Contents

SSH commands 1

SSH server commands 1
display ssh server 1
display ssh user-information 2
scp server enable 3
sftp server enable 4
sftp server idle-timeout 4
ssh server acl 5
ssh server authentication-retries 6
ssh server authentication-timeout 7
ssh server compatible-ssh1x enable 7
ssh server dscp 8
ssh server enable 9
ssh server ipv6 acl 9
ssh server ipv6 dscp 10
ssh server rekey-interval 11
ssh user 11

SSH client commands 14
bye 14
cd 14
cdup 15
delete 15
dir 16
display sftp client source 16
display ssh client source 17
exit 17
get 18
help 18
ls 19
mkdir 20
put 20
pwd 21
quit 21
remove 22
rename 22
rmdir 23
scp 23
scp ipv6 25
sftp 27
sftp client ipv6 source 28
sftp client source 29
sftp ipv6 30
ssh client ipv6 source 32
ssh client source 32
ssh2 33
ssh2 ipv6 35

SSH2 commands 37
display ssh2 algorithm 37
ssh2 algorithm cipher 38
ssh2 algorithm key-exchange 39
ssh2 algorithm mac 40
ssh2 algorithm public-key 40

SSH commands

The WX1800H series, WX2500H series, and WX3000H series access controllers do not support the **slot** keyword or the *slot-number* argument.

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** [**slot** *slot-number*] | **status** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

session: Displays the SSH server sessions.

status: Displays the SSH server status.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays SSH server session information for the active MPU.

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
```

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.

Display the SSH server sessions.

```
<Sysname> display ssh server session
UserPid   SessID Ver   Encrypt    State          Retries  Serv     Username   Idx
 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	Name of a user for logging in to the server.
Idx	Absolute number of the user line that the client uses to log in to the server. The value for this field is empty if the SSH connection for the user is not redirected.

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. If the authentication method is password authentication, this field does not display a value.
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

scp server enable

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

Use **undo scp server enable** to restore the default.

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 restore the default.

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.

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. If many SFTP connections concurrently exist, set a small value for the idle timeout timer to promptly release the connection resources.

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 user connections.

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

Syntax

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

undo ssh server acl

Default

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

Views

System view

Predefined user roles

network-admin

Parameters

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

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

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

Usage guidelines

The specified ACL filters IPv4 SSH users' connection requests. Only the IPv4 SSH users that the ACL permits can initiate SSH connections to the server.

All IPv4 SSH users can initiate SSH connections to the device when any one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have rules.

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 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 *times*

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

times: 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.

This configuration does not affect logged-in users. It affects only subsequently logged-in SSH users.

If the authentication method is **any**, the total number of authentication attempts (including both publickey and password authentication attempts) must not exceed the upper limit.

If the authentication method is **password-publickey**, the server first uses publickey authentication, and then uses password authentication to authenticate the SSH user. The process is considered one authentication attempt.

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 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 a small value for the authentication timeout timer.

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 configuration does not affect logged-in users. It affects only subsequently logged-in SSH users.

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 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 packets sent by the SSH server.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the outbound IPv4 packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for IPv4 packets sent by the SSH server.

```
<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 restore the default.

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 user connections.

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

Syntax

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

undo ssh server ipv6 acl

Default

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

Views

System view

Predefined user roles

network-admin

Parameters

ipv6 *basic-acl-number*: Specifies an IPv6 basic ACL number in the range of 2000 to 2999.

ipv6 *advanced-acl-number*: Specifies an IPv6 advanced ACL number in the range of 3000 to 3999.

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

Usage guidelines

The specified ACL filters IPv6 SSH users' connection requests. Only the IPv6 SSH users that the ACL permits can initiate SSH connections to the device.

All IPv6 SSH users can initiate SSH connections to the device when any one of the following conditions exists:

- You do not specify an ACL.
- The specified ACL does not exist.
- The specified ACL does not have rules.

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 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 packets sent by the SSH server.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies the DSCP value in the outbound IPv6 packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of an IPv6 packet specifies the priority of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value to 30 for IPv6 packets sent by the SSH server.

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

```
[Sysname] ssh server ipv6 dscp 30
```

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 *hours*

undo ssh server rekey-interval

Default

The minimum interval for updating the RSA server key pair is 0 hours.

Views

System view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

This command takes effect only on SSH1 clients.

The system starts to count down the 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. Starts to count down the interval again.

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

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

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign** { **pki-domain** *domain-name* | **publickey** *keyname* } }

undo ssh user *username*

Default

No SSH user exists.

Views

System view

Predefined user roles

network-admin

Parameters

username: Specifies an SSH 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. The *pureusername* argument is a string of 1 to 55 characters. The *domain* argument is a string of 1 to 24 characters. 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 an SSH user.

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

authentication-type: Specifies an authentication method for an 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*: Specifies the public key of the SSH client. The *keyname* argument represents the SSH client's public key configured on the server. It is a case-insensitive 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.

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.

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.

You can change the authentication parameters for a logged-in SSH user, but your changes take effect on the clients at the next login.

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

- If the authentication method is **password**, the working directory is authorized by AAA.
- 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.

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

- If the authentication method is **password**, the user role is authorized by the remote AAA server or the local device.
- 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.

Examples

Create an SSH user **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 **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 user role **network-admin** 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 an SFTP server and return to user view.

Syntax

bye

Views

SFTP client view

Predefined user roles

network-admin

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 an 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.

Usage guidelines

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

Examples

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

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

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.pu
```

NOTE:

The output format varies by SSH server device model.

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 configured for 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 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 configured for 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

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 an 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 the 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.

Syntax

help

Views

SFTP client view

Predefined user roles

network-admin

Usage guidelines

The **help** command has the same function as entering the question mark (?).

Examples

Display help information.

```
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
```

NOTE:

The output format varies by SSH server device model.

mkdir

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

```
sftp> mkdir test
```

put

Use **put** to upload a local file to an 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 an 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

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 an SFTP server.

Syntax

remove *remote-file*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-file: Specifies a file.

Usage guidelines

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

Examples

Delete the 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 an 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 the new name for the 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 an SFTP server.

Syntax

rmdir *remote-path*

Views

SFTP client view

Predefined user roles

network-admin

Parameters

remote-path: Specifies a directory.

Examples

Delete the 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

scp *server* [*port-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**public-key** *keyname* | **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.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file.

destination-file-name: Specifies the name of the target file. If you do not specify this argument, the target file uses the same filename as the source file.

identity-key: Specifies a public key algorithm for the client. The default is **dsa**. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature by using the local private key that is associated with the algorithm.

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

- **ecdsa**: Specifies the public key algorithm **ecdsa**.
- **rsa**: Specifies the public key algorithm **rsa**.

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

zlib: Specifies the compression algorithm **zlib**.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is **aes128-cbc**.

The following algorithms are listed in ascending order of security strength and computation time:

- **des-cbc**: Specifies the encryption algorithm **des-cbc**.
- **3des-cbc**: Specifies the encryption algorithm **3des-cbc**.
- **aes128-cbc**: Specifies the encryption algorithm **aes128-cbc**.
- **aes256-cbc**: Specifies the encryption algorithm **aes256-cbc**.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is **sha1**.

- **md5**: Specifies the HMAC algorithm **hmac-md5**.
- **md5-96**: Specifies the HMAC algorithm **hmac-md5-96**.
- **sha1**: Specifies the HMAC algorithm **hmac-sha1**. The algorithm **sha1** provides stronger security but costs more computation time than the algorithm **md5**.
- **sha1-96**: Specifies the HMAC algorithm **hmac-sha1-96**.

prefer-kex: Specifies the preferred key exchange algorithm. The default is **dh-group-exchange-sha1**.

- **dh-group-exchange-sha1**: Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.
- **dh-group1-sha1**: Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.
- **dh-group14-sha1**: Specifies the key exchange algorithm **diffie-hellman-group14-sha1**. The algorithm **dh-group14-sha1** provides stronger security but costs more computation time than the algorithm **dh-group1-sha1**.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is **aes128-cbc**. 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 **sha1**. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

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

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. To ensure successful SCP connections, H3C recommends that you 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.

Examples

Connect an SCP client to the SCP server **200.1.1.1**. Specify the public key of the server as **svkey**, and download the 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
```

scp ipv6

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

Syntax

scp ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**public-key** *keyname* | **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.

-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.

destination-file-name: Specifies the name of the target file. If you do not specify this argument, the target file uses the same filename as the source file.

identity-key: Specifies a public key algorithm for the client. The default is **dsa**. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature by using the local private key that is associated with the algorithm.

- **dsa**: Specifies the public key algorithm **dsa**.
- **ecdsa**: Specifies the public key algorithm **ecdsa**.
- **rsa**: Specifies the public key algorithm **rsa**.

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

zlib: Specifies the compression algorithm **zlib**.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is **aes128-cbc**.

The following algorithms are listed in ascending order of security strength and computation time:

- **des-cbc**: Specifies the encryption algorithm **des-cbc**.
- **3des-cbc**: Specifies the encryption algorithm **3des-cbc**.
- **aes128-cbc**: Specifies the encryption algorithm **aes128-cbc**.
- **aes256-cbc**: Specifies the encryption algorithm **aes256-cbc**.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is **sha1**.

- **md5**: Specifies the HMAC algorithm **hmac-md5**.
- **md5-96**: Specifies the HMAC algorithm **hmac-md5-96**.
- **sha1**: Specifies the HMAC algorithm **hmac-sha1**. The algorithm **sha1** provides stronger security but costs more computation time than the algorithm **md5**.
- **sha1-96**: Specifies the HMAC algorithm **hmac-sha1-96**.

prefer-kex: Specifies the preferred key exchange algorithm. The default is **dh-group-exchange-sha1**.

- **dh-group-exchange-sha1**: Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.
- **dh-group1-sha1**: Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.
- **dh-group14-sha1**: Specifies the key exchange algorithm **diffie-hellman-group14-sha1**. The algorithm **dh-group14-sha1** provides stronger security but costs more computation time than the algorithm **dh-group1-sha1**.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is **aes128-cbc**. 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 **sha1**. Supported algorithms are the same as the client-to-server HMAC algorithms (see the **prefer-ctos-hmac** keyword).

publickey *keyname*: Specifies the host public key of the server, which is used to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

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. To ensure successful SCP connections, H3C recommends that you 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.

Examples

Connect an SCP client to the SCP server **2000::1**. Specify the public key of the server as **svkey**, and download the 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
```

sftp

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

Syntax

sftp *server* [*port-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc | aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc | aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **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.

identity-key: Specifies a public key algorithm for the client. The default is **dsa**. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature by using the local private key that is associated with the algorithm.

- **dsa**: Specifies the public key algorithm **dsa**.
- **ecdsa**: Specifies the public key algorithm **ecdsa**.
- **rsa**: Specifies the public key algorithm **rsa**.

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

zlib: Specifies the compression algorithm **zlib**.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is **aes128-cbc**.

The following algorithms are listed in ascending order of security strength and computation time:

- **des-cbc**: Specifies the encryption algorithm **des-cbc**.
- **3des-cbc**: Specifies the encryption algorithm **3des-cbc**.
- **aes128-cbc**: Specifies the encryption algorithm **aes128-cbc**.
- **aes256-cbc**: Specifies the encryption algorithm **aes256-cbc**.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is **sha1**.

- **md5**: Specifies the HMAC algorithm **hmac-md5**.
- **md5-96**: Specifies the HMAC algorithm **hmac-md5-96**.
- **sha1**: Specifies the HMAC algorithm **hmac-sha1**. The algorithm **sha1** provides stronger security but costs more computation time than the algorithm **md5**.
- **sha1-96**: Specifies the HMAC algorithm **hmac-sha1-96**.

prefer-kex: Specifies the preferred key exchange algorithm. The default is **dh-group-exchange-sha1**.

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

- **dh-group1-sha1**: Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.
- **dh-group14-sha1**: Specifies the key exchange algorithm **diffie-hellman-group14-sha1**. The algorithm **dh-group14-sha1** provides stronger security but costs more computation time than the algorithm **dh-group1-sha1**.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is **aes128-cbc**. 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 **sha1**. 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 host public key of the server, which is used to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

source: Specifies a source IPv4 address or source interface for 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. To ensure successful SFTP connections, H3C recommends that you 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.

Examples

Connect an SFTP client to the IPv4 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 specify 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

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

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.

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 specify 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 route 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

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

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.

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

sftp ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **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.

-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 the client. The default is **dsa**. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature by using the local private key that is associated with the algorithm.

- **dsa**: Specifies the public key algorithm **dsa**.
- **ecdsa**: Specifies the public key algorithm **ecdsa**.
- **rsa**: Specifies the public key algorithm **rsa**.

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

zlib: Specifies the compression algorithm **zlib**.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is **aes128-cbc**.

The following algorithms are listed in ascending order of security strength and computation time:

- **des-cbc**: Specifies the encryption algorithm **des-cbc**.
- **3des-cbc**: Specifies the encryption algorithm **3des-cbc**.
- **aes128-cbc**: Specifies the encryption algorithm **aes128-cbc**.
- **aes256-cbc**: Specifies the encryption algorithm **aes256-cbc**.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is **sha1**.

- **md5**: Specifies the HMAC algorithm **hmac-md5**.
- **md5-96**: Specifies the HMAC algorithm **hmac-md5-96**.
- **sha1**: Specifies the HMAC algorithm **hmac-sha1**. The algorithm **sha1** provides stronger security but costs more computation time than the algorithm **md5**.
- **sha1-96**: Specifies the HMAC algorithm **hmac-sha1-96**.

prefer-kex: Specifies the preferred key exchange algorithm. The default is **dh-group-exchange-sha1**.

- **dh-group-exchange-sha1**: Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.
- **dh-group1-sha1**: Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.
- **dh-group14-sha1**: Specifies the key exchange algorithm **diffie-hellman-group14-sha1**. The algorithm **dh-group14-sha1** provides stronger security but costs more computation time than the algorithm **dh-group1-sha1**.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is **aes128-cbc**. 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 **sha1**. 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, which is used to authenticate the server. The *keyname* argument is a case-insensitive string of 1 to 64 characters.

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. To ensure successful SFTP connections, H3C recommends that you 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 IP address of the IPv6 SFTP packets.

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

Examples

Connect an SFTP client to the IPv6 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:
```

ssh client ipv6 source

Use **ssh client ipv6 source** to specify 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

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

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.

Examples

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

```
<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 specify 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 route 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

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

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.

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

ssh2 *server* [*port-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc | aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc | aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **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.

identity-key: Specifies a public key algorithm for the client. The default is **dsa**. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature by using the local private key that is associated with the algorithm.

- **dsa**: Specifies the public key algorithm **dsa**.
- **ecdsa**: Specifies the public key algorithm **ecdsa**.
- **rsa**: Specifies the public key algorithm **rsa**.

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

zlib: Specifies the compression algorithm **zlib**.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is **aes128-cbc**.

The following algorithms are listed in ascending order of security strength and computation time:

- **des-cbc**: Specifies the encryption algorithm **des-cbc**.
- **3des-cbc**: Specifies the encryption algorithm **3des-cbc**.
- **aes128-cbc**: Specifies the encryption algorithm **aes128-cbc**.
- **aes256-cbc**: Specifies the encryption algorithm **aes256-cbc**.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is **sha1**.

- **md5**: Specifies the HMAC algorithm **hmac-md5**.
- **md5-96**: Specifies the HMAC algorithm **hmac-md5-96**.
- **sha1**: Specifies the HMAC algorithm **hmac-sha1**. The algorithm **sha1** provides stronger security but costs more computation time than the algorithm **md5**.
- **sha1-96**: Specifies the HMAC algorithm **hmac-sha1-96**.

prefer-kex: Specifies the preferred key exchange algorithm. The default is **dh-group-exchange-sha1**.

- **dh-group-exchange-sha1**: Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.
- **dh-group1-sha1**: Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.
- **dh-group14-sha1**: Specifies the key exchange algorithm **diffie-hellman-group14-sha1**. The algorithm **dh-group14-sha1** provides stronger security but costs more computation time than the algorithm **dh-group1-sha1**.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is **aes128-cbc**. 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 **sha1**. 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 an escape character. By default, the escape character is a tilde (~).

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

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. To ensure successful Stelnet connections, H3C recommends that you 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.

H3C recommends that you use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Establish a connection to the IPv4 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

ssh2 ipv6 *server* [*port-number*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc | aes256-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc | aes256-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **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.

-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 the client. The default is **dsa**. If the server uses publickey authentication, you must specify this keyword. The client generates the digital signature by using the local private key that is associated with the algorithm.

- **dsa**: Specifies the public key algorithm **dsa**.
- **ecdsa**: Specifies the public key algorithm **ecdsa**.
- **rsa**: Specifies the public key algorithm **rsa**.

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

zlib: Specifies the compression algorithm **zlib**.

prefer-ctos-cipher: Specifies the preferred client-to-server encryption algorithm. The default is **aes128-cbc**.

The following algorithms are listed in ascending order of security strength and computation time:

- **des-cbc**: Specifies the encryption algorithm **des-cbc**.
- **3des-cbc**: Specifies the encryption algorithm **3des-cbc**.
- **aes128-cbc**: Specifies the encryption algorithm **aes128-cbc**.
- **aes256-cbc**: Specifies the encryption algorithm **aes256-cbc**.

prefer-ctos-hmac: Specifies the preferred client-to-server HMAC algorithm. The default is **sha1**.

- **md5**: Specifies the HMAC algorithm **hmac-md5**.
- **md5-96**: Specifies the HMAC algorithm **hmac-md5-96**.
- **sha1**: Specifies the HMAC algorithm **hmac-sha1**. The algorithm **sha1** provides stronger security but costs more computation time than the algorithm **md5**.
- **sha1-96**: Specifies the HMAC algorithm **hmac-sha1-96**.

prefer-kex: Specifies the preferred key exchange algorithm. The default is **dh-group-exchange-sha1**.

- **dh-group-exchange-sha1**: Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.
- **dh-group1-sha1**: Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.
- **dh-group14-sha1**: Specifies the key exchange algorithm **diffie-hellman-group14-sha1**. The algorithm **dh-group14-sha1** provides stronger security but costs more computation time than the algorithm **dh-group1-sha1**.

prefer-stoc-cipher: Specifies the preferred server-to-client encryption algorithm. The default is **aes128-cbc**. 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 **sha1**. 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 an escape character. By default, the escape character is a tilde (~).

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

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. To ensure successful Stelnet connections, H3C recommends that you 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 IP 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.

H3C recommends that you use the default escape character (~). Do not use any characters in SSH usernames as the escape character.

Examples

Establish a connection to the IPv6 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 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: dh-group-exchange-sha1 dh-group14-sha1 dh-group1-sha1
Public key algorithms: dsa rsa ecdsa
Encryption algorithms: aes128-cbc 3des-cbc des-cbc aes256-cbc
MAC algorithms: sha1 md5 md5-96 sha1-96
```

Table 4 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	MAC 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

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

undo ssh2 algorithm cipher

Default

SSH2 uses the encryption algorithms **aes128-cbc**, **aes256-cbc**, **3des-cbc**, and **des-cbc** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

aes128-cbc: Specifies the encryption algorithm **aes128-cbc**.

aes256-cbc: Specifies the encryption algorithm **aes256-cbc**.

3des-cbc: Specifies the encryption algorithm **3des-cbc**.

des-cbc: Specifies the 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 the algorithm **3des-cbc** as the encryption algorithm for SSH2.

```
<Sysname> system-view
[Sysname] ssh2 algorithm cipher 3des-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

ssh2 algorithm key-exchange { **dh-group-exchange-sha1** | **dh-group14-sha1** | **dh-group1-sha1** } *****

undo ssh2 algorithm key-exchange

Default

SSH2 uses the key exchange algorithms **dh-group-exchange-sha1**, **dh-group14-sha1**, and **dh-group1-sha1** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

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

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

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

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 the 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 MAC algorithms for SSH2.

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

Syntax

ssh2 algorithm mac { **sha1** | **sha1-96** | **md5** | **md5-96** } *

undo ssh2 algorithm mac

Default

SSH2 uses the MAC algorithms **sha1**, **sha1-96**, **md5**, and **md5-96** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

sha1: Specifies the HMAC algorithm **hmac-sha1**.

sha1-96: Specifies the HMAC algorithm **hmac-sha1-96**.

md5: Specifies the HMAC algorithm **hmac-md5**.

md5-96: Specifies the HMAC algorithm **hmac-md5-96**.

Usage guidelines

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

Examples

Specify the algorithm **md5** as the MAC 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

ssh2 algorithm public-key { **ecdsa** | **dsa** | **rsa** } *

undo ssh2 algorithm public-key

Default

SSH2 uses the public key algorithms **ecdsa**, **dsa**, and **rsa** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

ecdsa: Specifies the public key algorithm **ecdsa**.

dsa: Specifies the public key algorithm **dsa**.

rsa: Specifies the public key algorithm **rsa**.

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 the 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**