

---

## AAA

You can use the AAA template for all Viptela devices.

Viptela devices support configuration of authentication, authorization, and accounting (AAA) in combination with RADIUS and TACACS+.

To configure the user access and authentication using vManage templates:

1. Create a AAA feature template to configure AAA parameters, as described in this article.
2. Create a device template that incorporates the feature templates. See the Configuration ► [Templates](#) help topic.

---

## Navigate to the Template Screen

1. In vManage NMS, select the Configuration ► Templates screen.
2. From the Templates title bar, select Feature.
3. Click Add Template.
4. In the left pane, select one or more devices. The right pane displays the available templates for the selected devices.
5. Select the AAA template.

The right pane displays the AAA template form.

- The top of the form contains fields for naming the template.
- The bottom contains fields for defining parameters applicable to that template.
- A drop-down menu to the left of each parameter field defines the scope of the parameter. When you first open a feature template form, for each parameter that has a default value, the scope is set to Default. To edit a parameter field, change the scope to Global or Device Specific. Note that if a parameter's scope is Device Specific, you cannot enter a value for it in the feature template. Instead, you enter a value when you attach the template to a device.
- A plus sign (+) is displayed to the right when you can add multiple entries for the same parameter.

---

## Minimum AAA Configuration

There is no minimum or default configuration for AAA. You must configure all desired functionality.

---

## Configure Authentication Order and Fallback

To configure authentication order and authentication fallback on a Viptela device:



Parameter Name	Description
Template Name	Enter a name for the template. It can be up to 128 characters and can contain only alphanumeric characters.
Description (Template)	Enter a description of the template. It can be up to 2048 characters and can contain only alphanumeric characters.
Authentication Order	<p>The default order is <b>local</b>, then <b>radius</b>, and then <b>tacacs</b>.</p> <p>To change the default order of authentication methods that the software tries when verifying user access to a Viptela device:</p> <ol style="list-style-type: none"> <li>1. Click the dropdown arrow to display the list of authentication methods.</li> <li>2. In the list, click the up arrows to change the order of the authentication methods and click the boxes to select or deselect a method.</li> </ol> <p>If you select only one authentication method, it must be <b>local</b>.</p>
Authentication Fallback	Click On to configure authentication to fall back from RADIUS or TACACS+ to the next priority authentication method if the user cannot be authenticated or if the RADIUS or TACACS+ servers are unreachable. With the default configuration (Off), authentication falls back only if the RADIUS or TACACS+ servers are unreachable.
Admin Authentication Order	Have the "admin" user use the authentication order configured in the Authentication Order parameter. If you do not configure the admin authentication order, the "admin" user is always authenticated locally.
RADIUS Servers	List the tags for one or two RADIUS servers. You set the tag under the RADIUS tab.

CLI equivalent:

```

system
aaa
  admin-auth-order
  auth-fallback
  auth-order (local | radius | tacacs)
  radius-servers tag

```

## Configure Local Access for Users and User Groups

To configure local access for individual users, select the Local tab, click Users, and then click the plus sign (+) to add a user:

Parameter Name	Description
Username	Enter a username. It can be 1 to 32 characters long, and it must start with a letter. It can contain



Parameter Name	Description
	<p>lowercase letters, the digits 0 through 9, and the hyphen (–) and underscore (–) characters.</p> <p>The following usernames are reserved, so you cannot configure them: <b>backup</b>, <b>basic</b>, <b>bin</b>, <b>daemon</b>, <b>games</b>, <b>gnats</b>, <b>irc</b>, <b>list</b>, <b>lp</b>, <b>mail</b>, <b>man</b>, <b>news</b>, <b>nobody</b>, <b>proxy</b>, <b>quagga</b>, <b>root</b>, <b>sshd</b>, <b>sync</b>, <b>sys</b>, <b>uucp</b>, and <b>www-data</b>. Also, names that start with <b>viptela-reserved</b> are reserved.</p>
Password	<p>Enter a password for the user. The password is an MD5 digest string, and it can contain any characters, including tabs, carriage returns, and linefeeds. For more information, see <a href="#">Section 9.4</a> in RFC 7950, <i>The YANG 1.1 Data Modeling Language</i>.</p> <p>Each username must have a password. Each user is allowed to change their own password.</p> <p>The default password for the admin user is admin. It is strongly recommended that you change this password.</p>
Description	Enter a description for the user.
Groups	Select from the list of configured groups. You must assign the user to at least one group. The admin user is automatically placed in the netadmin group and is the only member of this group.

To configure local access for user groups, you first place the user into either the basic or operator group. The admin is automatically placed in the netadmin group. Then you can configure user groups. To do this, select the Local tab, click User Groups, and click the plus sign (+) to add a group:

Parameter Name	Description
Name	<p>Name of an authentication group. It can be 1 to 32 characters long, and must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, and the hyphen (–) and underscore (–) characters. (The name cannot contain any uppercase letters.)</p> <p>The Viptela software provides three standard user groups, <b>basic</b>, <b>netadmin</b>, and <b>operator</b>. The user <b>admin</b> is automatically placed in the group <b>netadmin</b> and is the only user in this group. All users learned from a RADIUS or TACACS+ server are placed in the group <b>basic</b>. All users in the <b>basic</b> group have the same permissions to perform tasks, as do all users in the <b>operator</b> group.</p> <p>The following groups names are reserved, so you cannot configure them: <b>adm</b>, <b>audio</b>, <b>backup</b>, <b>bin</b>, <b>cdrom</b>, <b>dialout</b>, <b>dip</b>, <b>disk</b>, <b>fax</b>, <b>floppy</b>, <b>games</b>, <b>gnats</b>, <b>input</b>, <b>irc</b>, <b>kmem</b>, <b>list</b>, <b>lp</b>, <b>mail</b>, <b>man</b>, <b>news</b>, <b>nogroup</b>, <b>plugdev</b>, <b>proxy</b>, <b>quagga</b>, <b>quaggavty</b>, <b>root</b>, <b>sasl</b>, <b>shadow</b>, <b>src</b>, <b>sshd</b>, <b>staff</b>, <b>sudo</b>, <b>sync</b>, <b>sys</b>, <b>tape</b>, <b>tty</b>, <b>uucp</b>, <b>users</b>, <b>utmp</b>, <b>video</b>, <b>voice</b>, and <b>www-data</b>. Also, group names that start with the string <b>viptela-reserved</b> are reserved.</p>
Task	Click the right arrow (>) to display the privilege roles for the group. The roles are <b>interface</b> , <b>policy</b> , <b>routing</b> , <b>security</b> , and <b>system</b> . Each role allows the group to read or write specific portions of the device's configuration and to execute specific types of operational commands. Select the appropriate boxes for Read, Write, and None to assign privileges to the group for each role.

To add another group, click the plus sign (+).



To delete a group, click the trash icon at the right side of the entry.

CLI equivalent:

```
system
aaa
  user username
  group group-name
  password password
  usergroup group-name
  task (interface | policy | routing | security | system) (read | write)
```

## Configure RADIUS Authentication

To configure RADIUS, select the RADIUS tab:

Parameter Name	Description
Retransmit Count	Specify how many times to search through the list of RADIUS servers while attempting to locate a server.  <i>Range:</i> 1 through 1000 <i>Default:</i> 3
Timeout	Specify how long to wait to receive a reply from the RADIUS server before retransmitting a request.  <i>Range:</i> 1 through 1000 <i>Default:</i> 5 seconds

To configure a connection to a RADIUS server, select the RADIUS tab, and click the plus sign (+):

Parameter Name	Description
IP Address	Enter the IP address of the RADIUS server host.
Tag	Enter a text string to identify the RADIUS server. The tag can be 4 to 16 characters long. The tag allows you to configure authentication for AAA, IEEE 802.1x, and IEEE 802.11i to use a specific RADIUS server or servers.
Authentication Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. <i>Default:</i> Port 1812
Accounting Port	Enter the UDP port to use to send 802.1x and 802.11i accounting information to the RADIUS server. <i>Range:</i> 0 through 65535 <i>Default:</i> 1813
Key (Deprecated)	This field is deprecated. Use the Secret Key field instead.
Secret Key	Enter the key the Viptela device passes to the RADIUS server for authentication and encryption. You can type the



Parameter Name	Description
	key as a text string from 1 to 32 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.
Source Interface	Enter the name of the interface on the local device to use to reach the RADIUS server.
VPN	Enter the VPN in which the RADIUS server is located or through which the server can be reached. If you configure multiple RADIUS servers, they must all be in the same VPN.
Priority	Enter the priority of a RADIUS server. A server with a lower number is given priority. <i>Range:</i> 0 through 7 <i>Default:</i> 0

To configure another RADIUS server, click the plus sign (+).

To remove a server, click the trash icon on the right side of the line.

*CLI equivalent:*

```

system
radius
  retransmit number
  server ip-address
  acct-port port-number
  auth-port port-number
  priority number
  secret-key key
  source-interface interface-name
  tag tag
  vpn vpn-id
  timeout seconds

```

## Configure TACACS+ Authentication

To configure the device to use TACACS+ authentication, select the TACACS tab:

Parameter Name	Description
Timeout	Enter how long to wait to receive a reply from the TACACS+ server before retransmitting a request. <i>Range:</i> 1 through 1000 <i>Default:</i> 5 seconds
Authentication	Set the type of authentication to use for the server password. The default authentication type is PAP. You can change it to ASCII.

To configure a connection to a TACACS+ server, select the TACACS tab, and click the plus sign (+):



Parameter Name	Description
IP Address	Enter the IP address of the TACACS+ server host.
Authentication Port	Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0. <i>Default: Port 49</i>
Key (Deprecated)	This field is deprecated. Use the Secret Key field instead.
Secret Key	Enter the key the Viptela device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 32 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server.
Source Interface	Enter the name of the interface on the local device to use to reach the TACACS+ server.
VPN	VPN in which the TACACS+ server is located or through which the server can be reached. If you configure multiple TACACS+ servers, they must all be in the same VPN.
Priority	Set the priority of a TACACS+ server. A server with lower priority number is given priority over one with a higher number. <i>Range: 0 through 7</i> <i>Default: 0</i>

To configure another TACACS+ server, click the plus sign (+).

To remove a server, click the trash icon on the right side of the line.

*CLI equivalent:*

```

system
tacacs
 authentication password-authentication
 server ip-address
   auth-port port-number
   priority number
   key key
   source-interface interface-name
   vpn vpn-id
 timeout seconds

```

## Release Information

Introduced in vManage NMS in Release 15.2.

