RIPE NCC

RIPE NCC Access SSO Account Authentication and Security Key Management Policy

Author: RIPE NCC
Document ID: ripe-843
Date: May 2025

---

1. Introduction

1.1 Purpose

This policy defines clear guidelines and standardised procedures for RIPE NCC Access account (Single Sign-On) authentication and API key creation. By aligning with industry best practices, it aims to strengthen account security and minimise the risk of unauthorised access.

1.2 Scope

This policy applies to all RIPE NCC Access account (SSO) holders and individuals creating a new RIPE NCC Access account (SSO), including LIR Portal users who require access to their LIR account to manage their IP resources, RPKI, and other related services. It includes clients, vendors, contractors, and third-party partners who use RIPE NCC Access accounts (SSO) to access the RIPE NCC's services.

2. Policy Statements

2.1 RIPE NCC Access (SSO) account requirements and rules

2.1.1 Users

- Anyone can create a RIPE NCC Access (SSO) account.

2.1.2 Two-Factor Authentication

- It is mandatory to enable two-factor authentication (2FA) on an SSO account. 2FA can be set up using a Time-based One-Time Password (TOTP). This is a method of 2FA that uses a unique code using an app which is generated based on the current time. Time-based One-Time Password (TOTP) or hardware/software passkeys can also be used to set up 2FA.

2.1.3 Email addresses

- Changing email addresses on an active RIPE NCC Access (SSO) account is not possible. This action has been disabled for users to perform themselves for security reasons.
    - Users will need to contact the RIPE NCC if changing emails is necessary.
- Email addresses previously used to register RIPE NCC Access (SSO) accounts cannot be used for new accounts.

2.1.4 Usernames

- Usernames are intended to be for one person.
- Sharing of usernames and login credentials is not advised.

2.2 Passwords

- Minimum password length is 14 characters.
- It is recommended that users change their passwords annually but password rotation will not be enforced.
    - The RIPE NCC will reset a password if there is reason to believe a password has been compromised.
        - If a user believes that their password has been compromised, they should reset their password.
    - A user without two-factor authentication cannot reset their password themselves. To do so, a user must contact the RIPE NCC to start the process. The RIPE NCC will request that the user perform an ID validation check and other due diligence checks. The ID validation checks are performed by our third party, IDenfy.

3. API Keys

API keys are subject to specific rules and requirements that must be strictly adhered to.

- API Keys can only be created by users with RIPE NCC Access (SSO) accounts and must not be shared with another SSO account holder or a person who is not an SSO account holder.
- All API keys must be at least 24 characters long and consist of letters and numbers, along with some special characters. Dashes ('-') and underscores ('_') are excluded from length calculations, and may be used for formatting and readability.
    - API keys will be stored as unique identifiers to keep them unique and to prevent collisions.
- API keys will have a maximum lifetime of one year.

- The RIPE NCC will send a notification email to the account owner of the associated API key two weeks before the API key expiration date and on the day of expiry.
- API keys are linked to a specific user’s account, when an SSO account is disabled, or when a user is removed as an account maintainer in the business application database where API key data is stored, the API key will be deactivated.