

How to Setup Public Key Authentication from OpenSSH to OpenVMS

Table of contents

1. How to Setup Public Key Authentication from OpenSSH to OpenVMS	3
2. Procedure	4
2.1 Generate and Verify the Key Pair	4
2.2 Transfer the Public Key	5
2.3 Configure the OpenVMS Server	6

1. How to Setup Public Key Authentication from OpenSSH to OpenVMS

This article describes how to configure public key authentication from an OpenSSH client to an OpenVMS SSH server.

Applies to:

- OpenVMS V7.3 and higher
- TCP/IP Services V5.4 ECO5 and higher
- UNIX (various versions)
- OpenSSH client with SSH-2 support

This article assumes that public key authentication is enabled on both the OpenSSH client and the OpenVMS SSH server, and that network connectivity between the client and server has been verified.

To test connectivity, run:

```
telnet openvms_host 22
```

If the connection succeeds and an SSH banner is displayed, the server is reachable and accepting connections. If the connection fails, contact the appropriate support team before continuing.

2. Procedure

2.1 Generate and Verify the Key Pair

1. Generate a key pair on the OpenSSH client.

```
cd ~/.ssh  
ssh-keygen
```

This creates the keypair:

- id_rsa (private key)
- id_rsa.pub (public key)

2. Verify the public key fingerprint:

```
ssh-keygen -l -f id_rsa.pub
```

Alternatively, generate a Bubble Babble fingerprint for comparison with the fingerprint displayed on OpenVMS:

```
ssh-keygen -B -f id_rsa.pub
```

If no fingerprint is returned, the public key is invalid. Regenerate the key pair and try again. If the issue persists, contact support.

3. Convert the public key to SSH.COM format.

```
ssh-keygen -e -f id_rsa.pub > id_rsa_sshcom.pub
```

2.2 Transfer the Public Key

The following methods can be used to install the public key on the OpenVMS server:

Method A: Use SFTP

Note

Password authentication is required for this step.

```
sftp OpenVMS
user@OpenVMS's password:

sftp> cd ssh2
sftp> put id_rsa_sshcom.pub
Uploading id_rsa_sshcom.pub to /SYS$SYSDEVICE/user/ssh2/id_rsa_sshcom.pub
id_rsa_sshcom.pub 100% 512 0.5KB/s 00:00

sftp> quit
```

Method B: Copy and Paste

Display the key:

```
cat id_rsa_sshcom.pub
```

On the OpenVMS system, open or create the public key file in the ssh2 directory:

```
$ SET DEF SYS$LOGIN:
$ SET DEF [.SSH2]
$ EDIT/EDT ID_RSA_SSHCOM.PUB
```

Copy the entire contents of `id_rsa_sshcom.pub` from the OpenSSH client and paste it into the editor on the OpenVMS system. Save the file and exit the editor.

2.3 Configure the OpenVMS Server

These steps require an interactive login to OpenVMS.

1. Verify the public key format.

```
$ SET DEF SYS$LOGIN:
$ SET DEF [.SSH2]
$ @SYS$MANAGER:TCPIP$DEFINE_COMMANDS
$ SSH_KEYGEN -"F" ID_RSA_SSHCOM.PUB
```

If a fingerprint is not returned, the key is not usable. Try Method A and/or Method B again. Contact appropriate support for further assistance.

2. Create the AUTHORIZATION file.

```
$ CREATE AUTHORIZATION.
KEY ID_RSA_SSHCOM.PUB
```

3. Set file protections.

```
$ SET FILE/PROT=(S,W,G,O:RE) AUTHORIZATION.
$ SET FILE/PROT=(S,W,G,O:RE) ID_RSA_SSHCOM.PUB
```

4. Test SFTP from the OpenSSH client.

```
sftp OpenVMS
```

Note

No password prompt should appear if public key authentication is configured correctly.

Example:

```
sftp> pwd
Remote working directory: /SYS$SYSDEVICE/USER
```