

Security Configuration Commands

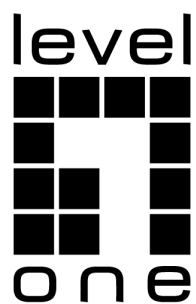


Table of Contents

Chapter 1	AAA Configuration Commands	1
1.1	AAA Authentication Configuration Commands.....	1
1.1.1	aaa authentication dot1x	1
1.1.2	aaa authentication login.....	2
1.1.3	aaa authentication ssh	2
1.2	Local Account Policy Configuration Commands	3
1.2.1	username.....	3
Chapter 2	RADIUS Configuration Commands	5
2.1	RADIUS Configuration Commands	5
2.1.1	radius-server host.....	5

Chapter 1 AAA Configuration Commands

This chapter describes the configuration commands for AAA. AAA configuration commands include authentication, authorization, accounting, and local account policy configuration commands.

1.1 AAA Authentication Configuration Commands

This chapter describes the commands used to configure AAA authentication methods. Authentication identifies users before they are allowed access to the network and network services.

AAA Authentication Configuration Commands include:

- `aaa authentication dot1x`
- `aaa authentication login`
- `aaa authentication ssh`

1.1.1 `aaa authentication dot1x`

Syntax

To configure dot1x access authentication, run the following command. To return to the default setting, use the no form of the above command.

`aaa authentication dot1x default {local | radius}`

`no aaa authentication dot1x default`

Parameter

Parameter	Description
local	Use the local username database for authentication.
radius	Use RADIUS for authentication.

Default

None

Command Mode

Global configuration mode

Usage Guidelines

Run the `aaa authentication dot1x` command to authenticate the connected dot1x users.

Related Command

None

1.1.2 aaa authentication login

Syntax

To set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode. To disable AAA authentication, use the no form of this command.

aaa authentication login default {local | radius}

no aaa authentication login default

Parameter

Parameter	Description
local	Use the local username database for authentication.
radius	Use RADIUS for authentication.

Default

local authentication

Command Mode

Global configuration mode

Usage Guidelines

Run the **aaa authentication login** command to apply the relevant commands of the relevant application (such as vty) to a specific line.

Related Command

None

1.1.3 aaa authentication ssh

Syntax

To set ssh login authentication, use the **aaa authentication ssh** command in global configuration mode. To disable ssh authentication, use the no form of this command.

aaa authentication ssh default {local | radius}

no aaa authentication ssh default

Parameter

Parameter	Description
local	Use the local username database for authentication.

radius	Use RADIUS for authentication.
---------------	--------------------------------

Default

local authentication

Command Mode

Global configuration mode

Usage Guidelines

Run the `aaa authentication ssh` command to apply the relevant commands of the relevant application (such as `vty`) to a specific line.

Related Command

None

1.2 Local Account Policy Configuration Commands

The section describes the commands for local account policy configuration. The local account policy is used for local authentication.

The local account policy configuration commands include:

- `username`

1.2.1 username

Syntax

To add users in the local user database for local authentication and authorization, run the following command. The `username` is by default in the global configuration mode. To return to the default setting, use the `no` form of this command.

`username` *username* **`password`** {**`encryption-type`**} *password* {privilege ***privilege-level***}

`no username` *username*

Parameter

Parameter	Parameter Description
<i>username</i>	user name character string
password	username password
<i>password</i>	Plain text of the password character string
encryption-type	Type of password encryption; 0 means no encryption, 6 means sha256 encryption

privilege	Specify the user level after login
<i>privilege-level</i>	Specify the specific value of the user level after login

Default

username admin password 0 admin

Command Mode

Global configuration mode

Usage Guidelines

The password cannot include spaces.

Our system only supports two encryption-types. The encryption type is 0 and 6 respectively. Parameter 0 indicates no password is defined and you enter a clear text password in the following encrypted-password blank. Parameter 6 indicates a sha256 algorithm is used for encryption and you enter encrypted text password in the following encrypted-password blank. This encrypted text password can be copied from the configuration file of other device.

Example

The following example shows how to add local users whose user name is someone and whose password is someother:

```
username someone password someother
```

The following example shows how to add the local user whose name is Oscar and whose password is Joan. The adopted encryption-type is 6. Enter the password ciphertext. 5 is the level of the user after logging in

```
username Oscar password 6 Joan privilege 5
```

Related command

aaa authentication login/dot1x/ssh

Chapter 2 RADIUS Configuration Commands

This chapter describes the commands used to configure RADIUS. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

For information on how to configure RADIUS, refer to the chapter "Configuring RADIUS".

2.1 RADIUS Configuration Commands

RADIUS Configuration Commands include:

- radius-server host

2.1.1 radius-server host

Syntax

To specify IP address of a RADIUS server, use the radius-server host command in global configuration mode. To delete the specified RADIUS host, use the no form of this command.

radius-server host *ip-address/ipv6-address* **key** *key* [**auth-port** *number*] [**timeout** *time*]

no radius-server host *ip-address/ipv6-address*

Parameter

Parameter	Description
<i>ip-address</i>	IP address of the RADIUS server host.
<i>ipv6-address</i>	IPv6 address of the RADIUS server host.
key	Password of the RADIUS server host.
<i>key</i>	The host's password.
auth-port	(Optional) Specifies the UDP destination port for authentication requests. Default: 1812
<i>auth-port</i>	UDP destination port.
timeout	(Optional) Authentication timeout. Default is 5 seconds
<i>time</i>	Timeout time

Default

No RADIUS host is specified;

Command Mode

Global configuration mode

Usage Guidelines

You can use multiple radius-server host commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

Example

The following example specifies host 1.1.1.1 as the RADIUS server and uses default ports for both accounting and authentication

```
radius-server host 1.1.1.1 key LevelOne
```

The following example specifies port 12 as the destination port for authentication requests on the RADIUS host with IP address 1.2.1.2, and the authentication timeout period is 3 seconds:

```
radius-server host 1.2.1.2 key LevelOne auth-port 12 timeout 3
```

Related Command

aaa authentication