SFTP CONNECTIVITY
SSH Host Keys

September 2018

Forte SFTP Connectivity

Forte provides clients an SFTP service over Internet to facilitate secure communication of sensitive data files. This document summarizes the security features of the SSH and SFTP protocols and provides guidance on how to most securely use the Forte SFTP service.

SSH Overview

What is SSH?

The SSH (Secure Shell) protocol is a cryptographic network protocol which not only facilitates the establishment of a secure channel to allow network services to communicate and share data securely over an unsecure network, but also defines an extensible process for user authentication as well (typically via a password or key)

At a high level, the following steps take place when establishing an SSH connection.

1. An unsecure TCP connection is established to a destination server.
2. The server advertises the supported SSH protocol version and server host key to the client over the unsecure connection.
3. The client verifies the identity of the server, and continues if the protocol version is supported.
4. The client and server agree on an encryption algorithm, and encrypt the connection using the Diffie-Hellman exchange. At this point, the connection between the client and server is now secure.
5. The client then authenticates with the server using their username and credentials. The server verifies the client is a valid user.
6. At this point, the client has logged in successfully and can begin to interact with the server over the agreed protocol – for example, SFTP.

What is SFTP?

The SFTP (Secure File Transfer Protocol) is an extension of the SSH protocol version 2.0 allowing it to provide secure file access, transfer, and management over any reliable data stream.

By leveraging the SSH protocol, SFTP protects itself against password sniffing and man-inthe-middle attacks, ensuring the integrity of the data and authenticating both the client and the server.

While SFTP could potentially be applied on any secure channel other than SSH channels, it typically is only used in the context of an established SSH channel, and as such, requirements for connections SSH typically hold true for SFTP connections as well.

Host Keys and Fingerprints

What is a host key?

A host key actually refers to a pair of asymmetric cryptographic keys. While asymmetric keys are typically used for encryption and decryption, a host key is used by a SSH server to identify itself to a newly incoming SSH connection.

The public portion of the key pair is presented as part of establishing the SSH connection (Step 2 in the SSH Overview).

What is a host key fingerprint?

The exact format of an SSH host key depends on the cipher algorithm used, but the following is an example DSA host key:

> ssh-dss AAAAB3NzaC1kc3MAAACBAJ3hB5SAF6mBXPlZlRoJEZi0KSIN+NU2iGiaXZXi9CDrgVxTp6/sc56UcYCp4qjfrZ2G3+6PWbxYso4P4YyUC+61RU5KPy4EcTJske3O+aNvec/20cW7PT3TvH1+sxwGrymD50kTiXDgo5nXdqFvibgM61WW2DGTKlEUsZys0njRAAAAFQDs7ukaTGJlZdeznwFUAttTH9LrwwAAAIAMm4sLCdvvBx9WPkvWDX0OIXSteCYckiQxesOfPvz26FfYxuTG/2dljDlalC+kYG05C1NEcmZWSNESGBGfccSYSfI3Y5ahSVUhOC2LMO3JNjVyYUnOM/iyhzrnRfQoWO9GFMaugq0jBMlhZA4UO26yJqJ+BtXIyItaEEJdc/ghIwAAAIBFeCZynstlbBjP648+mDKIvzNSS+JYr5klGxS3q8A56NPcYhDMxGn7h1DKbb2AV4pO6y+6hDrWo3UT4dLVuzK01trwpPYp6JXTSZZ12ZaXNPz7sX9/z6pzMqhX4UEfjVsLcuF+ZS6aQCPO0ZZEa1z+EEIZSD/ykLQsDwPxGjPBqw== someone@somewhere.com

As SSH Keys are long, it is possible to generate a short representation of the keys by using a hashing algorithm. This short version of the key is known as the fingerprint and typically is formatted for ease of human readability. The following is an example of fingerprint for a 1024 bit key:

> 8a:fe:7d:78:56:cd:1c:6f:1d:a1:1d:cd:1c:fb:85:72

What is the purpose of a host key?

Imagine you are tasked with the delivery of an important package to an individual who supposedly is waiting at a specified address. After arriving at that address and ringing the door bell, somebody opens the door and awaits receipt of the package. However - how do Forte SFTP Connectivity – Host Keys you know that this individual is the person who should be receiving this package? You would naturally ask to see some kind of proof of their identity.

When a network connection is established for the first time between two computers, they face the exact same dilemma. How does the client computer know that the server it is connecting to is indeed the intended destination? With this analogy in mind, the SSH host key is the server's identity.

Trusted third party

To continue the package delivery analogy in the previous section, suppose you asked the individual waiting at the door to present proof of their identity, what kind of documentation would you accept as valid? Most likely it would be something issued by the Government or other trusted institution. That institution is the trusted third party in this real-life example.

However, in the SSH Protocol, there is no such trusted third party used to verify the identity of the server, and when establishing a new connection, the client must know in advance what identification information will be accepted – in the case of SSH, this is the server's host key fingerprint.

As there must be an information exchange through some other media (e-mail, telephone) regarding usernames and credentials between a client-party and server-party as part of a setup, it is expected that the host key fingerprint information also be exchanged in advance as well.

Verification and Acceptance

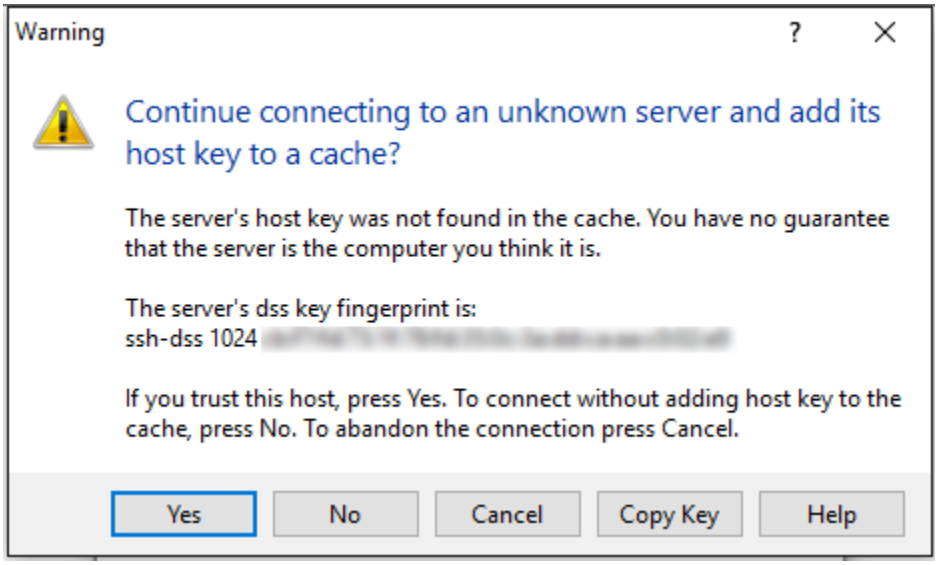
SSH host key verification

As mentioned in the previous section regarding the purpose of a host key, it is important that the SSH client verifies the host key of the server it is connecting to. To facilitate this, the SSH protocol ensure that whenever a client initiates a new connection, the server presents its host key's fingerprint for verification. If this host key has not been previously saved in the known hosts cache, the client software prompts the user to manually accept the new fingerprint before establishing the connection.

This manual prompt for new connections looks something like this in a terminal client:

> The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.
>
> The server's rsa2 key fingerprint is:
>
> ssh-rsa 2048 b6:71:38:38:95:20:1c:f2:34:74:fc:0b:0d:51:a1:77
>
> If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press, Cancel.

In a Windows SFTP Client (such as SCP), it will look like this:



As the client already knows the fingerprint of the server to expect (as this was previously exchanged during account setup), at this point the client can confirm if the presented fingerprint matches the expected value.

If not, then it is possible that the connection is currently being subjected to a man-in-the-middle attack and the connection should not be established.

SSH known hosts cache

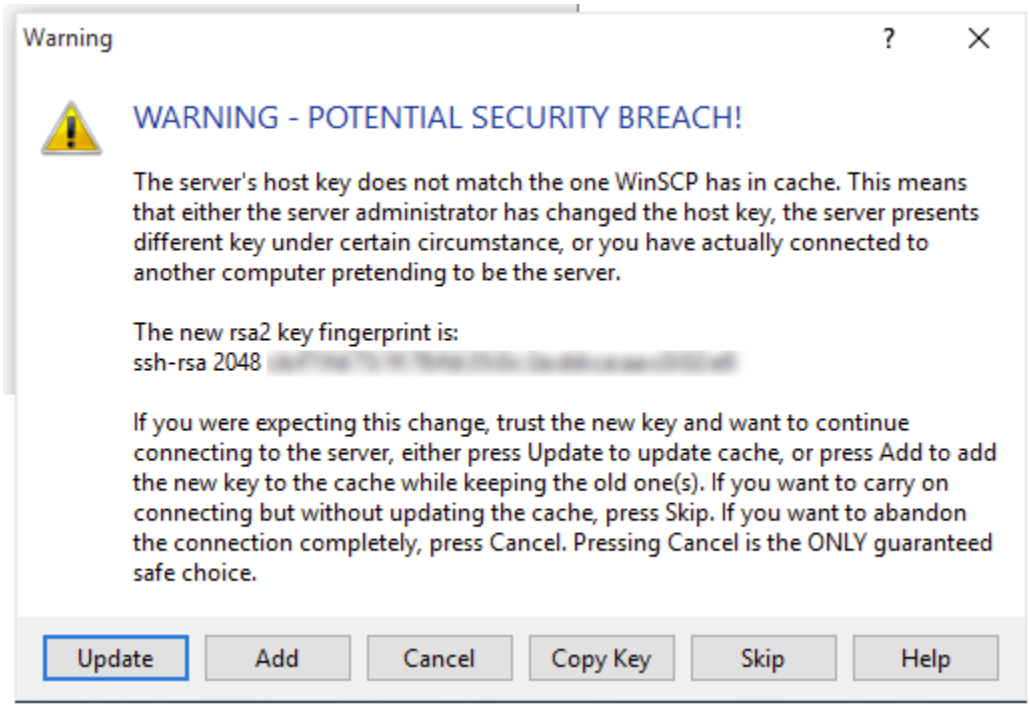
Once a new server host key fingerprint is accepted as part of establishing a connection for the first time, a typical SSH client would save this in a local cache called known hosts. As the host key and fingerprint has now been saved, it becomes trusted and all subsequent connections to that server will not require the client to manually accept the fingerprint again.

However, the SSH client software still verifies the host key on every subsequent connection established to ensure it is always connecting to the right server. Should the host key fingerprint presented by the server ever differ from the one that is saved in the client's known hosts cache, this indicates that the connection may be being subjected to a man-in-the-middle attack and must be manually accepted.

This manual prompt to accept a change in a host key looks like this in a terminal client:

> The host key sent by the server is different from the host key stored in the host key database for myserver (192.168.0.1), port 22. This may mean that a hostile party has "hijacked" your connection and you are not connected to the server you specified.
>
> It is recommended you verify your host key before accepting.
>
> Server's host key fingerprint (MD5 hash):
>
> b6:71:38:38:95:20:1c:f2:34:74:fc:0b:0d:51:a1:77
>
> If you trust this host, enter "y" to add the key to the host key database and connect. If you do not trust this host, enter "n" to abandon the connection.
>
> Accept and save? (y/n)

In a Windows SFTP Client (such as SCP), it will look like this:



It is important at this stage that the client-party verifies with the server-party system administrator via another medium (e-mail, telephone) if this change is expected, and if the new fingerprint matches the expected value.

Forte's Hosted SFTP Services

We recommend for the protection of your data that clients always perform their due diligence when connecting to Forte's Hosted SFTP services and always verify the fingerprint of the destination server against one of the official values below before establishing the connection.

Current fingerprint

ssh-rsa 2048 b6:71:38:38:95:20:1c:f2:34:74:fc:0b:0d:51:a1:77