Security and Privacy

Security

At Conflux we know that your data is extremely important to you, your business and your customers. The team at Conflux work continuously to protect the privacy, security and integrity of your account and data. The security of your information is required for our success as a business and we take steps every day to ensure that it remains safe.
Here, we describe our processes for maintaining security throughout Conflux.

Physical Location Security

We ensure that the machines within the Conflux network are protected at all times. Conflux is hosted on servers that are owned and operated by Amazon Web Services (AWS). AWS is an industry leader and provides a highly scalable cloud computing platform with end-to-end security and privacy features as standard.
Access to these data centres is strictly controlled and monitored using a variety of physical controls, intrusion detection systems, environmental security measures, 24 x 7 on-site security staff, biometric scanning, multi-factor authentications, video surveillance and other electronic means. All physical and electronic access to data centres by AWS employees is authorized strictly on a least privileged basis and is logged and audited routinely.
AWS maintains a large list of reports, certifications and independent assessments — including ISO 9001, PCI DSS Level 1, SOC1, SOC2, SOC3 and more — to ensure complete and ongoing state-of-the-art data centre security. You can find out more about data security at AWS here: https://aws.amazon.com/security/ and here: https://aws.amazon.com/compliance/
Conflux employees do not have physical access to our AWS servers. Electronic access to AWS servers and services is restricted to a core set of approved Conflux staff only.

Data Security

Passwords
All passwords are filtered from our logs and are one-way encrypted in the database.
Conflux staff cannot view your password. If you forget your password, you must go through the reset procedure for your account to be accessible again.
Third-Party Credentials
Credentials such as passwords, OAuth tokens and API keys may be required to access third party services. These Credentials are also encrypted and stored in our database. You can completely revoke Conflux's access to a service at any time.
Data Redundancy and Backups
We ensure that all practice data is replicated and regularly backed up.

Application, Systems and Software Security

We have implemented strong encryption via TLS throughout our application. By using encryption, we minimize the chances of someone possibly intercepting username-password combinations and/or other sensitive information.

We adhere to industry best practices to prevent gaps in the security policy of the application and the underlying systems and to prevent common web attack vectors.
Conflux also maintains a robust application audit log to include security events such as user log in and data changes.
We ensure that our software and its dependencies are up to date eliminating any potential security vulnerabilities. We employ a wide range of monitoring solutions for preventing and eliminating attacks to the site.

Communications Security

All Conflux application communications are encrypted over SSL which cannot be viewed by a third party and is the same level of encryption used by banks and financial institutions.

Security and Privacy Features Available in Conflux

The highest security risk to any system is usually the behavior of its users. We provide you with the tools you need to protect your own data. These Conflux features have been designed keeping in mind stringent, enterprise-level security requirements.
User Account Security
We provide a role-based administration system for user accounts.

Employee Access and Security

We regard your data stored within Conflux as private and confidential to your business and users. Our production environment is completely isolated from the other environments — including development and testing.
Conflux employees are granted access to systems and data based on their role in the company or on an as-needed basis.
Access to your data by Conflux employees is only used to assist with support and to resolve customer issues. When working on a support issue we do our best to respect your privacy as much as possible and only access the minimum data needed to resolve your issue.

Maintaining Security

Conflux adheres to industry best practices for design and development. We thoroughly test new features in order to rule out potential attacks such as CSRF, XSS, SQLI and many more.
We continuously improve our security policies as the threat landscape changes. Our engineering team continuously monitors ongoing security, performance and availability. We subscribe to all relevant security bulletins so that we can promptly address any security issues in the software we use.

Need to report a security vulnerability?

If you believe you have found a security vulnerability in Conflux we encourage you to make this known to us right away. We will investigate all legitimate reports and will address the issue immediately. Responsible submission of security vulnerabilities can be made to security@cnflx.io by following the guide below.
Reporting

Share the details of any suspected vulnerabilities with Conflux's Security Team by contacting us at security@cnflx.io.
Please do not publicly disclose these details without express written consent from Conflux. In reporting any suspected vulnerabilities, please include the following information:

- Vulnerability details with information to allow us to efficiently reproduce your steps
- Your email address

Our Commitment
If you identify a verified security vulnerability in compliance with our Responsible Disclosure Policy, we commit to:

- Promptly acknowledge receipt of your vulnerability report
- Provide an estimated timetable for resolution of the vulnerability
- Notify you when the vulnerability is fixed