Authenticating to Linux Server with SSH Keys

Once you have configured the server with SSH key authentication, you can follow this to attempt connection.

> NOTE: Using SSH key authentication does not require a password for the remote account.

From a Linux host, use this:

```
ssh username@remote_host
```

If this is your first time connecting to this host (if you used the last method above), you may see something like this:

```
OutputThe authenticity of host '203.0.113.1 (203.0.113.1)' can't be established.
ECDSA key fingerprint is fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.
Are you sure you want to continue connecting (yes/no)? yes
```

This means that your local computer does not recognize the remote host. Type “yes” and then press `ENTER` to continue.

If you did not supply a passphrase for your private key, you will be logged in immediately.

If you supplied a passphrase for the private key when you created the key, you will be prompted to enter it now.

> NOTE: your keystrokes will not display in the terminal session for security.

After authenticating, a new shell session should open for you with the configured account on the remote server.

Revision #1
Created 1 September 2025 06:41:07 by glwhite
Updated 1 September 2025 06:44:20 by glwhite