

SSH Client Commands

This chapter contains the following sections:

Note DSA keys are not supported when the device is in FIPS compliant mode. Therefore, when in FIPS compliant mode:

- Executing commands based on a DSA key will fail.
- The default DSA keys and certificates are not generated.

- ip ssh-client authentication, on page 2
- ip ssh-client change server password, on page 3
- ip ssh-client key, on page 4
- ip ssh-client password, on page 7
- ip ssh-client server authentication, on page 8
- ip ssh-client server fingerprint, on page 9
- ip ssh-client source-interface, on page 10
- ipv6 ssh-client source-interface, on page 11
- ip ssh-client username, on page 12
- show ip ssh-client, on page 13
- show ip ssh-client server, on page 15

ip ssh-client authentication

To define the SSH client authentication method used by the local SSH clients to be authenticated by remote SSH servers, use the **ip ssh-client authentication** command in Global Configuration mode.

To return to default, use the **no** format of the command.

Syntax

ip ssh-client authentication {**password** | **public-key** {**rsa** | **dsa**}}

no ip ssh-client authentication

Parameters

- **password**—Username and password are used for authentication.
- **public-key rsa**—Username and RSA public key are used for authentication.
- **public-key dsa**—Username and DSA public key are used for authentication.

Default Configuration

Username and password are used for authentication by the local SSH clients.

Command Mode

Global Configuration mode

User Guidelines

A user can use the **ip ssh-client key** command to generate/configure RSA/DSA keys if SSH authentication is by public key. Otherwise, the default keys generated by the switch are used.

Example

The following example specifies that, username and public key are used for authentication:

```
switchxxxxxx(config)# ip ssh-client authentication public-key rsa
```

ip ssh-client change server password

To change a password of an SSH client on a remote SSH server, use the **ip ssh-client change server password** command in Global Configuration mode.

Syntax

ip ssh-client change server password server {*host* | *ip-address* | *ipv6-address*} **username** *username* **old-password** *old-password* **new-password** *new-password*

Parameters

- ***host***—DNS name of a remote SSH server.
- ***ip-address***—Specifies the IP address of a remote SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.
- ***username*** —Username of the local SSH clients (1 - 70 characters).
- ***old-password*** —Old password of the local SSH client (1 - 70 characters).
- ***new-password***—New password for the local SSH client (1 - 70 characters). The password cannot include the characters "@" and ":".

Command Mode

Global Configuration mode

User Guidelines

Use the command to change a password on a remote SSH server. Use the **ip ssh-client password** command to change the SSH client password of the switch's SSH client so that it matches the new password set on the remote SSH server.

Example

The following example changes a password of the local SSH clients:

```
switchxxxxxx(config)# ip ssh-client change server password server 10.7.50.155 username john
 old-password &&&@@@aaff new-password &&&@@@aaee
```

ip ssh-client key

To create a key pair for SSH client authentication by public key (either by generating a key or by importing a key), use the **ip ssh-client key** command in Global Configuration mode. To remove a key, use the **no** form of the command.

Syntax

ip ssh-client key {**dsa** | **rsa**} {**generate | key-pair** *privkey pubkey***}**

encrypted ip ssh-client key {**dsa** | **rsa**} **key-pair** *encrypted-privkey pubkey*

no ip ssh-client key [**dsa** | **rsa**]

Parameters

- **dsa**—DSA key type.
- **rsa**—RSA key type.
- **key-pair**—Key that is imported to the device.

  privkey—Plaintext private key.

  encrypted-privkey—private key is in encrypted format.

  pubkey—The plaintext pubic key.

Default Configuration

The application creates a key automatically; this is the default key.

Command Mode

Global Configuration mode

User Guidelines

When using the keyword **generate**, a private key and a public key of the given type (RSA/DSA) are generated for the SSH client. Downloading a configuration file with a Key Generating command is not allowed, and such download will fail.

When using the keyword **key-pair,** the user can import a key-pair created by another device. In this case, the keys must follow the format specified by RFC 4716.

If the specified key already exists, a warning will be issued before replacing the existing key with a new key.

Use the **no ip ssh-client key** command to remove a key pair. Use this command without specifying a key-type to remove both key pairs.

Table 1: Keys, Defaults and Users

From/To	Show	Show (detailed)	Copy/Upload of Running Config	Copy/Upload of Startup Config	Downloa (TFTP/Ba
Startup Config	Only user-defined	N/A	All keys (default and user)	N/A	All keys
Running Config	Keys are not displayed.	All keys (default and user)	N/A	Only user defined.	Same as
Text-based CLI (TFTP/Backup)	As it was copied.	N/A	All keys (default and user)	Only user defined.	As a text

If no keys are included in text-based configuration file, the device generates it's own keys during initialization. If the Running Configuration contains default keys (not user-defined), the same default keys remain.

Example 1 - In the following example, a key pair of the RSA type is created:

```
switchxxxxxx(config)# ip ssh-client key rsa generate
The SSH service is generating a private RSA key.
This may take a few minutes, depending on the key size.
```

Example 2 - In the following example, both public and private keys of the RSA type are imported (private key as plaintext):

```
switchxxxxxx(config)# ip ssh-client key rsa key-pair
Please paste the input now, add a period (.) on a separate line after the input
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDH6CU/2KYRl8rYrK5+TIvwS4zvhBmiC4I31m9cR/1iRTFViMRuJ++TEr
p9ssqWyI1Ti9d0jzmG0N3jHzp2je5/DUTHZXvYaUzchBDnsPTJo8dyiBl4YBqYHQgCjUhk
tXqvloy+1uxRJTAaLVXCBAmuIU/kMLoEox8/zwjB/jsF9wIBIwKBgC2xZ5mQmvy0+yo2GU
FwlQO5f0yweuM11J8McTmqDgfVTRrdbroXwbs3exVqsfaUPY9wa8Le6JPX+DPp4XovEfC/
iglZBSC8SeDmI2U7D6HrkAyD9HHf/r32jukB+5Z7BlHPz2Xczs2clOOwrnToy+YTzjLUxy
WS7V/IxbBllipLAkEA/QluVSCfFmdMlZxaEfJVzqPO1cF8guovsWLteBf/gqHuvbHuNy0t
OWEpObKZs1m/mtCWppkgcqgrB0oJaYbUFQJBAMo/cCrkyhsiV/+ZsryeD26NbPEKiak16V
Tz2ayDstidGuuvcvm2YF7DjM6n6NYz3+/ZLyc5n82okbld1NhDONsCQQCmSAas+C4HaHQn
zSU+/lWlDI88As4qJN2DMmGJbtsbVHhQxWIHAG4tBVWa8bVl2+RPyuan/jnk8irniGyVza
FPAkEAiq8oV+1XYxA8V39V/a42d7FvRjMckUmKDl4Rmt32+u9i6sFzaWcdgs87+2vS3AZQ
afQDE5U6YSMiGLVewC4YWwJBAOFZmhO+dIlxT8Irzf2cUZGggopfnX6Y+L+Yl09MuZHbwH
tXaBGj6ayMYvXnloONecnApBjGEm37YVwKjO2DV2w=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMfoJT/YphGXytisrn5Mi/BLjO+EGaILgjfWb1xH/WJFMVWIxG4n75MSun2yyp
bIjVOL13SPOYbQ3eMfOnaN7n8NRMdle9hpTNyEEOew9Mmjx3KIGXhgGpgdCAKNSGS1eq+W
jL7W7FElMBotVcIECa4hT+QwugSjHz/PCMH+OwX3AgEj
-----END RSA PUBLIC KEY-----
```

Example 3 - In the following example, both public and private keys of the DSA type are imported (private key as encrypted):

```
switchxxxxxx(config)# encrypted ip ssh-client key rsa key-pair
(Need to encrypted SSH client RSA key pair, for example:)
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
gxeOjs6OzGRtL4qstmQg1B/4gexQblfa56RdjgHAMejvUT02elYmNi+m4aTu6mlyXPHmYP
lXlXny7jZkHRvgg8EzcppEB0O3yQzq3kNi756cMg4Oqbkm7TUOtdqYFEz/h8rJJ0QvUFfh
BsEQ3e16E/OPitWgK43WTzedsuyFeOoMXR9BCuxPUJc2UeqQVM2IJt5OM0FbVt0S6oqXhG
sEEdoTlhlDwHWg97FcV7x+bEnPfzFGrmbrUxcxOxlkFsuCNo3/94PHK8zEXyWtrx2KoCDQ
qFRuM8uecpjmDh6MO2GURUVstctohEWEIVCIOr5SBCbciaxv5oS0jIzXMrJA==
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBALLOeh3css8tBL8ujFt3trcX0XJyJLlxxt4sGp8Q3ExlSRN25+Mcac6togpIEg
tIzk6t1IEJscuAih9Brwh1ovgMLRaMe25j5YjO4xG6Fp42nhHiRcie+YTS1o309EdZkiXa
QeJtLdnYL/r3uTIRVGbXI5nxwtfWpwEgxxDwfqzHAgEj
-----END RSA PUBLIC KEY-----
```

Example 4 - In the following example, a DSA key pair is removed:

```
switchxxxxxx(config)# no ip ssh-client key dsa
```

Example 5 - In the following example, all key pairs (RSA and DSA types) are removed.

```
switchxxxxxx(config)# no ip ssh-client key
```

ip ssh-client password

To configure the password for SSH client authentication by password, use the **ip ssh-client password** command in Global Configuration mode. To return to default, use the **no** form of the command.

Syntax

ip ssh-client password *string*

encrypted ip ssh-client password *encrypted-string*

no ip ssh-client password

Parameters

- ***string***—Password for the SSH clients (1 - 70 characters). The password cannot include the characters "@" and ":".
- ***encrypted-string***—Password for the SSH client in encrypted form.

Default Configuration

The default password is anonymous.

Command Mode

Global Configuration mode

User Guidelines

If authentication is configured to use a password (using the command **ip ssh-client authentication**), use the **ip ssh-client password** command to define the password.

If the **encrypted** keyword is used, the password must be in the encrypted form.

Use the command **ip ssh-client change server password** to change the password on the remote SSH server so that it will match the new password of the SSH client.

Example

The following example specifies a plaintext password for the local SSH clients:

```
switchxxxxxx(config)# ip ssh-client password &&&111aaff
```

ip ssh-client server authentication

To enable remote SSH server authentication by the SSH client, use the **ip ssh-client server authentication** command in Global Configuration mode.

To disable remote SSH server authentication, use the **no** form of the command.

Syntax

ip ssh-client server authentication

no ip ssh-client server authentication

Parameters

This command has no arguments or keywords.

Default Configuration

SSH server authentication is disabled

Command Mode

Global Configuration mode

User Guidelines

When remote SSH server authentication is disabled, any remote SSH server is accepted (even if there is no entry for the remote SSH server in the SSH Trusted Remote Server table).

When remote SSH server authentication is enabled, only trusted SSH servers are accepted. Use the **ip ssh-client server fingerprint** command to configure trusted SSH servers.

Example

The following example enables SSH server authentication:

```
switchxxxxxx(config)# ip ssh-client server authentication
```

ip ssh-client server fingerprint

To add a trusted server to the Trusted Remote SSH Server Table, use the **ip ssh-client server fingerprint** command in Global configuration mode. To remove an entry or all entries from the Trusted Remote SSH Server Table, use the **no** form of the command.

Syntax

ip ssh-client server fingerprint {*host* | *ip-address*} *fingerprint*

no ip ssh-client server fingerprint [*host* | *ip-address*]

Parameters

- ***host***—DNS name of an SSH server.
- ***ip-address***—Specifies the address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.
- ***fingerprint***—Fingerprint of the SSH server public key (32 Hex characters).

Default Configuration

The Trusted Remote SSH Server table is empty.

Command Mode

Global Configuration mode

User Guidelines

Fingerprints are created by applying a cryptographic hash function to a public key. Fingerprints are shorter than the keys they refer to, making it simpler to use (easier to manually input than the original key). Whenever the switch is required to authenticate an SSH server's public key, it calculates the received key's fingerprint and compares it to the previously-configured fingerprint.

The fingerprint can be obtained from the SSH server (the fingerprint is calculated when the public key is generated on the SSH server).

The **no ip ssh-client server fingerprint** command removes all entries from the Trusted Remote SSH Server table.

Example

In the following example, a trusted server is added to the Trusted Servers table (with and without a separator ":"):

```
switchxxxxxx(config)# ip ssh-client server fingerprint 1.1.1.1
DC789788DC88A988127897BCBB789788
switchxxxxxx(config)# ip ssh-client server fingerprint 1.1.1.1
DC:78:97:88:DC:88:A9:88:12:78:97:BC:BB:78:97:88
```

ip ssh-client source-interface

To specify the source interface which IPv4 address will be used as the Source IPv4 address for communication with IPv4 SSH servers, use the **ip ssh-client source-interface** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

ip ssh-client source-interface *interface-id*

no ip ssh-client **source-interface**

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface then the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SSH servers.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# ip ssh-client source-interface vlan 100
```

ipv6 ssh-client source-interface

To specify the source interface whose IPv6 address will be used as the Source IPv6 address for communication with IPv6 SSH servers, use the **ipv6 ssh-client source-interface** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

ipv6 ssh-client source-interface *interface-id*

no ipv6 ssh-client **source-interface**

Parameters

- ***interface-id***—(Optional) Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface then the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SSH servers.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# ipv6 ssh-client source-interface vlan 100
```

ip ssh-client username

To configure the SSH client username of the switch, use the **ip ssh-client username** command in Global Configuration mode.

To return to default, use the **no** form of the command.

Syntax

ip ssh-client username *string*

no ip ssh-client username

Parameters

- ***string***—Username of the SSH client.The length is 1 - 70 characters. The username cannot include the characters "@" and ":".

Default Configuration

The default username is anonymous

Command Mode

Global Configuration mode

User Guidelines

The configured username is used when SSH client authentication is done both by password or by key.

Example

The following example specifies a username of the SSH client:

switchxxxxxx(config)# **ip ssh-client username jeff**

show ip ssh-client

To display the SSH client credentials, both default and user-defined keys, use the **show ip ssh-client** command in Privilege EXEC mode.

Syntax

show ip ssh-client

show ip ssh-client {mypubkey | key} {dsa | rsa}

Parameters

- **dsa**—Specifies displaying the DSA key type.
- **rsa**—Specifies displaying the RSA key type.
- **mypubkey**—Specifies that only the public key is selected to be displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Use the command with a specific key-type to display the SSH client key; You can either specify display of public key or private key, or with no parameter to display both private and public keys. The keys are displayed in the format specified by RFC 4716.

Example 1. The following example displays the authentication method and the RSA public key:

```
switchxxxxxx# show ip ssh-client mypubkey rsa
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:   DSA key
Username:                john
Key Source:              User Defined
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAudGEIaPARsKoVJVjs8XALAKqBN1WmXnY
kUf5oZjGY3QoMGDvNipQvdN3YmwLUBiKk31WvVwFB3N2K5a7fUBjoblkdjns
QKTKZiu4V+IL5rds/bD6LOEkJbjUzOjmp9hlIkh9uc0ceZ3ZxMtKhnORLrXL
aRyxYszO5FuirTo6xW8=
---- END SSH2 PUBLIC KEY ----
Public Key Fingerprint: 84:f8:24:db:74:9c:2d:51:06:0a:61:ef:82:13:88:88
```

Example 2. The following example displays the authentication method and DSA private key in encrypted format:

```
switchxxxxxx# show ip ssh-client key DSA
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:   DSA key
Username:                john
Key Source:              User Defined
Public Key Fingerprint: 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: RSA Public Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----
---- BEGIN SSH2 PRIVATE KEY ----
Comment: DSA Private Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PRIVATE KEY ----
```

Example 3. The following example displays the SSH client authentication method, the username and the password:

```
switchxxxxxx# show ip ssh-client
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:   DSA key
Username:                anonymous (default)
Password:                anonymous (default)
password(Encrypted):     KzGgzpYa7GzCHhaveSJDehGJ6L3Yf9ZBAU5nsxSxwic=
```

show ip ssh-client server

To display the SSH remote server authentication method and the Trusted Remote SSH Server table, use the **show ip ssh-client server** command in Privilege EXEC Configuration mode.

Syntax

show ip ssh-client server [*host* | *ip-address*]

Parameters

- ***host***—(Optional) DNS name of an SSH server.
- ***ip-address***—(Optional) IP Address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.

Default Configuration

None

Command Mode

Privileged EXEC mode

User Guidelines

If a specific SSH server is specified, only the fingerprint of this SSH server is displayed. Otherwise, all known servers are displayed.

Example 1 - In the following example, the SSH remote server authentication method and all trusted remote SSH servers are displayed:

```
switchxxxxxx# show ip ssh-client server
SSH Server Authentication is enabled
server address: 11.1.0.1
  Server Key Fingerprint: 5a:8d:1d:b5:37:a4:16:46:23:59:eb:44:13:b9:33:e9
server address: 192.165.204.111
  Server Key Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
server address: 4002:0011::12
  Server Key Fingerprint: a5:34:44:44:27:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

Example 2 - The following example displays the authentication method and DSA private key in encrypted format:

```
switchxxxxxx# show ip ssh-client key DSA
Authentication method:   DSA key
Username:                john
Key Source:              Default
Public Key Fingerprint: 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
```

```
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----
---- BEGIN SSH2 PRIVATE KEY ----
Comment: DSA Private Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PRIVATE KEY ----
```

Example 3 - The following example displays the SSH client authentication method, the username and the password:

```
switchxxxxxx# show ip ssh-client
Authentication method: password (default)
Username: anonymous (default)
password(Encrypted): KzGgzpYa7GzCHhaveSJDehGJ6L3Yf9ZBAU5
```