How to setup SSH Public Key Authentication on DGS-1510

[Topology]



[Overview]

- 1) Generate an RSA public / private keypair via PuTTY Key Generator
- 2) Copy RSA public key to Switch
- 3) Configure SSH on Switch
- 4) Access to Switch via PuTTY

[Configure]

Step 1. Generate an RSA public / private keypair via PuTTY Key Generator



1. Generate a 1024 bit SSH-2-RSA keypair

2. To generate a random key, PuTTY key generator uses the input of your mouse movement. Swing it around a bit until the keys are ready.

Put IT Key Generator					_
le Key Conversions Help					
Key					
Please generate some randomness	by moving the	e mouse ov	ver the blan	ik area.	
Actions					
Actions Generate a public/private key pair				Generate	
Actions Generate a public/private key pair				Generate	
Actions Generate a public/private key pair Load an existing private key file				Generate Load	•
Actions Generate a public/private key pair Load an existing private key file Save the generated key		Save publ	ic key	Generate Load Save private	; key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters		Save publ	ic key	Generate Load Save private	key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters Type of key to generate:	© ECDSA	Save publ	ic key	Generate Load Save private	key (RSA)

3. After finishing generate keys, please key-in Password "admin". for keys

e K	(ey	Conversion	ns Help					
Ke	G	Generate ke	y p <mark>ai</mark> r					
Pu	s	SH-1 key (RSA)	rize	ed_keys	file:		
A	• S	SH-2 RSA	cey	1/4	EtDwbY	1gHndcWC1aa		Â
B	s s	SH-2 DSA	key A key	BE	ip2+rqdfo	1+HasQYZPLun	OOEhqdCTk=	Ŧ
Ke	S	SH-2 ED25	519 key).f8	:06:be:0	d.f2:1e:83:1b:94	1:a2:b1:4b:2a:2f	
Confi	im pas	ssphrase:	•••••	admir				
Confi Actio	im pas ns	ssphrase:	••••	admir				
Confi Action Gene	irm pas Ins erate a	ssphrase: public/priva	ate key pair	admir			Generate	
Confi Action Gene Load	im pas ins erate a d an ex	ssphrase: a public/private	••••• ate key pair e key file	admir			Generate	
Confi Action Gene Load Save	im pas ins erate a d an ex e the g	ssphrase: a public/private sisting private enerated ke	e key pair e key file	admir	Save	e public key	Generate Load Save private ke	ÿ
Confi Action Gene Load Save Parar	im pas ins erate a d an ex e the g meters	ssphrase: public/priva disting private enerated ke	e key pair e key file	admir	Save	e public key	Generate Load Save private ke	ey.
Confi Action Gene Load Save Parar Type © R	im pas ins erate a d an ex e the g meters e of key SA	ssphrase: public/private isting private venerated ke y to generat © [e: DSA	admir © ECD	Save	e public key	Generate Load Save private ke	ey SA)

4. Copy the red part and save a public key file to "public key for DUT.pub"

PuTTY Key Generat	or		= publ	ic key for DUT.pub - WordPad
File Key Conversio	ons Help	Hon	ne Viev	v .
Key Public key for pasting ssh-rsa AAAAB3NzaC1yc2E, SFK-f7xWP5eteBC/f BvGyHP4eL/mVQto/ rsa-key-20170825	into OpenSSH authorized_keys file: AAAABJQAAAIEA22k/4EI0wbY1gHndcWC1aa3DRZurZgcTnIIQ 11175uldYJHkaezvlg91xcMRIBMYRcutg9PjluQbyLWE1J1vA9Ry KPz4kTzFLF4XJHUsIBEP2+rqdfd+HasQYZPLunOOEhqdCTk=	Clipboard	B 2	r New 11 A A' File Image: Second and the second an
Key fingerprint: Key comment: Key passphrase: Confirm passphrase: Actions Generate a public/prin Load an existing priva Save the generated k Parameters Type of key to genera © RSA Number of bits in a ge	ssh-rsa 1024 c0:59f8.06/be:0df2:1e:83:1b:94:a2b1:4b:2a:2f rsa-key-20170825 ••••• •vate key pair te key file Load ey Save public key Save private key te: DSA © ECDSA © ED25519 © SSH-1 (RSA) nerated key: 1024			ssh-rsa AAAABSNzaClyc2EAAAABJQAAAIEA2Zk/4EtDwbYlgHndcWClaa3DRZurZgcTnlIQS FK/f7xWP5eteBC/f117jSukfYjHkaezvIg91xcMRlsMYRctJfg9PljuOjbyLWE1J1 vA9RyBvGyHP4eL/mVQtoKP24fxTzFLF4XjHUslBEip2 +rqdfd+HasQYZPLunOOEhqdCTk= rsa-key-20170825

5. Hit the save private key buttons, and save private key to

"pub.v2.pri.ppk"

PuTTY Key Generat	tor		
File Key Conversio	ons Help	Organize 🔻 New folder	
Key Public key for pasting	into OpenSSH authorized_keys file:	Favorites	
ssh-rsa AAAAB3NzaC1yc2E SFK/f7xWP5eteBC/1 BvGyHP4eL/mVQto1 rsa-key-20170825	AAAABJQAAAIEA2Zk/4EtDwbY1gHndcWC1aa3DRZurZgcTnIIQ f117jSuldYjHkaezvlg91xcMRIsMYRctJfg9PljuOjbyLWE1J1vA9Ry KPz4fxTzFLF4XjHUsIBEip2+rqdfd+HasQYZPLunOOEhqdCTk=	Downloads File folder Recent Places Yesterday (4)	
Key fingerprint:	ssh-rsa 1024 c0:59f8:06:be:0df2:1e:83:1b:94:a2:b1:4b:2a:2f	Libraries = pub.v2.pri.ppk	
Key comment:	rsa-key-20170825	Documents 869 bytes	
Key passphrase:	•••••	Pictures admin.ppk	
Confirm passphrase:	•••••	Videos PPK File 301 bytes	
Actions Generate a public/pri	vate key pair Generate	Computer Local Disk (C:)	
Save the generated k	key Mie Load Key Save public key Save private key	CMAERA	
Parameters		File nathe: pub.v2.pri.ppk	-
Type of key to generate RSA	ate: DSA	Save as type: PuTTY Private Key Files (*.ppk)	
Number of bits in a ge	enerated key: 1024	Hide Folders Save	Cancel

Step 2. Copy RSA public key to Switch

Copy public key to file system via tftp server(10.90.90.99) Modify file name to "admin.pub" Input the below commands on Switch:

copy tftp: //10.90.90.99/ public key for DUT.pub flash: admin.pub

Step 3. Configure SSH on Switch

1. Create user dlink ; password dlink

config t username dlink privilege 15 password dlink exit

2. Enable SSH

configure terminal line ssh password ssh login local exit ip ssh server end 3. Configure authentication method to Public-Key for user "dlink"

config t

ssh user dlink authentication-method publickey c:/admin.pub

Step 4. Access to Switch via PuTTY

1. Open PuTTY and look for the Connection > SSH setting. Click on the browse button and select your private key file "pub.v2.pri.ppk"



2. Go to the main screen, key in 10.90.90.90 Switch IP and choose SSH connection. After finish settings, hit open button.

egory:						
Session	Basic options for your PuTTY session					
Logging Terminal Keyboard Bell Features Window	Specify the destination you want to Host Name (or IP address)	Port				
	Connection type: Raw Telnet Rlogin SSH Serial					
Appearance Behaviour	Load, save or delete a stored session Saved Sessions					
Selection	publick					
Colours	Default Settings 3130	Load				
Data	new	Save				
Proxy Telnet Blogin	Pablick	Delete				
™ Riogin ⊕ SSH Serial	Close window on exit: Always Never O	nly on clean exit				

3. Keep to hit Yes button when the windows prompts out.





4. Input username "dlink" and then input the key password "admin"



5. The key fingerprints match, let's see if we can connect:

P COM1 - PuTTY	Instantion Instantion In	Nuclear, Specific	
DGS-1510-28XMF	9 Gigabit Ethernet	SmartPro Switch	
Cc Fir Copyright(C) 2015 D- Switch#	ommand Line Interf mware: Build 1.33 Link Corporation.	ace .B007 All rights reserved.	
Switch# Switch# Switch# Switch# Switch# Switch# Switch#show ss Switch#show ssh			
SID Ver. Cipher	Userid	Client IP Address	
0 V2 aes256-cbc/hmac-shal	dlink	10.90.90.7	
Total Entries: 1			