

CDX Multi-Factor Authentication

Frequently Asked Questions (FAQs)





Table of Contents

General Questions	1
Q1: What is Multi-Factor Authentication?	1
Q2: Why is Multi-Factor Authentication important?	1
Q3: What factors can be used for Multi-Factor Authentication?	1
Q4: Is Multi-Factor Authentication secure?	1
Q5: Is Multi-Factor Authentication time-consuming or inconvenient?	1
Q6: How can I ensure a smooth user experience while using Multi-Factor Authentication?	1
Q7: Does Multi-Factor Authentication impact system performance or response times on CDX?	2
Q8: Are there any additional security measures or recommendations to enhance MFA on CDX?	2
Getting started	2
Q9: Is Multi-Factor Authentication mandatory on the Compliance Data Exchange platform?	2
Q10: How does Multi-Factor Authentication work?	2
Q11: How do I set up Multi-Factor Authentication?	2
Q12: Are there any specific requirements for the passwords used in conjunction with MFA on CDX?	2
Q13: I don't have a company mobile phone. Does this mean I can't use an Authenticator App for One-Time Passwords (OTPs)?	3
Apps and Devices	3
Q14: What should I do if I lose my device with the Authenticator App?	3
Q15: What if I don't have a mobile device? Can I still use Multi-Factor Authentication (MFA)?	3
Q16: Can I use an Authenticator app on multiple devices at the same time? ..	3
Q17: How secure are authenticator apps compared to SMS-based OTPs?	4

General Questions

Q1: What is Multi-Factor Authentication?

Multi-Factor Authentication is a security feature implemented on the Compliance Data eXchange (CDX) platform to provide an additional layer of protection for user accounts. It requires users to provide an additional factor of authentication during login, ensuring a higher level of security and reducing the risk of unauthorized access to sensitive compliance data.

Q2: Why is Multi-Factor Authentication important?

Multi-Factor Authentication is crucial for maintaining the security and integrity of compliance data on the platform. It helps prevent unauthorized access, data breaches, and identity theft by requiring users to provide additional verification beyond just a username and password.

Q3: What factors can be used for Multi-Factor Authentication?

The Compliance Data eXchange platform utilizes a combination of factors for Multi-Factor Authentication. These two factors are included:

- Something you know: username & password
- Something you possess: a mobile device, producing your One-Time Password (OTP)

Q4: Is Multi-Factor Authentication secure?

Yes, Multi-Factor Authentication significantly enhances security. By requiring additional factors beyond just a password, it becomes much more challenging for attackers to gain unauthorized access.

Q5: Is Multi-Factor Authentication time-consuming or inconvenient?

The OTPs authentication method can be completed quickly and easily. The slight inconvenience is a worthwhile trade-off for enhanced security.

Q6: How can I ensure a smooth user experience while using Multi-Factor Authentication?

To ensure a smooth user experience, it is recommended to educate users about the benefits of Multi-Factor Authentication, provide clear instructions on setup and usage, and offer support resources for any issues or questions that may arise.



Q7: Does Multi-Factor Authentication impact system performance or response times on CDX?

While Multi-Factor Authentication adds an additional step to the authentication process, there is no impact on system performance or response times within the application.

Q8: Are there any additional security measures or recommendations to enhance MFA on CDX?

Alongside Multi-Factor Authentication, it is recommended to follow best practices such as regularly updating software and devices, using secure networks, and being cautious of phishing attempts.

Getting started

Q9: Is Multi-Factor Authentication mandatory on the Compliance Data Exchange platform?

Yes, Multi-Factor Authentication is mandatory on the Compliance Data eXchange platform to ensure the highest level of security for compliance data. It is a vital requirement to meet regulatory standards and protect sensitive information.

Q10: How does Multi-Factor Authentication work?

When enabling Multi-Factor Authentication, users will be prompted to set up an additional authentication method. For CDX, this requires using an authenticator app on a mobile device to create One-Time passwords (OTPs). During login, users will be required to provide the additional factor in addition to their username and password.

Q11: How do I set up Multi-Factor Authentication?

To set up Multi-Factor Authentication, follow the step-by-step instructions provided on our CDX Webpage. The setup process is straightforward and ensures your account is well-protected.

Q12: Are there any specific requirements for the passwords used in conjunction with MFA on CDX?

Yes, strong and unique passwords should be used in combination with Multi-Factor Authentication for optimal security. Avoid using easily guessable passwords and consider using password manager tools to assist in generating and managing secure passwords.



Q13: I don't have a company mobile phone. Does this mean I can't use an Authenticator App for One-Time Passwords (OTPs)?

No, you can still use an Authenticator App on any personal device, like your smartphone or tablet. These apps enhance security through Multi-Factor Authentication (MFA) and do not compromise your phone's privacy or security. They also don't require internet access to generate OTPs.

Apps and Devices

Q14: What should I do if I lose my device with the Authenticator App?

If you lose your device with the Authenticator App, you need to contact your Company Administrator or the Service Desk immediately to reset your One-Time Password (OTP). They will assist you in reconfiguring your MFA settings. For detailed instructions, please refer to this link: [MFA reset](#).

Q15: What if I don't have a mobile device? Can I still use Multi-Factor Authentication (MFA)?

Yes, you can still use MFA without a mobile device by utilizing PC-based password wallet solutions like Enpass, KeePass or other similar applications. These tools can generate One-Time Passwords (OTPs) and provide the same level of security as mobile Authenticator Apps.

Storing both your passwords and OTP generator in the same password wallet can be convenient, however it does have potential downsides. Here are a few considerations:

- **Single Point of Failure:** If your password wallet is compromised, both your passwords and OTPs could be exposed, potentially giving an attacker access to your accounts.
- **Device Dependency:** If you lose access to the device where your password wallet is stored, you might find it difficult to recover both your passwords and OTPs.
- **Security Best Practices:** It's generally recommended to separate your authentication methods to reduce risk. Using a mobile device for OTPs and a password manager on your PC can provide an extra layer of security.

Q16: Can I use an Authenticator app on multiple devices at the same time?

Yes, many Authenticator apps allow you to synchronize your accounts on multiple devices. This can be helpful if you want to have a backup device. Make sure you set up the synchronization correctly and keep your backup codes safe.

Q17: How secure are authenticator apps compared to SMS-based OTPs?

Authenticator apps are generally more secure than SMS-based OTPs as they are not vulnerable to SIM swapping attacks and do not require an internet connection. They generate OTPs directly on your device and provide an extra layer of security.