Configure RADIUS for User Authentication

For supported software information, click here.

RADIUS is a distributed client-server system that secures networks against unauthorized access. A RADIUS server provides an external database that you can use to authenticate users before allowing them to access a network, a device, or related services.

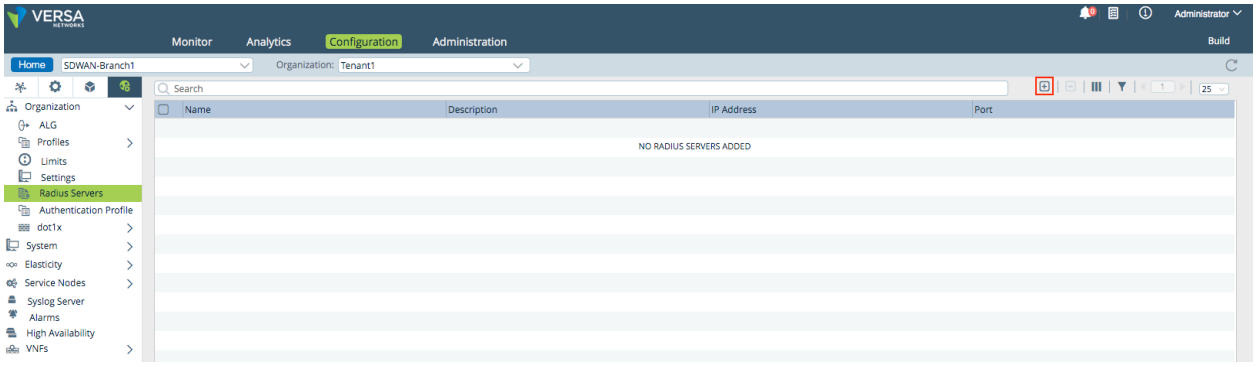
Configure RADIUS for User Authentication

You can configure RADIUS for secure access user authentication.

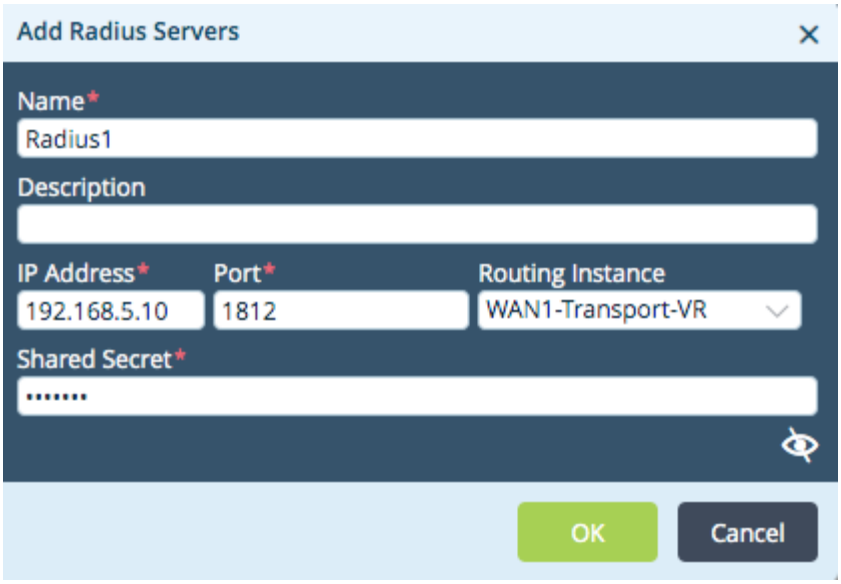
Note: For Release 20.2.2, RADIUS authentication is supported for MacOS-native and Windows-native clients only.

To configure RADIUS for user authentication:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Organization > RADIUS Servers in the left menu bar. The main pane displays the RADIUS servers that are already configured.

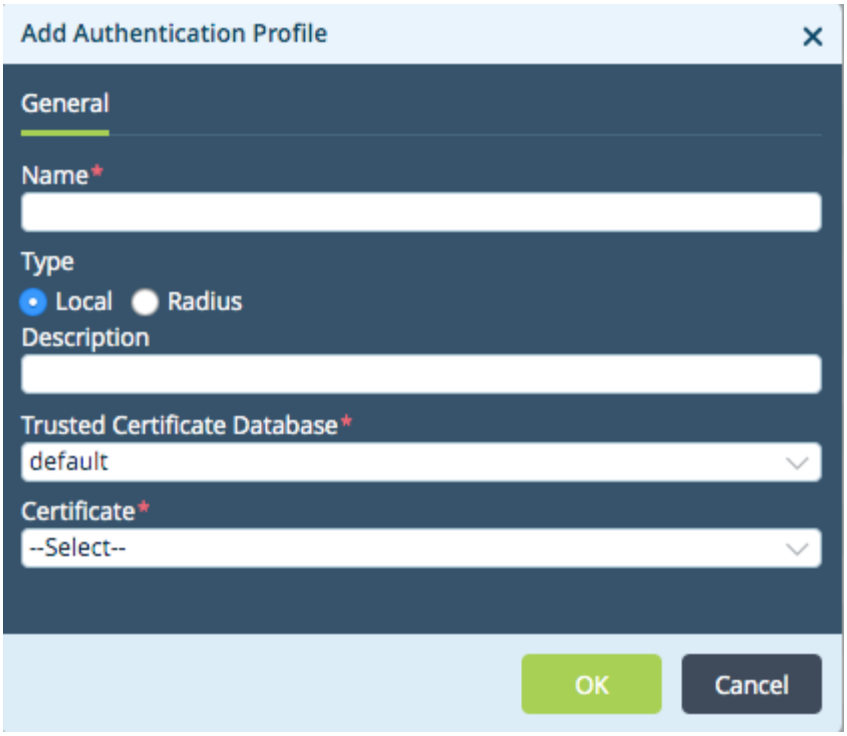


4. Click the Add icon, and in the Add RADIUS Servers popup window, enter information for the following fields.

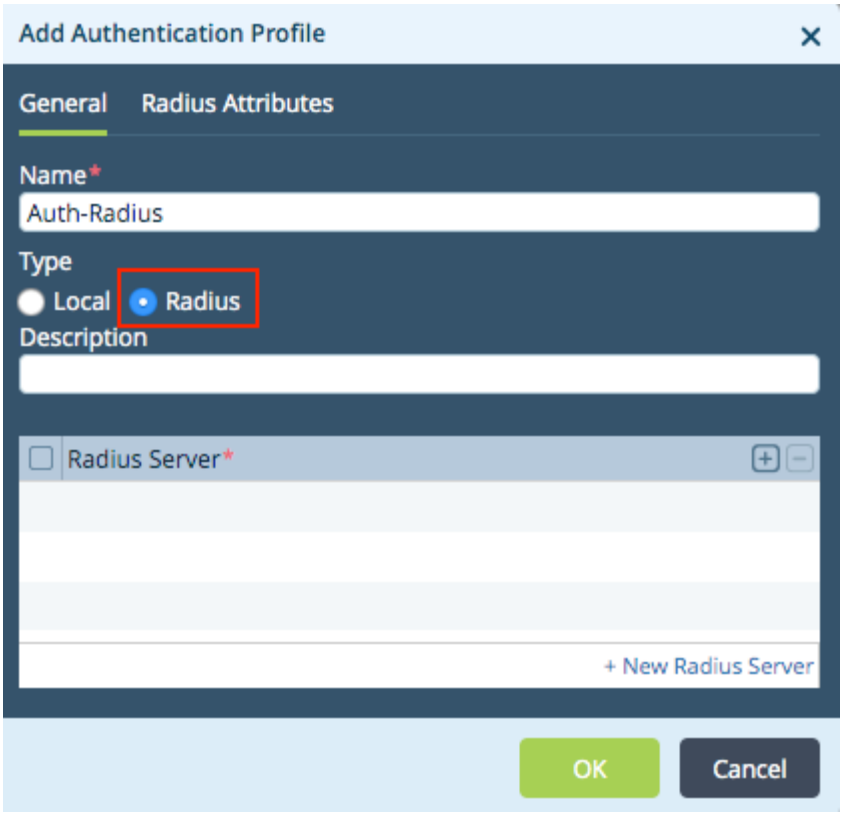


Field	Description
Name (Required)	Enter a name for the RADIUS server.
Description	Enter a text description for the RADIUS server.
IP Address (Required)	Enter the IP address of the RADIUS server.
Port (Required)	Enter the port number to use on the RADIUS server.
Routing Instance	Enter the routing instance to use to reach the RADIUS server.
Shared Secret (Required)	Enter the RADIUS shared secret (password) string.

5. Click OK.
6. Select Others > Organization > Authentication Profiles in the left menu bar. The main pane displays the Authentication Profiles that are already configured.
7. Click the Add icon. The Add Authentication Profile popup window displays.

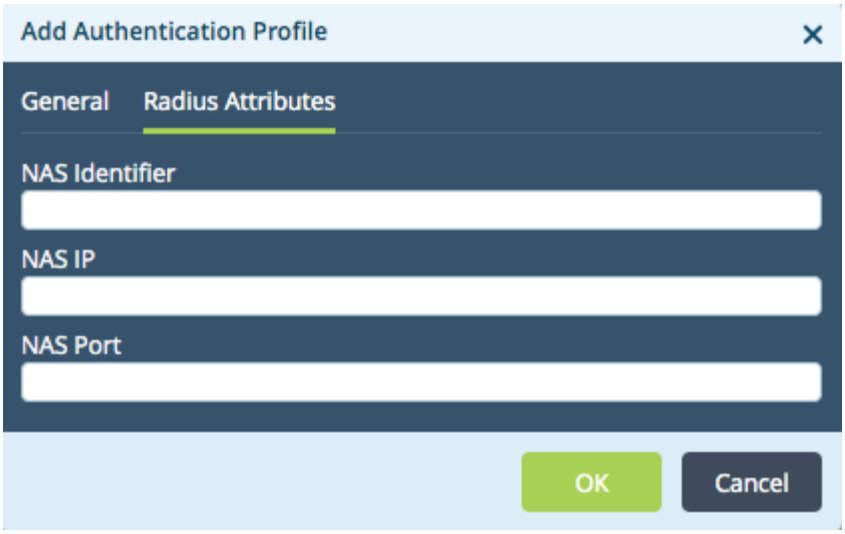


8. In the Name field, enter a name for the authentication profile.
9. In the Type field, click RADIUS, and enter information for the following fields. Note that when you click RADIUS, the RADIUS Attributes tab displays in the popup window.



Field	Description
Description	Enter a description for the RADIUS server
Radius Server (Required)	Click the Add icon and select a RADIUS server from the drop-down list. To configure a new RADIUS server, click + New Radius Server and enter the required information.

10. Select the RADIUS Attributes tab, and enter the information for the following fields.



Field	Description
NAS Identifier	Enter a text string to identify the network access server (NAS) that originates the access request.
NAS IP	Enter the IP address of the NAS that is requesting authentication. *Default:* None
NAS Port	Enter the number of the physical port number to use to connect to the NAS that is authenticating the user. Range: 0 through 65535 *Default:* None

11. Click OK.

Configure the RADIUS Server

The following example shows how to configure the freeRADIUS server on Ubuntu.

1. Edit the /etc/freeradius/users file, and configure users. For example:

```
"admin" Cleartext-Password := "admin"
Reply-Message = "Hello admin, %{User-Name}",
Versa-User-Group = admin
```

2. In the /etc/freeradius/eap.conf file, ensure that the default_eap_type is set to mschapv2.
3. In the /etc/freeradius/clients.conf file, configure the client's IP address and the RADIUS secret password. For example:

```
client versa {
ipaddr = 192.168.11.101  ## Egress IP address of RADIUS requests sent from VOS device
secret = "versa123"      ## Same password as set in VOS RADIUS server configuration
```

Supported Software Information

Releases 20.2.2 and later support all content described in this article.

Additional Information

Configure the Versa Secure Access Service