
Configure IEEE 802.1X Device Authentication

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

IEEE 802.1X is a port-based network access control (PNAC) protocol that authenticates devices before they can connect to the network and gain access to network resources. You can configure IEEE 802.1X to prevent unauthorized network devices from accessing the network and to allow known devices to connect to the network without requiring authentication. You configure IEEE 802.1X on a VNI interface.

IEEE 802.1X has three required components:

- **Supplicant**—A client that runs on the endpoint and submits credentials for authentication. A Versa Operating System™ (VOS™) interface always acts as an authenticator. If you configure a RADIUS server as the authenticating server, the VOS interface acts only as an authenticator and sends information about the supplicant to the authenticating server. If you use local authentication (that is, you do not use a RADIUS server or an identity provider server), the VOS interface acts as both the authenticator and the authenticating server.
- **Authenticator**—A network access device that facilitates the authentication process by relaying the credentials of the supplicant to the authentication server. The authenticator enforces both the locally configured network access policy and the dynamically assigned network access policy returned by the authentication server. If you configure a VOS interface with the authenticator role, the VOS interface acts as the authenticator.
- **Authentication server**—A server that validates the credentials sent by the supplicant and determines what level of network access the end user or device should receive. You can use a RADIUS server as the authentication server, or you can use local authentication so that the VOS device acts as the authentication server.

When you configure a VOS VNI interface to be an authenticator, a RADIUS server can authenticate each user or device connected to a port before that user or device can access any network services.

For Releases 22.1.3 and later, the VOS IEEE 802.1X software uses Extensible Authentication Protocol over LAN (EAPOL) for communication between a client device and a LAN switch. If a client does not use EAPOL (known as a non-EAPOL client), the MAC Authentication Bypass (MAB) protocol authenticates the client by sending their MAC address information to a RADIUS server. A non-EAPOL client is learned initially on a guest VLAN, and its MAC address is sent to a RADIUS server for authentication. You can send the MAC addresses with or without the colon (:) delimiter. The RADIUS server uses the MAC address as the username and password. After a non-EAPOL client has been authenticated, it is moved from the guest VLAN to the RADIUS-assigned VLAN or to the default VLAN.

The following table lists the RADIUS attributes that VOS devices support.

Value	Attribute Name	Data Type	Description
1	User-Name	Text	Name of user to authenticate
2	User-Password	String	Password of user to authenticate
4	NAS-IP-Address	IPv4 address	IP address of the network access server (NAS) that is requesting authentication of the user
5	NAS-Port	Integer	Physical port number of the NAS that is authenticating the user
6	Service-Type	Enumerated data type	Type of service that the user is requesting, or type of service to provide
8	Framed-IP-Address	IPv4 address	IP address to configure for the user
12	Framed-MTU	Integer	Maximum transmission unit size to configure for the user if the MTU is not negotiated some other way
24	State	String	String to use to maintain state information between the device and the RADIUS server
31	Calling-Station-Id	Text	Phone number from which the call originated
44	Acct-Session-Id	Text	Accounting identifier
49	Acct-Terminate-Cause	Enumerated data type	Reason that the service terminated
55	Event-Timestamp	Time	Time that the event occurred on the NAS, in seconds, since January 1, 1970 00:00 UTC.
61	NAS-Port-Type	Enumerated data type	Type of physical port that the NAS is using to authenticate the user.
80	Message-Authenticator	String	Authentication checksum

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_IEEE_...

Updated: Wed, 23 Oct 2024 08:19:50 GMT

Copyright © 2024, Versa Networks, Inc.

Value	Attribute Name	Data Type	Description
			of Access-Request packet

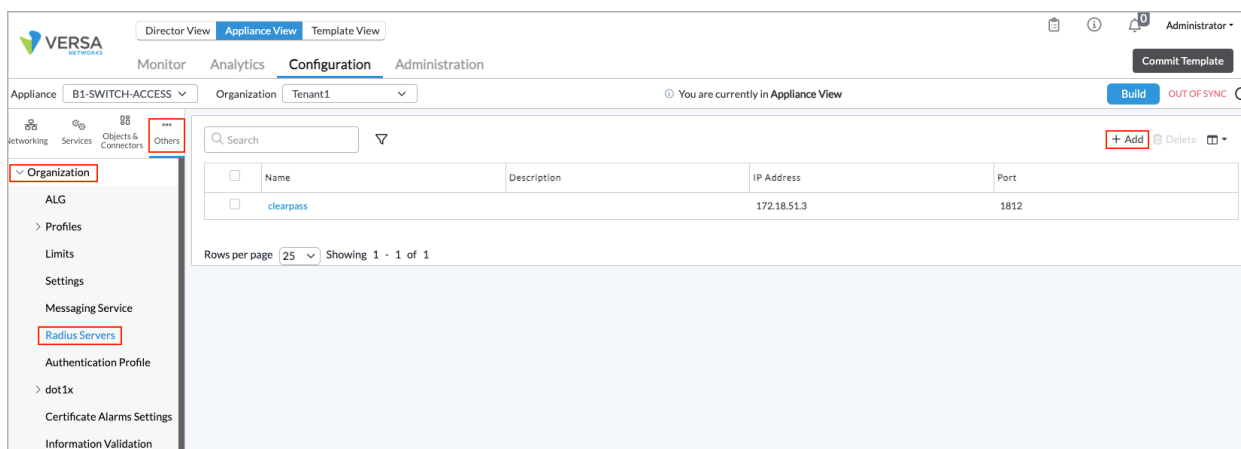
To configure IEEE 802.1X device authentication, you do the following:


- If you are using RADIUS as the 802.1X authentication server, configure the RADIUS server.
- Configure an 802.1X authentication profile for one of the following cases:
 - If you are using external RADIUS authentication, define the information that the authenticator (that is, the authenticating VOS device) uses to communicate with the RADIUS server.
 - If you are using local authentication, define the credentials of the authenticator so that it can communicate with the supplicant.
- To enable authentication on a specific interface, configure the interfaces for 802.1X authentication to control.

Configure a RADIUS Server

If you are using RADIUS as the 802.1X authentication server, configure the RADIUS server:

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 > RADIUS Servers in the left menu bar.



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

Add Radius Server

Name *

Description

IP Address *

Port *

Routing Instance

--Select--

Shared Secret *

OK

Cancel

Field	Description
Name (Required)	Enter the name of the RADIUS server. <i>Value:</i> Text string from 1 through 255 characters long <i>Default:</i> None
Description	Enter a text description for the RADIUS server. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
IP Address (Required)	Enter the IP address of the RADIUS server.
Port (Required)	Enter the number of the listening port on the RADIUS server. For UDP, port 1812 is used. <i>Range:</i> 0 through 65535 <i>Default:</i> None

Field	Description
Routing Instance	Select the routing instance to use to communicate with the RADIUS server.
Shared Secret (Required)	Enter a password that the VOS device uses to access the RADIUS server.


5. Click OK.

Configure an 802.1X Authentication Profile

You can configure an 802.1X authentication profile for one of the following cases:

- If you are using external RADIUS authentication, define the information that the authenticator (that is, the authenticating VOS device) uses to communicate with the RADIUS server.
- If you are using local authentication, define the credentials of the authenticator so that it can communicate with the supplicant.

To configure an 802.1X authentication profile:

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 > Authentication Profile in the left menu bar.
4. Click the  Add icon. In the Add Authentication Profile popup window, enter information for the following fields.

Add Authentication Profile

General

Name *

Type

☒ Local
☐ Radius

Description

Trusted Certificate Database *

Certificate *

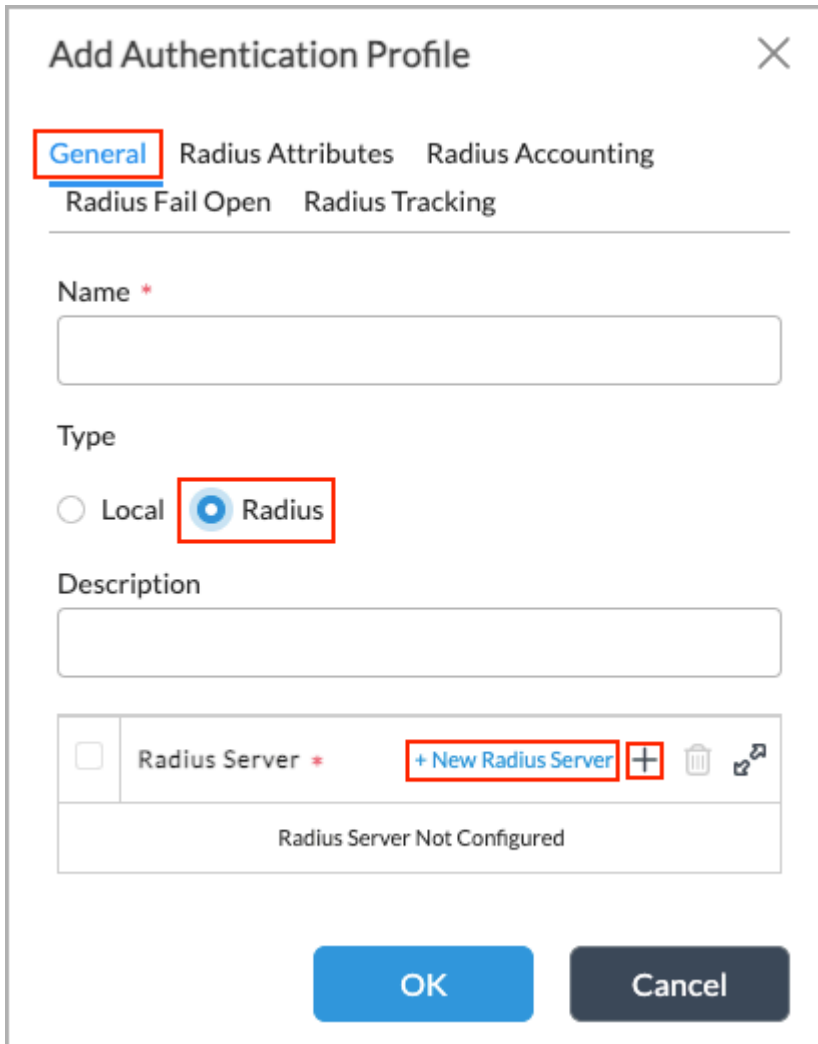
OK
Cancel

Field	Description
Name (Required)	Enter a name for the 802.1X authentication profile <i>Value:</i> Text string from 1 through 255 characters long <i>Default:</i> None
Type	Select the 802.1X authentication type: <ul style="list-style-type: none"> Local—Perform 802.1X authentication on the local VOS device. VOS device must be configured for TLS. RADIUS—Perform 802.1X authentication using a RADIUS server.

Field	Description
Description	Enter a text description of the 802.1X authentication profile. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Trusted Certificate Database	For the Local 802.1X authentication type, select the trusted certificate database
Certificate	For the Local 802.1X authentication type, select the certificate to use for local a

5. If you select RADIUS as the 802.1X authentication type, the Add Authentication Profile popup window displays.

For Releases 22.1.1 and later:



Add Authentication Profile [X]

General Radius Attributes Radius Accounting
Radius Fail Open Radius Tracking

Name *

Type

☐ Local ☒ Radius

Description

☐ Radius Server * + New Radius Server + [trash icon] [share icon]

Radius Server Not Configured

OK Cancel

For Releases 21.2 and earlier:

Add Authentication Profile [X]

General | Radius Attributes

Name*

Type

☐ Local ☒ Radius

Description

Radius Server*

+ New Radius Server

OK Cancel

- a. In the Name field, enter a name for the authentication profile.
- b. Click the Add icon in the RADIUS Server table, and then select the RADIUS server to associate with the authentication profile.
- c. If the server is not listed, click +New RADIUS Server, and then configure a RADIUS server. For redundancy, you can configure multiple RADIUS servers. For more information, see [Configure a RADIUS Server](#), above.
- d. Select the RADIUS Attributes tab to configure the RADIUS attributes to use to communicate AAA information between the authenticator and the RADIUS server. Enter information for the following fields.

For Releases 22.1.1 and later:

Add Authentication Profile

General

Radius Attributes

Radius Accounting

Radius Fail Open

Radius Tracking

NAS Identifier

NAS IP

NAS Port

OK

Cancel

For Releases 21.2 and earlier:

Add Authentication Profile

General

Radius Attributes

NAS Identifier

NAS IP

NAS Port

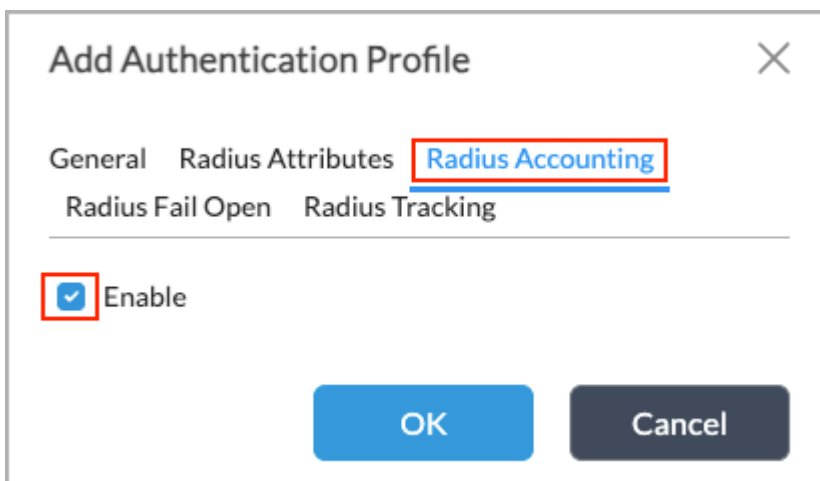
OK

Cancel

Field	Description
NAS Identifier	Enter a text string to identify the network access server (NAS) that originates t

Field	Description
NAS IP	Enter the IP address of the NAS that is requesting authentication. <i>Default: None</i>
NAS Port	Enter the number of the physical port to use to connect to the NAS that is authenticating. Range: 0 through 65535 <i>Default: None</i>

- e. (For Releases 22.1.3 and later.) Select the RADIUS Accounting tab, and then click Enable to enable RADIUS accounting. When you enable IP accounting, the VOS device sends accounting information, including framed IP information, to the RADIUS server.



The screenshot shows a dialog box titled "Add Authentication Profile" with a close button (X) in the top right corner. There are four tabs: "General", "Radius Attributes", "Radius Accounting" (which is selected and highlighted with a red box), and "Radius Fail Open". Below the tabs, there is a section with a checked checkbox (highlighted with a red box) and the label "Enable". At the bottom of the dialog are two buttons: "OK" and "Cancel".

- f. (For Releases 22.1.3 and later.) Select the RADIUS Fail Open tab, and then click Enable to enable RADIUS fail open. RADIUS fail open provides network access to EAPOL and non-EAPOL clients when the RADIUS server is not reachable.

Add Authentication Profile [X]

General Radius Attributes Radius Accounting
Radius Fail Open Radius Tracking

☒ Enable

OK Cancel

- g. (For Releases 22.1.3 and later.) Select the RADIUS Tracking tab, and then click Enable to enable RADIUS tracking. RADIUS tracking tracks the reachability of RADIUS servers to check for further authentication. Once a RADIUS server is reachable, the authentication is retried. Enter how often, in seconds, to send tracking requests. The interval can be from 30 through 300 seconds, and there is no default value.

Add Authentication Profile [X]

General Radius Attributes Radius Accounting
 Radius Fail Open Radius Tracking

Interval (secs)

☒ Enable

OK Cancel

6. Click OK.

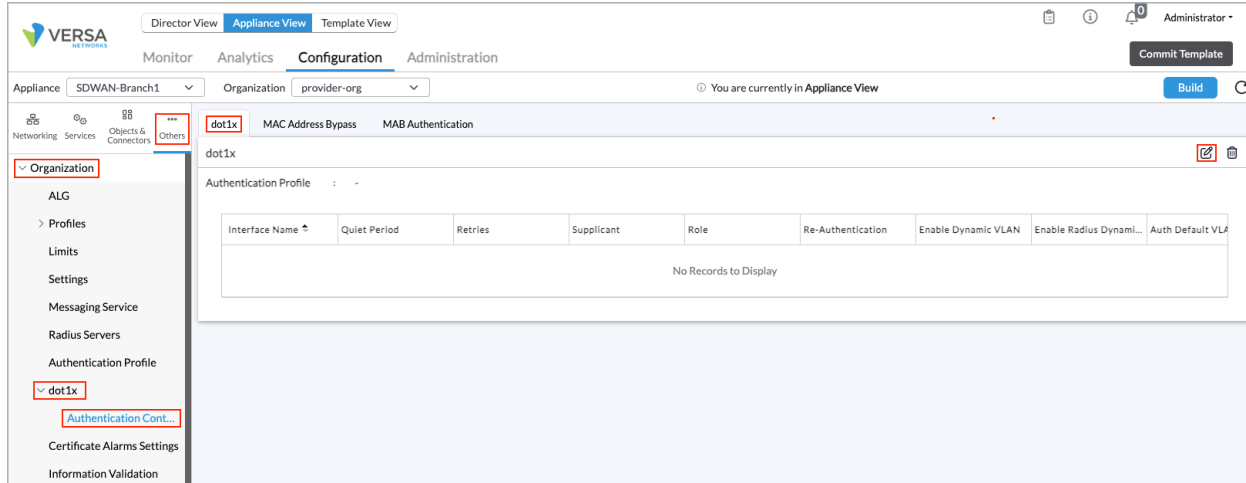
Configure 802.1X Authentication Control

To enable 802.1X authentication on a specific interface, configure the interface for 802.1X authentication to control:

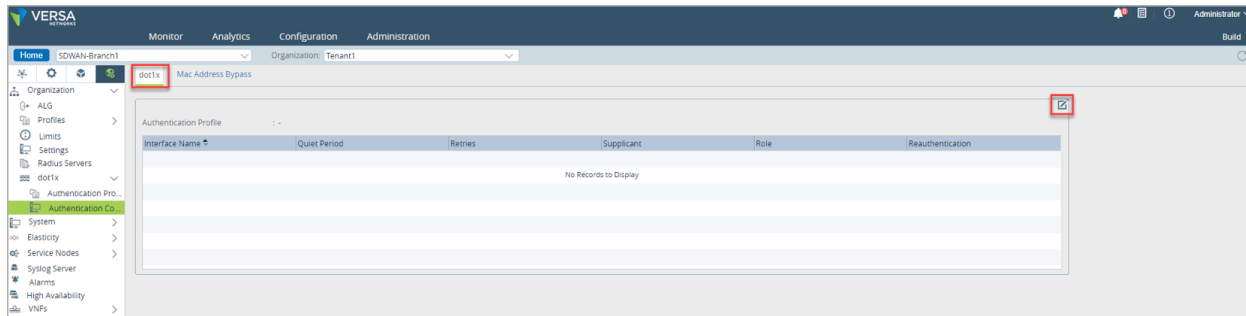
1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select the Appliances in the left menu bar.


- 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.

For Releases 22.1.1 and later:



For Releases 21.2 and earlier:



4. Click the  Edit icon to configure 802.1X on an interface. In the dot1x popup window, enter information for the following fields.

For Releases 22.1.1 and later:

dot1x

Authentication Profile *
--Select--

Interface Name *	Quiet Period	No Re-Authentication	Re-Authentication Interval	Retries	Role	Supplicant
--Select--	60	<input type="checkbox"/>		2	--Select--	--Select--

No Interface Added

OK
Cancel

dot1x

Authentication Profile *
--Select--

	Enable Dynamic VLAN	Enable Radius Dynamic VLAN	Auth Default VLAN ID	Auth Default Voice VLAN	Guest VLAN ID	Enable Multicast Frames	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				<input checked="" type="checkbox"/>	+

No Interface Added

OK
Cancel

For Releases 21.2 and earlier:

dot1x

Authentication Profile *
--Select--

Interface Name *	Quiet Period	No Reauthentication	Reauthentication Interval	Retries	Role	Supplicant
--Select--	60	<input type="checkbox"/>		2	--Select--	--Select--

NO INTERFACE ADDED

OK
Cancel

dot1x

Authentication Profile *


--Select--

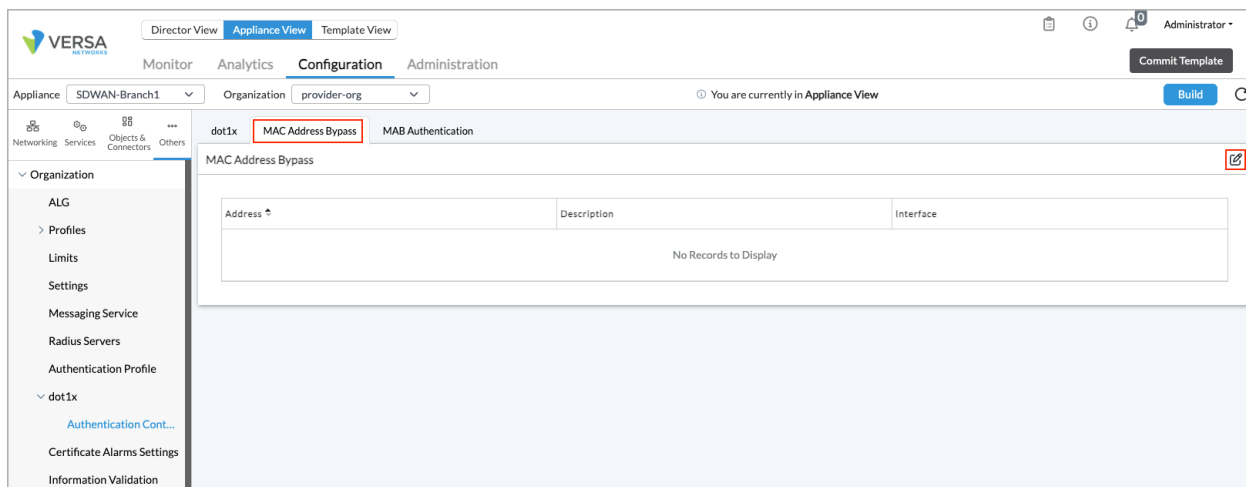
Role	Supplicant	Enable Dynamic VLAN	Enable RADIUS Dynamic ...	Auth Default VLAN ID	Guest VLAN ID
--Select--	--Select--	<input type="checkbox"/>	<input type="checkbox"/>		

OK
Cancel

Field	Description
Authentication Profile (Required)	Select the name of the 802.1X authentication profile. This is a profile that you can create in the Profile , above.
Interface Name (Required)	Select the interface on which to configure 802.1X authentication.
Quiet Period	Enter how long the interface waits after a failed authentication attempt before it can accept another attempt. <i>Range:</i> 0 through 600 seconds <i>Default:</i> None
No Reauthentication	Click to disable periodic reauthentication of users.
Reauthentication Interval	Enter the interval at which to reauthenticate the user. By default, a user is reauthenticated every 300 seconds. <i>Range:</i> 10 through 86400 seconds <i>Default:</i> None
Retries	Enter how many times to try to authenticate the port after an initial failure. The retries occur during the quiet period after the authentication attempt. <i>Range:</i> 1 through 10 <i>Default:</i> 2
Roles	Select the interface role:

Field	Description
	<ul style="list-style-type: none"> ◦ Authenticator—Interface acts as the authenticator. ◦ Supplicant—Interface acts as a supplicant. <p><i>Default: None</i></p>
Supplicant	<p>Select the type of supplicant:</p> <ul style="list-style-type: none"> ◦ Single—Authenticate only the first end device. All other end devices th without any further authentication. The subsequent devices effectively ◦ Single-secure—Allow only one end device to connect to the port at a ti device logs out. ◦ Multiple—Allow multiple end devices to connect to the port. Each end <p><i>Default: None</i></p>
Enable Dynamic VLAN	Click to enable dynamic VLANs.
Enable RADIUS Dynamic VLAN	Click to enable RADIUS dynamic VLANs.
Authentication Default VLAN ID	Enter the ID of the default VLAN to use for authentication.
Authentication Default Voice VLAN	(For Releases 22.1.3 and later.) Enter the ID of the default voice VLAN to u
Guest VLAN ID	Enter the ID of the guest VLAN.
Enable Multicast Frames	(For Releases 22.1.3 and later.) Click to enable multicast frames.


- Click the  Add icon to add the profile.
- Select the MAC Address Bypass tab in the horizontal menu bar,



https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_IEEE_...




Updated: Wed, 23 Oct 2024 08:19:50 GMT

Copyright © 2024, Versa Networks, Inc.

7. Click the  Edit icon to configure a list of MAC address bypasses on an interface. These are MAC addresses that do not need to be authenticated. Enter information for the following fields.

MAC Address Bypass

< >

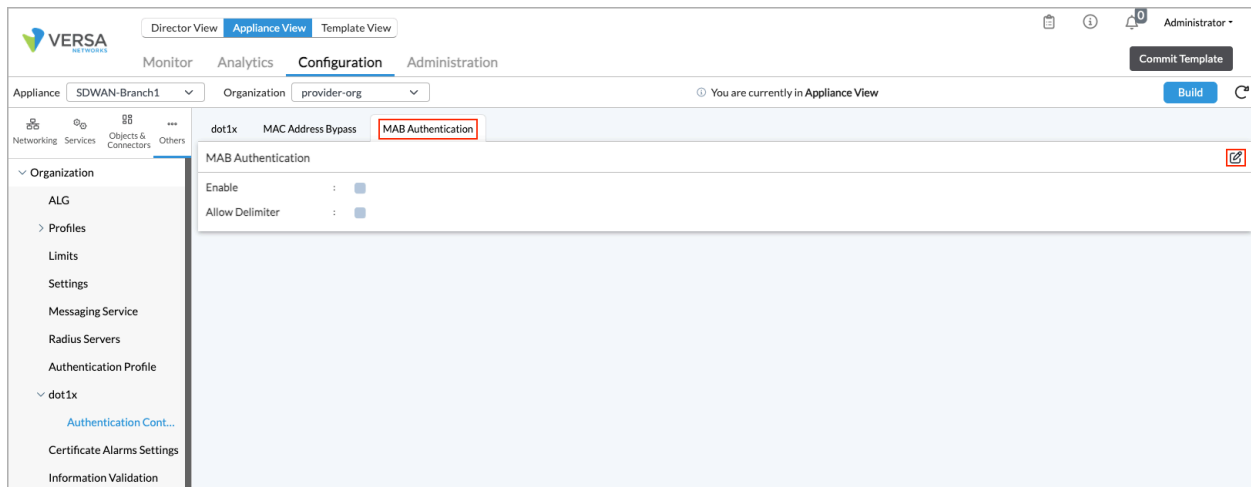
Address * 	Description	Interface Name	
<input type="text"/>	<input type="text"/>	--Select-- 	
No MAC Address Added			


OK

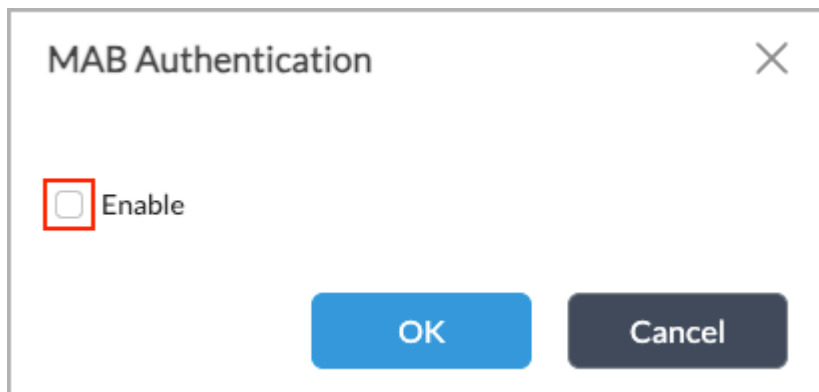
Cancel

Field	Description
Address	Enter the MAC address of the device that is allowed to bypass the 802.1X
Description	Enter a text description of the MAC address. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Interface Name	Select the interface that the MAC address is allowed to connect to without

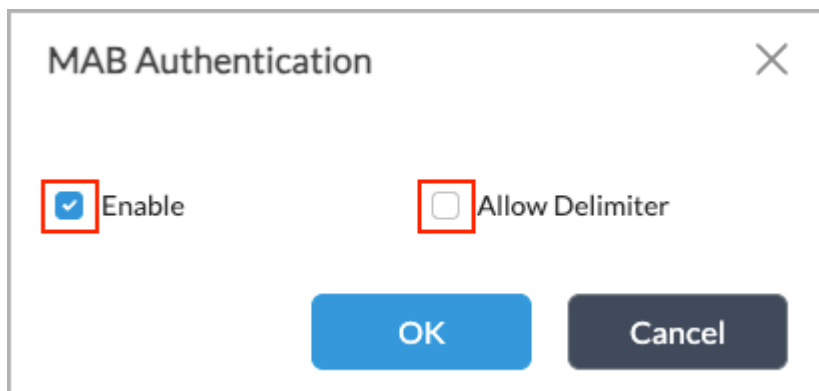
8. (For Releases 22.1.3 and later.) Select the MAB Authentication tab in the horizontal menu bar. Note that before you enable MAB authentication, you must configure the interface to be in trunk mode. For more information, see [Configure Trunk Interfaces](#).



9. Click the  Edit icon. The MAB Authentication popup window displays.



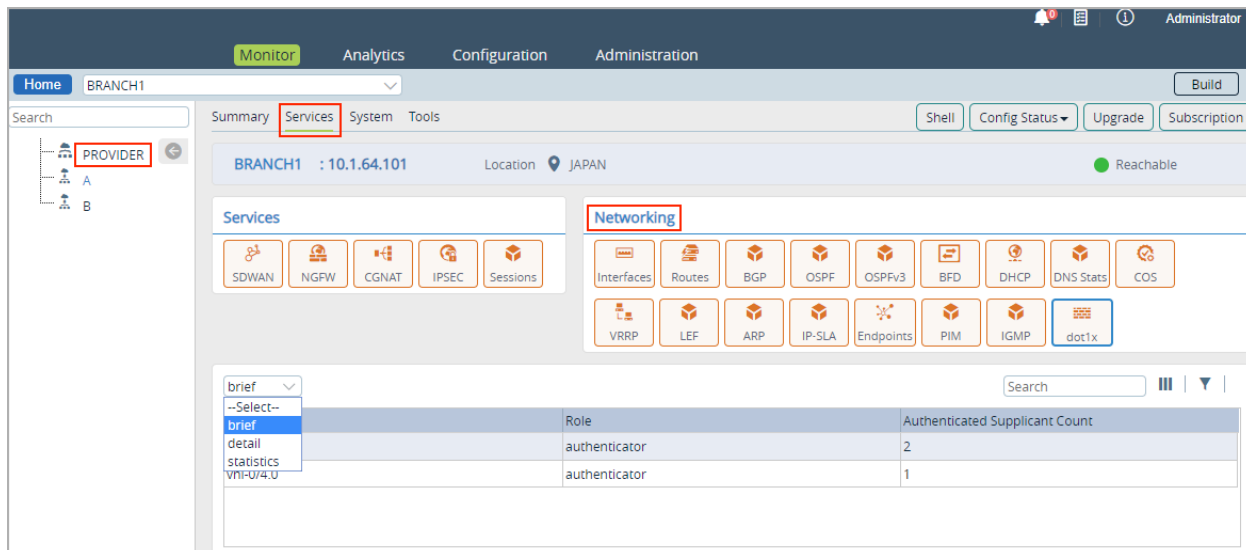
10. Click Enable to enable MAB authentication.



11. Click Allow Delimiter to send the MAC addresses with the colon (:) delimiter.
12. Click OK.

Verify 802.1x Authentication Information

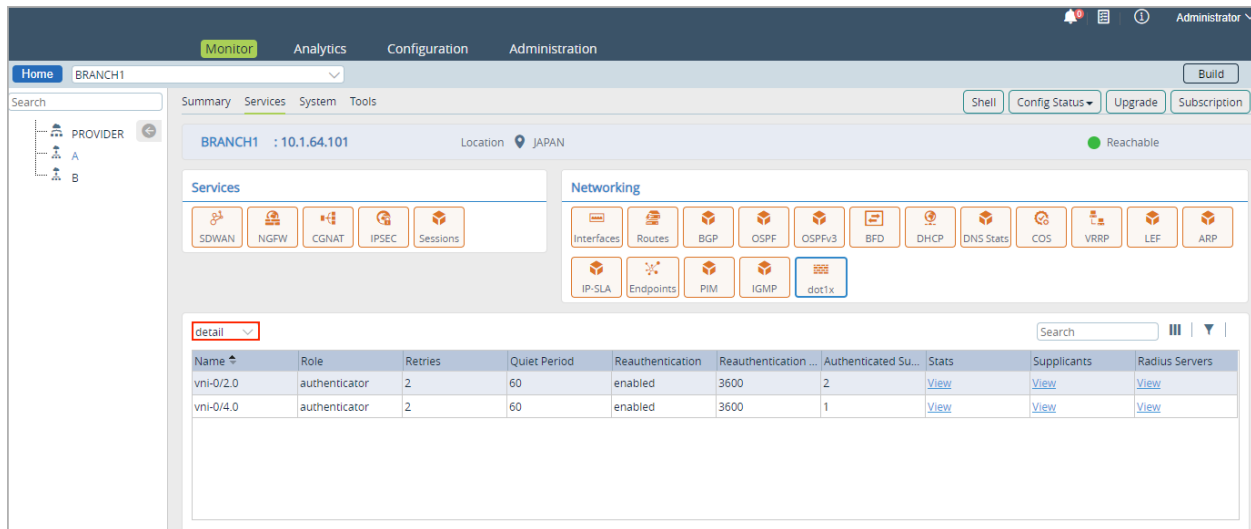
1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select the Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select an organization in the left menu, and then select the Services tab in the horizontal menu.
4. Select dot1x in the Networking section to view the interface details and other statistics. In the drop-down menu, select the level of detail to view.
5. Select Brief to view the interface roles as authenticator or supplicant. This view shows the authenticated supplicant count if the interface role is authenticator, and it shows the authentication state of the interface that is configured as a supplicant.



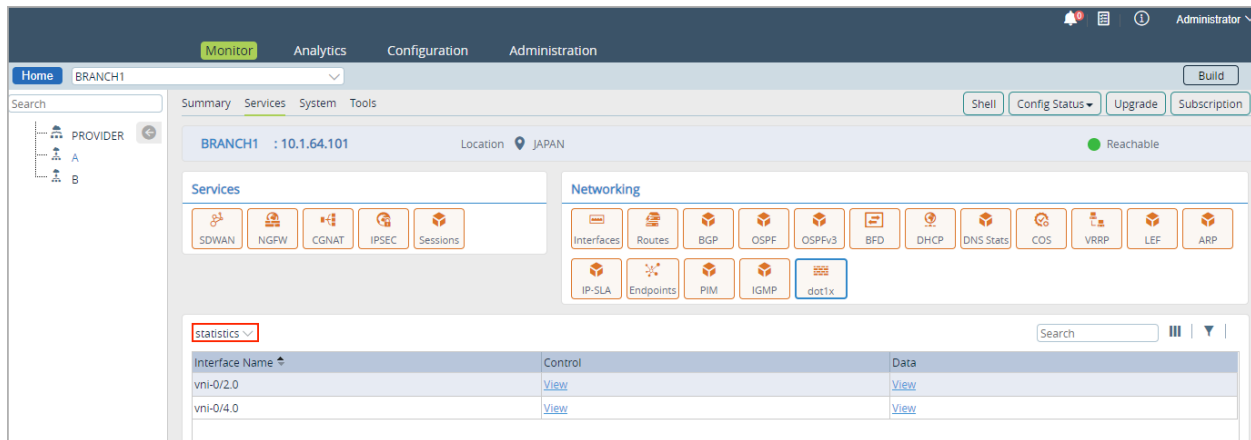
The screenshot shows the Versa Director interface. The top menu bar includes Monitor, Analytics, Configuration, and Administration. The left sidebar shows a tree view with PROVIDER, A, and B. The main panel displays the configuration for BRANCH1 (10.1.64.101) in JAPAN. The Services section is selected, and the Networking section is expanded. The dot1x configuration is visible, showing two interfaces: one configured as an authenticator with 2 authenticated supplicants, and another configured as an authenticator with 1 authenticated supplicant.

Role	Authenticated Supplicant Count
authenticator	2
authenticator	1

6. Select Detail to view details about the authenticator and supplicant for each interface, including configuration parameters, and authentication and EAP packet statistics. The Detail screen also provides information about the connected supplicant state for the interface that is configured as the authenticator.



7. Select Statistics to view per-interface packet statistics.



Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 22.1.3 supports MAB authentication bypass, RADIUS accounting, RADIUS failover, and RADIUS tracking.

Additional Information

[Configure Dynamic VLANs Using 802.1X Authentication Flows](#)

[Configure Layer 2 Forwarding](#)