Creating SSH Keys in Windows

General Notes

SSH keys can be easily generated in Windows, using PuttyGen.

See this article for an update based on obsolete SHA-1 RSA key usage: Ubuntu 22.04 SSH the RSA key isn't working since upgrading from 20.04

Based on the obsolescence of RSA keys in Ubuntu, it is advised to use ECDSA keys instead.

Needed Tooling

This tutorial uses PuttyGen to create SSH keys in Windows. So, download and install it if needed.
PuttyGen can be downloaded, here: PuTTYgen Download

Good SSH Key Conventions

Here are some good conventions to follow for key security and easy maintenance:

User Keys

Each user should have their own SSH keys. No sharing for obvious reasons.

If a user is fired or leaves, only the keys identified for that user need to be revoked.

Again. No sharing keys between users.

Client Devices

An SSH key should be created for each client device that a user connects from.

Having a unique set of keys for each client device compartmentalizes the risk of a lost or stolen device. Specifically, when a user’s laptop or phone is lost or compromised, only the SSH keys on that device need to be revoked. Other keys for that user remain unaffected.

Don’t use ssh keys creation for one device on another device. Don’t share them between clients! Sharing keys across clients does several things:

- It prevents the remote endpoint from accurately identifying the client.
- If a client is compromised, it is harder to identify and isolate the keys that need to be revoked for the compromised client.

SSH Key Naming

See this page for naming convention: SSH Key Naming Convention

---

Revision #1
Created 1 August 2025 07:49:25 by glwhite
Updated 1 August 2025 09:00:12 by glwhite