Tech Note | Revision A

Technote – HYPERION Secure Communication via SSH

Micron Optics Inc.
1852 Century Place NE
Atlanta, GA 30345 USA

phone 404 325 0005
fax 404 325 4082
www.micronoptics.com

Table of Contents

1. Introduction

With the release of HYPERION firmware version 12.12.1, all HYPERION instruments support secure TCP/IP communication via SSH tunneling.

One, many, or all of the TCP/IP communication ports can be tunneled through a secure SSH connection.

2. Description of Feature

HYPERION firmware exposes SSH port 22 for secure communications using the "hyperion" user. The "hyperion" user must use a key-based authentication to gain access to the instrument. The public key is shared via the unsecure command port 51971 using the `#AddSSHPublicKey` command. See "Optical Sensing Instrumentation and Software" for more information on this and other SSH-related commands.

Users can create an SSH tunnel using a number of methods including but not limited to:

- PuTTY GUI on Windows
- PuTTY command line on Windows
- SSH client already installed on Linux/Mac

This technote will go over the configuration of each of these approaches.

3. Usage

The following steps describe the usage of this feature.

3.1. Key Creation

A public/private must be created in order to initiate a secure communication link to the HYPERION instrument. The public key must be shared to the HYPERION instrument. The private key MUST BE KEPT SAFE. Do not share your private key as the security of SSH depends upon keeping your private key secret.

3.1.1. Windows (PuTTYgen)

PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is available with source code and is developed and supported by a group of volunteers. PuTTY normally is shipped with a tool for generating public/private key pairs call PuTTYgen. Both tools can be downloaded at www.putty.org.

Open PuTTYgen via the start menu on your Windows machine. The following directions describe creating a key pair:

1. Select the key type RSA by clicking the RSA radio button in the "Parameters" -> "Type of key to generate" section of the front panel.
2. Select the bit depth 2048 by entering 2048 in the text field in the "Parameters" -> "Number of bits in a generated key" field of the front panel.
3. Click the "Generate" button.
4. Follow the on screen instructions to generate the key pair.
5. It is strongly recommended to include a key passphrase with the key pair to increase security. Enter and re-enter a passphrase in the "Key passphrase" and "Confirm passphrase" fields.
6. Save the public key by clicking the "Save public key" button. Enter in a name for the public key. For example, enter in "myKey.pub".
    a. NOTE: PuTTYgen generates a public key that is formatted differently than the Linux command `ssh-keygen` and, thus, what they HYPERION expects during the import of the public key.
    b. In the PuTTYgen front panel, there is a field title "Public key for pasting into OpenSSH authorized_keys file". This is the format that is expected when adding the public key to the HYPERION. Use this formatted text when adding the public key below.
7. Save the private key by clicking the "Save private key" button. Enter in a name for the private key. For example, enter in "myKey". Note the extension ".ppk" is added for you.

3.1.2. Linux/Mac

Linux users can use `ssh-keygen` to generate these key pairs. By default, ssh-keygen generates a 2048 bit RSA key. Open a command prompt and following the following directions to create a key pair.

1. Open a command prompt.
2. Enter "`ssh-keygen`". This command will now walk you through creating a key pair.
3. Enter in a file name in which to save the keys.
4. Enter a passphrase. It is strongly recommended to include a key passphrase with the key pair to increase security.
5. Re-enter the passphrase from above.

This procedure results in two files. If "myKey" was entered in step 3 above, this procedure will result in the private key file name "myKey" and the public key file "myKey.pub". Note the private key does NOT have an extension.

NOTE: The private key must be converted with PuTTYgen if used with PuTTY (command line or GUI).

3.2. Transfer Public Key to the HYPERION

The public key is shared with the HYPERION instrument via the #AddSshPublicKey command on the unsecure TCP/IP port 51971. See "Optical Sensing Instrumentation and Software" for more information on this, other SSH-related commands, and the TCP/IP protocol used in communicating with the instrument. APIs are available in many common languages and can be found at www.micronoptics.com.

The command is used as follows:

```
Command: #AddSshPublicKey
Arguments: [Key Name] [Contents of public key]
```

Once shared with the instrument, a user can initiate a secure SSH connection.

NOTE: The public key generated and saved to a file in PuTTYgen is not the format expected by the HYPERION. See section Windows (PuTTYgen) for acquiring the contents of the public key for this command.

3.3. Creating the SSH Tunnel

This technote describes a specific configuration of SSH tunneling where one desires to have a secure communication between client code running on a remote PC and the HYPERION instrument and the PC are located on an unsecured network. The SSH client (tunnel), running on the remote PC, connects to the SSH server on the HYPERION instrument.

3.3.1. Windows (PuTTY GUI)

Windows users can use PuTTY to establish a secure connection to the HYPERION instrument.

1. Open the PuTTY GUI by navigating through the "Start" menu.
2. In the "Session" category, in the "Host Name (or IP address)" field, enter "hyperion@[IP Address]" , where [IP Address] is the IP address of the HYPERION instrument. This can be viewed on the LCD screen by pressing the CTRL button until it's displayed.
3. In the "Session" category, in the "Port" field, enter 22.
4. In the "Session" category, in the "Connection Type" field, click the "SSH" radio button.
5. In the "Connection->SSH->Auth" category, in the "Private key file for authentication" field, enter the location of the private key created above using PuTTYgen. You can also browse to the location by clicking the "Browse…" button.
    a. If using a private key generated in Linux with `ssh-keygen`, the key format must be converted using PuTTYgen.
6. In the "Connection->SSH->Tunnels" category, add the forwarded ports required for the remote PC client code. The following steps illustrate adding the single port of 51971.
    a. In the "Source port" field, enter "51971".

b. In the “Destination” field, enter “[IP Address]:51971” where [IP Address] is the IP address of the HYPERION instrument.
c. Click the “Add” button.

7. Following step 6 for each port required. For example, to connect with ENLIGHT, ports 51971 – 51973 should be added.
8. Click the “Open” button to initiate a connection.

3.3.2. Windows (PuTTY Command Line)

PuTTY can also be run via the command line.

1. Open a command prompt.
2. Enter “`[path to putty.exe] -ssh hyperion@[IP Address] -L51971:[IP Address]:51971 -L51972:[IP Address]:51972 -L 51973:[IP Address]:51973 -i [path to private key]`” where [path to putty.exe] is the path to PuTTY and is usually installed at “C:\Program Files\PuTTY\putty.exe”, [IP Address] is the IP address for the HYPERION instrument, and [path to private key] is the path to your private key created earlier.
    a. If using a private key generated in Linux with `ssh-keygen`, the key format must be converted using PuTTYgen.

3.3.3. Linux/Mac

An SSH client can be run via the command line.

1. Open a command prompt.
2. Enter “`ssh hyperion@[IP Address] -L 51971:[IP Address]:51971 -L 51972:[IP Address]:51972 -L 51973:[IP Address]:51973 -i [path to private key]`” where [IP Address] is the IP address for the HYPERION instrument and [path to private key] is the path to your private key created earlier using `ssh-keygen`. Private keys generated with PuTTYgen can be used as well.

3.4. Testing the Connection

The connection can be tested by using the Optical Sensing Software package ENLIGHT available at www.micronoptics.com.

1. On the Windows PC in which the SSH tunnel has been initiated with PuTTY, open ENLIGHT.
2. Choose “HYPERION” as the Swept Laser Core.
3. Enter “127.0.0.1” in the IP Address field.
4. Click the “OK” button.
5. You are secure!