

---

## AAA

Use the AAA template for all Viptela devices.

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

---

## Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Select the Basic Information tab.
6. To create a custom template for AAA, select the Factory\_Default\_AAA\_Template and click Create Template. The AAA template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining AAA parameters.
7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you <a href="#">attach a Viptela device to a device template</a>.</p> <p>When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see <a href="#">Create a Template Variables Spreadsheet</a>.</p>



Parameter Scope	Scope Description
	To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

## Configure Authentication Order and Fallback

To configure AAA authentication order and authentication fallback on a Viptela device, select the Authentication tab and configure the following parameters:

Parameter Name	Description
Authentication Order	<p>The default order is local, then radius, and then tacacs.</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.
Disable Netconf Logs	Click On to disable the logging of Netconf events. By default, these events are logged to the auth.info and messages log files.
Disable Audit Logs	Click On to disable the logging of AAA events. By default, these events are logged to the auth.info and messages log files.



Parameter Name	Description
RADIUS Server List	List the tags for one or two RADIUS servers. Separate the tags with commas. You set the tag under the RADIUS tab.

CLI equivalent:

```

system
aaa
  admin-auth-order
  auth-fallback
  auth-order (local | radius | tacacs)
  logs
    [no] audit-disable
    [no] netconf-disable
  radius-servers tag

```

## Configure Local Access for Users and User Groups

To configure local access for individual users, select the Local tab. To add a new user, select the User tab, click Add New User, and configure the following parameters:

Parameter Name	Description
Name	<p>Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters.</p> <p>The following usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. Also, names that start with viptela-reserved 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.
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.

Click Add to add the new user. Click Add New User again to add additional users.

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 configure user groups. To do this, select the Local tab, select the User Group tab, click Add New User Group, and configure the following parameters:

Parameter Name	Description
Name	<p>Name of an authentication group. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters.</p> <p>The Viptela software provides three standard user groups, basic, netadmin, and operator. The user admin is automatically placed in the group netadmin and is the only user in this group. All users learned from a RADIUS or TACACS+ server are placed in the group basic. All users in the basic group have the same permissions to perform tasks, as do all users in the operator group.</p> <p>The following groups names are reserved, so you cannot configure them: adm, audio, backup, bin, cdrom, dialout, dip, disk, fax, floppy, games, gnats, input, irc, kmem, list, lp, mail, man, news, nogroup, plugdev, proxy, quagga, quaggavty, root, sasl, shadow, src, sshd, staff, sudo, sync, sys, tape, tty, uucp, users, utmp, video, voice, and www-data. Also, group names that start with the string viptela-reserved are reserved.</p>
Feature	<p>The feature table lists the roles for the user group. These roles are Interface, Policy, Routing, Security, and System. Each role allows the user group to read or write specific portions of the device's configuration and to execute specific types of operational commands. Click the appropriate boxes for Read, Write, and None to assign privileges to the group for each role.</p>

Click Add to add the new user group.

To add another user group, click Add New User Group again.

To delete a user group, click the trash icon at the right side of the entry. You cannot delete the three standard user groups, basic, netadmin, and operator.

*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 authentication, select the RADIUS tab and configure the following parameters:

Parameter Name	Description
Retransmit Count	<p>Specify how many times to search through the list of RADIUS servers while attempting to locate a server.</p> <p><i>Range:</i> 1 through 1000</p> <p><i>Default:</i> 3</p>



Parameter Name	Description
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, click Add New Radius Server, and configure the following parameters:

Parameter Name	Description
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. For Cisco routers running Viptela software, this field is ignored.
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 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 ID	Enter the number of 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

Click Add to add the new RADIUS server.

To add another RADIUS server, click Add New RADIUS Server again.

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 and configure the following parameters:

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, click Add New TACACS Server, and configure the following parameters:

Parameter Name	Description
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:</i> Port 49
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 ID	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.



Parameter Name	Description
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:</i> 0 through 7 <i>Default:</i> 0

Click Add to add the new TACACS server.

To add another TACACS server, click Add New TACACS Server again.

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.

In Release 17.1, add Disable Netconf Logs and Disable Audit Logs fields.

