

---

## Configure AAA

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

This article describes how to configure authentication, authorization, and accounting (AAA) for users who access Versa Operating System™ (VOS™) devices.

Authentication identifies users to determine whether they are allowed to access a VOS device, the network, and related services. To authenticate a user, you can use an internal or an external user database. The external database can be on a RADIUS or TACACS+ server.

After a user is authenticated on a VOS device, each user action that they perform must be authorized. Authorization is the method for remote access control, including one-time authorization and service authorization based on user or user account and profile. The VOS software provisions three user types, or roles—System, Tenant, and Remote—that determine the access level for individual users. When you create a user, you assign them to the desired role.

Authorization uses a database to define the authorization methods. The database can be located locally on the access server or on a router, or it can be hosted remotely on a RADIUS or TACACS+ server. The authorization process assembles a set of attributes that describe what the user is authorized to perform, compares them to the information in the authorization database, and then returns to AAA the user's permissions and restrictions.

Accounting collects and sends security server information that is used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. The accounting information allows you to track the services that users are accessing and the amount of network resources they are consuming.

---

## Configure TACACS+

TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes.

To configure TACACS+:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select an organization in the Organization field in the horizontal menu bar.
3. Select Template > Templates in the horizontal menu bar.
4. Select SD-WAN in the horizontal menu bar.

- Click **+Add** to add a new template, or click the edit icon in the Actions column to edit an existing template. The **Configure Basic** screen displays.

**Configure Basic**

Template: Branch-5-hub-template

**Basic**

Name \*  
Branch-5-hub-template

Template Type  
SDWAN Post Staging

**Device Type**

Name  
SDWAN

☐ Full Mesh ☒ Hub ☐ Hub Controller ☐ Spoke

Region  
---Please Select---

**Subscription**

Solution Tier \*  
Premier-Secure-SDWAN

Service Bandwidth \*  
1 Gbps

License Year \*  
1 Years

Solution Add on Tier \*  
---Please Select---

No Records to Display

[Cancel](#) [Back](#) [Save](#) [Skip To Review](#) [Next](#)

- For Releases 21.2 and earlier, in Director view, select the **Workflows** tab in the top menu bar, select **Templates** in the left menu bar., and then click the **+ Add** icon to add a template, or select a template to edit it.

Name	Status
<a href="#">Hub-Template</a>	Saved
<a href="#">PoststagingTemplate1</a>	Saved
<a href="#">PoststagingTemplate2</a>	Saved
<a href="#">PoststagingTemplate3</a>	Deployed
<a href="#">Redundant1-Template</a>	Saved
<a href="#">SpokeToHubTemplate</a>	Deployed
<a href="#">SpokeToSpokeDirectTemplate</a>	Deployed

- Select the **Management Servers** tab, and then select the **TACACS+ Servers** tab.

Director View

Appliance View

Template View

1

Administrator

Monitor

Configuration

Workflows

Administration

Analytics

Commit Template

Organization

provider-org

You are currently in Director View

Workflows > Template > Templates

Infrastructure

Template

Devices

1

2

3

4

5

6

7

BASIC

INTERFACES

TUNNELS

ROUTING

INBOUND NAT

MANAGEMENT SERVERS

REVIEW

Configure Management Servers

Management Servers

Template: Branch-5-hub-template

NTP Servers(0)

Syslog Servers(0)

TACACS+ Servers(0)

RADIUS Servers(0)

SNMP Managers(0)

LDAP Servers(0)

Reachability via	IP Address	Authentication Key	Actions
<div>---Please Select---</div>	<input type="text"/>	<input type="text"/>	<div>authentication</div>
No Records to Display			

Cancel

Back

Save

Skip To Review

Next

For Releases 21.2 and earlier:

Create Template - Hub-Template

Basic Interfaces Routing Split Tunnels Inbound NAT Services Management Servers

**NTP Servers**

Reachability via \* IP Address \*

--Select-- 1.1.1.1

WAN1

**Syslog Servers**

Reachability via \* IP Address \*

--Select--

NO RECORDS ADDED

**AAA Servers**

☒ TACACS+ Servers ☐ RADIUS Servers

Reachability via \* IP Address \* Authentication Key \*

--Select-- 2.2.2.2 242525

WAN1

**SNMP Managers**

Versions ☐ v1 ☐ v2c ☐ v3

Community

Reachability via \* IP Address \*

--Select--

NO RECORDS ADDED

Back Cancel Save Create

8. Enter information for the following fields.

Field	Description
Reachability via	Select the reachability network between the Controller and TACACS+ server.
IP Address	Enter the IP address of the server to which to connect.
Authentication Key	Enter the authentication key. The key can consist of both numbers and letters, and it cannot include a hash mark (#) or spaces.
Actions	<p>(For Releases 22.1 and later.) Select the TACACS+ action:</p> <ul style="list-style-type: none"> <li>Accounting</li> <li>Authentication</li> </ul>

9. Click Save.

# Configure RADIUS

RADIUS is a distributed client-server system that secures networks against unauthorized access.

To configure RADIUS:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select an organization in the Organization field in the horizontal menu bar.
3. Select Template > Templates in the horizontal menu bar.
4. Select SD-WAN in the horizontal menu bar.
5. Click +Add to add a new template, or click the edit icon in the Actions column to edit an existing template. The Configure Basic screen displays.

The screenshot shows the Versa Networks Director interface. At the top, there's a navigation bar with 'Director View', 'Appliance View', and 'Template View' tabs. Below this is a horizontal menu bar with 'Monitor', 'Configuration', 'Workflows' (selected), 'Administration', and 'Analytics'. A 'Commit Template' button is on the right. The main area shows a breadcrumb trail: 'Workflows > Template > Templates'. Below this is a 'Configure Basic' section with a progress bar showing steps 1 through 7: BASIC, INTERFACES, TUNNELS, ROUTING, INBOUND NAT, MANAGEMENT SERVERS, and REVIEW. The 'BASIC' step is currently active. The 'Basic' configuration form includes a 'Name' field with 'Branch-5-hub-template', a 'Template Type' dropdown with 'SDWAN Post Staging', a 'Device Type' section with 'SDWAN' selected, and a 'Subscription' section with 'Premier-Secure-SDWAN', '1 Gbps', and '1 Years' selected. A 'Solution Add on Tier' dropdown is also present. At the bottom, there are buttons for 'Cancel', 'Back', 'Save', 'Skip To Review', and 'Next'.

6. For Releases 21.2 and earlier, in Director view, select the Workflows tab in the top menu bar, select Templates in the left menu bar., and then click the Add icon to add a template, or select a template to edit it.

Monitor
Configuration
Workflows
Administration
Analytics

SDWAN
Infrastructure
Template
Templates
Application Templ...
Spoke Groups
Service Chains
Devices

Search

	Name	Status
<input type="checkbox"/>	<a href="#">Hub-Template</a>	Saved
<input type="checkbox"/>	<a href="#">PoststagingTemplate1</a>	Saved
<input type="checkbox"/>	<a href="#">PoststagingTemplate2</a>	Saved
<input type="checkbox"/>	<a href="#">PoststagingTemplate3</a>	Deployed
<input type="checkbox"/>	<a href="#">Redundant1-Template</a>	Saved
<input type="checkbox"/>	<a href="#">SpokeToHubTemplate</a>	Deployed
<input type="checkbox"/>	<a href="#">SpokeToSpokeDirectTemplate</a>	Deployed

7. Select the Management Servers tab, and then select the RADIUS Servers tab.

VERSA NETWORKS
Director View
Appliance View
Template View

Monitor
Configuration
Workflows
Administration
Analytics

Organization: provider-org
You are currently in Director View
Workflows > Template > Templates

Infrastructure
Template
Devices

1 BASIC
2 INTERFACES
3 TUNNELS
4 ROUTING
5 INBOUND NAT
6 MANAGEMENT SERVERS
7 REVIEW

Configure Management Servers

Management Servers
Template: Branch-5-hub-template

NTP Servers(0)
Syslog Servers(0)
TACACS+ Servers(0)
RADIUS Servers(0)
SNMP Managers(0)
LDAP Servers(0)

Reachability via *	IP Address *	Authentication Key *	Actions *
---Please Select---			Select Option

No Records to Display

Cancel
Back
Save
Skip To Review
Next

For Releases 21.2 and earlier:

Create Template - Hub-Template

Basic Interfaces Routing Split Tunnels Inbound NAT Services Management Servers

**NTP Servers**

Reachability via \* IP Address \*

--Select-- 1.1.1.1 +

WAN1

**Syslog Servers**

Reachability via \* IP Address \*

--Select-- +

NO RECORDS ADDED

**AAA Servers**

☒ TACACS+ Servers ☐ RADIUS Servers

Reachability via \* IP Address \* Authentication Key \*

--Select-- 2.2.2.2 242525 +

WAN1

**SNMP Managers**

Versions ☒ v1 ☐ v2c ☐ v3

Community

Reachability via \* IP Address \*

--Select-- +

NO RECORDS ADDED

Back Cancel Save Create

8. In the Create Template popup window, select the Management Servers tab. Enter information for the following fields.

Field	Description
Reachability via	Select the reachability network between the controller and the RADIUS server.
IP Address	IP address of the server to connect to.
Authentication Key	Enter the authentication key. The key can consist of both numbers and letters, and it cannot include a hash mark (#) or spaces.
Actions	<p>(For Releases 22.1 and later.) Select the TACACS+ action:</p> <ul style="list-style-type: none"> <li>Accounting</li> <li>Authentication</li> </ul>

9. Click Save.

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_AAA](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_AAA)

Updated: Wed, 23 Oct 2024 08:20:28 GMT

Copyright © 2024, Versa Networks, Inc.

---

## Configure Local Authentication

VOS devices support the following users:

- Default users
- System users
- Organization users

Default users are system users created by default and cannot be deleted. VOS devices have the following default users:

- admin—Superuser with sudo privileges. An admin user can SSH to the VOS device using port 22.
- versa—Console user. These users can log in to the physical device or through a virtual console.

The default password for the admin and versa users is versa123. Password-less authentication can be set for admin via SSH public keys.

System users can log in to the VOS underlying operating system. The user is created in Linux when a system user is configured. System users can have the following roles:

- Admin—Can modify any part of the configuration.
- Operator—Can only view the configuration.

System users can have the following login types:

- Shell—Land at bash post-authentication prompt
- CLI—Land on at CLI prompt post-authentication prompt

Organization users can log in only to the VOS CLI. Organization users can SSH only to port 2024. SSH to port 22 is prohibited for all Organization users. Currently, VOS devices support password-less authentication for organization users.

The following predefined RBAC roles are available for organization users:

User	Description
adc-admin	Can view/modify ADC specific configuration only.
cgnat-admin	Can view/modify CGNAT specific configuration only.
sdwan-admin	Can view/modify configuration related to SDWAN.
security-admin	Can view/modify security configuration only.
tenant-admin	Can view/modify all tenant configuration.
oper	Can view all tenant configuration. No modification allowed.

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_AAA](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_AAA)

Updated: Wed, 23 Oct 2024 08:20:28 GMT



Copyright © 2024, Versa Networks, Inc.



To create unique Org usernames in the system, when an Organization user is created, the VOS device appends @Orgname to the username. For example, if the username is john@kayak, the user must SSH as ssh'john@kayak'@77.1.1.1 OR ssh77.1.1.1 -l john@kayak.

VOS devices also support password-less authentication for system users using SSH public key. This provides enhanced security and the system is then protected against SSH brute force password attacks. Multiple SSH keys can be configured for a system user.

## Add System Users


1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the left menu bar.
  - c. Select an organization in the left menu bar.
  - d. 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  > System > Appliance User Management > System Users in the left menu bar
4. Click the  Add icon. In the Add System User popup window, enter information for the following fields.

### Add System User



Username *	Login *	Role *
<input type="text"/>	--Select--	--Select--
Password *	Confirm Password *	
<input type="password"/>	<input type="password"/>	

#### SSH Public Key

Name *	Contents *	
<input type="text"/>	<input type="text"/>	
No Records to Display		


OK Cancel

Field	Description
Username	Enter the username.
Login	Select the login method: <ul style="list-style-type: none"> <li>◦ CLI</li> <li>◦ No Login</li> <li>◦ Shell</li> </ul>
Role	Select the user's role: <ul style="list-style-type: none"> <li>◦ Admin</li> <li>◦ Operator</li> </ul>
Password	Enter a password for the user.
Confirm Password	Confirm the password.
SSH	Enter the SSH details, if required.

5. Click OK.

---

## Add Organization Users

- In Director view:
  - Select the Configuration tab in the top menu bar.
  - Select Devices > Devices in the left menu bar.
  - Select an organization in the left menu bar.
  - Select a device in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Others  > System > Appliance User Management > Organization User in the left menu bar.

Director View **Appliance View** Template View

Administrator 4

Monitor Analytics **Configuration** Administration

Appliance SDWAN-Branch1 Organization provider-org You are currently in Appliance View Build

Commit Template

Networking Services Objects & Connectors Others

Search

Organization

System

Configuration

Speed Test

Domain Name Servers

Security Package Updates

Time & Date

Storage Configurations

Appliance User Manageme...

System Users

External AAA

Organization Users


Organization Groups

Search

+ Add Delete

	Username	Role
No Organization User Added		

Add

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

### Add Organization User ×

Username \* Role \*

--Select--

Password \* Confirm Password \*

OK Cancel

Field	Description
Username	Enter the username.
Role	Select the role to be assigned to the user.
Password	Enter a password for the user.
Confirm Password	Confirm the password.

5. Click OK.

---

## Configure AV Pairs for RADIUS and TACACS+

For RADIUS and TACACS+, VOS devices support the following attribute–value (AV) pairs:

- versa-user-group
- versa-admin-login
- versa-cli-idle-timeout

The versa-user-group AV defines the user role that can be assigned to the remote AAA user. The following are the commonly used roles:

- admin—Provides read and write permissions on the device to the user system administrator
- oper—Provides read-only permission to the user system operator

For the versa-user-group AV, VOS devices support the following other roles at the tenant level:

- *tenant-name-adc-admin-group*
- *tenant-name-cgnat-admin-group*
- *tenant-name-network-admin-group*
- *tenant-name-oper-admin-group*
- *tenant-name-sdwan-admin-group*
- *tenant-name-security-admin-group*
- *tenant-name-tenant-admin-group*

The versa-admin-login AV allows users assigned to the admin group to access a shell or the CLI. This AV allows a remote administrator to land on a shell or the CLI.

The versa-cli-idle-timeout AV sets the idle timeout for a user who has logged in.

For RADIUS and TACACS+, you must define a service name that is used by the user named “versa.” For example:

```
group = network_oper {
```

```

default service = permit
expires = "Jan 1 2025"
service = versa
{
    versa-user-group = oper
}
}

```

## Configure AV Pairs for RADIUS

For RADIUS, you configure AV pairs on the RADIUS server. In this section, we show example configurations on a FreeRADIUS server that is running on a Linux platform. Here, you configure entries in the `dictionary.versanetworks`, `/etc/freeradius/client.conf`, and `/etc/freeradius/users` files on the RADIUS server.

To define the attributes, ensure that the `dictionary.versanetworks` file contains the following entries:

```

VENDOR      VersaNetworks      42359
BEGIN-VENDOR VersaNetworks
ATTRIBUTE    Versa-User-Group 1 string
ATTRIBUTE    Versa-Acct-Command 2 string
ATTRIBUTE    Versa-User-Role 3 string
ATTRIBUTE    Versa-Tenant 4 string
ATTRIBUTE    Versa-Admin-Login 5 string
END-VENDOR   VersaNetworks

```

To allow clients from specific networks, add entries similar to the following in the `/etc/freeradius/client.conf` file:

```

client 172.18.0.0/24 {
    secret = "versa1234"
    shortname = network-1
}
client 192.168.0.0/16 {
    secret = "versa123456"
    shortname = network-2
}

```

To configure the RADIUS users, add entries similar to the following in the `/etc/freeradius/users` file:

```

User1 Cleartext-Password := "versa123"
    Reply-Message = "Hello, %{User-Name}",
    Versa-User-Group = "oper"
User2 Cleartext-Password := "versa123"
    Reply-Message = "Hello admin, %{User-Name}",
    Versa-User-Group = admin
User3 Cleartext-Password := "versa1234"
    Versa-User-Group = "admin",
    Versa-Admin-Login = "shell",
    Reply-Message = "Hello Ella, %{User-Name}"

```

---

## Configure AV Pairs for TACACS+

For TACACS+, you configure AV pairs on the TACACS+ server. In this section, we show example configurations for `tac_plus` that is being used as a TACACS+ process (daemon) on a Linux platform. Here, you edit the `/etc/tacacs/tacacs.conf` configuration file on the TACACS+ server, adding entries similar to the following:

```
# commands authorization, scripting authorization.
# See the man page for these features.
key = "versa1234"
accounting syslog;
accounting file = /var/log/tac_plus/tac_plus.acct
group = network_admin {
    default service = permit
    expires = "Jan 1 2025"
    service = versa {
        versa-user-group = admin
        versa-admin-login = shell
    }
}
group = network_oper {
    default service = permit
    expires = "Jan 1 2025"
    service = versa {
        versa-user-group = oper
    }
}
group = tenant1_admin {
    default service = permit
    expires = "Jan 1 2025"
    service = versa {
        versa-user-group = Tenant1-tenant-admin-group
        Versa-cli-idle-timeout = 10
    }
}
user = test-user {
    member = network_admin
    login = cleartext "password1234"
    enable = cleartext "password1234"
    global = cleartext "password1234"
}
user = test-user2 {
    member = network_oper
    login = cleartext "password1234"
    enable = cleartext "password1234"
    global = cleartext "password1234"
}
```

---

## Disable External Authentication


To disable TACACS+ and other external authentication:

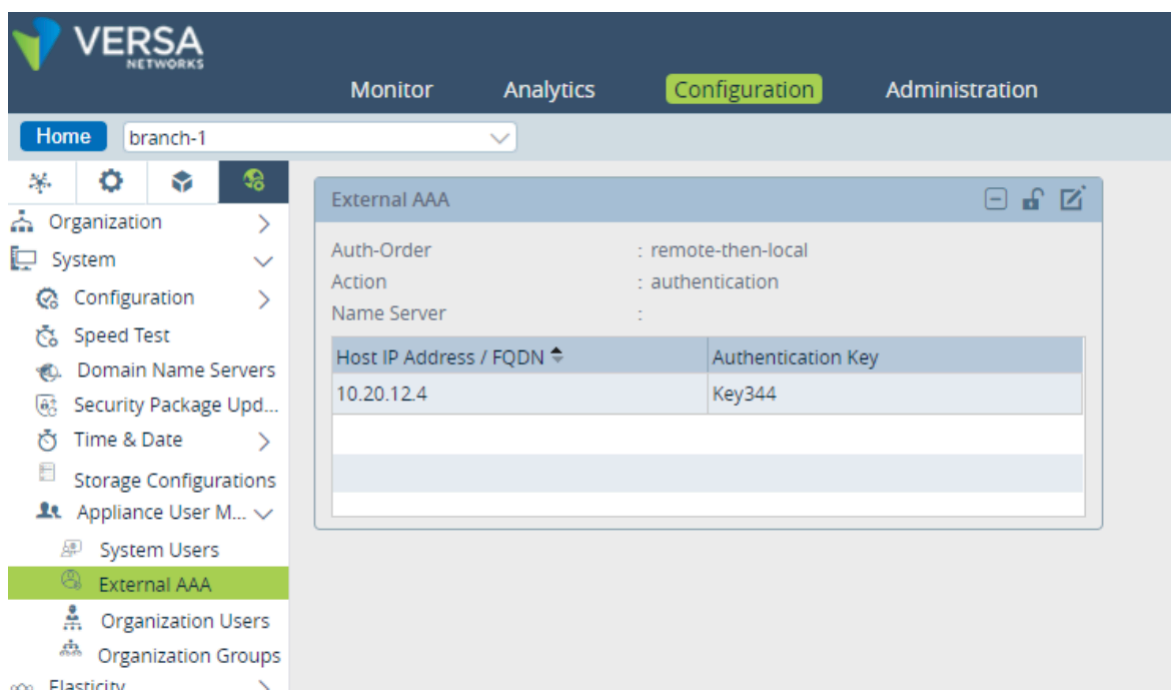
---


[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_AAA](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_AAA)

Updated: Wed, 23 Oct 2024 08:20:28 GMT

Copyright © 2024, Versa Networks, Inc.

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the left menu bar.
  - c. Select an organization in the left menu bar.
  - d. 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  > System > Appliance User Management > External in the left menu bar.



4. In the External AAA pane, select the external authentication device.
5. Click the  icon.

## Supported Software Information

Releases 20.2 and later support all content described in this article.

## Additional Information

[Configure AAA](#) (on Director nodes)

[Create and Manage Staging and Post-Staging Templates](#)

[Configure Single Sign-On Using Director](#)

[Configure TACACS+](#) (on Analytics nodes)