

# VMware Secure Access Configuration Guide

VMware Secure Access

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2023 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

- 1** About VMware Secure Access 4
- 2** About VMware Secure Access System Components 6
- 3** Get Started with VMware Secure Access Deployment 7
- 4** Deploy Secure Access Service Using SASE Orchestrator 9
- 5** Turn On Secure Access Service at the Profile or Edge Level 16
- 6** Enroll Devices with Workspace ONE Intelligent Hub 18
- 7** Monitor Secure Access Service Using the SASE Orchestrator 19
  - Secure Access Logs 19

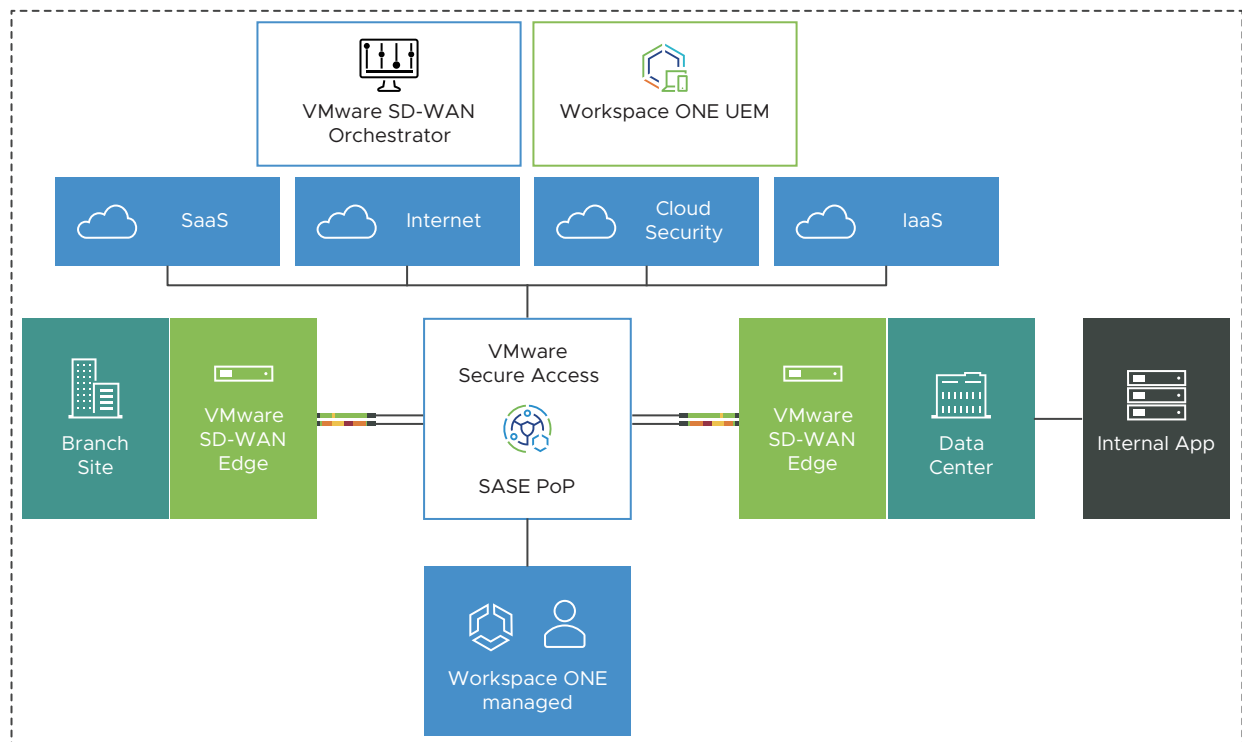
# About VMware Secure Access

1

VMware Secure Access™ is a remote access solution that is based on a Zero Trust Network Access (ZTNA) framework. The cloud-hosted solution offers multiple benefits over traditional VPN solutions, enabling users a consistent, optimal, and secure cloud application process.

The solution leverages VMware's global Points of Presence (PoPs) footprint and optimizes traffic handling capabilities for lower latency and better application performance, enabling customers to provide a branch-like experience to remote workers.

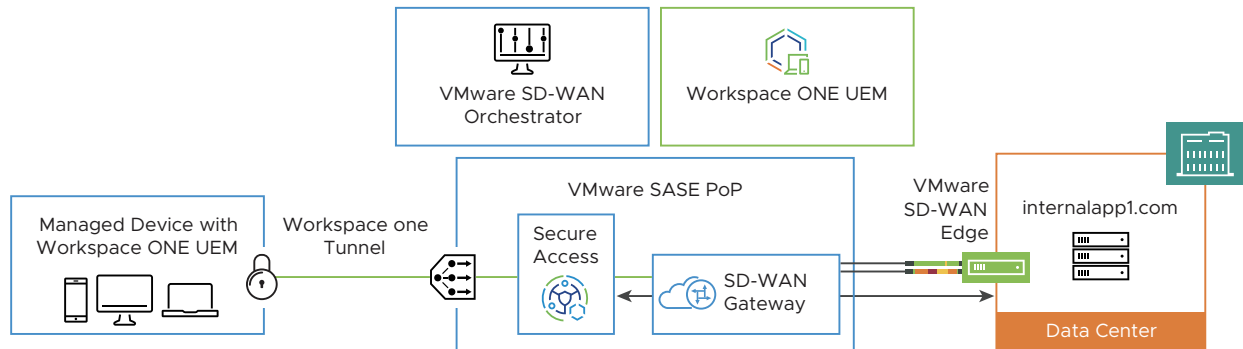
The following diagram illustrates the VMware Secure Access architecture:



- Consistent QoS policies across WAN
- Integrated & consistent WAN firewall policies
- Resilient (DPMO) access to DC hosted apps
- Dynamic tunneling to sites & DC (lower latency & contention)

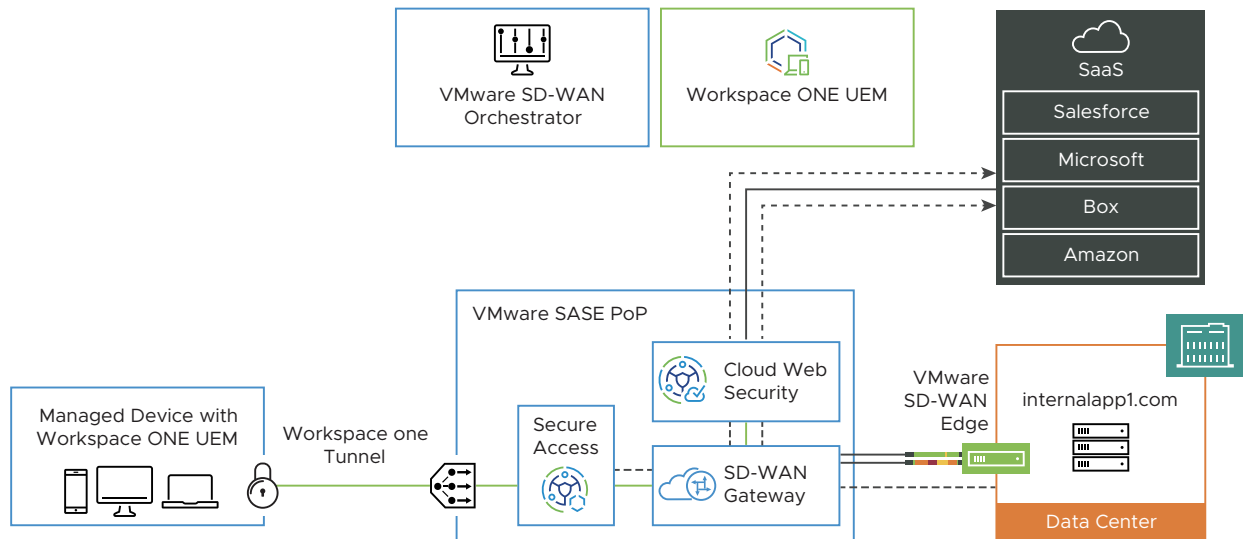
VMware Secure Access empowers remote users with access to cloud-based applications that are optimized for delivery and performance, leverages security and benefits of a cloud-hosted solution, and eases IT deployment and maintenance of costly remote access services.

The following diagram depicts the packet flow using Secure Access:



This integration allows customers to deliver a branch-like experience to remote workers. This is a hosted service meaning customers will not have to deploy and manage the VMware Unified Access Gateway component for tunnel use cases, delivering improved IT efficiency.

The following diagram depicts the packet flow using Secure Access and Cloud Web Security:



Remote users can enjoy improved performance as they access data behind the firewall. The ability to leverage global Points of Presence (PoPs) and optimized traffic handling capabilities helps to lower latency and drive better performance.

# About VMware Secure Access System Components

## 2

Following are the system components of VMware Secure Access:

- Workspace ONE UEM Console—Administrators use the Workspace ONE UEM Console through a Web browser to secure, configure, monitor, and manage devices and their access policies. The UEM Console has multiple deployment options including on-premise and hosted.
- VMware SASE Orchestrator—The VMware SASE Orchestrator provides centralized enterprise-wide installation, configuration, and real-time monitoring in addition to orchestrating the data flow through the cloud network. The SASE Orchestrator enables one-click provisioning of virtual services in the branch, the cloud, or the enterprise datacenter.
- VMware SD-WAN Edge (Optional)—VMware SD-WAN Edges are zero-touch enterprise-class appliances that provide secure optimized connectivity to private, public, and hybrid applications, compute, and virtualized services. SD-WAN Edges perform deep application recognition, application and packet steering, performance metrics, and end-to-end quality of service in addition to hosting virtual network function (VNF) services.

# Get Started with VMware Secure Access Deployment

## 3

To get started with VMware Secure Access, you must perform certain configurations on the Workspace ONE UEM to work with the tunnel service that will be deployed by Secure Access and provided as a service.

You can enroll existing users and groups of directory services such as Active Directory (AD), Lotus Domino, and Novell e-Directory. If you do not have such an infrastructure or choose not to integrate with it, you must manually create user accounts and perform basic enrollment in Workspace ONE UEM.

Perform the following tasks to complete basic enrollment in Workspace ONE UEM:

Step	Task	Refer to
1.	Create a new tenancy that includes parent and child organization groups. Organization groups are created for each business entity where devices are deployed.	<a href="#">Create Organization Groups</a>
2.	Create an administrator account and assign the organization group and role for the administrator.	<a href="#">Create an Admin Account</a>
3.	Create the required basic user accounts.	<a href="#">Create Basic User Accounts</a>
4.	Configure a Workspace ONE UEM tunnel. Keep in mind the following points when you configure the tunnel: <ul style="list-style-type: none"><li>■ Make a note of the Hostname that you enter when you configure this tunnel and ensure that you provide the same Hostname when you provision VMware Secure Access.</li><li>■ The domain suffix must be ".sa.gsm.vmware.com" as the tunnel server is hosted in a VMware SASE POP.</li><li>■ Use either port number 443 (recommended) or 8443 for the tunnel traffic.</li></ul>	<a href="#">Configure Per-App Tunnel</a>

Step	Task	Refer to
5.	Configure device traffic rules. You can define traffic rules for either Full Device or Per-Application.	<ul style="list-style-type: none"> <li>■ <a href="#">Create Device Traffic Rules</a></li> <li>■ <a href="#">Configuring Device Traffic Rules for iOS</a></li> <li>■ <a href="#">Configuring Device Traffic Rules for macOS</a></li> <li>■ <a href="#">Configuring Device Traffic Rules for Windows 10</a></li> <li>■ <a href="#">Configuring Device Traffic Rules for Android</a></li> </ul>
6.	Create a Per-App VPN Profile. Per-App VPN profile allows you to force selected applications to connect through your corporate VPN. Your VPN provider must support this feature, and you must publish the applications as managed applications. The VPN profile that you create is used to configure the Workspace ONE Tunnel client on the device to allow only designated applications to access content on internal servers.	<ul style="list-style-type: none"> <li>■ <a href="#">Creating Per-App VPN Profile for iOS</a></li> <li>■ <a href="#">Creating Per-App VPN Profile for macOS</a></li> <li>■ <a href="#">Creating Per-App VPN Profile for Windows 10</a></li> <li>■ <a href="#">Creating Per-App VPN Profile for Android</a></li> </ul>
7.	Deploy the Workspace ONE UEM tunnel that you created in step 4 on the managed devices.	<ul style="list-style-type: none"> <li>■ <a href="#">Distributing Workspace ONE Tunnel for iOS</a></li> <li>■ <a href="#">Distributing Workspace ONE Tunnel for macOS</a></li> <li>■ <a href="#">Distributing Workspace ONE Tunnel for Windows 10</a></li> <li>■ <a href="#">Distributing Workspace ONE Tunnel for Android</a></li> </ul>



# Deploy Secure Access Service Using SASE Orchestrator

## 4

To deploy VMware Secure Access service using SASE Orchestrator:

### Prerequisites

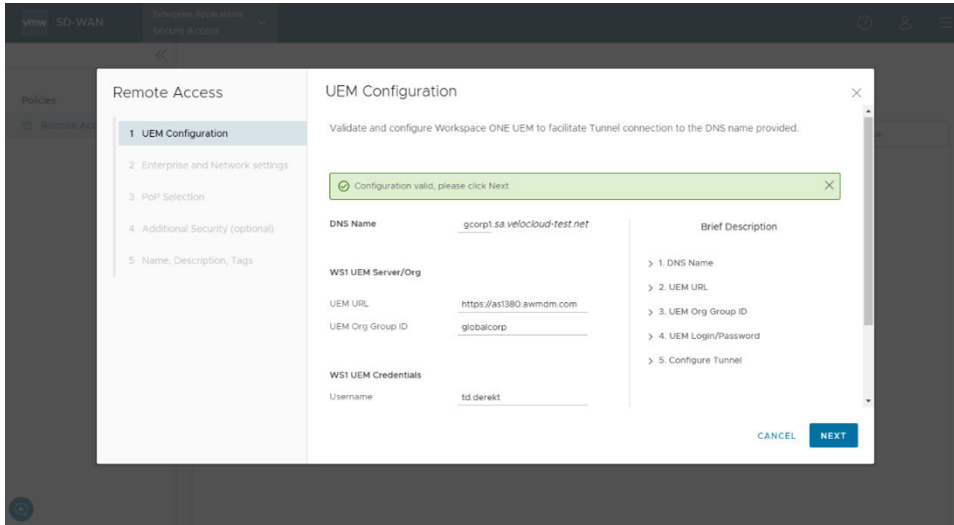
- Ensure that you have completed the required configuration on Workspace ONE UEM. For details, refer to [Chapter 3 Get Started with VMware Secure Access Deployment](#).
- Ensure that you have set the maximum number of PoPs for Secure Access in SASE Orchestrator. The maximum number depends on the number of VMware SASE PoPs deployed on the SASE Orchestrator. To set the maximum number of PoPs, go to **Configure > Customer > Customer Configuration > Service Access**.

### Procedure

- 1 Log in to SASE Orchestrator as an Enterprise user, and then click **Open New Orchestrator UI**.
- 2 In the **New Orchestrator UI** modal pop-up that appears, click **Launch New Orchestrator UI**.
- 3 From the **Enterprise Applications SD-WAN** drop-down list, select **Secure Access**.
- 4 In the **Secure Access** page that appears, click **+ New Service**.  
The **Remote Access** Wizard appears.
- 5 In the **UEM Configuration** screen of the **Remote Access** Wizard, complete the following configurations:
  - a In the **DNS Name** field, enter the hostname that you provided when you configured the Workspace ONE UEM tunnel. Refer to step 4 in [Chapter 3 Get Started with VMware Secure Access Deployment](#).
  - b In the **UEM URL** field, enter the Workspace ONE UEM API URL related to your UEM environment.
  - c In the **UEM Org Group ID** field, enter the organization group identifier that you created during the Workspace ONE UEM configuration. Refer to step 1 in [Chapter 3 Get Started with VMware Secure Access Deployment](#).
  - d In the **WS1 UEM Credentials** section, enter the username and password that you had set up when you created the administrator account in the Workspace ONE UEM console. Refer to step 2 in [Chapter 3 Get Started with VMware Secure Access Deployment](#).

- e Select the **Yes** check box to configure the UEM tunnel hostname within the organization group that you had created.
- f Click **Check**.

An API call is made to the UEM server to validate the details that you have entered. Once the validation is successful, click **Next**.



- 6 In the **Enterprise and Network settings** screen of the **Remote Access** Wizard, complete the following configurations:
  - a From the **Enterprise DNS Server** drop-down list, select the required DNS server configured for the Enterprise. The default is **Google** or **OpenDNS**.
  - b From the **SD WAN Segment** drop-down list, select the required segment for which you want to enable the **Secure Access** service. The default is **Global Segment**.

c In the **Enterprise IP Ranges** section, enter the following details:

- **Customer Subnet**—This is a subnet owned by the customer that will be used by remote users when accessing the network. This Customer Subnet functions as a super net that will be divided and distributed among as many SASE PoPs as the user has configured for their deployment (up to five PoPs can be configured).
- **Subnet Bits**—Configure from 1 to 3 Subnet Bits to divide the Customer Subnet into individual subnets that can be allocated to the PoPs.

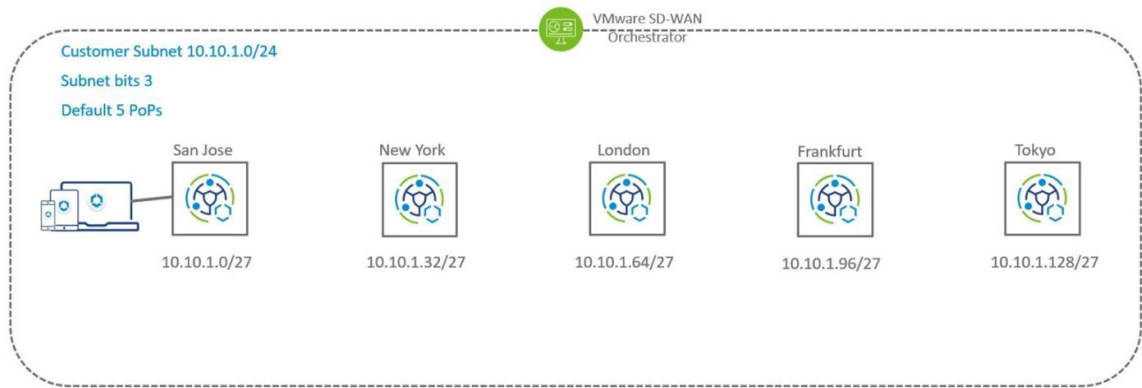
The following table illustrates the relation between the Customer Subnet and Subnet Bits:

Customer Subnet	Subnet Bits	Number of Subnets	Subnet per PoP
10.10.1.0/24	1	2	<ul style="list-style-type: none"> <li>■ 10.10.1.0/25</li> <li>■ 10.10.1.128/25</li> </ul>
10.10.1.0/24	2	4	<ul style="list-style-type: none"> <li>■ 10.10.1.0/26</li> <li>■ 10.10.1.64/26</li> <li>■ 10.10.1.128/26</li> <li>■ 10.10.1.192/26</li> </ul>
10.10.1.0/24	3	8	<ul style="list-style-type: none"> <li>■ 10.10.1.0/27</li> <li>■ 10.10.1.32/27</li> <li>■ 10.10.1.64/27</li> <li>■ 10.10.1.96/27</li> <li>■ 10.10.1.128/27</li> <li>■ 10.10.1.160/27</li> <li>■ 10.10.1.192/27</li> <li>■ 10.10.1.224/27</li> </ul>

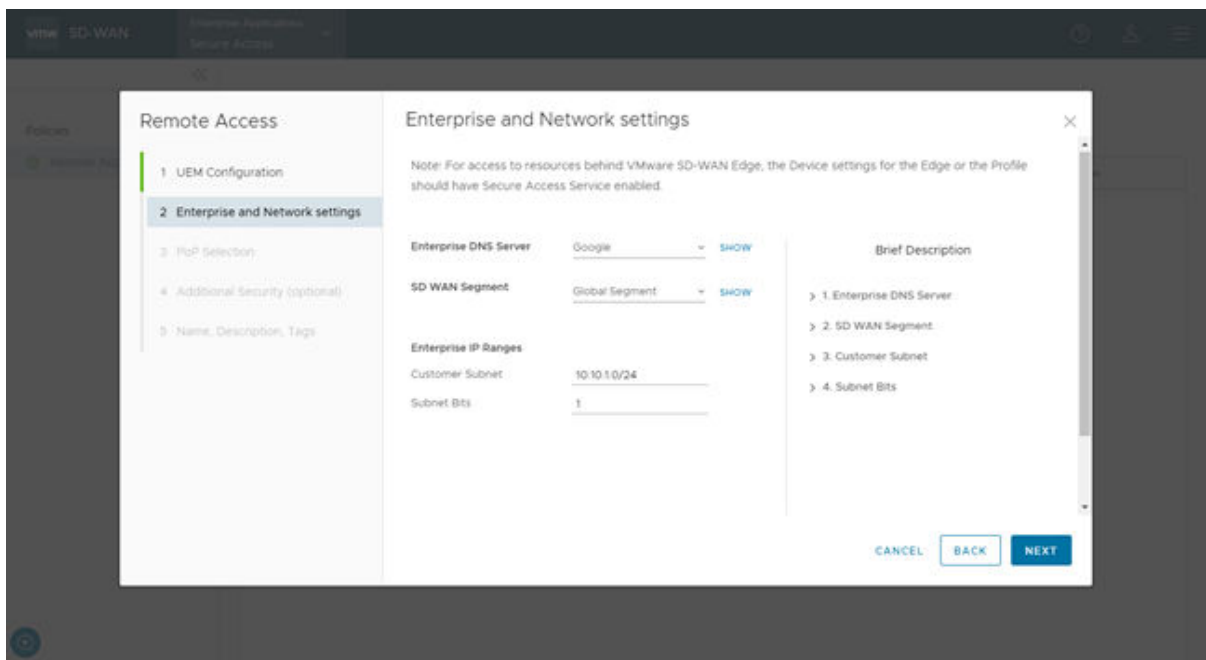
The number of Subnet Bits chosen determines the number of subnets that will be created from the Customer Subnet. As noted in the above table if you configure:

- One Subnet Bit, the Customer Subnet is divided into two subnets, which can be assigned to two PoPs.
- Two Subnet Bits, the Customer Subnet is divided into four subnets, which can be assigned to four PoPs.
- Three Subnet Bits, the Customer Subnet is divided into eight subnets, which can be assigned to a maximum of five PoPs and three subnets will remain unallocated.

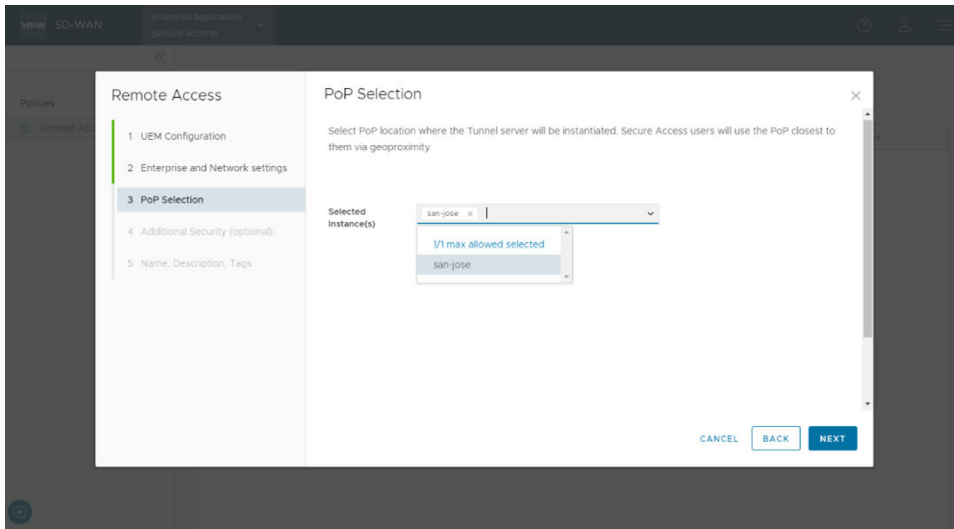
Following diagram depicts the relation between Customer Subnet and Subnet Bits:



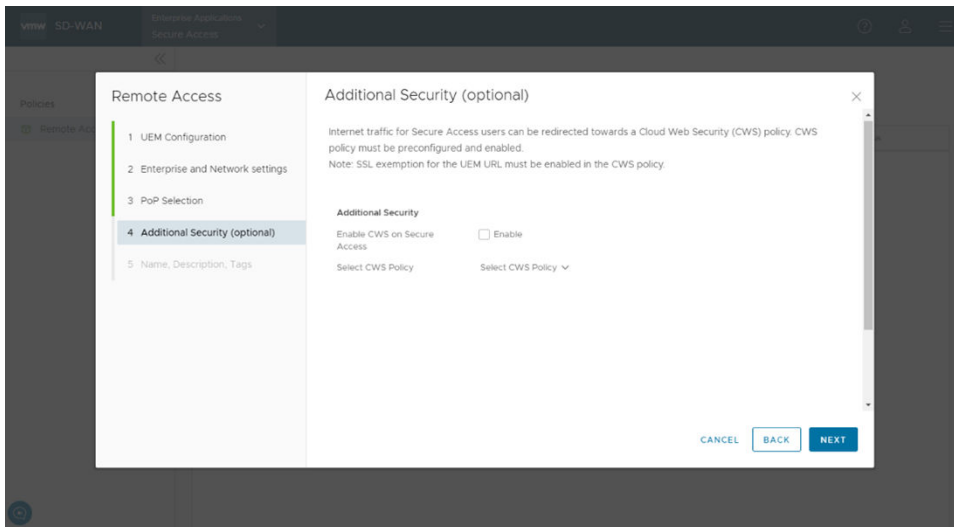
d Click **Next**.



- 7 In the **PoP Selection** screen of the **Remote Access** Wizard, from the **Selected Instance(s)** drop-down list, select the PoP location where the tunnel server will be instantiated. Click **Next**.

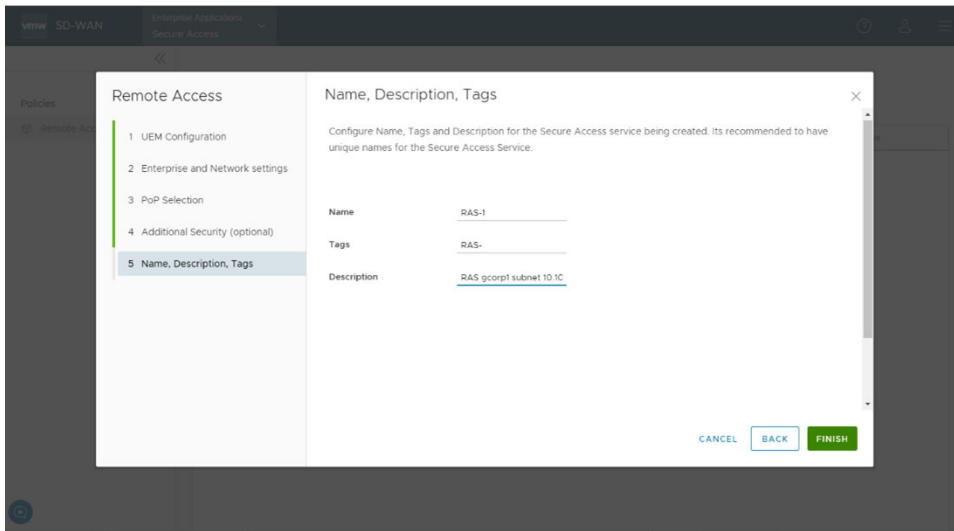


- 8 In the **Additional Security (optional)** screen of the **Remote Access** Wizard, you can choose to enable Cloud Web Security on Secure Access.



If Cloud Web Security is enabled, ensure that an SSL Inspection (Secure Socket Layer) Bypass/Exemption Rule is created in the CWS Policy under the SSL Inspection section. The default behavior of SSL Inspection is to decrypt all encrypted traffic. Creating SSL rules is covered in detail in the Cloud Web Security Configuration Guide. The rule will cover destination traffic sent to domain awmdm.com and will ensure that CWS does not decrypt this traffic. Click **Next**.

- 9 In the **Name, Description, Tags** screen of the **Remote Access** Wizard, enter the name of the Secure Access service, and add any tags or description, if required, and then click **Finish**.



## Results

It may take a few minutes to bring the tunnel server online and establish connectivity to the SASE PoP. The deployments status shows **In Progress** while the provisioning is taking place. Refresh the page to check the status. Once the tunnel server is established, the deployment status shows **Completed**.

See the table below for a description of the column titles for a secure access service.

## What to do next

You must enroll your devices with the Workspace ONE Intelligent Hub application. Refer to [Chapter 6 Enroll Devices with Workspace ONE Intelligent Hub](#).

## Modify and Update Tunnel Services

### Edit or Delete a Secure Access Service

After you have created a new service using the steps described in the previous section, you can **Edit**, **Delete**, or **Restart** the service. Select the service you want to edit or delete by clicking the check box next to the **Service Name**. Click **Edit** to make changes to the Workspace ONE UEM Configuration dialog. Click **Delete** to delete the Secure Access service.

### Restart the Secure Access Service

The Restart feature in the **Secure Access Policies** screen, updates the UEM tunnel server version the customer is using to the latest version, which includes more bug fixes and the log management feature. During UEM tunnel server update, users will be momentarily disconnected in batches, and then reconnected automatically. After this process is complete, user logs will be viewable via Monitor > Logs > Secure Access Logs in the Enterprise Secure Access Portal.

To Restart the Secure Access Service, click the checkbox next to the appropriate Service Name and click **Restart**.

**What to do next:**

View Secure Access logs via Monitor > Logs > Secure Access Logs in the Enterprise Secure Access Portal.

# Turn On Secure Access Service at the Profile or Edge Level

## 5

This section covers the Secure Access Service option found at either the Profile or Edge level: where the option is located, what the option does, and which customers should turn it on or leave it off.

### Secure Access Service

The **Secure Access Service** option can be turned on at either the Profile or Edge level by navigating to **Configure > Device > Configure Segments**. When **Secure Access Service** is set to On, the Edge builds tunnels to all Secure Access Gateways.



**Note** This setting must be turned on for Secure Access users to reach applications sitting behind that Edge.

By default, the Edge only builds tunnels to the Primary, Secondary, and Super Gateways based on the geolocation of the Edge. These Gateways can be different from the Gateways in use for Secure Access. For example, if an Edge located in Japan builds a tunnel to the Tokyo PoP, by default it does not build a tunnel to the New York PoP even though the New York PoP is where VMware Secure Access is being used.

If the Edge uses Secure Access without also turning on **Secure Access Service** option, this can cause issues due to the Edge having no tunnels to the New York PoP. Turning on **Secure Access Service** corrects this issue.

**Note** To see which Gateways are being used for a particular Edge, including the ones for Secure Access, go to **Remote Diagnostics > List Paths**.

The **Secure Access Service** option is recommended for customer sites with two exceptions:

- 1 A customer site has no applications on their premises that need to be accessed by users at other locations.



- 2 Turning on the **Secure Access Service** option incurs an additional five tunnels to be built which could exceed the tunnel capacity for entry level Edge models like the 510, 610, and 620. Usually a site with a lower-end Edge will have no applications that need to be accessed by other users and the option can safely be left off. The primary use case for this option is Hub Edge locations where on-premises applications usually reside. Hub Edges are usually higher-end models that can handle the additional five tunnels that are built when this option is on.

# Enroll Devices with Workspace ONE Intelligent Hub

## 6

You must first download and install the Workspace ONE Intelligent Hub app from <https://getwsone.com>, and then enroll your devices. For instructions, refer to the following topics:

- [macOS Device Enrollment](#)
- [Android Device Enrollment Overview](#)
- [Enrolling Windows 10 Devices into Workspace ONE UEM](#)
- [Enroll iOS Devices](#)

# Monitor Secure Access Service Using the SASE Orchestrator

## 7

This section describes how to monitor VMware Secure Access Service feature.

The following monitoring capabilities for Secure Access are displayed under Monitor in the navigation panel.

- [Secure Access Logs](#)

This chapter includes the following topics:

- [Secure Access Logs](#)

## Secure Access Logs

The Secure Access Log feature displays enterprise-level analytics based on the logs received from the tunnel service.

The 5.2 release supports the VMware Secure Access Log Management feature, which displays information for analyzing and debug purposes. Customers can also search/filter logs based on a broad spectrum of log parameters in the VMware SASE Orchestrator under **Secure Access Logs**.

### About this task:

- The Secure Access Logs feature supports 100 entries per page (to see beyond 100 entries, go to the next page).
- By default, the maximum log storage retention is seven days.
- Make sure your tunnel server version supports logging. If necessary, upgrade to the latest version of the tunnel server, which can be accomplished by going to the **Secure Access Policies** screen (Configure > Secure Access Policies) and clicking **Restart**.

---

**Note** When you click **Restart**, the tunnel sever gets updated to the latest version, which includes the Secure Access Log management feature. As the tunnel server restarts, users will get disconnected in batches momentarily and will get automatically reconnected. When this process is complete, Secure Access Logs will be visible in the **Secure Access Logs** page.

---

To view secure access logs:

- 1 In the Secure Access service of the Enterprise Portal, go to **Monitor > Secure Access Logs**. See image below.

Connection Time	Device User Name	Device Name	Device App	Remote Host Name	Remote Host IP	Connection	PoP Name	Flow ID	Session ID
May 17, 2023, 9:07:12 AM	sakhter.adm	EC2AMAZ-1G9RHOD	chrome	googleads.g.doubleclick.net	142.250.189.162	Stream	sjc2-ge	13905	10013
May 17, 2023, 9:06:30 AM	sakhter.adm	EC2AMAZ-1G9RHOD	chrome	safebrowsing.googleapis.com	142.250.189.234	Stream	sjc2-ge	13900	10013
May 17, 2023, 9:06:18 AM	sakhter.adm	EC2AMAZ-1G9RHOD	vpnagent	::ffff:8.8.4.4	8.8.4.4	Datagram	sjc2-ge	50002	10013
May 17, 2023, 9:06:18 AM	sakhter.adm	EC2AMAZ-1G9RHOD	chrome	android.clients.google.com	142.251.46.238	Stream	sjc2-ge	13908	10013
May 17, 2023, 9:06:18 AM	sakhter.adm	EC2AMAZ-1G9RHOD	vpnagent	::ffff:8.8.8.8	8.8.8.8	Datagram	sjc2-ge	50001	10013
May 17, 2023, 9:03:12 AM	sakhter.adm	EC2AMAZ-1G9RHOD	chrome	googleads.g.doubleclick.net	142.250.189.162	Stream	sjc2-ge	13905	10013
May 17, 2023, 9:02:30 AM	sakhter.adm	EC2AMAZ-1G9RHOD	vpnagent	::ffff:8.8.4.4	8.8.4.4	Datagram	sjc2-ge	50002	10013

2 See the table below for information about the Secure Access Logs screen.

Field	Description
Connection	Displays if the connection from the user device is a Session (tunnel client connecting to Tunnel service running in the PoP) or UDP datagram/TCP stream from user applications.
Connection Status	Displays status of the connection: Connected, Disconnected, or Closed.
Connection Time	Time of the event.
Connection Type	Displays the type of connection.
Device User Name	The ID the user used to log into Tunnel Client.
Device Name	The device name used to connect to the Secure Access service.
Device App	Name of the application running on the device that is accessing the resources.
Device VPN IP	Displays the device VPN IP.
Device UID	Displays the device UID.
Remote Host Name	The hostname of the resource being accessed by the application on the device (domain of the destination host).
Remote Host IP	The destination IP address of the flow.
Remote Host Port	
PoP Name	Name of the SASE PoP. This field displays the name of the PoP that user is connected to via Secure Access Service.
Flow ID	Displays the ID of the flow.

Field	Description
Session ID	Displays the ID of the session.
VPN Server IP	The IP Address assigned to Tunnel Server instance running in the SASE PoP.

3 Select a log to display more details, as shown in the image below.

The screenshot shows the VMware Secure Access Logs interface. On the left, there is a sidebar with 'Monitor' and 'Configure' tabs. Under 'Monitor', there are 'Events', 'Secure Access Events', and 'Logs'. The 'Logs' section is expanded, showing 'Secure Access Logs'. The main area displays a table of logs with columns for Date, User, Device Name, Remote Host Name, Connection, Flow ID, Remote Host Port, Connection Type, VPN Server IP, Device User Name, Device App, Remote Host IP, PoP Name, Session ID, Connection Status, Device UID, and Device VPN IP. A log entry is selected, and its details are shown in a 'Log Entry Details' section below the table.

Date	User	Device Name	Remote Host Name	Connection	Flow ID	Remote Host Port	Connection Type	VPN Server IP	Device User Name	Device App	Remote Host IP	PoP Name	Session ID	Connection Status	Device UID	Device VPN IP
May 17, 2023, 9:06:18 AM	sakhter.adm	EC2AMAZ-1GR6HOD	chrome	vpnagent	53	142.250.189.162	UDP	10.0.0.2	sakhter.adm	vpnagent	8.8.8.8	sjc2-qe	50001	Connected	2445736bda1e4135bd02ef8ba04025f0	172.31.19.90

**Log Entry Details**

Connection Time	May 17, 2023, 9:06:18 AM	Device User Name	sakhter.adm
Device Name	EC2AMAZ-1GR6HOD	Device App	vpnagent
Remote Host Name	::ffff:8.8.4.4	Remote Host IP	8.8.4.4
Connection	Datagram	PoP Name	sjc2-qe
Flow ID	50002	Session ID	10013
Remote Host Port	53	Connection Status	Connected
Connection Type	UDP	Device UID	2445736bda1e4135bd02ef8ba04025f0
VPN Server IP	10.0.0.2	Device VPN IP	::ffff:172.31.19.90

4 Use the Search/Filter feature to specify a specific time period and to find relevant logs.

- In the top, left corner of the **Secure Access Logs** page, select **Custom** from the drop-down menu, as shown in the image below.
- Click the **Calendar** icons to indicate your start to finish dates for your custom search.

The screenshot shows the VMware Secure Access Logs search interface. At the top, there is a 'Custom' search filter. Below it, there is a date range selector with '05/08/2023 02:45' as the start date and '05/08/2023 14:45' as the end date. An 'APPLY' button is visible to the right of the date range.

- Click the **Filters** button to open the filters dialog, as shown in the image below. In this dialog, indicate your filter parameters by selecting a filter name and using "is" or "contains" to refine the search. Click the **Apply** button when finished to conduct the search.

The screenshot shows the VMware Secure Access Logs filters dialog. At the top, there is a 'Custom' search filter. Below it, there is a date range selector with '05/08/2023 02:45' as the start date and '05/08/2023 14:45' as the end date. An 'APPLY' button is visible to the right of the date range. Below the date range, there is a 'FILTERS' button. The filters dialog is open, showing a list of filters: 'Device Name', 'Flow ID', and 'Remote Host IP'. Each filter has a dropdown menu for the operator and a text input for the value. The 'Device Name' filter is set to 'is' and 'test1'. The 'Flow ID' filter is set to 'is' and '123'. The 'Remote Host IP' filter is set to 'contains' and '127'. There is a '+', 'CLEAR', 'CLOSE', and 'APPLY' button at the bottom of the dialog. A message at the bottom states 'No items available as per selected filter criteria'.