API credentials overview

Coro REST API credentials can be generated from within the Coro Security Platform. This functionality includes several components that enhance the overall security when generating API credentials:

- API credential names.
- API credential expiration dates.
- Ability to rotate between up to 10 active sets of API credentials.
- Ability to see when a token was last generated from a set of API credentials.
- Ability to revoke existing API credentials.

API credential rotation offers enhanced security and mitigates the risk of unauthorized access to sensitive systems and data. By regularly changing API credentials, organizations can limit the exposure window for potential attackers who may have obtained old or compromised credentials. This practice also aligns with security best practices, ensuring that only authorized users or applications have access to critical APIs, reducing the likelihood of security breaches, and enhancing overall data protection and system integrity.

Setting API credential expiration dates provides an additional layer of security and control. It ensures that access permissions are time-limited, reducing the risk of long-term unauthorized access.

Note

Existing API credentials generated by Coro support have no expiration date. In order for your API credentials to expire, you must generate new credentials.

To learn more about creating API credentials, see **Creating API credentials**.

To learn more about deleting API credentials, see **Deleting API credentials**.