

Managing SSH Keys

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](#)

An SSH public key may be supplied for access. The private key stays on a device or protected key store you control.

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. Create a dedicated supported key with a passphrase, for example using ssh-keygen with the ed25519 key type.
2. Give the onboarding workflow only the public key file ending in .pub.
3. Test the key while keeping an existing recovery path available.
4. Revoke a lost key through the supported control or authorized_keys management, then test that it no longer works.

Verify the result

The new key authenticates and a revoked key is rejected. Keep private keys out of tickets, demos, shared folders and source control.

Help and related information

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

OpenSSH key-generation manual.