

How to Resolve the "Remote Host Identification Has Changed" Error

Table of contents

1. How to Resolve the "Remote Host Identification Has Changed" Error	3
--	---

1. How to Resolve the "Remote Host Identification Has Changed" Error

When connecting to an SSH server, you may receive the following message:

```
$ SSH ser1.empl.com

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@      WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!      @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

The fingerprint for the ED25519 key sent by the remote host is

SHA256:EXAMPLE_HOST_KEY_FINGERPRINT

Add correct host key in SYS$LOGIN:[SSH]KNOWN_HOSTS to get rid of this message.

Offending ECDSA key in SYS$LOGIN:[SSH]KNOWN_HOSTS:<line_number>
```

SSH uses host keys to verify the identity of a server. This warning occurs when the host key presented by the server does not match the key previously stored on the client.

Common causes include:

- The server's SSH host keys were regenerated.
- The server was upgraded from SSH.COM SSH to OpenSSH, resulting in new host keys.
- The server hostname or IP address was reassigned to a different system.
- A potential security issue, such as a man-in-the-middle attack.

Important

This error is usually caused by legitimate administrative changes, such as OpenVMS SSH upgrades. However, verify the cause before bypassing it. Before removing any host keys, contact the system administrator to confirm that the server's host keys have recently changed.

If the host key change is expected, do the following:

1. Remove the outdated key from the client.

For OpenSSH Clients

Edit the user's known_hosts file (SYS\$LOGIN:[SSH]KNOWN_HOSTS) and remove the entry associated with the affected hostname or IP address.

For SSH.COM Clients

Delete the server's old public host key from the user's directory in `SYSS$LOGIN:[SSH2.HOSTKEYS]`.

2. Reconnect to the Server using the command `$ SSH ser1.empl.com`.
3. When prompted to verify and accept the new host key, enter `yes`.

```
$ SSH ser1.empl.com
```

```
The authenticity of host 'ser1.empl.com (192.0.2.10)' can't be established.
```

```
ED25519 key fingerprint is
```

```
SHA256:EXAMPLE_HOST_KEY_FINGERPRINT
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

```
Warning: Permanently added 'ser1.empl.com' (ED25519) to list of known hosts.
```