

---

## Configure Dynamic VLAN Assignment Using 802.1X Authentication

 For supported software information, click [here](#).

You can configure a Versa Operating System™ (VOS™) device to use a RADIUS authentication server to dynamically assign VLANs to bridge ports using the 802.1X authentication. After a port is authenticated using 802.1X device authentication, the authentication server assigns a VLAN to the port.

You can configure dynamic VLAN assignment on Layer 2 VNI interfaces that are also 802.1X authenticator interfaces.

The 802.1X supplicant type can be one of the following:

- Single—Authenticate only the first end device. All other end devices that connect to the port later are allowed access without any further authentication. The subsequent devices effectively piggyback on the first end device's authentication.
- Single-secure—Allow only one end device to connect to the port at a time. No other end device can connect until the first device logs out.
- Multiple—Allow multiple end devices to connect to the port. Each end device is authenticated individually. You can configure multiple mode only on bridge interfaces that are in trunk mode. You configure the trunk interface with member VLANs, a native VLAN ID, which is one of the VLANs in the trunk interface, and 802.1X settings.

For Layer 2 trunk ports, you can configure only unit 1 of the interface as an 802.1X interface.

Before you configure dynamic VLAN assignment, you must create an access bridge (Layer 2) interface that has the same VLAN ID (802.1X setting). (For more information, see [Configure Access Interfaces](#) in the [Configure Layer 2 Forwarding](#) article.) Then, based on the interface's 802.1X authentication, the VLAN ID changes from its starting value to dynamic VLAN ID. To display information about the change and the dynamic VLAN ID for the interfaces, issue the **show interface detail** CLI command.

When you remove the 802.1X authentication configuration from the Layer 2 access interface, the initial or user-configured 802.1X VLAN ID takes effect for the interface.

VOS devices support the following 802.1X VLAN assignments:

- Authentication default VLAN ID—If 802.1X device authentication succeeds and if RADIUS dynamic VLAN is disabled, or if VLAN information is not received from the RADIUS server, the authentication default VLAN ID is assigned to interface.
- Guest VLAN ID—The guest VLAN provides limited access for devices that have failed authentication or that are nonresponsive end devices that are not 802.1X-enabled. If no device authenticates using 802.1X authentication, the guest VLAN ID is assigned to the interface.

- RADIUS dynamic VLAN—VLAN assignment is done based on the response from the RADIUS server authentication server. The RADIUS server must return the following attributes to the VOS device:
  - Tunnel-Type (Type 64) set to VLAN (13)
  - Tunnel-Medium-Type (Type 65) set to 802 (6)
  - Tunnel-Private-Group-ID (Type 81) set to VLAN ID

Before you configure dynamic VLANs using the 802.1X authentication, ensure that you familiar with the following:

- How to configure 802.1X authentication on VNI interfaces. For more information, see [Configure IEEE 802.1X Device Authentication](#).
- How to configure Layer 2 interfaces. For more information, see [Configure Layer 2 Forwarding](#).

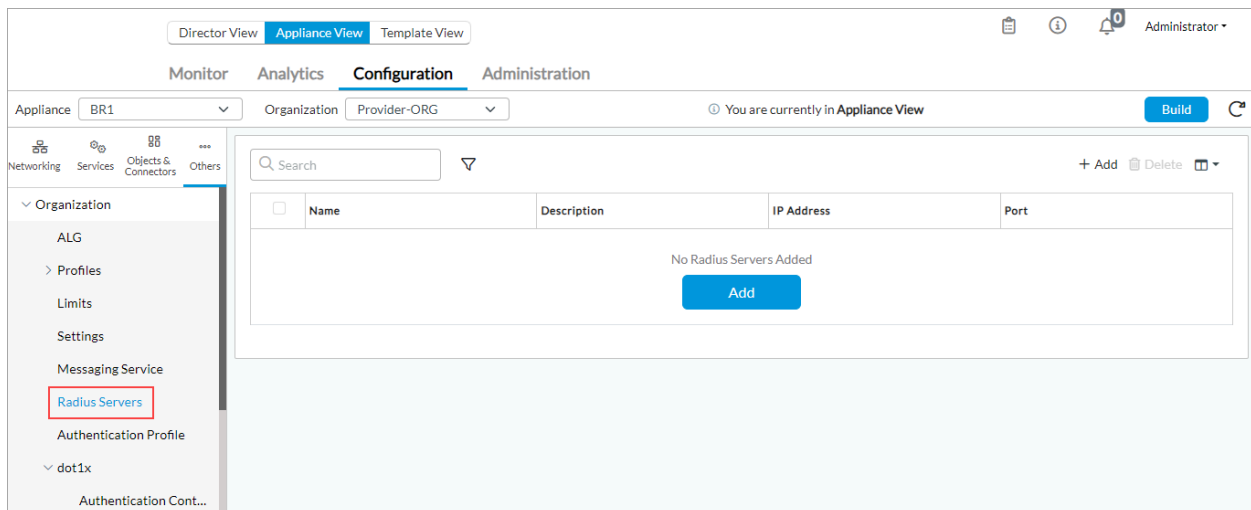
## Configure Dynamic VLANs using the 802.1X Authentication Flow


To configure dynamic VLAN assignment using 802.1X authentication, you do the following:

- Configure a RADIUS server.
- Configure an authentication profile that includes the RADIUS server you configured.
- Configure the dynamic VLAN assignment.

### Configure a RADIUS Server

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the horizontal menu bar.
  - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select Others > Organization > RADIUS Servers in the left menu bar.



3. Click the  Add icon. In the Add RADIUS Servers popup window, enter information for the following fields.

Add Radius Servers

Name \*

Description

IP Address \*

Port \*

Routing Instance

--Select--

Shared Secret \*

OK

Cancel

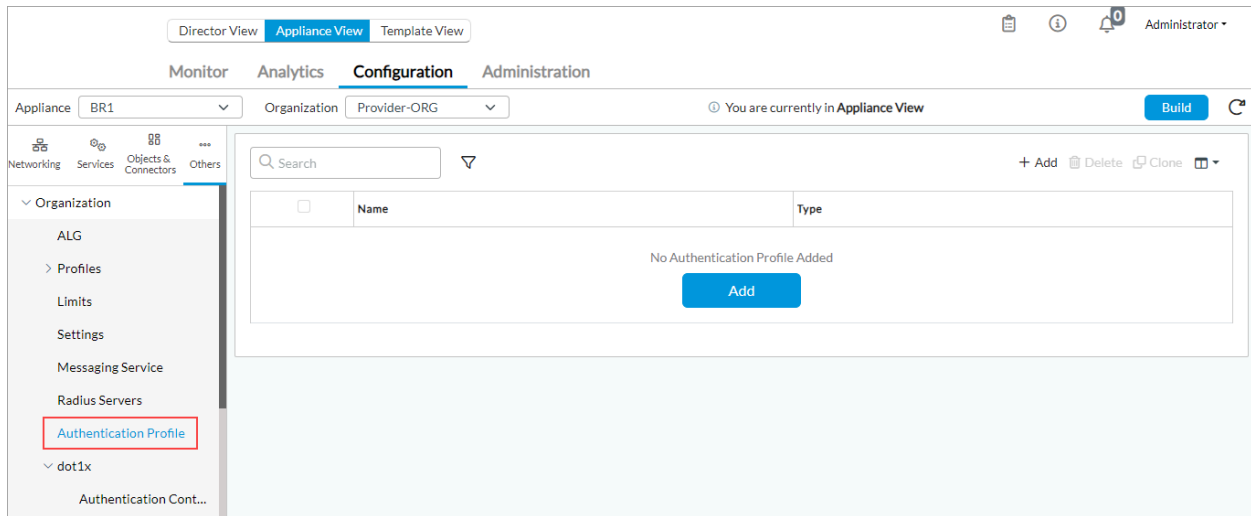
Field	Description
Name (Required)	Enter a name for the RADIUS server.
Description	Enter a description for the RADIUS server.
IP Address (Required)	Enter the IP address of RADIUS server.
Port (Required)	Enter the port to connect to on the RADIUS server.
Routing Instance	Select a routing instance to use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


4. Click OK.

---

## Configure an Authentication Profile

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the horizontal menu bar.
  - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select Others > Organization > Authentication Profile in the left menu bar.



3. Click the  Add icon. In the Add Authentication Profile popup window, select the General tab and enter information for the following fields.

Add Authentication Profile

General

Name \*

Type

☒ Local
☐ Radius

Description

Trusted Certificate Database \*


--Select--

Certificate \*

--Select--

OK
Cancel

Field	Description
Name (Required)	Enter a name for the authentication profile.
Type (Required)	Select an authentication type: <ul style="list-style-type: none"> <li>Local</li> <li>RADIUS</li> </ul>
Description	Enter a description for the local or RADIUS server.
Trusted Certificate Database (Required)	For local authentication type, select the trusted certificate database to use to verify and confirm the authority of the server certificate.
Certificate (Required)	For local authentication type, select a certificate to use to authenticate the server.

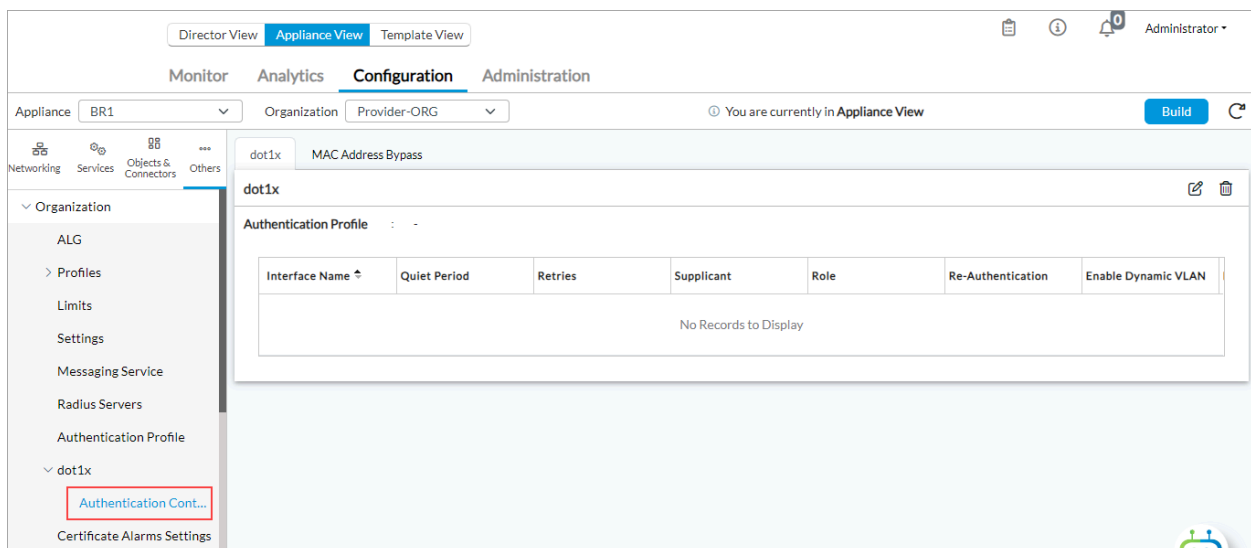
Field	Description
Radius Server (Required)	Click the  Add icon, and then select the RADIUS server. To add a new RADIUS server, click + New RADIUS Server. See <a href="#">Configure a RADIUS Server</a> .


4. Click OK.

## Configure Dynamic VLAN Assignment

To dynamically assign VLANs to bridge access ports using the 802.1X device authentication flow:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select the Appliances in the left menu bar.
  - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Organization > dot1x > Authentication Control in the left menu bar, and then select the dot1x tab in the horizontal menu bar.



4. Click the  Edit icon. In the dot1x popup window, enter information for the following fields.

dot1x

Authentication Profile \*

--Select--

Interface Name \*

--Select--

Quiet Period

60

No Re-Authentication

☐

Re-Authentication Interval

Retries

2

Role

--Select--

Supplicant

--Select--

No Interface Added


OK

Cancel

Field	Description
Authentication Profile (Required)	Select an authentication profile.
Interface Name (Required)	Select an interface name.
Quiet Period	<p>Enter how long the interface waits after a failed authentication attempt before trying to authenticate a user again.</p> <p><i>Range:</i> 0 through 600 seconds</p> <p><i>Default:</i> None</p>
No Reauthentication	Click to disable periodic reauthentication of users.
Reauthentication Interval	<p>Enter the interval at which to reauthenticate the user. By default, a user is reauthenticated at each configured interval.</p> <p><i>&lt;Range:</i> 10 through 86400 seconds</p> <p><i>Default:</i> None</p>
Retries	Enter how many times to try to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

Field	Description
	<p><i>Range:</i> 1 through 10</p> <p><i>Default:</i> 2</p>
Role	<p>Select the interface role:</p> <ul style="list-style-type: none"> <li>◦ Authenticator—Interface acts as the authenticator</li> <li>◦ Supplicant—Interface acts as a supplicant</li> </ul> <p><i>Default:</i> None</p>
Supplicant	<p>Select the type of supplicant:</p> <ul style="list-style-type: none"> <li>◦ Multiple—Allow multiple end devices to connect to the port. Each end device is authenticated individually. Multiple mode is supported only on bridge interfaces in trunk mode.</li> <li>◦ Single—Authenticate only the first end device. All other end devices that connect to the port later are allowed access without any further authentication. The subsequent devices effectively piggyback on the first end device's authentication.</li> <li>◦ Single-secure—Allow only one end device to connect to the port at a time. No other end device can connect until the first device logs out.</li> </ul> <p><i>Default:</i> None</p>
Enable Dynamic VLAN	Click to enable dynamic VLANs.
Enable RADIUS Dynamic VLAN	Click to enable RADIUS dynamic VLANs.
Auth Default VLAN ID	<p>Enter the ID for the default VLAN.</p> <p><i>Range:</i> 0 through 4094</p> <p><i>Default:</i> None</p>
Guest VLAN ID	<p>Enter the ID for the guest VLAN.</p> <p><i>Range:</i> 0 through 4094</p>



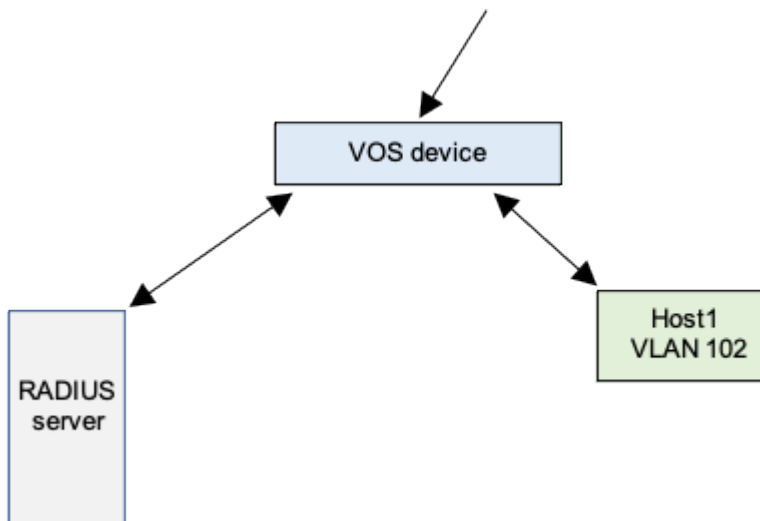
Field	Description
	<i>Default:</i> None
 Add Icon	Click to add the interface to the 802.1X profile.

5. Click OK.

## Configuration Examples

The examples in this section show how to configure a multiple supplicant and a single supplicant.

The following figure illustrates single-supplicant mode. Here, there is only one host (single supplicant) in the topology, Host1. You configure the interface in access mode with a VLAN ID of dot1x.



Edit Ethernet Interface - vni-0/6

General
Sub Interfaces

Interface \*

vni
0
6

☐ Disable

Description
Tags

☒ Promiscuous
☐ Virtual Wire
☐ Mirror Interface
☐ PPPoE base Interface
☐ DHCP Trusted

Native VLAN ID
MTU
Outer TPID
--Select--

Bandwidth
Others
Hold Time
PoE
Multihoming

Uplink (Kbps)
Downlink (Kbps)

OK
Cancel

Edit Ethernet Interface - vni-0/6

General
Sub Interfaces

☒ Subinterfaces
☐ Aggregate Member

+
☐
☐
☐
☐
☐
1
25

<input type="checkbox"/>	Unit	VLAN ID	IP Address/Mask		DHCPv4	DHCPv6	MTU	Bridge	
			IPv4	IPv6				Interface Mode	VLAN ID
<input type="checkbox"/>	0		192.168.11.251...		<input type="checkbox"/>	<input type="checkbox"/>			

OK
Cancel

Add Subinterface

General
IPv4
IPv6
Bridge

Interface Mode

Access

☒ dot1x

VLAN ID
dot1x

VLAN ID List

\*\*Deselect Interface Mode to enable IPv4 IPv6 configuration

OK
Cancel

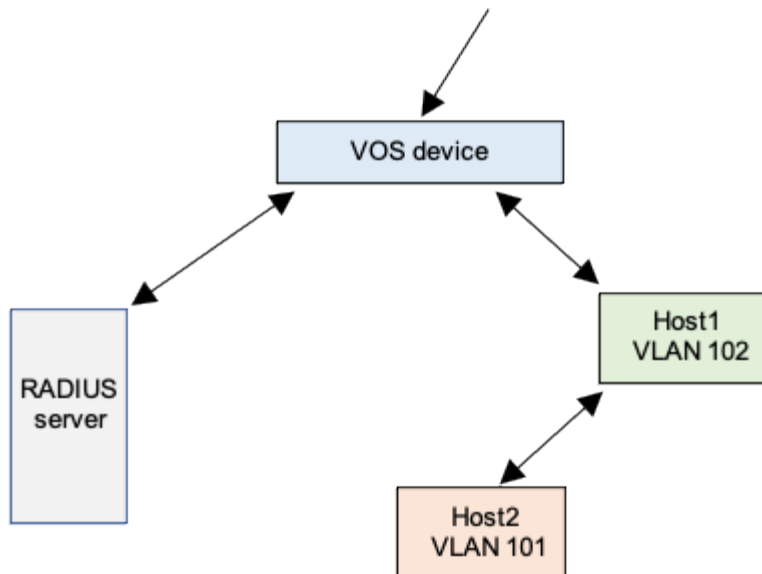
The following figure illustrates multiple-supplicant mode. Here, there are two hosts in the topology, Host1 and Host2.

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Common\\_Configuration/Configure\\_Dyna...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Dyna...)

Updated: Wed, 23 Oct 2024 08:27:27 GMT

Copyright © 2024, Versa Networks, Inc.

Host1 is assigned to one VLAN (here, VLAN ID 102), and Host2 is assigned to a different VLAN (here, VLAN ID 101). The RADIUS server assigns the VLAN ID based on the client authentication. You configure the 802.1X interface in trunk mode, and you enable multiple-supplicant mode. You also configure the interface with a native VLAN that is same as the guest VLAN.



Edit Ethernet Interface - vni-0/0

General

Sub Interfaces

Interface \*

vni - 0 / 0

☐ Disable

Description

Tags

☐ Promiscuous

☐ Virtual Wire

☐ Mirror Interface

☐ PPPoE base Interface

☐ DHCP Trusted

Native VLAN ID

MTU

Outer TPID

--Select--

Bandwidth

Others

Hold Time

PoE

Multihoming

Uplink (Kbps)

Downlink (Kbps)

OK

Cancel

Edit Subinterface

General
IPv4
IPv6
Bridge

Unit
0
VLAN ID
1\_4094
Inner VLAN ID
1\_4094
☐ Disable

Description
WAN interface: BR-WAN

MTU
72...9000
Interface Mode
--Select--

Publish Address
URL
Routing Instance
--Select--

Bandwidth
Uplink (Kbps)
1...10000000
Downlink (Kbps)
1...10000000

OK
Cancel

Edit Subinterface

General
IPv4
IPv6
Bridge

Interface Mode
Trunk
☐ dot1x
VLAN ID
1\_4094
VLAN ID List

\*\*Deselect Interface Mode to enable IPv4 IPv6 configuration

OK
Cancel

You can display the configuration and VLAN information as follows:

- In Director view, select Administration > Appliances and then select the device name.
- In Appliance view, select Configuration > Others > Organization > dot1x > Authentication Control and select the dot1x tab.

## Supported Software Information

Releases 21.2.1 and later support all content described in this article.

## Additional Information

[Configure IEEE 802.1X Device Authentication](#)

[Configure Layer 2 Forwarding](#)