

SSH Solutions Quick Reference Guide

MultiNet and TCPware TCP/IP Stacks and SSH for OpenVMS

Overview

Key Features	Function	Benefits
Replaces Telnet and R Services	SSH provides secure encrypted communication over unsecured networks such as the Internet. It replaces Telnet, rsh, rlogin, and rcp sessions as specified by the user.	SSH provides remote system access securely. It eliminates potential security breaches, such as spoofing and eavesdropping or hijacking of sessions.
Support for protocol version 1 and 2	The Process Software SSH products support protocol v1 and v2 on both the client and server. SSH v2 is more secure than SSH v1 and is an IETF standard.	An administrator has the flexibility to decide which protocol to use.
Secure File Transfer Protocol (SFTP) Server and Client	SFTP provides a secure mechanism for transferring, deleting, or copying files over the network using SSH file transfer protocol v4.	SFTP provides secure file transfer with an FTP-like interface.
Secure Copy Protocol - SCP	SCP provides a mechanism for transferring, deleting, copying or moving files securely.	Files can be transferred over a secure network.
Authentication	Authentication is used to verify the identity of a user logging into a system. RSA and DSA methods are used for authentication. The more secure Diffie-Hellman algorithm is used for the key exchange in SSH v2.	Authentication protects users against the possibility of a hacker forging their identity.
Encryption	Encryption is used to encode passwords and data. The options include DES, 3DES, ARCFOUR, Blowfish, IDEA, Twofish, CAST-128, and AES.	Encrypted data prevents a hostile user from being able to read the data as it is traversing the network.
Single Sign-On	Process Software's SSH solutions allow organizations to work with their existing PKI certificates and Kerberos V5 infrastructure.	Single sign-on simplifies management of an organizations security infrastructure.
Port Forwarding (Application Tunneling)	Third-party applications can be secured, such as, POP, SMTP, STREAM, database connections, and more.	A user can select which application to encrypt based on corporate security policy. Not all applications are encrypted avoiding unnecessary network overhead.



Overview

Key Features	Function	Benefits
X-11 Forwarding	X-11 applications can be sent across a network securely.	This feature protects X-11 Windows sessions.
Government Compliance	The Process Software SSH2 server and client are compiled from unaltered cryptographic source, which is FIPS 140-2 Level 2 compliant.	Government agencies can share information and collaborate securely while complying with stringent security mandates

Interoperability

Key Features	Function	Benefits
Third-Party Client and Server Interoperability	The Process Software SSH server and client work with most third-party clients and servers on the market today on UNIX, Windows, Linux, OpenVMS, and Macintosh platforms.	This provides the user with flexibility. Any SSH-compliant software will operate with the Process Software SSH server and client.
HP backward version compatibility	Runs on OpenVMS Alpha v6.2 or higher, OpenVMS VAX v5.5-2 or higher, and OpenVMS I64 v8.2 or higher.	Administrators do not have to go to the expense and time to upgrade to the latest OpenVMS OS or TCP/IP Services stack to use the Process Software SSH products.
ASCII and BINARY File Transfer Support	There is improved interoperability when converting files from local storage to a destination system (via SFTP or SCP), which uses different operating system file formats.	This feature provides seamless file transfer interoperability between heterogeneous operating systems.
Files Transfers Between OpenVMS systems	Process Software preserves the OpenVMS file attributes for file transfers between OpenVMS systems.	This gives users the flexibility to perform binary data transfer or stream-line files.

Management Tools

Key Features	Function	Benefits
Extensive Error Reporting	An error string is reported to users from the underlining file system during SFTP transactions.	More detailed error messages assist in troubleshooting problems.
Public Key Assistant & Server	This is a tool for setting up public key authentication on a remote system. The Assistant (user program) uploads the key to the server and the server performs the necessary updates to files so that the key can be used.	Provides remote management capabilities.



Management Tools

Key Features	Function	Benefits
Certificate Management	Process Software provides the CERTENROLL utility to register certificates; and the CERTVIEW utility for viewing and validating certificate details and displaying the configuration information, which can be used to build the certificate mapping file.	The CERTENROLL and CERTVIEW utilities make it easier to deploy and manage certificates.
Configuration Options	The SSH client and server have extensive configuration options available,SSH such as client-side server-side "SessionRestricted" keyword which helps restrict users to perform only specific types of operations	Robust configuration options make it easier to comply with an organization's security policy.

