Contents

Public key management 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*.

display public-key local public

Use **display public-key local public** to display local public keys.

Syntax

display public-key local { **dsa** | **ecdsa** | **rsa** } **public** [**name** *key-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dsa: Specifies the DSA key pair type.

ecdsa: Specifies the ECDSA key pair type.

rsa: Specifies the RSA key pair type.

name *key-name*: Specifies a local key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command displays the public keys of all local key pairs of the specified type.

Usage guidelines

You can copy and distribute the public key of a local key pair to peer devices.

You cannot display a host public key that has the default key pair name by specifying the **name** *key-name* option. To view a host public key that has the default key pair name, display all local public keys by using this command without specifying a key pair name.

Examples

Display all local RSA public keys.

```
<Sysname> display public-key local rsa public

=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
   667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
   C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
   FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
   2DA4C04EF5AE0835090203010001
=============================================
```

```
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100CAB4CACCA16442AD5F453442
   762F03897E0D494FEDE69224F5C051A441D290976733A278C9F0C0F5A198E66143EAB54A64
   DB608269CAE844B1E7CC64AD7E808972E7CF887F3B657F056E7930FC84FBF1AD83A01CC47E
   9D85C13413996ECD093B0203010001
==========================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D003081890281810 0DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

Display all local DSA public keys.

```
<Sysname> display public-key local dsa public

==========================================
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 15:41:37 2011/05/12
Key code:
   308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF038184000 2818041912CE34D12BCD2157E7AB1C2F03B3EF395
   100F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
   52DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
   887E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
==========================================
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
```

```
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

Display all local ECDSA public keys.

```
<Sysname> display public-key local ecdsa public

=============================================
Key name: ecdsakey (default)
Key type: ECDSA
Time when key pair created: 15:42:04 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004C10CF7CE42193F7FC2AF
   68F5DC877835A43009DB6135558A7FB8316C361B0690B4FD84A14C0779C76DD6145BF9362B
   1D
=============================================
Key name: ecdsa1
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
   AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
   4D
```

Display the public key of the local RSA key pair **rsa1**.

```
<Sysname> display public-key local rsa public name rsa1

=============================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
   426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
   1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
   9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
   92D8C6D940890BF4290203010001
```

Display the public key of the local DSA key pair **dsa1**.

```
<Sysname> display public-key local dsa public name dsa1

=============================================
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
```

```
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB9877236027 87E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

Display the public key of the local ECDSA key pair **ecdsa1**.

```
<Sysname> display public-key local ecdsa public name ecdsa1

=========================================
Key name: ecdsa1
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
   3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
   AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
   4D
```

Table 1 Command output

Field	Description
Key name	Name of the local key pair. If you did not specify a name when creating the key pair, the default name is used followed by the word **default** in brackets. The following is the default key pair name for each key algorithm: • **hostkey**—Default RSA host key pair name. • **serverkey**—Default RSA server key pair name. • **dsakey**—Default DSA host key pair name. • **ecdsakey**—Default ECDSA host key pair name.
Key type	Options include: • RSA. • DSA. • ECDSA.
Time when key pair created	Date and time when the local key pair was created.
Key code	Public key string.

Related commands

`public-key local create`

display public-key peer

Use **`display public-key peer`** to display information about peer host public keys.

Syntax

display public-key peer [**brief** | **name** *publickey-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

brief: Displays brief information about all peer host public keys. The brief information includes only the key type, key modulus, and key name.

name *publickey-name*: Displays detailed information about a peer host public key, including its key code. The *publickey-name* argument specifies a peer host public by its name, a case-sensitive string of 1 to 64 characters.

Usage guidelines

If you do not specify any keywords, this command displays detailed information about all peer host public keys configured on the local device.

You can use the **public-key peer** command or the **public-key peer import sshkey** command to configure a peer host public key on the local device.

Examples

Display detailed information about the peer host public key **idrsa**.

```
<Sysname> display public-key peer name idrsa

=============================================
Key name: idrsa
Key type: RSA
Key modulus: 1024
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100C5971581A78B5388
   B3C9063EC6B53D395A6704D9752B6F9B7B1F734EEB5DD509F0B050662C46FFB8D27F797E37
   918F6270C5793F1FC63638970A0E4D51A3CEF7CFF6E92BFAFD73F530E0BDE27056E81F2525
   6D0883836FD8E68031B2C272FE2EA75C87734A7B8F85B8EBEB3BD51CC26916AF3B3FDC32C3
   42C142D41BB4884FEB0203010001
```

Table 2 Command output

Field	Description
Key name	Name of the peer host public key.
Key type	Key type: RSA, DSA or ECDSA.
Key modulus	Key modulus length in bits.
Key code	Public key string.

Display brief information about all peer host public keys.

```
<Sysname> display public-key peer brief
Type  Modulus  Name
```

```
--------------------------
RSA   1024    idrsa
DSA   1024    10.1.1.1
```

Table 3 Command output

Field	Description
Type	Key type: RSA, DSA or ECDSA.
Modulus	Key modulus length in bits.
Name	Name of the peer host public key.

Related commands

public-key peer

public-key peer import sshkey

peer-public-key end

Use **peer-public-key end** to exit public key view to system view and save the configured peer host public key.

Syntax

peer-public-key end

Views

Public key view

Predefined user roles

network-admin

Usage guidelines

After you type the peer host public key on the local device, use this command to exit public key view and to save the peer host public key.

The system verifies the public key before saving it. If the key is not in the correct format, the system discards the key and displays an error message. If the key is valid, for example, the key was displayed by the **display public-key local public** command, the system saves the key.

Examples

Exit public key view and save the configured peer host public key.

```
<Sysname> system-view
[Sysname] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]30819F300D06092A864886F70D010101050003818D0030818902818
100C0EC8014F82515F6335A0A
[Sysname-pkey-public-key-key1]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E
719D1643135877E13B1C531B4
[Sysname-pkey-public-key-key1]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B
952ADF6B80EB5F52698FCF3D6
[Sysname-pkey-public-key-key1]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050
BD4A9B1DDE675AC30CB020301
[Sysname-pkey-public-key-key1]0001
```

```
[Sysname-pkey-public-key-key1] peer-public-key end
[Sysname]
```

Related commands

display public-key local public

display public-key peer

public-key peer

public-key local create

Use **public-key local create** to create local key pairs.

Syntax

In non-FIPS mode:

public-key local create { **dsa** | **ecdsa** [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**] | **rsa** } [**name** *key-name*]

In FIPS mode:

public-key local create { **dsa** | **ecdsa** [**secp256r1** | **secp384r1** | **secp521r1**] | **rsa** } [**name** *key-name*]

Default

No local key pairs exist.

Views

System view

Predefined user roles

network-admin

Parameters

dsa: Specifies the DSA key pair type.

ecdsa: Specifies the ECDSA key pair type.

- **secp192r1**: Uses the secp192r1 curve to create a 192-bit ECDSA key pair.
- **secp256r1**: Uses the secp256r1 curve to create a 256-bit ECDSA key pair.
- **secp384r1**: Uses the secp384r1 curve to create a 384-bit ECDSA key pair.
- **secp521r1**: Uses the secp521r1 curve to create a 521-bit ECDSA key pair.

By default, the secp192r1 curve is used in non-FIPS mode and the secp256r1 curve is used in FIPS mode.

rsa: Specifies the RSA key pair type.

name *key-name*: Assigns a name to the key pair. The *key-name* argument is a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not assign a name to the key pair, the key pair takes the default name.

Table 4 Default local key pair names

Type	Default name
RSA	• Host key pair: **hostkey** • Server key pair: **serverkey**
DSA	**dsakey**

Type	Default name
ECDSA	**ecdsakey**

Usage guidelines

The key algorithm must be the same as required by the security application.

When you create an RSA or DSA key pair, enter an appropriate key modulus length at the prompt. The longer the key modulus length, the higher the security, and the longer the key generation time.

When you create an ECDSA key pair, choose the appropriate elliptic curve. The elliptic curve determines the ECDSA key length. The longer the key length, the higher the security, and the longer the key generation time.

See Table 5 for more information about key modulus lengths and key lengths.

If you do not assign the key pair a name, the system assigns the default name to the key pair and marks the key pair as **`default`**. You can also assign the default name to another key pair, but the system does not mark the key pair as **default**. The name of a key pair must be unique among all manually named key pairs that use the same key algorithm. If a name conflict occurs, the system asks whether you want to overwrite the existing key pair.

The key pairs are automatically saved and can survive system reboots.

Table 5 A comparison of different types of asymmetric key algorithms

Type	Generated key pairs	Modulus/key length

RSA	• In non-FIPS mode:
	  ○ One host key pair, if you specify a key pair name.
	  ○ One server key pair and one host key pair, if you do not specify a key pair name.
	  Both key pairs use their default names.
	• In FIPS mode: One host key pair.
	NOTE:
	Only SSH 1.5 uses the RSA server key pair.
		RSA key modulus length:
		• In non-FIPS mode: 512 to 4096 bits, 1024 bits by default.
		To ensure security, use a minimum of 768 bits.
		• In FIPS mode: A multiple of 256 bits in the range of 2048 to 4096 bits, 2048 bits by default.

DSA	One host key pair.	DSA key modulus length: • In non-FIPS mode: 512 to 2048 bits, 1024 bits by default. To ensure security, use a minimum of 768 bits. • In FIPS mode: 2048 bits.
ECDSA	One host key pair.	ECDSA key length: • In non-FIPS mode: 192, 256, 384, or 521 bits. • In FIPS mode: 256, 384, or 521 bits.

Examples

Create local RSA key pairs with default names.

```
<Sysname> system-view
[Sysname] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
```

```
Input the modulus length [default = 1024]:
Generating Keys...
....
Create the key pair successfully.
```

Create a local DSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
....
Create the key pair successfully.
```

Create a local ECDSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local create ecdsa
Generating Keys...
Create the key pair successfully.
```

Create a local RSA key pair with the name **rsa1**.

```
<Sysname> system-view
[Sysname] public-key local create rsa name rsa1
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
..
Create the key pair successfully.
```

Create a local DSA key pair with the name **dsa1**.

```
<Sysname> system-view
[Sysname] public-key local create dsa name dsa1
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....
Create the key pair successfully.
```

Create a local ECDSA key pair with the name **ecdsa1**.

```
<Sysname> system-view
[Sysname] public-key local create ecdsa name ecdsa1
Generating Keys...
Create the key pair successfully.
```

In FIPS mode, create a local RSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local create rsa
```

```
The range of public key modulus is (2048 ~ 4096), a multiple of 256.
It will take a few minutes.Press CTRL+C to abort.
Input the modulus length [default = 2048]:
Generating Keys...
....
Create the key pair successfully.
```

In FIPS mode, create a local DSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key modulus is (2048 ~ 2048).
It will take a few minutes.Press CTRL+C to abort.
Input the modulus length [default = 2048]:
..
Create the key pair successfully.
```

Related commands

display public-key local public

public-key local destroy

public-key local destroy

Use **public-key local destroy** to destroy local key pairs.

Syntax

public-key local destroy { **dsa** | **ecdsa** | **rsa** } [**name** *key-name*]

Views

System view

Predefined user roles

network-admin

Parameters

dsa: Specifies the DSA key pair type.

ecdsa: Specifies the ECDSA key pair type.

rsa: Specifies the RSA key pair type.

name *key-name*: Specifies a local key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command destroys all key pairs of the specified type.

Usage guidelines

To avoid key compromise, destroy the local key pair and generate a new pair after any of the following conditions occurs:

- An intrusion event has occurred.
- The storage media of the device is replaced.
- The local certificate has expired. For more information about local certificates, see *Security Configuration Guide*.

Examples

Destroy the local RSA key pairs with the default names.

```
<Sysname> system-view
[Sysname] public-key local destroy rsa
Confirm to destroy the key pair? [Y/N]:y
```

Destroy the local DSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local destroy dsa
Confirm to destroy the key pair? [Y/N] :y
```

Destroy the local ECDSA key pair with the default name.

```
<Sysname> system-view
[Sysname] public-key local destroy ecdsa
Confirm to destroy the key pair? [Y/N]:y
```

Destroy the local RSA key pair **rsa1**.

```
<Sysname> system-view
[Sysname] public-key local destroy rsa name rsa1
Confirm to destroy the key pair? [Y/N]:y
```

Destroy the local DSA key pair **dsa1**.

```
<Sysname> system-view
[Sysname] public-key local destroy dsa name dsa1
Confirm to destroy the key pair? [Y/N] :y
```

Destroy the local ECDSA key pair **ecdsa1**.

```
<Sysname> system-view
[Sysname] public-key local destroy ecdsa name ecdsa1
Confirm to destroy the key pair? [Y/N]:y
```

Related commands

public-key local create

public-key local export dsa

Use **public-key local export dsa** to export a local DSA host public key.

Syntax

public-key local export dsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a local DSA key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local DSA key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh2: Exports the host public key in SSH 2.0 format.

filename: Specifies the name of the file for saving the DSA host public key. The file name is a case-insensitive string of 1 to 128 characters. The name cannot be all dots (.), hostkey, serverkey, dsakey, or ecdsakey, and cannot start with a slash (/) or contain ***./*** and ***../***. For more information about

file names, see *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local DSA host public key before distributing it to a peer device.

To distribute a local DSA host public key to a peer device:

1. Save the exported local host public key to a file by using one of the following methods:
   - Use the **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } command to export the local host public key, and then copy and paste the key to a file.
   - Use the **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export the key to a file. You cannot export the key to the folder **pkey** or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

SSH 2.0 and OpenSSH are different public key formats. Choose the correct format that is supported on the device where you import the host public key.

Examples

Export the host public key of the local DSA key pair with the default name in OpenSSH format to a file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub
```

Display the host public key of the local DSA key pair with the default name in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export dsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxw
vA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakd
MdasIjQLWYGyepFc3sTwmIflQeweUwLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo=
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local DSA key pair with the default name in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxw
vA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakd
MdasIjQLWYGyepFc3sTwmIflQeweUwLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo= dsa-key
```

Export the host public key of the local DSA key pair **dsa1** in OpenSSH format to the file **dsa1.pub**.

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

```
[Sysname] public-key local export dsa name dsa1 openssh dsa1.pub
```

Display the host public key of the local DSA key pair **dsa1** in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98
qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEY
ZullatZRH0km+DdpZ7CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local DSA key pair **dsa1** in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98
qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEY
ZullatZRH0km+DdpZ7CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq dsa-key
```

Related commands

public-key local create

public-key peer import sshkey

public-key local export ecdsa

Use **public-key local export ecdsa** to export a local ECDSA host public key.

Syntax

public-key local export ecdsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a local ECDSA key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local ECDSA key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh2: Exports the host public key in SSH 2.0 format.

filename: Specifies the name of the file for saving the local host public key. The file name is a case-insensitive string of 1 to 128 characters. The name cannot be dots (.), hostkey, serverkey, dsakey, or ecdsakey, and cannot start with a slash (/) or contain **./** and **../**. For more information about file names, see *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local ECDSA host public key before distributing it to a peer device.

To distribute a local ECDSA host public key to a peer device:

1. Save the exported ECDSA host public key to a file by using one of the following methods:
   - Use the **public-key local export ecdsa** [**name** *key-name*] { **openssh** | **ssh2** } command to export the local host public key, and then copy and paste it to a file.
   - Use the **public-key local export ecdsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export the host public key to a file. You cannot export the key to the folder **pkey** or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

SSH 2.0 and OpenSSH are different public key formats. Choose the correct format that is supported by the device where you import the host public key.

Only the ECDSA host public key generated by using the secp256r1 curve can be exported.

Examples

Export the host public key of the local ECDSA key pair with the default name in OpenSSH format to the file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export ecdsa openssh key.pub
```

Display the host public key of the local ECDSA key pair with the default name in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export ecdsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "ecdsa-sha2-nistp256-2014/07/06"
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBREw5tkARpbV+sYArt/xcW+UJEAevx7O
ckTtTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTIcxuBjuBap+pHc919C58=
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local ECDSA key pair with the default name in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export ecdsa openssh
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBREw5tkARpbV+sYArt/xcW+UJEAevx7O
ckTtTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTIcxuBjuBap+pHc919C58=
 ecdsa-key
```

Related commands

public-key local create

public-key peer import sshkey

public-key local export rsa

Use **public-key local export rsa** to export a local RSA host public key.

Syntax

In non-FIPS mode:

public-key local export rsa [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } [*filename*]

In FIPS mode:

public-key local export rsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

Views

System view

Predefined user roles

network-admin

Parameters

name *key-name*: Specifies a local RSA key pair by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not specify a key pair, this command exports the host public key of the local RSA key pair with the default name.

openssh: Exports the host public key in OpenSSH format.

ssh1: Exports the host public key in SSH 1.5 format.

ssh2: Exports the host public key in SSH 2.0 format.

filename: Specifies the name of the file for saving the RSA host public key. The file name is a case-insensitive string of 1 to 128 characters. The name cannot be all dots (.), hostkey, serverkey, dsakey, or ecdsakey, and cannot start with a slash (/) or contain **./** and **../**. For more information about file names, see *Fundamentals Configuration Guide*. If you do not specify a file name, this command displays the key on the monitor screen.

Usage guidelines

You can use this command to export a local RSA host public key before distributing it to a peer device.

To distribute a local RSA host public key to a peer device:

1. Save the exported local host public key to a file by using one of the following methods:
   - Use the **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } command to export the key, and then copy and paste it to a file.
   - Use the **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* command to export key to a file. You cannot export the key to the folder **pkey** or its subfolders.
2. Transfer a copy of the file to the peer device, for example, by using FTP in binary mode or TFTP. For more information about FTP and TFTP, see *Fundamentals Configuration Guide*.
3. On the peer device, use the **public-key peer import sshkey** command to import the host public key from the file.

Choose the correct public key format that is supported on the device where you import the host public key. In FIPS mode, the device only supports SSH 2.0 and OpenSSH.

Examples

Export the host public key of the local RSA key pair with the default name in OpenSSH format to the file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub
```

Display the host public key of the local RSA key pair with the default name in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/b
YcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvyvPJilneKJqhPT0xd
v4tlas+mLNloY0dImbwS2kwE71rgg1CQ==
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local RSA key pair with the default name in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/b
YcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvyvPJilneKJqhPT0xd
v4tlas+mLNloY0dImbwS2kwE71rgg1CQ== rsa-key
```

Export the host public key of the local RSA key pair **rsa1** in OpenSSH format to the file **rsa1.pub**.

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh rsa1.pub
```

Display the host public key of the local RSA key pair **rsa1** in SSH 2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+
q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8b
a8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ==
---- END SSH2 PUBLIC KEY ----
```

Display the host public key of the local RSA key pair **rsa1** in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+
q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8b
a8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ== rsa-key
```

Related commands

`public-key local create`

`public-key peer import sshkey`

public-key peer

Use **`public-key peer`** to assign a name to a peer host public key and enter public key view, or enter the view of an existing peer host public key.

Use **`undo public-key peer`** to delete a peer host public key.

Syntax

public-key peer *keyname*

undo public-key peer *keyname*

Default

No peer host public keys exist.

Views

System view

Predefined user roles

network-admin

Parameters

keyname: Specifies a key name, a case-sensitive string of 1 to 64 characters.

Usage guidelines

After you execute this command to enter the public key view, type the public key. Spaces and carriage returns are allowed, but are not saved.

To configure a peer host public key on the local device, first obtain the peer public key in hexadecimal notation, and then perform the following tasks on the local device:

1. Execute the **public-key peer** command to enter public key view.
2. Type the public key.
3. Execute the **peer-public-key end** command to save the public key and return to system view.

The public key you type in the public key view must be in a correct format. If the peer device is an H3C device, use the **display public-key local public** command to display and record its public key.

Examples

Assign the name **key1** to the peer host public key and enter public key view.

```
<Sysname> system-view
[Sysname] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]
```

Related commands

display public-key local public

display public-key peer

peer-public-key end

public-key peer import sshkey

Use **public-key peer import sshkey** to import a peer host public key from a public key file.

Use **undo public-key peer** to remove a peer host public key.

Syntax

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

Default

No peer host public keys exist.

Views

System view

Predefined user roles

network-admin

Parameters

keyname: Specifies a name for a peer host public key, a case-sensitive string of 1 to 64 characters.

filename: Specifies a public key file by its name, a case-insensitive string of 1 to 128 characters. The name cannot be all dots (.), hostkey, serverkey, dsakey, or ecdsakey, and cannot start with a slash (/) or contain ***./*** and ***../***. For more information about file names, see *Fundamentals Configuration Guide*.

Usage guidelines

After you configure this command, the system automatically transforms the host public key to the PKCS format, and saves the key.

Before you use this command, make sure you have got a copy of the public key file from the peer device through FTP in binary mode or through TFTP.

In non-FIPS mode, the device supports importing public keys in the format of SSH 1.5, SSH 2.0, and OpenSSH.

In FIPS mode, the device supports importing public keys in the format of SSH 2.0 and OpenSSH.

Examples

Import the peer host public key **key2** from the public key file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key peer key2 import sshkey key.pub
```

Related commands

display public-key peer

public-key local export dsa

public-key local export ecdsa

public-key local export rsa