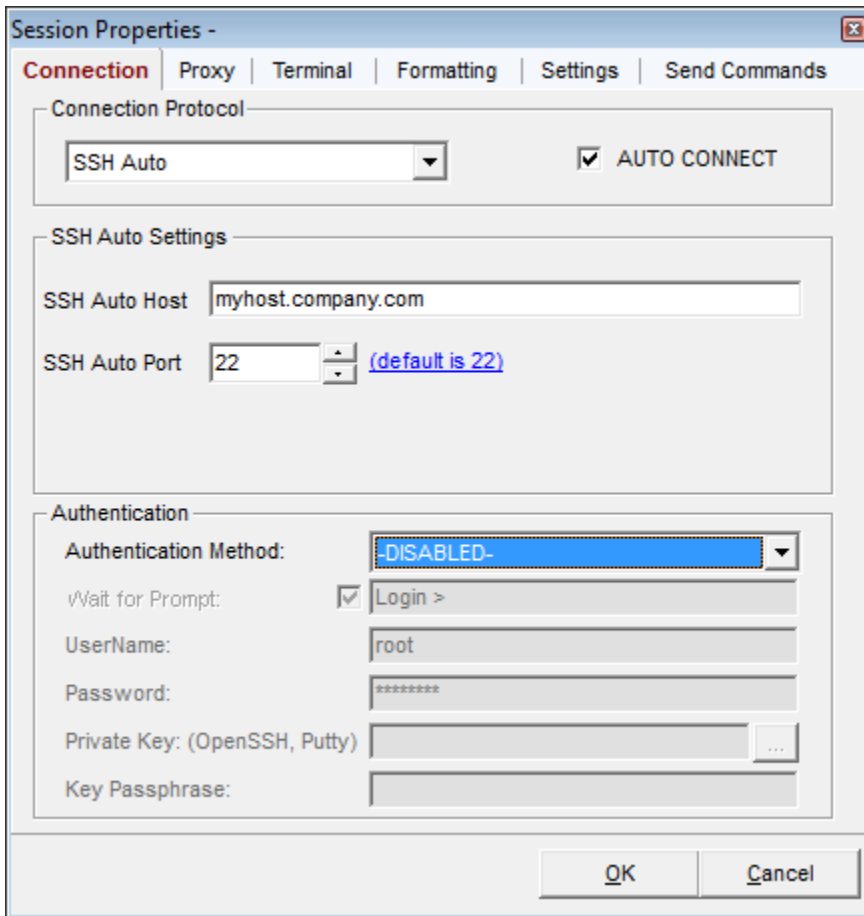


SSH Connection Settings

SSH Connection Settings

Each of the [Secure Shell](#) connection options: SSH1, SSH2, SSH AUTO use the same configuration dialog and settings.



(For more information on other session property configuration tabs, please see [Session Properties](#).)

The following SSH configuration settings are available to properly setup your device connection and terminal session.

Setting	Description
Auto Connect	If this option is enabled, then the terminal session will attempt to establish a connection immediately when opened in Indigo.
SSH Host	The SSH server/host should be provided in this configuration field. This entry can be an IP address, computer name, or DNS hostname.

SSH Port

The SSH server/host port can be used if a custom SSH port must be provided.
(The default port for the SSH protocol is port 22.)

SSH Connection Authentication Options

When using a SSH connection, Indigo can provide an option for automated password authentication.
(The SSH protocol intrinsically supports authentication as part of the protocol.)

Authentication

Authentication Method: Password (connection) ▼

Wait for Prompt: Login >

UserName: root

Password: *****

Private Key: (OpenSSH, Putty) ...

Key Passphrase:

Authentication

Authentication Method: Private Key & Password ▼

Wait for Prompt: Login >

UserName: root

Password: *****

Private Key: (OpenSSH, Putty) ...

Key Passphrase:

Setting

Description

Authentication Method

This option allows you to set the session authentication method. For SSH connections, Indigo supports the following options:

Authentication Method	Description
None	No authentication method is applied.
Password (connection)	Use this option to provide basic username and password credentials to the SSH server/host. <i>(This is a protocol based implementation, where the user credentials are negotiated as part of the SSH protocol at the time of connection.)</i>
Private Key	Use this option when required to use private key encryption to connect to the SSH server/host.
Private Key & Password	Use this option when required to use private key encryption and user credentials to connect to the SSH server/host.

Username

This is the user name that Indigo will provide when authenticating with the SSH server/host.
(This option is only available when using the Password or Private Key & Password authentication methods)

Password

This is the password that Indigo will provide when authenticating with the SSH server/host.
(This option is only available when using the Password or Private Key & Password authentication methods)

Private Key

This option allow you to select the private key file (*.PPK) to be used when negotiating authentication with the SSH server/host.
(This option is only available when using the Private Key or Private Key & Password authentication methods)

Key Passphrase

This option allow you to provide a private key passphrase to be used when negotiating authentication with the SSH server/host.

This field can remain empty if your private key file does not require a passphrase.

(This option is only available when using the Private Key or Private Key & Password authentication methods)