Contents

Modified feature: Password configuration and display

Feature change description

Modified password setup and display for password/key-related security features.

NOTE:

For security purposes, all passwords and keys, including those configured in plaintext, are stored in encrypted form.

Command changes

Modified command: bims-server

Old syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** *key*

New syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** [**cipher** | **simple**] *key*

Views

DHCP address pool view

Parameters

ip *ip-address*: Specifies the IP address of the BIMS server.

port *port-number*: Specifies the port number of the BIMS server, in the range of 1 to 65534.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

key: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key you enter must be a plaintext string of 1 to 16 characters.

After modification: You can enter a key in encrypted form or plaintext form.

Modified command: dhcp server bims-server

Old syntax

dhcp server bims-server ip *ip-address* [**port** *port-number*] **sharekey** *key* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

New syntax

dhcp server bims-server ip *ip-address* [**port** *port-number*] **sharekey** [**cipher** | **simple**] *key* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

Views

System view

Parameters

ip *ip-address*: Specifies the IP address of the BIMS server.

port *port-number*: Specifies the port number of the BIMS server, in the range of 1 to 65534.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

key: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

interface *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies an interface range. The *interface-type interface-number* arguments specify an interface by its type and number.

all: Specifies all interfaces.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key you enter must be a plaintext string of 1 to 16 characters.

After modification: You can enter a key in encrypted form or plaintext form.

Modified command: dldp authentication-mode

Old syntax

dldp authentication-mode { **none** | **simple** *simple-password* | **md5** *md5-password* }

New syntax

dldp authentication-mode { **none** | { **simple** | **md5** } *password* }

Views

System view

Parameters

none: Specifies not to perform authentication.

simple: Specifies the simple authentication mode and sets a plaintext or ciphertext password.

md5: Specifies the MD5 authentication mode and sets a plaintext or ciphertext password.

password: Sets the password. This argument is case sensitive. It must be a plaintext string of 1 to 16 characters, or a ciphertext string of 33 to 53 characters.

Change description

Before modification:

- For simple authentication, you can set only a plaintext password of 1 to 16 characters.
- For MD5 authentication, you can set a plaintext or ciphertext password. A plaintext password comprises 1 to 16 characters, and a ciphertext password is a ciphertext string corresponding to the plaintext password.

After modification: Both simple authentication and MD5 authentication support plaintext or ciphertext passwords. A plaintext password is a string of 1 to 16 characters, and a ciphertext password is a string of 33 to 53 characters.

Modified command: key (HWTACACS scheme view)

Old syntax

key { **accounting** | **authentication** | **authorization** } *string*

New syntax

key { **accounting** | **authentication** | **authorization** } [**cipher** | **simple**] *string*

Views

HWTACACS scheme view

Parameters

accounting: Sets the key for secure HWTACACS accounting communication.

authentication: Sets the key for secure HWTACACS authentication communication.

authorization: Sets the key for secure HWTACACS authorization communication.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

string: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key for securing HWTACACS authentication, authorization, or accounting communication must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure HWTACACS authentication, authorization, or accounting communication.

Modified command: key (RADIUS scheme view)

Old syntax

key { **accounting** | **authentication** } *string*

New syntax

key { **accounting** | **authentication** } [**cipher** | **simple**] *string*

Views

RADIUS scheme view

Parameters

accounting: Sets the key for secure RADIUS accounting communication.

authentication: Sets the key for secure RADIUS authentication/authorization communication.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

string: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key for securing RADIUS authentication/authorization or accounting communication must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure RADIUS authentication/authorization or accounting communication.

Modified command: local-server nas-ip

Old syntax

local-server nas-ip *ip-address* **key** *password*

New syntax

local-server nas-ip *ip-address* **key** [**cipher** | **simple**] *password*

Views

System view

Parameters

nas-ip *ip-address*: Specifies the IP address of the network access server through which users can access the local RADIUS authentication/authorization server. The IP address must be in dotted decimal notation.

key [**simple** | **cipher**] *password*: Sets the key to share between the local RADIUS authentication/authorization server and the network access server.

- **cipher**: Sets a ciphertext key.
- **simple**: Sets a plaintext key.
- *password*: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key to share between the local RADIUS authentication/authorization server and the network access server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to share between the local RADIUS authentication/authorization server and the network access server.

Modified command: mac-authentication authmode usernameasmacaddress

Old syntax

mac-authentication authmode usernameasmacaddress [**usernameformat** { **with-hyphen** | **without-hyphen** } { **lowercase** | **uppercase** } | **fixedpassword** *password*]

New syntax

mac-authentication authmode usernameasmacaddress [**usernameformat** { **with-hyphen** | **without-hyphen** } { **lowercase** | **uppercase** } | **fixedpassword** [**cipher** | **simple**] *password*]

Views

System view

Parameters

usernameformat: Specifies the username and password input format for MAC-based accounts.

with-hyphen: Uses the hyphenated MAC address of a user, such as 00-05-e0-1c-02-e3, as the username and password for MAC authentication of the user.

without-hyphen: Uses the unhyphenated MAC address of a user, such as 0005e01c02e3, as the username and password for MAC authentication of the user.

lowercase: Enters letters of the MAC address in lower case.

uppercase: Enters letters of the MAC address in upper case.

fixedpassword [**simple** | **cipher**] *password*: Uses a fixed password, instead of user MAC addresses, for MAC authentication users.

- **cipher**: Sets a ciphertext password.
- **simple**: Sets a plaintext password.
- *password*: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The password you enter must be a plaintext string.

After modification: You can enter a password in encrypted form or plaintext form.

Modified command: mac-authentication authpassword

Old syntax

mac-authentication authpassword *password*

New syntax

mac-authentication authpassword [**cipher** | **simple**] *password*

Views

System view

Parameters

[**cipher** | **simple**] *password*: Sets the password of the shared account for MAC authentication users.

- **cipher**: Sets a ciphertext password.
- **simple**: Sets a plaintext password.
- *password*: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The password you enter must be a plaintext string.

After modification: You can enter a password in encrypted form or plaintext form.

Modified command: ntp-service authentication-keyid

Old syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** *value*

New syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** [**cipher** | **simple**] *value*

Views

System view

Parameters

keyid: Specifies a key ID in the range of 10 to 4294967295.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

value: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 32 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 73 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key you enter must be a plaintext string of 1 to 32 characters.

After modification: You can enter a key in encrypted form or plaintext form.

Modified command: password (Remote-ping test group view)

Old syntax

password *password*

New syntax

password [**cipher** | **simple**] *password*

Views

Remote-ping test group view

Parameters

cipher: Sets a ciphertext FTP password.

simple: Sets a plaintext FTP password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 32 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 73 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The FTP password must be a plaintext string of 1 to 32 characters.

After modification: You can set an FTP password in encrypted form or plaintext form.

Modified command: password (local user view)

Syntax

password { **cipher** | **simple** } *password*

Views

Local user view

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive.

- If **simple** is specified, it is a plaintext string of 1 to 63 characters.
- If **cipher** is specified, it is a string of 1 to 117 characters. If you specify a password of 1 to 63 characters and the system can decrypt the password, the system considers that you have specified

a ciphertext password. If you specify a password of 1 to 63 characters but the system cannot decrypt the password, the system considers that you have specified a plaintext password. A password comprising 64 to 117 characters is always considered a ciphertext password.

Change description

Before modification: If **cipher** is specified, you can set an 88-character password or a password of 1 to 63 characters.

After modification: If **cipher** is specified, you can set a password of 1 to 117 characters.

Modified command: primary accounting (RADIUS scheme view)

Old syntax

primary accounting { *ip-address* | **ipv6** *ipv6-address* } [*port-number*] [**key** *string*]

New syntax

primary accounting { *ip-address* | **ipv6** *ipv6-address* } [*port-number*] [**key** [**cipher** | **simple**] *string*]

Views

RADIUS scheme view

Parameters

ip-address: Specifies the IPv4 address of the primary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS accounting server.

port-number: Specifies the service port number of the primary RADIUS accounting server, a UDP port number in the range of 1 to 65535.

key [**cipher** | **simple**] *string*: Sets the key for secure communication with the primary RADIUS accounting server.

- **cipher**: Sets a ciphertext key.
- **simple**: Sets a plaintext key.
- *string*: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key for securing communication with the primary RADIUS accounting server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure communication with the primary RADIUS accounting server.

Modified command: primary authentication (RADIUS scheme view)

Old syntax

primary authentication { *ip-address* | **ipv6** *ipv6-address* } [*port-number*] [**key** *string*]

New syntax

primary authentication { *ip-address* | **ipv6** *ipv6-address* } [*port-number*] [**key** [**cipher** | **simple**] *string*]

Views

RADIUS scheme view

Parameters

ip-address: Specifies the IPv4 address of the primary RADIUS authentication/authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary RADIUS authentication/authorization server.

port-number: Specifies the service port number of the primary RADIUS authentication/authorization server, a UDP port number in the range of 1 to 65535.

key [**cipher** | **simple**] *string*: Sets the key for secure communication with the primary RADIUS authentication/authorization server.

- **cipher**: Sets a ciphertext key.
- **simple**: Sets a plaintext key.
- *string*: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key for securing communication with the primary RADIUS authentication/authorization server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure communication with the primary RADIUS authentication/authorization server.

Modified command: secondary accounting (RADIUS scheme view)

Old syntax

secondary accounting { *ip-address* | **ipv6** *ipv6-address* } [*port-number*] [**key** *string*]

New syntax

secondary accounting { *ip-address* | **ipv6** *ipv6-address* } [*port-number*] [**key** [**cipher** | **simple**] *string*]

Views

RADIUS scheme view

Parameters

ip-address: Specifies the IPv4 address of the secondary RADIUS accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary RADIUS accounting server.

port-number: Specifies the service port number of the secondary RADIUS accounting server, a UDP port number in the range of 1 to 65535.

key [**cipher** | **simple**] *string*: Sets the key for secure communication with the primary RADIUS accounting server.

- **cipher**: Sets a ciphertext key.
- **simple**: Sets a plaintext key.
- *string*: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key for securing communication with the secondary RADIUS accounting server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure communication with the secondary RADIUS accounting server.

Modified command: secondary authentication (RADIUS scheme view)

Old syntax

secondary authentication { *ip-address* | **ipv6** *ipv6-address* } [*port-number*] [**key** *string*]

New syntax

secondary authentication { *ip-address* | **ipv6** *ipv6-address* } [*port-number*] [**key** [**cipher** | **simple**] *string*]

Views

RADIUS scheme view

Parameters

ip-address: Specifies the IPv4 address of the secondary RADIUS authentication/authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary RADIUS authentication/authorization server.

port-number: Specifies the service port number of the secondary RADIUS authentication/authorization server, a UDP port number in the range of 1 to 65535.

key [**cipher** | **simple**] *string*: Sets the key for secure communication with the secondary RADIUS authentication/authorization server.

- **cipher**: Sets a ciphertext key.

- **simple**: Sets a plaintext key.
- *string*: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key for securing communication with the secondary RADIUS authentication/authorization server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure communication with the secondary RADIUS authentication/authorization server.

Modified command: set authentication password

Syntax

set authentication password { **simple** | **cipher** } *password*

Views

User interface view

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

key: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a plaintext string of 1 to 16 characters. If **cipher** is specified, it can be a plaintext string of 1 to 16 characters or a ciphertext string of 17 to 53 characters.

Change description

Before modification: When you specify the **cipher** keyword, you can enter a string of 1 to 16 characters or a string of 24 characters as the password.

After modification: When you specify the **cipher** keyword, you can enter a string of 1 to 53 characters as the password.

Modified command: snmp-agent usm-user v3

Syntax

snmp-agent usm-user v3 *user-name group-name* [[**cipher**] **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128** | **des56** } *priv-password*]] [**acl** *acl-number*]

Views

System view

Parameters

user-name: Specifies a username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies a group name, a case-sensitive string of 1 to 32 characters.

cipher: Specifies that *auth-password* and *priv-password* are encrypted keys, which can be calculated to a hexadecimal string by using the **snmp-agent calculate-password** command. If this keyword is not specified, *auth-password* and *priv-password* are plaintext keys.

authentication-mode: Specifies an authentication algorithm. MD5 is faster but less secure than SHA. For more information about these algorithms, see *Security Configuration Guide*.

- **md5**: Specifies the MD5 authentication algorithm.
- **sha**: Specifies the SHA-1 authentication algorithm.

auth-password: Specifies a case-sensitive plaintext or encrypted authentication key. A plaintext key is a string of 1 to 64 visible characters. If the **cipher** keyword is specified, the encrypted authentication key length requirements differ by authentication algorithm and key string format, as shown in Table 1.

Table 1 Encrypted authentication key length requirements

Authentication algorithm	Hexadecimal string	Non-hexadecimal string
MD5	32 characters	53 characters
SHA	40 characters	57 characters

privacy-mode: Specifies an encryption algorithm for privacy. The three encryption algorithms AES, 3DES, and DES are in descending order of security. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements.

- **des56**: Specifies the DES algorithm.
- **aes128**: Specifies the AES algorithm.

priv-password: Specifies a case-sensitive plaintext or encrypted privacy key. A plaintext key is a string of 1 to 64 characters. If the **cipher** keyword is specified, the encrypted privacy key length requirements differ by authentication algorithm and key string format, as shown in Table 2.

Table 2 Encrypted privacy key length requirements

Authentication algorithm	Encryption algorithm	Hexadecimal string	Non-hexadecimal string
MD5	AES128 or DES-56	32 characters	53 characters
SHA	AES128 or DES-56	40 characters	53 characters

acl *acl-number*: Specifies a basic ACL to filter NMSs by source IPv4 address. The *acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv4 addresses permitted in the ACL can use the specified username to access the SNMP agent.

local: Represents a local SNMP entity user.

engineid *engineid-string*: Specifies an SNMP engine ID as a hexadecimal string. The *engineid-string* argument must comprise an even number of hexadecimal characters, in the range of 10 to 64. All-zero and all-F strings are invalid.

Change description

Before modification: Only authentication and privacy keys in hexadecimal format are supported.

After modification: Both hexadecimal and non-hexadecimal format authentication and privacy keys are supported.

- For encrypted authentication key length requirements, see Table 1.
- For encrypted privacy key length requirements, see Table 2.

Modified command: super password

Syntax

super password [**level** *user-level*] { **cipher** | **simple** } *password*

Views

System view

Parameters

level *user-level*: Specifies a user privilege level in the range of 1 to 3. The default is 3.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

key: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a plaintext string of 1 to 16 characters. If **cipher** is specified, it can be a plaintext string of 1 to 16 characters or a ciphertext string of 17 to 53 characters.

Change description

Before modification: When you specify the **cipher** keyword, you can enter a string of 1 to 16 characters or a string of 24 characters as the password.

After modification: When you specify the **cipher** keyword, you can enter a string of 1 to 53 characters as the password.

Removed feature: Local user password display mode configuration

Feature change description

The **local-user password-display-mode** command is not available to set the method for displaying local user passwords.

Removed commands

local-user password-display-mode

Syntax

local-user password-display-mode { **auto** | **cipher-force** }

undo local-user password-display-mode

Views

System view