

How to get device information by SSH

Preparation

SecureCRT software

You can download this tool from 400FTP Path :/17 Thermal/02 Product support/04 Tool/SecureCRT/

Steps:

1. Go to **Configuration** → **System** → **Security** → **Security Service**. Enable SSH. Click **save** to save settings.



2. Open SecureCRT and click Quick Connect.



l 🔳 no	ot connected - Se	ecureCRT		and the second	
<u>F</u> ile	<u>E</u> dit <u>V</u> iew	<u>Options</u> <u>T</u> ran	sfer <u>S</u> cript	Too <u>l</u> s <u>H</u> elp	
5	Connect	Alt+C	53	28 1 1 🞯 🖃 📮	
3	Quick Connect.	Alt+Q		W	×
្រា	Connect in Ta <u>b</u>	Alt+B			<u>^</u>
5	<u>R</u> econnect				
	Reconnect <u>A</u> ll				
X	<u>D</u> isconnect				
	Disc <u>o</u> nnect All				
	Clo <u>n</u> e Session				
	Connect SFTP T	ab Alt+P			Ξ
	Loc <u>k</u> Session				
	<u>P</u> rint	•			
	Print Set <u>u</u> p				
	Log Session				
	Ra <u>w</u> Log Sessio	on 🛛			
	<u>T</u> race Options				-
i.	<u>1</u> Serial-COM5	(23)	1, 1	24 Rows, 80 Cols VT100	CAP NUM
	· · · · -	· • • ·			
)	alact CCU2				
3. S	elect SSH2.	CPT			
3. Si	elect SSH2.	cureCRT	1 No. 1	and fill in correct H	
3. So 1 no <u>F</u> ile	elect SSH2. ht connected - Se <u>E</u> dit <u>V</u> iew	cureCRT Quick Connec	t No. a		
3. Si in no Eile Eile	elect SSH2. ht connected - Se Edit View	CureCRT Quick Connec	t		
3. Si in no Eile Si Si Si Si Si Si Si Si Si Si	elect SSH2. t connected - Se <u>E</u> dit <u>V</u> iew [] [] (] (3) (3) []	Quick Connec	t SSH2 SSH2	<u> </u>	
3. Si no Eile Si Si C	elect SSH2. ht connected - Se Edit View	Quick Connec Protocol: Hostname:	t SSH2 SSH2 SSH1 Totot		
3. Si no <u>File</u>	elect SSH2. t connected - Se <u>E</u> dit <u>V</u> iew E dit <u>V</u> iew	Quick Connect Protocol: Hostname: Port:	t SSH2 SSH2 SSH1 Telnet Telnet/SSL	v ewall: None	
3. Si in no Eile Si Si Si Si Si Si Si Si Si Si	elect SSH2. t connected - Se <u>E</u> dit <u>V</u> iew <u>C</u> <u>S</u> <u>S</u>	Quick Connec Protocol: Hostname: Port: Username:	t SSH2 SSH1 Telnet Telnet/SSL RLogin Serial	v ewall: None	
3. Si in no File Si Si Si Si Si Si Si Si Si Si	elect SSH2. t connected - Se Edit View Constant View	Quick Connect Protocol: Hostname: Port: Username:	t SSH2 SSH1 Telnet Telnet/SSL RLogin Serial TAPI	ewall: None	
3. Si	elect SSH2.	Quick Connect Protocol: Hostname: Port: Username: Authenticatio	t SSH2 SSH1 Telnet Telnet/SSL RLogin Serial TAPI on	ewall: None	
3. Si	elect SSH2.	Quick Connect Protocol: Hostname: Port: Username: Authentication Passwor Publicke	t SSH2 SSH1 Telnet Telnet/SSL RLogin Serial TAPI on d y	ewall: None	
3. Si	elect SSH2.	Quick Connect Protocol: Hostname: Port: Username: Authenticatii Ø Passwor Ø Publicke Ø Keyboar	t SSH2 SSH2 SSH1 Telnet Telnet/SSL RLogin Serial TAPI on d y d Interactive	ewall: None	
3. Si	elect SSH2.	Quick Connec Protocol: Hostname: Port: Username: Authentication Passwor Publicke Keyboar GSSAPI	t SSH2 SSH1 Telnet Telnet/SSL RLogin Serial TAPI on d y d Interactive	ewall: None	
3. Si	elect SSH2.	Quick Connect Protocol: Hostname: Port: Username: Authenticatic Vasswor Publicke Keyboar GSSAPI	t SSH2 SSH1 Telnet Telnet/SSL RLogin Serial TAPI on d y d Interactive	ewall: None	
3. Si	elect SSH2.	Quick Connec Protocol: Hostname: Port: Username: Authentication VPublicke VKeyboar GSSAPI	t SSH2 SSH1 Telnet Telnet/SSL RLogin Serial TAPI on d J y d Interactive	ewall: None	
3. Si	elect SSH2.	Quick Connect Protocol: Hostname: Port: Username: Authentication Passwor Publicke Keyboar GSSAPI	tt SSH2 SSH1 Telnet Telnet/SSL RLogin Serial TAPI on d y d Interactive	tup Save session	
3. Si	elect SSH2.	Quick Connec Protocol: Hostname: Port: Username: Authenticatio VPasswor VPublicke Keyboar GSSAPI	t SSH2 SSH1 Telnet Telnet/SSL RLogin Serial TAPI on d y d Interactive	ewall: None Properties Properties tup Save session Open in a tab Connect Cancel	
3. Si	elect SSH2.	Quick Connec Protocol: Hostname: Port: Username: Authentication Passwor Publicke Keyboar GSSAPI	tt SSH2 SSH1 Telnet Telnet/SSL RLogin Serial TAPI on d y d Interactive	tup Save session	

Input the Hostname (IP address), port (22) and user name. Click Connect.



Quick Connect		
Protocol: Hostname: Port: Username: Authentication Password PublicKey Keyboard I GSSAPI	SSH2 10.5.5.12 22 Firewall: None admin Interactive	
Show quick c	onnect on startup Save session Open in a tab Connect Cancel	

4. Input the password and press OK.

Enter Secure	Shell Password	×
admin@10.5. enter a passv	5.12 requires a password. Please vord now.	OK Cancel
Usemame:	admin	
Password:	••••••	

5. Input "zhimakaimen", get the device key.



6. Access to OA System, Tech-Support->PSH QUERY->PSH Shell, Input the device key, then get the security code.



017年10月16日 星期— 欢迎您: huangbaojun		
nu « PSH Shell ×		
PASSWORD Reset		中文 ENGLISH
	Device Password Resetting	
	Custom Message *	
	Security Trust	
	Device Key	
	BQAAAChXvnRkdUbMDws=	
	Security Code	
	zrSvgSqgU05TwUtL/EfJqS0DTKYP6rGgTx2mKRD1zKyRssFSaLh3 MYFFMbbNae2wjFe8111Q4HCAVaRFbkhwztmVaRP423aVd2mHoscs	vuRL irTi
	Vf1V7U10TVgSnjv2Yau+R2jdfU2LhdNdLhBj/1+/yn1+D2Q4GdnS 3Tc=	9eF+
		\checkmark

7. Input this security code, then enter to the device debug mode.



8. Go to Options-Session Options—Log file settings, check the parameters shown as below.



	Log File		
Logon Actions Serial Terminal	Log file name F:\\og\%S-%M%	D.log	
Emulation Modes Emacs Mapped Keys Advanced Appearance ANSI Color Window Log File Printing X/Y/Zmodem	Options Prompt for filen Start log upon o Raw log Start pow log	ame © Overwrite file connect © Append to file	
	Upon connect:	[%M-%D %h:%m:%s]	
	On each line:	[%M-%D %h:%m:%s] n data	
	Log file name and %H - hostname %S - session name	custom log data substitutions %M - 2-digit month %h - 2-digit hour %D - 2-digit day See Help for more	2

- **9.** Enter 'outputOpen', if hint error message, please enter outputClose first, then input outputOpen again.
- **10.** Save all the information during the troubleshooting time then send the log file to us.

First Choice for Security Professionals HIKVISION Technical Support