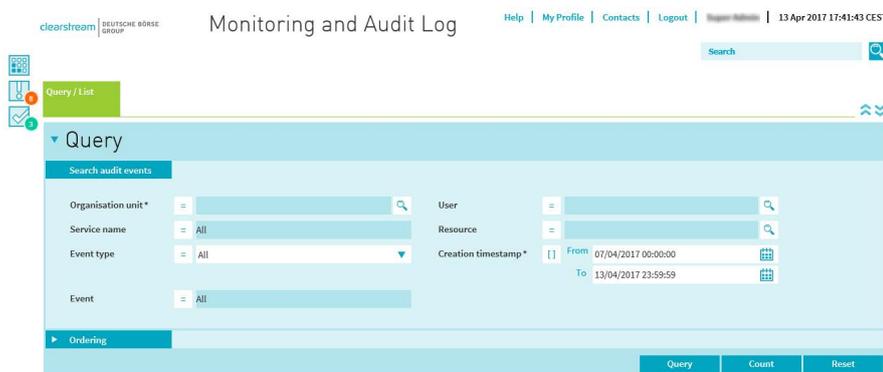
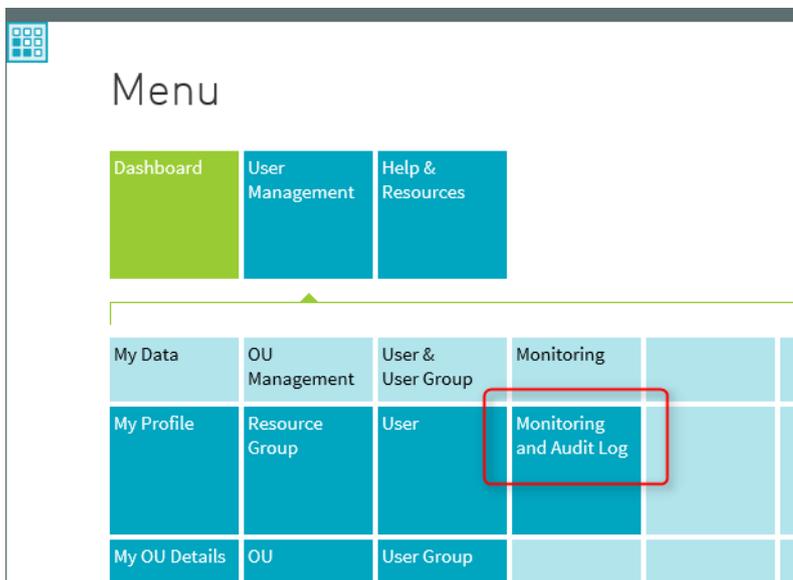
Allowed values are:

- 2-eyes
- 4-eyes

There is a separate N-eyes principle property available for each business service subdomain, for example, Securities Instructions, Cash Instructions, so that you can choose a different eyes level per business service.

Audit log

All actions taken by users in the OU are audited and stored in the Monitoring and Audit Log of the OU. The OU Administrator can access the Audit Log via Xact Web Portal and query the recorded audit events.



Digital signatures

When submitting instructions to Clearstream the instruction data is digitally signed (SHA512) with the private key of your user certificate and the signature is submitted to Clearstream. There your signature is verified and if accepted you will see the following message:



The signature is stored with the instruction for audit purposes.

Additional client-side recommended security measures

It is the user's responsibility to ensure that:

- the Operating System and other software installed is up-to-date and receives the regular security updates;
- they are not logged-in with the administrator account;
- an anti-virus software is running on the PC and anti-virus signatures are updated regularly;
- no software received from unknown sources or via email is installed.

Penetration test reports

The security of the Xact Web Portal application is regularly reviewed by an external security company and the resulting penetration test reports are available on request.

Data encryption

For data in transit a TLS session is established between the browser and web server. All messages pass over this encrypted session. Commercial strength 256-bit keys are used for the encrypted session and no ability to negotiate weak keys is possible.

Data at rest is stored in the application database which is encrypted. In addition it is protected by the highest level of physical security and access to the database is restricted to only a limited number of Clearstream Banking staff who are subject to strict confidentiality agreements.

ClearstreamXact Security Guide

This page has intentionally been left blank.

2. Xact File Transfer via Internet

Xact File Transfer via Internet is a file transfer service that clients can integrate into their own backends or file transfer solutions to automate the sending of instructions and retrieval of reports.

Instruction files are sent via the URL <https://www.cdinternet.com> to Clearstream Banking where they are stored in a client-specific area (the "filestore"). They are then immediately transferred to the Creation platform for clearing and settlement. Reports generated by the Creation platform are stored in the filestore from where you can browse them or save them locally.

By using the Secure Sockets Layer (SSL) over the secure HyperText Transfer Protocol (HTTPS) or secure File Transfer Protocol (FTPs) (RFC 2228), Xact File Transfer via Internet is a highly secure service that is accessible from your desktop, provided that you have access to the public internet from a web browser highly secure service for backend to backend integration.

Certificates to access the application are x.509 certificates with a 4096 bit RSA key, generated by the Xact Web Portal application.

Network

Via Internet the Xact File Transfer service is available at <https://www.cdinternet.com>.

The IP address is 194.36.230.109

Integrating with firewalls

Xact File Transfer via Internet is implemented using internet technologies. It is therefore highly recommended that clients using Xact File Transfer via Internet protect their interior networks from the outside world using a Firewall architecture.

In order to run Xact File Transfer via Internet through a firewall, the following protocols need to be allowed to traverse the firewall:

If HTTP protocol is used

- HTTPS uses TCP port 443 for the initial web site connection and for the interaction with the application.

if FTP protocol is used

- FTP uses TCP port 21 for control;
- FTP uses TCP port 54000 to 55000 for data connection.

if SFTP (SecureSSH) protocol is used

- SFTP uses TCP port 22 for control and data transfer.

ClearstreamXact Security Guide

This page has intentionally been left blank.

Contact

www.clearstream.com

Published by

Clearstream Banking Luxembourg

Registered address

Clearstream Banking S.A.
42, Avenue JF Kennedy
L-1855 Luxembourg

Postal address

Clearstream Banking
L-2967 Luxembourg

March 2026

Document number: 6209
