

Managing VPN Profiles

Version 1.0.0 | Updated 2026-09-05 | 1 min read

Preparation / invited access

In this guide: [Before you start](#) | [Steps](#) | [Verify the result](#) | [Help and related information](#)

Profiles contain machine credentials and routing rules. They must remain separate from human sign-in passwords.

Before you start

Use the access and features actually assigned to your account. Keep a rollback or recovery route before changing existing service settings.

Steps

1. Label the device and intended route clearly.
2. Store the profile in the supported client or protected local storage.
3. Use a unique profile for each device so a lost device can be revoked independently.
4. After replacement or revocation, test both the new access and rejection of the old profile.

Verify the result

Only the intended device profile works. Do not post configuration files or private keys in support conversations.

Help and related information

Contact support, service status, and Customer Access. Never send passwords or recovery codes.