# AN 939: JTAG Connections Over SSH

Updated for Intel® Quartus® Prime Design Suite: **21.2**

# Contents

# 1. JTAG Connections Over SSH

Intel® Quartus® Prime software provides a JTAG Server that enables JTAG connectivity over TCP/IP with Intel FPGA devices for client applications such as the Intel Quartus Prime Programmer, System Console and Debugging Toolkits, and Signal Tap logic analyzer. Communication between the JTAG Server and client is not encrypted.

To secure JTAG communication with encryption, ensure that JTAG connections use SSH tunneling, also called SSH port forwarding.

Typically, SSH tunnels are established with the `ssh` command on Linux* operating systems and with the PuTTY utilities on Windows* operating systems.

This publication shows you how you can use SSH tunnels to securely connect JTAG servers and clients on different host machines. Local SSH loops (SSH server and client on the same machine) are not supported for JTAG communication.

After you have established your SSH tunnel, you can use any Intel Quartus Prime utility that uses a JTAG connection as you usually would.

## 1.1. SSH Server and SSH Client Prerequisites

The instructions in this publication assume that you have installed and configured an SSH server on the remote machine and an SSH client on the local machine.

SSH servers are typically provided with Linux operating systems (`sshd`) but not Windows operating systems. You must install and configure the SSH server software on your systems before you continue.

This publication uses the `ssh` utility (on Linux operating systems) or the PuTTY ssh utility (on Windows operating systems) as SSH clients.

The instructions in this document assume that the remote machine hosts the SSH server, while the local machine runs the SSH client. Either the remote or local machine can have the FPGA board installed.

SSH software installation and configuration for SSH clients and SSH servers is outside of the scope of this document. Refer to your SSH software documentation for installation and configuration instructions.

Intel Corporation. All rights reserved. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Intel warrants performance of its FPGA and semiconductor products to current specifications in accordance with Intel's standard warranty, but reserves the right to make changes to any products and services at any time without notice. Intel assumes no responsibility or liability arising out of the application or use of any information, product, or service described herein except as expressly agreed to in writing by Intel. Intel customers are advised to obtain the latest version of device specifications before relying on any published information and before placing orders for products or services.
*Other names and brands may be claimed as the property of others.

ISO
9001:2015
Registered

## 1.2. Filepath Variables Used in this Publication

In this publication, <*quartus_installdir*> refers to the location where you installed Intel Quartus Prime Design Suite.

The default Intel Quartus Prime Design Suite installation location depends on your operating system:

| | |
|---|---|
| *Linux* | `/home/<username>/intelFPGA_pro/<version>` |
| *Windows* | `C:\intelFPGA_pro\<version>` |

# 2. SSH Tunnels and the JTAG Server

The Intel Quartus Prime JTAG Server communicates with your FPGA hardware and allows multiple Intel Quartus Prime tools to use JTAG resources at the same time. Typically, the JTAG Server is run automatically as a Windows service or a Linux daemon.

By default, the JTAG Server listens to TCP/IP port 1309, and JTAG client applications connect to the same port.

Intel Corporation. All rights reserved. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Intel warrants performance of its FPGA and semiconductor products to current specifications in accordance with Intel's standard warranty, but reserves the right to make changes to any products and services at any time without notice. Intel assumes no responsibility or liability arising out of the application or use of any information, product, or service described herein except as expressly agreed to in writing by Intel. Intel customers are advised to obtain the latest version of device specifications before relying on any published information and before placing orders for products or services.
*Other names and brands may be claimed as the property of others.

ISO
9001:2015
Registered

# 3. Securing JTAG Communication with SSH

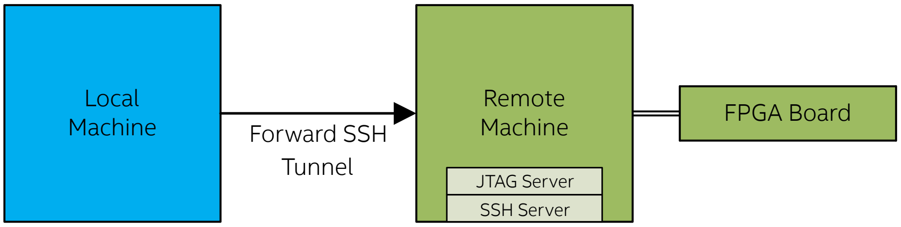
Use SSH to encrypt communication between the Intel Quartus Prime JTAG Server and JTAG clients such as the Intel Quartus Prime Programmer.

Two scenarios are supported for JTAG communication with SSH tunnels:

- Remote machine has the FPGA board attached

  In this scenario, the SSH server and JTAG Server run on the remote machine, while the SSH client and JTAG clients run on the local machine. This scenario is called *SSH tunneling* or *SSH local port forwarding*.

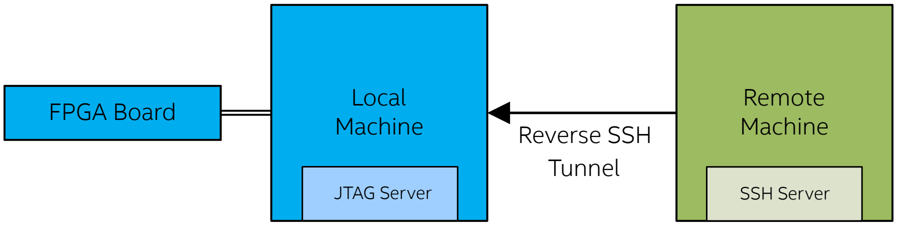
  The following block diagram is a simplified representation of this scenario:



- Local machine has the FPGA board attached

  In this scenario, the SSH client and JTAG Server run on the local machine, while the SSH server and JTAG clients run on the remote machine. This scenario is called *reverse SSH tunneling* or *SSH remote port forwarding*.

  The following block diagram is a simplified representation of this scenario:



Establishing an SSH tunnel between the JTAG Server and JTAG clients ensures that communication between them is encrypted and better protected from network eavesdropping.

Intel Corporation. All rights reserved. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Intel warrants performance of its FPGA and semiconductor products to current specifications in accordance with Intel's standard warranty, but reserves the right to make changes to any products and services at any time without notice. Intel assumes no responsibility or liability arising out of the application or use of any information, product, or service described herein except as expressly agreed to in writing by Intel. Intel customers are advised to obtain the latest version of device specifications before relying on any published information and before placing orders for products or services.
*Other names and brands may be claimed as the property of others.

To prepare your machines to establish an SSH tunnel for secure JTAG communication, complete the following prerequisites:

1. Ensure that you are using the most recent version of SSH server and client software to ensure that they have all the latest security updates.
2. Ensure that you have your SSH server software configured and running on the remote machine.
3. Ensure that you have an SSH client installed and configured on the local machine.
4. Ensure that your SSH server and SSH client are on different machines. Having the SSH client and server run on the same machine is not supported for JTAG communication.

   For these instructions, the remote machine runs the SSH server and the local machine runs the SSH client.

After you completed these prerequisites, you can continue with one of the following procedures:

- Secure your JTAG communication with an SSH tunnel.
- Secure your JTAG communication with a reverse SSH tunnel.

## 3.1. Securing JTAG Communication with an SSH Tunnel

Use an SSH tunnel (also known as SSH port forwarding) to encrypt communication between the Intel Quartus Prime JTAG Server on a remote machine and JTAG clients such as the Intel Quartus Prime Programmer on a local machine.

These instructions assume that the FPGA board is attached to the remote machine. If you have the FPGA board attached to the local machine, refer to Securing JTAG Communication with a Reverse SSH Tunnel on page 9.

Before you establish an SSH tunnel for JTAG communications, ensure that you have completed the prerequisites in Securing JTAG Communication with SSH on page 6.

To establish an SSH tunnel for secure JTAG communication:

1. On the local machine, disable the JTAG Server:

   | | |
   |---|---|
   | *Linux operating systems* | Use the `kill` command to stop the JTAG Server process (`jtagd`). Stopping this process disables the JTAG Server. |
   | *Windows operating systems* | Disable the JTAG Server service on Windows operating systems with the following command: `<`*`quartus_installdir`*`>\quartus\bin64\jtagserver.exe --stop`. |

2. On the remote machine, ensure that the SSH server is running.

   Refer to your SSH software documentation for instructions on how to start the SSH server and confirm that it is running.
3. On the local machine, start the SSH client to establish an SSH tunnel between your local and remote machines as follows:

*Linux operating systems*

On the local machine, start a terminal session and run the following command:

```
ssh -L 1309:localhost:1309 <remote_machine>
```

For <*remote_machine*>, you can specify either the IP address or the host name of the remote machine.

After you log on to the SSH server, start another terminal session to run the commands in the later steps in this procedure.

*Windows operating systems*

On the local machine, start a command prompt session and run the following command:

```
putty.exe -ssh -L 1309:localhost:1309 <remote_machine>
```

For <*remote_machine*>, you can specify either the IP address or the host name of the remote machine.

The `putty` command launches a separate window for you to enter your SSH credentials. Return to the command prompt session you originally used to run the `putty` command to run the commands in the later steps in this procedure.

4. On the remote machine (where the FPGA board is installed), start the JTAG Server:

   — On Linux* operating systems, run the following command:

   ```
   $ <quartus_installdir>/quartus/linux64/jtagd
   ```

   — On Windows operating systems, run the following command:

   ```
   > <quartus_installdir>\quartus\bin64\jtagserver.exe --start
   ```

   The JTAG Server uses TCP/IP port 1309.

5. Confirm that JTAG works over your SSH tunnel as follows:

   a. On the local machine, run the following command:

   ```
   jtagconfig
   ```

   This command returns a list of available JTAG connections.

   b. On the remote machine, run the following command:

   ```
   jtagconfig
   ```

   Confirm that this list of available JTAG connections matches the list of JTAG connections listed on the local machine.

6. Start your JTAG client application.

   JTAG client applications include the Intel Quartus Prime Programmer, System Console and Debugging Toolkits, and Signal Tap logic analyzer.

After you have finished using your JTAG client applications, you can close the SSH tunnel in one of the following ways:

- Running the `exit` command in the same terminal or command prompt window where you started the SSH client on the local machine.
- Terminate or close the terminal or command prompt window where you started the SSH client on the local machine.

You can confirm that the SSH tunnel is closed by running the `jtagconfig` command as follows:

- On the local machine, the `jtagconfig` command returns a `No JTAG hardware available` message.
- On the remote machine, the `jtagconfig` command lists only local JTAG connections.

## 3.2. Securing JTAG Communication with a Reverse SSH Tunnel

Use a reverse SSH tunnel (also known as SSH remote port forwarding) to encrypt communication between the Intel Quartus Prime JTAG Server on the local machine and JTAG clients such as the Intel Quartus Prime Programmer on the remote machine.

These instructions assume that the FPGA board is attached to the local machine. If you have the FPGA board attached to the remote machine, refer to Securing JTAG Communication with an SSH Tunnel on page 7.

Before you establish a reverse SSH tunnel for JTAG communications, ensure that you have completed the prerequisites in Securing JTAG Communication with SSH on page 6.

To establish a reverse SSH tunnel for secure JTAG communication:

1. On the remote machine, do the following tasks:
   a. Disable the JTAG Server:

      *Linux operating systems*
      Use the `kill` command to stop the JTAG Server process (`jtagd`). Stopping this process disables the JTAG Server.

      *Windows operating systems*
      Disable the JTAG Server service on Windows operating systems with the following command: `<`*`quartus_installdir`*`>\quartus\bin64\jtagserver.exe --stop`.

   a. Ensure that the SSH server is running.

      Refer to your SSH software documentation for instructions on how to start the SSH server and confirm that it is running.
2. On the local machine, start the SSH client to establish a reverse SSH tunnel between your local and remote machines as follows:

   *Linux operating systems*
   On the local machine, start a terminal session and run the following command:

   ```
   ssh -R 1309:localhost:1309 <remote_machine>
   ```

   For `<`*`remote_machine`*`>`, you can specify either the IP address or the host name of the remote machine.

After you log on to the SSH server, start another terminal session to run the commands in the later steps in this procedure.

*Windows operating systems*

On the local machine, start a command prompt session and run the following command:

```
putty.exe -ssh -R 1309:localhost:1309 <remote_machine>
```

For <*remote_machine*>, you can specify either the IP address or the host name of the remote machine.

The `putty` command launches a separate window for you to enter your SSH credentials. Return to the command prompt session you originally used to run the `putty` command to run the commands in the later steps in this procedure.

3. On the local machine (where the FPGA board is installed), start the JTAG Server:
   - On Linux operating systems, run the following command:

     ```
     $ <quartus_installdir>/quartus/linux64/jtagd
     ```

   - On Windows operating systems, run the following command:

     ```
     > <quartus_installdir>\quartus\bin64\jtagserver.exe --start
     ```

   The JTAG Server uses TCP/IP port 1309.
4. Confirm that JTAG works over your SSH tunnel as follows:
   a. On the remote machine, run the following command:

      ```
      jtagconfig
      ```

      This command returns a list of available JTAG connections.

   b. On the local machine, run the following command:

      ```
      jtagconfig
      ```

      Confirm that this list of available JTAG connections matches the list of JTAG connections listed on the local machine.
5. Start your JTAG client application.

   JTAG client applications include the Intel Quartus Prime Programmer, System Console and Debugging Toolkits, and Signal Tap logic analyzer.

After you have finished using your JTAG client applications, you can close the SSH tunnel in one of the following ways:

- Running the `exit` command in the terminal or command prompt window where you started the SSH client on the local machine.
- Terminate or close the terminal or command prompt window where you started the SSH client on the local machine.

You can confirm that the SSH tunnel is closed by running the `jtagconfig` command as follows:

- On the local machine, the `jtagconfig` command lists only local JTAG connections.
- On the remote machine, the `jtagconfig` command returns a `No JTAG hardware available` message.

# 4. Document Revision History for AN 939: JTAG Connections Over SSH

| Document Version | Intel Quartus Prime Version | Changes |
|---|---|---|
| 2021.07.07 | 21.2 | Initial release. |

Intel Corporation. All rights reserved. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Intel warrants performance of its FPGA and semiconductor products to current specifications in accordance with Intel's standard warranty, but reserves the right to make changes to any products and services at any time without notice. Intel assumes no responsibility or liability arising out of the application or use of any information, product, or service described herein except as expressly agreed to in writing by Intel. Intel customers are advised to obtain the latest version of device specifications before relying on any published information and before placing orders for products or services.
*Other names and brands may be claimed as the property of others.

ISO 9001:2015 Registered