1

# How to configure SSH on Cisco

SSH (Secure Shell) is a secure method for remote access as is includes authentication and encryption. To do this, it uses a RSA public/private keypair.

There are two versions: version 1 and 2. Version 2 is more secure and commonly used.

Last but not least, to configure SSH you require an IOS image that supports crypto features. Otherwise, you won’t be able to configure SSH.

## Configuration

To demonstrate SSH, I will use the following topology:

# R1 R2 Gigabit Links

### SSH Server

the name of the RSA keypair will be the hostname and domain name of the router. Let’s configure a hostname:

Router(config)#**hostname R1**

And a domain name:

R1(config)#**ip domain-name NETWORKLESSONS.LOCAL**

Now we can generate the RSA keypair:

R1(config)#**crypto key generate rsa**

The name for the keys will be: R1.NETWORKLESSONS.LOCAL

Choose the size of the key modulus in the range of 360 to 4096 for your

 General Purpose Keys. Choosing a key modulus greater than 512 may take

 a few minutes.

How many bits in the modulus [512]: **2048**

% Generating 2048 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 3 seconds)

When you use the **crypto key generate rsa** command, it will ask you how many bits you want to use for the key size. How much should you pick?

It’s best to check the [next generation encryption](https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html) article from Cisco for this.  At this moment, a key size of 2048 bits is acceptable. Key sizes of 1024 or smaller should be avoided. Larger key sizes also take longer to calculate.

Once the keypair has been generated, the following message will appear:

R1#

%SSH-5-ENABLED: SSH 1.99 has been enabled

As you can see above, SSH version 1 is the default version. Let’s switch to version 2:

R1(config)#**ip ssh version 2**

SSH is enabled but we also have to configure the VTY lines:

R1(config)#**line vty 0 4**

R1(config-line)#**transport input ssh**

R1(config-line)#**login local**

This ensures that we only want to use SSH (not telnet or anything else) and that we want to check the local database for usernames. Let’s create a user:

R1(config)#**username admin password my\_password**

Everything is now in place. We should be able to connect to R1 through SSH now.

### SSH Client

The most common SSH client is probably putty. The only thing you have to do is to select the SSH protocol, enter the IP address and leave the default port at 22:



You will see this on the putty console:

login as: **admin**

Using keyboard-interactive authentication.

Password:

R1>

You can also use another Cisco IOS device as a SSH client. Here’s how:

R2#**ssh ?**

 -c Select encryption algorithm

 -l Log in using this user name

 -m Select HMAC algorithm

 -o Specify options

 -p Connect to this port

 -v Specify SSH Protocol Version

 -vrf Specify vrf name

 WORD IP address or hostname of a remote system

There are quite some options but as a minimum, we should specify a username and IP address:

R2#**ssh -l admin 192.168.12.1**

Password:

R1>

We are now connected to R1 through SSH.