PuTTY How To Guide

Contents

- 1 Introduction 2 Connecting to the Swivel appliance
- 3 Next Steps
- 4 Certificates • 5 Known Issues
- 6 Troubleshooting
 6.1 WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!

Introduction

There are various applications which will provide SSH and SFTP functionality. We recommend the use of PuTTY for SSH console connectivity to the Swivel appliance. If you wish to transfer files to and from the appliance, please see the WinSCP How To Guide.

Connecting to the Swivel appliance

When you run PuTTY, you are presented with the following screen, where you can manage stored sessions.

Basic options for your PuTTY session	
Specify the destination you want to Host Name (or IP address)	Port 22
Connection type: Raw Telnet Rlogin	● SSH
Load, save or delete a stored session Saved Sessions	
Default Settings	Load Save Delete
Close window on exit:	
	Specify the destination you want to Host Name (or IP address) Connection type: Raw Telnet Rlogin Load, save or delete a stored sess Saved Sessions Default Settings

To connect to the Swivel appliance enter the IP address of the PINsafe appliance into the Host Name field (the default out of the box IP address is 192.168.0.35 for the standalone appliance).

Session	Basic options for your PuTTY session		
- Logging - Terminal - Keyboard - Bell - Features	Specify the destination you want Host Name (or IP address) 192.168.0.35 Connection type:	to connect to Port 22	
 Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial 	 Raw Telnet Rlogin SSH Serial Load, save or delete a stored session Saved Sessions 		
	Default Settings	Load Save Delete	
	Close window on exit: Always Never	Only on clean exit	

Click the Open button at the bottom of the window, to initiate the SSH session. You may be prompted to add or update the security key.

PuTTY Secu	urity Alert 📉 🗶
	WARNING - POTENTIAL SECURITY BREACH! The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server. The new rsa2 key fingerprint is: ssh-rsa 1024 47:10:a9:a2:20:33:0b:7e:b5:dc:3a:8d:25:0f:df:d3 If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting. If you want to carry on connecting but without updating the cache, hit No. If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.
	Yes No Cancel

You should then be presented with the following screen, where you are prompted to enter the username and password. The default username on Swivel appliances is **admin** (on older appliances it is **root**). The default password is **lockbox** - you are advised to change this, but make sure that you have a record of the new password - recovering access if you have forgotten the password is possible, but it is a complex process.



Once logged in successfully, you should be presented with the following screen, which is the CMI. The left image shows the v2 CMI and the right shows v3.



Next Steps

See the Getting Started Basic CMI configuration guide.

Certificates

		?
le Key Conversions Help		
Кеу		
No key.		
Actions		
Actions Generate a public/private key pair		Generate
and the second		<u>G</u> enerate Load
Generate a public/private key pair	Save p <u>u</u> blic key	
Generate a public/private key pair Load an existing private key file	Save p <u>u</u> blic key	Load
Generate a public/private key pair Load an existing private key file Save the generated key Parameters Type of key to generate:		Load
Generate a public/private key pair Load an existing private key file Save the generated key Parameters		Load

Some appliances may be configured to use certificates. The program PuTTYgen allows keys to be imported and also converted to a format used by PuTTY.

To import a certificate start PuTTYgen, and click the Load button. If the file you are loading is not a .ppk file, such as a .pem file, then select All Files from the File Type dropdown, and choose then select the relevant file.

Upon loading the file, PuTTYgen should display a message 'Successfully imported foreign key...,'. You will then need to click on 'Save private key' to save it as a PuTTY Private Key file (.ppk). You will also be prompted to 'Enter a passphrase' if required.

The PuTTY configuration allows a key to be specified under Connection/SSH/Auth of the PuTTY session you're configuring.

Known Issues

A break in Network connectivity will cause the PuTTY session to terminate.

Troubleshooting

- Check that the IP address is the correct IP for the appliance;
- . Check that internal firewall policies allow connection to port 22.

WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!

The following message may be seen when connecting between Swivel virtual or hardware appliances.

backup the file /root/.ssh/known_hosts in the appliance which is initiating the connection and remove the old key.

When a connection is made the new host is added

[admin@gbcar-swvl2 ~]# ssh admin@192.168.1.1 The authenticity of host '192.178.1.1 (192.168.1.1)' can't be established. RSA key fingerprint is 29:d2:2f:70.3a:34:d2:ed:aa:8f:fa:50:a9:65:a2:45. Are you sure you want to continue connecting (yes/no)? Warning: Permanently added '192.168.1.1' (RSA) to the list of known hosts. Connection closed by 192.168.1.1