SSH credentials

# SSH credentials#

You can use these credentials to authenticate the following nodes:

• SSH

## Prerequisites#

• Create a remote server with SSH enabled.

• Create a user account that can ssh into the server using one of the following:  
Their own password  
An SSH private key

ssh

• Their own password

• An SSH private key

## Supported authentication methods#

• Password: Use this method if you have a user account that can ssh into the server using their own password.

ssh

• Private key: Use this method if you have a user account that uses an SSH key for the server or service.

## Related resources#

Secure Shell (SSH) protocol is a method for securely sending commands over a network. Refer to Connecting to GitHub with SSH for an example of SSH setup.

## Using password#

Use this method if you have a user account that can ssh into the server using their own password.

ssh

To configure this credential, you'll need to:

• Enter the IP address of the server you're connecting to as the Host.

• Enter the Port to use for the connection. SSH uses port 22 by default.

22

• Enter the Username for a user account with ssh access on the server.

ssh

• Enter the Password for that user account.

## Using private key#

Use this method if you have a user account that uses an SSH key for the server or service.

To configure this credential, you'll need to:

• Enter the IP address of the server you're connecting to as the Host.

• Enter the Port to use for the connection. SSH uses port 22 by default.

22

• Enter the Username of the account that generated the private key.

• Enter the entire contents of your SSH Private Key.

• If you created a Passphrase for the Private Key, enter the passphrase.  
If you didn't create a passphrase for the key, leave blank.

• If you didn't create a passphrase for the key, leave blank.