

Configure and Troubleshoot Secure Access (SSE) Integration on Catalyst SD-WAN

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Cisco Secure Access](#)

[Preliminary configurations](#)

[Create Loopback Interfaces](#)

[Configure New API Keys on SSE Portal](#)

[Configure SSE on Catalyst Manager](#)

[Set up Cloud Credentials](#)

[Configure SSE Tunnels Using Policy Group](#)

[Configure Policy Group](#)

[Configure Policy Group to Redirect Traffic to SSE](#)

[Verify](#)

[Manager](#)

[Secure Access Dashboard](#)

[Command Line Interface \(CLI\) Commands](#)

Introduction

This document describes how to configure the active-active SSE integration on Catalyst SD-WAN and guides troubleshooting it.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Software-Defined Wide Area Network (SD-WAN)
- Configuration Groups
- Policy Groups

Components Used

The information in this document is based on these software and hardware versions:

- C8000V version 17.15.02
- vManage version 20.15.02

- Cisco Secure Access account

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Cisco Secure Access

Cisco Secure Access is a cloud-based Security Service Edge (SSE) solution that converges multiple network security services, delivering them from the cloud to support a hybrid workforce. Cisco SD-WAN Manager leverages REST APIs to retrieve policy information from Cisco Secure Access and distributes this information to Cisco IOS XE SD-WAN devices. This integration enables seamless, transparent, and secure Direct Internet Access (DIA) for users, allowing them to connect from any device, anywhere, securely.

Cisco SSE allows SD-WAN devices to establish connections with SSE providers using IPSec tunnels. This document is intended for users of Cisco Secure Access.

Preliminary configurations

- Enable Domain Lookup for the Device: Navigate to **Configuration Groups > System Profile > Global** and enable **Domain Lookup**.



Note: By default, Domain Lookup is disabled.

- Configure DNS: The Router can resolve DNS and access the internet on VPN 0.
- Configure NAT DIA: The DIA configuration needs to be present on the router where the SSE tunnel is created.

Create Loopback Interfaces

If both tunnels in an Active/Active configuration connect to the same destination data center and use the same WAN interface as the source, then two loopback IP addresses need to be created.



Note: When two tunnels are configured with the same source and destination, IKEv2 forms an identity pair consisting of a Local ID and a Remote ID. By default, the Local ID is the IP address of the tunnel's source interface. This identity pair must be unique and cannot be shared between two tunnels. To prevent confusion within the IKEv2 state, each tunnel uses a different loopback interface as its source. Although IKE packets are translated (NATed) on the DIA interface, the Local ID remains unchanged and retains the original loopback IP address.

1. Navigate to **Configuration > Configuration Groups > Configuration Group Name > Transport & Management Profile** > click on **Edit**.
2. Click on the **plus** sign (+) on the right side of the transport VPN Profile (main profile). This opens an **Add Feature** menu located at the far right.
3. Click on **Ethernet Interface**. It adds a new internet interface under **Transport VPN**.

Transport VPN

edge_basic_vpn0

Ethernet Interface

Select Ethernet Interface

Ethernet Interface

edge_basic_vpn0

Ethernet Interface

edge_basic_vpn0_inet

Back No Changes Made

4. Create the two Loopback interfaces using RFC1918 IPv4 addresses, as the Loopback0 example in the picture.

Ethernet Interface

Name: Loopback0

Description(optional):

Basic Configuration | Ether Channel | Tunnel | NAT | ARP | ACL/QoS | Advanced

Shutdown: ☐ ☒

Interface Name: Loopback0

Description: <SYSTEM DEFAULT>

Service Provider: <SYSTEM DEFAULT>

Bandwidth Upstream: <SYSTEM DEFAULT>

Bandwidth Downstream: <SYSTEM DEFAULT>

Auto Detect Bandwidth: ☐ ☒

IPv4 Settings

☐ Dynamic ☒ Static

IP Address: 10.1.1.1

Subnet Mask: /32 255.255.255.255

Cancel Save

Transport VPN

edge_basic_vpn0

Ethernet Interface: Loopback1

Ethernet Interface: Loopback0

Ethernet Interface: edge_basic_vpn0_mpls

Ethernet Interface: edge_basic_vpn0_inet

New Loopback interfaces

Back All Changes Saved

- After applying the loopback configuration, proceed to deploy the configuration change to the device. Notice that the provisioning status changes from **1/1** to **0/1**.

Name	Type	Profile	Provisioning Status ¹ Sync Devices / Associated Devices	Origin	Updated By
Hub2-SIG	Single Router	4	 0 / 1	user	cisco

Configure New API Keys on SSE Portal

1. Access to the SSE Portal <https://login.sse.cisco.com/>
2. Navigate to **Admin > API Keys**



Home



Experience
Insights



Connect



Resources



Secure



Monitor

Admin



Account Settings

Accounts

Authentication

Management

API Keys

Third-party Integrations

Log Management

Subscription

Integrations

6. Copy the API key and Key Secret into a notepad and select **ACCEPT AND CLOSE**

Click Refresh to generate a new key and secret.

API Key

[Redacted API Key]



Key Secret

[Redacted Key Secret]



Copy the Key Secret. For security reasons, it is only displayed once. If lost, it cannot be retrieved.

ACCEPT AND CLOSE

7. Under the URL <https://dashboard.sse.cisco.com/#some-numbers#/admin/apikeys> the **#some-numbers#** is your organisation ID. Copy that information into your notepad as well.



Discover your SSE organization ID

Configure SSE on Catalyst Manager

Set up Cloud Credentials

1. Navigate to **Administration > Settings > Cloud Credentials > Cloud Provider Credentials**, and enable **Cisco Secure Access** and enter the details.

Settings / External Services

Cloud Credentials

Cloud Provider Credentials

Umbrella DNS Certificate

Configure Cisco Umbrella, Zscaler, and Cisco Secure Access credentials to enable Cisco Catalyst SD-WAN Manager to create automatic SIG tunnels to Cisco Umbrella or Zscaler endpoints.

☐ Umbrella

☐ Zscaler

☒ Cisco SSE

Organization Id

Api Key

Secret

☒ Context Sharing

2. **Optional:** You can enable context sharing for enhanced functionality. For more information, please refer to the [Cisco SSE User Guide on context sharing](#).

Configure SSE Tunnels Using Policy Group

On the SD-WAN Manager navigate to **Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge** and click on **Add Secure Service Edge (SSE)**.

Cisco Catalyst SD-WAN

The network is out of compliance due to licensing, please [click here](#) for more actions.

Snooze

Monitor

Configuration

Analytics

Workflows

Tools

Resource

SSE-Policy

SSE Provider


☒ Cisco Secure Access ☐ Zscaler

In order to proceed, it is required to first create SSE Credentials in Administration Settings. Creation of SSE Credentials is a one-time process.

[Click here to add cisco-sse credentials](#)

Cancel

Save

 **Note:** If cloud credentials have not been configured yet, you can add them at this step. If credentials have already been configured, they are loaded automatically.

Add cisco-sse Credentials



Cisco SSE Organization Id*

[Redacted]

Cisco SSE API Key*

[Redacted]

Cisco SSE API Secret*

..... [SHOW](#)



Context Sharing

[Cancel](#)

[Add](#)

1. Configure the SSE Tracker. In this example, the tracker URL is set to <http://www.cisco.com>, and the source IP address is assigned from one of the loopback interfaces.

Add Tracker



Name



cisco-tracker

API URL Of Endpoint



<http://www.cisco.com>

Threshold



300

Probe Interval



60

Multiplier



3

[Cancel](#)

[Add](#)

SSE-Policy

SSE Provider
☒ Cisco Secure Access ☐ Zscaler

Context Sharing
☒ VPN ☐ SGT

Tracker
Source IP address

[+ Add Tracker](#)

Name	Threshold	Interval	Multiplier	API URL Of Endpoint	Action
cisco-tracker	300	60	3	http://www.cisco.com	

1 Record

Items per page: 5 1 of 1 |< < > >|

Optionally, since context sharing was enabled when the cloud credentials were configured, **VPN** is selected as the option in this example.

2. Click on **Add Tunnel**

Configuration
[+ Add Tunnel](#)

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
There is no data.					

0 Record

Items per page: 5 0 of 0 |< < > >|

Region
☒ Auto

3. In this example, the Loopback0 interface is used as the tunnel source, while the GigabitEthernet1 interface serves as the WAN interface to route traffic.

Add Tunnel

Tunnel Type

☒ ipsec

Interface Name(1..255)

Tunnel Source Interface*

Tracker

Tunnel Route-via Interface

Data Center

☒ Primary ☐ Secondary

[> Advanced Options](#)

Cancel

Add

Since the tracker was configured in this example, the setting is changed to **Global**, and the preconfigured **cisco-tracker** is selected.

4. For the second tunnel, repeat the same steps using the same parameters, but change the Interface Name from ipsec1 to ipsec2, and the Source Interface Name to Loopback1.



Add Tunnel

Tunnel Type

☒ ipsec

Interface Name(1..255)



ipsec2

Tunnel Source Interface*



Loopback1

Tracker



cisco-tracker



Tunnel Route-via Interface



GigabitEthernet1

Data Center

☒ Primary

☐ Secondary

> Advanced Options

Cancel

Add

Both tunnels are configured to be active simultaneously, without a backup.

5. Click on **Add Interface Pair**.

6. Click on **Add**. The active interface is set to ipsec1, and no backup interface is specified.



Add Interface Pair

Active Interface



ipsec1



Active Interface Weight



1

Backup Interface



None



Backup Interface Weight



1

Cancel

Add

7. The same operation is repeated for the second tunnel, ipsec2.

Configuration
+ Add Tunnel

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1		☑ false	☑	⊕ 1400	✎ ✕
ipsec2		☑ false	☑	⊕ 1400	✎ ✕

2 Records

Items per page: 5 1 - 2 of 2 [[<](#) [>](#)]

Region
 Auto

High Availability
+ Add Interface Pair

Active Interface	Active Interface Weight	Backup Interface	Backup Interface Weight	Action
ipsec1	⊕ 1	⊕ None	⊕ 1	✎ ✕
ipsec2	⊕ 1	⊕ None	⊕ 1	✎ ✕

2 Records

Items per page: 5 1 - 2 of 2 [[<](#) [>](#)]

8. Save the configuration.

Configure Policy Group

1. You can just select the policy previously created within the policy group and save.

Policy Groups

Policy Group 1 Application Priority & SLA 0 NGFW 0 Secure Internet Gateway / Secure Service Edge 2 DNS Security 0

+ Add Policy Group Export Import

As of: 29 de julio de 2025, 1:09 p.m.

Search

Name	Description	Number of Policies	Number of Devices	Devices Up to Date	Updated By	Last Updated On	Actions
PG-SSE-C8V							⋮ ^

Policy Group Name

Description(optional)

Application Priority

NGFW

Secure Internet Gateway / Secure Service Edge

DNS Security

Device Solution

Type sdwan

Deployment

Associated + Add

[Save](#) [Deploy](#)

2. Once the device or devices have been associated with the policy group, proceed to deploy the policy group.

PG-SSE-C8V

Policy Group Name

Description(optional)

Application Priority

NGFW

Secure Internet Gateway / Secure Service Edge

DNS Security

Device Solution

Type sdwan

Deployment

Associated 1 device

[Save](#) [Deploy](#)

Configure Policy Group to Redirect Traffic to SSE

1. On the SD-WAN Manager, navigate to **Configuration > Policy Groups > Application Priority & SLA**.

- Select **Add Application Priority & SLA Policy**
- Specify a name for the policy.

Policy Groups

Policy Group 1 **Application Priority & SLA** 0 NGFW 0 Secure Internet Gateway / Secure Service Edge 2 DNS Security 0



No Application Priority & SLA policy added, add your first Application Priority & SLA policy

[Add Application Priority & SLA Policy](#)

2. Once the new policy is displayed, select the **Advanced Layout** toggle.

Policies > Application Priority & SLA
SSE-Redirect [✎](#)

[Additional Settings](#) Advanced Layout ☒

3. Select **Add Traffic Policy List**.

- Configure the VPNs to redirect traffic to the SSE tunnel.
- Set the **Direction** and the **Default Action** as needed and **save**.

Edit Traffic Policy List

Policy Name

SSE-Redirect

VPN(s)

edge_basic_vpn1

Direction

Service

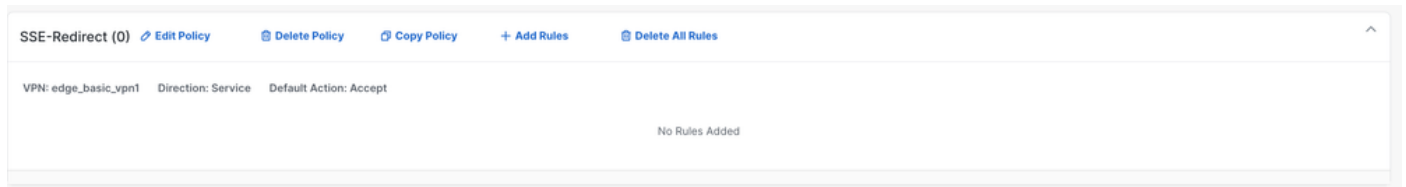
Default Action

☒ Accept ☐ Drop

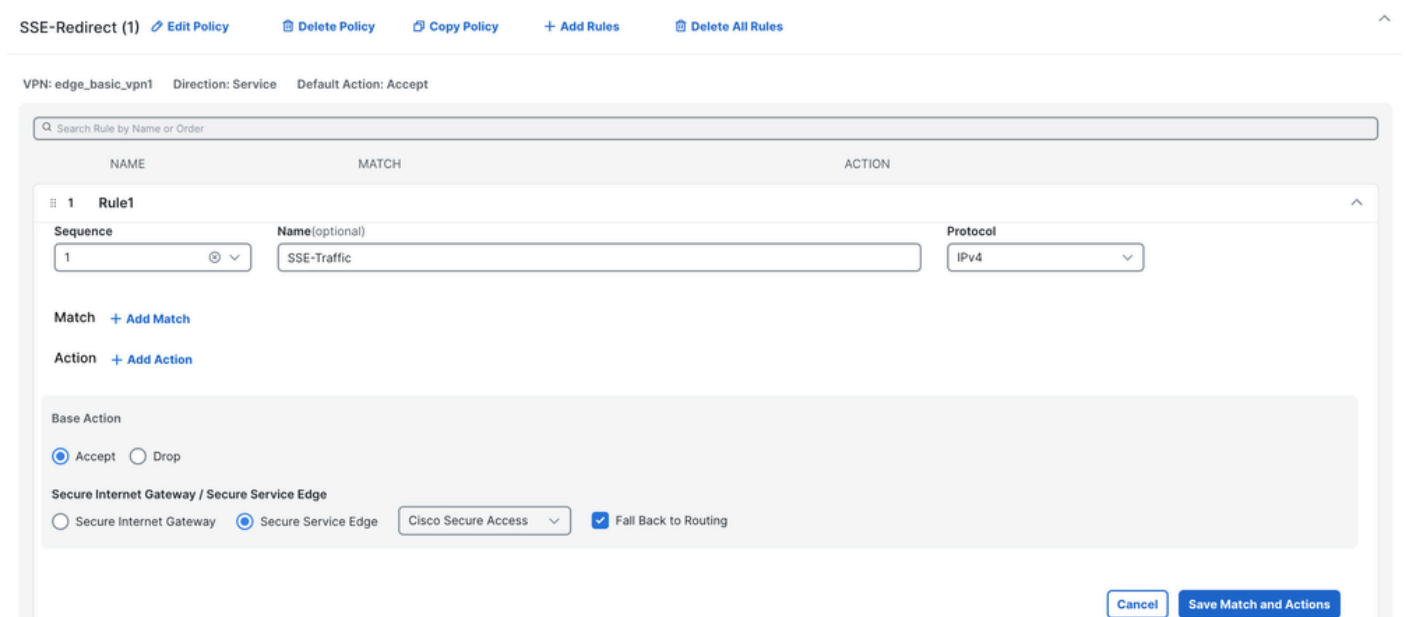
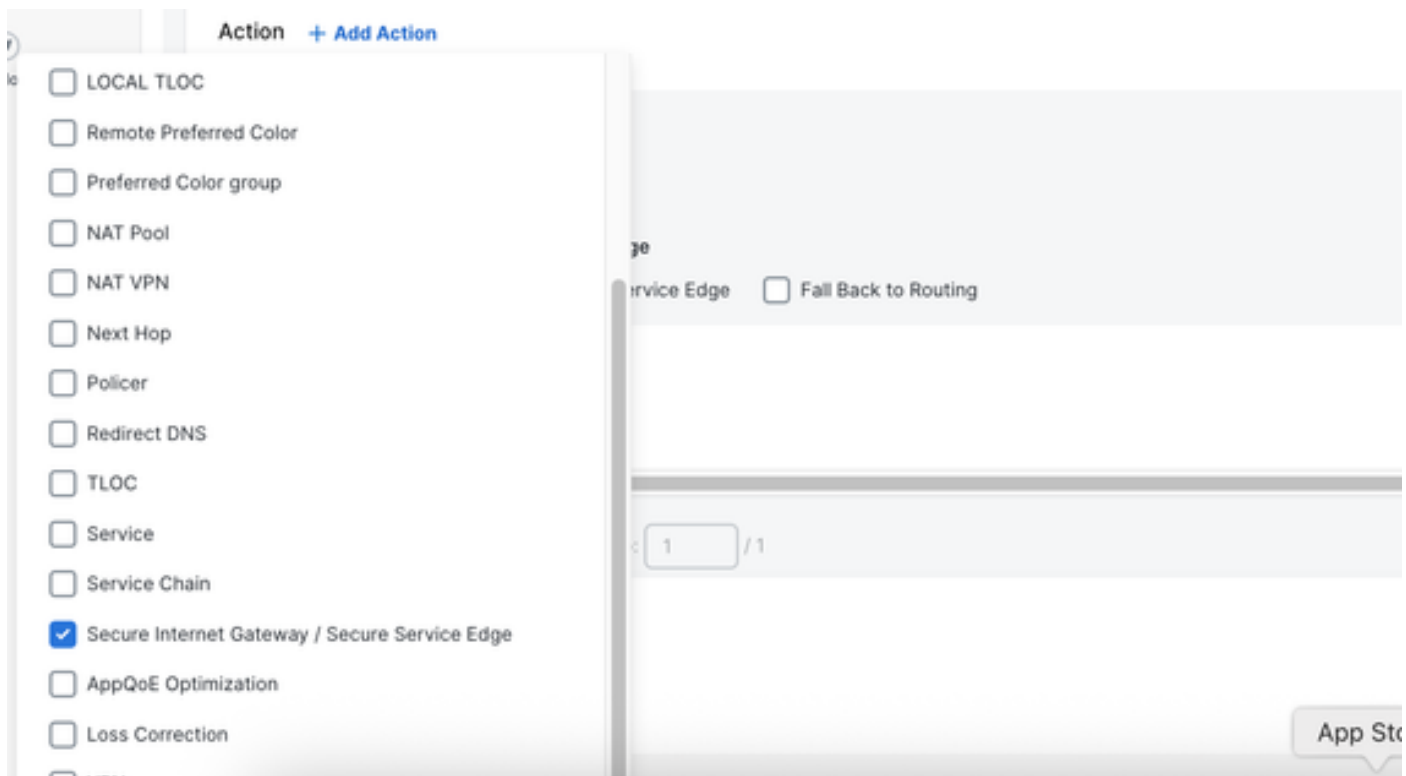
[Cancel](#)

[Save](#)

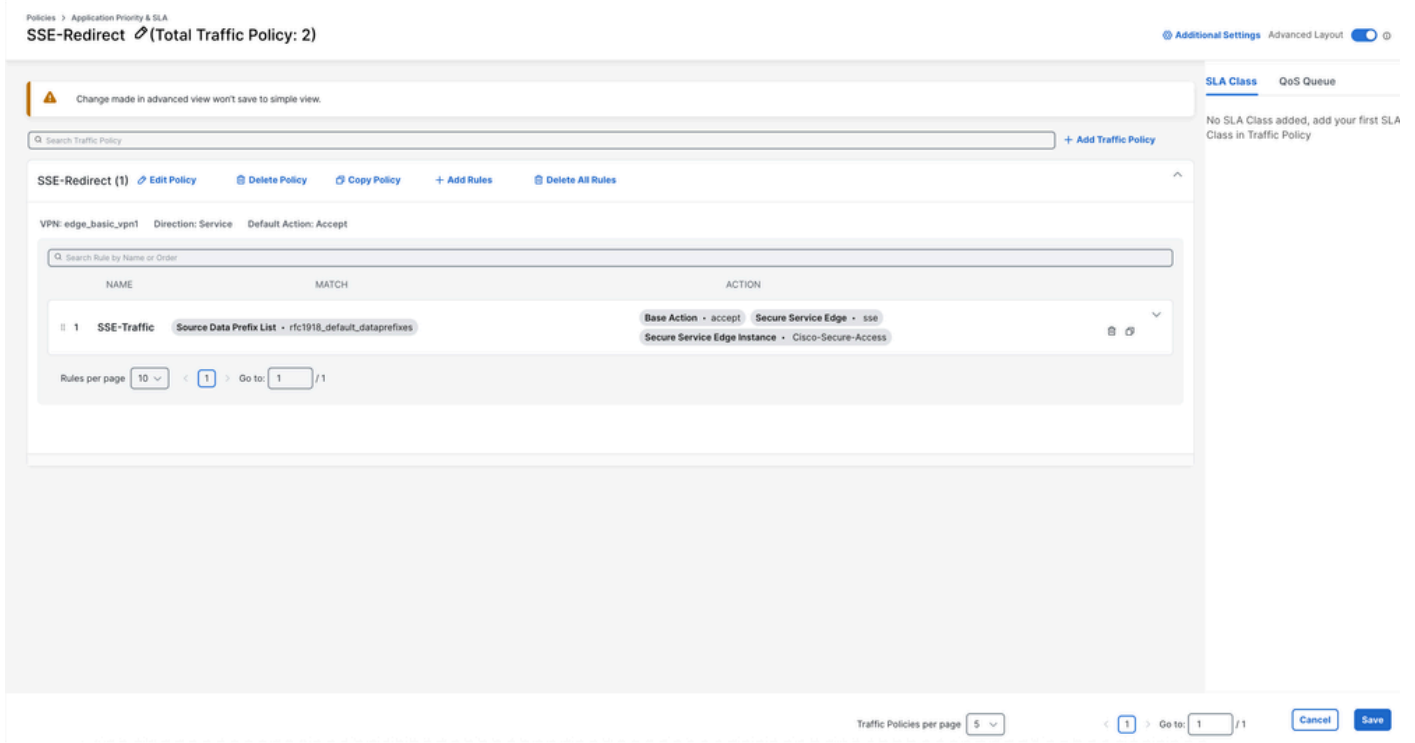
4. Select + **Add Rule**.



5. Configure your match traffic criteria to redirect traffic to the SSE.
6. Select **Accept** as the base action, then click on **+ Action**.
7. Look for the **Secure Internet Gateway / Secure Service Edge** action and set it to **Secure Service Edge**.



8. Click on **Save Match and Actions**



9. Click on **Save**.

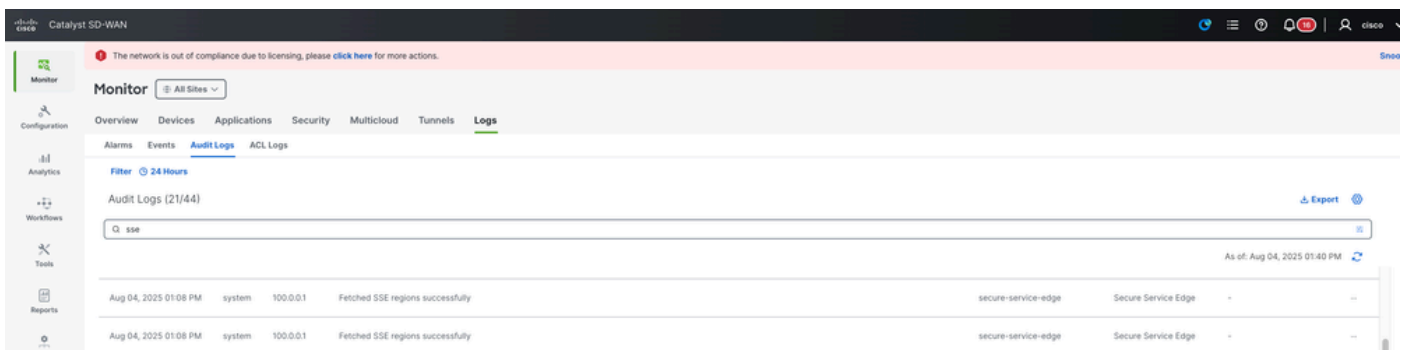
10. Navigate to **Configuration > Policy Groups** and select the **Application Priority** policy you just created. **Save** and then **Deploy**.



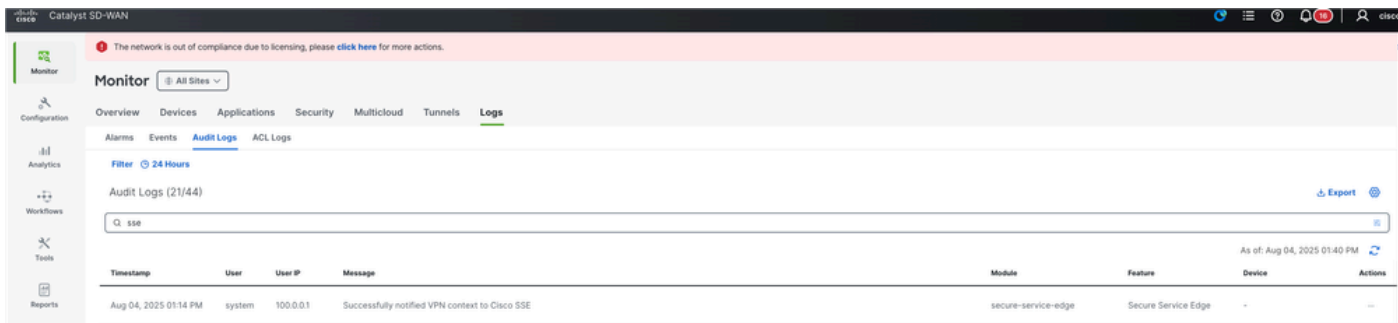
Verify

Manager

1. **Monitor > Logs > Audit Logs** and search for "sse".



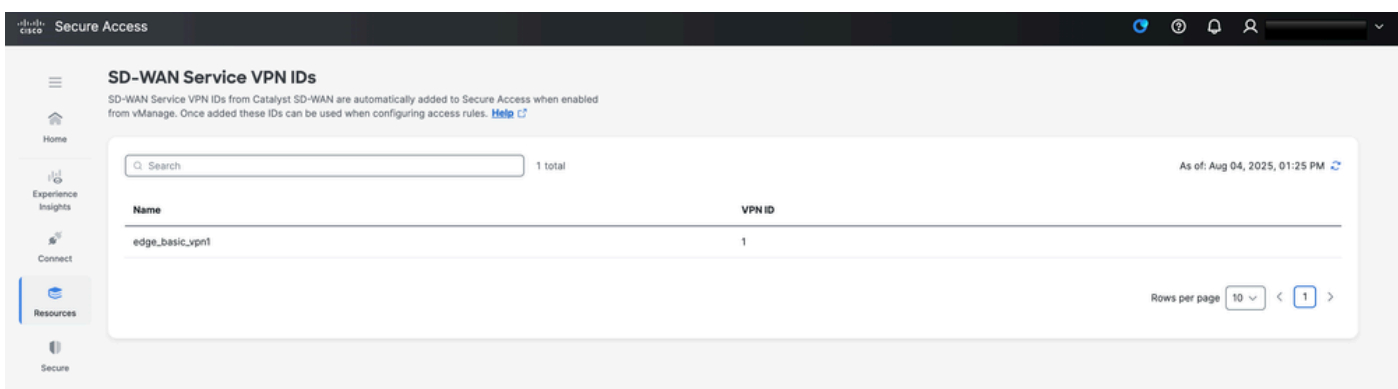
2. You can verify if the context sharing VPN is enabled successfully by checking the Manager.



Secure Access Dashboard

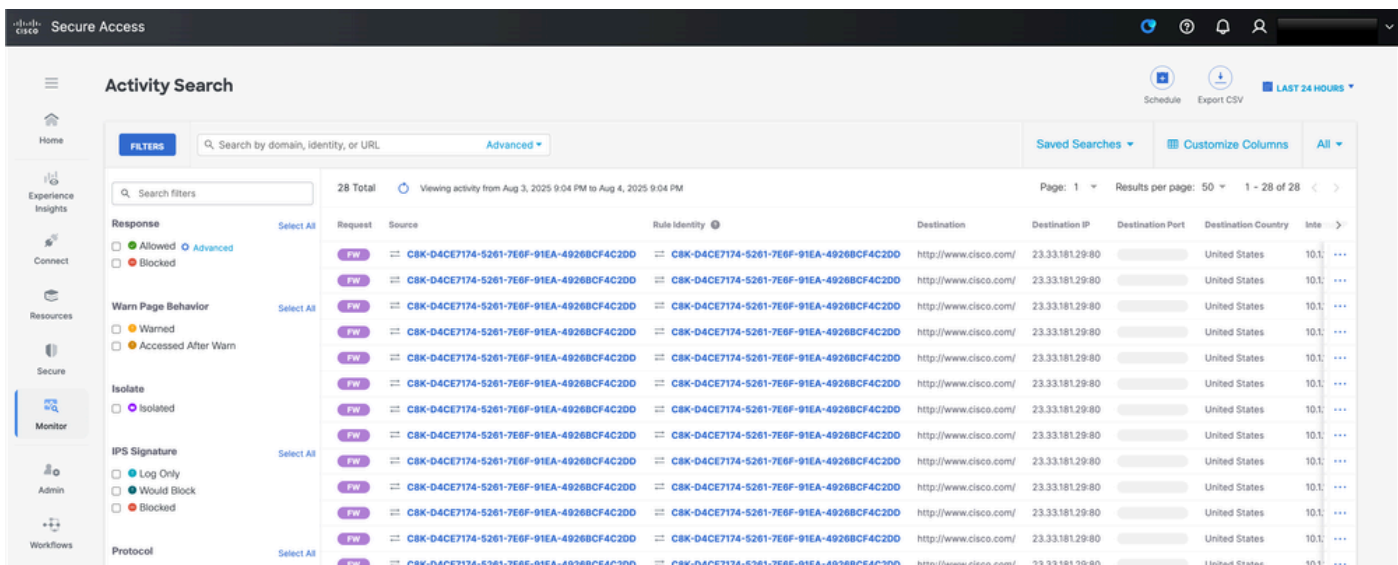
Context Sharing

You can verify if the context sharing VPN is enabled successfully by checking the SSE dashboard, **Resources > SD-WAN Service VPN IDs**



Tunnel Up

When the tunnel is up and the tracker is operational with traffic flowing through the tunnel, you can validate this by navigating to **Monitor > Activity Search**. On this screen, you see traffic passing through the tunnel, such as requests to www.cisco.com generated by the tracker. This visibility confirms that the tracker is up and actively monitoring traffic through the tunnel



Comand Line Interface (CLI) Commands

<#root>

Hub2-SIG#show sse all

SSE Instance Cisco-Secure-Access

Tunnel name : Tunnel16000001

Site id: 2

Tunnel id: 655184839

SSE tunnel name: C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD

HA role: Active

Local state: Up

Tracker state: Up

Destination Data Center: 44.217.195.188

Tunnel type: IPSEC

Provider name: Cisco Secure Access

Context sharing: CONTEXT_SHARING_SRC_VPN

Related Information

- [Configure Context Sharing SD-WAN](#)
- [Cisco Secure Access Integration with SD-Routing](#)
- [Technical Support & Documentation - Cisco Systems](#)