

---

## Configure Versa Messaging Service

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

Versa Messaging Service (VMS) is a scalable, high-performance messaging service for streaming dynamically changing, high frequency, low latency data between Versa products (for example, Versa Operating System, Versa Director, Versa Controller, Versa Concerto, Versa Analytics) as well as between third-party sources (for example, Microsoft Active Directory, Palo Alto Panorama, and OAM systems) and Versa products.

VMS uses a Kubernetes architecture to deliver scalable, reliable applications. It delivers real-time messages from multiple external sources to VOS devices and to other Versa services and platforms.

You can enable the following services for each VMS node:

- Third-party authorization—Verify user identity without requiring any authentication action. Secure SD-WAN CPE devices use VMS for third-party authentication, eliminating the need for users to authenticate themselves through a captive portal.
- XIP EIP—Converts Palo Alto Networks host information profile (HIP) reports into the VOS endpoint information profile (EIP) report format. You can configure VOS gateways to subscribe to XIP EIP, and you can then use these reports to enforce security policies.
- SASE-on-SIM or SASE for SIM—Allows organizations to deploy SASE in a flexible manner, requiring minimal infrastructure changes. It seamlessly integrates into the existing networks of mobile network operators (MNOs) by adding a SASE domain.

This article describes how VMS interfaces with the Versa headend components, describes the requirements for deploying VMS, and describes how to configure Versa Director so that VMS can communicate with Versa headend components and with external components.

---

## VMS and Versa Headend Components

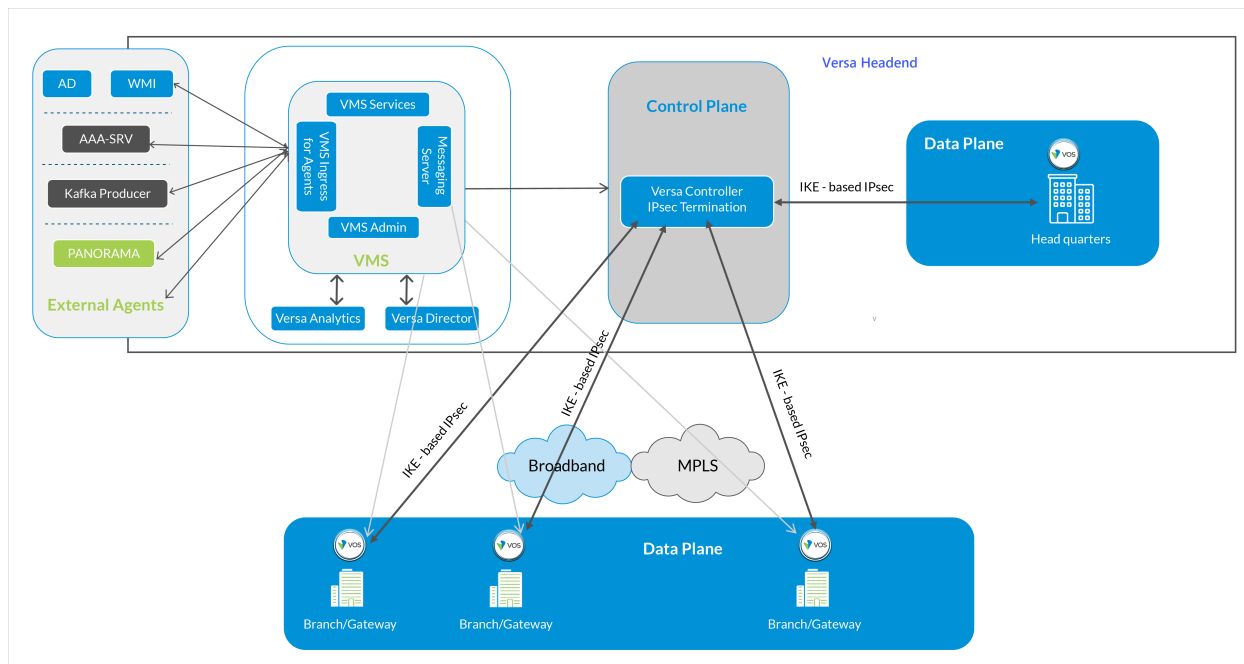
You can configure VMS with the following Versa headend components:

- Versa Director or Concerto—From Versa Director or Concerto, you configure user, tenant, and group orchestration.
- Versa Controller—You configure a Versa Controller to connect to VOS devices over IPsec tunnels, and you create an application delivery controller (ADC) to connect to Versa Analytics.
- Versa Analytics nodes—You configure these for logging and analytics services.

VMS can interact with the following components:

- Versa headend—VMS connects with other Versa headend components through the management plane. Over the management plane, VMS receives the configurations for tenants and services, and the configurations for connecting to and communicating with other Versa headend components through Versa Director. To configure communication between VMS and Versa Director, you configure a VMS cluster in the Director connector to establish communication between VMS and the Director node.
- External sources and agents—The VMS elastic interface interacts with external sources and agents, including AAA servers, Kafka, Panorama, and the Versa WMI agent for Active Directory (AD), to receive data.
- VOS devices—VOS devices establish long-term communication with VMS to send and receive streamed data. It is recommended that you stream logs from VOS devices to VMS using SD-WAN.

VMS is a component of the Versa headend, as shown in the following figure.



The figure above illustrates the following workflow in VMS:

- Each VOS device subscribes to VMS for a service (for example, SASE for SIM, third-party authentication, or XIP EIP), and sends and receives streaming data.
- External components and agents send data or stream logs to VMS.
- VMS processes the streamed data from external sources, converts it to a format for VOS devices, and streams it to the VOS devices that subscribe to a service.
- VMS streams data to subscribed VOS devices and forwards logs and exceptions to Versa Analytics nodes. VMS can also send data or logs to external components.

To configure VMS for Concerto or Director, you do the following:

- Configure a VMS connector on a Director node. For more information, see [Configure VMS from Versa Director](#) below.
- Perform tenant onboarding related to VMS from Concerto.
- Configure users and user groups for tenants on Concerto or Director nodes. These configurations then share group,

[https://docs.versa-networks.com/Management\\_and\\_Orchestration/Versa\\_Messaging\\_Service/Passive\\_Authentication/01\\_Co...](https://docs.versa-networks.com/Management_and_Orchestration/Versa_Messaging_Service/Passive_Authentication/01_Co...)

Updated: Wed, 23 Oct 2024 08:49:43 GMT

Copyright © 2024, Versa Networks, Inc.

tenant, IMSI (user ID), and solution tier information with VMS.

You configure VMS for Versa Analytics for logs related to entitlement, debugging, and exceptions. Versa Analytics analyzes these logs and events, and generates reports and analytics for events shared by VMS. The following are the types of VMS events:

- Activities—Start–stop events for each IMSI-to-IP address combination
- Exceptions—Errors that occur during data processing for orchestration, accounting, and Kafka

VMS uses a Versa Controller node to connect to a VOS device over an IPsec tunnel and to configure an application delivery controller (ADC) for Analytics. ADC is a component of a VOS device that accepts TCP or UDP connections from a process that initiates a connection. For more information, see [Application Delivery Controllers](#).

---

## VMS Deployment Overview

To deploy VMS, you install it as a node in the control plane. A control plane node is the initial node in a VMS cluster, and it controls the functioning of the VMS cluster and is the initial node in the VMS cluster. You perform the initial VMS configuration on this node, and in the process of configuring VMS< you set up the VMS cluster. The control plane node manages the VMS administration and configuration database, and it sets up the control plane and the software required for VMS deployment. The control plane node also monitor sand maintains the health of the VMS cluster.

This section describes the hardware and interface requirements to deploy a VMS node.

It is recommended that you deploy VMS on physical servers. The following table provides the minimum requirements for a VMS node.

Node Type	Control Plane Node	Worker Node
CPU	32 cores, no-hyperthreading	32 cores
Memory	64 GiB RAM	64 GiB RAM
Disk	256 GiB SSD (IOPS of 600 MBPS in mixed mode)	256 GiB SSD (IOPS of 600 MBPS in mixed mode)
Network interfaces	3	3

When you deploy VMS, it is recommended that you configure the following interfaces and links:

- Management interface for management of internal cluster communication and has one IP address.
- Interface that connects to external agents that has two IP addresses:
  - One IP address for external agents such as RADIUS accounting server, Kafka Broker, Kafka Producer, or

Kafka Consumer Topic to communicate with VMS.

- The second address is an elastic or floating IP address and is assigned to a cluster for connectivity to Versa Director and for AAA proxy servers.
- Interface for connectivity to VOS devices

To deploy VMS, you do the following:

1. Install the VMS software on a bare-metal platform. See [Install VMS](#), below.
2. Perform initial configuration of VMS from the shell of the bare-metal platform. See [Configure a VMS Server Using the CLI](#), below.
3. Configure VMS from Versa Director. See [Configure VMS from Versa Director](#), below.
4. Configure a VMS server profile for a VOS device to communicate with the VMS server. You can then enable VMS services to send or receive stream feeds. See [Configure VMS Messaging Service](#), below.
5. Repeat Steps 3 and 4 for each service that you want to enable for a tenant.

---

## Install VMS

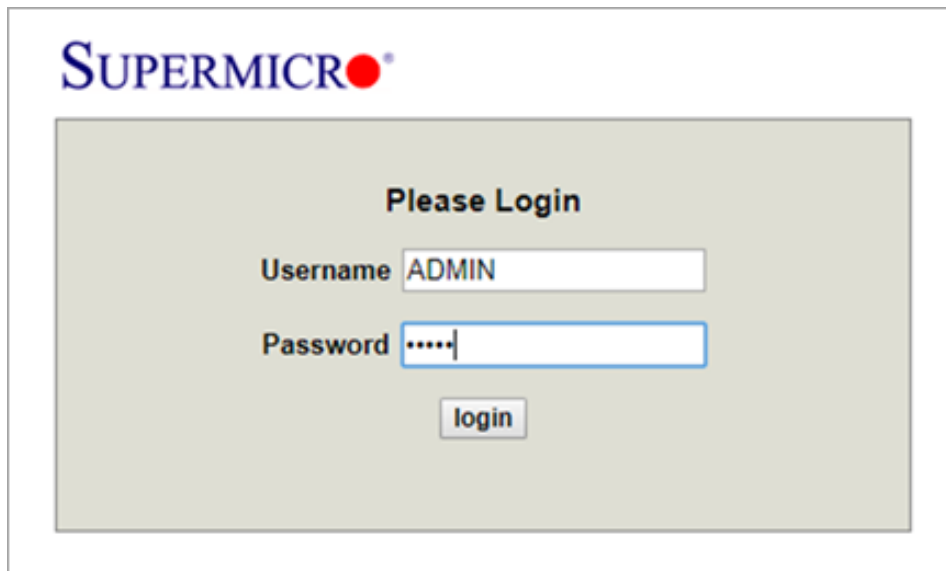
To install the VMS software, you install the VMS ISO image on a bare-metal platform. The VMS image can be an AMI, an ISO, and OVA, or a QCOW2 image.

The figures in this section show VMS software installation on a Supermicro server. The screens may differ based on the server you use.

To access the bare-metal platform remotely, configure intelligent platform management interface (IPMI) on the bare-metal server.

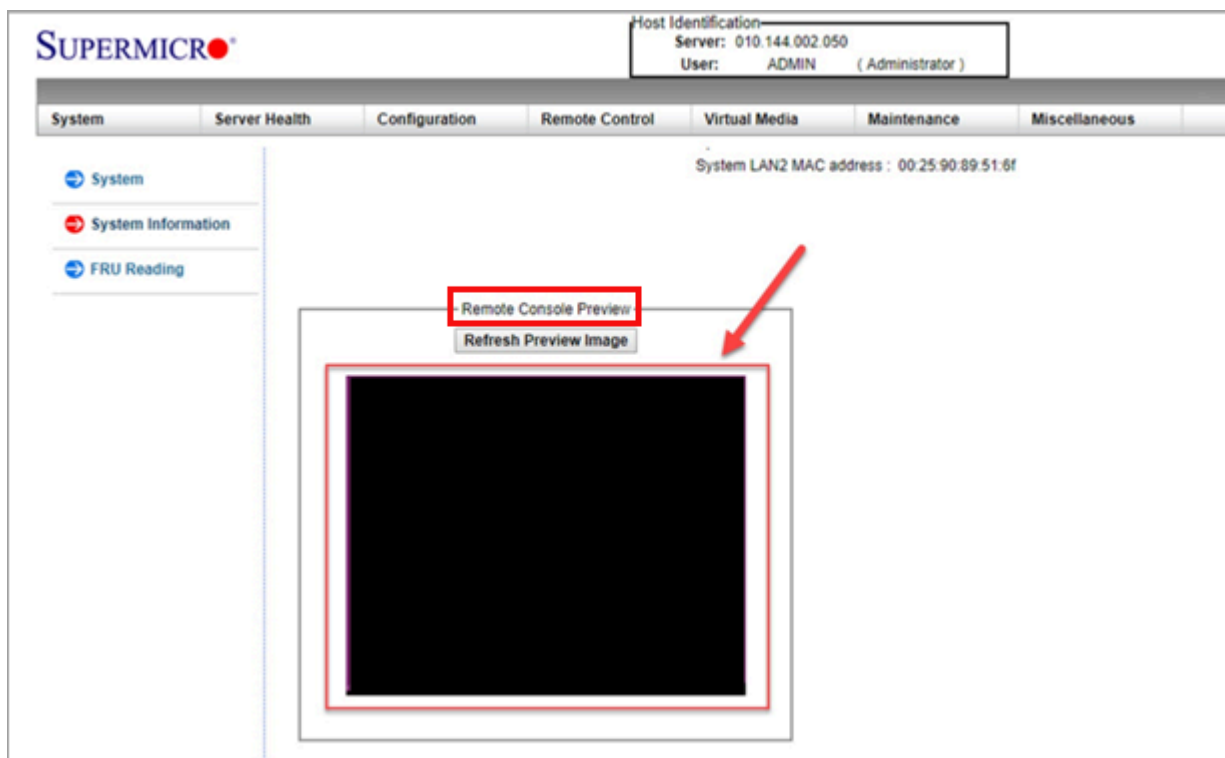
To install the VMS software:

1. Log in to the remote console.

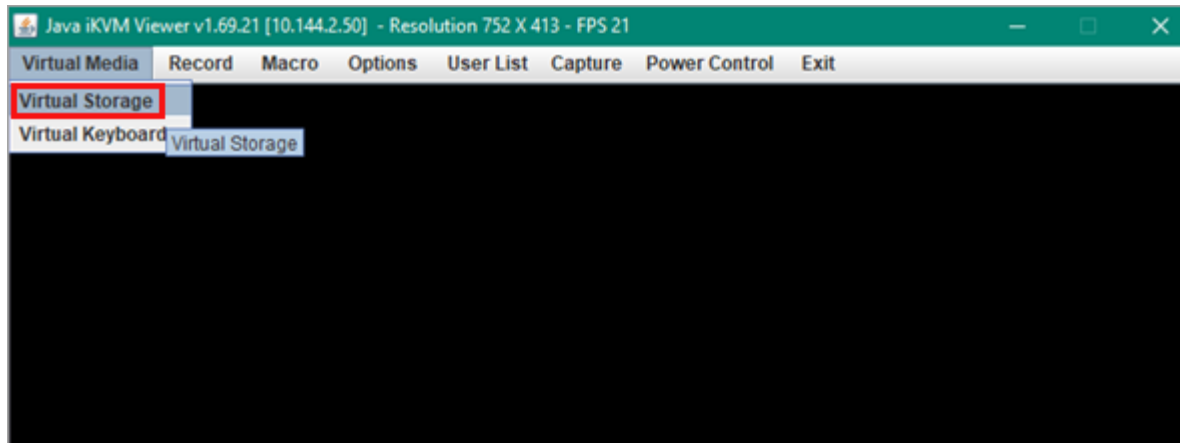


The image shows a login page for Supermicro. At the top left is the Supermicro logo. In the center, the text "Please Login" is displayed. Below this, there are two input fields: "Username" with the value "ADMIN" and "Password" with masked characters ".....". A "login" button is positioned below the password field.

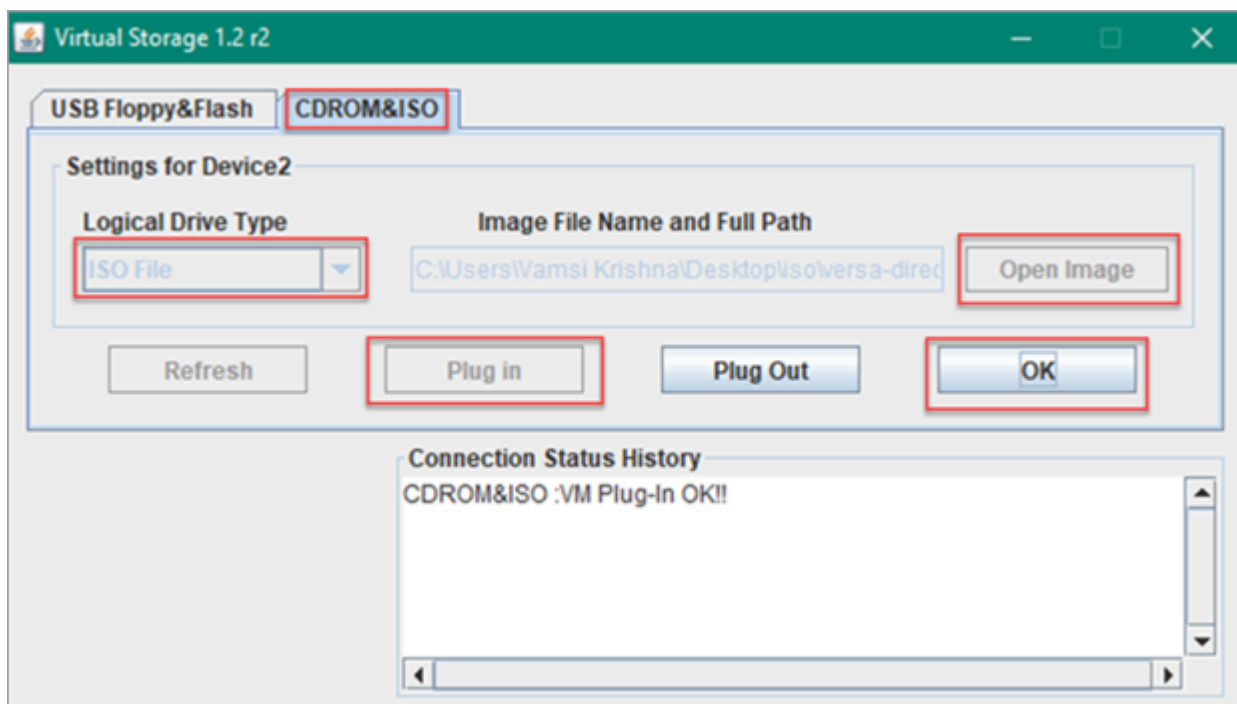
2. Click anywhere in the Remote Console Preview window to launch the remote console. If the Java SE Development Kit is installed on the server, you can launch the remote console from the development kit.



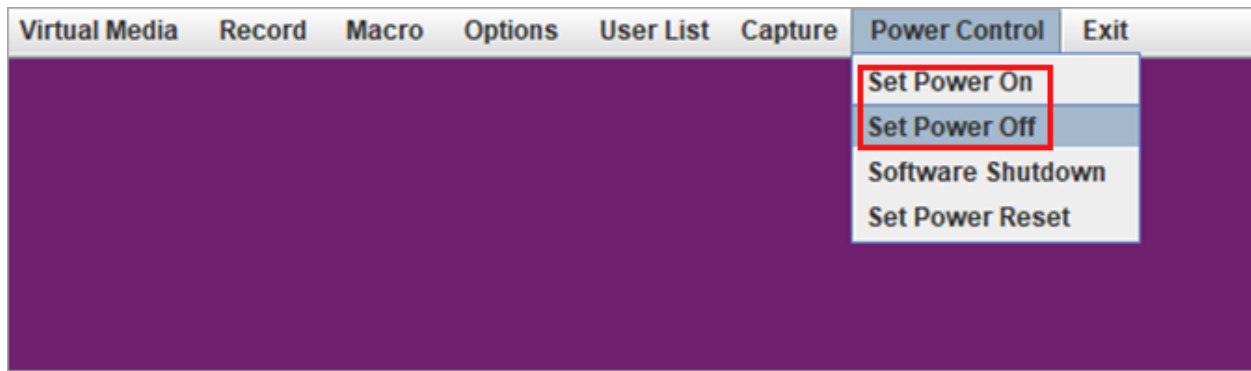
3. In the Virtual Media tab, click Virtual Storage.



4. In the Virtual Storage window, select the CDROM & ISO tab. The Settings for Device2 window displays.



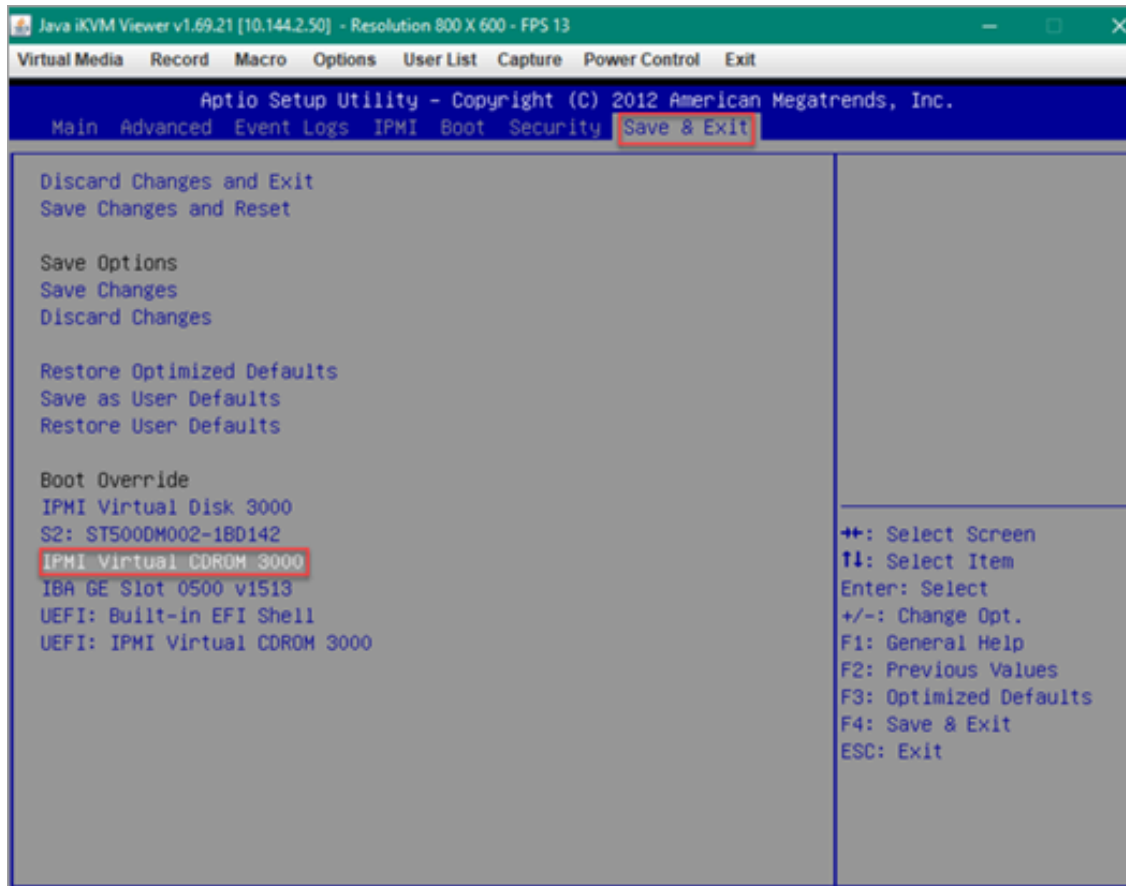
- a. In the Logical Drive Type field, select ISO File.
  - b. Click Open Image and type the full path name of the software image. You can find the image at <https://versanetworks.app.box.com/s/d7jh1z6y3kaijd3yfwil0uxchr1w9ton/folder/256571398920>
  - c. Click Plug In.
  - d. Click OK.
5. Select the Power Control tab.



- a. Click Set Power Off to power down the device.
  - b. Click Set Power On to restart the device.
6. After the device restarts, the remote console window displays the server banner.



7. To perform device setup, press the Delete key.
8. In the Setup Utility window, select the Save and Exit tab.



9. Click IPMI Virtual CDROM 3000 to run the ISO file from a local partition.
10. Press Enter.
11. Install the ISO image, and then configure the primary IP address and hostname. For example:

```
[admin@versa-Msgservice: ~] $ sudo vi /etc/network/interfaces
[sudo] password for admin:
[admin@versa-msgservice: ~] $ sudo vi /etc/hosts
host.conf hostname hosts hosts.allow hosts.deny
[admin@versa-msgservice: ~] $ sudo vi /etc/hosts
[admin@versa-msgservice: ~] $ sudo vi /etc/hostname
sudo: unable to resolve host versa-msgservice: Resource temporarily unavailable
[admin@versa-msgservice: ~] $ sudo reboot
```

After the reboot completes, VMS release information, including the version, release date, and package ID display.

12. Check the status of the server by issuing the **vsh status** CLI command. Note that the command output may show that the status of Kubelet as inactive. For example:

```
=====
Versa Package Info: versa-msgservice-20240412-090117-d203801-5.1.1
=====
Info: SYSTEM-SERVICES-STATUS
```



```
kubelet:activating
docker:active (3945)
vms-admin:inactive
vms-db:inactive
```

---

## Configure a VMS Server Using the CLI

To configure the VMS server, you do the following:

- Configure interfaces and a hostname on the VMS node.
- Generate self-signed certificates.
- Perform the initial VMS configuration, which installs the Kubernetes control plane, creates a Docker overlay, and loads containers.
- Regenerate certificates.

You perform the initial configuration from the shell of the VMS server.

To configure VMS server:

1. Issue the **sudo vi /etc/network/interfaces** CLI command to configure interfaces (here eth0 and eth1) and hostname. For example:

```
[admin@versa-msgservice: ~] $ sudo vi /etc/network/interfaces
[sudo] password for admin:
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d
#auto eth0
iface eth0 inet static
    address 10.40.2.201
    netmask 255.255.0.0
    gateway 10.40.0.1
    dns-nameserver 10.48.0.99
    dns-nameserver 8.8.8.8

# auto eth1
# iface eth1 inet static
#   address 10.43.17.231
#   netmask 255.255.0.0
#   broadcast 172.17.2.255
#   gateway 172.17.9.1
```

2. Issue the **sudo /opt/versa/vms/certs/vms\_cert\_gen.sh** CLI command to generate self-signed certificates. For example:

```
[admin@versa-msgservice: ~] $ sudo /opt/versa/vms/certs/vms_cert_gen.sh
[sudo] password for admin:

Domain is mandatory
Usage:
```

```

vms_cert_gen
Description:
Generate private key and certificate signing request (CSR) for CA to sign
Example:
sudo /opt/versa/vms/certs/vms_cert_gen.sh --domain vms01 --country US --state CA --locality SC
--organization acme.com --organizationalunit IT --email cert-admin@acme.com --keypass
acmetest123
--validity 3650 --san vms-01.acme.com,DNS.1:vms-01,DNS.2:vms-elastic-fqdn,DNS.3:vms-02,IP.
1:10.10.10.10,IP.2:10.10.10.11
Options:
-h, --help          Show this help message and exit.
--domain            <Fully qualified domain name>
--country           <Country name>
--state             <State name>
--locality          <Locality name>
--organization      <Organization name>
--organizationalunit <Organizationalunit Name>
--email             <email>
--keypass           <private key password, if you want the private key is encrypted>
[--validity]        <certificate validity in days>
[--san]             <Fully qualified domain name for Subject Alt-Name, please refer to example for
providing
multiple values, DNS: DNS name; Each DNS value should not exceed 64 characters>
Optionally provide IP addresses for SAN

```

The results display after you generate self-signed certificates. For example:

```

[admin@versa-msgservice: ~] $ sudo /opt/versa/vms/certs/vms_cert_gen.sh --domain vms-1 --country
US --state CA --locality SC
--organization mvno.com --organizationalunit QA --email admin@mvno.com --keypass versa123 --
validity 3650 --organization
=> Generating Key and CSR for request domain: vms-1, key_pass: versa123
=> Request details: [/emailAddress=admin@mvno.com/C=US/ST=CA/L=SC/O=mvno.com/OU=QA/
CN=vms-1]
=> Generating Root Certificate with password encrypted keypass: versa123 and Root Certificate
=> Successfully generated Key file: /opt/versa/vms/certs//root-ca-key.pem
=> Please copy the file out of the system and maintain it
=> Successfully generated ROOT CA file: /opt/versa/vms/certs//root-ca-cert.pem
Generating RSA private key, 4096 bit long modulus (2 primes)
*****
+++
*****
+++
e is 65537 (0x010001)
=> Successfully generated Key file: /opt/versa/vms/certs//ca-key.pem
Ignoring -days; not generating a certificate
=> Successfully generated INTERMEDIATE_CSR_FILE: /opt/versa/vms/certs//ca-csr.pem
Using configuration from /opt/versa/vms/certs//openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 4096 (0x1000)
    Validity

```

```

Not Before: Jun  7 07:57:45 2024 GMT
Not After : Jun  5 07:57:45 2034 GMT
Subject:
countryName      = US
stateOrProvinceName = CA
organizationName  = mvno.com
organizationalUnitName = QA
commonName       = vms-1 Intermediate Cert Authority
emailAddress      = admin@mvno.com
X509v3 extensions:
X509v3 Subject Key Identifier:
    68:D0:EA:73:6E:6A:61:13:0C:1C:42:DF:BC:60:AA:A2:7D:01:65:EB
X509v3 Authority Key Identifier:
    keyid:51:87:05:2D:EF:E5:C1:0B:08:93:AF:4D:58:E8:94:BF:8D:5F:7F:E7

X509v3 Basic Constraints: critical
    CA:TRUE, pathlen:0
X509v3 Key Usage: critical
    Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Jun  5 07:57:45 2034 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
=> Successfully generated INTERMEDIATE CA file: /opt/versa/vms/certs//ca-cert.pem
=> Successfully verified INTERMEDIATE CA file: /opt/versa/vms/certs//ca-cert.pem
=> Successfully generated the Private CA Chain
=> Please copy the /opt/versa/vms/certs//root-ca-key.pem out of this system and store it safely
=> Please use the Password "versa123" during server and client cert generation for '\vsh configure\'

```

- Issue the **vsh configure** CLI command to install the Kubernetes control plane, create a Docker overlay, and load containers.
- For the initial configuration, respond **Y** to the following prompt, and then enter the IP address that the VMS server uses to connect to VOS devices. For example:

```

Is the primary interface configuration finalized? (y/N) : Y
Management Interface IP of this VMS server
Please Enter this VMS Server Management/Primary Interface IP Address : 10.40.2.201

```

- Respond **Y** to the following prompt, and then enter the primary and secondary Versa Director IP address and FQDN or hostname. VMS uses this information to communicate with the Director node and to fetch Director certificates for TLS communication. Note that only a Director that is configured can communicate with VMS. For example:

```

Is the hostname of this VMS server finalized? (y/N) : Y

```

- Enter the VMS server IP address. For example:

```

FQDN/Hostname of this VMS server
Is the hostname of this VMS server finalized? (y/N) : Y
Please enter the Hostname of this VMS Server: vms-1.mvno.com
This may take up to 10 minutes to complete initialization

```

- In response to the following prompt, enter **Y** to complete the configuration. For example:

[https://docs.versa-networks.com/Management\\_and\\_Orchestration/Versa\\_Messaging\\_Service/Passive\\_Authentication/01\\_Co...](https://docs.versa-networks.com/Management_and_Orchestration/Versa_Messaging_Service/Passive_Authentication/01_Co...)

Updated: Wed, 23 Oct 2024 08:49:43 GMT

Copyright © 2024, Versa Networks, Inc.

```
Adding new hosts entry.
VMS server configuration
Is this the 1st Control Plane Node of the cluster? (y/N) : y
```

```
=====
This may take up to 10 minutes to complete initialization
=====
```

```
Info: Installing Kubernetes ...
Info: Creating auto completions for kubectl
Info: Disabling Swap ...
Info: Creating Docker overlay ....
disabled_plugins = []
imports = []
oom_score = 0
plugin_dir = ""
required_plugins = []
root = "/var/lib/containerd"
state = "/run/containerd"
temp = ""
version = 2
```

When the Kubernetes control plane initializes, the success message displays. For example:

```
[kubelet-start] Starting the kubelet
[wait-control-plane] Waiting for the kubelet to boot up the control plane as
sta tic Pods from directory "/etc/kubernetes/manifests". This can take
up to 4m0s
[apiclient] All control plane components are healthy after 7.014799 seconds
[upload-config] Storing the configuration used in ConfigMap "kubeadm-config"
in the "kube-system" Namespace
[kubelet] Creating a ConfigMap "kubelet-config" in namespace kube-system with
th e configuration for the kubelets in the cluster
[upload-certs] Storing the certificates in Secret "kubeadm-certs" in the "kube-
s ystem" Namespace
[upload-certs] Using certificate key:
8a93eb6463d2d9d961706b16a229bd1b4330337341cdef2a85765597542e3717
[mark-control-plane] Marking the node vms-1.mvno.com as control-plane by
adding the labels: [node-role.kubernetes.io/control-plane node.
kubernetes.io/exclude-fr om-external-load-balancers]
[mark-control-plane] Marking the node vms-1.mvno.com as control-plane by
adding the taints [node-role.kubernetes.io/control-plane:NoSchedule]
[bootstrap-token] Using token: mttojz.2pr32kh3x5e4h01j
[bootstrap-token] Configuring bootstrap tokens, cluster-info ConfigMap, RBAC
Rol es
[bootstrap-token] Configured RBAC rules to allow Node Bootstrap tokens to get
no des
[bootstrap-token] Configured RBAC rules to allow Node Bootstrap tokens to post
C SRs in order for nodes to get long term certificate credentials
[bootstrap-token] Configured RBAC rules to allow the csrapprover controller
auto matically approve CSRs from a Node Bootstrap Token
[bootstrap-token] Configured RBAC rules to allow certificate rotation for all
no de client certificates in the cluster
[bootstrap-token] Creating the "cluster-info" ConfigMap in the "kube-public"
nam espace
```

```
[kubelet-finalize] Updating "/etc/kubernetes/kubelet.conf" to point to a
rotatab                               le kubelet client certificate and key
[addons] Applied essential addon: CoreDNS
[addons] Applied essential addon: kube-proxy
```

Your Kubernetes control-plane has initialized successfully!

To start using your cluster, you need to run the following as a regular user:

```
mkdir -p $HOME/.kube
sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
sudo chown $(id -u):$(id -g) $HOME/.kube/config
```

Alternatively, if you are the root user, you can run:

```
export KUBECONFIG=/etc/kubernetes/admin.conf
```

You should now deploy a pod network to the cluster.

Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:

<https://kubernetes.io/docs/concepts/cluster-administration/addons/>

You can now join any number of the control-plane node running the following  
comm and on each as root:

```
kubeadm join vms-1.mvno.com:6443 --token mttojz.2pr32kh3x5e4h01j \
--discovery-token-ca-cert-hash
sha256:10902b525bf71ab2d9ee1c49b27c4c06cb
b4b5cc1ac56bd26633c38f7b8ae805 \
--control-plane --certificate-key
8a93eb6463d2d9d961706b16a229bd1b433033
7341cdef2a85765597542e3717
```

Please note that the certificate-key gives access to cluster sensitive data,  
kee p it secret!

As a safeguard, uploaded-certs will be deleted in two hours; If necessary, you  
c an use

"kubeadm init phase upload-certs --upload-certs" to reload certs afterward.

Then you can join any number of worker nodes by running the following on each  
as root:

```
kubeadm join vms-1.mvno.com:6443 --token mttojz.2pr32kh3x5e4h01j \
--discovery-token-ca-cert-hash
sha256:10902b525bf71ab2d9ee1c49b27c4c06cb
b4b5cc1ac56bd26633c38f7b8ae805
```

Info: Kube Init successful

Info: Init Flannel

namespace/kube-flannel created

clusterrole.rbac.authorization.k8s.io/flannel created

clusterrolebinding.rbac.authorization.k8s.io/flannel created

serviceaccount/flannel created

configmap/kube-flannel-cfg created

daemonset.apps/kube-flannel-ds created

readOnlyPort: 0

protectKernelDefaults: true

When all resources are allocated, the following information displays and this completes the initial set up and configuration of this VMS node:

Allocated resources:

(Total limits may be over 100 percent, i.e., overcommitted.)

Resource	Requests	Limits
----------	----------	--------

```

-----
cpu          950m (7%)  0 (0%)
memory       290Mi (1%) 340Mi (1%)
ephemeral-storage 0 (0%)  0 (0%)
hugepages-1Gi 0 (0%)  0 (0%)
hugepages-2Mi 0 (0%)  0 (0%)
Events:
Type      Reason          Age   From      Message
-----
Normal    Starting        108s  kube-proxy
Normal    Starting        2m2s  kubelet    Starting kubelet.
Warning   InvalidDiskCapacity 2m2s  kubelet    invalid capacity 0
on
Normal    NodeAllocatableEnforced 2m1s  kubelet    Updated Node
Allocata  ble limit across pods
Normal    NodeHasNoDiskPressure 2m1s  kubelet    Node vms-1.mvno.com
s        tatus is now: NodeHasNoDiskPressure
Normal    NodeHasSufficientPID 2m1s  kubelet    Node vms-1.mvno.com
s        tatus is now: NodeHasSufficientPID
Normal    NodeHasSufficientMemory 2m1s  kubelet    Node vms-1.mvno.com
s        tatus is now: NodeHasSufficientMemory
Normal    Starting        2m    kubelet    Starting kubelet.
Warning   InvalidDiskCapacity 2m    kubelet    invalid capacity 0
on
Normal    NodeHasSufficientMemory 119s  kubelet    Node vms-1.mvno.com
s        tatus is now: NodeHasSufficientMemory
Normal    NodeHasNoDiskPressure 119s  kubelet    Node vms-1.mvno.com
s        tatus is now: NodeHasNoDiskPressure
Normal    NodeHasSufficientPID 119s  kubelet    Node vms-1.mvno.com
s        tatus is now: NodeHasSufficientPID
Normal    NodeAllocatableEnforced 119s  kubelet    Updated Node
Allocata  ble limit across pods
Normal    RegisteredNode    109s  node-controller Node vms-1.mvno.com
e        vent: Registered Node vms-1.mvno.com in Controller
Normal    NodeReady        98s   kubelet    Node vms-1.mvno.com
s        tatus is now: NodeReady

Info: Kubernetes component status
Warning: v1 ComponentStatus is deprecated in v1.19+
NAME      STATUS MESSAGE ERROR
scheduler Healthy ok
controller-manager Healthy ok
etcd-0    Healthy ok

Info: Kubernetes Cluster Information
Kubernetes control plane is running at https://vms-1.mvno.com:6443
CoreDNS is running at https://vms-1.mvno.com:6443/api/v1/namespaces/kube-
system/
services/kube-dns:dns/proxy

To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
Fri Jun 7 01:45:21 PDT 2024 File /opt/versa/etc/install/initial_install is (re-
)created by /opt/versa/scripts/install/vms_install_helper.sh

Info: Initial Installation is completed

```

```
=====
Updating existing hosts entry.
```

```
Info: Initial Setup of the node is complete
```

```
Info: Please re-run "vsh configure" to complete setup and configuration of
this node
```

```
Initial set-up completed
```

```
Please copy certificates from /var/tmp/copy_certs/ directory to begin your
confi guration from Versa Orchestrator
=====
```

8. Issue the **vsh configure** CLI command again to regenerate the certificates, configure interfaces, and enter the elastic IP address.
9. Configure the FQDN of the VMS server to generate and validates certificates. The FQDN for the floating IP address of the node must be present in the SAN of the certificates. Agents use this FQDN to connect to VMS.
10. Enter the subject alternative names (SANs) to be secured by the certificate. For example:

```
Please Enter Subject ALT Name 1 used in Versa Message Service certificate file : sdwan-vms-1-elastic.
provider.com
Please Enter Subject ALT Name 2 used in Versa Message Service certificate file : sdwan-vos.provider.com
```

11. Respond **Y** to the following prompt to confirm the FQDN. For example:

```
Do you want to continue with sdwan-vms-1.provider.com as the entry?(y/N): Y
```

12. Enter a unique name for the VMS node for server identification. This is required for HA fail-over. For example:

```
Please provide the below server identification information
This Information is needed for HA fail-over
Please Enter a unique name for this VMS node : sdwan-vms-1
```

13. Enter the application certificate keystore password and confirm the password. For example:

```
Application Certificate KeyStore Credentials
Enter Password for Application Certificate KeyStore :
RE-Enter Password for Application Certificate KeyStore : secret/default-server-secret created
```

14. Enter the IP address of the VMS cluster to which the VOS device or ADC connects. For example:

```
IP Address of VMS-Cluster where VOS/ADC will connect
Please Enter IP Address for this VMS Cluster where VOS/ADC will connect : 192.168.73.253
```

15. Enter the FQDN of VMS cluster to which applications connect. Note that this FQDN must be included in the server certificates. For example:

```
FQDN of VMS-Cluster where applications will connect (ELASTIC/Floating FQDN/hostname)
** This FQDN must exist in Server Certificates
Please Enter FQDN used as Entry for applications : sdwan-vms-1-elastic.provider.com
```

16. Enter the elastic floating IP address of the VMS cluster to which agents send traffic. The floating IP address is not assigned to any VMS node, the FQDN associated with this IP address is different from the VMS FQDN, and you cannot change this IP address after the configuration. For example:

```
Elastic Floating IP of this VMS Cluster where agents will send traffic to VMS Cluster
```

```
The FQDN associated with this IP is separate from VMS FQDN. This is a floating IP not assigned to any VMS node
This IP cannot be changed after configuration
Is the Elastic IP of this VMS Cluster finalized? (y/N) : y
Please enter the Elastic IP of this VMS Server: 10.40.173.25
Updating existing hosts entry.
```

After the certificate regenerates, the certificate information displays after the certificate regenerates. The following example output shows some of the information that displays:

```
writing new private key to '/opt/versa/vms/certs/db_certs/node-key.pem'
-----
Using configuration from /opt/versa/scripts/certificates/ca-csr.conf
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number:
    76:ac:e3:5f:6a:6c:3f:a5:b5:e9:7d:89:5a:99:08:32:76:a5:47:ff
  Validity
    Not Before: May 20 17:14:40 2024 GMT
    Not After : Mar 25 17:14:40 2031 GMT
  Subject:
    countryName      = IN
    organizationName = Versa Networks Inc.
    commonName       = node
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    X509v3 Key Usage:
      Digital Signature, Non Repudiation, Key Encipherment
    X509v3 Subject Alternative Name:
      DNS:sdwan-vms-1.provider.com, DNS:localhost, DNS:127.0.0.1
Certificate is to be certified until Mar 25 17:14:40 2031 GMT (2500 days)

Write out database with 1 new entries
Data Base Updated
Converting node-cert.pem to node.crt and node-key.pem to node.key
Generating certificates for root client
Using configuration from /opt/versa/scripts/certificates/ca-csr.conf
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number:
    76:ac:e3:5f:6a:6c:3f:a5:b5:e9:7d:89:5a:99:08:32:76:a5:48:00
  Validity
    Not Before: May 20 17:14:41 2024 GMT
    Not After : Mar 25 17:14:41 2031 GMT
  Subject:
    countryName      = IN
    organizationName = Versa Networks Inc.
    commonName       = root
  X509v3 extensions:
    X509v3 Basic Constraints:
```



CA:FALSE  
Netscape Cert Type:  
SSL Client, S/MIME  
Netscape Comment:  
OpenSSL Generated Client Certificate  
X509v3 Subject Key Identifier:  
A7:65:D0:82:E8:AD:16:42:53:91:36:68:A1:5F:3E:FE:BC:E0:EF:71  
X509v3 Authority Key Identifier:  
keyid:44:5C:AF:E7:11:AD:B1:9D:D6:37:DC:89:59:F4:70:D4:DD:90:60:60

X509v3 Key Usage: critical  
Digital Signature, Non Repudiation, Key Encipherment  
X509v3 Extended Key Usage:  
TLS Web Client Authentication, E-mail Protection

Certificate is to be certified until Mar 25 17:14:41 2031 GMT (2500 days)

Write out database with 1 new entries

Data Base Updated

Generating certificates for versa client

Using configuration from /opt/versa/scripts/certificates/ca-csr.conf

Check that the request matches the signature

Signature ok

Certificate Details:

Serial Number:

76:ac:e3:5f:6a:6c:3f:a5:b5:e9:7d:89:5a:99:08:32:76:a5:48:01

Validity

Not Before: May 20 17:14:42 2024 GMT

Not After : Mar 25 17:14:42 2031 GMT

Subject:

countryName = IN

organizationName = Versa Networks Inc.

commonName = versa

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Cert Type:

SSL Client, S/MIME

Netscape Comment:

OpenSSL Generated Client Certificate

X509v3 Subject Key Identifier:

32:1E:4B:31:EF:DB:26:BC:BF:EF:2D:C1:86:84:98:6C:C8:B4:44:E3

X509v3 Authority Key Identifier:

keyid:44:5C:AF:E7:11:AD:B1:9D:D6:37:DC:89:59:F4:70:D4:DD:90:60:60

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key Encipherment

X509v3 Extended Key Usage:

TLS Web Client Authentication, E-mail Protection

Certificate is to be certified until Mar 25 17:14:42 2031 GMT (2500 days)

Write out database with 1 new entries

Data Base Updated

Successfully generated all certificates at /opt/versa/vms/certs/db\_certs/

Installing Database

cockroach-v23.1.8.linux-amd64-fips/cockroach

```

cockroach-v23.1.8.linux-amd64-fips/lib/libgeos.so
cockroach-v23.1.8.linux-amd64-fips/lib/libgeos_c.so
v23.1.8
Cockroach Installation/Upgrade successful !
v23.1.8
Using certificates in path: /opt/versa/vms/certs/db_certs/
Starting nodes
Starting the DB node
DB Node started.
Initilizing node
ERROR: cluster has already been initialized
Failed running "init"
DB node initilized
Loading data from SQL File: /opt/versa/vms/db/db_script.sql
CREATE DATABASE
NOTICE: schedule "core_schedule_label" already exists, skipping
SCHEDULED BACKUP 0
SET
NOTICE: relation "vms_supported_services" already exists, skipping
CREATE TABLE
INSERT 0 1
INSERT 0 1
INSERT 0 1
INSERT 0 1
INSERT 0 1
INSERT 0 1
INSERT 0 1
INSERT 0 1
INSERT 0 1
INSERT 0 1
SQL data successfully loaded!

Initial set-up completed
Please copy certificates from /var/tmp/copy_certs/ directory to begin your configuration from Versa
Orchestrator

```

17. Copy the following server certificates from the /var/tmp/copy\_certs/ directory to the first VMS node. After you have copied the certificates, you can configure VMS on Versa Director.
  - root-ca-cert.pem—This is the VMS root certificate. Upload it to the Files and Folders directory on the Director node and then associate it with a configuration template. VOS devices use this certificate to configure the VMS server.
  - server-cert.pem—Upload this certificate to the Director node when you configure the VMS connector for TLS. The Director node validates the VMS certificate.

---

## Configure VMS from Versa Director

To configure VMS from a Director node, you create a VMS connector. In creating the VMS connection, you configure a VMS cluster that establishes a connection to a VMS node. While you can configure VMS from either the primary or secondary Director node, it is recommended that you configure the first control plane node from the primary Director node.

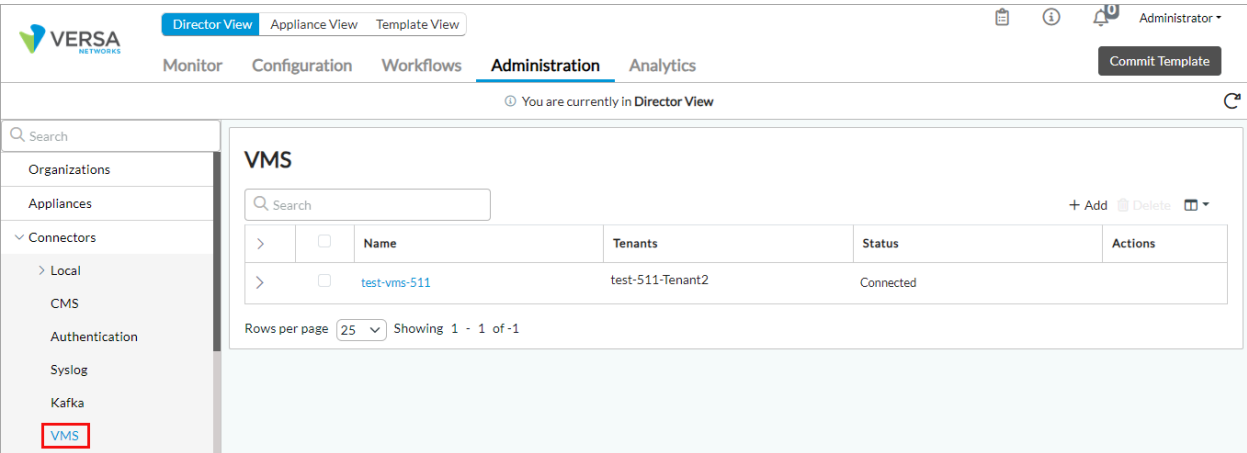
As part of configuring the VMS connector, you select the VMS interfaces that connects to your VOS devices and to which external agents connect; specify the Analytics controller node to which to send logs; and configure third-party authentication, XIP EIP, and the SASE-for-SIM Kafka and RADIUS services for tenants.

## Configure a VMS Connector

You use the VMS connector configuration wizard to configure and establish the initial connection to the VMS cluster on the first node of the VMS cluster.

To configure a VMS connector:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Connectors > VMS Connector in the left menu bar.



3. Click + Add. The Configure VMS Connection configuration wizard displays.
4. In the Step 1, VMS Connection screen, enter information for the following fields.

**VMS CONNECTION**

VMS Connector: VMS-Cluster-1

**VMS Connection**

Upload your VMS node certificate, and enter your VMS node IP and name

VMS Cluster Name \*  
VMS-Cluster-1

Certificate \*  
cacert.pem Browse

<input type="checkbox"/> VMS IP ADDRESS / FQDN	NODE TYPE	VMS NAME
<input type="checkbox"/> vms1-versa.networks.com	Control Node	VMS-Main

Cancel Back Next

Field	Description
VMS Connector Name	Enter a name for the VMS connector.
Certificate	Click Browse, and then upload the server certificate that you generated on the first VMS control plane node and saved in the /var/tmp/ folder. The file containing the server certificate must be in PEM format.
VMS IP Address/FQDN (Table)	Click the + Add icon to enter information about the VMS node. You must add at least one VMS address.
<ul style="list-style-type: none"> <li>VMS IP Address/FQDN</li> </ul>	Enter the IP address or FQDN of the VMS node. The value that you enter must be present as the subject alternative name (SAN) of the VMS node.
<ul style="list-style-type: none"> <li>Node Type</li> </ul>	Select the VMS node type: <ul style="list-style-type: none"> <li>Control Node</li> <li>Worker Node</li> </ul>
<ul style="list-style-type: none"> <li>VMS Name</li> </ul>	Enter a name for the VMS node.

- Click Next to go to the Step 2, VMS Cluster screen, and then enter information for the following fields.

✓

VMS CONNECTION

2

VMS CLUSTER

3

TENANTS & SERVICES

4

REVIEW

Configure VMS Cluster

VMS Connector: VMS-Cluster-1

### Authentication

Enter an administrative login credential for Versa Director.

Username

Below are the director assigned to your VMS Cluster during high availability. If you prefer, you can change the address to your preference.

Primary Director IP Address / Fully Qualified Domain Name (FQDN) \*

Secondary Director IP Address / Fully Qualified Domain Name (FQDN) \*

Select the interface of the VMS node that connects to your Versa OS (VOS) devices.

VMS Interface \*

---Please Select---

VMS Cluster Name \*

Select the VMS interface where external agents will connect.

VMS Elastic IP for Agents \*

VMS Elastic Hostname / FQDN for Agents \*

Enter the address to the Versa Analytics Controller you want to send logs to.

Controller IP Address \*

Controller Port \*

Cancel

Back

Next

Field	Description
Username	By default, the username vmsadmin displays. When you add the first VMS on a Director node, configure the credentials by entering the password and then confirm the password.
Primary Director IP Address/Fully Qualified Domain Name	Enter the primary IP address or FQDN of the Director node to which you have logged in.
Secondary Director IP Address/Fully Qualified Domain Name	Enter the secondary IP address or FQDN of the Director node.
VMS Interface	Select the VMS interface to use to communicate with VOS devices.
VMS Cluster Name	Enter a name for the VMS cluster. VMS high availability (HA) uses the name to identify the cluster.
VMS Elastic IP for Agents	Enter the IP address that external agents, such as Kafka Broker, Kafka Consumer Topic, Kafka Producer, and the RADIUS accounting server, use to communicate with VMS. This IP address is also called the elastic or floating IP address, and it is assigned to the VMS cluster. The VMS load balancer, which is initiated on the first node in the cluster when the cluster is installed, attracts traffic intended for this IP address (or for a contiguous range of IP addresses) and forwards the traffic to the microservice that serves this traffic. You associate the floating IP address with an FQDN, and this FQDN must have a SAN entry in the VMS server certificate. Note that the elastic or floating IP must be associated with an IP address in the same subnet address space as the subnet of the network interfaces that are connected to the agent.
VMS Elastic Hostname/FQDN for Agents	Enter the VMS FQDN or hostname that external agents use to communicate with VMS.
Controller IP Address	Enter the IP address of the Controller node to which to send syslog messages from VMS to Analytics node. VMS sends syslog messages for all start, stop, and exception events to Analytics nodes.
Controller Port	Enter the Controller port number to which to send syslog messages from VMS to Analytics nodes.

- Click Next to go to the Step 3, Tenants and Services screen. The following screen displays.

**Configure TENANTS & SERVICES**

VMS Connector: VMS-Cluster-1

**VMS Connection**

Upload your VMS node certificate, and enter your VMS node IP and name

Available: 12 Select all Deselect all

- ☒ Customer-1
- ☐ test-511-Tenant5
- ☐ AG-Testing-T2
- ☐ Tenant-Test-1
- ☐ AG-Testing-T3
- ☐ AG-Testing-T1
- ☐ test-511-Tenant3
- ☐ test-511-Tenant4
- ☐ AG-Testing-T4
- ☐ test-511-Tenant1
- ☐ test-511-Provider-Org
- ☐ test-511-Tenant2

**Tenant Selected**

▼ CUSTOMER-1

Cancel Back Submit Next

7. Select the tenants for which you want to enable VMS services. The selected tenants display in the Tenant Selected pane.
8. To enable services for a tenant, click the down arrow to display the available service options, and then slide the toggle to enable a service. Enter information for the following fields.

## Tenant Selected

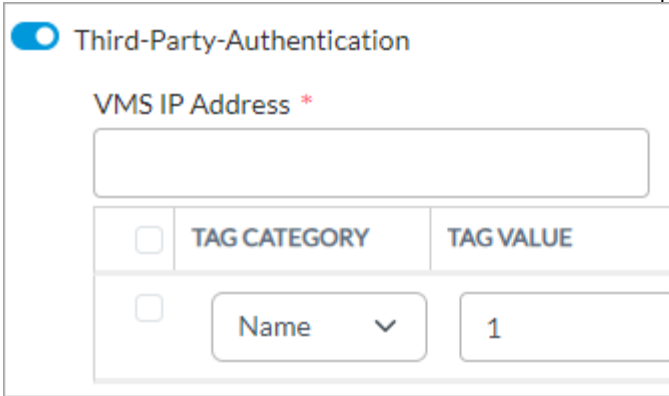
^ CUSTOMER-1

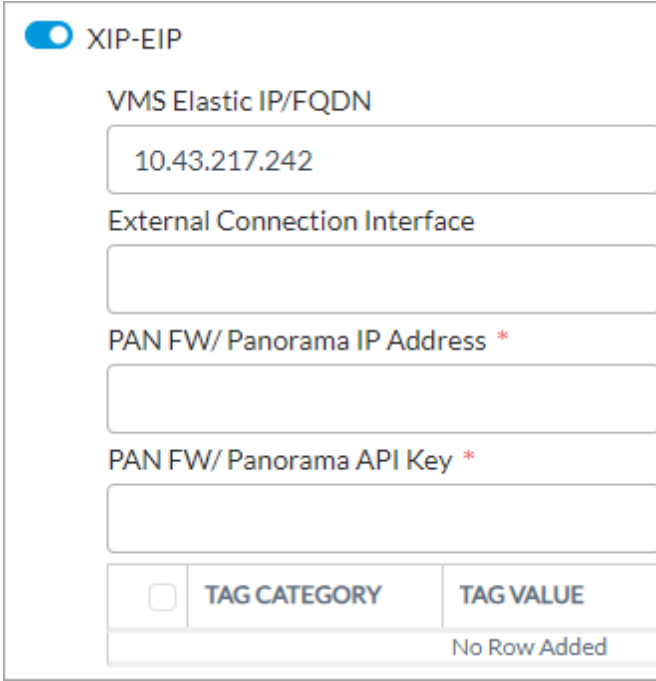
### Services

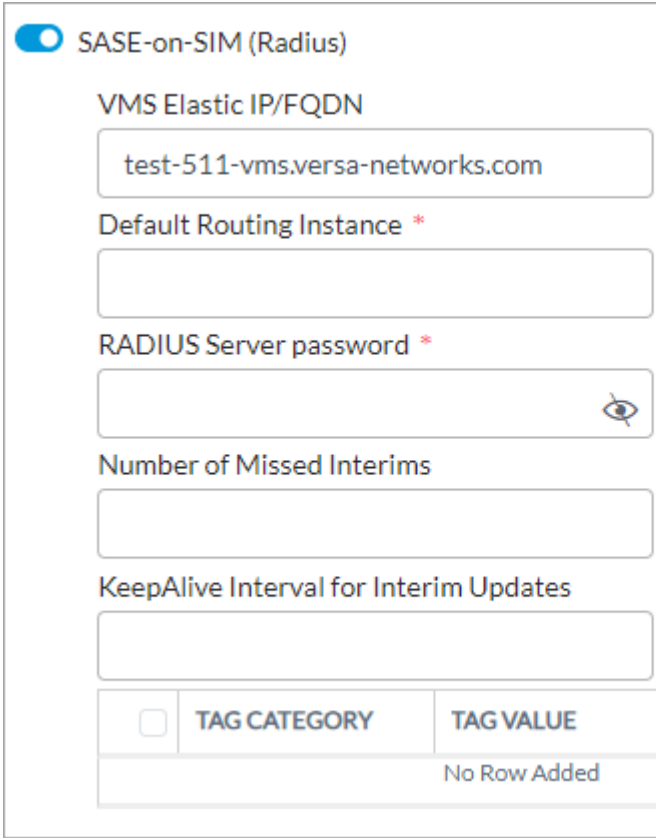
Choose which services to enable for your tenant.

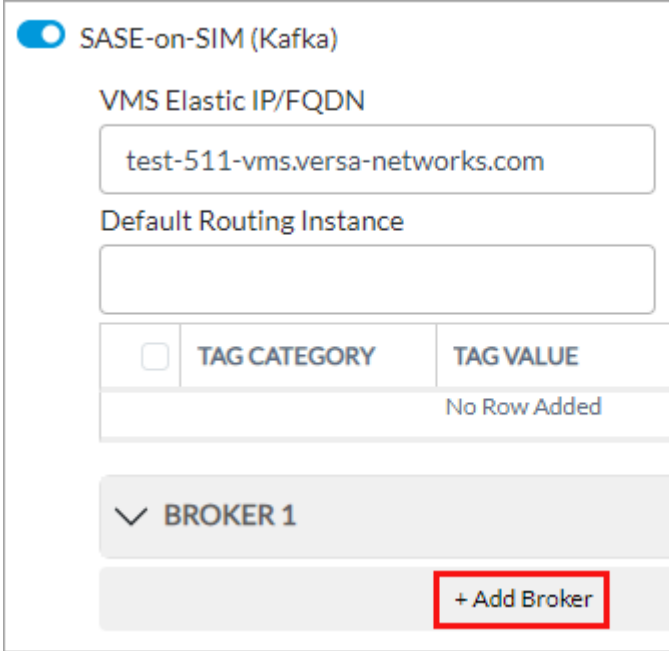
- ☐ Third-Party-Authentication
- ☐ XIP-EIP
- ☐ SASE-on-SIM (Radius)
- ☐ SASE-on-SIM (Kafka)



Field	Description
Third-Party Authentication	<p>Click the Third-Party Authentication toggle to enable third-party authentication. You can use third-party authentication to check and confirm user identity without requiring the user to perform any authentication action. When secure SD-WAN CPEs use VMS for third-party authentication, users do not have to authenticate themselves using a captive portal. VMS functions alongside the customer Active Directory (AD). When Active Directory authenticates a user, the Windows WMI agent notifies VMS about user login and logoff events. The notification contains information about the user IP address, which VMS disseminates to all secure SD-WAN devices in the network.</p> 
<ul style="list-style-type: none"> <li>VMS IP Address</li> </ul>	Enter the IP address of the VMS server that the Windows WMI agent notifies about user login and logoff events.
XIP EIP	<p>Click the XIP EIP toggle to enable XIP EIP. EIP converts Palo Alto Networks host information profile (HIP) reports into the VOS endpoint information profile (EIP) report format. You can configure VOS gateways to subscribe to XIP EIP, and you can then use these reports to enforce security policies. When you enable XIP, the following sequence of events occurs:</p> <ol style="list-style-type: none"> <li>1. Panorama sends syslog messages to the VMS Panorama agent.</li> <li>2. For syslog messages that require an action, the VMS Panorama agent retrieves HIP reports that include the device security postures. These syslog messages are: gateway register (for internal gateway users), gateway connected (for external gateway users), gateway logout, and gateway HIP report (check for device posture).</li> </ol>

	<p>updates).</p> <ol style="list-style-type: none"> <li>3. XIP EIP converts HIP reports to EIP format and shares the device name, username, IP address, and security posture with VMX.</li> <li>4. The messaging service establishes a TCP connection to all VOS devices and shares each device's EIP profile, which is used by the tenant for security enforcement. User traffic is allowed or denied based the NGFW access policy.</li> </ol> <p>For more information about EIP, see <a href="#">Configure Endpoint Information Profiles</a>.</p>
	
◦ Panorama Agent IP FQDN	Enter the elastic FQDN of the Panorama agent to configure on the VMS server. Panorama sends syslog messages to this FQDN.
◦ Panorama Agent Elastic IP	Enter the elastic IP address of the Panorama agent to configure on VMS server. Panorama sends syslog messages to this IP address.
◦ Panorama FW/Panorama IP/FQDN	Enter the IP address or FQDN of the Panorama host from which the VMS Panorama agent fetches the HIP report.

◦ Panorama FW/Panorama API Key	Enter the Panorama API key that fetches the Host Information Profile report from Panorama or Panorama firewall.
SASE on SIM (RADIUS)	<p>Click the SASE on SIM (RADIUS) toggle to enable SASE on SIM for RADIUS. SASE on SIM is a clientless solution that helps secure SIM-enabled IoT and user devices connected over 2G, 3G, 4G, and 5G networks. For more information, see <a href="#">Configure SASE for SIM</a>.</p> 
◦ VMS Elastic IP/FQDN	Enter the FQDN of VMS host to which the accounting server sends RADIUS accounting events. This value is same as the elastic FQDN of the VMS cluster.
◦ Default Routing Instance	Enter the IP address of the routing instance on the Versa Cloud Gateway (VCG) or SASE gateway (VOS device) to which the aggregator forwards the ingress traffic.

◦ RADIUS Server Password	Enter the password for the RADIUS server.
◦ Number of Missed Interims	Enter the total number of times an interim message can be missed before the entry is considered stale and is removed from the VMS and VOS. devices. A combination of this value and the keepalive interval is used to remove a user entry from the system.
◦ Keepalive Interval for Interim Updates	Enter the interval, in seconds, between two interim messages. For AAA, the range is 60 through 3600 seconds. For RADIUS, this is a user-defined value. The combination of this value and value in the Number of Misses Interims field is used to remove a user entry from the system.
SASE on SIM (Kafka)	<p>Click the SASE on SIM (Kafka) toggle to enable SASE on SIM for Kafka.</p> 
◦ VMS Elastic IP/FQDN	Enter the FQDN of VMS host to which the Kafka producer connects to VMS server. This value is same as the elastic FQDN of the VMS cluster.
◦ Default Routing Instance	Select the default routing instance on the VCG or SASE gateway (VOS device) to which the aggregator

	forwards the ingress traffic.
Tags	Enter information that describes all the services.
<ul style="list-style-type: none"> <li>◦ Tag Category</li> </ul>	<p>Select a category for the third-part service description:</p> <ul style="list-style-type: none"> <li>◦ Active Directory Domain Name</li> <li>◦ Name</li> <li>◦ Region</li> <li>◦ Custom</li> </ul>
<ul style="list-style-type: none"> <li>◦ Tag Value</li> </ul>	<p>Enter a value that corresponds to the value you select in the Tag Category field:</p> <ul style="list-style-type: none"> <li>◦ Active Directory Domain Name—Enter the AD domain name in which the VMS server is located.</li> <li>◦ Name—Enter a name for the VMS server.</li> <li>◦ Region—Enter the region in which the VMS server is located.</li> <li>◦ Custom—Enter a custom value.</li> </ul>
<ul style="list-style-type: none"> <li>◦ Tag Label</li> </ul>	Enter a text string that describes the third-party authentication service.

9. Click Next to go to Step 4, Review.

✓ VMS CONNECTION
✓ VMS CLUSTER
✓ TENANTS & SERVICES
4 REVIEW

Review

VMS Connector: test-511-vms1

---

**VMS Connection** [Edit](#)

**Name**  
VMS-Cluster-1

**Certificate**  
root-ca-cert.pem

**Cluster Details**

VMS IP Address / Fully Qualified Domain Name (FQDN)	Node Type	VMS Name
test-511-vms1.versa-networks.com	Active	test-511-vms1

---

**VMS Authentication** [Edit](#)

**Primary Director IP Address / Fully Qualified Domain Name (FQDN)**  
10.43.217.242

**Secondary Director IP Address / Fully Qualified Domain Name (FQDN)**  
10.43.217.243

**VMS Interface**  
192.168.51.11

**VMS Master Name**  
test-511-vms1

**Agent Interface**  
10.43.217.120

**Controller IP Address**  
192.168.51.4

**Controller Port**  
4321

---

**Tenant & Services** [Edit](#)

Tenants	Services
test-511-Provider-Org	sase-for-mobility-kafka , redis
Customer-1	third-party-authentication , redis

Cancel
Back
Submit

10. Review the information in all the sections. To make changes, click the Edit icon.
11. Click Submit.

---

## Configure VMS Messaging Service

You configure the VMS messaging service for your VOS device to communicate with the VMS server and to enable VMS services to send and receive stream feeds.

To configure the VMS messaging service, you do the following:

- Configure a messaging server profile for the VOS device to communicate with the VMS.
- Use the server profile to enable VMS services to send and receive stream feeds from the VMS server.

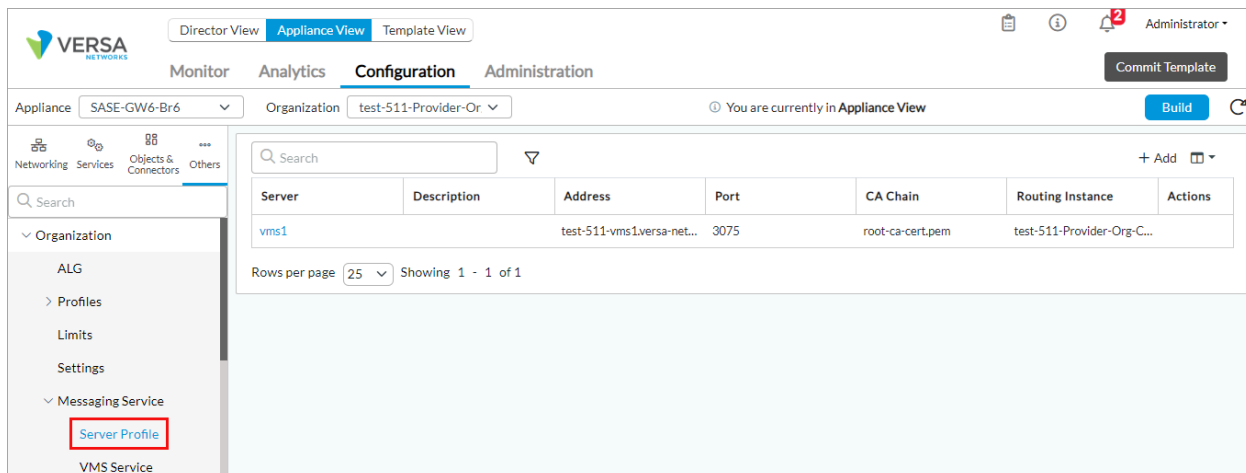
---

## Configure a Messaging Server Profile

You configure a messaging server profile for the VOS device to communicate with the VMS server.

To add a messaging server 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 > Messaging Service > Server Profile in the left menu bar.



4. Click the + Add icon. In the Add Messaging Service Server popup window, enter information for the following fields.

Add Messaging Service Server

Name \*

Description

Routing Instance \*

---Please Select---

CA Chain \*

default

Port

1024..65535

Address

FQDN \*

OK

Cancel



Field	Description
Name (Required)	Enter a name for the messaging server.  <i>Value:</i> Text string from 1 through 127 characters  <i>Default:</i> None
Description	Enter a text description for the VMS messaging server.
Routing Instance (Required)	Select the routing instance through which the VMS messaging server is reachable.
CA Chain (Required)	Select the certificate authority (CA) chain to use for the server. This adds the certificate file in Versa Director.
Port	Enter the port number for the VMS messaging server.  <i>Default:</i> 1376
Address	
◦ FQDN	Enter the fully qualified domain name of the messaging server.

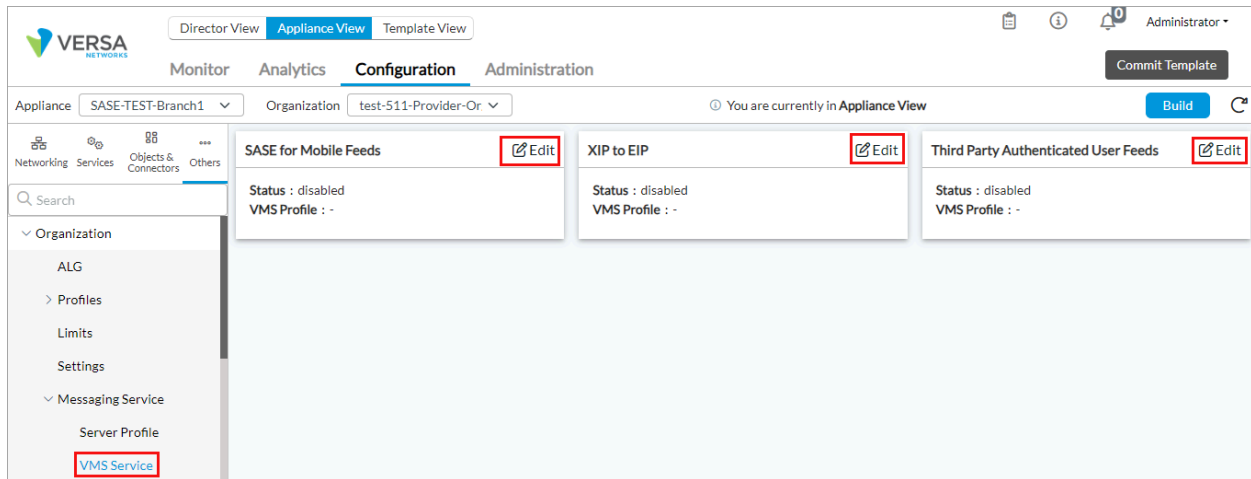
5. Click OK.


## Enable Stream Feeds for VMS Services

You can enable VMS services such as SASE on SIM, XIP EIP, and third party authentication to receive streaming feeds from the VMS server. To do this, you associate a messaging server profile with the services that you configured in [Configure a VMS Connector](#), above.

To enable a VMS service to send or receive streaming feeds:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select an Appliance 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 > Messaging Service > VMS Service in the left menu bar.



4. Click the  Edit icon next to a service. The Edit VMS Service popup window displays.

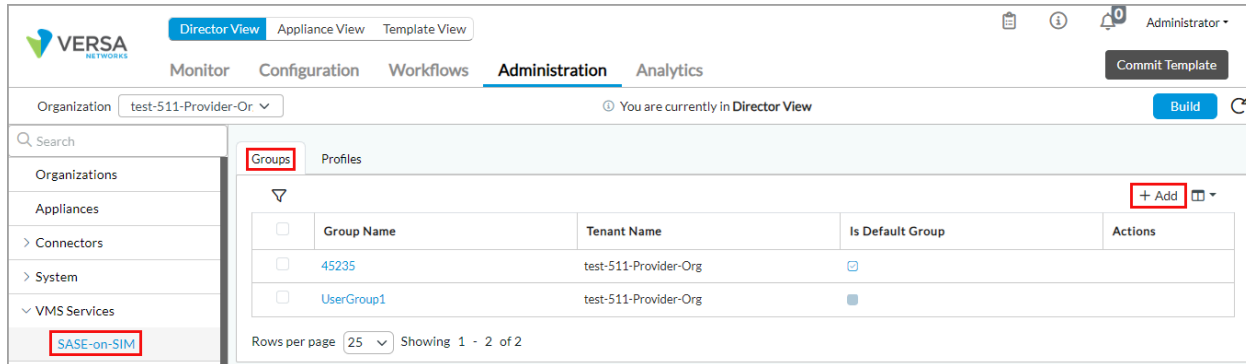
5. In the VMS Profile field, select a VMS server profile. For more information, see [Configure a Messaging Server Profile](#), above.
6. Click Enabled to enable the service.
7. (Optional) Enter tags for the VMS service, and then press Enter to add a tag.
8. Click OK.
9. Repeat Steps 4 to 8 for each service for which you want to enable stream feeds.

## Configure User Groups and Profiles for SASE on SIM

You configure SASE on SIM (or SASE for SIM) user groups to manage groups of mobile devices in a private mobile network. You then add profiles and associate groups with profiles. For more information, see [Configure SASE for SIM](#).

### Configure User Groups

1. In Director view, select the Administration tab in the top menu bar.
2. Select VMS Services > SASE-on-SIM in the left menu bar.



3. Select the Groups tab, and then click + Add. In the Add Groups popup window, enter information for the following fields.

### Add Groups

Group Name \*

Tenant Name \*

---Please Select---

Solution Tier \*

---Please Select---

☐ Is Default Group

OK

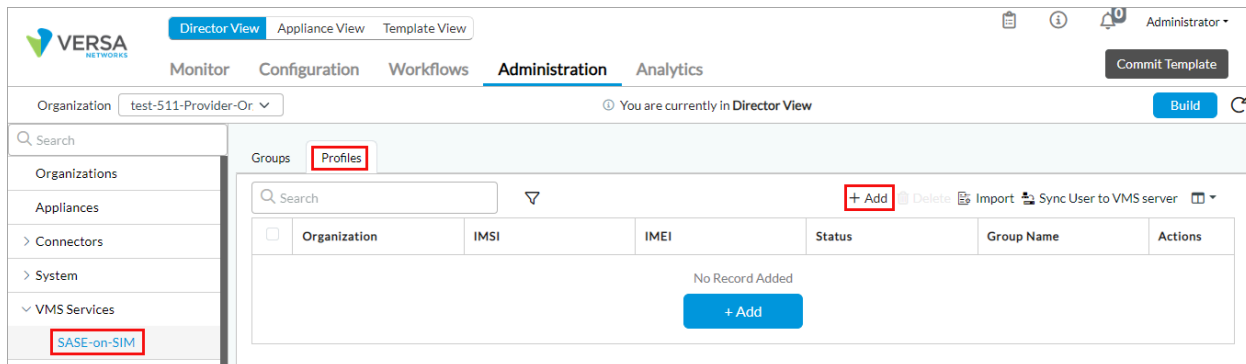
Cancel

Field	Description
Group Name	Enter a name for the user group.  <i>Value:</i> Text string from 1 through 32 characters.
Tenant Name	Select a Tenant to which the user group belongs.
Solution Tier	Select the product solution tier: <ul style="list-style-type: none"> <li>◦ VSA Essentials (Versa Secure Access)—Provides secure access to the internet for the service provider user.</li> <li>◦ SWG (secure web gateway)—Provides secure access to private enterprise resources for the service provider user.</li> <li>◦ Bundle—Provides secure access to the internet and private enterprise resources for the service provider user</li> </ul>
Is Default Group	Select to make this the default user group. Note than you can have only one default group for a tenant.

- Click OK.

## Configure User Profiles

- In Director view, select the Administration tab in the top menu bar.
- Select VMS Services > SASE-on-SIM in the left menu bar.



- Select the Profiles tab and click + Add. The Add Profiles popup windows displays.

Add Profiles

General
Users

Organization \*
test-511-Provider-Org
Solution Tier \*
VSA Essentials

IMSI \*
IMEI
☐ Enable IMEI lock

MSISDN
Status
---Please Select---

Group ID
SOC Code

Tags
Add Tag

User Groups

User Groups

---Please Select---

No Records to Display

OK
Cancel

- Select the General tab, and then enter information for the following fields.

Field	Description
Tenant Name	Select a Tenant to which the user group belongs.
Solution Tier	<p>Select the product solution tier:</p> <ul style="list-style-type: none"> <li>◦ VSA Essentials (Versa Secure Access)—Provides secure access to the internet for the service provider user.</li> <li>◦ SWG (secure web gateway)—Provides secure access to private enterprise resources for the service provider user.</li> <li>◦ Bundle—Provides secure access to the internet and private enterprise resources for the service provider user</li> </ul>
IMSI	Enter the international mobile subscriber identity (IMSI) to authorize devices in a network.
IMEI	Enter the 15-digit International Mobile Equipment Identity (IMEI) number of the device.
MSISDN	Enter the Mobile Station International Subscriber Directory Number (MSISDN), which is the phone number associated with a single SIM card and is the number to which you call or send an SMS message.
Status	<p>Select the status:</p> <ul style="list-style-type: none"> <li>◦ New</li> <li>◦ Claimed</li> <li>◦ Deployed</li> </ul>
Group ID	Displays the group identifier associated with the user groups you select from the User Groups field.
SOC Code	Enter the 12-bit System Operator Code (SOC) that identifies a service provider. A mobile station uses SOC along with System Identity (SID) to acquire or reject services offered by specific service providers.
Tags	Enter tags to identify the profile. Press Enter to add the tags.
User Groups	Select a user group to associate with the profile. For more information, see <a href="#">Configure User Groups</a> , above.

5. Select the Users tab, and then enter information for the following fields.

[https://docs.versa-networks.com/Management\\_and\\_Orchestration/Versa\\_Messaging\\_Service/Passive\\_Authentication/01\\_Co...](https://docs.versa-networks.com/Management_and_Orchestration/Versa_Messaging_Service/Passive_Authentication/01_Co...)

Updated: Wed, 23 Oct 2024 08:49:43 GMT

Copyright © 2024, Versa Networks, Inc.

Add Profiles

General
Users

Locale

Custom Variables

Field 1
Field 2
Field 3

OK
Cancel

Field	Description
Locale	Enter the geographic location of the users.
Custom Variables	Enter user variables to associate with the profile.

6. Click OK.

## Supported Software Information

Versa Director Releases 22.1.4 and later support all content described in this article.

VMS Releases 5.1.1 and later support all content described in this article.

## Additional Information

[Configure SASE for SIM](#)

[Versa Analytics Configuration Concepts](#)