

---

## Configuring User Access and Authentication

This article describes how to use AAA in combination with RADIUS and TACACS+ to configure authentication, authorization, and accounting for users wishing to access Viptela devices.

---

### Configuring AAA

AAA allows you to configure local users on the Viptela device. AAA configuration is done in two steps:

- Configure users—First, you configure usernames and passwords for individuals who are allowed to access the Viptela device. The Viptela software provides one standard username, **admin**, and you can also create custom usernames, as needed.
- Configure groups—Second, you place users in groups, which define the specific configuration and operational commands that the users are authorized to view and modify. A single user can be in one or more groups. See [Role-Based Access for AAA](#) for more information about user and group privileges and the authorization that they provide.

---

### Creating Users

The Viptela software provides one standard username, **admin**. Only a user who is logged in as the admin user is permitted to create additional users.

To create a user account, configure the username and password, and place the user into a group:

```
Viptela(config) # system aaa
Viptela(config) # user username password password
Viptela(config-aaa) # group group-name
```

*username* 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. Some usernames are reserved, so you cannot configure them. For a list of them, see the [aaa](#) configuration command.

*password* is the password for the user. Each username must have a password, and each user is allowed to change their own password. The CLI immediately encrypts the string and never displays a readable version of the password. When a user is logging in to the Viptela device, they have five chances to enter the correct password. After the fifth incorrect attempt, the user is locked out of the device, and they must wait 15 minutes before attempting to log in again.

*group-name* is the name of one of the standard Viptela groups (**basic**, **netadmin**, or **operator**) or of a group configured with the **usergroup** command (discussed below). If an **admin** user changes the permission of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

The factory-default password for the **admin** username is **admin**. It is strongly recommended that you modify this password the first time you configure a Viptela device.

```
Viptela(config) # system aaa admin password password
```

Configure the password as an ASCII string. The CLI immediately encrypts the string and never displays a readable



version of the password. For example:

```
vEdge(config-user-admin)# show config
system
aaa
  user admin
    password $1$xULc8yYH$k71cTjvKESmeIGgImNDaC.
  !
  user eve
    password $1$8z3q4qoU$F6DMBr9vPBF0s/sl45ax5.
    group basic
  !
!
```

If you are using RADIUS to perform AAA authentication, you can configure a specific RADIUS server to use:

```
Viptela(config)# system aaa radius-servers tag
```

*tag* is a string that you defined with the **radius server tag** command, as described below.

---

## Creating Groups

The Viptela software provides three fixed group names: **basic**, **netadmin**, and **operator**. The username **admin** is automatically placed in the **netadmin** usergroup.

To create a custom group with specific authorization, configure the group name and privileges:

```
Viptela(config)# system aaa usergroup group-name task privilege
```

*group-name* 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. Some group names are reserved, so you cannot configure them. For a list of them, see the [aaa](#) configuration command.

If a remote RADIUS or TACACS+ server validates authentication but does not specify a user group, the user is placed into the user group **basic**. If a remote server validates authentication and specifies a user group (say, X) using VSA Viptela-Group-Name, the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).

In the **task** option, list the privilege roles that the group members have. The role can be one or more of the following: **interface**, **policy**, **routing**, **security**, and **system**.

In the following example, the **basic** user group has full access to the **system** and **interface** portions of the configuration and operational commands, and the **operator** user group can use all operational commands but can make no modifications to the configuration:

```
vEdge# show running-config system aaa
system
aaa
  usergroup basic
    task system read write
    task interface read write
  !
  usergroup operator
    task system read
    task interface read
    task policy read
    task routing read
    task security read
  !
  user admin
    password $1$tokPB7tf$VchR2JI9Sw1/dqgkqup9S.
  !
!
```



---

## Configuring RADIUS Authentication

To have a Viptela device use RADIUS servers for user authentication, configure one or up to 8 servers:

```
Viptela(config) # system radius
Viptela(config-radius) # server ip-address
Viptela(config-server) # secret-key password
Viptela(config-server) # priority number
Viptela(config-server) # auth-port port-number
Viptela(config-server) # acct-port port-number
Viptela(config-server) # source-interface interface-name
Viptela(config-server) # tag tag
Viptela(config-server) # vpn vpn-id
```

For each RADIUS server, you must configure, at a minimum, its IP address and a password, or key. You can specify the key as a clear text string up to 32 characters long or as an AES 128-bit encrypted key. The local device passes the key to the RADIUS server. The password must match the one used on the server. To configure more than one RADIUS server, include the **server** and **secret-key** commands for each server.

The remaining RADIUS configuration parameters are optional.

To set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.

By default, the Viptela device uses port 1812 for authentication connections to the RADIUS server and port 1813 for accounting connections. To change these port numbers, use the **auth-port** and **acct-port** commands.

If the RADIUS server is reachable via a specific interface, configure that interface with the **source-interface** command.

You can tag RADIUS servers so that a specific server or servers can be used for AAA, IEEE 802.1x, and IEEE 802.11i authentication and accounting. Define the tag here, with a string from 4 to 16 characters long. Then associate the tag with the [radius-servers](#) command when you configure AAA, and when you configure interfaces for 802.1x and 802.11i.

If the RADIUS server is located in a different VPN from the Viptela device, configure the server's VPN number so that the Viptela device can locate it. If you configure multiple RADIUS servers, they must all be in the same VPN.

When a Viptela device is trying to locate a RADIUS server, it goes through the list of servers three times. To change this, use the **retransmit** command, setting the number to a value from 1 to 1000:

```
Viptela(config-radius) # retransmit number
```

When waiting for a reply from the RADIUS server, a Viptela device waits 3 seconds before retransmitting its request. To change this time interval, use the **timeout** command, setting a value from 1 to 1000 seconds:

```
Viptela(config-radius) # timeout seconds
```



---

## Configuring TACACS+ Authentication

To have a Viptela device use TACACS+ servers for user authentication, configure one or up to 8 servers:

```
Viptela(config) # system tacacs
Viptela(config) # server ip-address
Viptela(config-server) # secret-key password
Viptela(config-server) # priority number
Viptela(config-server) # auth-port port-number
Viptela(config-server) # source-interface interface-name
Viptela(config-server) # vpn vpn-id
```

For each TACACS+ server, you must configure, at a minimum, its IP address and a password, or key. You can specify the key as a clear-text string up to 32 characters long or as an AES 128-bit encrypted key. The local device passes the key to the TACACS+ server. The password must match the one used on the server. To configure more than one TACACS+ server, include the **server** and **secret-key** commands for each server.

The remaining TACACS+ configuration parameters are optional.

To set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.

By default, the Viptela device uses port 49 to connect to the TACACS+ server. To change this, use the **auth-port** command.

If the TACACS+ server is reachable via a specific interface, configure that interface with the **source-interface** command.

If the TACACS+ server is located in a different VPN from the Viptela device, configure the server's VPN number so that the Viptela device can locate it. If you configure multiple TACACS+ servers, they must all be in the same VPN.

By default, PAP is used as the authentication type for the password for all TACACS+ servers. You can change the authentication type to ASCII:

```
Viptela(config-tacacs) # authentication ascii
```

When waiting for a reply from the TACACS+ server, a Viptela device waits 5 seconds before retransmitting its request. To change this time interval, use the **timeout** command, setting a value from 1 to 1000 seconds:

```
Viptela(config-tacacs) # timeout seconds
```

---

## Configuring the Authentication Order

The authentication order dictates the order in which authentication methods are tried when verifying user access to a Viptela device. The default authentication order is **local**, then **radius**, and then **tacacs**. With the default authentication order, the authentication process occurs in the following sequence:

- The authentication process first checks whether a username and matching password are present in the running



configuration on the local device.

- If local authentication fails, and if you have not configured authentication fallback (with the [auth-fallback](#) command), the authentication process stops. However, if you have configured authentication fallback, the authentication process next checks the RADIUS server. For this method to work, you must configure one or more RADIUS servers with the [system radius server](#) command. If a RADIUS server is reachable, the user is authenticated or denied access based on that server's RADIUS database. If a RADIUS server is unreachable and if you have configured multiple RADIUS servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's RADIUS database.
- If the RADIUS server is unreachable (or all the servers are unreachable), the authentication process checks the TACACS+ server. For this method to work, you must configure one or more TACACS+ servers with the [system tacacs server](#) command. If a TACACS+ server is reachable, the user is authenticated or denied access based on that server's TACACS+ database. If a TACACS+ server is unreachable and if you have configured multiple TACACS+ servers, the authentication process checks each server sequentially, stopping when it is able to reach one of them. The user is then authenticated or denied access based on that server's TACACS+ database.
- If the TACACS+ server is unreachable (or all TACACS+ servers are unreachable), user access to the local Viptela device is denied.

To modify the default order, use the **auth-order** command:

```
Viptela(config-system-aaa) # auth-order (local | radius | tacacs)
```

Specify one, two, or three authentication methods in the preferred order, starting with the one to be tried first. If you configure only one authentication method, it must be **local**.

When you log in from a console port, you are authenticated locally. No other authentication methods can be used.

To have the "admin" user use the authentication order configured in the **auth-order** command, use the following command:

```
Viptela(config-system-aaa) # admin-auth-order
```

If you do not include this command, the "admin" user is always authenticated locally.

You can configure authentication to fall back to a secondary or tertiary authentication mechanism when the higher-priority authentication method fails to authenticate a user, either because the user has entered invalid credentials or because the authentication server is unreachable (or all the servers are unreachable):

```
Viptela(config-system-aaa) # auth-fallback
```

Fallback to a secondary or tertiary authentication mechanism happens when the higher-priority authentication server fails to authenticate a user, either because the credentials provided by the user are invalid or because the server is unreachable.

The following examples illustrate the default authentication behavior and the behavior when authentication fallback is enabled:

- If the authentication order is configured as **radius local**:



- With the default authentication, local authentication is used only when all RADIUS servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for local authentication.
- With authentication fallback enabled, local authentication is used when all RADIUS servers are unreachable or when a RADIUS server denies access to a user.
- If the authentication order is configured as **local radius**:
  - With the default authentication, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device.
  - With authentication fallback enabled, RADIUS authentication is tried when a username and matching password are not present in the running configuration on the local device. In this case, the behavior of two authentication methods is identical.
- If the authentication order is configured as **radius tacacs local**:
  - With the default authentication, TACACS+ is tried only when all RADIUS servers are unreachable, and local authentication is tried only when all TACACS+ servers are unreachable. If an authentication attempt via a RADIUS server fails, the user is not allowed to log in even if they have provided the correct credentials for the TACACS+ server. Similarly, if a TACACS+ server denies access, the user cannot log via local authentication.
  - With authentication fallback enabled, TACACS+ authentication is used when all RADIUS servers are unreachable or when a RADIUS server denies access a user. Local authentication is used next, when all TACACS+ servers are unreachable or when a TACACS+ server denies access to a user.

If a remote server validates authentication but does not specify a user group, the user is placed into the user group **basic**.

If a remote server validates authentication and specifies a user group (say, X), the user is placed into that user group only. However, if that user is also configured locally and belongs to a user group (say, Y), the user is placed into both the groups (X and Y).

If a remote server validates authentication and that user is not configured locally, the user is logged in to the vshell as the user **basic**, with a home directory of `/home/basic`.

If a remote server validates authentication and that user is configured locally, the user is logged in to the vshell under their local username (say, eve) with a home direction of `/home/username` (so, `/home/eve`).

---

## Configuring NAS Attributes

For RADIUS and TACACS+, you can configure Network Access Server (NAS) attributes for user authentication and authorization. To do this, you create a vendor-specific attributes (VSA) file, also called a RADIUS dictionary or a TACACS+ dictionary, on the RADIUS or TACACS+ server that contains the desired permit and deny commands for each user. The Viptela device retrieves this information from the RADIUS or TACACS+ server.

The VSA file must be named `dictionary.viptela`, and it must contain text in the following format:



```
localhost$ more dictionary.viptela
# -*- text -*-
#
# dictionary.viptela
#
#
# Version:      $Id$
#
VENDOR          Viptela                      41916
BEGIN-VENDOR     Viptela
ATTRIBUTE        Viptela-Group-Name          1      string
```

The Viptela software has three predefined user groups, as described above: **basic**, **netadmin**, and **operator**. These groups have the following permissions:

```
Viptela# show aaa usergroup
GROUP      USERS  TASK      PERMISSION
-----
basic      -        system    read
           -        interface read
netadmin   admin  system    read write
           admin  interface read write
           -        policy    read write
           -        routing   read write
           -        security  read write
operator   -        system    read
           -        interface read
           -        policy    read
           -        routing   read
           -        security  read
```

To create new user groups, use this command:

```
Viptela(config)# system aaa usergroup group-name task privilege
```

Here is a sample user configuration on a RADIUS server, which for FreeRADIUS would be in the file "users":

```
user1  Cleartext-password := "user123"
       Service-Type = NAS-Prompt-User,
       Viptela-Group-Name = operator,
```

Then in the dictionary on the RADIUS server, add a pointer to the VSA file:

```
$INCLUDE      /usr/share/freeradius/dictionary.viptela
```

For TACACS+, here is a sample configuration, which would be in the file tac\_plus.conf:

```
group = test_group {
    default service = permit
    service = ppp protocol = ip {
        Viptela-Group-Name = operator
    }
}
user = user1 {
    pap = cleartext "user123"
    member = test_group
}
```

## Additional Information

[Configuring IEEE 802.1x and IEEE 802.11i Authentication](#)

[Role-Based Access with AAA](#)

[show aaa usergroup](#)



[show users](#)

