Contents

SSH commands 1

SSH server commands 1
display ssh server 1
display ssh user-information 2
free ssh 3
scp server enable 4
sftp server enable 5
sftp server idle-timeout 5
ssh server acl 6
ssh server acl-deny-log enable 7
ssh server authentication-retries 8
ssh server authentication-timeout 8
ssh server compatible-ssh1x enable 9
ssh server dscp 10
ssh server enable 10
ssh server ipv6 acl 11
ssh server ipv6 dscp 12
ssh server key-re-exchange enable 12
ssh server pki-domain 13
ssh server port 14
ssh server rekey-interval 14
ssh user 15
SSH client commands 18
bye 18
cd 18
cdup 19
delete 19
delete ssh client server-public-key 19
dir 20
display scp client source 21
display sftp client source 21
display ssh client server-public-key 22
display ssh client source 23
exit 24
get 24
help 25
ls 25
mkdir 26
put 27
pwd 27
quit 28
remove 28
rename 28
rmdir 29
scp 29
scp client ipv6 source 33
scp client source 33
scp ipv6 34
scp ipv6 suite-b 38
scp suite-b 40
sftp 41
sftp client ipv6 source 44
sftp client source 45
sftp ipv6 46
sftp ipv6 suite-b 49
sftp suite-b 51
ssh client ipv6 source 52

ssh client source ····· 53
ssh2 ····· 54
ssh2 ipv6 ····· 57
ssh2 ipv6 suite-b ····· 60
ssh2 suite-b ····· 62
SSH2 commands ····· 64
display ssh2 algorithm ····· 64
ssh2 algorithm cipher ····· 65
ssh2 algorithm key-exchange ····· 66
ssh2 algorithm mac ····· 67
ssh2 algorithm public-key ····· 68

SSH commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

SSH server commands

display ssh server

Use **display ssh server** on an SSH server to display the SSH server status or sessions.

Syntax

display ssh server { **session** | **status** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

session: Specifies the SSH server sessions.

status: Specifies the SSH server status.

Examples

Display the SSH server status.

```
<Sysname> display ssh server status
 Stelnet server: Disable
 SSH version : 2.0
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
 SFTP server Idle-Timeout: 10 minute(s)
 NETCONF server: Disable
 SCP server: Disable
 SSH Server PKI domain name: aaa
```

Table 1 Command output

Field	Description
Stelnet server	Whether the Stelnet server is enabled.
SSH version	SSH protocol version. When the SSH supports SSH1, the protocol version is 1.99. Otherwise, the protocol version is 2.
SSH authentication-timeout	Authentication timeout timer.

Field	Description
SSH server key generating interval	Minimum interval for updating the RSA server key pair.
SSH authentication retries	Maximum number of authentication attempts for SSH users.
SFTP server	Whether the SFTP server is enabled.
SFTP server Idle-Timeout	SFTP connection idle timeout timer.
NETCONF server	Whether NETCONF over SSH is enabled.
SCP server	Whether the SCP server is enabled.
SSH Server PKI domain name	Name of the PKI domain specified for the SSH server.

Display the SSH server sessions.

```
<Sysname> display ssh server session
UserPid   SessID Ver   Encrypt    State          Retries  Serv     Username
 184       0     2.0   aes128-cbc Established    1        Stelnet  abc@123
```

Table 2 Command output

Field	Description
UserPid	User process ID.
SessID	Session ID.
Ver	Protocol version of the SSH server.
Encrypt	Encryption algorithm used on the SSH server.
State	Session state: • **Init**—Initialization. • **Ver-exchange**—Version negotiation. • **Keys-exchange**—Key exchange. • **Auth-request**—Authentication request. • **Serv-request**—Session service request. • **Established**—The session is established. • **Disconnected**—The session is terminated.
Retries	Number of authentication failures.
Serv	Service type: • SCP. • SFTP. • Stelnet. • NETCONF.
Username	Username that the client uses to log in to the server.

display ssh user-information

Use **display ssh user-information** to display information about SSH users on an SSH server.

Syntax

display ssh user-information [*username*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

username: Specifies an SSH username, a case-sensitive string of 1 to 80 characters. If you do not specify an SSH user, this command displays information about all SSH users.

Usage guidelines

This command displays information only about SSH users that are configured by using the **ssh user** command on the SSH server.

Examples

Display information about all SSH users.

```
<Sysname> display ssh user-information
 Total ssh users:2
 Username            Authentication-type  User-public-key-name  Service-type
 yemx                password                                   Stelnet|SFTP
 test                publickey            pubkey                SFTP
```

Table 3 Command output

Field	Description
Total ssh users	Total number of SSH users.
Authentication-type	Authentication methods: • Password authentication. • Publickey authentication. • Password-publickey authentication. • Any authentication.
User-public-key-name	Public key name of the user. This field is empty if the authentication method is password authentication.
Service-type	Service types: • Stelnet. • SFTP. • SCP. • NETCONF. If multiple service types are available for an SSH user, they are separated by vertical bars (|).

Related commands

ssh user

free ssh

Use **free ssh** to disconnect SSH sessions.

Syntax

free ssh { **user-ip** { *ip-address* | **ipv6** *ipv6-address* } [**port** *port-number*] | **user-pid** *pid-number* | **username** *username* }

Views

User view

Predefined user roles

network-admin

Parameters

user-ip: Specifies the user IP address of the SSH sessions to be disconnected.

ip-address: Specifies the user IPv4 address of the SSH sessions to be disconnected.

ipv6 *ipv6-address:* Specifies the user IPv6 address of the SSH sessions to be disconnected.

port *port-number*: Specifies the source port of the SSH session to be disconnected, in the range of 1 to 65535. If you do not specify a source port, this command disconnects all SSH sessions using the specified IP address.

user-pid *pid-number*: Specifies the user process ID of the SSH session to be disconnected, in the range of 1 to 2147483647. To view the user process ID of an SSH session, use the **display ssh server session** command.

username *username*: Specifies the username of the SSH session to be disconnected. To view the username of an SSH session, use the **display ssh server session** command.

Examples

Disconnect the SSH sessions with user IPv4 address 192.168.15.45.

```
<Sysname> free ssh user-ip 192.168.15.45
Releasing SSH connection. Continue? [Y/N]:y
```

Disconnect the SSH sessions with user IPv6 address 2000::11.

```
<Sysname> free ssh user-ip ipv6 2000::11
Releasing SSH connection. Continue? [Y/N]:y
```

Disconnect the SSH session with user process ID 417.

```
<Sysname> free ssh user-pid 417
Releasing SSH connection. Continue? [Y/N]:y
```

Disconnect the SSH session with username **sshuser**.

```
<Sysname> free ssh username sshuser
Releasing SSH connection. Continue? [Y/N]:y
```

Related commands

display ssh server session

scp server enable

Use **scp server enable** to enable the SCP server.

Use **undo scp server enable** to disable the SCP server.

Syntax

scp server enable

undo scp server enable

Default

The SCP server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the SCP server.

```
<Sysname> system-view
[Sysname] scp server enable
```

Related commands

display ssh server

sftp server enable

Use **sftp server enable** to enable the SFTP server.

Use **undo sftp server enable** to disable the SFTP server.

Syntax

sftp server enable

undo sftp server enable

Default

The SFTP server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the SFTP server.

```
<Sysname> system-view
[Sysname] sftp server enable
```

Related commands

display ssh server

sftp server idle-timeout

Use **sftp server idle-timeout** to set the idle timeout timer for SFTP connections on an SFTP server.

Use **undo sftp server idle-timeout** to restore the default.

Syntax

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

Default

The idle timeout timer is 10 minutes for SFTP connections.

Views

System view

Predefined user roles

network-admin

Parameters

time-out-value: Specifies an idle timeout timer in the range of 1 to 35791 minutes.

Usage guidelines

If an SFTP connection is idle when the idle timeout timer expires, the system automatically terminates the connection. To promptly release connection resources, set the idle timeout timer to a small value when many SFTP connections concurrently exist.

Examples

Set the idle timeout timer to 500 minutes for SFTP connections.

```
<Sysname> system-view
[Sysname] sftp server idle-timeout 500
```

Related commands

display ssh server

ssh server acl

Use **ssh server acl** to specify an ACL to control IPv4 SSH connections to the server.

Use **undo ssh server acl** to restore the default.

Syntax

ssh server acl { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

undo ssh server acl

Default

No ACLs are specified and all IPv4 SSH clients can initiate SSH connections to the server.

Views

System view

Predefined user roles

network-admin

Parameters

advanced-acl-number: Specifies an IPv4 advanced ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies an IPv4 basic ACL number in the range of 2000 to 2999.

mac *mac-acl-number:* Specifies a Layer 2 ACL by its number in the range of 4000 to 4999.

Usage guidelines

The ACL specified in this command filters IPv4 SSH clients' connection requests. Only the IPv4 SSH clients that the ACL permits can access the device. If the specified ACL does not exist or contains no rules, all IPv4 SSH clients can access the device.

The ACL takes effect only on SSH connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users at 1.1.1.1 to initiate SSH connections to the server.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ssh server acl 2001
```

Related commands

display ssh server

ssh server acl-deny-log enable

Use **ssh server acl-deny-log enable** to enable logging for SSH login attempts that are denied by the SSH login control ACL.

Use **undo ssh server acl-deny-log enable** to disable logging for SSH login attempts that are denied by the SSH login control ACL.

Syntax

ssh server acl-deny-log enable

undo ssh server acl-deny-log enable

Default

Logging is disabled for SSH login attempts that are denied by the SSH login control ACL.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Only SSH clients permitted by the SSH login control ACL can access the SSH server. The logging feature generates log messages for SSH login attempts that are denied by the SSH login control ACL, and sends the messages to the information center.

For information about log message output, see the information center in *Network Management and Monitoring Configuration Guide*. For information about configuring an SSH login control ACL, see the **ssh server acl** or **ssh server ipv6 acl** command.

Examples

Enable logging for SSH login attempts that are denied by the SSH login control ACL.

```
<Sysname> system-view
[Sysname] ssh server acl-deny-log enable
```

Related commands

ssh server acl

ssh server ipv6 acl

ssh server authentication-retries

Use **ssh server authentication-retries** to set the maximum number of authentication attempts for SSH users.

Use **undo ssh server authentication-retries** to restore the default.

Syntax

ssh server authentication-retries *retries*

undo ssh server authentication-retries

Default

The maximum number of authentication attempts is 3 for SSH users.

Views

System view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of authentication attempts for SSH users, in the range of 1 to 5.

Usage guidelines

Setting the maximum number of authentication attempts prevents malicious hacking of usernames and passwords.

If the total number of authentication attempts exceeds the upper limit specified in this command, further authentication is not allowed.

- For **any** authentication, an authentication attempt is a publickey or password authentication process.
- For **password-publickey** authentication, an authentication attempt contains both a publickey authentication process and a password authentication process. The server first uses publickey authentication, and then uses password authentication to authenticate the SSH user.

This configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Set the maximum number of authentication attempts to 4 for SSH users.

```
<Sysname> system-view
[Sysname] ssh server authentication-retries 4
```

Related commands

display ssh server

ssh server authentication-timeout

Use **ssh server authentication-timeout** to set the SSH user authentication timeout timer on the SSH server.

Use **undo ssh server authentication-timeout** to restore the default.

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

Default

The SSH user authentication timeout timer is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-out-value: Specifies an authentication timeout timer in the range of 1 to 120 seconds.

Usage guidelines

If a user does not finish the authentication when the timeout timer expires, the connection cannot be established.

To prevent malicious occupation of TCP connections, set the authentication timeout timer to a small value.

Examples

Set the authentication timeout timer to 10 seconds for SSH users.

```
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

Related commands

display ssh server

ssh server compatible-ssh1x enable

Use **ssh server compatible-ssh1x enable** to enable the SSH server to support SSH1 clients.

Use **undo ssh server compatible-ssh1x** [**enable**] to restore the default.

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x [**enable**]

Default

The SSH server does not support SSH1 clients.

Views

System view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command is not available in FIPS mode.

The **undo** form of this command restores the default setting whether you specify the **enable** keyword or not.

This configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Enable the SSH server to support SSH1 clients.

```
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

Related commands

display ssh server

ssh server dscp

Use **ssh server dscp** to set the DSCP value in the IPv4 SSH packets that the SSH server sends to SSH clients.

Use **undo ssh server dscp** to restore the default.

Syntax

ssh server dscp *dscp-value*

undo ssh server dscp

Default

The DSCP value is 48 in IPv4 SSH packets.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the IPv4 SSH packets, in the range of 0 to 63. A bigger DSCP value represents a higher priority.

Usage guidelines

The DSCP value of a packet specifies the priority of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 30 for IPv4 SSH packets.

```
<Sysname> system-view
[Sysname] ssh server dscp 30
```

ssh server enable

Use **ssh server enable** to enable the Stelnet server.

Use **undo ssh server enable** to disable the Stelnet server.

Syntax

ssh server enable

undo ssh server enable

Default

The Stelnet server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the Stelnet server.

```
<Sysname> system-view
[Sysname] ssh server enable
```

Related commands

display ssh server

ssh server ipv6 acl

Use **ssh server ipv6 acl** to specify an ACL to control IPv6 SSH connections to the server.

Use **undo ssh server ipv6 acl** to restore the default.

Syntax

ssh server ipv6 acl { **ipv6** { *advanced-acl-number* | *basic-acl-number* } | **mac** *mac-acl-number* }

undo ssh server ipv6 acl

Default

No ACLs are specified and all IPv6 SSH clients can initiate SSH connections to the server.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

advanced-acl-number: Specifies an IPv6 advanced ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies an IPv6 basic ACL number in the range of 2000 to 2999.

mac *mac-acl-number:* Specifies a Layer 2 ACL by its number in the range of 4000 to 4999.

Usage guidelines

The ACL specified in this command filters IPv6 SSH clients' connection requests. Only the IPv6 SSH clients that the ACL permits can access the device. If the specified ACL does not exist or contains no rules, all IPv6 SSH clients can access the device.

The ACL takes effect only on SSH connections that are initiated after the ACL configuration.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure ACL 2001 and permit only the users on the subnet 1::1/64 to initiate SSH connections to the server.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl6-ipv6-basic-2001] rule permit source 1::1 64
[Sysname-acl6-ipv6-basic-2001] quit
[Sysname] ssh server ipv6 acl ipv6 2001
```

Related commands

display ssh server

ssh server ipv6 dscp

Use **ssh server ipv6 dscp** to set the DSCP value in the IPv6 SSH packets that the SSH server sends to SSH clients.

Use **undo ssh server ipv6 dscp** to restore the default.

Syntax

ssh server ipv6 dscp *dscp-value*

undo ssh server ipv6 dscp

Default

The DSCP value is 48 in IPv6 SSH packets.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the IPv6 SSH packets, in the range of 0 to 63. A bigger DSCP value represents a higher priority.

Usage guidelines

The DSCP value of an IPv6 packet specifies the priority of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value to 30 for IPv6 SSH packets.

```
<Sysname> system-view
[Sysname] ssh server ipv6 dscp 30
```

ssh server key-re-exchange enable

Use **ssh server key-re-exchange enable** to enable SSH algorithm renegotiation and key re-exchange.

Use **undo ssh server key-re-exchange enable** to disable SSH algorithm renegotiation and key re-exchange.

Syntax

ssh server key-re-exchange enable [**interval** *interval*]

undo ssh server key-re-exchange enable

Default

SSH algorithm renegotiation and key re-exchange are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies an interval for SSH algorithm renegotiation and key re-exchange, in the range of 1 to 24 hours. If you do not specify this option, the SSH server initiates SSH algorithm renegotiation and key re-exchange at intervals of 1 hour.

Usage guidelines

This command is not available in FIPS mode.

This command enables the SSH server to renegotiate algorithms and re-exchange keys at regular intervals after the first algorithm negotiation and key exchange with SSH clients.

This command takes effect only on new SSH connections that are established after the command is configured, and it does not affect existing SSH connections.

Examples

Enable SSH algorithm renegotiation and key re-exchange.

```
<Sysname> sysname
[Sysname] ssh server key-re-exchange enable
```

ssh server pki-domain

Use **ssh server pki-domain** to specify a PKI domain for an SSH server.

Use **undo ssh server pki-domain** to restore the default.

Syntax

ssh server pki-domain *domain-name*

undo ssh server pki-domain

Default

No PKI domain is specified for an SSH server.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the name of the PKI domain used to verify the SSH server. The PKI domain name is a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

Examples

Specify PKI domain **serverpkidomain** for the SSH server.

```
<Sysname> system-view
```

```
[Sysname] ssh server pki-domain serverpkidomain
```

ssh server port

Use **ssh server port** to specify the SSH service port.

Use **undo ssh server port** to restore the default.

Syntax

ssh server port *port-number*

undo ssh server port

Default

The SSH service port is 22.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

If you modify the SSH port number when the SSH server is enabled, the SSH service is restarted and all SSH connections are terminated after the modification. SSH users must reconnect to the SSH server to access the server.

If you set the SSH port to a well-known port number, the service that uses the well-known port number might fail to start. Well-known port numbers are in the range of 1 to 1024.

Examples

Set the SSH service port to 1025.

```
<Sysname> system-view
[Sysname] ssh server port 1025
```

ssh server rekey-interval

Use **ssh server rekey-interval** to set the minimum interval for updating the RSA server key pair.

Use **undo ssh server rekey-interval** to restore the default.

Syntax

ssh server rekey-interval *interval*

undo ssh server rekey-interval

Default

The minimum interval for updating the RSA server key pair is 0 hours. The system does not update the RSA server key pair.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the minimum interval for updating the RSA server key pair, in the range of 1 to 24 hours.

Usage guidelines

This command is not available in FIPS mode.

Periodically updating the RSA server key pair prevents malicious hacking to the key pair and enhances security of the SSH connections.

The system starts to count down the configured minimum update interval after the first SSH1 user logs in to the server. If a new SSH1 user logs in to the server after the interval, the system performs the following operations:

1. Updates the RSA server key pair.
2. Uses the updated RSA server key pair for key pair negotiation with the new user.
3. Resets the interval and starts to count down the interval again.

This command takes effect only on SSH1 clients.

Examples

Set the minimum interval to 3 hours for updating the RSA server key pair.

```
<Sysname> system-view
[Sysname] ssh server rekey-interval 3
```

Related commands

display ssh server

ssh user

Use **ssh user** to create an SSH user and specify the service type and authentication method.

Use **undo ssh user** to delete an SSH user.

Syntax

In non-FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign** { **pki-domain** *domain-name* | **publickey** *keyname*&<1-6> }] }

undo ssh user *username*

In FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | **password-publickey** [**assign** { **pki-domain** *domain-name* | **publickey** *keyname*&<1-6> }] }

undo ssh user *username*

Default

No SSH users exist.

Views

System view

Predefined user roles

network-admin

Parameters

username: Specifies an SSH username, a case-sensitive string of 1 to 80 characters. The username cannot be **a**, **al**, or **all**. In addition, the username cannot include vertical bars (|), colons (:), asterisks (*), question marks (?), or angle brackets (< >). The at sign (@), slash (/), and backslash (\) can only be used to append ISP domain names to usernames in the *pureusername@domain*, *pureusername*/*domain*, and *domain**pureusername* format. Do not include hyphens (-) in the username of an SCP user. Otherwise, SCP logins using that username will fail.

service-type: Specifies a service type for the SSH user.

- **all**: Specifies service types Stelnet, SFTP, SCP, and NETCONF.
- **scp**: Specifies the service type SCP.
- **sftp**: Specifies the service type SFTP.
- **stelnet**: Specifies the service type Stelnet.
- **netconf**: Specifies the service type NETCONF.

authentication-type: Specifies an authentication method for the SSH user.

- **password**: Specifies password authentication. This authentication method provides easy and fast encryption, but it is vulnerable. It can work with AAA to implement user authentication, authorization, and accounting.
- **any**: Specifies either password authentication or publickey authentication.
- **password-publickey**: Specifies both password authentication and publickey authentication for SSH2 clients. In SSH2, the password-publickey authentication method provides higher security. If the client runs SSH1, this keyword specifies either password authentication or publickey authentication.
- **publickey**: Specifies publickey authentication. This authentication method has complicated and slow encryption, but it provides strong authentication that can defend against brute-force attacks. This authentication method is easy to use. If this method is configured, the authentication process completes automatically without entering any password.

assign: Specifies parameters used for client verification.

- **pki-domain** *domain-name*: Specifies the PKI domain that verifies the client's digital certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). The server uses the CA certificate that is saved in the PKI domain to verify the client's digital certificate. In this scenario, the server does not need to save clients' public keys in advance.
- **publickey** *keyname*&<1-6>: Specifies a space-separated list of up to six SSH client public keys. The *keyname* argument represents the SSH client's public key configured on the server. It is a case-sensitive string of 1 to 64 characters. The server uses the client's public key to check the validity of the client. If the public key file of the client is changed, you must update the client's public key on the server promptly. If you specify multiple client public keys, the device verifies the user identity by using the public keys in the order they are specified. The user is valid if the user passes one public key check.

Usage guidelines

Use this command to configure an SSH user depending on the authentication method.

- If the authentication method is **publickey**, you must create an SSH user and a local user on the SSH server. The two users must have the same username, so that the SSH user can be assigned the correct working directory and user role.
- If the authentication method is **password**, you must perform one of the following tasks:

- For local authentication, configure a local user on the SSH server.
- For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

You do not need to create an SSH user by using the **ssh user** command. However, if you want to display all SSH users, including the password-only SSH users, for centralized management, you can use this command to create them. If such an SSH user has been created, make sure you have specified the correct service type and authentication method.

- If the authentication method is **password-publickey** or **any**, you must create an SSH user on the SSH server and perform one of the following tasks:
  - For local authentication, configure a local user on the SSH server.
  - For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

  In either case, the local user or the SSH user configured on the remote authentication server must have the same username as the SSH user.

For an SFTP or SCP user, the working directory depends on the authentication method.

- If the authentication method is **publickey** or **password-publickey**, the working directory is specified by the **authorization-attribute** command in the associated local user view.
- If the authentication method is **password**, the working directory is authorized by AAA.

For an SSH user, the user role also depends on the authentication method.

- If the authentication method is **publickey** or **password-publickey**, the user role is specified by the **authorization-attribute** command in the associated local user view.
- If the authentication method is **password**, the user role is authorized by AAA.

If you use this command to specify a host public key or a PKI domain for a user multiple times, the most recent configuration takes effect. If neither a host public key nor a PKI domain is specified for the user, the user uses certificate authentication for login. The server uses the PKI domain of its own certificate to verify the client's certificate.

The command configuration does not affect logged-in users. It affects only users that attempt to log in after the configuration.

Examples

Create an SSH user named **user1**. Specify the service type as **sftp** and the authentication method as **password-publickey** for the user. Assign the host public key **key1** to the user.

```
<Sysname> system-view
[Sysname] ssh user user1 service-type sftp authentication-type password-publickey assign publickey key1
```

Create a local device management user named **user1**. Specify the password as **123456TESTplat&!** in plain text and the service type as **ssh** for the user. Assign the working directory **flash:** and the **network-admin** user role to the user.

```
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] password simple 123456TESTplat&!
[Sysname-luser-manage-user1] service-type ssh
[Sysname-luser-manage-user1] authorization-attribute work-directory flash: user-role network-admin
```

Related commands

authorization-attribute

display ssh user-information

local-user

pki domain

SSH client commands

bye

Use **bye** to terminate the connection with the SFTP server and return to user view.

Syntax

bye

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as the **exit** and **quit** commands.

Examples

Terminate the connection with the SFTP server.

```
sftp> bye
<Sysname>
```

cd

Use **cd** to change the working directory on the SFTP server.

Syntax

cd [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-path: Specifies the name of a directory on the server.

Usage guidelines

You can use the **cd ..** command to return to the upper-level directory.

You can use the **cd /** command to return to the root directory of the system.

Examples

Change the working directory to **new1**.

```
sftp> cd new1
Current Directory is:/new1
sftp> pwd
Remote working directory: /new1
sftp>
```

cdup

Use **cdup** to return to the upper-level directory.

Syntax

cdup

Views

SFTP client view

Predefined user roles

network-admin

Example

Return to the upper-level directory from the current working directory **/test1**.

```
sftp> cd test1
Current Directory is:/test1
sftp> pwd
Remote working directory: /test1
sftp> cdup
Current Directory is:/
sftp> pwd
Remote working directory: /
sftp>
```

delete

Use **delete** to delete a file from the SFTP server.

Syntax

delete *remote-file*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-file: Specifies a file by its name.

Usage guidelines

This command has the same function as the **remove** command.

Examples

Delete file **temp.c** from the SFTP server.

```
sftp> delete temp.c
Removing /temp.c
```

delete ssh client server-public-key

Use **delete ssh client server-public-key** to delete server public key information saved in the public key file of the SSH client.

Syntax

delete ssh client server-public-key [**server-ip** *ip-address*]

Views

System view

Predefined user roles

network-admin

Parameters

server-ip *ip-address*: Specifies the IP address of the server whose public key information will be deleted. If you do not specify a server IP address, this command deletes the public keys of all servers from the client's public key file.

Examples

Delete all server public keys saved in the public key file of the SSH client.

```
<Sysname> system-view
[Sysname] delete ssh client server-public-key
Public keys of all SSH servers will be deleted. Continue? [Y/N]:y
```

Delete the public key of server 2.2.2.1 saved in the public key file of the SSH client.

```
<Sysname> system-view
[Sysname] delete ssh client server-public-key server-ip 2.2.2.1
```

dir

Use **dir** to display information about the files and subdirectories under a directory.

Syntax

dir [**-a** | **-l**] [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

-a: Displays detailed information about files and subdirectories under a directory in a list, including the files and subdirectories with names starting with dots (.).

-l: Displays detailed information about the files and subdirectories under a directory in a list, excluding the files and subdirectories with names starting with dots (.).

remote-path: Specifies the name of the directory to be queried. If you do not specify this argument, the command displays information about the files and subdirectories under the current working directory.

Usage guidelines

If you do not specify both of the **-a** and **-l** keywords, this command displays the names of the files and subdirectories under a directory.

This command has the same function as the **ls** command.

Examples

Display detailed information about the files and subdirectories under the current directory, including the files and subdirectories with names starting with dots (.).

```
sftp> dir -a
drwxrwxrwx    2 1        1               512 Dec 18 14:12 .
drwxrwxrwx    2 1        1               512 Dec 18 14:12 ..
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

Display detailed information about the files and subdirectories under the current directory, excluding the files and subdirectories with names starting with dots (.).

```
sftp> dir -l
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

display scp client source

Use **display scp client source** to display the source IP address configuration of the SCP client.

Syntax

display scp client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source IP address configuration of the SCP client.

```
<Sysname> display scp client source
The source IP address of the SCP client is 192.168.0.1.
The source IPv6 address of the SCP client is 2:2::2:2.
```

Related commands

scp client ipv6 source
scp client source

display sftp client source

Use **display sftp client source** to display the source IP address configuration of the SFTP client.

Syntax

display sftp client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source IP address configuration of the SFTP client.

```
<Sysname> display sftp client source
The source IP address of the SFTP client is 192.168.0.1
The source IPv6 address of the SFTP client is 2:2::2:2.
```

Related commands

sftp client ipv6 source

sftp client source

display ssh client server-public-key

Use **display ssh client server-public-key** to display server public key information saved in the public key file of the SSH client.

Syntax

display ssh client server-public-key [**server-ip** *ip-address*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

server-ip *ip-address*: Specifies the IP address of the server whose public key information will be displayed. If you do not specify a server IP address, this command displays the public keys of all servers saved in the client's public key file.

Usage guidelines

When a user connects to an unauthenticated server and selects to save the server's public key, the server public key will be saved to the public key file. Server public key information saved in the public key file is not available in the configuration file. To display such server public key information on the SSH client, you must use this command.

Examples

Display all server public keys saved in the public key file of the SSH client.

```
<Sysname> display ssh client server-public-key
 Server address: 10.153.124.209
 Key type: ecdsa-sha2-nistp256
 Key length: 256
 Key code:
   AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAOGpJfwJExK
   eYb53KKqmrZ0V/XnYZKZEchyN9ax1IBt+toIXHeW5NfBE5ymeklPSNgQNhcndkU/
   422fT15UmgM=

 Server address: 2.2.2.1
 Key type: rsa
 Key length: 1024
 Key code:
   AAAAB3NzaC1yc2EAAAADAQABAAAAgQDIUrHbeLx/W7xElB1Ny3zeA8/uV9K6sj1p
```

```
  dSlhx5XcOatdNMoD/sioYgSsy9IxKZPqBs+vadqx/wCCB5+T2GLLu2qgaT0P9J+v
  RR/9Y8fI2b4tS7PoNf/QKDVD7XnoiZ+dqd0tnnRf6GV+74cp8ZEUQdAoTeDzzaAh
  7t6FbxrNrQ==
```

Display the public key of server 2.2.2.1 saved in the public key file of the SSH client.

```
<Sysname> display ssh client server-public-key server-ip 2.2.2.1
 Server address: 2.2.2.1
 Key type: rsa
 Key length: 1024
 Key code:
   AAAAB3NzaC1yc2EAAAADAQABAAAAgQDIUrHbeLx/W7xElB1Ny3zeA8/uV9K6sj1p
   dSlhx5XcOatdNMoD/sioYgSsy9IxKZPqBs+vadqx/wCCB5+T2GLLu2qgaT0P9J+v
   RR/9Y8fI2b4tS7PoNf/QKDVD7XnoiZ+dqd0tnnRf6GV+74cp8ZEUQdAoTeDzzaAh
   7t6FbxrNrQ==
```

Table 4 Command output

Field	Description
Server address	IP address of the SSH server.
Key type	Type of the public key: • **dsa**—DSA public key. • **ecdsa-sha2-nistp256**—256-bit ECDSA public key created by using the secp256r1 curve. • **ecdsa-sha2-nistp384**—384-bit ECDSA public key created by using the secp384r1 curve. • **rsa**—RSA public key.
Key length	Length of the public key, in bits.
Key code	Content of the public key.

display ssh client source

Use **display ssh client source** to display the source IP address configuration of the Stelnet client.

Syntax

display ssh client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source IP address configuration of the Stelnet client.

```
<Sysname> display ssh client source
The source IP address of the SSH client is 192.168.0.1
The source IPv6 address of the SSH client is 2:2::2:2.
```

Related commands

ssh client ipv6 source

ssh client source

exit

Use **exit** to terminate the SFTP connection and return to user view.

Syntax

exit

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as the **bye** and **quit** commands.

Examples

Terminate the SFTP connection.

```
sftp> exit
<Sysname>
```

get

Use **get** to download a file from the SFTP server and save it locally.

Syntax

get *remote-file* [*local-file*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-file: Specifies the name of a file on the SFTP server.

local-file: Specifies the name for the local file. If you do not specify this argument, the file will be saved locally with the same name as the file on the SFTP server.

Examples

Download file **temp1.c** and save it as **temp.c** locally.

```
sftp> get temp1.c temp.c
Fetching /temp1.c to temp.c
/temp.c                                                100% 1424     1.4KB/s   00:00
```

help

Use **help** to display help information on the SFTP client.

Syntax

help

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as entering the question mark (?).

Examples

Display help information on the SFTP client.

```
sftp> help
Available commands:
  bye                          Quit sftp
  cd [path]                    Change remote directory to 'path'
  cdup                         Change remote directory to the parent directory
  delete path                  Delete remote file
  dir [-a|-l][path]            Display remote directory listing
       -a                        List all filenames
       -l                        List filename including the specific
                                 information of the file
  exit                         Quit sftp
  get remote-path [local-path] Download file
  help                         Display this help text
  ls [-a|-l][path]             Display remote directory
       -a                          List all filenames
       -l                          List filename including the specific
                                   information of the file
  mkdir path                   Create remote directory
  put local-path [remote-path] Upload file
  pwd                          Display remote working directory
  quit                         Quit sftp
  rename oldpath newpath       Rename remote file
  remove path                  Delete remote file
  rmdir path                   Delete remote empty directory
  ?                            Synonym for help
```

ls

Use **ls** to display information about the files and subdirectories under a directory.

Syntax

ls [**-a** | **-l**] [*remote-path*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

-a: Displays detailed information about files and subdirectories under a directory in a list, including the files and subdirectories with names starting with dots (.).

-l: Displays detailed information about the files and subdirectories under a directory in a list, excluding the files and subdirectories with names starting with dots (.).

remote-path: Specifies the name of the directory to be queried. If you do not specify this argument, the command displays information about the files and subdirectories under the current working directory.

Usage guidelines

If you do not specify both of the **-a** and **-l** keywords, this command displays the names of the files and subdirectories under a directory.

This command has the same function as the **dir** command.

Examples

Display detailed information about the files and subdirectories under the current directory, including the files and subdirectories with names starting with dots (.).

```
sftp> ls -a
drwxrwxrwx    2 1        1               512 Dec 18 14:12 .
drwxrwxrwx    2 1        1               512 Dec 18 14:12 ..
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

Display detailed information about the files and subdirectories under the current working directory, excluding the files and subdirectories with names starting with dots (.).

```
sftp> ls -l
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

mkdir

Use **mkdir** to create a directory on the SFTP server.

Syntax

mkdir *remote-path*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-path: Specifies the name of a directory.

Examples

Create a directory named **test** on the SFTP server.

```
sftp> mkdir test
```

put

Use **put** to upload a local file to the SFTP server.

Syntax

put *local-file* [*remote-file*]

Views

SFTP client view

Predefined user roles

network-admin

Parameters

local-file: Specifies the name of a local file.

remote-file: Specifies the name of a file on an SFTP server. If you do not specify this argument, the file will be remotely saved with the same name as the local file.

Examples

Upload the local file **startup.bak** to the SFTP server and save it as **startup01.bak**.

```
sftp> put startup.bak startup01.bak
Uploading startup.bak to /startup01.bak
startup01.bak                                 100% 1424     1.4KB/s   00:00
```

pwd

Use **pwd** to display the current working directory of the SFTP server.

Syntax

pwd

Views

SFTP client view

Predefined user roles

network-admin

Examples

Display the current working directory of the SFTP server.

```
sftp> pwd
Remote working directory: /
```

The output shows that the current working directory is the root directory.

quit

Use **quit** to terminate the SFTP connection and return to user view.

Syntax

quit

Views

SFTP client view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command has the same function as the **bye** and **exit** commands.

Examples

Terminate the SFTP connection.

```
sftp> quit
<Sysname>
```

remove

Use **remove** to delete a file from the SFTP server.

Syntax

remove *remote-file*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-file: Specifies a file by its name.

Usage guidelines

This command has the same function as the **delete** command.

Examples

Delete file **temp.c** from the SFTP server.

```
sftp> remove temp.c
Removing /temp.c
```

rename

Use **rename** to change the name of a file or directory on the SFTP server.

Syntax

rename *old-name new-name*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

oldname: Specifies the name of an existing file or directory.

newname: Specifies a new name for the existing file or directory.

Examples

Change the name of a file on the SFTP server from **temp1.c** to **temp2.c**.

```
sftp> dir
aa.pub  temp1.c
sftp> rename temp1.c temp2.c
sftp> dir
aa.pub  temp2.c
```

rmdir

Use **rmdir** to delete a directory from the SFTP server.

Syntax

rmdir *remote-path*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-path: Specifies a directory.

Examples

Delete subdirectory **temp1** under the current directory on the SFTP server.

```
sftp> rmdir temp1
```

scp

Use **scp** to establish a connection to an IPv4 SCP server and transfer files with the server.

Syntax

In non-FIPS mode:

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** |

ecdh-sha2-nistp384 } | **prefer-stoc-cipher** { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* }| **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * [**user** *username* [**password** *password*]]

In FIPS mode:

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* }| **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * [**user** *username* [**password** *password*]]

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.

- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, SHA2-512, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv4 address or source interface for SCP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SCP packets. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify that interface's IPv4 address as the source IPv4 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv4 address of this interface is the source IPv4 address of the SCP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

user *username*: Specifies an SCP username, a case-sensitive string of 1 to 80 characters. If the username contains an ISP domain name, use the *pureusername@domain*, *pureusername*/*domain*, or *domain**pureusername* format.

password *password*: Specifies a password in plaintext form, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

If you do not specify a username and password in the command, you must provide the username and password in an interactive way.

If the SCP server uses publickey authentication, the password specified by this command is ignored.

Examples

Connect the SCP client to SCP server **200.1.1.1**. Specify the public key of the server as **svkey**, and download file **abc.txt** from the server. The SCP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> scp 200.1.1.1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher
aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key
svkey
```

```
Username:
```

scp client ipv6 source

Use **scp client ipv6 source** to configure the source IPv6 address for SCP packets that are sent by the SCP client.

Use **undo scp client ipv6 source** to restore the default.

Syntax

scp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo scp client ipv6 source

Default

The source IPv6 address for outgoing SCP packets is not configured. The SCP client automatically selects an IPv6 address for outgoing SCP packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SCP client selects the interface's address that most specifically matches the destination address of outgoing SCP packets as the source address of the SCP packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 SCP connections. The source IPv6 address specified in the **scp ipv6** command takes effect only on the current IPv6 SCP connection. If you specify the source IPv6 address in both this command and the **scp ipv6** command, the source IPv6 address specified in the **scp ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SCP packets.

```
<Sysname> system-view
[Sysname] scp client ipv6 source ipv6 2:2::2:2
```

Related commands

display scp client source

scp client source

Use **scp client source** to configure the source IPv4 address for SCP packets that are sent by the SCP client.

Use **undo scp client source** to restore the default.

Syntax

scp client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo scp client source

Default

The source IPv4 address for outgoing SCP packets is not configured. The SCP client uses the primary IPv4 address of the output interface in the matching routing entry as the source IPv4 address for outgoing SCP packets.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SCP client uses the primary IPv4 address of the interface as the source address of outgoing SCP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all SCP connections. The source IPv4 address specified in the **scp** command takes effect only on the current SCP connection. If you specify the source IPv4 address in both this command and the **scp** command, the source IPv4 address specified in the **scp** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SCP packets.

```
<Sysname> system-view
[Sysname] scp client source ip 192.168.0.1
```

Related commands

display scp client source

scp ipv6

Use **scp ipv6** to establish a connection to an IPv6 SCP server and transfer files with the server.

Syntax

In non-FIPS mode:

scp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name*} | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc**

|**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* }| **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] * [**user** *username* [**password** *password*]]

In FIPS mode:

scp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name*} | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* }| **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] * [**user** *username* [**password** *password*]]

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for SCP packets. This option is used only when the server uses a link-local address to provide the SCP service for the client. The specified output interface on the SCP client must have a link-local address.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.

- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.

  x509v3-ecdsa-sha2-nistp384: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, SHA2-512, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.

- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv6 address or source interface for IPv6 SCP packets. By default, the device automatically selects a source address for IPv6 SCP packets in compliance with RFC 3484. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify that interface's IPv6 address as the source IPv6 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SCP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

user *username*: Specifies an SCP username, a case-sensitive string of 1 to 80 characters. If the username contains an ISP domain name, use the *pureusername@domain*, *pureusername*/*domain*, or *domain**pureusername* format.

password *password*: Specifies a password in plaintext form, a case-sensitive string of 1 to 63 characters.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

If you do not specify a username and password in the command, you must provide the username and password in an interactive way.

If the SCP server uses publickey authentication, the password specified by this command is ignored.

Examples

Connect an SCP client to SCP server **2000::1**. Specify the public key of the server as **svkey**, and download file **abc.txt** from the server. The SCP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> scp ipv6 2000::1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher
aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key
svkey
Username:
```

scp ipv6 suite-b

Use **scp ipv6 suite-b** to establish a connection to an IPv6 SCP server based on Suite B algorithms and transfer files with the server.

Syntax

scp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] * [**user** *username* [**password** *password*]]

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for SCP packets. Specify this option when the server uses a link-local address to provide the SCP service for the client. The specified output interface on the SCP client must have a link-local address.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 5.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31

characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

source: Specifies a source IPv6 address or source interface for IPv6 SCP packets. By default, the device automatically selects a source address for IPv6 SCP packets in compliance with RFC 3484. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify the IPv6 address of the interface as the source IPv6 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SCP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

user *username*: Specifies an SCP username, a case-sensitive string of 1 to 80 characters. If the username contains an ISP domain name, use the *pureusername@domain*, *pureusername*/*domain*, or *domain**pureusername* format.

password *password*: Specifies a password in plaintext form, a case-sensitive string of 1 to 63 characters.

Usage guidelines

Table 5 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

If you do not specify a username and password in the command, you must provide the username and password in an interactive way.

If the SCP server uses publickey authentication, the password specified by this command is ignored.

Examples

Use the 192-bit Suite B algorithms to establish a connection to SCP server **2000::1** and download the file **abc.txt** from the server. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> scp ipv6 2000::1 get abc.txt suite-b 192-bit pki-domain clientpkidomain
server-pki-domain serverpkidomain
Username:
```

scp suite-b

Use **scp suite-b** to establish a connection to an SCP server based on Suite B algorithms and transfer files with the server.

Syntax

scp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * [**user** *username* [**password** *password*]]

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file, a case-sensitive string of 1 to 255 characters.

destination-file-name: Specifies the name of the target file, a case-sensitive string of 1 to 255 characters. If you do not specify this argument, the target file uses the same file name as the source file.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 6.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

source: Specifies a source IP address or source interface for SCP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SCP packets. As a best practice to ensure successful SCP connections, specify a loopback interface as the source interface or specify the IPv4 address of the interface as the source IPv4 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv4 address of this interface is the source IPv4 address of the SCP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

user *username*: Specifies an SCP username, a case-sensitive string of 1 to 80 characters. If the username contains an ISP domain name, use the *pureusername@domain*, *pureusername*/*domain*, or *domain**pureusername* format.

password *password*: Specifies a password in plaintext form, a case-sensitive string of 1 to 63 characters.

Usage guidelines

Table 6 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

If you do not specify a username and password in the command, you must provide the username and password in an interactive way.

If the SCP server uses publickey authentication, the password specified by this command is ignored.

Examples

Use the 128-bit Suite B algorithms to establish a connection to SCP server **200.1.1.1** and download the file **abc.txt** from the server. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> scp 200.1.1.1 get abc.txt suite-b 128-bit pki-domain clientpkidomain
server-pki-domain serverpkidomain
Username:
```

sftp

Use **sftp** to establish a connection to an IPv4 SFTP server and enter SFTP client view.

Syntax

In non-FIPS mode:

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name*} | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1**

| **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | { **public-key** *keyname* | **server-pki-domain** *domain-name* }| **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

In FIPS mode:

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name*| **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* }| **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3

public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, SHA2-512, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

public-key *keyname*: Specifies the server's host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv4 address or source interface for the SFTP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SFTP packets. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify that interface's IPv4 address as the source IPv4 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SFTP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Connect an SFTP client to SFTP server **10.1.1.2** and specify the public key of the server as **svkey**. The SFTP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> sftp 10.1.1.2 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
```

sftp client ipv6 source

Use **sftp client ipv6 source** to configure the source IPv6 address for SFTP packets that are sent by the SFTP client.

Use **undo sftp client ipv6 source** to restore the default.

Syntax

sftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo sftp client ipv6 source

Default

The source IPv6 address for outgoing SFTP packets is not configured. The SFTP client automatically selects an IPv6 address for outgoing SFTP packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SFTP client selects the interface's address that most specifically matches the destination address of outgoing SFTP packets as the source address of the SFTP packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 SFTP connections. The source IPv6 address specified in the **sftp ipv6** command takes effect only on the current IPv6 SFTP connection. If you specify the source IPv6 address both in this command and the **sftp ipv6** command, the source IPv6 address specified in the **sftp ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SFTP packets.

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

Related commands

display sftp client source

sftp client source

Use **sftp client source** to configure the source IPv4 address for SFTP packets that are sent by the SFTP client.

Use **undo sftp client source** to restore the default.

Syntax

sftp client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo sftp client source

Default

The source IPv4 address for outgoing SFTP packets is not configured. The SFTP client uses the primary IPv4 address of the output interface in the matching routing entry as the source IPv4 address of outgoing SFTP packets.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SFTP client uses the primary IPv4 address of the interface as the source address of outgoing SFTP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all SFTP connections. The source IPv4 address specified in the **sftp** command takes effect only on the current SFTP connection. If you specify the source IPv4 address both in this command and the **sftp** command, the source IPv4 address specified in the **sftp** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SFTP packets.

```
<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1
```

Related commands

display sftp client source

sftp ipv6

Use **sftp ipv6** to connect an SFTP client to an IPv6 SFTP server and enter SFTP client view.

Syntax

In non-FIPS mode:

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* |{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

In FIPS mode:

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name*| **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** |

sha2-512 }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* }| **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SFTP packets. This option is used only when the server uses a link-local address to provide the SFTP service for the client. The specified output interface on the SFTP client must have a link-local address.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.

- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, SHA2-512, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

public-key *keyname*: Specifies the host public key of the server that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv6 address or source interface for IPv6 SFTP packets. By default, the device automatically selects a source address for IPv6 SFTP packets in compliance with RFC 3484. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify that interface's IPv6 address as the source IPv6 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SFTP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Connect an SFTP client to SFTP server **2000::1** and specify the public key of the server as **svkey**. The SFTP client uses publickey authentication. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> sftp ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
Username:
```

sftp ipv6 suite-b

Use **sftp ipv6 suite-b** to establish a connection to an IPv6 SFTP server based on Suite B algorithms and enter SFTP client view.

Syntax

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SFTP packets. The specified outgoing interface must have a link-local address. This

option is used only when the server uses a link-local address to provide the SFTP service for the client.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 7.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

source: Specifies a source IP address or source interface for IPv6 SFTP packets. By default, the device automatically selects a source address for IPv6 SFTP packets in compliance with RFC 3484. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify the IPv6 address of the interface as the source IPv6 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IP address of the IPv6 SFTP packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

Table 7 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

Examples

Use the 192-bit Suite B algorithms to establish a connection to SFTP server **2000::1**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> sftp ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

sftp suite-b

Use **sftp suite-b** to establish a connection to an IPv4 SFTP server based on Suite B algorithms and enter SFTP client view.

Syntax

sftp *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress** **zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 8.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

source: Specifies a source IP address or source interface for the SFTP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SFTP packets. As a best practice to ensure successful SFTP connections, specify a loopback interface as the source interface or specify the IPv4 address of the interface as the source IPv4 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SFTP packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

Table 8 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

Examples

Use the 128-bit Suite B algorithms to establish a connection to SFTP server **10.1.1.2**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> sftp 10.1.1.2 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

ssh client ipv6 source

Use **ssh client ipv6 source** to configure the source IPv6 address for SSH packets that are sent by the Stelnet client.

Use **undo ssh client ipv6 source** to restore the default.

Syntax

ssh client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo ssh client ipv6 source

Default

The source IPv6 address for outgoing SSH packets is not configured. The Stelnet client automatically selects an IPv6 address for outgoing SSH packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The Stelnet client selects the interface's address that most specifically matches the destination address of outgoing SSH packets as the source address of the SSH packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 Stelnet connections. The source IPv6 address specified in the **ssh2 ipv6** command takes effect only on the current IPv6 Stelnet connection. If you specify the source IPv6 address both in this command and the **ssh2 ipv6** command, the source IPv6 address specified in the **ssh2 ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SSH packets that are sent by the Stelnet client.

```
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

Related commands

display ssh client source

ssh client source

Use **ssh client source** to configure the source IPv4 address for SSH packets that are sent by the Stelnet client.

Use **undo ssh client source** to restore the default.

Syntax

ssh client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo ssh client source

Default

The source IPv4 address for outgoing SSH packets is not configured. The Stelnet client uses the primary IPv4 address of the output interface in the matching routing entry as the source address of outgoing SSH packets.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The Stelnet client uses the primary IPv4 address of the interface as the source address of outgoing SSH packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all Stelnet connections. The source IPv4 address specified in the **ssh2** command takes effect only on the current Stelnet connection. If you specify the source IPv4

address both in this command and the **ssh2** command, the source IPv4 address specified in the **ssh2** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SSH packets.

```
<Sysname> system-view
[Sysname] ssh client source ip 192.168.0.1
```

Related commands

display ssh client source

ssh2

Use **ssh2** to establish a connection to an IPv4 Stelnet server.

Syntax

In non-FIPS mode:

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name*| **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | **escape** *character* |{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

In FIPS mode:

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name*} | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* }| **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.
- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, SHA2-512, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.

- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

public-key *keyname*: Specifies the host public key of the server that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv4 address or source interface for SSH packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SSH packets. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify that interface's IPv4 address as the source IPv4 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SSH packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line.

As a best practice, use the default escape character (~). Do not use any character in SSH usernames as the escape character.

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Establish a connection to Stelnet server **3.3.3.3** and specify the public key of the server as **svkey**. The Stelnet client uses publickey authentication. Specify the dollar sign ($) as the escape character. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> ssh2 3.3.3.3 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
escape $
```

ssh2 ipv6

Use **ssh2 ipv6** to establish a connection to an IPv6 Stelnet server.

Syntax

In non-FIPS mode:

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name*| **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | **escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* }| **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

In FIPS mode:

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher**

{ **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* }| **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name:* Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SSH packets. This option is used only when the server uses a link-local address to provide the Stelnet service for the client. The specified output interface on the Stelnet client must have a link-local address.

identity-key: Specifies a public key algorithm for publickey authentication of the client. The default is DSA in non-FIPS mode and is RSA in FIPS mode. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature or certificate by using the local private key that is associated with the specified algorithm.

- **dsa**: Specifies public key algorithm DSA.
- **ecdsa-sha2-nistp256**: Specifies the ECDSA algorithm with 256-bit key strength.
- **ecdsa-sha2-nistp384**: Specifies the ECDSA algorithm with 384-bit key strength.
- **rsa**: Specifies public key algorithm RSA.
- **x509v3-ecdsa-sha2-nistp256**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.
- **x509v3-ecdsa-sha2-nistp384**: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.
- **pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument is a case-insensitive string of 1 to 31 characters. When the x509v3 public key algorithm is used, you must specify this option for the client to get the correct local certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is AES128-CTR. Supported algorithms are DES-CBC, 3DES-CBC, AES128-CBC, AES128-CTR, AES128-GCM, AES192-CTR, AES256-CBC, AES256-CTR, and AES256-GCM, in ascending order of security strength and computation time.

- **3des-cbc**: Specifies encryption algorithm 3DES-CBC.
- **aes128-cbc**: Specifies encryption algorithm AES128-CBC.
- **aes128-ctr**: Specifies encryption algorithm AES128-CTR.

- **aes128-gcm**: Specifies encryption algorithm AES128-GCM.
- **aes192-ctr**: Specifies encryption algorithm AES192-CTR.
- **aes256-cbc**: Specifies encryption algorithm AES256-CBC.
- **aes256-ctr**: Specifies encryption algorithm AES256-CTR.
- **aes256-gcm**: Specifies encryption algorithm AES256-GCM.
- **des-cbc**: Specifies encryption algorithm DES-CBC.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is SHA2-256. Supported algorithms are MD5, MD5-96, SHA1, SHA1-96, SHA2-256, SHA2-512, in ascending order of security strength and computation time.

- **md5**: Specifies HMAC algorithm HMAC-MD5.
- **md5-96**: Specifies HMAC algorithm HMAC-MD5-96.
- **sha1**: Specifies HMAC algorithm HMAC-SHA1.
- **sha1-96**: Specifies HMAC algorithm HMAC-SHA1-96.
- **sha2-256**: Specifies HMAC algorithm HMAC-SHA2-256.
- **sha2-512**: Specifies HMAC algorithm HMAC-SHA2-512.

prefer-kex: Specifies the preferred key exchange algorithm. The default is ecdh-sha2-nistp256. Supported algorithms are diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, and ecdh-sha2-nistp384, in ascending order of security strength and computation time.

- **dh-group-exchange-sha1**: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1-sha1**: Specifies key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14-sha1**: Specifies key exchange algorithm diffie-hellman-group14-sha1.
- **ecdh-sha2-nistp256**: Specifies key exchange algorithm ecdh-sha2-nistp256.
- **ecdh-sha2-nistp384**: Specifies key exchange algorithm ecdh-sha2-nistp384.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is AES128-CTR. Supported algorithms are the same as the client-to-server encryption algorithms (see the **prefer-ctos-cipher** keyword).

prefer-stoc-hmac: Specifies the preferred server-to-client HMAC algorithm. The default is SHA2-256. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

public-key *keyname*: Specifies the server by its host public key that the client uses to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

source: Specifies a source IPv6 address or source interface for IPv6 SSH packets. By default, the device automatically selects a source address for IPv6 SSH packets in compliance with RFC 3484.

As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify that interface's IPv6 address as the source IPv6 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SSH packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line.

As a best practice, use the default escape character (~). Do not use any characters in SSH usernames as the escape character.

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Establish a connection to Stelnet server **2000::1** and specify the public key of the server as **svkey**. The SSH client uses publickey authentication. Specify the dollar sign ($) as the escape character. Use the following algorithms:

- Preferred key exchange algorithm: **dh-group14-sha1**.
- Preferred server-to-client encryption algorithm: **aes128-cbc**.
- Preferred client-to-server HMAC algorithm: **sha1**.
- Preferred server-to-client HMAC algorithm: **sha1-96**.
- Preferred compression algorithm: **zlib**.

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
escape $
```

ssh2 ipv6 suite-b

Use **ssh2 ipv6 suite-b** to establish a connection to an IPv6 Stelnet server based on Suite B algorithms.

Syntax

ssh2 ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number:* Specifies an output interface by its type and number for IPv6 SSH packets. Specify this option when the server uses a link-local address to provide the Stelnet service for the client. The specified output interface on the Stelnet client must have a link-local address.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 9.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

source: Specifies a source IP address or source interface for IPv6 SSH packets. By default, the device automatically selects a source address for IPv6 SSH packets in compliance with RFC 3484. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify the IPv6 address of the interface as the source IPv6 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IP address of the IPv6 SSH packets.
- **ipv6** *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

Table 9 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line. As a best practice, use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Use the 192-bit Suite B algorithms to establish a connection to Stelnet server **2000::1**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> ssh2 ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

ssh2 suite-b

Use **ssh2 suite-b** to establish a connection to an IPv4 Stelnet server based on Suite B algorithms.

Syntax

ssh2 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

suite-b: Specifies the Suite B algorithms. If neither the 128-bit keyword nor the 192-bit keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see Table 10.

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes (').

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. Invalid characters are tildes (~), asterisks (*), backslashes (\), vertical bars (|), colons (:), dots (.), angle brackets (< >), quotation marks ("), and apostrophes ('). If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies compression algorithm zlib.

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

source: Specifies a source IP address or source interface for SSH packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SSH packets. As a best practice to ensure successful Stelnet connections, specify a loopback interface as the source interface or specify the IPv4 address of the interface as the source IPv4 address.

- **interface** *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SSH packets.
- **ip** *ip-address*: Specifies a source IPv4 address.

Usage guidelines

Table 10 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AES128-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
192-bit	ecdh-sha2-nistp384	AES256-GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AES128-GCM AES256-GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next

line. As a best practice, use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Use the 128-bit Suite B algorithms to establish a connection to Stelnet server **3.3.3.3**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> ssh2 3.3.3.3 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

SSH2 commands

display ssh2 algorithm

Use **`display ssh2 algorithm`** to display algorithms used by SSH2 in the algorithm negotiation stage.

Syntax

`display ssh2 algorithm`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display algorithms used by SSH2 in the algorithm negotiation stage.

```
<Sysname> display ssh2 algorithm
 Key exchange algorithms : ecdh-sha2-nistp256 ecdh-sha2-nistp384 dh-group-exchange-sha1
dh-group14-sha1 dh-group1-sha1
 Public key algorithms : x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 rsa dsa
 Encryption algorithms : aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm
aes128-cbc 3des-cbc aes256-cbc des-cbc
 MAC algorithms : sha2-256 sha2-512 sha1 md5 sha1-96 md5-96
```

Table 11 Command output

Field	Description
Key exchange algorithms	Key exchange algorithms in descending order of priority for algorithm negotiation.
Public key algorithms	Public key algorithms in descending order of priority for algorithm negotiation.
Encryption algorithms	Encryption algorithms in descending order of priority for algorithm negotiation.
MAC algorithms	HMAC algorithms in descending order of priority for algorithm negotiation.

Related commands

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm mac

ssh2 algorithm public-key

ssh2 algorithm cipher

Use **ssh2 algorithm cipher** to specify encryption algorithms for SSH2.

Use **undo ssh2 algorithm cipher** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm cipher { **3des-cbc** |**aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } *

undo ssh2 algorithm cipher

In FIPS mode:

ssh2 algorithm cipher { **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** } *

undo ssh2 algorithm cipher

Default

SSH2 uses encryption algorithms AES128-CTR, AES192-CTR, AES256-CTR, AES128-GCM, AES256-GCM, AES128-CBC, 3DES-CBC, AES256-CBC, and DES-CBC in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

3des-cbc: Specifies encryption algorithm 3DES-CBC.

aes128-cbc: Specifies encryption algorithm AES128-CBC.

aes128-ctr: Specifies encryption algorithm AES128-CTR.

aes128-gcm: Specifies encryption algorithm AES128-GCM.

aes192-ctr: Specifies encryption algorithm AES192-CTR.

aes256-cbc: Specifies encryption algorithm AES256-CBC.

aes256-ctr: Specifies encryption algorithm AES256-CTR.

aes256-gcm: Specifies encryption algorithm AES256-GCM.

des-cbc: Specifies encryption algorithm DES-CBC.

Usage guidelines

If you specify the encryption algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **aes256-cbc** as the encryption algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm cipher aes256-cbc
```

Related commands

display ssh2 algorithm

ssh2 algorithm key-exchange

ssh2 algorithm mac

ssh2 algorithm public-key

ssh2 algorithm key-exchange

Use **ssh2 algorithm key-exchange** to specify key exchange algorithms for SSH2.

Use **undo ssh2 algorithm key-exchange** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm key-exchange { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *

undo ssh2 algorithm key-exchange

In FIPS mode:

ssh2 algorithm key-exchange { **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *

undo ssh2 algorithm key-exchange

Default

SSH2 uses key exchange algorithms ecdh-sha2-nistp256, ecdh-sha2-nistp384, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1 in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

dh-group-exchange-sha1: Specifies key exchange algorithm diffie-hellman-group-exchange-sha1.

dh-group1-sha1: Specifies key exchange algorithm diffie-hellman-group1-sha1.

dh-group14-sha1: Specifies key exchange algorithm diffie-hellman-group14-sha1.

ecdh-sha2-nistp256: Specifies key exchange algorithm ecdh-sha2-nistp256.

ecdh-sha2-nistp384: Specifies key exchange algorithm ecdh-sha2-nistp384.

Usage guidelines

If you specify the key exchange algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **dh-group1-sha1** as the key exchange algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm key-exchange dh-group1-sha1
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm mac

ssh2 algorithm public-key

ssh2 algorithm mac

Use **ssh2 algorithm mac** to specify HMAC algorithms for SSH2.

Use **undo ssh2 algorithm mac** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm mac { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *

undo ssh2 algorithm mac

In FIPS mode:

ssh2 algorithm mac { **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *

undo ssh2 algorithm mac

Default

SSH2 uses HMAC algorithms SHA2-256, SHA2-512, SHA1, MD5, SHA1-96, and MD5-96 in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

md5: Specifies HMAC algorithm HMAC-MD5.

md5-96: Specifies HMAC algorithm HMAC-MD5-96.

sha1: Specifies HMAC algorithm HMAC-SHA1.

sha1-96: Specifies HMAC algorithm HMAC-SHA1-96.

sha2-256: Specifies HMAC algorithm HMAC-SHA2-256.

sha2-512: Specifies HMAC algorithm HMAC-SHA2-512.

Usage guidelines

If you specify the HMAC algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **md5** as the HMAC algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm mac md5
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm public-key

ssh2 algorithm public-key

Use **ssh2 algorithm public-key** to specify public key algorithms for SSH2.

Use **undo ssh2 algorithm public-key** to restore the default.

Syntax

In non-FIPS mode:

ssh2 algorithm public-key { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } *

undo ssh2 algorithm public-key

In FIPS mode:

ssh2 algorithm public-key { **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } *

undo ssh2 algorithm public-key

Default

SSH2 uses public key algorithms x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, RSA, and DSA in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

dsa: Specifies public key algorithm DSA.

ecdsa-sha2-nistp256: Specifies the ECDSA algorithm with 256-bit key strength.

ecdsa-sha2-nistp384: Specifies the ECDSA algorithm with 384-bit key strength.

rsa: Specifies public key algorithm RSA.

x509v3-ecdsa-sha2-nistp256: Specifies public key algorithm x509v3-ecdsa-sha2-nistp256.

x509v3-ecdsa-sha2-nistp384: Specifies public key algorithm x509v3-ecdsa-sha2-nistp384.

Usage guidelines

If you specify the public key algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify algorithm **dsa** as the public key algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm public-key dsa
```

Related commands

display ssh2 algorithm

ssh2 algorithm cipher

ssh2 algorithm key-exchange

ssh2 algorithm mac