H3C AAA Configuration Examples

Software version: Release 7595
Document version: 6W100-20201031

Contents

Introduction

This document provides AAA configuration examples for Telnet and SSH users.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of AAA.

Example: Configuring HWTACACS authentication and authorization for Telnet users

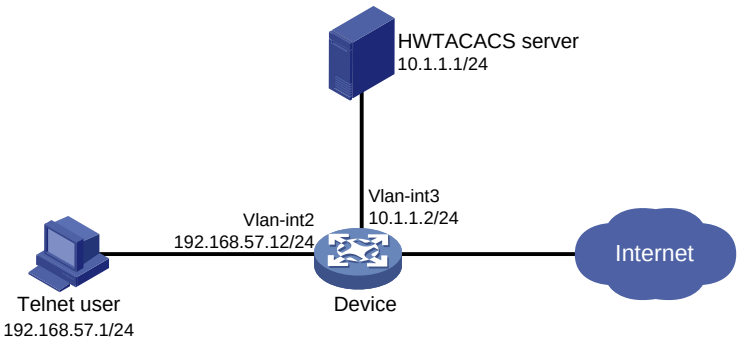
Network configuration

As shown in Figure 1, configure the device to meet the following requirements:

- The HWTACACS server is used to provide authentication and authorization services for Telnet users.
- The authenticated users are permitted to execute the **display** commands of all system features and resources.

Add a user account with username **user@bbb** and password **aabbcc** on the HWTACACS server.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure the Telnet username and password on the HWTACACS server to identify valid users.
- For Telnet users to perform AAA, set the authentication mode to **scheme** on VTY user lines.

- Configure the same shared key on the device and the HWTACACS server to secure HWTACACS communication. When the shared key is configured, the device and the HWTACACS server transfer passwords safely and the device can verify the integrity of each HWTACACS response.
- Configure HWTACACS authentication and authorization by performing the following tasks on the device:
  - Create an HWTACACS scheme.
  - Specify the authentication and authorization servers.
  - Apply the HWTACACS scheme to the ISP domain to which the Telnet users belong on the device.
- Configure the HWTACACS server to assign the user role **network-operator** to the users, so the users can use all **display** commands.

Procedures

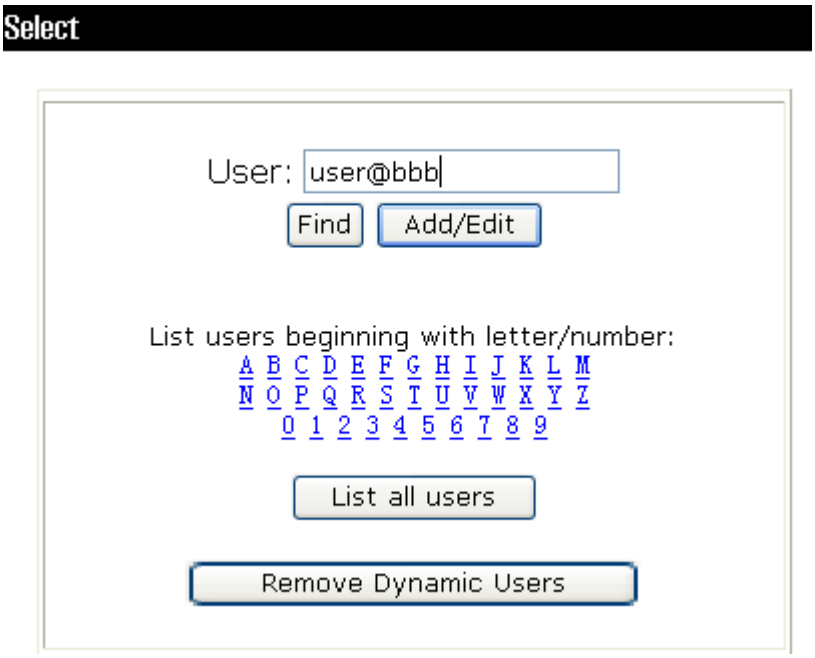
Configuring the HWTACACS server

In this example, the server runs ACS 4.0.

Adding a user

1. In the navigation tree, click **User Setup**.
2. Enter **user@bbb** in the **User** field and click **Add/Edit**, as shown in Figure 2.

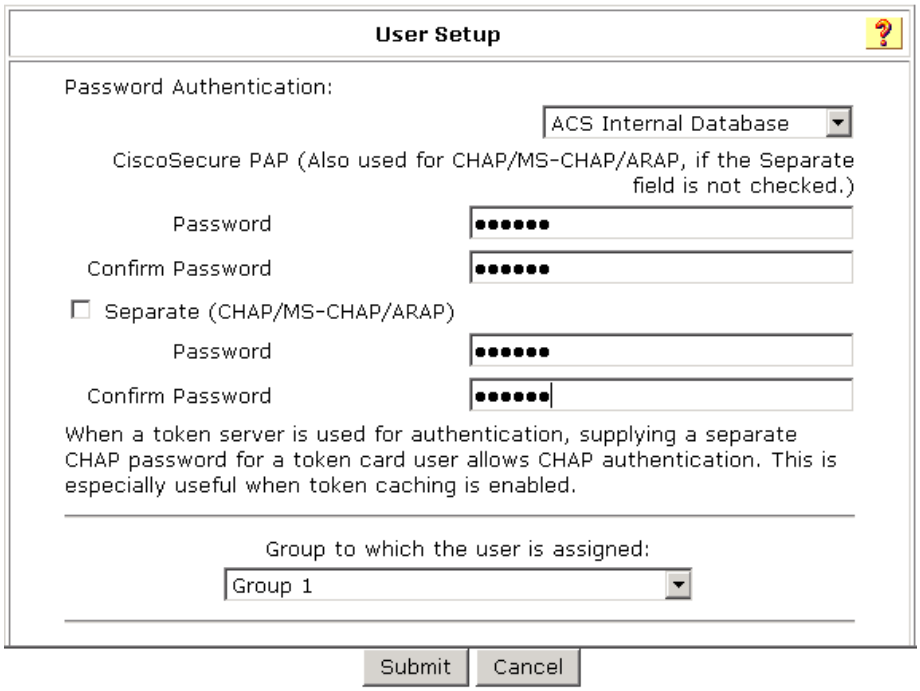
Figure 2 Adding a user



Configuring the user

1. On the **User Setup** page, configure the following parameters, as shown in Figure 3:
   - Enter **aabbcc** in the **Password** and **Confirm Password** fields.
   - Assign the user to user group **Group 1**.

Figure 3 Configuring the user password



2. Click **Submit**.

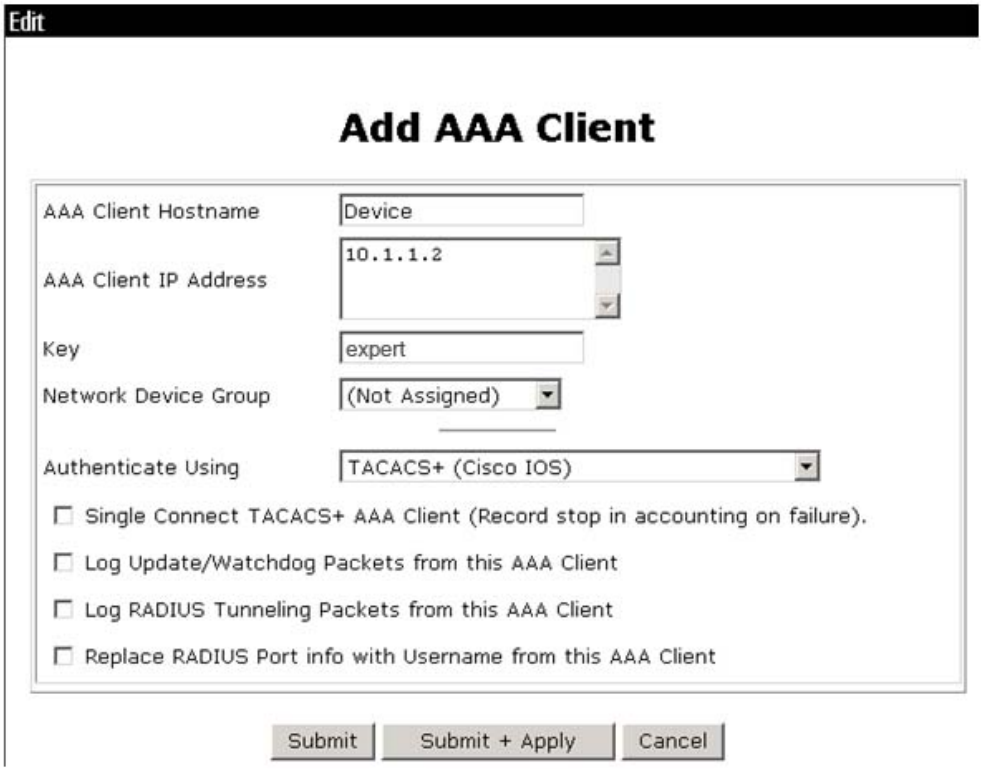
Configuring the network settings

1. In the navigation tree, click **Network Configuration**.
2. On the **Add AAA Client** page, configure the following parameters, as shown in Figure 4:
   - Enter an AAA client hostname in the **AAA Client Hostname** field. This example uses **Device**.
   - Enter **10.1.1.2** in the **AAA Client IP Address** field.

     The IP address is the source IP address for outgoing HWTACACS packets on the device.
   - Enter **expert** in the **Key** field.

     The key configured here is the same as the authentication, authorization, and accounting keys configured on the device for secure HWTACACS communication.
   - Select **TACACS+ (Cisco IOS)** from the **Authenticate Using** list.

Figure 4 Configuring the network settings

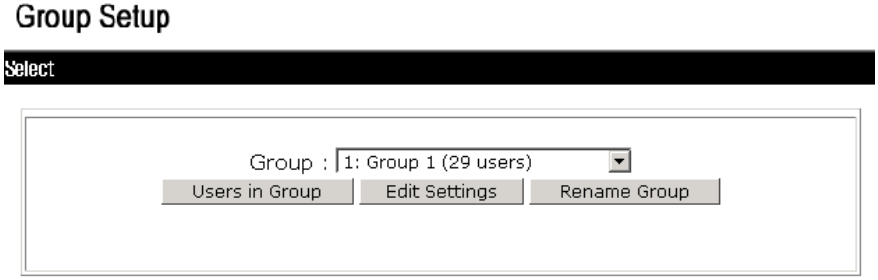


3. Click **Submit + Apply**.

Configuring the user group

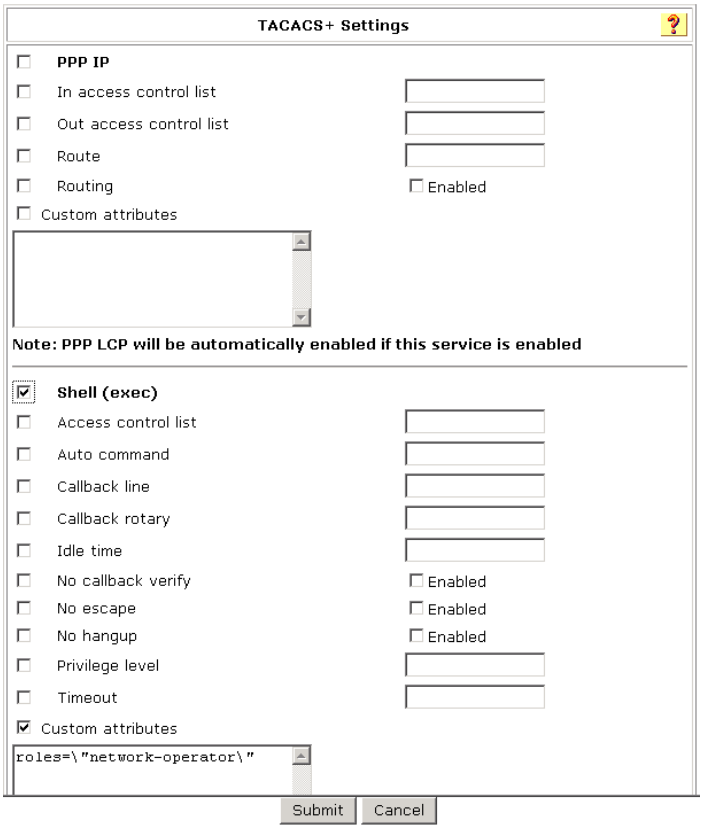
1. In the navigation tree, click **Group Setup**.
2. Select **1: Group 1 (29 users)** from the **Group** list and click **Edit Settings**, as shown in Figure 5.

Figure 5 Selecting a user group



3. On the **TACACS+ Settings** page, configure the following parameters, as shown in Figure 6:
   - Select **Shell(exec)**, which enables command execution for all users in the group.
   - Select **Custom attributes**, and enter **roles=\"network-operator\"** in the **Custom attributes** field.
   - Configure other settings as needed.

Figure 6 Configuring the user group



4. Click **Submit**.

Configuring the device

Create VLAN 2 and assign Ten-GigabitEthernet 2/0/2 to the VLAN.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port ten-gigabitethernet 2/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.57.12 255.255.255.0
[Device-Vlan-interface2] quit
```

Create VLAN 3 and assign Ten-GigabitEthernet 2/0/1 to the VLAN.

```
[Device] vlan 3
[Device-vlan3] port ten-gigabitethernet 2/0/1
[Device-vlan3] quit
```

Assign an IP address to VLAN-interface 3. The device will use this IP address as the source IP address for outgoing HWTACACS packets.

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

Enable the Telnet server feature.

```
[Device] telnet server enable
```

Enable scheme authentication on VTY user lines 0 through 63.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

Create an HWTACACS scheme named **hwtac**.

```
[Device] hwtacacs scheme hwtac
```

Specify the primary HWTACACS server with IP address **10.1.1.1** and port number **49**.

```
[Device-hwtacacs-hwtac] primary authentication 10.1.1.1 49
[Device-hwtacacs-hwtac] primary authorization 10.1.1.1 49
[Device-hwtacacs-hwtac] primary accounting 10.1.1.1 49
```

Specify the shared key as **expert** for secure HWTACACS communication between the device and HWTACACS server.

```
[Device-hwtacacs-hwtac] key authentication simple expert
[Device-hwtacacs-hwtac] key authorization simple expert
[Device-hwtacacs-hwtac] key accounting simple expert
[Device-hwtacacs-hwtac] quit
```

Create an ISP domain named **bbb**, and specify the domain to use HWTACACS scheme **hwtac** as the AAA methods of login users.

```
[Device] domain bbb
[Device-isp-bbb] authentication login hwtacacs-scheme hwtac
[Device-isp-bbb] authorization login hwtacacs-scheme hwtac
[Device-isp-bbb] accounting login hwtacacs-scheme hwtac
[Device-isp-bbb] quit
```

Verifying the configuration

Telnet to the device, and enter username **user@bbb** and password **aabbcc**. The user logs in to the device. (Details not shown.)

Verify that the user can use the **display** commands of all system features and resources. (Details not shown.)

Configuration files

```
#
 telnet server enable
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.57.12 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet2/0/2
 port link-mode bridge
```

```
 port access vlan 2
#
interface Ten-GigabitEthernet2/0/1
 port link-mode bridge
 port access vlan 3
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
hwtacacs scheme hwtac
 primary authentication 10.1.1.1
 primary authorization 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$X3oR/wjLFjDqIyjdAmvjwAhiuqewGABglQ==
 key authorization cipher $c$3$5pmuq0RJ9UWMWDkRNNERX6HFM0aRv5txFg==
 key accounting cipher $c$3$FSdSiBY1u+ZNkAYYlPw9YkGxJA4iR8MDjw==
#
 domain bbb
  authentication login hwtacacs-scheme hwtac
  authorization login hwtacacs-scheme hwtac
  accounting login hwtacacs-scheme hwtac
#
```

Example: Configuring RADIUS authentication and authorization for SSH users

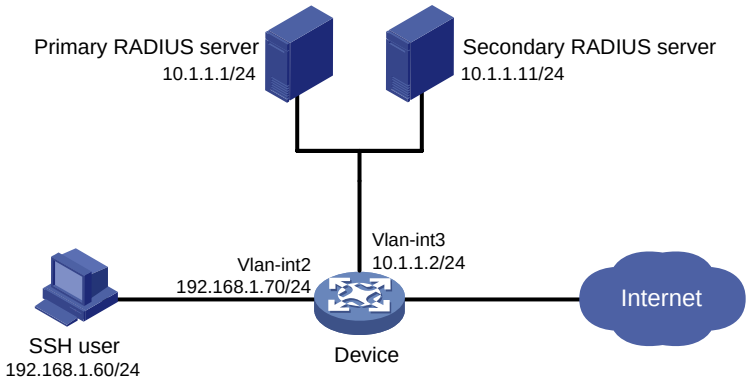
Network configuration

As shown in Figure 7, configure the device to meet the following requirements:

- The RADIUS servers are used to provide authentication and authorization services for SSH users. One server acts as the primary server and the other acts as the secondary server.
- Domain names are included in the usernames sent to the RADIUS servers.
- The authenticated users are permitted to use the **display** commands of all system features and resources.

The RADIUS servers run IMC. Add a user account with username **hello@bbb** and password **aabbcc** on each RADIUS server.

Figure 7 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure the SSH username and password on the primary and secondary RADIUS servers to identify valid users.
- For SSH users to perform AAA, set the authentication mode to **scheme** on VTY user lines.
- Configure the same shared key on the device and the RADIUS servers to secure RADIUS communication. When the shared key is configured, the device and the RADIUS servers transfer passwords safely and the device can verify the integrity of each RADIUS response.
- Configure RADIUS authentication and authorization by performing the following tasks on the device:
  - Create a RADIUS scheme.
  - Specify the primary and secondary servers for authentication and authorization.
  - Apply the RADIUS scheme to the ISP domain to which the SSH users belong.
- Configure the RADIUS servers to assign the user role **network-operator** to the users, so the users can use all **display** commands.

Restrictions and guidelines

When you configure RADIUS authentication and authorization for SSH users, follow these restrictions and guidelines:

- The Stelnet server supports only 256-bit and 384-bit ECDSA key pairs.
- Local DSA, ECDSA, and RSA key pairs for SSH use default names. You cannot assign names to the key pairs.

Procedures

Configuring RADIUS servers

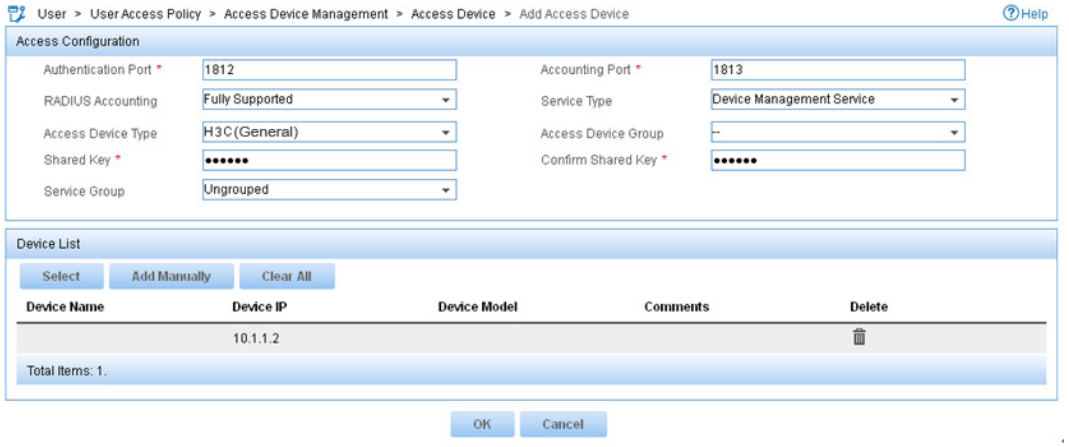
In this example, RADIUS servers run IMC PLAT 7.0 (E0102) and IMC UAM 7.0 (E0201). This example describes the configuration of the primary RADIUS server. Configure the secondary RADIUS server in the same way the primary RADIUS server is configured.

Adding the device to IMC as an access device

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy** > **Access Device Management** > **Access Device**.

   The access device list is displayed.
3. Click **Add**.
4. On the **Add Access Device** page, configure the following parameters, as shown in Figure 8:
   - Enter **1812** and **1813** in the **Authentication Port** and **Accounting Port** fields, respectively.
   - Enter **expert** in the **Shared Key** and **Confirm Shared Key** fields.
   - Select **Device Management Service** from the **Service Type** list.
   - Select **H3C(General)** from the **Access Device Type** list.
   - Use the default values for other parameters in the **Access Configuration** area.
   - In the **Device List** area, click **Select** or **Add Manually** to add the device (10.1.1.2) to IMC as an access device.

   Figure 8 Adding an access device



5. Click **OK**.

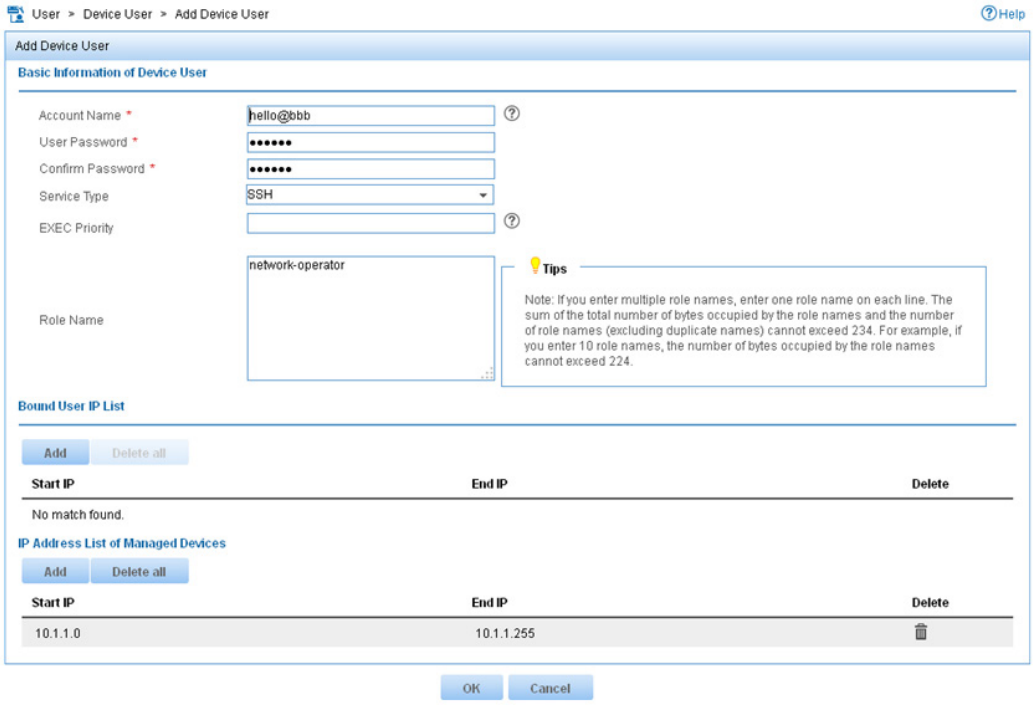
Adding a device management user

1. Click the **User** tab.
2. From the navigation tree, select **Access User** > **Device User**.

   The device management user list is displayed.
3. Click **Add**.
4. On the **Add Device User** page, configure the following parameters, as shown in Figure 9:
   - Enter **hello@bbb** in the **Account Name** field.
   - Enter **aabbcc** in the **User Password** and **Confirm Password** fields.
   - Select **SSH** from the **Service Type** list.
   - Enter **network-operator** in the **Role Name** field.

     The network-operator user role has access to the **display** commands of all system features and resources.
   - In the **IP Address List of Managed Devices** area, click **Add** to specify an IP segment (from 10.1.1.0 to 10.1.1.255) for management. The IP segment must contain the IP address of the access device.

Figure 9 Adding a device management user



5. Click **OK**.

Configuring the device

Create VLAN 2 and assign Ten-GigabitEthernet 2/0/2 to the VLAN.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port ten-gigabitethernet 2/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Device-Vlan-interface2] quit
```

Create VLAN 3 and assign Ten-GigabitEthernet 2/0/1 to the VLAN.

```
[Device] vlan 3
[Device-vlan3] port ten-gigabitethernet 2/0/1
[Device-vlan3] quit
```

Assign an IP address to VLAN-interface 3.

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

Create local RSA key pairs with default names.

```
[Device] public-key local create rsa
The range of public key size 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 DSA key pair with the default name.

```
[Device] public-key local create dsa
The range of public key size 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 256-bit ECDSA key pair with the default name.

```
[Device] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

Create a local 384-bit ECDSA key pair with the default name.

```
 [Device] public-key local create ecdsa secp384r1
Generating Keys...
.
Create the key pair successfully.
```

Enable the Stelnet server feature.

```
[Device] ssh server enable
```

Enable scheme authentication on VTY user lines 0 through 63.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

Create a RADIUS scheme named **rad**.

```
[Device] radius scheme rad
```

Specify the primary authentication RADIUS server with IP address **10.1.1.1** and port number **1812**.

```
[Device-radius-rad] primary authentication 10.1.1.1 1812
```

Specify the secondary authentication RADIUS server with IP address **10.1.1.11** and port number **1812**.

```
[Device-radius-rad] secondary authentication 10.1.1.11 1812
```

Specify the primary accounting RADIUS server with IP address **10.1.1.1** and port number **1813**.

```
[Device-radius-rad] primary accounting 10.1.1.1 1813
```

Specify the secondary accounting RADIUS server with IP address **10.1.1.11** and port number **1813**.

```
[Device-radius-rad] secondary accounting 10.1.1.11 1813
```

Set the authentication and accounting shared keys to **expert** in plain text for secure communication between the device and the RADIUS server.

```
[Device-radius-rad] key authentication simple expert
[Device-radius-rad] key accounting simple expert
```

Include domain names in the usernames sent to the RADIUS server.

```
[Device-radius-rad] user-name-format with-domain
[Device-radius-rad] quit
```

Create an ISP domain named **bbb**, and configure the ISP domain to use RADIUS scheme **rad** as the AAA methods of login users.

```
[Device] domain bbb
[Device-isp-bbb] authentication login radius-scheme rad
[Device-isp-bbb] authorization login radius-scheme rad
[Device-isp-bbb] accounting login radius-scheme rad
[Device-isp-bbb] quit
```

Verifying the configuration

Initiate an SSH connection to the device, and enter username **hello@bbb** and password **aabbcc**. The user logs in to the device. (Details not shown.)

Verify that the user can use the **display** commands of all system features and resources. (Details not shown.)

Display RADIUS scheme configuration.

```
<Sysname> display radius scheme
Total 1 RADIUS schemes

------------------------------------------------------------------
RADIUS scheme name: rad
  Index: 0
  Primary authentication server:
    IP   : 10.1.1.1                                Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
    Weight: 0
  Primary accounting server:
    IP   : 10.1.1.1                                Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 0
  Second authentication server:
    IP   : 10.1.1.11                               Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
    Weight: 0
  Second accounting server:
    IP   : 10.1.1.11                               Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 0
  Accounting-On function                    : Disabled
    extended function                       : Disabled
```

```
    retransmission times                     : 50
    retransmission interval(seconds)         : 3
  Timeout Interval(seconds)                  : 3
  Retransmission Times                       : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)               : 5
  Realtime Accounting Interval(seconds)      : 720
  Stop-accounting packets buffering          : Enabled
    Retransmission times                     : 500
  NAS IP Address                             : Not configured
  VPN                                        : Not configured
  User Name Format                           : with-domain
  Data flow unit                             : Byte
  Packet unit                                : One
  Attribute 15 check-mode                    : Strict
  Attribute 25                               : Standard
  Attribute Remanent-Volume unit             : Kilo
  server-load-sharing                        : Disabled
  Attribute 31 MAC format                    : HH-HH-HH-HH-HH-HH
```

The output shows that the primary RADIUS server is in **Active** state.

Disconnect the device from the primary RADIUS server. (Details not shown.)

Verify that the primary RADIUS server has changed to the **Block** state in the RADIUS scheme. (Details not shown.)

Configuration files

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.70 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet2/0/2
 port link-mode bridge
 port access vlan 2
#
interface Ten-GigabitEthernet2/0/1
 port link-mode bridge
 port access vlan 3
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
```

```
 ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 secondary authentication 10.1.1.11
 secondary accounting 10.1.1.11
 key authentication cipher $c$3$GBZ1jhslcGwSOpSejsESMnOr8Gb8SIT5ew==
 key accounting cipher $c$3$nGb/DWK8pxbHaLXQVc+xsmbUr1etIZVd7Q==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
```

Related documentation

- *H3C S7500X Switch Series Security Command Reference-R759X*
- *H3C S7500X Switch Series Security Configuration Guide-R759X*