

Prisma SD-WAN CloudBlade Integrations

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2024-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

April 2, 2025

Table of Contents

AWS Transit Gateway CloudBlade Integration.....	5
AWS and Prisma SD-WAN CloudBlade Prerequisites.....	7
Configure the AWS Transit Gateway Integration.....	10
Configure and Install the AWS Transit Gateway Integration CloudBlade.....	11
Validate the AWS Transit Gateway Integration CloudBlade.....	13
Setup Application Path Policy Rules.....	16
Manage, Monitor, and Troubleshoot the AWS Transit Gateway Integration CloudBlade.....	18
Azure Virtual WAN with vION CloudBlade Integration.....	23
Plan the Azure Virtual WAN with vION Integration.....	27
Configure the Azure Virtual WAN with vION CloudBlade.....	31
Validate the Azure Virtual WAN Integration CloudBlade.....	34
Manage and Monitor the Azure Virtual WAN with vION CloudBlade.....	37
Azure Virtual WAN CloudBlade Integration.....	39
Azure vWAN and Prisma SD-WAN CloudBlade Prerequisites.....	40
Create and Acquire the Azure Information.....	43
Configure and Install the Azure Virtual WAN CloudBlade.....	49
Assign tags to objects in the Prisma SD-WAN.....	50
Validate the Prisma SD-WAN Configuration.....	52
Edit Application Network Path Policy Rules.....	54
Manage and Troubleshoot the Azure vWAN CloudBlade.....	56
Chatbot CloudBlade for Slack Integration.....	59
Configure Chatbot CloudBlade for Slack.....	60
Install Prisma SD-WAN Chatbot via Slack Authentication.....	62
Chatbot Supported Commands.....	64
Manage and Monitor the Chatbot CloudBlade for Slack Integration.....	74
Chatbot MS Teams CloudBlade Integration.....	77
Create User Groups and Configure Chatbot MS Teams.....	78
Configure Chatbot MS Teams.....	80
Assign Chatbot to a Channel/Team.....	81
Chatbot Supported Commands.....	81
GCP-NCC CloudBlade Integration.....	93
Plan the GCP-NCC CloudBlade Integration.....	95
Configure GCP-NCC CloudBlade.....	97
Configure GCP-NCC CloudBlade in Prisma SD-WAN.....	99

Validate the GCP-NCC Integration CloudBlade.....	103
Manage and Monitor the GCP-NCC Integration CloudBlade.....	106
ServiceNow CloudBlade Integration.....	109
Configure ServiceNow CloudBlade in Prisma SD-WAN.....	114
Configure ServiceNow.....	120
Create and Resolve Incidents on ServiceNow.....	124
Monitor ServiceNow Status in Prisma SD-WAN.....	126
Shasta LAN Integration.....	129
Configure Shasta LAN.....	130
Onboard Using Zero Touch Provisioning.....	131
Onboard New Switches and Access Points.....	133
Branch Microsegmentation.....	139
Shasta Supported Access Points and Switches.....	140
Zoom QSS CloudBlade Integration.....	143
Configure the Zoom QSS CloudBlade in Prisma SD-WAN.....	144
Access Zoom Application Experience Data.....	145
Zscaler Internet Access CloudBlade Integration.....	149
Plan the Zscaler CloudBlade Deployment.....	151
Acquire the Zscaler Information.....	153
Create Security Zone and Security Policy for GRE Tunnels Creation.....	157
Configure and Install the Zscaler Integration.....	158
Configure IPSec and GRE in Prisma SD-WAN.....	160
Tag the Circuit Categories.....	168
Validate the Zscaler Configuration.....	169
Edit Application Network Policy Rules.....	170
Troubleshoot Installation Scenarios.....	171
Troubleshoot Standard VPNs.....	173
Enable, Pause, Disable, and Uninstall the CloudBlade.....	175

AWS Transit Gateway CloudBlade Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> ❑ Prisma SD-WAN license ❑ AWS Transit Gateway CloudBlade

While enterprises of all sizes are rapidly adopting the cloud to gain agility, scale, and performance, poor access to cloud applications from the remote office can derail cloud migration projects. Inconsistent user experience, unreliable connectivity, and poor performance can result in frustration with IT.

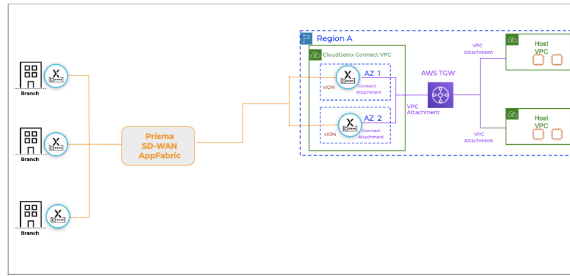
As enterprises continue to adopt IaaS services, such as AWS to host their business-critical applications, there is a compelling need for connecting all remote branch sites to the application VPCs hosted in AWS. Traditionally, enterprises back haul all traffic destined for services hosted in their AWS VPCs to a central data center site on the corporate network. This creates unnecessary bottlenecks and can significantly degrade application performance. An ineffective alternate approach that was adopted by enterprises earlier was to manually establish IPSEC VPNs from each remote office to the Transit Gateway. This does not scale well for large enterprises and considerably slows down enterprise scale and expansion.

Enterprises are also plagued with throughput challenges and the lack of support for dynamic routing, further hindering the adoption of Cloud hosted services.

AWS and Palo Alto Networks Prisma SD-WAN have jointly delivered a solution for high-performance delivery of services from AWS to remote offices worldwide to address these challenges.

Prisma SD-WAN CloudBlades™ platform enables the secure delivery of best-of-breed branch infrastructure from the cloud. The Prisma SD-WAN AWS Transit Gateway Integration CloudBlade optimizes branch to AWS connectivity by securely and seamlessly integrating your enterprise WAN with AWS.

The CloudBlade automatically deploys a Prisma SD-WAN Data Center in the cloud and establishes BGP peering with AWS Transit Gateway over AWS Connect attachment. This allows remote sites to securely reach the Application VPCs in AWS over the Zero touch Prisma SD-WAN and the AWS Transit Gateway connect attachment allows enterprises to enjoy the benefits of higher throughput and dynamic routing.



As your organization migrates new applications to AWS or opens new remote offices, your enterprise WAN and AWS are always synchronized. The AWS Transit Gateway Integration CloudBlade eliminates the need for complex error-prone operations.

AWS and Prisma SD-WAN CloudBlade Prerequisites

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ AWS Transit Gateway CloudBlade

Prisma SD-WAN

- An active Prisma SD-WAN subscription with sufficient licenses to install at least 2 x v7108 IONs, per region.

AWS

- An AWS account with permissions to create, update, and delete CloudFormation templates (CFT) and associated VPC resources.

The following JSON file can be used to create an IAM policy to give the appropriate permissions used by the CloudBlade. This can then be assigned to the user/role that has programmatic access.

To import this file in the AWS console, navigate to **IAM > Policies > Create Policy > JSON** and paste the complete JSON below.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "cloudformation:SetStackPolicy",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation>DeleteStack",
        "cloudformation:SetStackPolicy",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "ec2>DeleteTransitGatewayConnectPeer",
        "ec2>CreateTransitGatewayConnect",

```

```
"ec2:CreateNatGateway",
"ec2:CreateTags",
"ec2:CreateVpc",
"ec2:ModifyTransitGateway",
"ec2:CreateTransitGatewayConnectPeer",
"ec2:CreateTransitGatewayVpcAttachment",
"ec2>DeleteTransitGatewayVpcAttachment",
"ec2:CreateRoute",
"ec2>DeleteTransitGatewayConnect",
"ec2>DeleteNatGateway",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:DeleteSubnet",
"ec2:TerminateInstances",
"ec2:AttachVpnGateway",
"ec2>DeleteRoute",
"ec2>DeleteNetworkInterface",
"ec2:CreateRouteTable",
"ec2:RunInstances",
"ec2:AttachInternetGateway",
"ec2>DeleteRouteTable",
"ec2:RevokeSecurityGroupIngress",
"ec2:CreateNetworkInterface",
"ec2:CreateRoute",
"ec2:CreateSecurityGroup",
"ec2:CreateInternetGateway",
"ec2>DeleteSecurityGroup",
"ec2>DeleteInternetGateway",
"ec2:CreateSubnet",
"ec2:DescribeAddresses",
"ec2:DescribeInstances",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeVpcs",
"ec2:DescribeAccountAttributes",
"ec2:DescribeTransitGateways",
"ec2:DescribeNatGateways",
"ec2:DescribeTransitGatewayConnects",
"ec2:DescribeTransitGatewayVpcAttachments",
"ec2:DescribeTransitGatewayConnectPeers",
"ec2:DescribeSubnets",
"ec2:DescribeRouteTables",
"ec2:ReleaseAddress",
"ec2:DisassociateAddress",
"ec2:CreateTags",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:DetachInternetGateway",
"ec2:DisassociateRouteTable",
"ec2:DescribeSecurityGroups",
"ec2:AllocateAddress",
"ec2:AssociateRouteTable",
"ec2:DescribeInternetGateways",
"s3:GetObject",
"ec2:DescribeNetworkInterfaces",
"ec2:CreateInternetGateway",
"sts:DecodeAuthorizationMessage",
"ec2:ModifyVpcAttribute",
"ec2>DeleteVpc",
```



```
"ec2:DescribeRegions"
  ],
  "Resource": "*"
}
]
```

- The AWS account must have sufficient permissions to generate AWS access keys.
- An active [AWS marketplace subscription](#) to the Prisma SD-WAN ION Virtual Appliance.



In an upgrade scenario from version 2.0.0 to version 2.1.0 of the CloudBlade, existing deployments will not be impacted, however, any new deployments will require to subscribe to this marketplace.

- The AWS account must have at least 2 Elastic IP addresses available per region for allocation.
- An existing Transit Gateway in the regions where you wish to deploy a Prisma SD-WAN Data center.



The AWS Transit Gateway CloudBlade creates the transit gateway attachment between the Prisma SD-WAN VPC and the Transit Gateway. It also configures the BGP peering between the Prisma SD-WAN Data center IONs and the Transit Gateway.

- Routing from the application VPCs to reach Prisma SD-WAN remote networks and the VPC attachment between Application VPCs and the Transit Gateway must be configured by the customer.

Plan the Deployment

The AWS Transit Gateway Integration CloudBlade provides the automatic creation, management, and maintenance of an HA pair of Prisma SD-WAN DC vIONs in an AWS Connect VPC and the establishment of BGP peering over a GRE VPN between the Prisma SD-WAN DC vIONs and the AWS Transit Gateway connect peer.

The CloudBlade automates the following configuration steps required to establish end to end connectivity from remote sites to the Application VPCs in AWS:

- Deploys a Connect VPC in the region(s) where the transit gateway(s) are deployed.
- Deploys a pair of vIONs within the connect VPC(s) in separate availability zones.
- Claims and assigns the vION HA pair to a DC site per region.
- Configures the Transit Gateway Connect attachment for each vION.
- Configures GRE tunnels and BGP parameters on both the Prisma SD-WAN vIONs and the AWS Transit Gateway.
- Activates the DC site.

Configure the AWS Transit Gateway Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license AWS Transit Gateway CloudBlade

To configure the AWS Transit Gateway Integration CloudBlade, retrieve the following information from your AWS account:

STEP 1 | Generate AWS Access key ID and secret access key.

The screenshot shows the AWS IAM console. In the left sidebar, the 'Users' link under 'Access management' is highlighted with a red box. The main panel shows the 'Summary' page for a user. The 'Security credentials' tab is selected and highlighted with a red box. Under the 'Sign-in credentials' section, the 'Summary' indicates the user does not have console management access. Below this, the 'Access keys' section shows a table with one active access key. The 'Create access key' button is highlighted with a red box.

Access key ID	Created	Last used	Status
AKIAI44QH8DHBVS7G	2021-06-15 15:43 PDT	N/A	Active

STEP 2 | The AWS Transit Gateway CloudBlade adds a CIDR block in one of the fields. Ensure that the CIDR block does not overlap with the VPC CIDR.

The screenshot shows the AWS Transit Gateway console. The 'Create Transit Gateway' page is displayed. The 'Transit Gateway ID' field is highlighted with a red box, showing the value 'tgw-01288e057412a6f0'. The 'CIDR block' field is also highlighted with a red box, showing the value '10.0.0.0/16'. The 'Owner account ID' is 50957883509.

Configure and Install the AWS Transit Gateway Integration CloudBlade

STEP 1 | Go to **Strata Cloud Manager > Manage > Prisma SD-WAN > CloudBlades**.

STEP 2 | Locate the **AWS Transit Gateway** CloudBlade and click **Configure**.

If this CloudBlade does not appear in the list, contact the Palo Alto Support team.

STEP 3 | Provide the **AWS Access Key ID** and the **Access Key ID Secret** retrieved from the previous step.

STEP 4 | Provide the **Transit Gateway ID** in the format **Region:TGW-ID**.

Only one region must be mapped to one TGW ID. Multiple TGW entries can be populated in a comma separated format.

STEP 5 | Provide a **VPC CIDR** block in the format **<AWS Region:VPC_CIDR>** for region based CIDRs and **<CIDR>** for global CIDRs for all regions in the TGW field.

The VPC CIDR block must have a subnet mask between /16 and /26. Four distinct subnets are carved out for the public and private subnets on each vION. This should be in the RFC 1918 address space. The same VPC CIDR is reused on all regions in multi-region deployments.

STEP 6 | Provide the **TGW GRE CIDR Block** in the format **<AWS Region:GRE_CIDR>** for region based CIDRs and **<CIDR>** for global CIDRs for all regions in the TGW field.

The TGW GRE Tunnel CIDR block must not overlap the VPC CIDR block. The GRE CIDR block can have any one of the following subnet masks /8, /16, or /24. The same VPC CIDR is reused on all regions in multi-region deployments.

STEP 7 | Provide the **BGP Peer IP Address CIDR** in the format **<AWS Region:BGP_CIDR>** for region based CIDRs or **<CIDR>** for global CIDRs for all regions in the TGW field. Allocate a /29 IP subnet for the GRE tunnel interface on both the ends.

This address block can also be used for establishing core peering from both the Data Center virtual IONs with the Transit Gateway's connect peers. The CIDR block has to be in the "169.254.x.x/29" subnet as required by AWS. Only one /29 prefix is needed, the CloudBlade

uses this as a base and increments as many /29 subnets required based on the number of regions deployed.

Name

Vendor

Installed Version

AWS Transit Gateway Integration

aws-tgw dev

2.0.0

DISABLED ▲

VERSION

2.1.0 ▼

STATUS

ga

PERMISSIONS

View

ADMIN STATE

Enabled ▼

GA Release

ACCESS KEY ID

AKIAXX4Q

ACCESS KEY ID SECRET

.....

unmask

TRANSIT GATEWAY ID

us-west-2:tgw-0, us-east-1:tgw-0e68t

VPC CIDR

us-west-2:16.0.0.0/16, us-east-1:18.0.0.0/16

TGW GRE CIDR BLOCK

us-west-2:172.19.12.0/24, us-east-1:172.18.12.0/24


BGP PEER IP ADDRESS CIDR

us-west-2:169.254.100.0/29, us-east-1:169.254.100.0/29

Uninstall

Cancel

Save

 Ensure at least 2 licenses are available to deploy both v7108 IONs, for each region you wish to deploy the Data Center site.

STEP 8 | Select **Install** once all fields in the CloudBlade configuration is populated.

Validate the AWS Transit Gateway Integration CloudBlade

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ AWS Transit Gateway CloudBlade

The Prisma SD-WAN AWS Transit Gateway Integration CloudBlade automatically provisions a pair of vIONs in an AWS Connect VPC. The AWS route tables for the Data Center IONs are updated to establish a GRE tunnel between the AWS DC vIONs and the Transit Gateway Connect peers. BGP core peering will be established over the GRE tunnel.

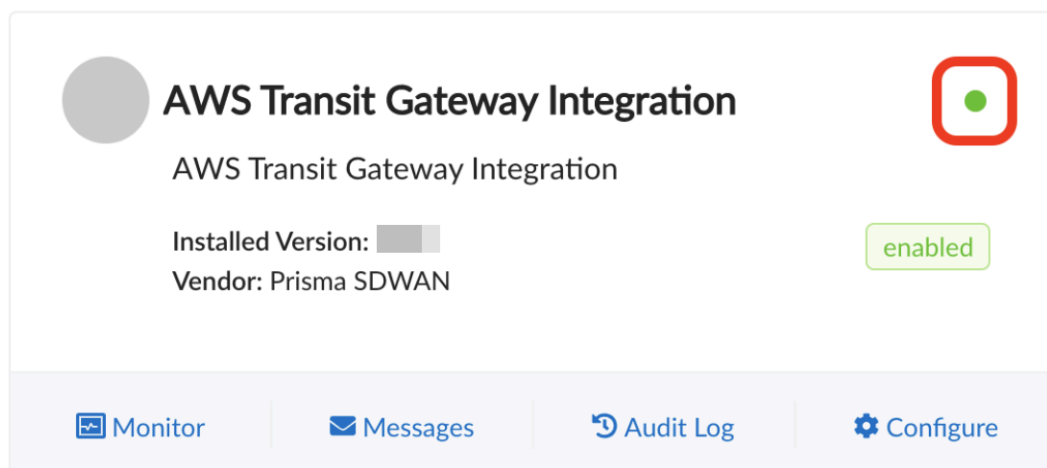


The AWS transit gateway ASN number should not match with the Prisma SD-WAN default ASN value of 64512.

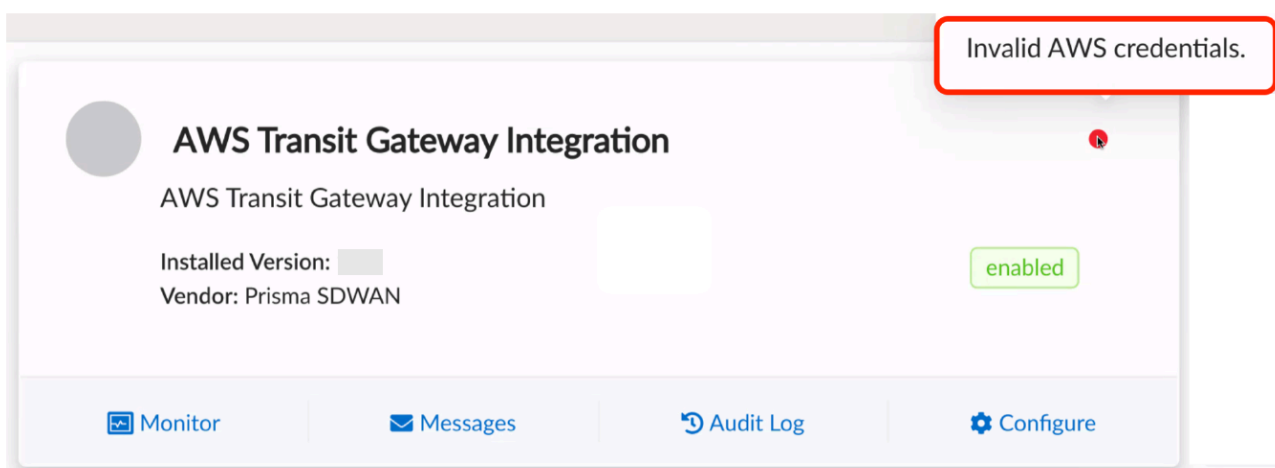
The following steps can be used to validate if the CloudBlade is working as intended:

STEP 1 | Check the status indicator on the CloudBlade window.

Once enabled and deployed correctly, the status indicator should turn green.



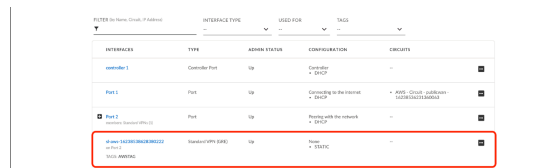
If the access credentials are invalid, the status indicator will throw an **Invalid AWS credentials** error message.



STEP 2 | Check if the Prisma SD-WAN data center site has been created in the AWS cloud and if the vION HA pair has been assigned to this site.

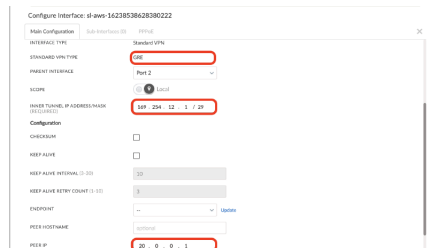
NAME	STATUS	CREATED	# PROXIES	SHARED	NOTE
Prisma SD-WAN-Route1	Created	2024-01-11 10:00:00	1	Yes	
Prisma SD-WAN-Route2	Created	2024-01-11 10:00:00	1	Yes	

STEP 3 | Go to the Active ION's **Interfaces** configuration window and check if the GRE VPN has been created.



INTERFACE	TYPE	ADDRESS STATUS	CONFIGURATION	ACTIONS
Port 1	Port	Configured by the network	BGP	
Port 2	Port	Configured by the network	BGP	
Port 3	Port	Configured by the network	BGP	
Port 4	Port	Configured by the network	BGP	
Port 5	Port	Configured by the network	BGP	
Port 6	Port	Configured by the network	BGP	
Port 7	Port	Configured by the network	BGP	
Port 8	Port	Configured by the network	BGP	
Port 9	Port	Configured by the network	BGP	
Port 10	Port	Configured by the network	BGP	
Port 11	Port	Configured by the network	BGP	
Port 12	Port	Configured by the network	BGP	
Port 13	Port	Configured by the network	BGP	
Port 14	Port	Configured by the network	BGP	
Port 15	Port	Configured by the network	BGP	
Port 16	Port	Configured by the network	BGP	
Port 17	Port	Configured by the network	BGP	
Port 18	Port	Configured by the network	BGP	
Port 19	Port	Configured by the network	BGP	
Port 20	Port	Configured by the network	BGP	
Port 21	Port	Configured by the network	BGP	
Port 22	Port	Configured by the network	BGP	
Port 23	Port	Configured by the network	BGP	
Port 24	Port	Configured by the network	BGP	
Port 25	Port	Configured by the network	BGP	
Port 26	Port	Configured by the network	BGP	
Port 27	Port	Configured by the network	BGP	
Port 28	Port	Configured by the network	BGP	
Port 29	Port	Configured by the network	BGP	
Port 30	Port	Configured by the network	BGP	
Port 31	Port	Configured by the network	BGP	
Port 32	Port	Configured by the network	BGP	
Port 33	Port	Configured by the network	BGP	
Port 34	Port	Configured by the network	BGP	
Port 35	Port	Configured by the network	BGP	
Port 36	Port	Configured by the network	BGP	
Port 37	Port	Configured by the network	BGP	
Port 38	Port	Configured by the network	BGP	
Port 39	Port	Configured by the network	BGP	
Port 40	Port	Configured by the network	BGP	
Port 41	Port	Configured by the network	BGP	
Port 42	Port	Configured by the network	BGP	
Port 43	Port	Configured by the network	BGP	
Port 44	Port	Configured by the network	BGP	
Port 45	Port	Configured by the network	BGP	
Port 46	Port	Configured by the network	BGP	
Port 47	Port	Configured by the network	BGP	
Port 48	Port	Configured by the network	BGP	
Port 49	Port	Configured by the network	BGP	
Port 50	Port	Configured by the network	BGP	
Port 51	Port	Configured by the network	BGP	
Port 52	Port	Configured by the network	BGP	
Port 53	Port	Configured by the network	BGP	
Port 54	Port	Configured by the network	BGP	
Port 55	Port	Configured by the network	BGP	
Port 56	Port	Configured by the network	BGP	
Port 57	Port	Configured by the network	BGP	
Port 58	Port	Configured by the network	BGP	
Port 59	Port	Configured by the network	BGP	
Port 60	Port	Configured by the network	BGP	
Port 61	Port	Configured by the network	BGP	
Port 62	Port	Configured by the network	BGP	
Port 63	Port	Configured by the network	BGP	
Port 64	Port	Configured by the network	BGP	
Port 65	Port	Configured by the network	BGP	
Port 66	Port	Configured by the network	BGP	
Port 67	Port	Configured by the network	BGP	
Port 68	Port	Configured by the network	BGP	
Port 69	Port	Configured by the network	BGP	
Port 70	Port	Configured by the network	BGP	
Port 71	Port	Configured by the network	BGP	
Port 72	Port	Configured by the network	BGP	
Port 73	Port	Configured by the network	BGP	
Port 74	Port	Configured by the network	BGP	
Port 75	Port	Configured by the network	BGP	
Port 76	Port	Configured by the network	BGP	
Port 77	Port	Configured by the network	BGP	
Port 78	Port	Configured by the network	BGP	
Port 79	Port	Configured by the network	BGP	
Port 80	Port	Configured by the network	BGP	
Port 81	Port	Configured by the network	BGP	
Port 82	Port	Configured by the network	BGP	
Port 83	Port	Configured by the network	BGP	
Port 84	Port	Configured by the network	BGP	
Port 85	Port	Configured by the network	BGP	
Port 86	Port	Configured by the network	BGP	
Port 87	Port	Configured by the network	BGP	
Port 88	Port	Configured by the network	BGP	
Port 89	Port	Configured by the network	BGP	
Port 90	Port	Configured by the network	BGP	
Port 91	Port	Configured by the network	BGP	
Port 92	Port	Configured by the network	BGP	
Port 93	Port	Configured by the network	BGP	
Port 94	Port	Configured by the network	BGP	
Port 95	Port	Configured by the network	BGP	
Port 96	Port	Configured by the network	BGP	
Port 97	Port	Configured by the network	BGP	
Port 98	Port	Configured by the network	BGP	
Port 99	Port	Configured by the network	BGP	
Port 100	Port	Configured by the network	BGP	

1. Click on the interface to check the IP address configuration.



Configure Interface: si-aws-162385386280222

Main Configuration: Sub Interface ID: si-aws-162385386280222

INTERFACE TYPE: GRE

UNDERLYING VPC TYPE: Port 2

PRESENT VPC SUBNET: 192.168.1.0 / 24

CONFIGURATION: GRE

KEEP ALIVE: 30

KEEP ALIVE RETRY COUNT (1-10): 3

ENDPOINT: 192.168.1.1

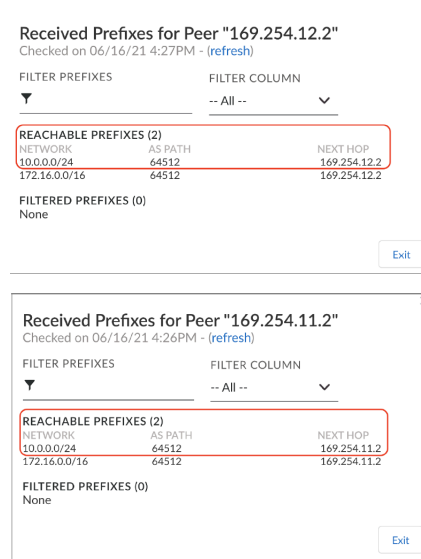
IPV4 HOSTNAME: 192.168.1.1

IPV4 IP: 192.168.1.1

2. Go to the 2nd ION's interface configuration window and check the GRE tunnel interface configuration.

STEP 4 | Check if the core BGP peering between each vION and the Transit Gateway Connect peer is **UP**.

STEP 5 | Check if both the vIONs have learned the prefixes from the Application VPC behind the AWS Transit Gateway and the active ION has learned and advertised the routes.



Received Prefixes for Peer "169.254.12.2"
Checked on 06/16/21 4:27PM - ([refresh](#))

FILTER PREFIXES ▼ FILTER COLUMN -- All -- ▼

REACHABLE PREFIXES (2)		
NETWORK	AS PATH	NEXT HOP
10.0.0.0/24	64512	169.254.12.2
172.16.0.0/16	64512	169.254.12.2

FILTERED PREFIXES (0)
None

[Exit](#)

Received Prefixes for Peer "169.254.11.2"
Checked on 06/16/21 4:26PM - ([refresh](#))

FILTER PREFIXES ▼ FILTER COLUMN -- All -- ▼

REACHABLE PREFIXES (2)		
NETWORK	AS PATH	NEXT HOP
10.0.0.0/24	64512	169.254.11.2
172.16.0.0/16	64512	169.254.11.2

FILTERED PREFIXES (0)
None

[Exit](#)

Advertised Prefixes for Peer "169.254.10.2"

Checked on 12/15/21 2:09PM - ([refresh](#))

FILTER (by prefix)



ADVERTISED PREFIXES (1)

172.16.60.0/24

[Exit](#)

Setup Application Path Policy Rules

Once the CloudBlade configures the appropriate entities within Prisma SD-WAN, the administrator can configure path policies to allow the ION devices to make intelligent per-app path selections.

The Prisma SD-WAN Secure Application Fabric (AppFabric) enables granular controls for virtually an unlimited number of policy permutations down to the sub-application level. Below is an example of configuring a path policy rule to use the Prisma SD-WAN VPN to the AWS DC ION.

In **Strata Cloud Manager**, go **Manage > Policies > Path** and choose a policy set of interest. Within the policy set, click the **Add Rule** and define the following: name, network contexts, destination, prefixes or apps of interest (or a combination of both apps and prefixes), active and backup paths, and service and DC groups.

In this example, we will use a destination prefix-based rule since we have already defined a path prefix that matches the IP address of the service running in the AWS Application VPC.

SOURCE PREFIX (If none selected will use any)

Filter on prefix name

SHOW SELECTED

☒ None

☐ AWS-PREFIX

☐ Azure-Applications

☐ Branch2-destination-prefix

☐ EnterpriseGlobalPrefix

DESTINATION PREFIX (If none selected will use any)

Filter on prefix name

SHOW SELECTED

☐ None

☒ AWS-PREFIX

☐ Azure-Applications

☐ Branch2-destination-prefix

☐ EnterpriseGlobalPrefix

SHOW ALL CIRCUIT CATEGORIES

ACTIVE PATH ☒ AWS

BACKUP PATH ☒ AWS

L3 FAILURE PATH ☒ AWS

OVERLAY

None

CIRCUIT CATEGORY

AWS Public

OVERLAY

None

CIRCUIT CATEGORY

None

OVERLAY

None

CIRCUIT CATEGORY

None

Manage, Monitor, and Troubleshoot the AWS Transit Gateway Integration CloudBlade

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> □ Prisma SD-WAN license □ AWS Transit Gateway CloudBlade

Enable, Pause, Disable, and Uninstall the Integration

After the Integration has been set up, operations can be done in the CloudBlade panel. These operations have various effects on the tunnels and configurations in Prisma SD-WAN and AWS.

Set the CloudBlade to Enabled

This is the standard, expected mode of operation for the Extension. The CloudBlade will run every 60 seconds. If there are configuration changes, the CloudBlade will automatically reconfigure the integration on AWS and Prisma SD-WAN. In addition, during this integration run if any settings were previously modified manually on either Prisma SD-WAN or AWS (e.g. VPC resource was accidentally removed in the AWS portal) these will be reverted to the known good state automatically.



Prisma SD-WAN resources such as GRE tunnel on port 2, Port 1 circuit, Static route, and BGP routing, if deleted or modified can be recreated by the AWS Transit Gateway CloudBlade.



AWS resources such as VPC attachment, Connect attachment, Connect peers in connect attachment, if deleted can be recreated by the AWS Transit Gateway CloudBlade.

Set the CloudBlade to Paused

Pausing the CloudBlade stops all future integration runs but leaves any created objects intact. This stops any future objects from getting created, but does NOT prevent removal of any unconfigured / untagged objects on either Prisma SD-WAN or AWS.

Set the CloudBlade to Disabled

Disabling the CloudBlade removes / deletes all resources created in the AWS environment and the Prisma SD-WAN environment. This can cause communication interruptions if policy is not set to use other paths.



If we need to remove all the configurations from AWS and Prisma SD-WAN, you must disable the CloudBlade. For a clean disable, ensure all Service and DC groups configurations for the traffic is unconfigured and no extra VMs are created in connect vpc in AWS.

Uninstall the CloudBlade

Uninstalling the CloudBlade removes the configuration for the CloudBlade, and immediately stops any changes by the CloudBlade. Uninstalling the CloudBlade does not automatically remove

configuration from all sites and objects. CloudBlades may be uninstalled and reinstalled to facilitate upgrades or downgrades to different versions without traffic interruption. To completely remove all items, set the CloudBlade to Disabled for 5-6 Integration Run periods (360 seconds) before uninstalling.

Troubleshoot the AWS Transit Gateway Integration vION does not show up under unclaimed devices

1. Check on AWS if the CloudFormation stack creation was successful.
2. Confirm if at least 2 x v7108 licenses are available for the vION HA pair creation, for each region where you wish to deploy.
3. Check if there are at least 2 Elastic IPs available, for each region where you wish to deploy.

BGP peering is down

1. Check if the GRE tunnel is created.
2. Check if the connect attachment and connect peers are configured. Ensure the connect BGP peers is in Available state.
3. Check on AWS if the Prisma SD-WAN Connect VPC's route table has a route to the TGW CIDR.
4. Check if EBGP Multihop is configured for the BGP peer on the Prisma SD-WAN portal for each ION.

End to end traffic does not go through

1. Check if Prisma SD-WAN VPNs are up between branch site and AWS DC site.
2. Check if the BGP peering between Datacenter IONs and the Transit Gateway is up and the routes are learned and advertised from the active ION.
3. Check the flow browser for the branch ION from where the traffic is being sent to the AWS VPC.
4. Check if the service and DC group includes the AWS Datacenter.
5. Check the Path policy.
6. Check if there is a security policy rule that is blocking traffic.
7. Check Application VPC's route table and security group.

Monitor the AWS Transit Gateway CloudBlade

On the AWS Transit Gateway CloudBlade page, select **Monitor** to view the AWS status and AWS site connectivity. The Monitor tab shows if a deployment fails, or if any exceptions occur during deployment and points to the cause of the disruption.

The **AWS Status** tab provides the site name, AWS Connect VPC name, AWS region, deployment status, time of the last event occurred, and the summary of the deployment.

CloudBlades /

AWS Transit Gateway Integration

Monitoring

AWS Status

AWS Site Connectivity

Refresh | Columns

SITE NAME	AWS CONNECT VPC NAME	AWS REGION	DEPLOYMENT STATUS	TIMESTAMP	SUMMARY
Prisma-SDWAN-aws-tgw-site-us-east-2	Prisma-SDWAN-CGNXConnectVPC-us-east-2	us-east-2	DEPLOYED	Dec 13, 2021 02:43:49pm	-
Prisma-SDWAN-aws-tgw-site-us-east-1	Prisma-SDWAN-CGNXConnectVPC-us-east-1	us-east-1	DEPLOYED	Dec 13, 2021 02:43:49pm	-
-	Prisma-SDWAN-CGNXConnectVPC-us-east-2	us-east-2	DELETION SUCCESSFUL	Dec 13, 2021 02:22:08pm	-
-	Prisma-SDWAN-CGNXConnectVPC-us-east-1	us-east-1	DELETION SUCCESSFUL	Dec 13, 2021 02:22:08pm	-
-	Prisma-SDWAN-CGNXConnectVPC-us-east-2	us-east-2	DELETION SUCCESSFUL	Dec 13, 2021 02:20:04pm	-
-	Prisma-SDWAN-CGNXConnectVPC-us-east-1	us-east-1	DELETION SUCCESSFUL	Dec 13, 2021 02:20:04pm	-
-	Prisma-SDWAN-CGNXConnectVPC-us-east-2	us-east-2	DELETION SUCCESSFUL	Dec 13, 2021 02:17:59pm	-
-	Prisma-SDWAN-CGNXConnectVPC-us-east-1	us-east-1	DELETION SUCCESSFUL	Dec 13, 2021 02:17:59pm	-
-	Prisma-SDWAN-CGNXConnectVPC-us-east-2	us-east-2	DELETION SUCCESSFUL	Dec 13, 2021 02:15:56pm	-
-	Prisma-SDWAN-CGNXConnectVPC-us-east-1	us-east-1	DELETION SUCCESSFUL	Dec 13, 2021 02:15:56pm	-

< 1 2 3 4 5 >

The **AWS Site Connectivity** tab provides the site name, name of the device, AWS region, AWS Connect VPC names, AWS transit gateway ID, GRE tunnel status, BGP status, GRE tunnel uptime, and the BGP uptime.

CloudBlades /

AWS Transit Gateway Integration

Monitoring

AWS Status

AWS Site Connectivity

Refresh | Columns

SITE NAME	DEVICE NAME	AWS REGION	AWS CONNECT VPC NAME	AWS TGW ID	GRE TUNNEL STATUS	BGP STATUS	GRE TUNNEL UPTIME	BGP UPTIME
Prisma-SDWAN-aws-tgw-site-us-east-1	Prisma-SDWAN-vION7KInstance-us-east-1	us-east-1	Prisma-SDWAN-CGNXConnectVPC-us-east-1	tgw-04d732c9b8c991d0c	UP	UP	0:29:07	0:23:40
Prisma-SDWAN-aws-tgw-site-us-east-1	Prisma-SDWAN-vION7KInstance-us-east-1-HA	us-east-1	Prisma-SDWAN-CGNXConnectVPC-us-east-1	tgw-04d732c9b8c991d0c	UP	UP	0:29:07	0:23:39
Prisma-SDWAN-aws-tgw-site-us-east-2	Prisma-SDWAN-vION7KInstance-us-east-2	us-east-2	Prisma-SDWAN-CGNXConnectVPC-us-east-2	tgw-0516ac533d6d3200f	UP	UP	0:29:07	0:23:40
Prisma-SDWAN-aws-tgw-site-us-east-2	Prisma-SDWAN-vION7KInstance-us-east-2-HA	us-east-2	Prisma-SDWAN-CGNXConnectVPC-us-east-2	tgw-0516ac533d6d3200f	UP	UP	0:29:07	0:23:39

Azure Virtual WAN with vION CloudBlade Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> ❑ Prisma SD-WAN license ❑ Azure Virtual WAN with vION CloudBlade

With the growth of Hybrid Cloud deployments, most enterprises have moved workloads to the cloud and need to enable secured connectivity from branch sites to these application workloads. In addition, enterprises are moving towards hybrid and multi-cloud architecture with their on-premise infrastructure. This transition must work seamlessly while ensuring SLAs (Service Level Agreements) are met for applications hosted on-iaaS, PaaS, SaaS environments, and on-premise with the right level of visibility and security controls.

The central entity in Azure that provides the branch integrations through vION devices is the Virtual WAN (virtual WAN). Azure Virtual WAN is a networking service with a single operational interface that provides networking, security, and routing functionalities together. These functionalities include branch connectivity through SD-WAN devices (vION), intra-cloud connectivity (transitive connectivity for virtual networks), Azure Firewall, and encryption for private connectivity, amongst others that may be applicable in a typical hybrid cloud integration environment.

According to Microsoft Azure, the virtual WAN architecture is a hub and spoke architecture with built-in scale and performance for branches (VPN/SD-WAN devices), virtual networks, users (Azure VPN/OpenVPN/IKEv2 clients), and ExpressRoute circuits. In addition, it enables a global transit network architecture, where the cloud-hosted network hub enables transitive connectivity between endpoints that may be distributed across different types of spokes.

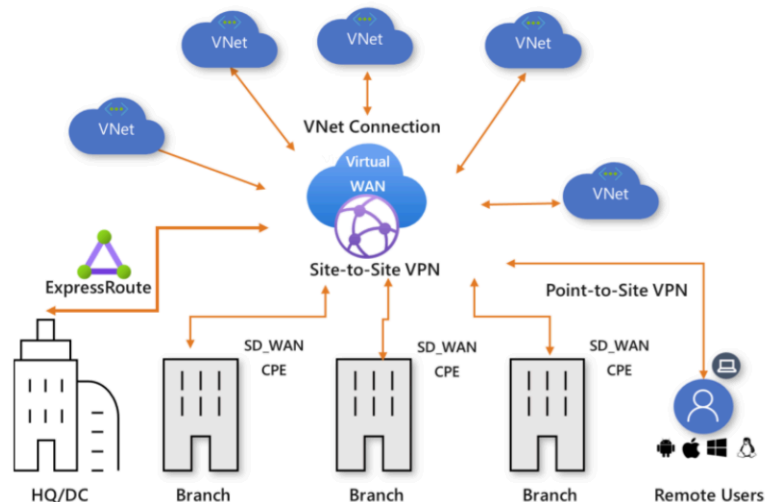


IMAGE SOURCE: Azure Product Documentation

Prisma SD-WAN and Azure Integration Prerequisites

The following items are required for configuring Prisma SD-WAN and Azure Virtual WAN with vION CloudBlade:

Prisma SD-WAN

- An active Prisma SD-WAN subscription with sufficient licenses to install at least 2 x v7108 IONs per region.

Azure

- An Azure account with permissions to create and update Azure Resource Groups, VNET (Virtual Network), and Virtual Machines.

The Azure vWAN uses the following list of APIs with vION CloudBlade.

- `subscriptions.get()`
- `subscriptions.list_locations()`
- `resource_groups.create_or_update()`
- `resource_groups.check_existence()`
- `resource_groups.get()`
- `resource_groups.begin_delete()`
- `resources.list_by_resource_group()`
- `resources.get()`
- `resources.get_by_id()`
- `resources.begin_delete_by_id()`
- `deployments.get()`
- `deployments.begin_validate()`
- `deployments.begin_create_or_update()`
- `deployments.list_by_resource_group()`
- `deployments.delete()`
- `subnets.begin_create_or_update()`
- `network_interfaces.begin_create_or_update()`
- `security_rules.begin_create_or_update()`
- `virtual_hub_bgp_connection.begin_create_or_update()`
- `virtual_hub_bgp_connections.list()`
- `virtual_hub_bgp_connection.begin_delete()`
- `hub_virtual_network_connections.get()`
- `hub_virtual_network_connections.list()`
- `hub_virtual_network_connections.begin_delete()`
- `virtual_wans.get()`
- `virtual_hubs.begin_delete()`
- `network_security_groups.get()`
- `resources()`
- `AuthenticationContext()`
- `acquire_token_with_client_credentials()`
- As the Azure vWAN with vION CloudBlade automates the deployments of Virtual Machines through API calls, you must [enable the programmatic access](#) through the Azure portal.
- An active Azure marketplace subscription to the Prisma SD-WAN Virtual ION Appliance.

- The Azure vWAN with vION CloudBlade utilizes the ION images for deployments in the Azure marketplace. To begin using these resources (through the CloudBlade), you must accept the Azure Marketplace terms and conditions and [follow the guidelines of usage](#) of the marketplace listings.
- The CloudBlade will require **Read Access** to Virtual Network resources in Brownfield deployment scenarios to determine the attached Virtual Networks and their associated address prefixes. You can access the Virtual Networks via the Virtual Network Connections to the identified Virtual WAN entity in Brownfield deployment scenarios.

In addition, the CloudBlade will also need read/write access in Brownfield scenarios to Virtual WAN and Virtual Hub resources to configure BGP peers necessary for the exchange of routes with the Virtual Hub(s) to remote Virtual Networks. The read/write access needs to be explicitly provided in the case where the Virtual Networks or the Virtual WAN/Virtual Hub resources were created with a different subscription and, therefore, associated credentials than what is used by the CloudBlade. Refer to [Azure resource management and subscriptions](#) for more information.

- A [resource group](#) with Azure vWAN with a single or multiple [Virtual Hub](#), defined for the regions of deployment (Brownfield Deployments only).
- To enable the [Azure BGP peering](#) with the Virtual WAN hub feature in this release, you must contact the Azure team with the Resource ID of your Virtual WAN resource.
- All regions must support the Azure Virtual Machine model Standard D8s v3 (8 vCPUs, 32 GiB).

Plan the Azure Virtual WAN with vION Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ Azure Virtual WAN with vION CloudBlade

To enable the transition to hybrid deployment environments more efficiently; the Azure virtual WAN integration solution is enhanced by installing a pair of HA vIONs in a vNET as a spoke environment to an Azure virtual hub router instance. This enables a cleaner integration of branch sites to customer workload vNETs through the virtual hub, enabling LQM measurements. In addition, this helps with path selection, application-based routing, enables different kinds of link aggregation and avoids user-defined routes between the vION and the virtual hub router, as the virtual hub enables the exchange of routes over BGP.

The Azure Virtual WAN with vION integration can be done for both Greenfield deployments (where the vHUB and vWAN resources are created by the CloudBlade) and Brownfield deployments (where the existing vWAN and vHUB(s) are referenced by the CloudBlade).

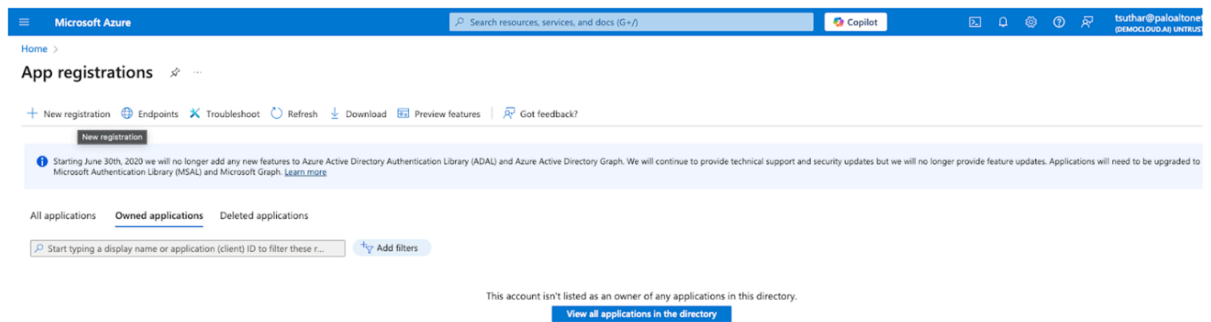
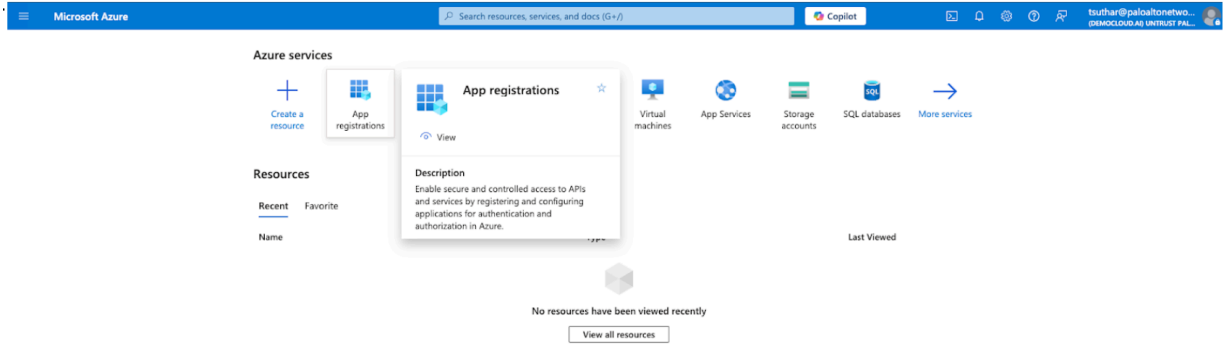
The CloudBlade automates the following configuration steps required to establish end-to-end connectivity on Prisma SD-WAN and Azure.

- Deploys a pair of vION devices within the Transit vNET in Azure in separate availability zones based on the Azure regions.
- Attaches the vION devices in the Transit VNET as a spoke to the virtual WAN hub.
- Claims and assigns each vION to a data center site per region.
- Configures the Transit vNET with the needed three subnets - private/LAN, public/Internet, and controller subnets.
- Creates a static route from vIONs to the virtual hub.
- Configures the BGP dynamic routing protocol on both Prisma SD-WAN ION and virtual WAN hub router.
- Activates the Data Center site.

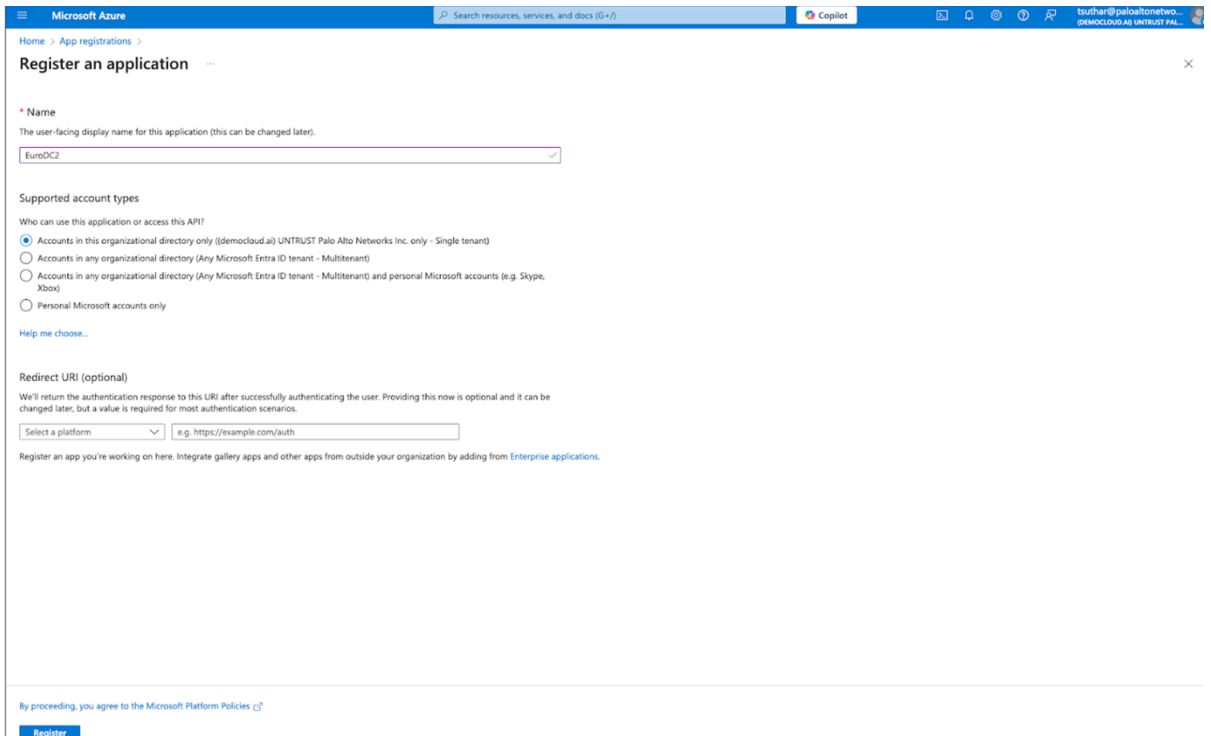
Create Application Registration Object in Azure

Before configuring Prisma SD-WAN to integrate with Azure virtual WAN, perform the following steps in the Azure portal to create an application registration object. This step is not required if you already have the application registration object.

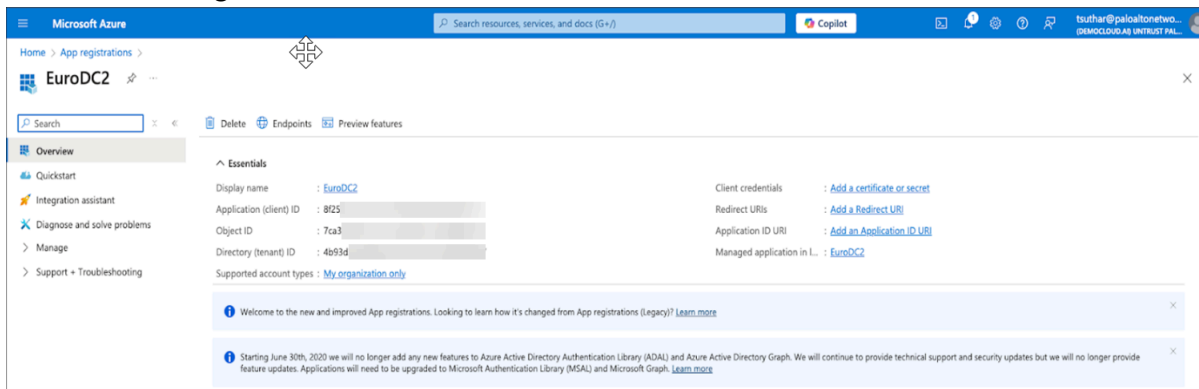
1. Go to Azure services > App registrations > New registration.



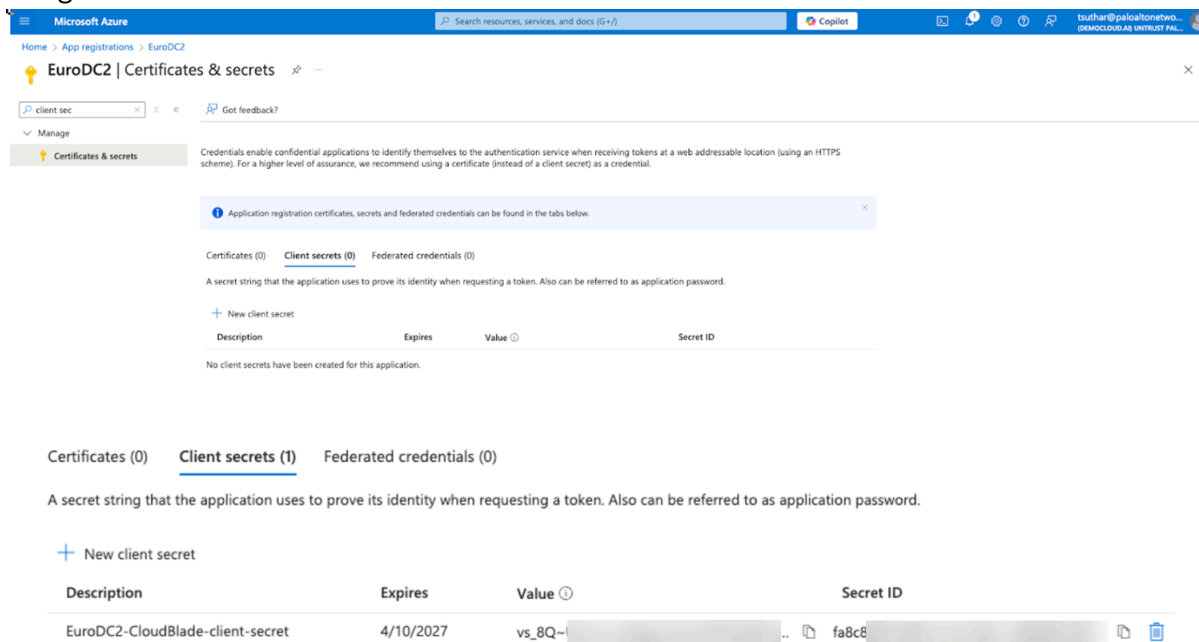
2. Enter the display Name of the application, choose the Supported Account Type, and select Register.



3. Copy the **Application (client) ID** and **Directory (tenant) ID** to be used later in Prisma SD-WAN CloudBlade configuration.



4. Generate and copy a new **client secret** to be used later in Prisma SD-WAN CloudBlade configuration.



5. Assign Contributor role to the new Application Registration object created in Step 1.

The top screenshot shows the 'Access control' page for a subscription. The 'Add role assignment' dropdown menu is open, showing options: 'Add role assignment', 'Add role assignment', and 'Add custom role'. The 'Add role assignment' option is selected. Below the dropdown, there is a search bar and a table of role assignments. The table has columns for 'Name', 'Object ID', and 'Type'. The first row shows 'EuroDC2' with object ID 'd8b0...' and type 'App'.

The bottom screenshot shows the 'Add role assignment' wizard. The 'Role' tab is selected, and 'Contributor' is chosen. The 'Assign access to' section has 'User, group, or service principal' selected. The 'Members' section shows a table with columns 'Name', 'Object ID', and 'Type'. The first row shows 'EuroDC2' with object ID 'd8b0...' and type 'App'.

6. Locate the Azure subscription ID and copy to be used later in the Prisma SD-WAN CloudBlade configuration.

The screenshot shows the 'Subscriptions' page in the Microsoft Azure portal. A table lists subscriptions with columns: 'Subscription name', 'Subscription ID', 'My role', 'Current cost', 'Secure Score', 'Parent management group', and 'Status'. The first row shows 'SASE-TME' with subscription ID '9d6...' and status 'Active'.

Configure the Azure Virtual WAN with vION CloudBlade

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license Azure Virtual WAN with vION CloudBlade

Before deploying the CloudBlade, it's important to determine the kind of deployment that you are going to do. We support two deployment scenarios, Greenfield and Brownfield. Depending on the type of deployment you are doing it will determine which fields that need to be completed in the CloudBlade configuration.

Brownfield Deployment

- This is the most common deployment model.
- This would be used when you already have the Azure Virtual WAN and associated vWAN Hub(s) in the region or regions that you wish to deploy the SD-WAN data centers.
- The CloudBlade will deploy a Resource Group with a Transit VNET (per region), the ION devices will be deployed in the Resource Group and the VNET will be connected to the local regional Hub.

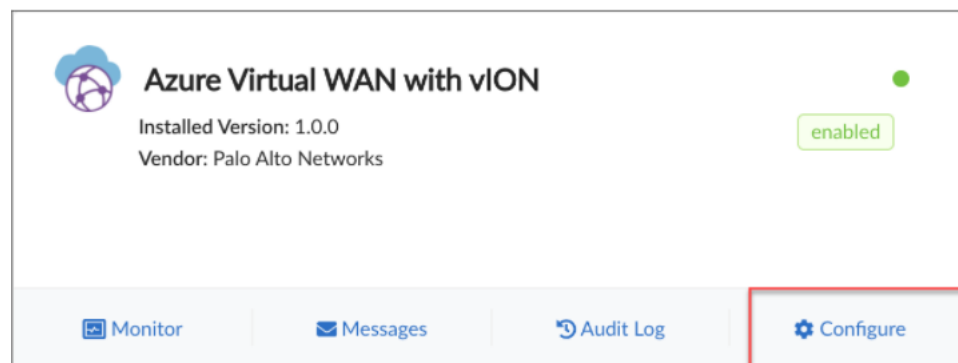
Greenfield Deployment

- This is a less common deployment model.
- This would be used when you do not have a Virtual WAN configured in your Azure environment.
- The CloudBlade will deploy a Virtual WAN and a vWAN Hub in the region or regions that you wish to deploy the SD-WAN data centers.
- Once completed the CloudBlade will deploy a Resource Group with a Transit VNET (per region), the ION devices will be deployed in the Resource Group and the VNET will be connected to the local regional Hub.

To configure the Azure virtual WAN Integration app in Prisma SD-WAN:

STEP 1 | In **Strata Cloud Manager**, go to **Manage > CloudBlades**.

STEP 2 | Locate the **Azure Virtual WAN with vION** and select **Configure**.



STEP 3 | In the **Azure Virtual WAN with vION Integration** page, enter the following information in the fields shown below, change where appropriate.

Brownfield Configuration Example

Greenfield Configuration Example

- **VERSION:** Select the version of the Azure Virtual Network Integration CloudBlade.
- **ADMIN STATE:** For Admin State, select/retain Enabled.
- **AZURE TENANT ID:** Provide the Directory (tenant) ID generated in the previous section on Azure application registration. It is the ID of the Azure Active directory in which an application is created.
- **AZURE CLIENT ID:** Provide the Application (client) ID generated in the previous section on Azure application registration. Client ID uniquely identifies an application in the Microsoft identity platform.
- **AZURE CLIENT SECRET:** Provide the client secret generated under the Azure application registration. Client secret represents the authentication key string that is generated for a given app registration.
- **AZURE SUBSCRIPTION ID:** Provide the subscription ID noted down from the previous section. Subscription ID is a GUID that uniquely identifies the subscription to use Azure services
- **TRANSIT VIRTUAL NETWORK CIDR:** Provide comma-separated list of non-overlapping CIDRs for each region. The CIDR represents the private address space of the Virtual Network that hosts the Prisma SD-WAN vION instances and their associated resources

in Azure. Prefix lengths of /16 up to /26 are supported. Format: **<Azure Region Code>:<CIDR>**. Example: westus:10.10.0.0/16.

Enter information for TRANSIT VIRTUAL NETWORK CIDR if you have a brownfield or greenfield deployment.

- **Optional VIRTUAL HUB CIDR:** Provide a comma-separated list of non-overlapping CIDRs for each virtual hub to be deployed. Prefix lengths between /1 and /24 are supported. This field is required only for new virtual hub deployments (Greenfield). Format: **<Azure Region Code>:<CIDR>** Example: westus:10.35.0.0/24.

Enter information for VIRTUAL HUB CIDR only if you have a greenfield deployment.

- **Optional VIRTUAL WAN RESOURCE:** Provide the name of the virtual WAN resource to be considered. This virtual WAN resource is used when deploying new vHUB(s) or referring to existing vHUB(s) identified in the Virtual Hub Resource(s) configuration. Format: **<Resource Group Name>:<Virtual WAN Name>**.

Enter information for VIRTUAL WAN RESOURCE only if you have a brownfield deployment.

- **Optional VIRTUAL HUB RESOURCES:** Provide a comma-separated list of virtual hub resource(s) in the respective region(s) with which peering is established. All virtual hubs need to reside within the same vWAN instance identified by the Virtual WAN Resource configuration. Format: **<Virtual Hub Name>**.

Enter information for VIRTUAL HUB RESOURCES only if you have a brownfield deployment.



Only virtual hubs in the same region can be associated with the transit vNET deployment in that region.

STEP 4 | Click **Save** and **Install** after the settings are configured.



The deployment time for Greenfield deployments is around 20 to 25 minutes and the time taken for Brownfield deployments is around 10 to 15 minutes.

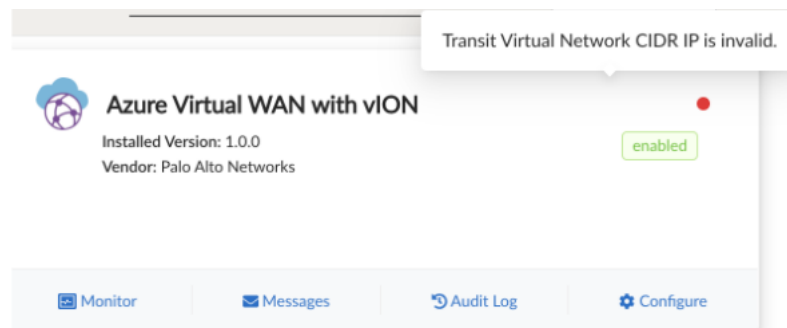
Validate the Azure Virtual WAN Integration CloudBlade

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license Azure Virtual WAN Integration CloudBlade

Validate if the Azure Virtual WAN Integration CloudBlade is deployed as intended and the resources are created in Azure and Prisma SD-WAN controller.


STEP 1 | Check the status indicator on the CloudBlade window.

Once enabled and deployed correctly, the status indicator should turn green. If the access credentials are invalid, the status indicator will display an invalid credentials error message.



STEP 2 | Go to **Workflows > Prisma SD-WAN Setup > Data Centers** to check if the controller has created the Prisma SD-WAN Data Center site and assigned the vION HA pair to this site.

NAME	LOCATION	CIRCUITS	IP PREFIXES	DEVICES	MODE
Prisma-SDWAN-Azure-Site-uk-south <small>Created by: CDR-Azure-CD TAGS: AZURETAG-uk-south</small>	London	AZURE - Circuit - publicwan - 16426763010140215	10.13.0.0/16 10.14.0.0/16 + 2 More	<ul style="list-style-type: none"> Prisma SD-WAN vION-1-uk-south (jon 7108v) Prisma SD-WAN vION-2-uk-south (jon 7108v) 	Control

 The CloudBlade will provision both vIONs and set the standard device names as *Prisma-SD-WAN-vION-1-
<region_name>* and *Prisma-SD-WAN-vION-2-
<region_name>*. It is recommended not to change these device names, as doing so may cause configuration sync issues between the vIONs.

STEP 3 | Select the site name to check if the **Secure Fabric Links** are created between the newly created Azure Data Center ION devices and the branch site devices.

STEP 4 | Go to the Active ION device Interface configuration window and check if Port 1 and Port 2 configurations are created.

Configure Interface: 1

Main Configuration

Sub-Interfaces (0)

PPPoE

INTERFACE STATUS

ADMIN UP?

NAME

DESCRIPTION

TAGS (MAX 10)

INTERFACE TYPE

USE THIS PORT FOR...

CIRCUIT LABEL

CONFIGURATION

IP ADDRESS/MASK (REQUIRED)

DEFAULT GATEWAY (REQUIRED)

DNS SERVERS (3 MAX)

Port 1

☐ No ☒ Yes

1

Optional

Port

Connect to Internet

Ethernet Internet (AZURE - Circuit - publicwan - 16426763090540215) - update

STATIC

10 . 7 . 8 . 4 / 21

10 . 7 . 8 . 1

Configure Interface: 2

Main Configuration

Sub-Interfaces (0)

PPPoE

INTERFACE STATUS

ADMIN UP?

NAME

DESCRIPTION

TAGS (MAX 10)

INTERFACE TYPE

USE THIS PORT FOR...

CIRCUIT LABELS

CONFIGURATION

IP ADDRESS/MASK (REQUIRED)

DEFAULT GATEWAY

Port 2

☐ No ☒ Yes

2

Optional

Port

Peer with a Network

Select Circuits...

STATIC

10 . 7 . 16 . 4 / 21

10 . 7 . 16 . 1

STEP 5 | Check if the IPs provided on port 1 and port 2 of the element in the controller match the ION deployed in the Azure environment.

STEP 6 | Check if the BGP core peering between each vION and the Azure virtual hub is up.

STEP 7 | Verify the static route configuration for each vION interface.
Static routes are required as Azure's virtual hub router advertises workload/application prefixes to the virtual IONs. In order for the vIONs to forward branch traffic to these destination prefixes, the vION(s) first need to send the traffic to the hub router and the static route entries enable that routing.

STEP 8 | Check the advertised application VNET prefixes to the Virtual hub.

DEVICES	IP PREFIXES (View Global)
✓ Prisma-SD-WAN-vION-1-uksouth (i...	10.13.0.0/16
✓ Prisma-SD-WAN-vION-2-uksouth (i...	10.14.0.0/16
Assign Device	10.15.0.0/16
	10.16.0.0/16
	Change IP Prefixes

STEP 9 | Check the received routes from the Cloud Router.

×

Received Prefixes for Peer "10.0.3.68"

Checked on 01/20/22 5:03PM - [refresh](#)

FILTER PREFIXES

▼

FILTER COLUMN

-- All --

▼

REACHABLE PREFIXES (5)

NETWORK	AS PATH	NEXT HOP
10.0.3.0/24	65515	10.0.3.68
10.15.0.0/16	65515	10.0.3.68
10.16.0.0/16	65515	10.0.3.68
10.13.0.0/16	65515, 65520, 65520	10.0.3.68
10.14.0.0/16	65515, 65520, 65520	10.0.3.68

FILTERED PREFIXES (1)

NETWORK	AS PATH	NEXT HOP
192.168.150.0/24	65515, 65412, 65412, 65412, 65412, 65412	10.0.3.68

Exit

Manage and Monitor the Azure Virtual WAN with vION CloudBlade

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license Azure Virtual WAN with vION CloudBlade

After you set the integration, go to Azure Virtual WAN with vION CloudBlade to perform the following operations from the CloudBlade configuration screen.

Enable the CloudBlade

This is the default mode of operation for the CloudBlade. In this mode, the CloudBlade performs its desired and intended functionality. Any configuration changes will automatically reconfigure the integration on Azure Virtual WAN and Prisma SD-WAN in 60 seconds.

Pause the CloudBlade

Pausing the CloudBlade stops all future integrations but leaves any created resources intact. This stops any future user resources from getting created. When paused, the CloudBlade will not deploy or delete the resources, nor will it prevent the user from deleting any resources. Changes will be tracked by the CloudBlade and reverted once enabled.

Disable the CloudBlade

Disabling the CloudBlade indicates the system to remove and delete all resources created by the CloudBlade.

Uninstall the CloudBlade

Uninstalling the CloudBlade removes the resources for the CloudBlade and immediately stops any changes by the CloudBlade. Set the CloudBlade to disabled for 2-3 integration run periods before uninstalling to remove all items. The Azure Virtual WAN with vION CloudBlade must always be disabled before uninstalling; if you wish to reinstall in the same region, it may not create the resources. Also, check the Monitor tab in the Prisma SD-WAN web interface if all resources are empty/deleted before uninstalling.

Monitor the Azure Virtual WAN with vION CloudBlade

On the **Azure Virtual WAN with vION CloudBlade** page, select **Monitor** to view the **Azure Deployment Status** and **Azure Site Connectivity**. The Monitoring tab shows if a deployment fails and fails or any exceptions occur during deployment and points to the cause of the disruption.

The **Azure Site Connectivity** provides the site name, name of the device, Azure region of deployment, the Azure VNET, the Azure Virtual WAN, the Azure hub, VNET CIDR, BGP status, BGP uptime, and received prefixes of the deployment.

Monitoring

Azure Deployment Status Azure Site Connectivity Refresh Columns

SITE NAME	DEVICE NAME	AZURE REGION	AZURE VNET NAME	AZURE VWAN NAME	AZURE HUB NAME	VNET CIDR	BGP STATUS	BGP UPTIME	RECEIVED PREFIXES
Prisma-SDWAN-Azure-Site-northcentralus	Prisma-SD-WAN-vION-1	northcentralus	Test-Hello-un-install-northcentralus	Test-Hello-un-install-vHub-northcentralus	Prisma-SD-WAN-vHub	10.0.0.0/16	UP	00:00:01	-
Prisma-SDWAN-Azure-Site-northcentralus	Prisma-SD-WAN-vION-1	northcentralus	Test-Hello-un-install-northcentralus	Test-Hello-un-install-vHub-northcentralus	Prisma-SD-WAN-vHub	10.0.0.0/16	UP	00:00:01	-
Prisma-SDWAN-Azure-Site-northcentralus	Prisma-SD-WAN-vION-2	northcentralus	Test-Hello-un-install-northcentralus	Test-Hello-un-install-vHub-northcentralus	Prisma-SD-WAN-vHub	10.0.0.0/16	UP	00:00:01	-
Prisma-SDWAN-Azure-Site-northcentralus	Prisma-SD-WAN-vION-2	northcentralus	Test-Hello-un-install-northcentralus	Test-Hello-un-install-vHub-northcentralus	Prisma-SD-WAN-vHub	10.0.0.0/16	UP	00:00:00	-

The Azure Deployment Status provides the site name, name of the VNET, name of the Azure hub, Azure region, deployment status, time of the last occurred event, and summary of the deployment.

Monitoring

Azure Deployment Status Azure Site Connectivity Refresh Columns

SITE NAME	VNET NAME	V-HUB NAME	AZURE REGION	DEPLOYMENT STATUS	TIMESTAMP	SUMMARY
Prisma-SDWAN-Azure-Site-northcentralus	Test-Hello-un-install-northcentralus	Prisma-SD-WAN-vHub	northcentralus	ONGOING	Jan 11, 2022 08:32:27pm	-
-	Test-Hello-un-install-northcentralus	Prisma-SD-WAN-vHub	northcentralus	DELETION SUCCESSFUL	Jan 11, 2022 03:47:31pm	-
-	Test-Hello-un-install-northcentralus	Prisma-SD-WAN-vHub	northcentralus	ONGOING	Jan 11, 2022 03:31:15pm	FATAL ERROR: Transit Virtual Network Resource. Removing VNET Resource Group.
Prisma-SDWAN-Azure-Site-uksouth	Test-Hello-uksouth	Prisma-SD-WAN-vHub	uksouth	DELETION SUCCESSFUL	Jan 11, 2022 01:48:49pm	-
Prisma-SDWAN-Azure-Site-northcentralus	Test-Hello-northcentralus	Prisma-SD-WAN-vHub	northcentralus	DELETION SUCCESSFUL	Jan 11, 2022 01:48:49pm	-
Prisma-SDWAN-Azure-Site-uksouth	Test-Hello-uksouth	Prisma-SD-WAN-vHub	uksouth	DEPLOYED	Jan 11, 2022 01:23:36pm	-
Prisma-SDWAN-Azure-Site-northcentralus	Test-Hello-northcentralus	Prisma-SD-WAN-vHub	northcentralus	DEPLOYED	Jan 11, 2022 01:23:36pm	-
-	Test-Hello-uksouth	Prisma-SD-WAN-vHub	uksouth	DELETION SUCCESSFUL	Jan 11, 2022 10:54:00am	-
-	Test-Hello-northcentralus	Prisma-SD-WAN-vHub	northcentralus	DELETION SUCCESSFUL	Jan 11, 2022 10:54:00am	-
-	Test-Hello-uksouth	Prisma-SD-WAN-vHub	uksouth	ONGOING	Jan 11, 2022 10:37:27am	FATAL ERROR: Transit Virtual Network Resource. Removing VNET Resource Group.

< 1 2 3 4 5 >

Azure Virtual WAN CloudBlade Integration

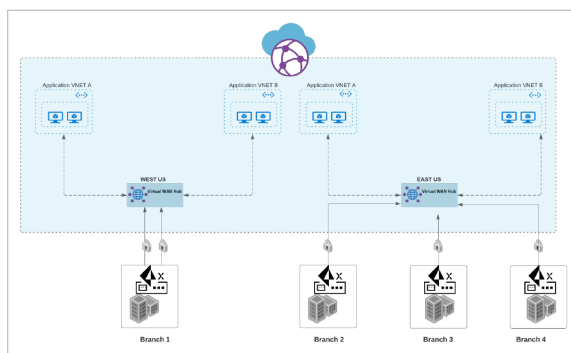
Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> ❑ Prisma SD-WAN license ❑ Azure Virtual WAN CloudBlade

While enterprises of all sizes are rapidly adopting the cloud to gain agility, scale, and performance, poor access to cloud applications from the remote office can derail cloud migration projects. Inconsistent user experience, unreliable connectivity, and poor performance can result in frustration with IT.

Microsoft and Prisma SD-WAN have jointly delivered a solution to address these challenges and bring in high performance delivery of Microsoft Azure to remote offices worldwide. Microsoft Azure Virtual WAN (vWAN) provides a high-speed global network with minimal latencies. Prisma SD-WAN CloudBlades™ platform enables the secure delivery of best-of-breed branch infrastructure from the cloud. The Prisma SD-WAN Azure CloudBlade optimizes branch to Azure connectivity by securely and seamlessly integrating your enterprise WAN with Azure Virtual WAN.

Microsoft Azure Virtual WAN provides a global network with minimal latencies. The 60+ Azure regions distributed globally serve as hubs or entry points into the high-speed Azure network. The Prisma SD-WAN CloudBlade connects each remote office to a specified Azure region using secure tunnels. These secure tunnels can be established over any WAN type, including low cost broadband connections. The CloudBlade then programs Azure to integrate your enterprise WAN and the Azure network - without the need for complex VPN setup or routing protocol management.

Prisma SD-WAN prioritizes business applications on Azure by analyzing all available paths and using the highest performing path in real-time. As your organization migrates new applications to Azure, uses new Azure regions, or opens new remote offices, your enterprise WAN and Azure are synchronized. The CloudBlade eliminates the need for complex error-prone operations.



Azure vWAN and Prisma SD-WAN CloudBlade Prerequisites

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> ❑ Prisma SD-WAN license ❑ Azure Virtual WAN CloudBlade

Prisma SD-WAN:

- An active Prisma SD-WAN subscription with sufficient licenses to install at least 2 x v7108 IONs, per region.

Azure:

- An Azure account with permissions to create and update Azure Resource Groups, VNET (Virtual Network), and Virtual Machines.

The Azure vWAN uses the following list of APIs with vION CloudBlade.

- `subscriptions.get()`
 - `subscriptions.list_locations()`
 - `resource_groups.create_or_update()`
 - `resource_groups.check_existence()`
 - `resource_groups.get()`
 - `resource_groups.begin_delete()`
 - `resources.list_by_resource_group()`
 - `resources.get()`
 - `resources.get_by_id()`
 - `resources.begin_delete_by_id()`
 - `deployments.get()`
 - `deployments.begin_validate()`
 - `deployments.begin_create_or_update()`
 - `deployments.list_by_resource_group()`
 - `deployments.delete()`
 - `subnets.begin_create_or_update()`
 - `network_interfaces.begin_create_or_update()`
 - `security_rules.begin_create_or_update()`
 - `virtual_hub_bgp_connection.begin_create_or_update()`
 - `virtual_hub_bgp_connections.list()`
 - `virtual_hub_bgp_connection.begin_delete()`
 - `hub_virtual_network_connections.get()`
 - `hub_virtual_network_connections.list()`
 - `hub_virtual_network_connections.begin_delete()`
 - `virtual_wans.get()`
 - `virtual_hubs.begin_delete()`
 - `network_security_groups.get()`
 - `resources()`
 - `AuthenticationContext()`
 - `acquire_token_with_client_credentials()`
- As the Azure vWAN with vION CloudBlade automates the deployments of Virtual Machines through API calls, you must [enable the programmatic access](#) through the Azure portal.
 - An active Azure marketplace subscription to the Prisma SD-WAN Virtual ION Appliance.

- The Azure vWAN with vION CloudBlade utilizes the ION images for deployments in the Azure marketplace. To begin using these resources (through the CloudBlade), you must accept the Azure Marketplace terms and conditions and [follow the guidelines of usage](#) of the marketplace listings.
- The CloudBlade will require **Read Access** to Virtual Network resources in Brownfield deployment scenarios to determine the attached Virtual Networks and their associated address prefixes. You can access the Virtual Networks via the Virtual Network Connections to the identified Virtual WAN entity in Brownfield deployment scenarios.

In addition, the CloudBlade will also need read/write access in Brownfield scenarios to Virtual WAN and Virtual Hub resources to configure BGP peers necessary for the exchange of routes with the Virtual Hub(s) to remote Virtual Networks. The read/write access needs to be explicitly provided in the case where the Virtual Networks or the Virtual WAN/Virtual Hub resources were created with a different subscription and, therefore, associated credentials than what is used by the CloudBlade. Refer to [Azure resource management and subscriptions](#) for more information.

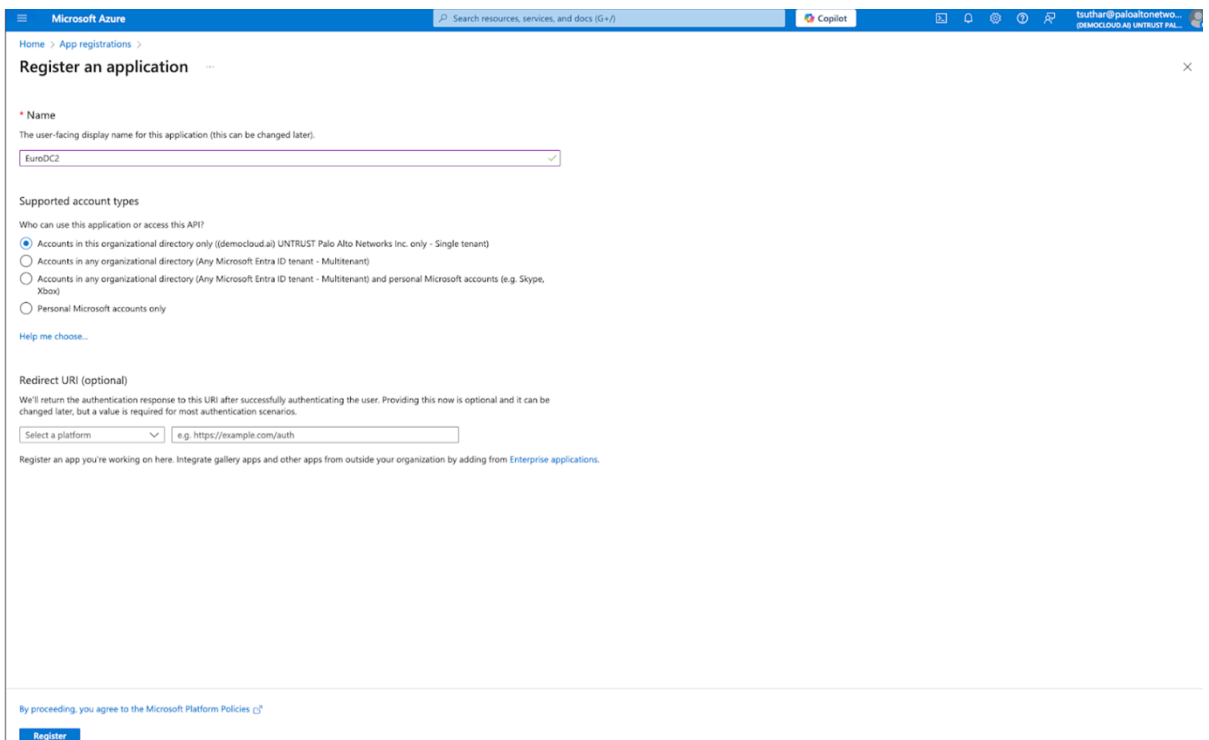
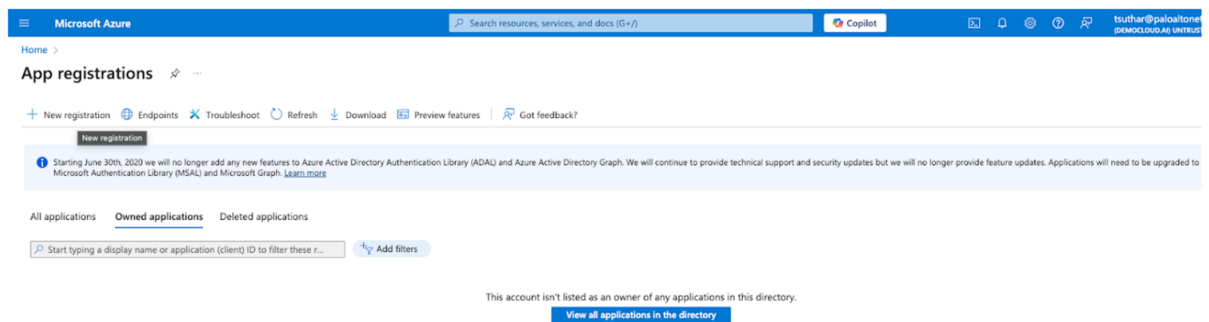
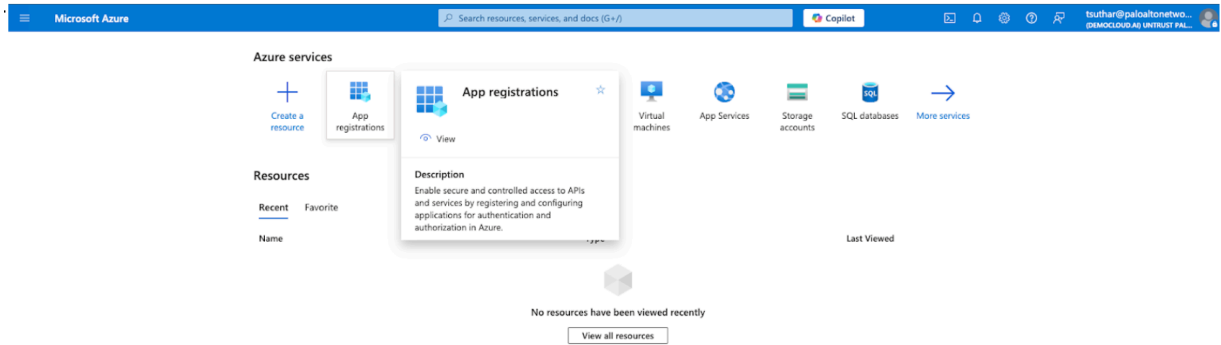
- A [resource group](#) with Azure vWAN with a single or multiple [Virtual Hub](#), defined for the regions of deployment (Brownfield Deployments only).
- To enable the [Azure BGP peering](#) with the Virtual WAN hub feature in this release, you must contact the Azure team with the Resource ID of your Virtual WAN resource.
- All regions must support the Azure Virtual Machine model Standard D8s v3 (8 vCPUs, 32 GiB).

Create and Acquire the Azure Information

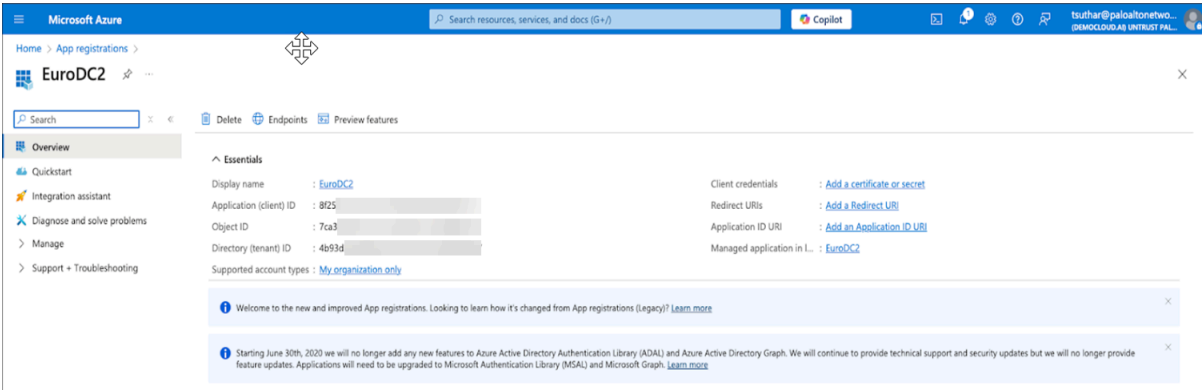
Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ Azure Virtual WAN CloudBlade

Before configuring Prisma SD-WAN to integrate with Azure vWAN, perform the following:

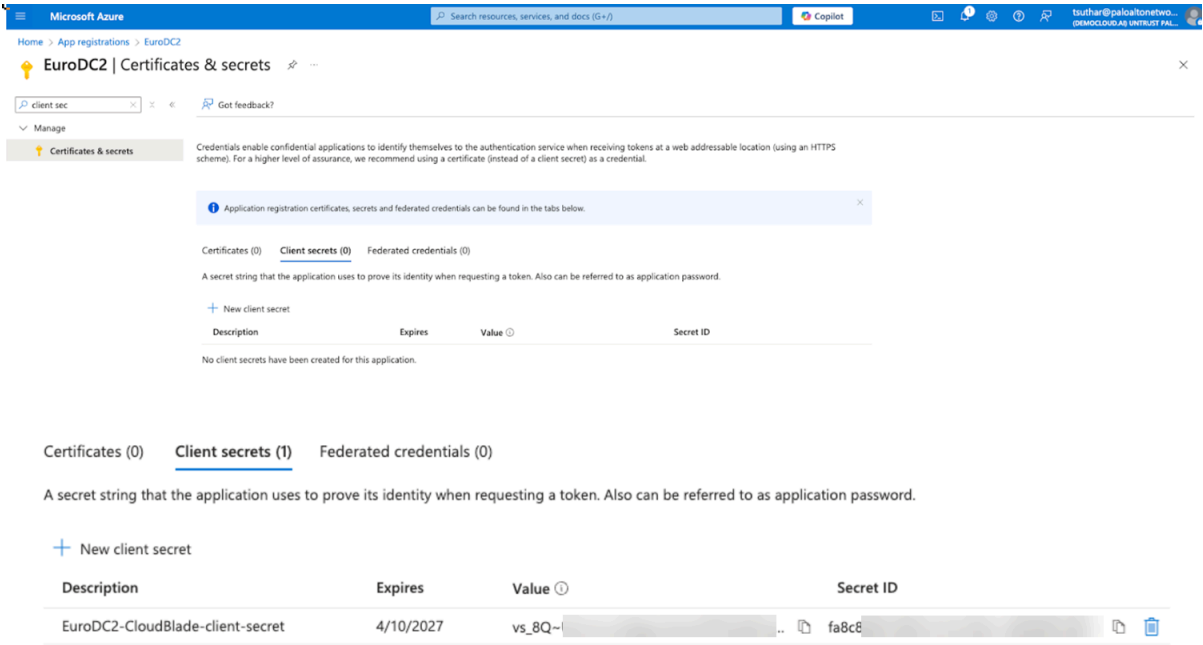
STEP 1 | Create an application registration object.



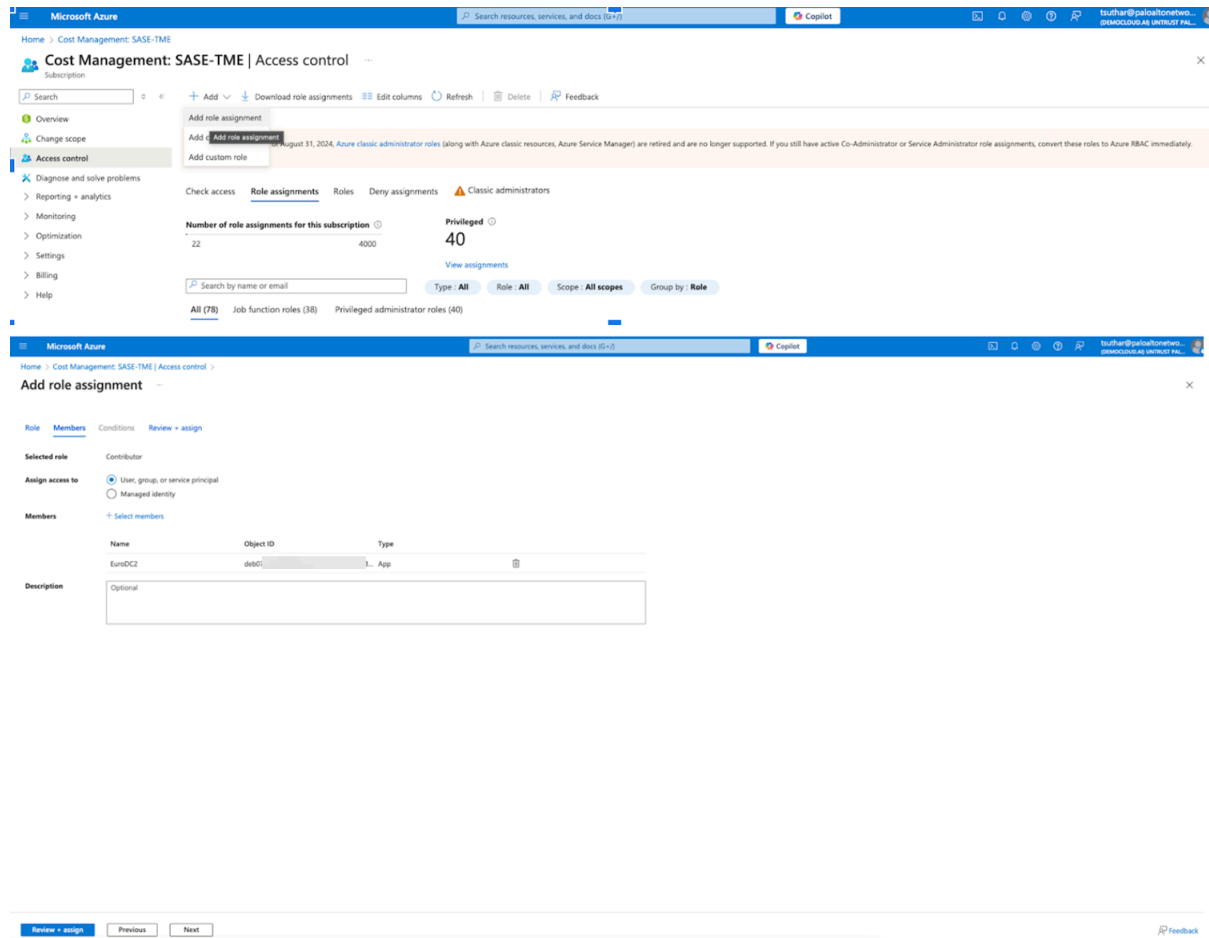
STEP 2 | Copy the Application Client ID and Directory tenant ID to be used later in Prisma SD-WAN CloudBlade configuration.



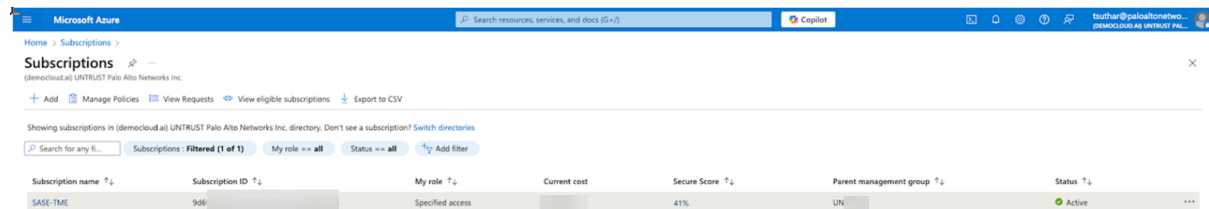
STEP 3 | Generate and copy a new client secret to be used later in Prisma SD-WAN CloudBlade configuration.



STEP 4 | Assign Contributor role to the new Application Registration object created in Step 1.



STEP 5 | Locate the Azure subscription ID and copy to be used later in Prisma SD-WAN CloudBlade configuration.



[Home](#) > [VisualStudioDevelopment](#) > [demo-virtual-wan](#) >

Create virtual hub

[Backs](#) [Site to site](#) [Point to site](#) [ExpressRoute](#) [Tags](#) [Review](#) > [create](#)

A virtual hub is a Microsoft managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premise network (spoke). The hub is the core of your network in the region. There can only be one hub per Azure region. When you create a hub using Azure portal, it creates a virtual hub, VNet and a virtual hub originatively. [Learn more](#)

Project details

The hub will be created under the same subscription and resource group as the vRNs.

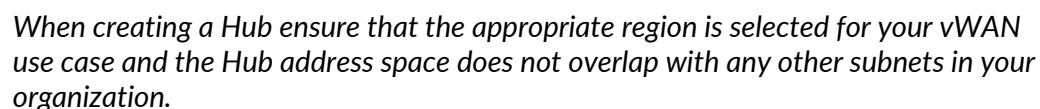
Subscription	AzureCOTIME
Resource group	VWAN-Demo-RG

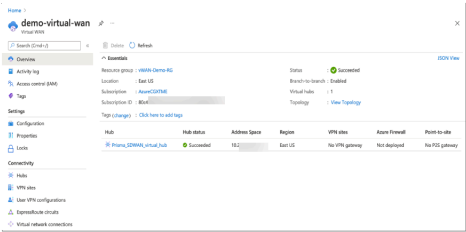
Virtual Hub Details

Region *	East US
Name *	Promia SOWAN, virtual hub
Hub private address space *	10.255.255.0/24

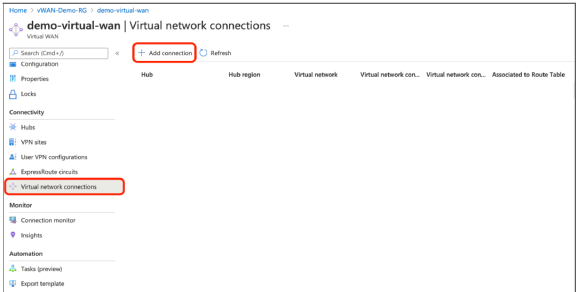
Creating a hub with a gateway will take 30 minutes.

[Review & create](#) [Previous](#) [Next: Site to site](#)





STEP 7 | (Optional) Add a virtual network connection to Virtual WAN in order to associate an existing VNET hosting applications and services to a vWAN Hub, such that this network could be reachable via vWAN.



Add connection

Connection name *

Demo-vWAN-VNET

Hubs *

Prisma_SDWAN_virtual_hub

Subscription *

AzureCOTME

Resource group *

vWAN-Demo-RG

Virtual network *

vWAN-Demo-VNET

Routing configuration

Propagate to none

Yes No

Associate Route Table

Propagate to Route Tables

0 selected

Propagate to labels

0 selected

Configure and Install the Azure Virtual WAN CloudBlade

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> ❑ Prisma SD-WAN license ❑ Azure Virtual WAN CloudBlade

Configure the Prisma SD-WAN CloudBlade to prepare the Prisma SD-WAN controller for integration.

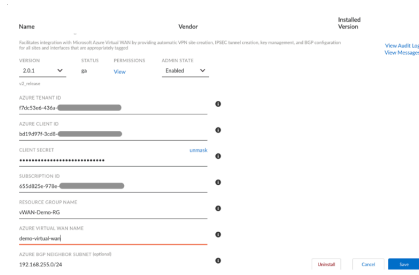
STEP 1 | From the Prisma SD-WAN Portal, choose the **CloudBlades** menu and select the Azure Virtual WAN Integration CloudBlade. If this CloudBlade does not appear, please contact Palo Alto Networks support.



STEP 2 | Clicking on the **Azure Virtual WAN Integration** CloudBlade will bring up the installation page. Provide the following information:

1. **Version:** Select the version of the Azure Virtual Network Integration CloudBlade.
2. **Admin State:** For Admin State, select/retain Enabled.
3. **Directory (tenant) ID:** Provide the Directory ID generated in the previous section on Azure application registration.
4. **Application (client) ID:** Provide the client ID generated in the previous section on Azure application registration.
5. **Client Secret:** Provide the client secret generated under the Azure application registration.
6. **Subscription ID:** Provide the subscription ID noted down from the previous section. Subscription ID is a GUID that uniquely identifies the subscription to use Azure services.
7. **Resource Group:** Provide the name of the resource group created in the previous section.
8. **Azure Virtual WAN Name:** Provide the name of the vWAN object created in the previous section.
9. **Azure BGP Neighbor Subnet:** Provide an IP block the CloudBlade can pull, to be used when provisioning the Standard tunnel interface on the ION, which will also be the BGP neighbor defined in the Azure vWAN VPN site object.

STEP 3 | Once the settings have been configured, click **Install** and **Save**.



Assign tags to objects in the Prisma SD-WAN

Once the CloudBlade is configured, the next task is to tag Prisma SD-WAN sites and interfaces to denote which sites and interfaces are candidates for integration with Azure Virtual WAN.

STEP 1 | In **Strata Cloud Manager**, go to **Workflows > Branch Sites** and select the site that needs to be tagged.

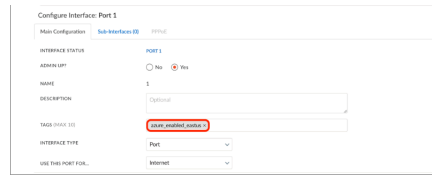
STEP 2 | Select the edit icon, and in the **Tags** (case sensitive.) field, add the **azure_enabled** tag and enable it for Azure vWAN.

The screenshot shows the Prisma SD-WAN configuration interface for a branch site. The 'NAME' field is 'Prisma-sdwan-Branch1'. The 'DESCRIPTION' field is 'test description 0529'. The 'TAGS' field is highlighted with a red box and contains the tag 'azure_enabled'. The 'ADDRESS SEARCH' field is 'JD'. The 'ADDRESS LINE 1' field is empty. The 'ADDRESS LINE 2' field is empty. The 'CITY' field is empty. The 'STATE' field is empty. The 'POSTAL CODE' field is empty. The 'COUNTRY' field is empty. The 'LATITUDE' field is '37'. The 'LONGITUDE' field is '-121'.

STEP 3 | Select **Done**.

STEP 4 | Now, tag the interface that you can use to establish a Standard tunnel to the virtual WAN. Go to **Workflows > Devices** and select the device to view the device configuration screen. Locate the interfaces tab, select the interface connected to the circuit you want to use to

build the tunnel to Azure, and add a region-specific tag that corresponds to the region the vWAN Hub you want to connect to is in (e.g. **azure_enabled_eastus**).



The screenshot shows the 'Configure Interface: Port 1' configuration page. The 'TAGS (max: 10)' field is highlighted with a red box and contains the tag 'azure_enabled_eastus'. Other fields include 'NAME' (1), 'DESCRIPTION' (Optional), 'INTERFACE TYPE' (Port), and 'USE THIS PORT FOR...' (Internet).



*This interface must have a public IP address configured statically or via DHCP, or if behind a NAT device one must have the **External NAT Address & Port** defined under the Advanced Options for this interface.*

In version 1.0.1, an Azure vWAN limitation restricts tagging and using only one interface to build a tunnel to a single vWAN hub in Azure. This restriction prevents the use of multiple transports to connect to the same vWAN hub. However, starting from version 2.0.1, Azure has removed this limitation, allowing multiple interfaces to build tunnels to the same vWAN hub. This enables the use of these tunnels in active/active mode for enhanced connectivity to the vWAN hub

STEP 5 | After completing this configuration, the next integration cycle (approximately 60 seconds) will initiate the creation and onboarding of Standard IPSEC tunnels between the Prisma SD-WAN ION and the Azure virtual WAN Hub. It may take several cycles for the tunnels to appear and become active on the Prisma SD-WAN and for the VPN site objects to show up in the Azure.

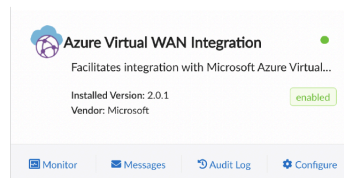
Validate the Prisma SD-WAN Configuration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license Azure Virtual WAN CloudBlade

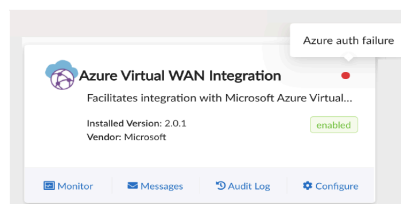
The Azure vWAN CloudBlade provisions the VPN sites, BGP peering configuration, and vWAN Hub association on Azure. On the Prisma SD-WAN ION device, two Standard IPSEC VPN tunnel interfaces, BGP peer configuration, and a static route to facilitate the BGP peering will be created. In addition, at a Prisma SD-WAN system level a Standard endpoint and service group will be created which can be used in path policies to direct the desired application traffic to Azure.

The following steps can be used to validate if the CloudBlade is working as intended:

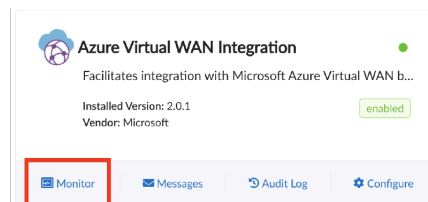
STEP 1 | Check the status indicator on the CloudBlade window. Once enabled and deployed correctly, the status indicator should turn green.



STEP 2 | If the access credentials are invalid, the status indicator will throw an **Azure auth failure** error message.



STEP 3 | The **Monitor** tab on the CloudBlade shows the deployment status of the integration.

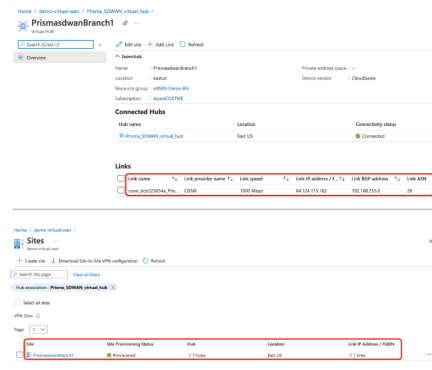


STEP 4 | The below example is from the Azure portal deployment for the Branch site in the previous section. The CloudBlade creates a single VPN site object with the public IP address of the demo Branch ION. This is associated with the vWAN hub in the East US region, which was

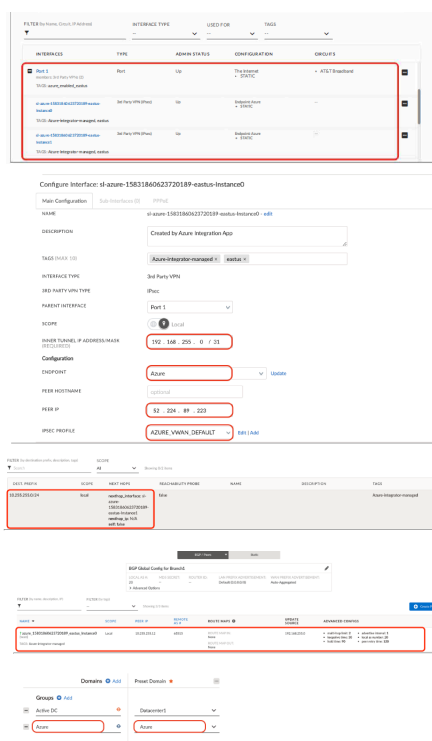
created earlier when the tag was applied to interface 1. The VPN site has BGP enabled with the AS# configured on the ION, and the peering address is the Standard inner tunnel IP.



If no previous BGP AS# is available on the ION, a BGP AS number is automatically assigned from the private AS range by the CloudBlade.



STEP 5 | The below example is the CloudBlade configuration on Prisma SD-WAN (Standard tunnel interface, static route, BGP peer, Standard endpoint & group).



Once the configuration is validated and the tunnel and BGP session is up, the administrator can modify the path policy applied to the site to direct the appropriate application traffic toward Azure.

Edit Application Network Path Policy Rules

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license Azure Virtual WAN CloudBlade

Once the CloudBlade configures the appropriate Standard objects within Prisma SD-WAN and Azure, the administrator can reference the path (Standard VPN) and service group (Azure) within application network policies. The ION devices will make intelligent per-app path selections using the network policies to chain multiple path options together in Active-Active and Active-Backup modes.

Example:

Application A: Take Standard VPN to Azure as the only path option.

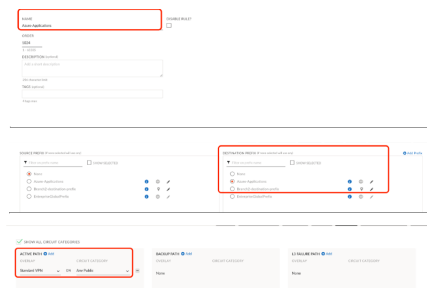
Application B: Active Standard VPN to Azure; Backup Prisma SD-WAN VPN

Application C: Active Prisma SD-WAN VPN; Backup Standard VPN to Azure

The Prisma SD-WAN secure Application Fabric (AppFabric) enables granular controls for virtually unlimited number of policy permutations down to the sub-application level. Below is an example of how to configure a path policy rule to use the Standard VPN to Azure. For a more in-depth description of how to configure path policies, Standard groups, and domains, refer to the [Prisma SD-WAN Admin Guide](#).

In **Strata Cloud Manager**, go to **Manage > Policies > Path** and choose a policy set of interest. Within the policy set, click **Add Rule** and define the following; Name, Network Contexts, destination prefixes or apps of interest (or a combination of both apps and prefixes), active and backup paths, and service and DC groups.

We will use a destination prefix-based rule in this example since we have already defined a path prefix representing all of our Azure subnets. Also, we will only use a Standard VPN path to the Standard Azure group. If the Standard VPN goes down, traffic destined to any of those prefixes will have no available paths. We could have specified alternate active or backup paths such as the Prisma SD-WAN VPN to the Data Center site(s).





*If **Standard VPN** is used in a network policy, then you must have a Standard Services and DC Group defined in the policy for the traffic to transit through that group. If not, traffic will be black-holed.*

*If **Required** is selected, traffic will always transit through the Services and DC Group. If not selected, traffic may or may not transit through the Services and DC Group as per the paths allowed.*

Manage and Troubleshoot the Azure vWAN CloudBlade

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ Azure Virtual WAN CloudBlade

The following sections detail various operations and troubleshooting scenarios related to the integration process:

Enable, Pause, Disable and Uninstall the Integration

After the Integration has been set up, operations can be done in the CloudBlade panel. These operations have various effects on the Tunnels and configurations in Prisma SD-WAN and Azure.

Set the CloudBlade to Enabled

This is the standard, expected mode of operation for the Extension. The CloudBlade will run every 60 seconds, find any new Sites/Interfaces with the appropriate tags, and configure the integration on Azure and Prisma SD-WAN. In addition, during this integration run if any settings were previously modified manually on either Prisma SD-WAN or Azure (e.g. VPN site object accidentally removed in the Azure portal) these will be reverted to the known good state automatically.

Set the CloudBlade to Paused

Pausing the CloudBlade stops all future integration runs but leaves any created objects intact. This stops any future objects from getting created, but does NOT prevent removal of any unconfigured/untagged objects on either Prisma SD-WAN or Azure.

Set the CloudBlade to Disabled

Disabling the CloudBlade tells the system to remove and delete all configurations created by the CloudBlade. This can cause communication interruptions if policy is not set to use other paths. Note that IPSEC policies, IKE policies, and Prisma SD-WAN Endpoints and Service and DC groups are not automatically deleted and must be removed manually.

Uninstall the CloudBlade

Uninstalling the CloudBlade removes the configuration for the CloudBlade, and immediately stops any changes by the CloudBlade. Uninstalling the CloudBlade does not automatically remove configuration from all sites and objects. CloudBlades may be Uninstalled and Reinstalled to facilitate upgrades or downgrades to different versions without traffic interruption. To completely remove all items, please set the CloudBlade to Disabled for 2-3 Integration Run periods (180 seconds) before Uninstalling.

List of Interface Specific Tags

The following is the list of interface specific tags that can be applied to an ION which correspond to a specific Azure region. The vWAN Hub must exist in the region before you apply the region-specific tag to the interface(s).

- azure_enabled_australiacentral
- azure_enabled_australiacentral2
- azure_enabled_australiaeast
- azure_enabled_australiasoutheast
- azure_enabled_brazilsouth
- azure_enabled_canadacentral
- azure_enabled_canadaeast
- azure_enabled_centralus
- azure_enabled_eastasia
- azure_enabled_eastus
- azure_enabled_eastus2
- azure_enabled_francecentral
- azure_enabled_francesouth
- azure_enabled_centralindia
- azure_enabled_southindia
- azure_enabled_westindia
- azure_enabled_japaneast
- azure_enabled_japanwest
- azure_enabled_koreacentral
- azure_enabled_koreasouth
- azure_enabled_northcentralus
- azure_enabled_northeurope
- azure_enabled_southcentralus
- azure_enabled_southeastasia
- azure_enabled_uksouth
- azure_enabled_ukwest
- azure_enabled_westcentralus
- azure_enabled_westeurope
- azure_enabled_westus
- azure_enabled_westus2

Chatbot CloudBlade for Slack Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> ❑ Prisma SD-WAN license ❑ Chatbot CloudBlade for Slack

Today, most enterprises rely on collaborative applications such as Slack and Microsoft Teams to do their day-to-day tasks. These applications come equipped with Bots that can be integrated into the Prisma SD-WAN Controller through the SDK to provide instant real-time data analytics.

Prisma SD-WAN introduces the **Chatbot CloudBlade for Slack** which provides instant SD-WAN visibility. The Chatbot interactively queries analytics on any device and from any location without logging into a corporate network. You can access information on site health, on-site and device configuration, device inventory, event notifications, metrics on bandwidth utilization, application health, and application performance. It supports NLP (Natural Language Processing) for commands, which helps in having an interactive discussion with the Bot rather than a fixed set of static commands.

Prerequisites

To set up the Chatbot CloudBlade for Slack, you must install the bot corresponding to your Prisma SD-WAN Controller region (Elcapitan, Sugarloaf, and Hood) in the Slack workspace. You can determine the region your tenant is hosted from the controller URL.

- An active Prisma SD-WAN subscription.
- An active Slack workspace.

Install Prisma SD-WAN Chatbot

You can install the Slackbot for the corresponding region by selecting one of the below **Add to Slack** options:

For Prisma SD-WAN (Hood)	For Prisma SD-WAN (Elcapitan)	For Prisma SD-WAN (Sugarloaf)
Add to Slack	Add to Slack	Add to Slack

Configure Chatbot CloudBlade for Slack

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license Chatbot CloudBlade for Slack

STEP 1 | Configure the CloudBlade in Prisma SD-WAN.

- From the Strata Cloud Manager, navigate to **Manage > Prisma SD-WAN > CloudBlades**.
- On the **Chatbot - Slack** configuration page, enter the following information, and change where appropriate.

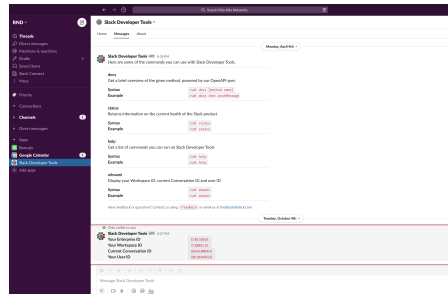
The screenshot shows the configuration page for the 'Chatbot - Slack' CloudBlade. The top section displays the name 'Chatbot - Slack', vendor 'Palo Alto Networks', and installed version '1.0.0'. Below this, there are tabs for 'VERSION', 'STATUS', 'PERMISSIONS', and 'ADMIN STATE'. The 'VERSION' tab is selected, showing '1.0.0'. The 'STATUS' tab shows 'OK'. The 'PERMISSIONS' tab shows 'View'. The 'ADMIN STATE' tab shows 'Enabled'. The 'SLACK WORKSPACE INFORMATION' section contains a text field with the value 'T02RQ2T9G5A'. Below this, there is a section for 'MAX NUMBER OF RECORDS TO BE SENT IN CHANNEL FOR A REQUEST' with a value of '100'. There are also checkboxes for 'ENABLE ALERTS/ALARMS NOTIFICATION' and 'EVENT CODES (optional)' with a dropdown menu showing 'DEVICEHW_INTERFACE_DOWN'. At the bottom, there is a field for 'SLACK [ENTERPRISE ID, WORKSPACE ID AND CHANNEL ID FOR EVENT CODES (optional)]' with the value 'ECDC3DSRE7IAJNGFRRD03ACBW04CR'. Buttons for 'Uninstall', 'Cancel', and 'Save' are at the bottom right.

- Version:** Select the latest version of the Chatbot CloudBlade for Slack.
- Admin State:** For Admin State, select Enabled.
- Slack Workspace Information:** Enter the Enterprise ID and Workspace ID as comma-separated values. It must be entered in the format `<Enterpriseld1:Workspaceld1,Enterpriseld2:Workspaceld2>`. If the Enterprise ID is not available, enter the Workspace ID. Workspace ID represents the Slack Workspace in which the bot is installed, and if the team belongs to an Enterprise

Grid, the enterprise_id will indicate the enterprise organization. These values can be obtained by typing the below command in the Slack user interface.

```
/sdt whoami
```

The ID will display in a snippet output.



- **Max Number of Records to be Sent In Channel for Request:** Enter the maximum number of records to be shown on the chat screen for a single command.
- **Enable Alerts/Alarms Notification:** Enable or disable sending notifications about new alarms/alerts to the configured channel.
- **Optional Event Codes:** Select from the list of Event Codes to be configured. Notifications are sent only for those alarms or alerts which have event codes.
- **Optional Slack Enterprise ID, Workspace ID and Channel ID for Event Codes:** Enter the Channel/ Workspace ID and the Enterprise ID of the channel which need to notify alerts/alarms. Channel ID and Workspace ID are mandatory parameters. If you have an Enterprise ID, it must be entered in the format **<EnterpriseId:WorkspaceId:ChannelId>**.

The Enterprise ID and Workspace ID entered here must be configured previously in the **Slack Workspace Information** field. The Alarms and Alerts notifications will only be sent to those channels where the workspace is bound to the tenant.

3. Click **Save** and **Install**.

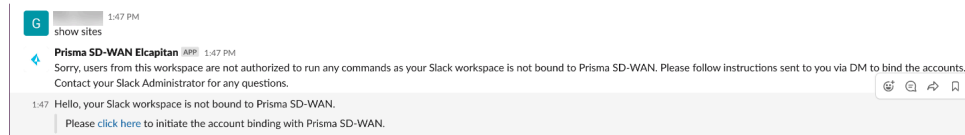
The CloudBlade generates a unique Authentication key of 64 characters, displayed on the **Monitoring > Integration Status** screen of the CloudBlade. You need to provide this Authentication key when binding a workspace to the Prisma SD-WAN tenant.

STEP 2 | Authorization and Account binding status of the workspace.

1. Go to **CloudBlades > Chatbot - Slack > Monitoring** and select the **Integration Status** tab.
The Authorization and Account binding status of each workspace will be visible.

ENTERPRISE	WORKSPACE	ACCOUNT BINDING STATUS	AUTHENTICATION KEY
-	TO2RQ2TNGSA	Bound	-
ECOC3DSUK	TO1RW2RQ2IA	Not Bound	ada7bed457134f46b7d435bda60473c7c9c902803a84ab18b0b6a6db1445d9f

2. Go to the Prisma SD-WAN Chatbot Slack app messages and type any command; otherwise, you can tag the bot from any Slack channel and type a command.



If the workspace is not bound to the tenant, the app displays an error message and provides a link to initiate the binding process.

3. Enter the 64-character Authentication key previously generated from the **Monitoring** screen and **Connect with your account**.



You will receive a Slack message confirming that the account binding is done.



You can unbind the workspace by deleting the Enterprise ID and Workspace ID from the CloudBlade configuration screen. To perform this action, you must be an authorized user on the Prisma SD-WAN controller with the right set of permissions (Admin).

Install Prisma SD-WAN Chatbot via Slack Authentication

STEP 1 | Add Chatbot CloudBlade for Slack to the channel.

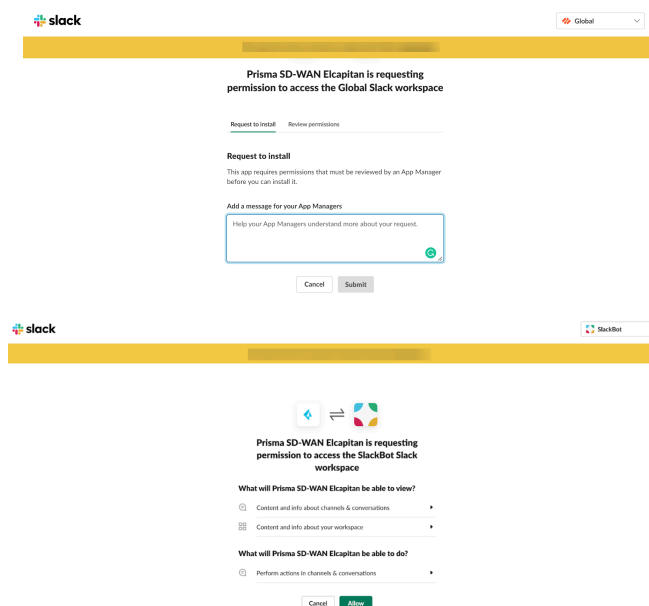
If the Chatbot is not installed in your workspace, go to the Prisma SD-WAN [Chatbot CloudBlade for Slack Integration](#) page, and select the required controller region-specific **Add to Slack** from the table.

You must install the Chatbot specific to the region your tenant is deployed. The Slack App Store will contain a Chatbot for each Prisma SD-WAN Controller region; Elcapitan, Sugarloaf, and Hood. You can determine the region your tenant is hosted from the controller URL.

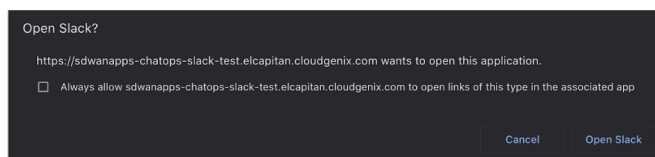
STEP 2 | Select the workspace where you wish to add the Chatbot. By default, Slack automatically selects one of your existing workspaces. You can add a new workspace, if required.



STEP 3 | Submit a request to your App Manager to install the Chatbot. Review and select **Allow** to accept the permissions listed.



STEP 4 | After accepting the Chatbot permissions, the browser redirects to the Slack desktop app or the web app.



STEP 5 | Install the Chatbot to a channel by typing **@Prisma SD-WAN (Controller region)**.

STEP 6 | You can now start a chat conversation with the Chatbot supported commands.

Chatbot Supported Commands

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ Chatbot CloudBlade for Slack

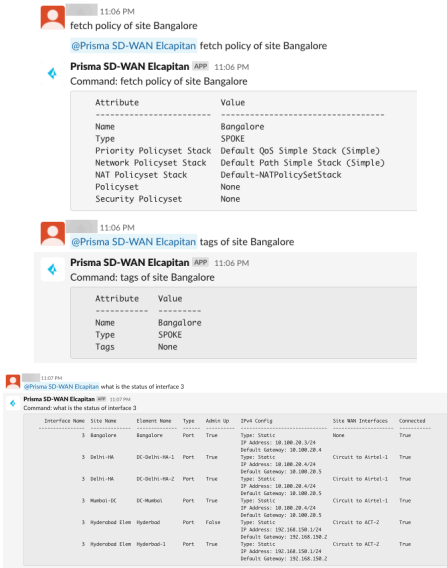
You can start a session by either typing **Help** or directly entering the command. The format of the command must include **@Prisma SD-WAN Chatbot <command>**.

For example:

```
@Prisma SD-WAN Elcapitan show sites
```

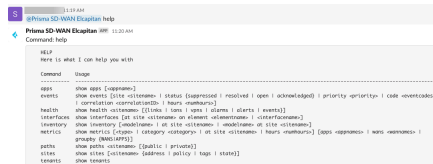
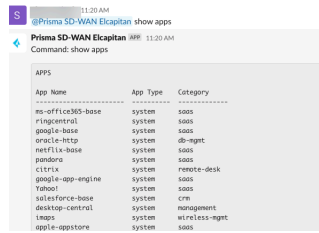
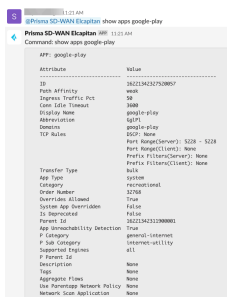
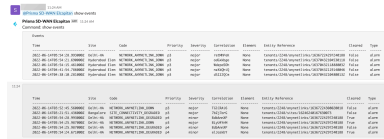
You can continue the conversation in the same channel OR directly message the bot 1-1. Based on the page size configured on Chatbot CloudBlade for Slack, the bot displays that many maximum records. You must type at least one of the options. If the site names have a space, enter the site name in double quotes. When the response for a command exceeds the supported size, the bot chunks the response.

The Chatbot supports **NLP (Natural Language Processing)** for commands, which helps in having an interactive discussion with the bot rather than a fixed set of static commands. The following examples do not display the supported command, however, the bot intelligently formulates and provides the correct response.

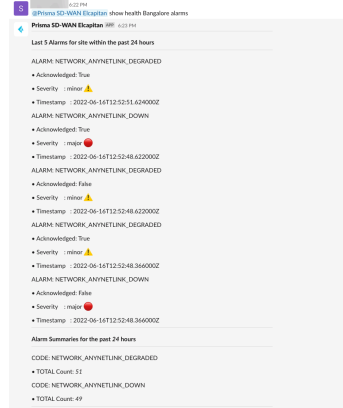
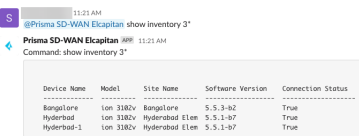



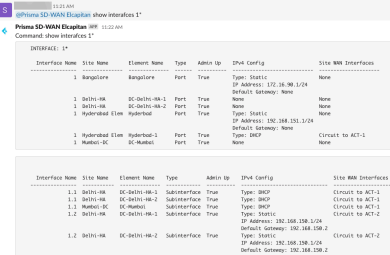
The Chatbot commands, supported options, and their descriptions are listed below:



Commands	Command Descriptions
help	
help	Lists all the supported commands.

Commands	Command Descriptions
<command> help	Displays the command syntax acceptable by the bot with all the options mentioned in the command. 
show apps	Lists all apps defined on the system. 
show apps <appname>	Lists all the application-specific attributes for the application app name. 
show events	
show events site <sitename>	Filters the list of events for a particular site. 
show events <status><suppressed resolved open acknowledged>	Filters the output to display the status of the events.
show events site <sitename>priority<priority>	Filters the events for a site based on the event priority.
show events code <eventcodes>	Filters the events for a particular event code.

Commands	Command Descriptions
show events correlation <correlationID>	Filters the events for a particular correlation ID.
show events hours <numhours>	Filters the events for a particular time frame.
show health	
show health <sitename>	<p>Displays the following attributes depicting the health of the site:</p>  <ul style="list-style-type: none"> • ION device connectivity status • critical and significant events • number of active events count by severity • physical link status • VPN health (Prisma SD-WAN and 3rdparty)
show health <sitename> links	<p>Filters the output to display physical link health.</p> 
show health <sitename> ions	Filters the output to display device health.
show health <sitename> vpns	<p>Filters the output to display VPN link health.</p> 

Commands	Command Descriptions
show health <sitename> alarms	Filters the output to display alarms. 
show inventory	
show inventory	Lists all the devices in the system (both claimed and unclaimed) with the device name, model, site name, software version, and connection status attributes. 
show inventory <modelname>	Lists the inventory to display devices of the specified model type. 
show inventory at site <sitename>	Lists the inventory to display devices at the specified site.
show inventory <modelname> at site <sitename>	Lists the inventory assigned to a site(s). 
show interfaces	
show interfaces at site <sitename> on element<elemname>	Displays the following interface attributes of admin status, type, name, ipv4_config, secondary_ip_configs, and site_wan_interface_ids.

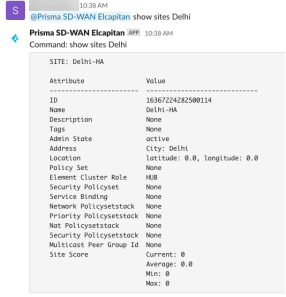
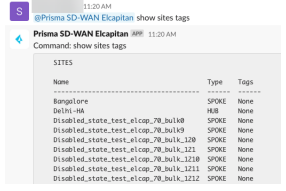
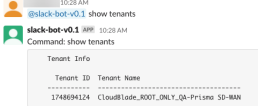
Commands	Command Descriptions
	<div></div>
<p>show interfaces <interfacename></p>	<p>Displays interface configurations of all the interfaces with the interface name with the following attributes:</p> <div></div> <ul style="list-style-type: none">• sitename• element name• admin status• type• ipv4_config• secondary_ip_configs• site_wan_interface_ids• connected
<p>show metrics—All metrics-related commands must have the options metric type, category, site, and hours. If the site name or the app name has a space, ensure the names are typed in double-quotes.</p>	
<p>show metrics <type> category <category> at site<sitename> hours <numhours> groupby<groupby></p>	<p>Displays specific metrics for the given site for the specified number of hours. The output displays a statistical distribution of the metrics queried for:</p> <ul style="list-style-type: none">• Count (Number of data points)• Mean• Standard Deviation• Minimum Value• Maximum Value• Percentile Values: 50, 75, 90
<p>Show metrics network <category> <bw> at site<sitename>hours <numhours>groupby<APPS></p>	<p>Displays the metrics, where the metric type is a network and the category is bandwidth for a given site for the specified number of hours for a given app(s).</p>

Commands	Command Descriptions
Show metrics network <category> <bw> at site<sitename>hours <numhours>	Displays the metrics, where the metric type is a network and the category is bandwidth for a given site for the specified number of hours. 
Show metrics network <category> <bw> at site<sitename> hours<numhours>groupby<APPS> groupby<WANS>	Displays the metrics, where the metric type is a network and the category is bandwidth for a given site for the specified number of hours, for a given app(s), and the selected WANs.
Show metrics network <category> <bw> at site< sitename>hours <numhours>groupby <Top10>groupby<APPS>	Displays the metrics for the top 10 apps where the metric type is a network and the category is bandwidth for a given site for the specified number of hours.
Show metrics network <category>tcp<tcp-xsact>at site <sitename>hours <numhours>	Displays the TCP metrics where the metric type is a network and the category is tcp-xsact for a given site for the specified number of hours. 
Show metrics network <category> tcp<tcp-xsact>at site <sitename> hours<numhours>groupby<APPS>	Displays the TCP metrics, where the metric type is a network and the category is tcp-xsact for a given site for the specified number of hours for a given app(s).
Show metrics network <category> <tcp-xsact> atsite <sitename>hours<numhours> >groupby<WANS>	Displays the TCP metrics, where the metric type is a network and the category is tcp-xsact for a given site for the specified number of hours and selected WANs.
Show metrics network <category> <tcp-xsact> atsite <sitename>hours<numhours> groupby<APPS> groupby<WANS>	Displays the TCP metrics, where the metric type is a network and the category is tcp-xsact for a given site for the specified number of hours, for a given app(s), and the selected WANs.

Commands	Command Descriptions
Show metrics app <category> <health> at site<sitename> hours <numhours>groupby<APPS>	Displays the app(s) health metrics, for a given site for the specified number of hours for a given app(s).
Show metrics app <category> <health> at site<sitename> hours<numhours>groupby <APPS>groupby<WANS>	Displays the app(s) health metrics for a given site for the specified number of hours, for a given app(s) and the selected WANs or all WANs. 
Show metrics app <category> <app-response> atsite <sitename>hours<numhours> groupby<APPS>	Displays the app response metrics, for a given site for the specified number of hours for a given app(s).
Show metrics app <category> <app-response> atsite <sitename>hours<numhours> groupby<APPS> groupby<WANS>	Displays the app response metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs.
Show metrics media <category> <audio-bw> atsite <sitename>hours<numhours> >groupby<APPS>	Displays the audio bandwidth metrics, for a given site for the specified number of hours for a given app(s).
Show metrics media <category> <audio-bw> atsite <sitename>hours<numhours> >groupby<APPS>groupby<WANS>	Displays the audio bandwidth metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs.
Show metrics media <category> <audio-jitter> atsite <sitename>hours<numhours> >groupby<APPS>	Displays the audio jitter metrics, for a given site for the specified number of hours for a given app(s).

Commands	Command Descriptions
Show metrics media <category> <audio-jitter> atsite <sitename>hours<numhours> groupby<APPS>groupby<WANS>	Displays the audio jitter metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs.
Show metrics media <category> <video-jitter> atsite <sitename>hours<numhours> >groupby<APPS>	Displays the video jitter metrics, for a given site for the specified number of hours for a given app(s).
Show metrics media <category> <audio-loss> atsite <sitename>hours<numhours> <groupby><APPS>	Displays the audio-loss metrics, for a given site for the specified number of hours for a given app(s).
Show metrics media <category> audio-loss> atsite <sitename>hours<numhours> groupby<APPS>groupby<WANS>	Displays the audio loss metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs.
Show metrics media <category> <video-loss> atsite <sitename>hours<numhours> <groupby><APPS>	Displays the video-loss metrics, for a given site for the specified number of hours for a given app(s).
Show metrics media <category> video-loss> atsite <sitename>hours<numhours> groupby<APPS>groupby<WANS>	Displays the video loss metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs.
Show metrics media <category> <audio-mos> atsite <sitename>hours<numhours> <groupby><APPS>	Displays the audio-mos metrics, for a given site for the specified number of hours for a given app(s).
Show metrics media <category> audio-mos> atsite <sitename>hours<numhours>	Displays the audio-mos metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs.

Commands	Command Descriptions
groupby<APPS>groupby<WANS>	
show paths	
show paths <sitename>	<p>Displays all the paths, overlay + underlays, at a given site.</p>  <ul style="list-style-type: none"> • Internet • Private WAN • VPN over Internet • VPN over Private WAN • Standard VPN
show paths <sitename> public	<p>Displays the public paths, overlay + underlays, at a given site.</p> <ul style="list-style-type: none"> • Internet • VPN over Internet • Standard VPN
show paths <sitename> private	<p>Displays the private paths, overlay +underlays, at a given site.</p> <ul style="list-style-type: none"> • Private WAN • VPN over Private WAN
show sites	
show sites	<p>Lists all the sites, site type (hub v/s spoke), admin state, tags, and domain.</p> 

Commands	Command Descriptions
show sites <sitename>	<p>Lists all the site properties such as an address, location, tags, and attached policies.</p>  <pre> SITE: Delhi-HA ----- Attribute Value ----- ID 16367224262580114 Name Delhi-HA Description None Tags None Admin State active Address City: Delhi Location Latitude: 0.0, Longitude: 0.0 Policy Set None Element Cluster-Role HUB Security Policyset None Service Binding None Network Policysetstack None Priority Policysetstack None Nat Policysetstack None Security Policysetstack None Multicast Peer Group Id None Site Score Current: 0 Average: 0.0 Min: 0 Max: 0 </pre>
show sites <sitename> address	Lists the addresses of all the sites.
show sites <sitename> policy	Lists the path, QoS, Security, and NAT policies attached to the site.
show sites <sitename> tags	<p>Lists the tags attached to the site.</p>  <pre> SITES ----- Name Type Tags ----- Bangalore SPOKE None Delhi-HA HUB None Disabled_state_test_elcop_78_hu140 SPOKE None Disabled_state_test_elcop_78_hu149 SPOKE None Disabled_state_test_elcop_78_hu150 SPOKE None Disabled_state_test_elcop_78_hu151 SPOKE None Disabled_state_test_elcop_78_hu152 SPOKE None Disabled_state_test_elcop_78_hu153 SPOKE None Disabled_state_test_elcop_78_hu154 SPOKE None </pre>
show tenants	
show teanants	<p>Lists tenant information like tenant ID and tenant name.</p>  <pre> Tenant Info ----- Tenant ID Tenant Name ----- 1748094124 CloudBlade_ROOT_ONLY_Qa-Prisma SD-WAN </pre>

Manage and Monitor the Chatbot CloudBlade for Slack Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> ❑ Prisma SD-WAN license ❑ Chatbot CloudBlade for Slack

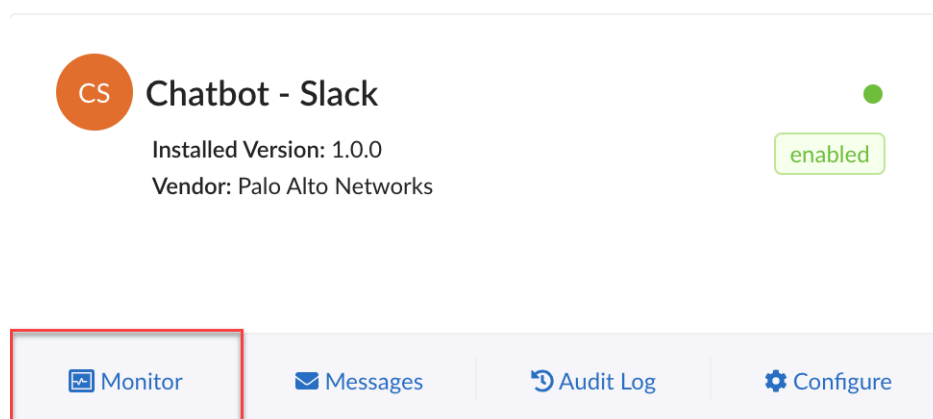
The following sections explain various scenarios related to the integration process.

Administrators can manage the Chatbot Slack through the Prisma SD-WAN web interface by setting the bot in several states.

- **Enable**—This is the expected mode of operation for the CloudBlade. In this mode, the CloudBlade is performing its desired and intended functionality. Any configuration changes will automatically reconfigure the integration on Chatbot Slack and Prisma SD-WAN in 60 seconds.
- **Paused**—Pausing the CloudBlade stops all future integration runs. The chatbot responses will be paused in this state.
- **Disable**—Disabling the CloudBlade tells the system to remove and delete the Slack workspace and channel information created by the CloudBlade.
- **Uninstall**—Uninstalling the CloudBlade removes all configuration parameters pertinent to the CloudBlade, mainly the Slack workspace ID and channel information for the CloudBlade. Therefore, for a clean uninstall, it is recommended to set the CloudBlade to a disabled state for 2-3 minutes before uninstalling.

Monitor the Chatbot CloudBlade for Slack

The Chatbot Slack CloudBlade provides indicators to determine the operational status, displays integration status, and real-time error messages. Select **Monitor** on the **Chatbot - Slack** tile to view the **Command History** and **Usage Trend** of the Chatbot CloudBlade for Slack.



The **Integration Status** tab provides information on the account-binding status of the workspace with the following attributes:

CloudBlade > Monitoring "Chatbot - Slack"

Chatbot - Slack

Monitoring

Integration Status Command History Usage Trend

Refresh Columns

ENTERPRISE	WORKSPACE	ACCOUNT BINDING STATUS	AUTHENTICATION KEY
-	T02RQ2T9G5A	Bound	-
ECOC3DSUK	T01RW2RQ21A	Not Bound	a6a78ed457134446b9d435a8da0473f5c9f02803a84b18b03a66db51445d9

- **Enterprise:** The enterprise Id of the Slack workspace entered when configuring the CloudBlade.
- **Workspace:** The workspace Id of the Slack workspace entered when configuring the CloudBlade.
- **Account Binding Status:** Displays whether the account is bound or not.
- **Authentication key:** The authentication key is visible if a workspace is not bound to a Prisma SD-WAN tenant.

The **Command History** tab maintains a list of commands executed through the Chatbot the following attributes:

CloudBlade > Monitoring "Chatbot - Slack"

Chatbot - Slack

Monitoring

Command History Usage Trend

Refresh Columns

SLACK USER NAME	SLACK USER ID	COMMAND	STATUS	TIME	MESSAGE
Gen Jacob	U02RMQXDUN7	help	Success	2022-06-10 05:54:54	-
Gen Jacob	U02RMQXDUN7	show events	Success	2022-06-10 05:55:08	-
Gen Jacob	U02RMQXDUN7	show metrics network category bw at site Bangalore hours 24	Success	2022-06-10 05:55:58	-
Gen Jacob	U02RMQXDUN7	show apps	Success	2022-06-10 05:56:19	-
Gen Jacob	U02RMQXDUN7	show apps google play	Success	2022-06-10 05:56:39	-
Shyam Singh	U02RSL4FEH	show health Delhi PK	Success	2022-06-09 05:03:49	-
Shyam Singh	U02RSL4FEH	help	Success	2022-06-09 05:03:03	-
Shyam Singh	U02RSL4FEH	health help	Success	2022-06-09 05:03:16	-
Shyam Singh	U02RSL4FEH	show health alarms	Fail	2022-06-09 05:03:29	Invalid format. Please use 'health help' for details on supported syntax.
Shyam Singh	U02RSL4FEH	show health Bangalore alarms	Success	2022-06-09 05:03:47	-

1 2 3 4 5 ... 14 > 10 / page

- **Slack User Name:** The user name of the chat application user.
- **Slack User ID:** The ID of the chat application user.
- **Command:** The command given.
- **Status:** The status of the command (Success or Fail).
- **Time:** The time when the command was given.
- **Message:** Displays real-time error messages.

The **Usage Trend** tab displays statistics on the bot usage for the past 24 hours and a seven day average with the following data:

CloudBlade > Monitoring "Chatbot - Slack"

Chatbot - Slack

Monitoring

Command History Usage Trend

Refresh Columns

COMMAND	24 HOUR COUNT - COMMAND	7 DAY AVERAGE - COMMAND	UNIQUE USERS - 24H	UNIQUE USERS - 7D
show health	9	4	1	1
help	14	3	1	1
show sites	24	6	1	1
show apps	21	4	1	1
show events	0	1	0	1
show inventory	14	3	1	1
show interfaces	0	1	0	1
show metrics	0	1	0	1
show paths	0	1	0	1

- **Command:** The command given.
- **24 Hour Count Command:** The command count runs in the past 24 hours.

- **7 Day Average Command:** The average count of commands in the past seven days.
- **Unique Users-24H:** The count of users in the past 24 hours.
- **Unique Users-7D:** The count of users in the past 7 days.

Chatbot MS Teams CloudBlade Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> ❑ Prisma SD-WAN license ❑ Chatbot MS Teams CloudBlade

Today, most enterprises are shying away from emails for their day-to-day collaborative work and increasingly use applications like MS Teams to enable seamless collaboration. These applications come equipped with Bots that allow you to interact using predefined options to access real-time information.

Prisma SD-WAN introduces the Prisma SD-WAN Chatbot MS Teams CloudBlade that allows efficient collaboration by giving the end-user access to the Prisma SD-WAN network at any time from anywhere through the MS Teams Chatbot. As part of this integration, a user group is created on MS Teams, and the Azure ID of the User Group generated is then used to configure the Chatbot MS Teams CloudBlade on Prisma SD-WAN. You can access real-time information on on-site and device configuration, site health, device inventory, events, and metrics on bandwidth utilization, application health, and application performance. The data can be consumed directly on MS Teams applications, enabling Network Operation Center teams to manage the Prisma SD-WAN network.

Prerequisites

To set up the Prisma SD-WAN Chatbot, a user group needs to be created on Microsoft Teams. This user group is then configured on the Chatbot MS Teams CloudBlade to let Prisma SD-WAN know the users authorized to use the chatbot. Administrators can configure multiple user groups on the Chatbot MS Teams CloudBlade, allowing multiple teams and users to access the bot through their channel.

- An active Prisma SD-WAN subscription.
- An Active MS Teams account.

Create User Groups and Configure Chatbot MS Teams

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ Chatbot MS Teams CloudBlade

STEP 1 | Create a user group on MS Teams. You can follow any of the following methods to create a user group:

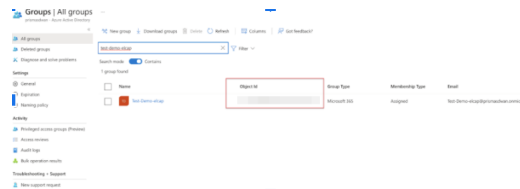
- [Create a user group on Azure Active Directory](#)
- [Create a team/user group from scratch](#)
- [Create a team from an existing team](#)
- [Create a team from an existing group](#)

STEP 2 | After a user group is created on MS Teams, copy the User Group ID (object ID).

Enter the ID when configuring the Chatbot-MS Teams CloudBlade on Prisma SD-WAN. You can configure more than one user group on the CloudBlade. The User Group ID(s) can be retrieved by any of the following methods:

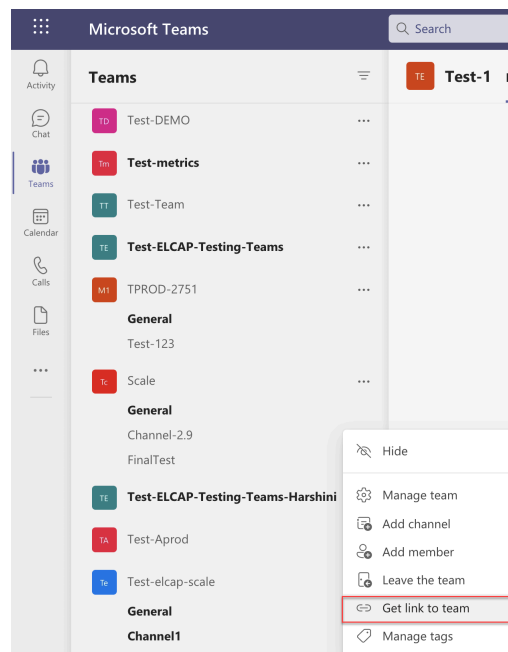
- **Azure Active Directory**

1. Go to the **Azure Active Directory** portal and select **Groups** on the left panel.
2. Search and select the specific **User Group** and copy the **object-id** from the Azure portal.



- **Microsoft Teams**

1. Go to your **Team > More Options > Get a link to Team**.
2. This provides a URL that contains the group-id.



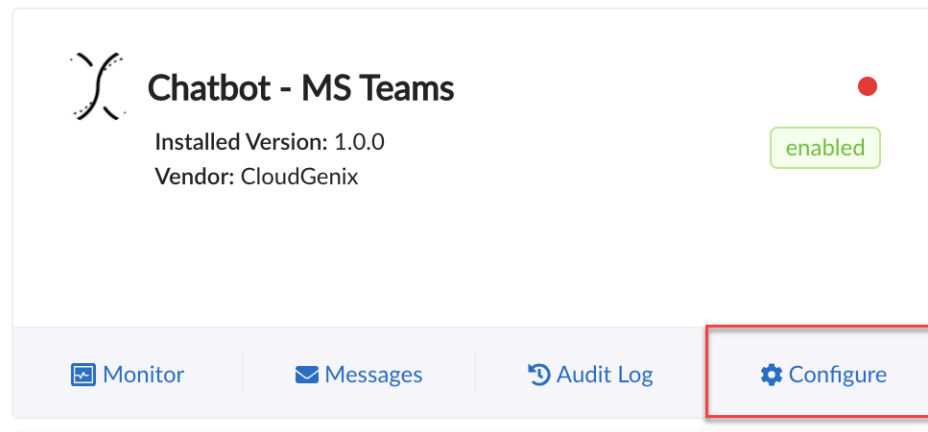
For example, the **Get link to Team** option will display a URL like the one below. Embedded in the URL is the **groupId** highlighted below. Only copy the groupId text between = and & for configuration on the CloudBlade.

```
https://teams.microsoft.com/l/team/19%3afZljepRtSxrVfX1hkf876XCvPFY_jion787GBcD5lvY1%40thread.tacv2/conversations?groupId=abc6d320-b3f1-87c2-8755-02e9endaeda1&tenantId=123dr678-h456-b758-b010-41830555h3bd
```

Configure Chatbot MS Teams

STEP 1 | From the Strata Cloud Manager, select **Manage > Prisma SD-WAN > CloudBlades**.

STEP 2 | In CloudBlades, locate the **Chatbot MS Teams** tile and click **Configure**.



Contact the Palo Alto Support team if this CloudBlade does not appear in the list.

STEP 3 | In the **Chatbot-MS Teams** page, enter the following information in the fields shown below, change where appropriate.

- **Version:** Select the latest version of the Chatbot-MS Teams CloudBlade.
- **Admin State:** For Admin State, select Enabled.

STEP 4 | Microsoft Teams Group Information: Enter the Teams group Azure Active Directory ID obtained in the previous section.

To add multiple user groups, enter the IDs as comma-separated values. For example:
Teams_group_AAD_ID1, Teams_group_AAD_ID2, Teams_group_AAD_ID3.

Name	Vendor	Installed Version
Chatbot - MS Teams	CloudGenix	1.0.0
VERSION 1.0.0	STATUS beta	PERMISSIONS View
ADMIN STATE Enabled		View Audit Log View Messages
MS TEAMS GROUP INFORMATION d76d0a77-23e8-4d91-9f05-af3c38a799fa		
Uninstall		Cancel Save

STEP 5 | Click **Save and Install**.

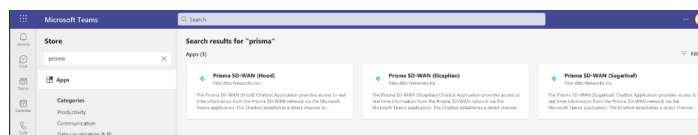
Assign Chatbot to a Channel/Team

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license Chatbot MS Teams CloudBlade

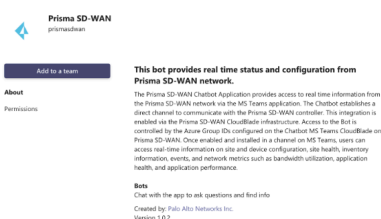
STEP 1 | Go to Microsoft Teams App store and search for **Prisma SD-WAN Chatbot**.



You must install the bot specific to the region your tenant is deployed. The Microsoft App Store will contain a Chatbot for each Prisma SD-WAN Controller region; Elcapitan, Sugarloaf, and Hood. You can determine the region your tenant is hosted from the controller URL.



STEP 2 | Click on the **Prisma SD-WAN Chatbot-MS Team** tile, select **Add to a Team** from the options.



STEP 3 | Select the team(s) where you want to set up the bot from the drop-down.

The teams where you can configure the Chatbot are listed on the left navigation pane.

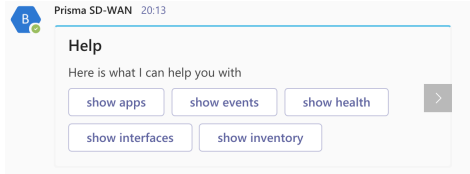
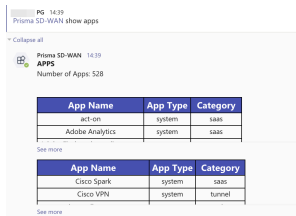

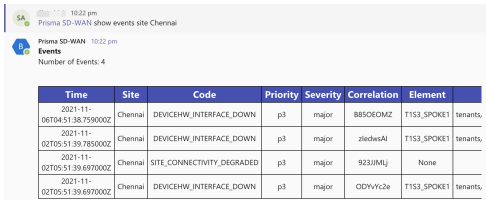
STEP 4 | You can now start a chat conversation with the Chatbot supported commands.

Chatbot Supported Commands

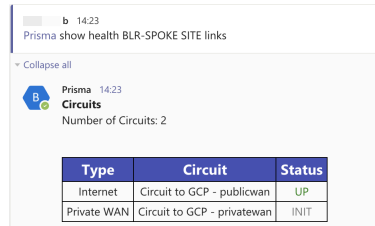
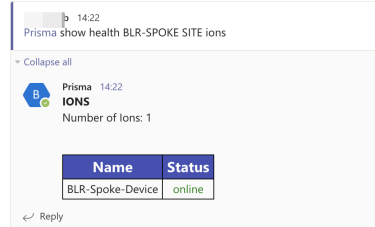
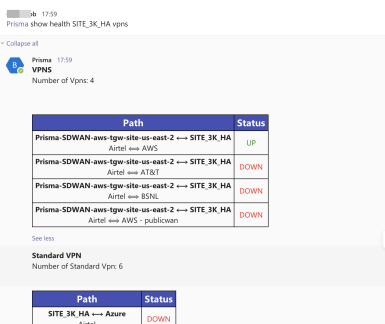
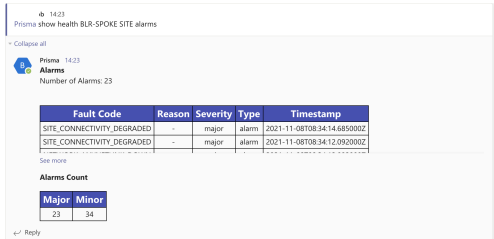
You can start a session by either typing **Help** or directly entering the command. The format of the command must include **@Prisma SD-WAN Chatbot <command>**. For example:

```
@Prisma SD-WAN Chatbot show sites
```

You can continue the conversation in the same window OR click **New Conversation** to start a new chat session. When the response for a command exceeds the supported size, the bot chunks the response. The bot will retrieve a maximum of 500 records for any category in the initial release. You will require to type at least one of the options. If the site names have a space, enter the site name in double quotes. The commands, supported options, and their descriptions are listed below:

Commands	Command Descriptions
help	
help	Lists all the supported commands.
<command> help	Displays the command syntax acceptable by the bot with all the options mentioned in the command. <div>  </div>
show apps	
show apps	Lists all apps defined on the system. <div>  </div>
show apps <appname>	Lists all the application-specific attributes for the application app name. <div>  </div>
show events	
show events site <sitename>	Filters the list of events for a particular site. <div>  </div>
show events <status><suppressed>	Filters the output to display the status of the events.

Commands	Command Descriptions
resolved open acknowledged>	
show events site <sitename> priority <priority>	<p>Filters the events for a site based on the event priority.</p> 
show events code <eventcodes>	<p>Filters the events for a particular event code.</p> 
show events correlation <correlationID>	<p>Filters the events for a particular correlation ID.</p> 
show events hours <numhours>	<p>Filters the events for a particular time frame.</p> 
show health	
show health <sitename>	<p>Displays the following attributes depicting the health of the site:</p> <ul style="list-style-type: none"> • ION device connectivity status • critical and significant events • number of active events count by severity • physical link status • VPN health (Prisma SD-WAN and 3rdparty)

Commands	Command Descriptions
show health <sitename> links	<p>Filters the output to only display physical link health.</p> 
show health <sitename> ions	<p>Filters the output to only display device health.</p> 
show health <sitename> vpns	<p>Filters the output to only display VPN link health.</p> 
show health <sitename> alarms	<p>Filters the output to only display alarms.</p> 
show inventory	
show inventory	<p>Lists all the devices in the system (both claimed and unclaimed) with the device name, model, site name, software version, and connection status attributes.</p>

Commands

Command Descriptions

TK Prisma SD-WAN (Elcapitan) 12:50 PM show inventory

B Prisma SD-WAN (Elcapitan) 12:50 PM
DEVICES
Number of Devices: 21

Device Name	Model	Site Name	Software Version	Connection Status
DAL-7K-1	ion 7108v	Dallas Data Center	4.5.0-b9	True
DAL-7K-2	ion 7108v	Dallas Data Center	4.5.0-b9	True
DHL-1	ion 2000	Dale Hollow	0.2.A55.157	False
ION-2K-A	ion 2000	Branch4-Rio	0.2.A55.157	False
ION-2K-B	ion 2000	Branch4-Rio	0.2.A55.157	False
MAD-7K-1	ion 7108v	Madrid DC Site	4.5.0-b9	True
MAD-7K-2	ion 7108v	Madrid DC Site	4.5.0-b9	True
MAN-3K-1	ion 3102v	Manchester Branch 3	4.5.0-b9	False
MIL-3K-1	ion 3102v	Milan Branch 2	4.5.0-b9	True
NI-3K-1	ion 3102v	New Jersey Branch 1	4.5.0-b9	False
Portland Sales Office ION	ion 3102v	Portland Sales Office	5.1.5-b4	False
SJ Branch	ion 3102v	SJ Branch	5.1.3-b16	False
None	ion 7108v	None	4.4.1-b47	False
None	ion 3102v	None	4.5.1-b1	False
None	ion 3102v	None	5.0.1-b6	False
None	ion 7108v	None	4.4.1-pre-b24	False
None	ion 3102v	None	4.4.1-pre-b24	False
None	ion 3102v	None	4.4.1-pre-b24	False
None	ion 3102v	None	5.0.1-b6	False
None	ion 3000	None	0.2.A55.157	False
None	ion 3000	None	0.2.A55.157	False

show inventory
<modelname>

Lists the inventory to display devices of the specified model type.

TK Prisma SD-WAN (Elcapitan) 12:53 PM show inventory ion 2000

B Prisma SD-WAN (Elcapitan) 12:53 PM
DEVICES
Number of Devices: 3

Device Name	Model	Site Name	Software Version	Connection Status
DHL-1	ion 2000	Dale Hollow	0.2.A55.157	False
ION-2K-A	ion 2000	Branch4-Rio	0.2.A55.157	False
ION-2K-B	ion 2000	Branch4-Rio	0.2.A55.157	False

See less

Reply

show inventory at site
<sitename>

Lists the inventory to display devices at the specified site.

TK Prisma SD-WAN (Elcapitan) 12:53 PM show inventory at site Dale Hollow

B Prisma SD-WAN (Elcapitan) 12:53 PM
DEVICES
Number of Devices: 1

Device Name	Model	Site Name	Software Version	Connection Status
DHL-1	ion 2000	Dale Hollow	0.2.A55.157	False

show inventory
<modelname> at site
<sitename>

Lists the inventory assigned to a site(s).

SS gh 13:06 Prisma SD-WAN show inventory ion 3104v at site AKASH1_BR-SITE3-ZSCALER

B Prisma SD-WAN 13:06
INVENTORY
Number of Inventory: 2

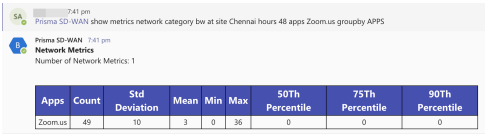
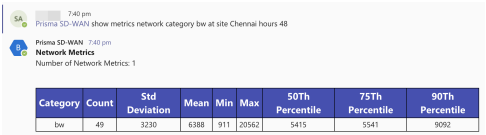
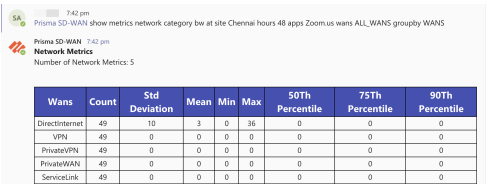
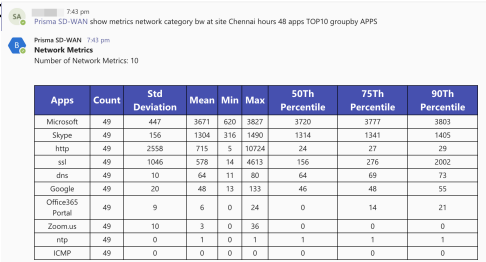

Device Name	Model	Site Name	Software Version	Connection Status
AKASH1_BR-SITE3-ELEM1-ZSCALER	ion 3104v	AKASH1_BR-SITE3-ZSCALER	5.5.1-b7	True
AKASH1_BR-SITE3-ELEM2-ZSCALER	ion 3104v	AKASH1_BR-SITE3-ZSCALER	5.5.1-b7	True

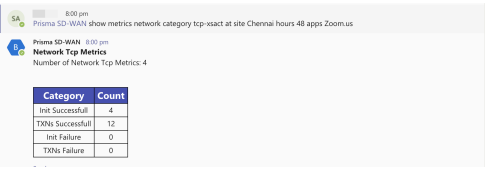
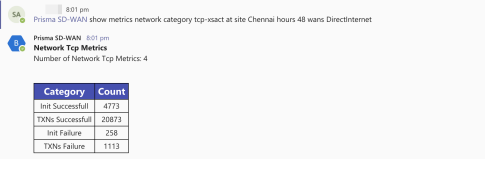

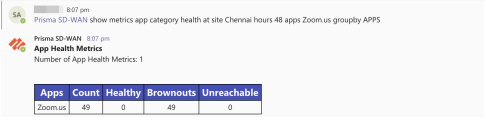
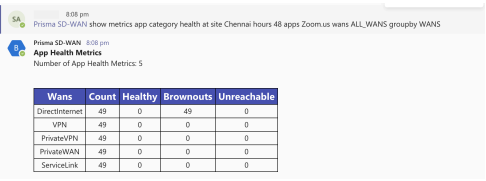
show interfaces

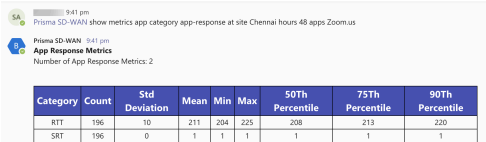
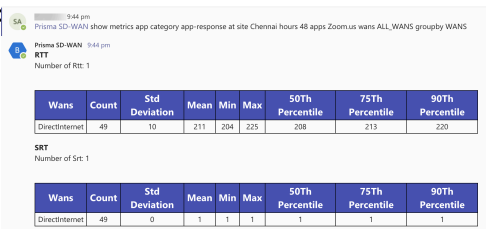
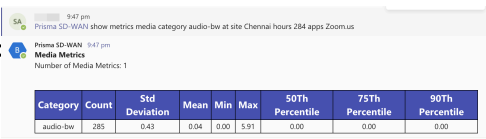
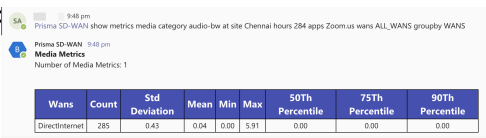
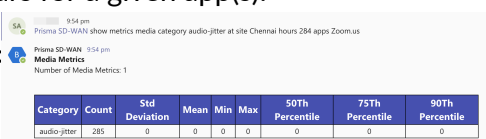
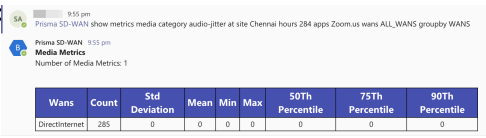
show interfaces at
site <sitename> on
element<elemname>

Displays the following interface attributes of admin status, type, name, ipv4_config, secondary_ip_configs, and site_wan_interface_ids.

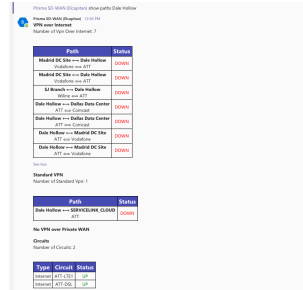
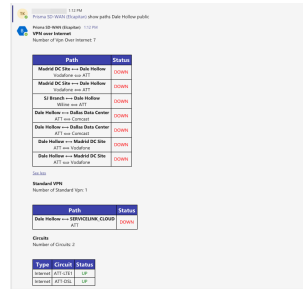
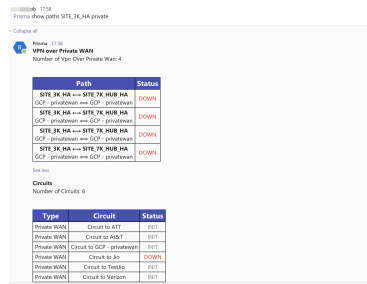
Commands	Command Descriptions																																																
	<div><div><div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div><div><div><div></div><div></div></div></div></div></div><div><div>14:59</div><div>Prisma SD-WAN show interfaces at site on element </div><div>Prisma SD-WAN</div><div>INTERFACES</div><div>Number of Interfaces: 7</div></div><table><thead><tr><th>Name</th><th>Type</th><th>Admin Up</th><th>Ipv4 Config</th><th>Secondary Ip Configs</th><th>Site Wan Interfaces</th></tr></thead><tbody><tr><td>1</td><td>Port</td><td>True</td><td>{'type': 'static', 'static_config': {'address': '172.16.90.1/24'}, 'dhcp_config': None, 'dns_v4_config': {'name_servers': ['8.8.8.8']}, 'routes': None}}</td><td>None</td><td>None</td></tr><tr><td>2</td><td>Port</td><td>True</td><td>{'type': 'dhcp', 'static_config': None, 'dhcp_config': None, 'dns_v4_config': None, 'routes': None}}</td><td>None</td><td>None</td></tr><tr><td>3</td><td>Port</td><td>False</td><td>None</td><td>None</td><td>None</td></tr><tr><td>4</td><td>Port</td><td>False</td><td>None</td><td>None</td><td>None</td></tr><tr><td>5</td><td>Port</td><td>False</td><td>None</td><td>None</td><td>None</td></tr><tr><td>6</td><td>Port</td><td>False</td><td>None</td><td>None</td><td>None</td></tr><tr><td>controller 1</td><td>Port</td><td>True</td><td>{'type': 'dhcp', 'static_config': None, 'dhcp_config': None, 'dns_v4_config': None, 'routes': None}}</td><td>None</td><td>None</td></tr></tbody></table></div>	Name	Type	Admin Up	Ipv4 Config	Secondary Ip Configs	Site Wan Interfaces	1	Port	True	{'type': 'static', 'static_config': {'address': '172.16.90.1/24'}, 'dhcp_config': None, 'dns_v4_config': {'name_servers': ['8.8.8.8']}, 'routes': None}}	None	None	2	Port	True	{'type': 'dhcp', 'static_config': None, 'dhcp_config': None, 'dns_v4_config': None, 'routes': None}}	None	None	3	Port	False	None	None	None	4	Port	False	None	None	None	5	Port	False	None	None	None	6	Port	False	None	None	None	controller 1	Port	True	{'type': 'dhcp', 'static_config': None, 'dhcp_config': None, 'dns_v4_config': None, 'routes': None}}	None	None
Name	Type	Admin Up	Ipv4 Config	Secondary Ip Configs	Site Wan Interfaces																																												
1	Port	True	{'type': 'static', 'static_config': {'address': '172.16.90.1/24'}, 'dhcp_config': None, 'dns_v4_config': {'name_servers': ['8.8.8.8']}, 'routes': None}}	None	None																																												
2	Port	True	{'type': 'dhcp', 'static_config': None, 'dhcp_config': None, 'dns_v4_config': None, 'routes': None}}	None	None																																												
3	Port	False	None	None	None																																												
4	Port	False	None	None	None																																												
5	Port	False	None	None	None																																												
6	Port	False	None	None	None																																												
controller 1	Port	True	{'type': 'dhcp', 'static_config': None, 'dhcp_config': None, 'dns_v4_config': None, 'routes': None}}	None	None																																												
show interfaces <interfacename>	<div>Displays interface configurations of all the interfaces with the interface name with the following attributes:</div> <ul style="list-style-type: none">• sitename• element name• admin status• type• name• ipv4_config• secondary_ip_configs• site_wan_interface_ids• connected <div><div>14:54</div><div>Prisma SD-WAN show interfaces 1*</div><div>Prisma SD-WAN</div><div>INTERFACES</div><div>Number of Interfaces: 3</div></div> <table><thead><tr><th>Interface Name</th><th>Site Name</th><th>Element Name</th><th>Type</th><th>Admin Up</th><th>Ipv4 Config</th><th>Site Wan Interfaces</th><th>Connected</th></tr></thead><tbody><tr><td>1</td><td>Bangalore</td><td>Bangalore</td><td>Port</td><td>True</td><td>{'type': 'static', 'static_config': {'address': '172.16.90.1/24'}, 'dns_v4_config': {'name_servers': ['8.8.8.8']}}</td><td>None</td><td>True</td></tr><tr><td>1</td><td>None</td><td>None</td><td>Port</td><td>False</td><td>None</td><td>None</td><td>True</td></tr><tr><td>1</td><td>Hyderabad</td><td>Hyderabad</td><td>Port</td><td>False</td><td>None</td><td>None</td><td>True</td></tr></tbody></table>	Interface Name	Site Name	Element Name	Type	Admin Up	Ipv4 Config	Site Wan Interfaces	Connected	1	Bangalore	Bangalore	Port	True	{'type': 'static', 'static_config': {'address': '172.16.90.1/24'}, 'dns_v4_config': {'name_servers': ['8.8.8.8']}}	None	True	1	None	None	Port	False	None	None	True	1	Hyderabad	Hyderabad	Port	False	None	None	True																
Interface Name	Site Name	Element Name	Type	Admin Up	Ipv4 Config	Site Wan Interfaces	Connected																																										
1	Bangalore	Bangalore	Port	True	{'type': 'static', 'static_config': {'address': '172.16.90.1/24'}, 'dns_v4_config': {'name_servers': ['8.8.8.8']}}	None	True																																										
1	None	None	Port	False	None	None	True																																										
1	Hyderabad	Hyderabad	Port	False	None	None	True																																										
show metrics—All metrics-related commands must have the options metric type, category, site, and hours. If the site name or the app name has a space, ensure the names are typed in double-quotes.																																																	
show metrics <type> category <category> at site<sitename> hours <numhours> groupby<groupby>	<div>Displays specific metrics for the given site for the specified number of hours. The output displays a statistical distribution of the metrics queried for:</div> <ul style="list-style-type: none">• Count (Number of data points)• Mean• Standard Deviation• Minimum Value• Maximum Value• Percentile Values: 50, 75, 90																																																

Commands	Command Descriptions
Show metrics network <category> <bw> at site<sitename>hours <numhours>groupby<APPS>	Displays the metrics, where the metric type is a network and the category is bandwidth for a given site for the specified number of hours for a given app(s). 
Show metrics network <category> <bw> at site<sitename>hours <numhours>	Displays the metrics, where the metric type is a network and the category is bandwidth for a given site for the specified number of hours. 
Show metrics network <category> <bw> at site<sitename>hours<numhours>groupby<APPS>groupby<WANs>	Displays the metrics, where the metric type is a network and the category is bandwidth for a given site for the specified number of hours, group by given APPS and by the Selected WANs. 
Show metrics network <category> <bw> at site<sitename>hours <numhours>groupby<Top10>groupby<APPS>	Displays the metrics for the top 10 apps where the metric type is a network and the category is bandwidth for a given site for the specified number of hours. 
Show metrics network <category>tcp<tcp- xsact>at site <sitename>hours <numhours>	Displays the TCP metrics where the metric type is a network and the category is tcp-xsact for a given site for the specified number of hours. 

Commands	Command Descriptions
Show metrics network <category> tcp<tcp-xsact>at site <sitename>hours<numhours>groupby<APPS>	Displays the TCP metrics, where the metric type is a network and the category is tcp-xsact for a given site for the specified number of hours for a given app(s). 
Show metrics network <category> <tcp-xsact> atsite <sitename>hours<numhours>groupby<WANs>	Displays the TCP metrics, where the metric type is a network and the category is tcp-xsact for a given site for the specified number of hours and selected WANs. 
Show metrics network <category> <tcp-xsact> atsite <sitename>hours<numhours>groupby<APPS>	Displays the TCP metrics, where the metric type is a network and the category is tcp-xsact for a given site for the specified number of hours, for a given app(s), and the selected WANs. 
Show metrics app <category> <health> at site<sitename>hours <numhours>groupby<APPS>	Displays the app(s) health metrics, for a given site for the specified number of hours for a given app(s). 
Show metrics app <category> <health> at site<sitename>hours<numhours>groupby<APPS>groupby<WANs>	Displays the app(s) health metrics for a given site for the specified number of hours, for a given app(s) and the selected WANs or all WANs. 
Show metrics app <category> <app-response> atsite <sitename>hours<numhours>groupby<APPS>	Displays the app response metrics, for a given site for the specified number of hours for a given app(s).

Commands	Command Descriptions
	
Show metrics app <category> <app-response> atsite <sitename>hours<numhours>groupby<APP>	Displays the app response metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs.
	
Show metrics media <category> <audio-bw> atsite <sitename>hours<numhours>groupby<APP>	Displays the audio bandwidth metrics, for a given site for the specified number of hours for a given app(s).
	
Show metrics media <category> <audio-bw> atsite <sitename>hours<numhours>groupby<APP>	Displays the audio bandwidth metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs.
	
Show metrics media <category> <audio-jitter> atsite <sitename>hours<numhours>groupby<APP>	Displays the audio jitter metrics, for a given site for the specified number of hours for a given app(s).
	
Show metrics media <category> <audio-jitter> atsite <sitename>hours<numhours>groupby<APP>	Displays the audio jitter metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs.
	
Show metrics media <category>	Displays the video jitter metrics, for a given site for the specified number of hours for a given app(s).

Commands	Command Descriptions
<code><video-jitter> atsite</code> <code><sitename>hours<numhours>groupby<APP></code>	
Show metrics media <code><category> <audio-loss></code> <code>atsite<sitename>hours<numhours><group></code>	Displays the audio-loss metrics, for a given site for the specified number of hours for a given app(s). 
Show metrics media <code><category></code> <code>audio-loss> atsite</code> <code><sitename>hours<numhours>groupby<APPS>groupby<WANS></code>	Displays the audio loss metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs.
Show metrics media <code><category> <video-loss></code> <code>atsite<sitename>hours<numhours><group></code>	Displays the video-loss metrics, for a given site for the specified number of hours for a given app(s). 
Show metrics media <code><category></code> <code>video-loss> atsite</code> <code><sitename>hours<numhours>groupby<APP></code>	Displays the video loss metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs. 
Show metrics media <code><category> <audio-mos></code> <code>atsite<sitename>hours<numhours><group></code>	Displays the audio-mos metrics, for a given site for the specified number of hours for a given app(s). 
Show metrics media <code><category></code> <code>audio-mos> atsite</code> <code><sitename>hours<numhours>groupby<APP></code>	Displays the audio-mos metrics for a given site for the specified number of hours, for a given app(s), and the selected WANs or all WANs. 
show paths	

Commands	Command Descriptions
show paths <sitename>	<p>Displays all the paths, overlay + underlays, at a given site.</p> <ul style="list-style-type: none"> Internet Private WAN VPN over Internet VPN over Private WAN Standard VPN 
show paths <sitename> public	<p>Displays only the public paths, overlay+underlays, at a given site.</p> <ul style="list-style-type: none"> Internet VPN over Internet Standard VPN 
show paths <sitename> private	<p>Displays only the private paths, overlay +underlays, at a given site.</p> <ul style="list-style-type: none"> Private WAN VPN over Private WAN 

Commands

Command Descriptions

show sites

show sites

Lists all the sites, site type (hub v/s spoke), admin state, tags, and domain.

PG 13:53
Prisma show sites

Prisma SD-WAN 13:53
SITES
Number of Sites: 26

Name	Admin State	Tags	Type	Domain
AMS86 - Santiago	active	AUTO-scaler, HA	SPOKE	Preset Domain
AWS-DC-SITE	active	CL_IGNORE	HUB	None
DC-Site-Chennai	active	CL_IGNORE	HUB	None
GCP-NCC-BR-14	active	None	SPOKE	Preset Domain
Mumbai IND	active	CL_IGNORE	HUB	None
SITE_1K	active	None	SPOKE	Preset Domain
TEST	disabled	None	SPOKE	Preset Domain
Test	disabled	None	SPOKE	Preset Domain
Test space for site	disabled	None	SPOKE	Preset Domain
Test-buz-app	disabled	None	SPOKE	Preset Domain

show sites <sitename>

Lists all the site properties such as an address, location, tags, and attached policies.

VP 14:37
Prisma SD-WAN show sites AKASH1_CONFIG_UTIL_CID_BRT

Prisma SD-WAN 14:37
Site: AKASH1_CONFIG_UTIL_CID_BRT

Attribute	Value
ID	1635247401747070
Name	AKASH1_CONFIG_UTIL_CID_BRT
Description	None
Tags	None
Admin State	active
Address	None
Location	{ "longitude": 0.0, "latitude": 0.0, "description": None }
Policy Set	None
Element Cluster Role	SPOKE
Security Policyset	None
Service Binding	Preset Domain
Network Policysetstack	Default Path Simple Stack (Simple)
Priority Policysetstack	Default QoS Simple Stack (Simple)
Nat Policysetstack	Default-NATPolicySetStack
Security Policysetstack	None

show sites <sitename>
address

Lists the addresses of all the sites.

show sites <sitename>
policy

Lists the path, QoS, Security, and NAT policies attached to the site.

VP 13:55
Prisma SD-WAN show sites AKASH1_BR-SITE1-CONFIG-CICD policy

Prisma SD-WAN 13:55
Site: AKASH1_BR-SITE1-CONFIG-CICD

Attribute	Value
Name	AKASH1_BR-SITE1-CONFIG-CICD
Type	SPOKE
Priority Policyset Stack	PriorityPolicySetStack
Network Policyset Stack	NetworkPolicySetStack
NAT Policyset Stack	Default-NATPolicySetStack
Policyset	None
Security Policyset	None

[Site Info](#)

show sites <sitename>
tags

Lists the tags attached to the site.

PG 13:55
Prisma SD-WAN show sites TAGS

Prisma SD-WAN 13:55
SITES
Number of Sites: 26

Name	Type	Tags
AMS86 - Santiago	SPOKE	AUTO-scaler, HA
AWS-DC-SITE	HUB	CL_IGNORE
DC-Site-Chennai	HUB	CL_IGNORE
GCP-NCC-BR-14	SPOKE	None
Mumbai IND	HUB	CL_IGNORE
SITE_1K	SPOKE	None
TEST	SPOKE	None
Test	SPOKE	None
Test space for site	SPOKE	None
Test-buz-app	SPOKE	None
Test_create_site	SPOKE	None
teste	SPOKE	None
运营处理	SPOKE	None

GCP-NCC CloudBlade Integration

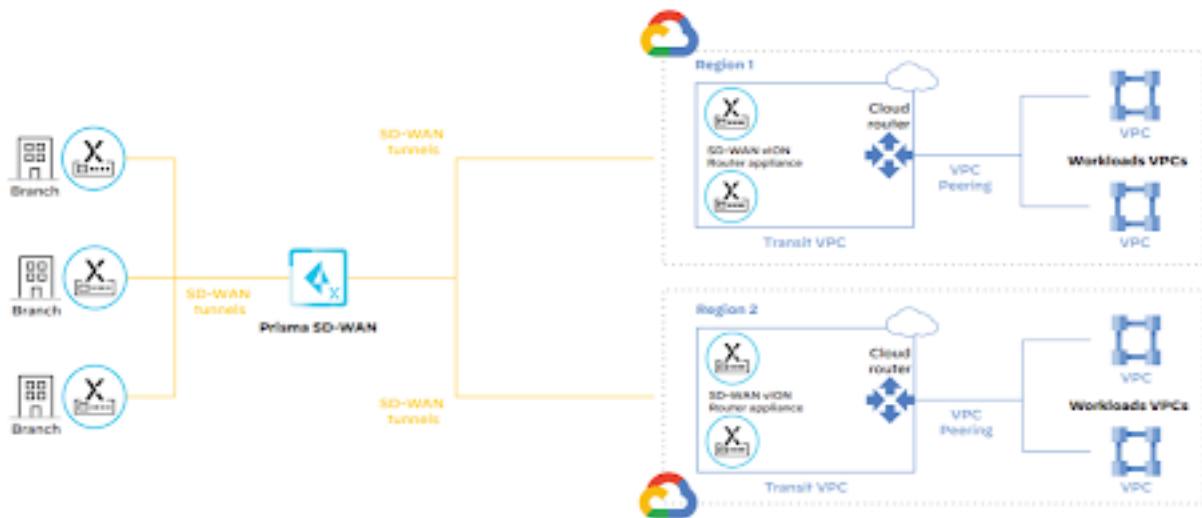
Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license GCP-NCC CloudBlade

Prisma SD-WAN GCP-NCC CloudBlade allows seamless integration between Prisma SD-WAN branches and Google Cloud Platform **Network Connectivity Center** (NCC) to streamline and automate site-to-cloud connectivity at scale.

Network Connectivity Center in Google Cloud is a hub and spoke model for network connectivity management. The hub resource delivers a reliable connectivity on demand and reduces the operational complexity through a simple, centralized connectivity management.

NCC can connect VPNs, partner dedicated interconnects, as well as third party routers and SD-WAN. Wherever your applications or users are in the network, you can optimize the connectivity, reduce the operational load, and lower costs.

Cloud Router is a fully distributed and managed Google Cloud service that programs custom dynamic routes and scales with network traffic. It dynamically exchanges routes between Virtual Private Cloud (VPC) and on-premise networks using Border Gateway Protocol (BGP).



Prerequisites

Prisma SD-WAN

- An active Prisma SD-WAN subscription with sufficient licenses to install at least 2 x v7108 ION devices per region.
- Sufficient [quota](#) for the CloudBlade to create three VPCs in the project.

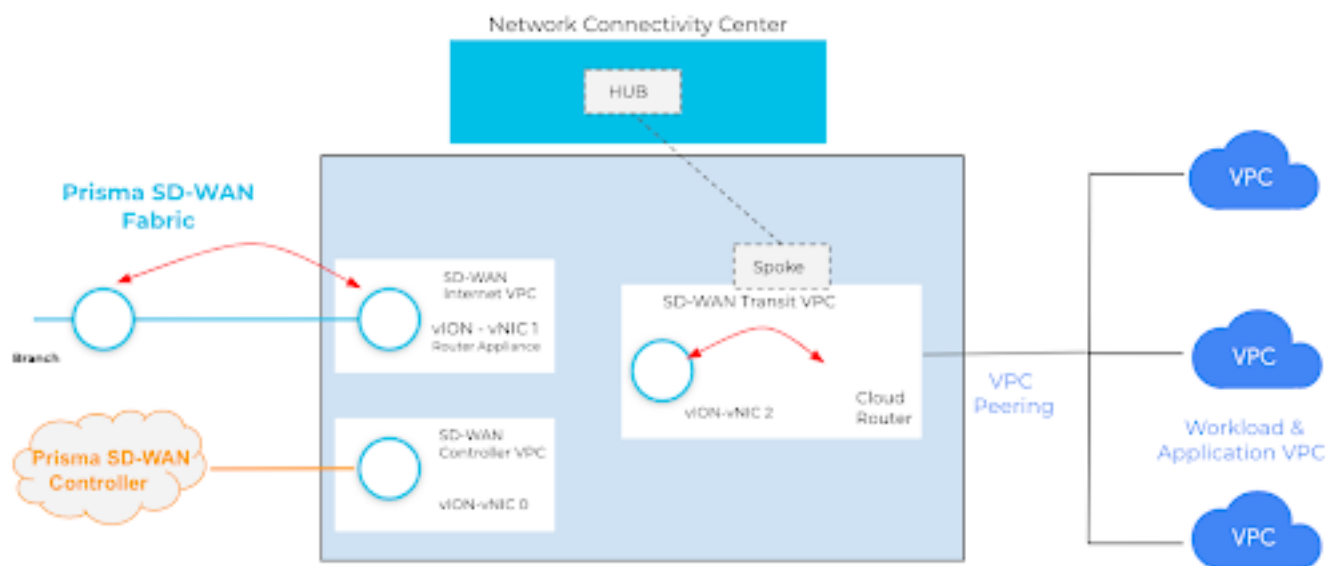
GCP

- A GCP service account with permissions to call Rest APIs like Deployment Manager API, Compute Engine API, Cloud Router API, and Network Connectivity API. Access to these APIs must be enabled in the project before deploying the CloudBlade.
- The Service Account must have permissions to create, update, and delete resources like (VPC, Firewall, Subnet, IP addresses, Routes, VM (instance), Cloud Router, Router Interfaces, BGP Peers, NCC Spoke, and NCC Hub).
- An active GCP marketplace subscription for the Prisma SD-WAN ION Virtual Appliance.
- From version 1.0.0 onwards, GCP regions must support instance machine type as First Generation N1.

Plan the GCP-NCC CloudBlade Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license GCP-NCC CloudBlade

The GCP-NCC CloudBlade provides the automatic creation, management, and maintenance of an HA pair of Prisma SD-WAN Data Center virtual ION devices across multiple locations/regions in GCP. It establishes BGP peering to a GCP Cloud Router from the Prisma SD-WAN Data Center vIONs and the GPC Transit VPC to advertise branch prefixes and provide connectivity to compute resources within the GCP regions.



The CloudBlade automates the following configuration steps required to establish end-to-end connectivity from the Prisma SD-WAN sites to the VPCs in GCP.

1. Creates an NCC Hub.

An NCC Hub is a global resource; however, once a virtual ION is attached to an NCC hub as a spoke, the NCC will be part of that particular virtual ION device's VPC. All the virtual ION devices are connected to the same NCC hub as spokes.

2. Creates three VPCs in GCP (Controller, Internet, and Transit) using **Deployment Manager**.

1. Controller and Internet VPC Subnets is configured in 255.255.x.0/24 format.
2. Transit VPC (Greenfield) Subnet is configured in 10.255.x.0/24 format.

3. Deploys two Prisma SD-WAN virtual ION 7K data center devices and the subnet CIDR range for the specific region in the VPC created.

4. Creates cloud routers with interfaces for specific regions.

A cloud router is part of a region and is attached to the hub (Virtual ION) through BGP peering. In multi-region deployments, multiple virtual ION and cloud routers are deployed across the same VPC in multiple regions (Controller VPC, Internet VPC, and Transit VPC).

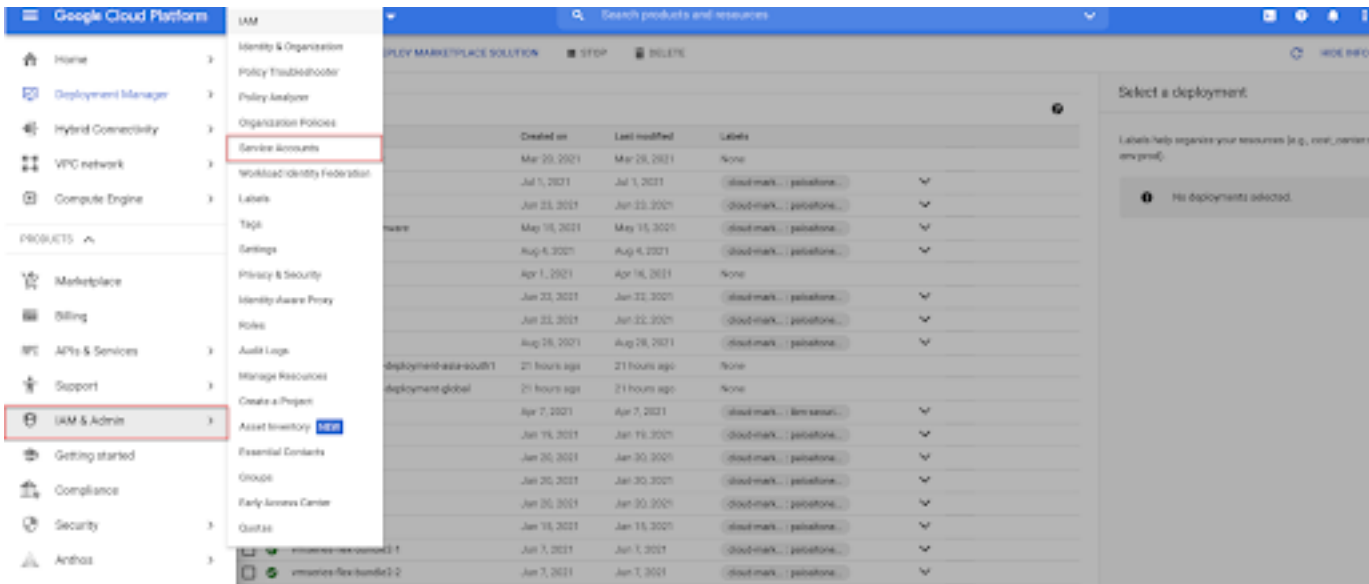
5. Configures and establishes BGP peering session between the cloud router and the virtual ION 7K.
6. Attaches the virtual ION 7k as a spoke to the NCC hub along with the cloud router.
7. Configures routing on each VPC.
8. Creates a data center site in the Prisma SD-WAN controller and configures the devices (Dual Virtual ION 7Ks) with the site.
9. Updates the **Interfaces** configuration for port 1 and port 2 for each device on the cloud controller.
10. Creates BGP core peer routing for each device.

Configure GCP-NCC CloudBlade

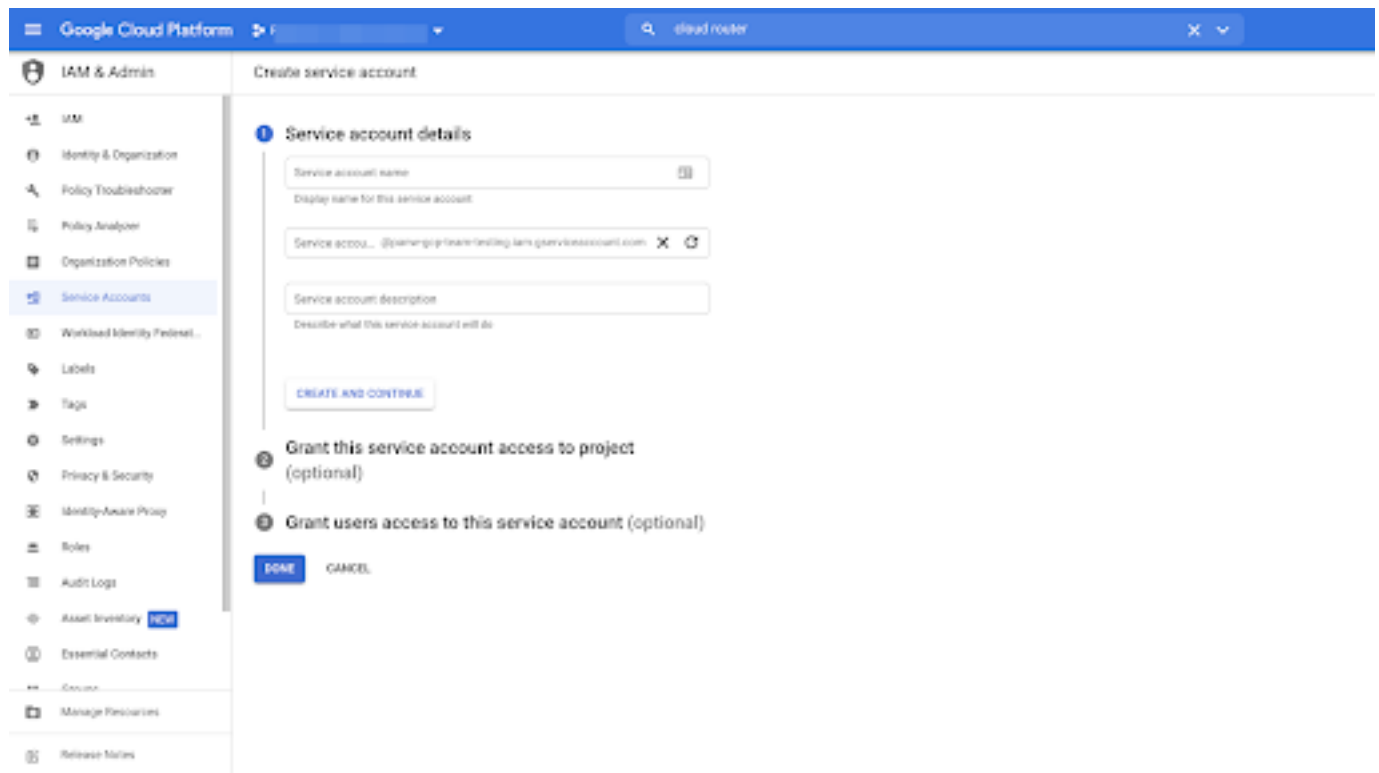
Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ GCP-NCC CloudBlade

To configure the GCP-NCC CloudBlade, retrieve the following information from your GCP-NCC account:

STEP 1 | Go to the GCP-NCC portal menu, select **IAM & Admin > Service Accounts**.



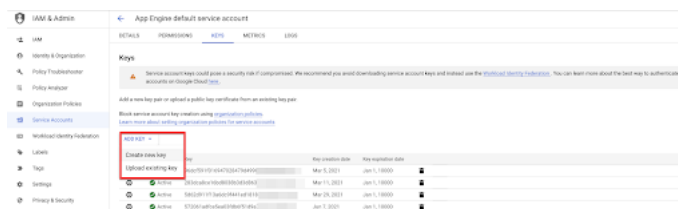
STEP 2 | Select a **Service Account** from the list, or to add a new service account, and click **Create Service Account**.



STEP 3 | Enter the Service Account name/description and click **Create and Continue**.

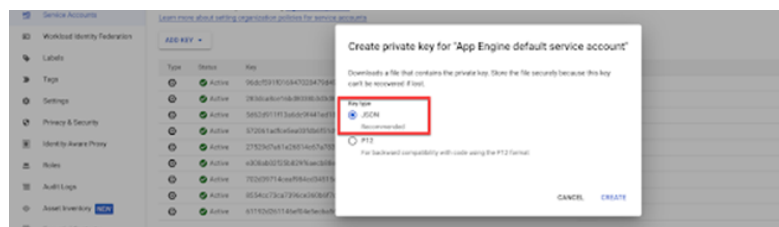
STEP 4 | Select the **Service Account** and click **Keys > Add Key**.

You can either create a new key OR update an existing key.



STEP 5 | Select **JSON** as the key type and click **Create**.

The file downloads on your system and contains information required to configure the GCP-NCC CloudBlade.

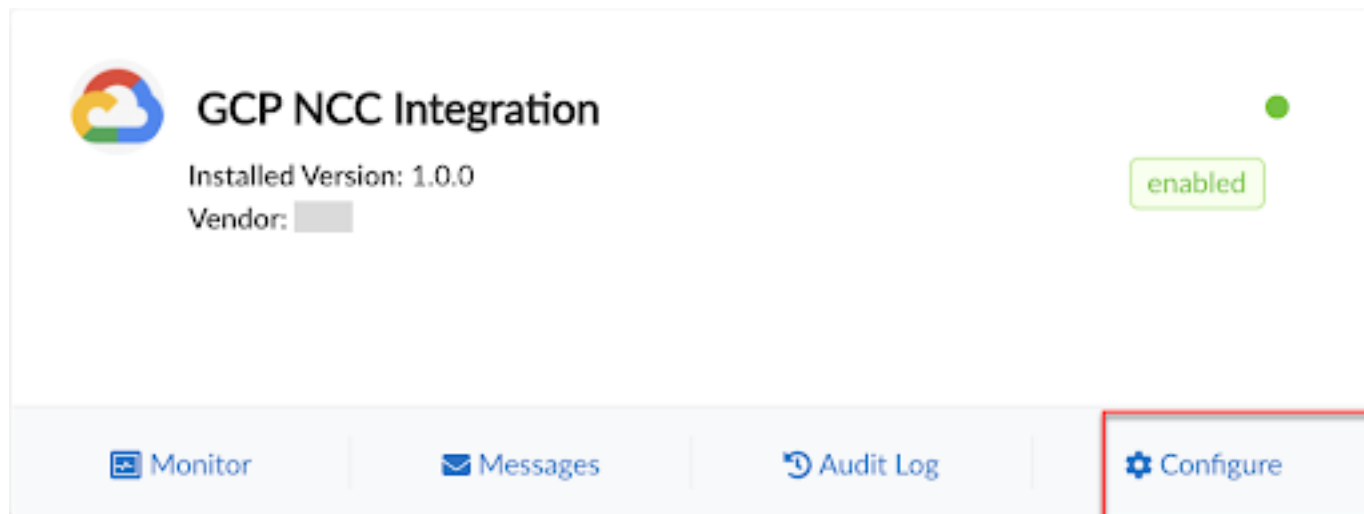


Configure GCP-NCC CloudBlade in Prisma SD-WAN

To configure the GCP-NCC Integration in Prisma SD-WAN:

STEP 1 | From the Strata Cloud Manager, navigate to **Manage > Prisma SD-WAN > CloudBlades**.

STEP 2 | In CloudBlades, locate the **GCP-NCC Integration** tile, and click **Configure**.



STEP 3 | In the **GCP-NCC Integration** page, enter the following information in the fields shown below, change where appropriate. The values in the service account JSON file created and downloaded need to be populated in these fields.

- **VERSION:** Select the version of the GCP- NCC Integration CloudBlade.
- **ADMIN STATE:** For Admin State, select/retain Enabled.
- **PROJECT ID:** Enter the project ID, which is a unique string used to differentiate your project from all others in Google Cloud. To locate your project ID, go to the API Console. From the projects list, select **Manage all projects**. The names and IDs for all the projects you are the member is displayed.
- **CLIENT EMAIL:** Enter the email address for the GCP service account. A service account is an identity that Google Cloud can use to run API requests.
- **PRIVATE KEY ID:** Enter the private key ID for the GCP service account.
- **PRIVATE KEY:** Enter the private key for the GCP service account. Ensure to include everything within quotes from the "private_key" entry in the JSON file.
- **GCP REGIONS:** Enter the GCP regions/locations where you want to access the GCP application resources as comma-separated values. Example: asia-south1,us-central1.
- **TRANSIT VPC:** For Brownfield (existing deployments), enter the name of the existing Transit VPC. Transit VPC is used to connect the Prisma SD-WAN ION devices to the GCP

cloud router and the GCP Application VPC. If one does not exist with that name, a new Transit VPC is created in the specified region.

- **Transit CIDR:** For Brownfield (existing deployments), enter region-specific CIDR for Transit VPC subnets as comma-separated values. Example: us-central1:10.255.255.0/24,asia-south1:10.255.254.0/24.

Name	Vendor	Installed Version
GCP NCC Integration		Not installed

VERSION

1.0.0

▼

STATUS

alpha

PERMISSIONS

View

ADMIN STATE

Enabled

▼

View Messages

PROJECT ID

CLIENT EMAIL

PRIVATE KEY ID

PRIVATE KEY

unmask

GCP REGIONS

TRANSIT VPC (optional)

TRANSIT CIDR (optional)

Uninstall

Cancel

Install

STEP 4 | Click **Save** and **Install** after the settings are configured.

Configure Cloud Router Advertisement

To configure the cloud router advertisement in GCP:

STEP 1 | Select **GCP menu > Cloud Routers > Router Details**.

STEP 2 | Click **Edit**.

STEP 3 | Select **Create custom routes > Advertise all subnets visible to the Cloud Router**.

STEP 4 | Provide the IP address range under **Custom Ranges** of the advertised routes.

Google Cloud Platform PANW-GCP-TEAM-TESTING Cloud router

Hybrid Connectivity VPN Interconnect Cloud Routers Network Connectivity Center

Router details EDIT DELETE

Advertised routes

Routes

☐ Advertise all subnets visible to the Cloud Router (Default)

☒ Create custom routes

Advertise all subnets

☒ Advertise all subnets visible to the Cloud Router

Filter Enter property name or value

Subnet ↑	IP ranges
prisma-sdwan-1114-transit-vpc-subnet-asia-south1	10.255.254.0/24
prisma-sdwan-1114-transit-vpc-subnet-us-central1	10.255.255.0/24

Custom ranges

Add IP ranges to advertise

Edit item

Source
Custom IP range

IP address range *
192.168.11.0/24

Description

DONE

Create VPC Network Peering

To create VPC peering between the workload VPC and the Transit VPC.

STEP 1 | Select **GCP menu > VPC Network > VPC Network Peering > Create peering connection**.

STEP 2 | Enter the **Name** and select **Your VPC network**.

STEP 3 | Select your project, choose to import and export custom routes, and choose to import and export subnet routes with public IP over the VPC peering connection.

This establishes the peering connection to the VPC network.

VPC network

VPC networks

External IP addresses

Bring your own IP

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

Create peering connection

Your VPC network will be fully connected to the peered VPC network (full mesh topology). Routes to subnets in the peered VPC network will be automatically created.

Name *

Name is required

Your VPC network *

Peered VPC network

☒ In project panw-gcp-team-testing

☐ In another project

VPC network name *

Exchange custom routes ?

You can choose to import or export static and dynamic routes over the VPC peering connection

☒ Import custom routes ?

☒ Export custom routes ?

Exchange subnet routes with public IP ?

You can choose to import or export subnet routes with public IP over the VPC peering connection

☐ Import subnet routes with public IP ?

☒ Export subnet routes with public IP ?

CREATE

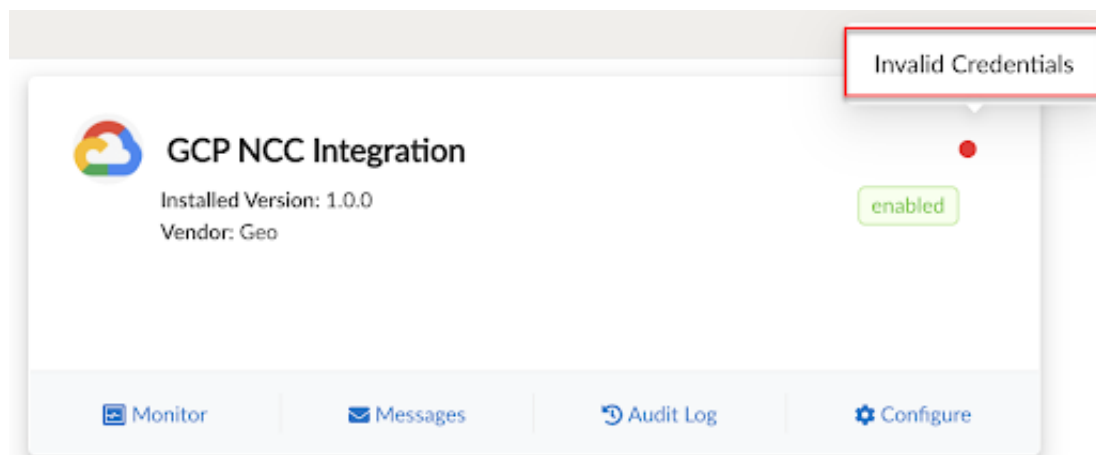
CANCEL

Validate the GCP-NCC Integration CloudBlade

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license GCP-NCC CloudBlade

Validate the GCP-NCC Integration CloudBlade deployment and check the GCP and Prisma SD-WAN controller-created resources.

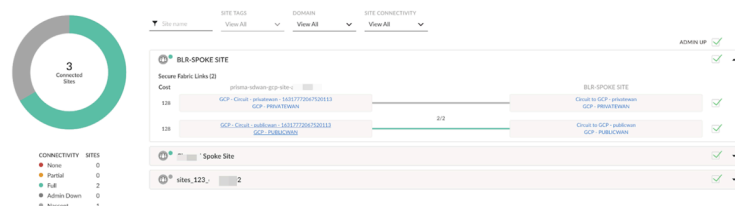
STEP 1 | Check the status indicator on the CloudBlade window. Once enabled and deployed correctly, the status indicator should turn green. If the access credentials are invalid, the status indicator will display an invalid credentials error message.



STEP 2 | Check if the Prisma SD-WAN data center site has been created in the Prisma SD-WAN controller and if the Virtual ION HA pair has been assigned to this site. To verify, navigate to **Workflows > Prisma SD-WAN Setup > Branch Sites**.

NAME	LOCATION	CIRCUITS	IP PREFIXES	DEVICES	MODE
prisma-sdwan-gcp-site-asia-south1 Created by Prisma SD-WAN GCP CB VMS: PRISMA-GCP-site-south1	Mumbai	GCP - Circuit - publicwan - 16317772067520113, GCP - Circuit - privatenet - 16317772067520113	None	<ul style="list-style-type: none"> prisma-sdwan-1114-asia-south1-b-16092021072348 (ion 7108v) prisma-sdwan-1114-asia-south1-c-16092021072347 (ion 7108v) 	Control

STEP 3 | In Prisma SD-WAN, go to **Site Details** and check if the **Secure Fabric Links** are created between the newly created GCP Data Center ION devices and the branch site devices.



STEP 5 | Verify if the IP subnets are in the range of 255.255.x.0/24 for Controller and Internet VPC, and the range for Transit VPC follows the RFC 1918 10.255.x.0/24.

STEP 6 | In GCP, check if the **Cloud Routers** created region-wise are integrated with the devices deployed in the respective regions and attached to the NCC Hub.

STEP 7 | Check if the BGP core peering between each Virtual ION and the cloud router is up.

©2025 Palo Alto Networks, Inc.

STEP 8 | Check the advertised Branch prefixes to the Cloud Router.

×

Advertised Prefixes for Peer "10.255.254.5"
Checked on 09/22/21 2:48PM - [refresh](#)

FILTER (by prefix)
▼

ADVERTISED PREFIXES (5)

10.255.254.0/24	10.255.255.0/24	192.168.1.0/24
192.168.2.0/24	192.168.11.0/24	

Exit

STEP 9 | Check the received routes from the Cloud Router.

×

Received Prefixes for Peer "10.255.254.5"
Checked on 09/22/21 2:48PM - [refresh](#)

FILTER PREFIXES
▼

FILTER COLUMN
-- All -- ▼

REACHABLE PREFIXES (0)
None

FILTERED PREFIXES (3)

NETWORK	AS PATH	NEXT HOP
10.255.254.0/24	65011	10.255.254.1
10.255.255.0/24	65011	10.255.254.1
192.168.11.0/24	65011	10.255.254.1

Exit

Manage and Monitor the GCP-NCC Integration CloudBlade

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ GCP-NCC CloudBlade

After the integration is set up, you can choose to change the Admin State of the CloudBlade to the following scenarios from the CloudBlade configuration page.

Set the CloudBlade to Enabled

This is the default mode of operation for the CloudBlade. The CloudBlade will run, find any new resources, and configure the integration on GCP-NCC related resources.

Set the CloudBlade to Paused

Pausing the CloudBlade stops all future integration runs but leaves any created GCP-NCC resources intact. This stops any future resources from getting created. When paused the CloudBlade will not deploy or delete the resources nor will it stop the user from deleting any resources. Changes will be tracked by the CloudBlade and reverted once enabled.

Set the CloudBlade to Disabled

Disabling the CloudBlade tells the system to remove and delete all GCP-NCC resources created by the CloudBlade.

Set the CloudBlade to Uninstalled

Uninstalling the CloudBlade removes the resources for the CloudBlade, and immediately stops any changes by the CloudBlade. To completely remove all items, set the CloudBlade to disabled for 2-3 Integration Run periods before uninstalling. The GCP-NCC CloudBlade must always be disabled before uninstalling, else, if you wish to reinstall in the same region, it may not create the resources. Also, check the **Status Monitor** tab in the Prisma SD-WAN web interface, if all resources are empty/deleted before uninstalling.

Monitor the GCP-NCC Integration CloudBlade

On the GCP-NCC CloudBlade page, click **Monitor** to view the GCP deployment status and GCP site connectivity.

- The **GCP Deployment Status** tab provides the site name, GCP VPC name, GCP region of deployment, deployment status, time of the last event occurred, and the summary of the deployment.

GCP NCC Integration

Monitoring

GCP Deployment Status

GCP Site Connectivity

Refresh

Columns

SITE NAME	GCP VPC NAMES	GCP REGION	DEPLOYMENT STATUS	TIMESTAMP OF LAST EVENT	SUMMARY
-	prisma-sdwan-2751-controller-vpc, prisma-sdwan-2751-internet-vpc, prisma-sdwan-2751-transit-vpc	GLOBAL	DONE	2021-09-24T03:13:37.679-07:00	-
prisma-sdwan-gcp-site-us-west3	prisma-sdwan-2751-controller-vpc, prisma-sdwan-2751-internet-vpc, prisma-sdwan-2751-transit-vpc	us-west3	DONE	2021-09-24T03:15:55.750-07:00	-

- The **GCP Site Connectivity** tab provides the site name, name of the device, GCP region, GCP VPC names, name of the GCP cloud router, BGP status, uptime, and summary of the deployment.

GCP Deployment Status		GCP Site Connectivity				Refresh Columns	
SITE NAME	DEVICE NAME	GCP REGION	GCP VPC NAME	GCP CLOUD ROUTER NAME	BGP STATUS	UPTIME	SUMMARY
prisma-sdwan-gcp-site-us-west3	prisma-sdwan-2751-us-west3-a-24092021061539	us-west3	prisma-sdwan-2751-transit-vpc	prisma-sdwan-2751-cloud-router-us-west3	prisma-sdwan-2751-ra-1-0-bgp-peer-0-us-west3-a : UP	20 minutes, 17 seconds	-
prisma-sdwan-gcp-site-us-west3	prisma-sdwan-2751-us-west3-b-24092021061539	us-west3	prisma-sdwan-2751-transit-vpc	prisma-sdwan-2751-cloud-router-us-west3	prisma-sdwan-2751-ra-1-0-bgp-peer-0-us-west3-b : UP	19 minutes, 32 seconds	-
prisma-sdwan-gcp-site-us-west3	prisma-sdwan-2751-us-west3-a-24092021061539	us-west3	prisma-sdwan-2751-transit-vpc	prisma-sdwan-2751-cloud-router-us-west3	prisma-sdwan-2751-ra-1-0-bgp-peer-1-us-west3-a : UP	20 minutes, 18 seconds	-
prisma-sdwan-gcp-site-us-west3	prisma-sdwan-2751-us-west3-b-24092021061539	us-west3	prisma-sdwan-2751-transit-vpc	prisma-sdwan-2751-cloud-router-us-west3	prisma-sdwan-2751-ra-1-0-bgp-peer-1-us-west3-b : UP	19 minutes, 28 seconds	-

ServiceNow CloudBlade Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> ❑ Prisma SD-WAN license ❑ ServiceNow CloudBlade

The ServiceNow CloudBlade is used to translate events raised on Prisma SD-WAN into incident tickets on ServiceNow. Once a ticket is created in ServiceNow, the IT Operations team can be alerted to check the network condition and take immediate action for remediation, thus making sure that network Service Level Agreements (SLAs) and thereby application SLAs are met. The following sections provide information about the Prisma SD-WAN events and alerts.

The ServiceNow CloudBlade can also be used to create incident tickets on any of the Circuit Insights. Similar to events, customers can subscribe to the insights they want to be alerted on via ServiceNow. More details on the Circuit Insights can be found in the datasheet [here](#).

Prisma SD-WAN Events

In day-to-day network functioning, many incidents occur that may be a cause for concern. Prisma SD-WAN identifies these incidents that occur in the network and classifies them into two types to determine the type of fault.








An **alarm** is an indication of a fault in the system. Alarms can be raised and cleared, and can be of the following severity:

- **Critical** – Whole or part of a network is down, and requires immediate action.
- **Major** – Network is impacted, and needs immediate attention.
- **Minor** – Network is degraded, and needs attention soon.

An **alert** may or may not be an indication of fault in the network. An alert is raised when system-defined or customer-defined thresholds are reached.

These alerts and alarms can be viewed from the **Events** tab of the Prisma SD-WAN portal.

Events (18)

FAULTS (ALARMS)	ALERTS	
	SITE CONNECTIVITY DOWN All site WAN connectivity is down.	01/12/23 11:05:00am
	SITE MISSING CIRCUIT(S) FOR POLICY Site is missing all circuit definitions specified in the Policy Set assigned to the site. Applications at the site will be affected since there are no circuits to forward the traffic.	01/06/23 2:47:53pm
	DEVICE DISCONNECTED FROM CONTROLLER Device has remained disconnected from the Controller for a prolonged duration.	Acknowledge
	DEVICE ANALYTICS DISCONNECTED Device analytics connection has remained disconnected from the Controller for a prolonged duration.	01/05/23 9:35:01pm
	DEVICE FLOWS DISCONNECTED Device flows connection has remained disconnected from the Controller for a prolonged duration.	01/05/23 9:35:01pm
	DEVICE ANALYTICS DISCONNECTED Device analytics connection has remained disconnected from the Controller for a prolonged duration.	01/05/23 9:35:01pm
	DEVICE DISCONNECTED FROM CONTROLLER Device has remained disconnected from the Controller for a prolonged duration.	01/05/23 9:30:00pm

Alerts and alarms generated in the system are triggered by different types of events, categorized broadly as hardware issues, software issues, device interface issues, device registration issues, peering issues, site level issues, tunnel issues, and application performance issues. These issues, based on the type of event, may originate from the ION device or the controller.

Alert and Alarm Attributes

Each event contains a bunch of attributes that can be used to gain more information on the condition. Depending on the type of event, the attributes that constitute the event differ.

An alarm typically consists of the following attributes:

```
{
  "_created_on_utc": "2021-07-15T05:48:39.121000Z",
  "_etag": 1,
  "_updated_on_utc": "2021-07-15T05:48:39.121000Z",
  "acknowledged": false,
  "acknowledgement_info": null,
  "cleared": false,
  "code": "SITE_CONNECTIVITY_DEGRADED",
  "correlation_id": "6Qeqj3iD",
  "element_id": null,
  "entity_ref": "tenants/1092/sites/16015589439620037",
  "id": "60efcc376534671b7600e09f",
  "info": null,
  "notes": null,
  "policy_info": {
    "policy_applied_time": "2021-07-15T05:48:39.121000Z",
    "policyrule_id": null,
    "policyset_id": "16226851857240070"
  },
  "priority": "p3",
  "severity": "major",
  "site_id": "16015589439620037",
  "suppressed": false,
  "suppressed_info": {
    "event_ids": null,
    "other_reasons": null,
    "summary_event_ids": null,
    "suppressed_time": null
  }
}
```

```
    },  
    "time": "2021-07-15T05:10:00.098000Z",  
    "type": "alarm"  
  }  
}
```

ID

A unique ID used to identify an event.

Code

An event code which describes the event.

Correlation ID*

Correlation ID is a system-generated ID for a raised alarm. An Alarm is associated with two states – **raise** and **clear**. At any given time, there can be multiple alarms with the same event code in either a raised or cleared state. Using the Correlation ID, you may distinguish among alarms with the same event code.

When an alarm is cleared, the Correlation ID will indicate that the specific alarm is cleared. This ID will continue to be associated with an alarm, even if the alarm is cleared or resolved.

Time

The time at which this condition was seen or the event was raised or cleared.

Element ID

ID of the device on which this condition was seen.

Site ID

If the device is associated with a site, **site_id** will also be packaged in the event. If not, this attribute is not present.

Type

This field indicates the event type i.e. alert or alarm.

Severity

Severity for alarms are based on the following categories:

- Critical - Whole or part of a network is down, and requires immediate action.
- Major - Network is impacted, and needs immediate attention.
- Minor - Network is degraded, and needs attention soon.

Entity Reference

Entity reference refers to the specific entity where the alarming condition is seen. This string can be used as an API URI to query the entity using the Prisma SD-WAN SDK. In the example above, the **entity_ref** attribute contains information about the element that is disconnected from the controller.

Info

Info sheds more lights on the entity that is causing the alarming condition. It can contain information regarding interfaces, or IP addresses if there is a collision. The value in this field changes depending on the event code.

Notes

The Notes field is used to add remarks or comments to events. You can edit notes for active alarms only.

Priority

This attribute indicates the priority of the event or alarm.

Suppressed

Suppressed is a boolean attribute that indicates if the event is suppressed by the Prisma SD-WAN Event Correlation & Suppression engine.

Suppressed Info

If the event is suppressed, suppressed_info contains details about the suppression time and correlated event IDs.

Policy Info

If the event was updated using an event policy rule, the policy_info attribute contains details about the event policy set, event policy rule, and rule application time.

Clear*

This attribute is Boolean and indicates if the event condition still exists or is cleared. A value of True indicates that the condition no longer exists. When an alarm is raised, it is raised with Clear set to False.

Acknowledged*

This attribute is Boolean and indicates if an event has been acknowledged by a user. If acknowledged, the **acknowledgement_info** field contains the time and the user who acknowledged the event.

(*) indicates it is not part of the Prisma SD-WAN alert.

A Prisma SD-WAN alert contains most of these attributes except cleared, acknowledged and correlation_id - as alerts are not standing conditions. Here's a sample alert:

```
{
  "info": {
    "name": "internet 1",
    "circuit_labels": "Budapest-INET-VZ"
  },
  "code": "DEVICEHW_INTERFACE_ERRORS",
  "severity": "major",
  "updated_on_utc": "2019-12-23T14:04:34.736000Z",
  "site_id": "15282991838450011",
  "id": "5e00c972d7b0fa2f8cb418ce",
  "entity_ref": "tenants/1083/sites/15282991838450011/elements/15230097588400085/interfaces/15230098062640233",
  "correlation_id": null,
  "time": "2019-12-23T14:04:31.395000Z",
  "element_id": "15230097588400085",
  "created_on_utc": "2019-12-23T14:04:34.736000Z",
  "type": "alert",
  "_etag": 1
}
```



```
}
```

Configure ServiceNow CloudBlade in Prisma SD-WAN

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ ServiceNow CloudBlade

Before you configure the ServiceNow CloudBlade, your ServiceNow instance should be configured and ready for integration. The following sections provide information about how to configure ServiceNow CloudBlade in Prisma SD-WAN and the prerequisites that need to be considered while configuring the CloudBlade:

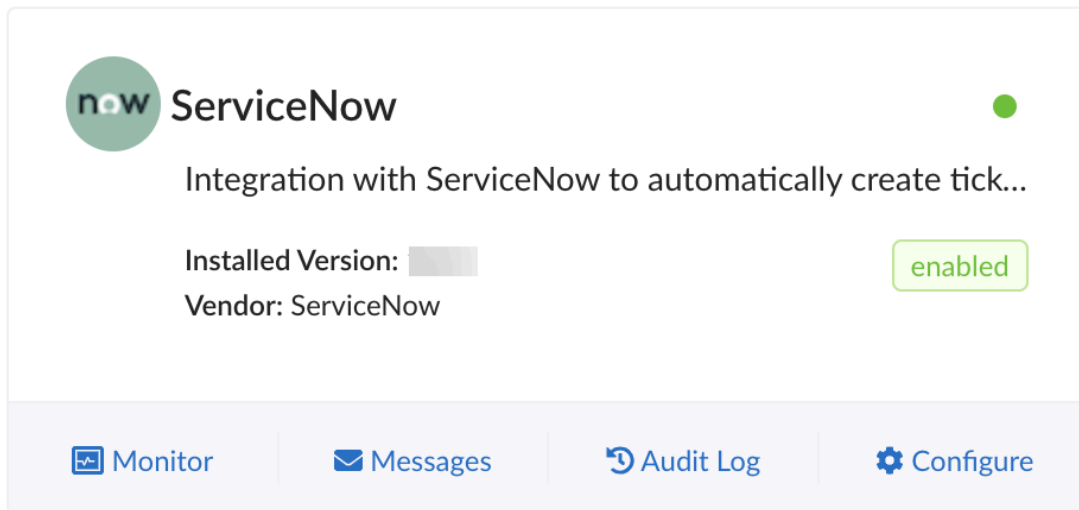
Prerequisites

Consider the following key design points before you configure the ServiceNow CloudBlade in Prisma SD-WAN:

- Build the ServiceNow Table and allocate columns to map mandatory fields such as **event code**, **correlation ID**, **severity**, and **incident state**.
- For more meaningful information in the tickets, you can create columns to store fields from the Prisma SD-WAN events such as **entity_ref**, **info**, **site name**, **element name**, **type**– if opting to create tickets for both alerts and alarms, cleared, acknowledged.
- For Circuit Insights, build the ServiceNow Table and allocate columns to map details about the insight, site, circuit, start time, end time and the insight data.
- ServiceNow CloudBlade communicates with the ServiceNow instance using REST based Table APIs.
- Create a user that will be used by Prisma SD-WAN to perform CRUD operations on the ServiceNow instance table using the table APIs. Make sure this user has the following privileges: **web_service_admin**, **rest_api_explorer**, or **admin**.

Configure the Prisma SD-WAN CloudBlade to prepare the Prisma SD-WAN controller for integration as follows:

STEP 1 | From the Strata Cloud Manager, navigate to **Manage > Prisma SD-WAN > CloudBlades** tab.



STEP 2 | In **CloudBlades**, locate the **ServiceNow** CloudBlade. If this CloudBlade does not appear, contact Palo Alto Networks Support.

For Insights, look for the **ServiceNow - Circuit Insights** CloudBlade.

On the **ServiceNow CloudBlade**, click **Configure** to configure ServiceNow parameters.



Some of the ServiceNow parameters display the column name and not the label, which is typically displayed on the user interface as the column header.

ServiceNow Parameters	Description
ServiceNow URL	This field contains the URL that will be used to connect to the ServiceNow instance via the ServiceNow Table APIs. The URL must include the entire domain name and the table name. The URL follows the following format: <code>https://<domain name>/api/now/table/myTable</code> where myTable is the name of the Table on ServiceNow where tickets will be created.
ServiceNow Username	Incident tickets on ServiceNow will be created using this User. Make sure that the User has the right set of privileges, especially to make changes to the table via APIs. The ServiceNow Developers document lists the following roles to be assigned to a user: Role required: web_service_admin , rest_api_explorer , or admin
ServiceNow Password	Password for the above user. These credentials will be used by the CloudBlade to create/edit tickets on the ServiceNow instance using the ServiceNow Table APIs.

ServiceNow Parameters	Description
Poll Interval	Poll Interval is the interval time in seconds. After you install, the CloudBlade will query the controller for any standing alarms based on the set poll interval.
Retry Attempts	Retry attempts indicate the number of attempts that happen when a ticket could not be created for an event. Retry attempts can be anywhere between 0 and 5. The default value is 3.
Exclude Events Raised and Cleared during Poll Interval	When this option is checked, the events which are created and cleared (resolved) during the poll interval will not be ticketed in ServiceNow.
Event Codes	These are event codes used in monitoring and which need incident tickets to be created in ServiceNow. These event codes need to match the Prisma SD-WAN event codes. You can select one or multiple event codes from the drop-down, for example: NETWORK_VPNLINK_DOWN, NETWORK_DIRECTINTERNET_DOWN, NETWORK_DIRECTPRIVATE_DOWN.
ServiceNow Table Column to Store: EventCode	Column name on the Incident table to store Prisma SD-WAN event code .
ServiceNow Table Column to Store: CorrelationID	Column name on the Incident table to store Prisma SD-WAN event correlation_id .
ServiceNow Table Column to Store: Severity	Column name on the Incident table to store Prisma SD-WAN event severity .
ServiceNow Table Column to Store: EventID	This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN Event ID .
ServiceNow Table Column to Store: Time	This is an optional field. This is a Column name on the Incident table to store the Prisma SD-WAN event time .
ServiceNow Table Column to Store: Site_ID	This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event site_id , which is translated to its site name .
ServiceNow Table Column to Store: Element_ID	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event element_id , which is translated to its device name.
ServiceNow Table Column to Store: Entity_Ref	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event entity_ref , after a name-ID translation.

ServiceNow Parameters	Description
ServiceNow Table Column to Store: Info	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event info , after a name-ID translation.
ServiceNow Table Column to Store: Acknowledged	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event acknowledged attribute.
ServiceNow Table Column to Store: Cleared	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event cleared attribute.
ServiceNow Table Column to Store: Type	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event type .
ServiceNow Table Column to Store: Suppressed	This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event suppressed state.
ServiceNow Table Column to Store: Suppressed_Info	This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event suppressed info .
ServiceNow Table Column to Store: Policy_Info	This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event policy info .
ServiceNow Table Column to Store: Notes	This is an optional field. This is a Column name on the Incident table to store the Prisma SD-WAN event notes .
ServiceNow Table Column to store Incident State	This is a mandatory field. This is a Column name to store the state of an incident . This column will be set to Resolved, once the event condition for which the ticket was created is resolved.
ServiceNow Table: Custom	This is an optional field. This field is for any custom value that you intend to include for every incident ticket. This is typically used by IT organizations to include details about an environment or to include caller information. Enter a value in JSON format for this field i.e. key-value pairs For example: "caller": "Prisma SDWAN Auto Ticketing", "environment": "Production"

For **Insights**, the following columns need to be populated:

Circuit Insight Parameters	Description
ServiceNow URL	This field contains the URL that will be used to connect to the ServiceNow instance via the ServiceNow Table APIs. The URL must include the entire domain name and the table name. The URL follows the following format: <code>https://<domain name>/api/now/table/myTable</code> , where myTable is the name of the Table on ServiceNow where tickets will be created.
ServiceNow Username	Incident tickets on ServiceNow will be created using this User. Make sure that the User has the right set of privileges, especially to make changes to the table via APIs. The ServiceNow Developers document lists the following roles to be assigned to a user: Role required: web_service_admin , rest_api_explorer , or admin .
ServiceNow Password	Password for the above user. These credentials will be used by the CloudBlade to create or edit tickets on the ServiceNow instance using the ServiceNow Table APIs.
Poll Interval	Poll Interval is the interval time in days. After you install, the CloudBlade will query the controller for any circuit insights based on the set poll interval.
Circuit Insights	These are circuit insights generated by the Prisma SD-WAN controller for which incident tickets will be created in ServiceNow. You can select one or multiple insights from the drop-down.
Insight Type	This is a mandatory field. This is the name of the column where the insight type or the insight name will be stored.
Site Name	This is a mandatory field. This is the name of the column to store the name of the site where this insight was generated.
Circuit Name	This is a mandatory field. This is the name of the column to store the name of the circuit where this insight was generated.
Start Time	This is a mandatory field. This is the name of the column to store the start time when this insight was detected.
End Time	This is a mandatory field. This is the name of the column to store the end time when this insight was detected.

Circuit Insight Parameters	Description
Direction	This is a mandatory field. This is the name of the column to store the traffic direction where the insight was observed.
Data	This is a mandatory field. This is the name of the column to store all the relevant data pertaining to the insight viz, metrics data, top talkers, bw utilization, etc.

Configure ServiceNow

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ ServiceNow CloudBlade

The following sections provide information about the Prisma SD-WAN ServiceNow CloudBlade configuration:

ServiceNow CloudBlade Infrastructure

Once the CloudBlade configuration parameters are set up and the CloudBlade is installed, the CloudBlade infrastructure will perform the following tasks:

- Extract configuration parameters received from the CloudBlade
- Query for events based on the event codes provided
- Create or resolve existing tickets
- Wait until poll_interval for next iteration

Query for Events

Once the ServiceNow configuration is extracted, the CloudBlade queries for events using the following API query:

```
events_query_payload = {
  "limit": {
    "count": 100,
    "sort_on": "time",
    "sort_order": "descending"
  },
  "query": {
    "code": event_codes
  },
  "severity": [],
  "start_time": start_time}
```

Here, the **event_codes** is a list of event codes configured on the UI. Once the events are retrieved, they are mapped against an internal database to check if a ticket is already created in ServiceNow. If the event is cleared and a ticket exists, the ticket is set to **Resolved** in ServiceNow. If the ticket does not exist on ServiceNow, the event is ignored. If the clear is set to False, a new ticket is created in ServiceNow.

Convert Prisma SD-WAN Events to ServiceNow Constructs

Before a ticket is created on ServiceNow, the Prisma SD-WAN event JSON is converted to a data structure understood by the ServiceNow instance. This mapping is dependent on the parameters

configured on the CloudBlade. For example, the CloudBlade configuration below is translated in the following manner:

Name

ServiceNow

Vendor

ServiceNow

Installed Version

Integration with ServiceNow to automatically create tickets to handle incidents, problems or change in your CloudGenix managed network

VERSION

STATUS

beta

PERMISSIONS

View

ADMIN STATE

Enabled

Beta Release

SERVICENOW URL

https://dev57534.service-now.com/api/now/table/u_end_to_end_regression_s...

SERVICENOW USERNAME

admin

SERVICENOW PASSWORD

unmask

POLL INTERVAL (SECONDS) (optional)

300

RETRY ATTEMPTS (optional)

3

☐ EXCLUDE EVENTS RAISED AND CLEARED DURING POLL INTERVAL

EVENT CODES

57 selected

SERVICENOW TABLE COLUMN TO STORE: EVENTCODE

u_eventcode

SERVICENOW TABLE COLUMN TO STORE: CORRELATIONID

u_correlationid

SERVICENOW TABLE COLUMN TO STORE: SEVERITY

u_severity

SERVICENOW TABLE COLUMN TO STORE: PRIORITY (optional)

View Audit Log

View Messages

Prisma SD-WAN Event Attributes	ServiceNow Construct
code	u_code
correlation_id	u_correlation_id
severity	u_urgency
id	u_event_id
time	u_time
site_id	u_site

Prisma SD-WAN Event Attributes	ServiceNow Construct
element_id	u_element
entity_ref	u_entity_ref
info	u_info
acknowledged	u_acknowledged
cleared	u_cleared
type	u_type
severity	impact

The following Prisma SD-WAN attributes are translated before converting to the ServiceNow construct:

Entity_Ref

The IDs in the entity_ref are translated to their respective names and a meaningful string is generated that provides the user information about the entity of the alarm

For example, the entity_ref below:

```
tenants/1083/sites/15282991838450011/elements/15230097588400085/
interfaces/15230098062640233"
```

is translated to the string:

```
Site: Portland Office
Element: Portland3K-A
Interface: internet1
```



The ServiceNow CloudBlade does a topology mapping once a week. If new VPN links are created since the last topology mapping, then it may result in certain VPN link IDs not being translated to names.

Info

Similar to entity_ref, the IDs in the info are also translated to their respective names.

Site ID

If a **site_id** exists in the Prisma SD-WAN event, it is translated to its name before populating the ServiceNow construct with the value.

Element ID

If an **element_id** exists in the Prisma SD-WAN event, it is also translated to its name before populating the ServiceNow construct with the value.

Severity

In the above example, the Prisma SD-WAN **severity** is directly mapped to **u_urgency**. However, this field is also mapped to another attribute named **impact**. The following translation takes place before the ServiceNow construct is populated.

Prisma SD-WAN Severity	ServiceNow Impact
critical	1 - High
major	2 - Medium
minor	3 - Low

The impact value may change depending on the tags configured at the site and/or element level. More about this feature is discussed in length under the section **CloudBlade Advanced Configurations**.

Along with the attributes above, the CloudBlade also populates the tenant name in an attribute called **company**.

Create and Resolve Incidents on ServiceNow

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license ServiceNow CloudBlade

Once all the Prisma SD-WAN attributes are translated and populated into the ServiceNow construct, a session is established with the ServiceNow instance configured in the CloudBlade using Basic HTTP Authentication. An incident ticket is created where the Prisma SD-WAN Event attributes are mapped to ServiceNow table columns. Upon successful ticket creation, ServiceNow returns HTTP code 201 – Created and the response package contains the incident ticket number.

This incident ticket number is stored locally in a database and mapped to the Prisma SD-WAN **event_id**.

		acknowledged	cleared	code	correlation_id	element	entity_ref	event_id	incident_state	info	site	urgency	type
	1	false	true	DEVICEHR_INTERFACE_DOWN	8dWwVM	NJ-3K-1	Site: New Jersey Branch 1 Element: NJ-3K...	5e015b686115c07ac3ae804	Resolved	(circuit_label, name-si- asure-15011179...	New Jersey Branch 1	2 - Medium	alarm
	1	false	true	NETWORK_VPNLINK_DOWN	VTZvMBc1	MAD-7K-1	Site: Madrid DC Site	5e0152b486115c07ac3ae804	Resolved	Could not query anynet link 150116987121...	Madrid DC Site	2 - Medium	alarm
	1	false	true	DEVICEHR_INTERFACE_DOWN	WQDWS4	NJ-3K-1	Site: New Jersey Branch 1 Element: NJ-3K...	5e044b486115c099d3ae5a	Resolved	(circuit_label, name-si- asure-15011179...	New Jersey Branch 1	2 - Medium	alarm
	1	false	true	NETWORK_VPNLINK_DOWN	xlHJICG	MAN-3K-1	Site: Manchester Branch 3	5e0406c86115c073d3ae597	Resolved	Could not query anynet link 150112796781...	Manchester Branch 3	2 - Medium	alarm
	1	false	true	DEVICEHR_INTERFACE_DOWN	EwQZTKx	NJ-3K-1	Site: New Jersey Branch 1 Element: NJ-3K...	5e04f91d86115c17d3ae823	Resolved	(circuit_label, name-si- asure-15011179...	New Jersey Branch 1	2 - Medium	alarm
	1	false	true	NETWORK_VPNLINK_DOWN	UGUORpuy	MAN-3K-1	Site: Manchester Branch 3	5e04052286115c073d3ae821	Resolved	Could not query anynet link 150112729193...	Manchester Branch 3	2 - Medium	alarm
	1	false	true	NETWORK_VPNLINK_DOWN	LHSDKNE	MAN-3K-1	Site: Manchester Branch 3	5e04f93986115c0429ae994	Resolved	Could not query anynet link 150112796781...	Manchester Branch 3	2 - Medium	alarm
	1	false	true	NETWORK_VPNLINK_DOWN	uQZfPu8	DAL-7K-1	Site: Dallas Data Center	5e04c986115c17d3ae802	Resolved	Could not query anynet link 150112729193...	Dallas Data Center	2 - Medium	alarm
	1	false	true	NETWORK_VPNLINK_DOWN	GaeBldve	MIL-3K-1	Site: Milan Branch 2	5e04f9e86115c17d3ae80a	Resolved	Could not query anynet link 150112800790...	Milan Branch 2	2 - Medium	alarm
	1	false	true	DEVICEHR_INTERFACE_DOWN	cdNjKvc	NJ-3K-1	Site: New Jersey Branch 1 Element: NJ-3K...	5e04f9e86115c0429ae8e1	Resolved	(circuit_label, name-si- asure-15011179...	New Jersey Branch 1	2 - Medium	alarm

Resolve Incident in ServiceNow

When an event clears on Prisma SD-WAN, the CloudBlade retrieves the incident ticket number from the local database and sets the ticket as **Resolved**. In the above example, the column **u_incident_state** is configured to store the incident state and will be set to the value **Resolved**. IT Operators managing ServiceNow tickets use this column as a filtering mechanism and can choose to ignore tickets marked as **Resolved**.

The incident on ServiceNow is updated any time there is an update on the following Prisma SD-WAN event parameters:

- acknowledged
- suppressed
- notes
- cleared

ServiceNow Advanced Configurations

To **Manage Incident Impact**, all Prisma SD-WAN events have a severity associated with them. Information on event severity can be found in the **Alerts and Alarms** section in the Prisma SD-WAN Administrator's Guide. However, incidents generated from certain sites or devices may have a higher or lower impact than the Prisma SD-WAN event severity. To handle such scenarios, the ServiceNow CloudBlade makes use of tags that can be configured at the site and device level to adjust the impact mapping in ServiceNow.

The tags **snow-high**, **snow-med**, and **snow-low** can be used to adjust impact of events generated from sites and/or elements. If any of these tags are configured at the site or device, all events generated from that particular site or device will have the corresponding impact.

Alarm Severity	Site/Element Tag	Modified Impact
critical, major, minor	snow-high	1 - High
critical, major, minor	snow-med	2 - Medium
critical, major, minor	snow-low	3 - Low

Block Incident Creation

When the **snow-block** tag is configured at the site or device, the Cloudblade will not forward any event generated from those sites or elements to ServiceNow.

Monitor ServiceNow Status in Prisma SD-WAN

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license ServiceNow CloudBlade

To monitor the status of the events, go to **Manage > Prisma SD-WAN > CloudBlades > ServiceNow > Monitor**.

The **Stats** view in the **Monitoring** tab provides information on events created / retrieved, tickets resolved, and lists any errors during each CloudBlade iteration. This view is only updated when at least one event is retrieved. CloudBlade status can only be monitored for up to 7 days.

ITERATION TIME	TOTAL EVENTS RETRIEVED	TOTAL TICKETS CREATED	TOTAL TICKETS RESOLVED	ERRORS
Aug 16, 2021 10:07:21am	1	0	0	-
Aug 16, 2021 10:02:03am	1	0	0	-
Aug 16, 2021 09:56:46am	1	0	0	-
Aug 16, 2021 09:51:28am	1	0	0	-
Aug 16, 2021 09:46:11am	1	0	0	-
Aug 16, 2021 09:40:54am	1	0	0	-
Aug 16, 2021 09:35:35am	1	0	0	-
Aug 16, 2021 09:30:17am	1	0	0	-
Aug 16, 2021 09:25:00am	1	0	0	-
Aug 16, 2021 09:19:43am	1	0	0	-

Field	Description
Iteration Time	CloudBlade iteration time.
Total Events Retrieved	Total number of events retrieved from Prisma SD-WAN Controller.
Total Tickets Created	Total number of tickets created on ServiceNow Incident Management Table.
Total Tickets Resolved	Total number of tickets resolved.
Errors	Error messages displayed whenever the Cloudblade encounters an error during the app run.

The **Details** view provides information on all the tickets that are created. The CloudBlade status can only be monitored for up to 7 days.

CloudBlade / ServiceNow

Monitoring

Stats Details Refresh Columns

TIME	EVENT ID	EVENT CODE	CREATED	SERVICENOW SYS ID	CORRELATION ID	RESOLVED STATUS	TICKET RESOLUTION TIME	EVENT TYPE	RETRY ATTEMPTS	STATUS CODE
1, 2021 02:55:43am	4509e433b4646e00722b9de	DEVICESW_DISCONNECTED_FROM_CONTROLLER	False	-	TTSYnew	NOT RESOLVED	N/A	ALARM	3	200
4, 2021 02:50:40am	4509e2b464646e00722b9f1	DEVICESW_DISCONNECTED_FROM_CONTROLLER	False	-	B709HUB	NOT RESOLVED	N/A	ALARM	3	200
1, 2021 02:50:38am	4509e2b464646e00722b9f8	DEVICESW_DISCONNECTED_FROM_CONTROLLER	False	-	TTSYnew	NOT RESOLVED	N/A	ALARM	3	200
3, 2021 03:27:52pm	4509f29a30b460070ed6c7	DEVICESW_GENERAL_PROCESSRESTART	True	05e464b8713010bdc8517eab63598	N/A	N/A	N/A	ALERT	0	201
3, 2021 03:27:52pm	4509f29a30b460070ed6c6	DEVICESW_INTERFACE_DOWN	True	8b464b8713010bdc8517eab63532	LMC3/DZ	RESOLVED	Aug 3, 2021 03:32:54pm	ALARM	0	201
3, 2021 03:27:51pm	4509f29a30b460070ed6c5	SITE_CONNECTIVITY_DEGRADED	True	8b464b8713010bdc8517eab63536	enK0h4E	RESOLVED	Aug 3, 2021 03:32:55pm	ALARM	0	201
3, 2021 10:41:34am	4508e95030b460070af771	DEVICESW_GENERAL_PROCESSRESTART	True	4b33efab87313010bdc8517eab63590	N/A	N/A	N/A	ALERT	0	201
3, 2021 10:41:34am	4508e95030b460070af772	DEVICESW_GENERAL_PROCESSRESTART	True	8b332b2d87313010bdc8517eab63514	N/A	N/A	N/A	ALERT	0	201
3, 2021 10:41:33am	4508e95030b460070af55	DEVICESW_GENERAL_PROCESSRESTART	True	0333efab87313010bdc8517eab6358f	N/A	N/A	N/A	ALERT	0	201
3, 2021 10:41:33am	4508e95030b460070af56	DEVICESW_GENERAL_PROCESSRESTART	True	72332b2d87313010bdc8517eab63513	N/A	N/A	N/A	ALERT	0	201

Field	Description
Event Time	Time of the event
Event ID	Unique ID of the event.
Event Code	Code of the event.
Created	Status of event creation (True / False).
ServiceNow Sys ID	ServiceNow ID of the event.
Correlation ID	Correlation ID of the event.
Resolved Status	Status of the ticket (Resolved/Not Resolved/NA).
Ticket Resolution Time	Time when the ticket was resolved.
Event Type	Type of Event (Alarm/Alert).
Retry Attempts	The number of attempts made to create/resolve the ticket. Retry attempts can be anywhere between 0 and 5. The default value is 3.
Status Code	Status Code returned by ServiceNow Incident Management Table API endpoint for ticket creation/resolution.

Shasta LAN Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> □ Prisma SD-WAN license

Palo Alto Networks is at the forefront of networking and security, delivering a unified, streamlined Universal ZTNA solution that enables programmatic provisioning, visibility, and control for branch networks. This comprehensive approach integrates SD-WAN, switching, access points, and cloud-delivered security, ensuring seamless connectivity and robust protection across the entire network.

Through our partnership with Shasta Cloud, a cloud-based network management platform, we enhance LAN and WLAN (Wi-Fi) provisioning, configuration, and monitoring with a centralized interface for managing switches, access points, and LAN policies. When combined with Prisma SD-WAN, organizations gain a fully integrated, security-driven branch solution that simplifies deployment, operations, and Zero Trust enforcement—delivering seamless connectivity, enhanced security, and operational efficiency for modern enterprises.

Key Features of the Shasta LAN integration with Prisma SASE are:

- **Zero Touch Provisioning (ZTP)** - Automates the onboarding of LAN, WLAN, and SD-WAN devices, reducing manual configuration.
- **Unified Tenant Management** - Provides centralized control for wired, wireless, and SD-WAN infrastructure.
- **Enhanced Visibility** - Delivers detailed insights into site health, user and device connectivity, and end-to-end troubleshooting for proactive issue resolution.
- **Microsegmentation** - Enforces host isolation by preventing communication between wireless and wired ports within the same segment.

For more information on Shasta LAN integration, see:

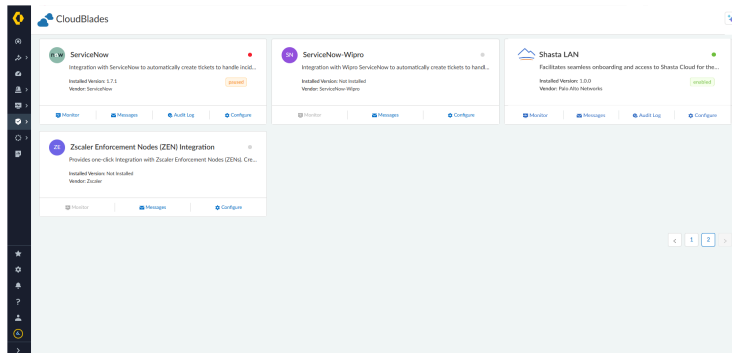
- [Configure Shasta LAN](#)
- [Branch Microsegmentation](#)
- [Shasta Supported Access Points and Switches](#)

Configure Shasta LAN

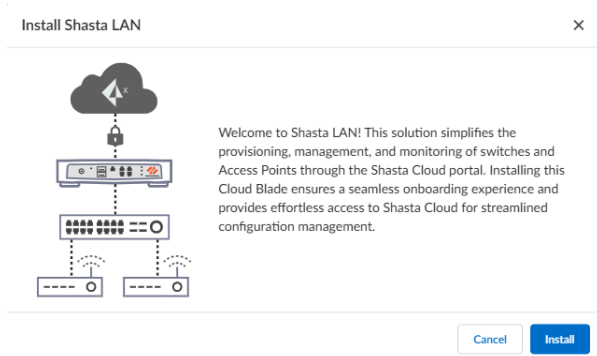
Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<input type="checkbox"/> Prisma SD-WAN license

To configure Shasta LAN:

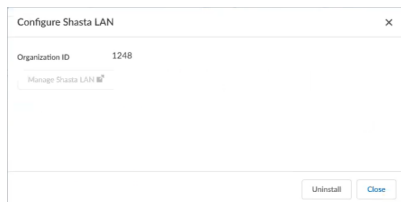
STEP 1 | On the CloudBlades page, select Configure on the Shasta LAN tile.



STEP 2 | Install the Shasta LAN.



STEP 3 | After the installation, configure and manage Shasta LAN on the Shasta Cloud portal.



As a first-time user, you will need to register on Shasta Cloud. After you register, you will receive an email invitation to log into Shasta Cloud. Complete the registration process to access the Shasta Cloud portal.

If you have access to Shasta Cloud, you can configure sites on Shasta Cloud.

STEP 4 | After saving the configuration, the Shasta LAN tile shows as enabled on the CloudBlade page.

Onboard Using Zero Touch Provisioning

ZTP simplifies and automates the onboarding of new branch sites to the Prisma SASE portal. To onboard branch sites:

STEP 1 | Navigate to **Branch Sites** and select a site.

STEP 2 | Select to **Configure** Shasta LAN.

←

Chicago Branch

Branch

Chicago, IL 60606, United States

Site Summary

Experience

Configuration

Overlay Connections

CONNECTIVITY

Physical: 1 of 3

Secure Fabric: 0 of 3

Prisma Access: 1 of 2

Standard VPN: 0 of 3

MODE

Control

DOMAIN

Preset Domain

PATH POLICY SET STACK

Default Path Simple Stack (Sim...

PERFORMANCE MANAGEMENT POLICY SET STACK

Default Performance Policy Se...

QOS POLICY SET STACK

Default QoS Simple Stack (Sim...

NAT POLICY SET STACK

Default-NATPolicySetStack

SECURITY POLICY SET

None

WAN MULTICAST

No profile

Create Profile

WAN Multicast Configurations

INTERNET CIRCUITS

Circuit to AT&T

Circuit to Airtel

Circuit to Tmobile

Change Circuits

PRIVATE WAN CIRCUITS

No private WAN circuits

Add Circuits

DEVICES

Chicago Branch ION (ion 1200-s-c5g...

Assign Device

IP PREFIXES (View)

No IP prefixes

Add IP Prefixes

VRF Profile

Global Profile

Create Profile

1 DHCP Scope

IOT DEVICE VISIBILITY

Enabled

IOT DISCOVERY PROFILE

Default Profile

Create Profile

Configure IOT SNMP Start Nodes

BRANCH GATEWAY

Disabled

SECURITY GROUP INFO

Disabled

SHASTA LAN

Configure

INTEGRATE WITH ZSCALER

Configure

STEP 3 | Click **Next**.

Configure Shasta LAN

×

1 About Shasta LAN

2 ZTP Onboarding

3 Select Networks

4 Configure ION Devices

With Shasta LAN, we provide a seamless onboarding solution for managing both LAN and Access Points, simplifying the process of integrating new devices.

As part of this workflow, a dedicated onboarding DHCP range will be established to dynamically provision new switches and access points at this branch site.

Cancel

← Previous

Next →

STEP 4 | Enter the DHCP information like **Subnet**, **Default Gateway**, **IP Range**, and **DNS Servers**. You can up to three DNS servers.

Configure Shasta LAN ×

1 About Shasta LAN For ZTP onboarding process by explaining that we require an infrastructure subnet with DHCP enabled.

2 ZTP Onboarding

3 Select Networks

4 Configure ION Devices

Subnet 10.10.100.0/24

Default Gateway 10.10.100.1

IP Range Start End

10.10.100.10 10.10.100.200

DNS Servers 8.8.8.8 +

Cancel Previous Next

STEP 5 | To complete the Shasta LAN onboarding configuration, **Select Networks** that should be pushed to the access points associated with this site.

For a first site deployment, define the wireless network parameters such as SSID name, authentication mechanisms, and isolation policy for segmentation.

You can also configure additional VLANs for the data traffic, supporting both switch and wireless users and devices.

Configure Shasta LAN ×

1 About Shasta LAN

2 ZTP Onboarding

3 Select Networks

4 Configure ION Devices

Select the wireless networks to associate with this site for user and device access.

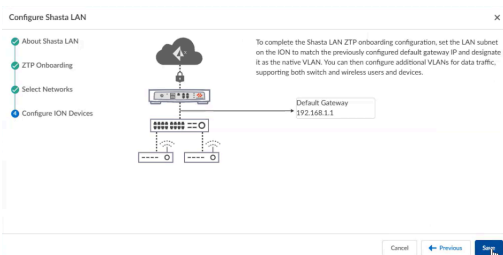
Wireless Networks Manage Networks

Network Name	Type
<input checked="" type="checkbox"/> guest-wireless	Passphrase
<input type="checkbox"/> test	Passphrase
<input type="checkbox"/> quarantined-network	Public
<input type="checkbox"/> IoT	Passphrase
<input checked="" type="checkbox"/> corp-wireless	Enterprise AAA

2 Rows Selected 10 Rows Page 1 of 1

Cancel Previous Next

STEP 6 | Click Next and **Save** your changes, and you can see the DHCP and network configured on the Shasta LAN.



STEP 7 | Now, you can update and manage Shasta LAN ZTP network and Wireless network settings by selecting the **Manage** button. You can also **Monitor** Shasta LAN by using the link below the Manage button.

You can monitor the LAN infrastructure at the site along with the clients connected to the LAN infrastructure by clicking the Monitor link. This takes you to the CloudBlade **Monitor** tab.

The screenshot shows the CloudBlade Configuration page for the Chicago Branch. The Configuration tab is active, displaying various network settings. A red box highlights the 'SHASTA LAN' section, which indicates 'DHCP Scope is configured' and provides links to 'Manage' and 'Monitor'.

Configuration Tab Settings:

- CONNECTIVITY:** Physical: 1 of 3, Secure Fabric: 0 of 3, Prisma Access: 1 of 2, Standard VPN: 0 of 0.
- MODE:** Control (dropdown).
- DOMAIN:** Preset Domain (dropdown).
- PATH POLICY SET STACK:** Default Path Simple Stack (Sim...).
- PERFORMANCE MANAGEMENT POLICY SET STACK:** Default Performance Policy Se...
- QOS POLICY SET STACK:** Default QoS Simple Stack (Sim...).
- NAT POLICY SET STACK:** Default-NATPolicySetStack.
- SECURITY POLICY SET STACK:** None.
- WAN MULTICAST:** No profile (dropdown). Create Profile, WAN Multicast Configurations.
- INTERNET CIRCUITS:** Circuit to AT&T, Circuit to Airtel, Circuit to Tmobile. Change Circuits.
- PRIVATE WAN CIRCUITS:** No private WAN circuits. Add Circuits.
- DEVICES:** Chicago Branch ION (ion 1200-...). Assign Device.
- IP PREFIXES (View):** No IP prefixes. Add IP Prefixes.
- VRF Profile:** Global Profile (dropdown). Create Profile.
- 2 DHCP Scopes:**
- IOT DEVICE VISIBILITY:** Enabled (toggle).
- IOT DISCOVERY PROFILE:** Default Profile (dropdown). Create Profile, Configure IoT SNMP Start Nodes.
- BRANCH GATEWAY:** Disabled (toggle).
- SECURITY GROUP INFO:** Disabled (toggle).
- SHASTA LAN:** DHCP Scope is configured. Manage | Monitor.
- INTEGRATE WITH ZSCALER:** Configure.

Onboard New Switches and Access Points

After enabling ZTP provisioning for Shasta LAN at a site, you can now connect Shasta Switches and Access Points to your branch network. Connect your switch uplink ports to the ION device's LAN interface. After the device receives a DHCP address, it will automatically connect to the Shasta Cloud portal, apply the default switch profile (default profiles can be modified in the Shasta Cloud portal), and be provisioned as part of a Venue (also known as a Prisma SD-WAN site). Any additional switches and access points connected will automatically attach to the Venue moving forward.

To monitor the status of switches and access points, navigate to the **CloudBlade > Shasta LAN > Monitor** page. Here, you can view real-time connectivity, device health, performance metrics, and event logs, ensuring optimal network operation and troubleshooting capabilities.

General - The General tab displays the total number of connected access points, switches, and clients to the site.

← Cloudblades

Shasta LAN

Monitoring

General

Switches

Access Points

Wireless Clients

Wired Clients

Block List

Notifications

Refresh

TOTAL MANAGED SWITCHES	TOTAL MANAGED ACCESS POINTS	TOTAL CONNECTED CLIENTS
1	2	12


<

1

>

Switches - Switches shows the switches connected to the venue and their status.

← Cloudblades

 Shasta LAN ●

Monitoring

GeneralSwitchesAccess PointsWireless ClientsWired ClientsBlock ListNotifications


Refresh

NAME	SITE/VENUE	STATUS	SWITCH PROFILE	PRIVATE IP
PAN 4150-54P	Chicago Branch	connected	Base	10.10.100.43

< 1 >

Access Points - Access Points shows the access points connected to the venue and their status.

← Cloudblades

 Shasta LAN ●

Monitoring

GeneralSwitchesAccess PointsWireless ClientsWired ClientsBlock ListNotifications

NAME	SITE/VENUE	STATUS	AP PROFILE	RF PROFILE
PAN EAP102	Chicago Branch	connected	Base	Base
PAN 630C	Chicago Branch	connected	Base	Base

Wireless Clients - The page lists the wireless clients connected to the site.



Cloudblades



Shasta LAN ●

Monitoring

- General
- Switches
- Access Points
- Wireless Clients
- Wired Clients
- Block List
- Notifications

NAME	SITE	MAC ADDRESS	NETWORK	INFRASTRUCTURE
WiFi-Socket	Chicago Branch	3873eae3411e	guest-wireless	PAN 630C
HP Laptop 14-dq0xxx	Chicago Branch	c0bfbed5fee5	guest-wireless	PAN 630C
Tapo-C210	Chicago Branch	dc6279a5bfb2	guest-wireless	PAN 630C

Wired Clients - The page lists the wired clients connected to the site.



Cloudblades



Shasta LAN ●

Monitoring

- General
- Switches
- Access Points
- Wireless Clients
- Wired Clients
- Block List
- Notifications

NAME	SITE	MAC ADDRESS	NETWORK	INFRASTRUCTURE	VLAN	STATE	CONNECTED
Palo Alto Networks	Chicago Branch	04472a0ba2c2	Ethernet1	PAN 4150-54P	1	-	63 Day(s)
Palo Alto Networks	Chicago Branch	04472a0ba2ca	Ethernet2	PAN 4150-54P	1	-	63 Day(s)
Palo Alto Networks	Chicago Branch	04472a0ba2e1	Ethernet2	PAN 4150-54P	1	-	63 Day(s)
PAN 630C	Chicago Branch	24fe9a0f9969	Ethernet2	PAN 4150-54P	1	-	63 Day(s)
CyberTAN Technology Inc.	Chicago Branch	24fe9a0f996a	Ethernet2	PAN 4150-54P	1	-	11 Hr(s)
CyberTAN Technology Inc.	Chicago Branch	24fe9a0f996b	Ethernet2	PAN 4150-54P	1	-	11 Hr(s)
PAN EAP102	Chicago Branch	d4dc85960852	Ethernet3	PAN 4150-54P	1	-	4 Hr(s)
-	Chicago Branch	d4dc85960854	Ethernet3	PAN 4150-54P	1	-	4 Hr(s)
-	Chicago Branch	d4dc85960855	Ethernet3	PAN 4150-54P	1	-	4 Hr(s)

Block Lists - The Block lists show the list of clients that are banned or quarantined from connecting to the network. This is useful when dealing with a compromised device that you need to quarantine from the rest of the network to prevent lateral threats from moving throughout your LAN and WAN.

← Cloudblades

Shasta LAN

Monitoring

General

Switches

Access Points

Wireless Clients

Wired Clients

Block List

Notifications

Refresh

Delete

Add

<input type="checkbox"/>	NAME	MAC ADDRESS	DATE CREATED
<input type="checkbox"/>	-	dc:62:79:a5:bbe6	2025-05-15T18:14:19.745Z

< 1 >

To add a device to the list, click **Add** to specify the Mac address and click **Apply**.

Add Block List

×

Enter mac address

Cancel

Apply

You can unblock clients that were banned earlier by using the **Delete** button.

Notifications - The Notifications shows any incidents and alarms for the switching and wireless infrastructure.

Branch Microsegmentation

To enforce host segmentation and isolate wireless and wired ports, you must update the Shasta switch profile to enable Port Isolation and the Network SSID to Client Isolation.

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<input type="checkbox"/> Prisma SD-WAN license

STEP 1 | On the CloudBlades page, select **Configure** on the Shasta LAN tile and select **ManageShasta**.

STEP 2 | Select **Infrastructure > Profiles** and edit the switch profile that you want to enable segmentation.

STEP 3 | Select Configuration and **Enable Port Isolation**.

STEP 4 | Choose the **Uplink** and **Downlink Ports** that connect to other Shasta devices and Prisma SD-WAN ION devices.

L2 Settings

Spanning Tree Protocol

None

Port Isolation

☒

Uplink Ports*

Downlink Ports

STEP 5 | To apply isolation to Access Points, navigate to **Networks**, select the name, and apply Client Isolation.

General Settings > Authentication > Network Settings > Association

Network Settings

VLAN

Enter number

Client Downstream Rate-Limit(Mbps)

E.g. 100

Client Upstream Rate-Limit(Mbps)

E.g. 100

Client Isolation*

Network Wide

Client Idle Timeout (Seconds)

300

Wireless Settings

Select Bands

☒ 2G ☒ 5G ☐ 6G

Hide Network

☐

802.11K Neighbor Reporting

☒ ON

802.11r Roaming

☒ ON

Client Steering

☒ ON

Shasta Supported Access Points and Switches

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> □ Prisma SD-WAN license

Shasta is continuously expanding its lineup of hardware [Access Points](#) and [Switches](#). Below is the latest list as of January 2025.

Table 1: Access Points

Access Points	Description
RAP630C-311G - Ceiling AP	Wi-Fi 6 2x2 dual-band (2.4/5GHz), 1 x 2.5GB Uplink (PoE-In), 2 x 1GB LAN
RAP630W-311G - Wallplate	Wi-Fi 6, 2x2 dual-band (2.4/5GHz), 1 x 1GB Uplink (PoE-In), 3 x 1GB LAN (1 PoE-Out)
EAP-101T - Ceiling AP	Wi-Fi 6 2x2 dual-band (2.4/5GHz), 1 x 2.5GB Uplink (PoE-In), 2 x 1GB LAN, BLE/Zigbee Support
EAP-104T - Wallplate AP	Wi-Fi 6, 2x2 dual-band (2.4/5GHz), 1 x 1GB Uplink (PoE-In), 4 x 1GB LAN (1 PoE Out), BLE/Zigbee support
EAP-104LTL-Wallplate AP	Wi-Fi 6, 2x2 dual-band (2.4/5GHz), 1 x 1GB Uplink (PoE-In), 4 x 1GB LAN
EAP-111T-Ceiling AP	Wi-Fi 6 2x2 dual-band (2.4/5GHz), 1x1GB Uplink (PoE-In), 1xGB LAN, BLE, Zigbee, Thread Support
WF-186H - Wallplate AP	Wi-Fi 6, 2x2 dual-band (2.4/5GHz), 1 x 1GB Uplink (PoE-In), 2 x 1GB LAN
WF-186W - Wallplate AP	Wi-Fi 6, 2x2 dual-band (2.4/5GHz), 1 x 1GB Uplink (PoE-In), 4 x 1GB LAN
WF-188N - Ceiling AP	Wi-Fi 6, 2x2 dual-band (2.4/5GHz), 1 x 1 GB Uplink (PoE-In), 1 x 1GB LAN
WF-660A - Outdoor AP	Wi-Fi 6, 2x2 dual-band (2.4/5GHz), 1 x 2.5GB Uplink (PoE-In), IP67
WF-196 - Ceiling AP	Wi-Fi 6E, 4x4 Tri-band (2.4/5/6GHz), 1 x 5GB Uplink (PoE-In), 1 x 2.5GB LAN

Access Points	Description
EAP-102T - Ceiling AP	Wi-Fi 6, 4x4 dual-band (2.4/5GHz), 1 x 2.5GB Uplink (PoE-In), 1 x 2.5 GB LAN, BLE Support
OAP-101T-Outdoor AP	Wi-Fi 6, 2x2 dual-band (2.4/5GHz), 1 x 2.5GB PoE WAN, 1 x 1GB LAN, IP68, BLE Support
EAP105T-Ceiling AP	Wi-Fi 7, 2x2 Tri-band (2.4/5/6GHz), 1 x 5GB Uplink (PoE-In), 1 x 1GB LAN
EAP106T-Ceiling AP	Wi-Fi 7, 4x4 Tri-band (2.4/5/6GHz), 1 x 10GB Uplink (PoE-In), 1 x 1GB LAN
OAP106T-Outdoor AP	Wi-Fi 7, 2x2 Tri-band (2.4/5/6GHz), 1 x 5GB Uplink (PoE-In), 1 x 1GB LAN

Table 2: Switches

Switches	Description
ECS2100-10P-T-Access switch	8 x 1GB PoE, af/at 120 watts, 2 x 1GB SPF, 20 Gbps switching capacity
ECS4125-10P-T - Access switch	8 x 2.5GB PoE++, 2 X 10GB (SFP+), 30W on 8 ports or 60W on 4 ports for a total of 240W
ECS4150-28P-T - Access switch	24 x 1GB PoE+, 4 X 10GB (SFP+), total of 370W
ECS2100-28PP-T-Access switch	24 x 1GB PoE+, 4 X 1GB (SFP+), total of 370W
ECS-4150-54P-T-Access switch	48 x 1GB PoE++, 6 X 25GB (SFP28), total of 740W
EPS-202-T - Access switch	48 x 1G (RJ-45) PoE++ (up to 60W), 4 x 25G (SFP28) WAN ports, PoE budget 1, 560W with 2 PSUs
ECS552018-T Aggregation switch	16 x 10GB SFP+, 2 x 40GB QSFP+, 2 PSUs

Zoom QSS CloudBlade Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • Strata Cloud Manager 	<ul style="list-style-type: none"> ❑ Prisma SD-WAN license ❑ Zoom QSS CloudBlade

There's an increasing trend of cloud-delivered **Unified communications as a service (UCaaS)** solutions. The most significant UCaaS trend is the demand for video-first user experiences and collaboration-centric features. Zoom is the leading provider of collaboration solutions like video meetings, content sharing, and collaboration-enabled conferences.

The application performance and user experience for cloud-delivered collaboration solutions depend on the application scalability and efficiency of the network connecting users to the cloud-based applications. For troubleshooting issues with Zoom application performance and reachability in SD-WAN networks, you require visibility into Zoom application data. To easily identify potential issues, IT teams find it helpful when Zoom- provided application metrics are available for consumption.

Prisma SD-WAN and Zoom QSS Prerequisites

The following are required for configuring Prisma SD-WAN and Zoom QSS CloudBlade:

- You must have administrative or owner privileges to the Zoom account to grant authorization for the SD-WAN app in the Zoom marketplace. You can disable the Zoom integration for your tenants at any time, but if you do so and later want to enable the Zoom integration for that tenant, you will be required to repeat the authorization process.
- The Zoom QSS in Prisma SD-WAN CloudBlade must be installed from the Prisma SASE portal to onboard a tenant.
- You must have purchased a Zoom Quality of Service Subscription (QSS) as an add-on from Zoom. Zoom QSS offers packet loss, latency, jitter, framerate and resolution for every user.
- The Zoom QSS feature can be authorized through the Autonomous DEM (ADEM) interface, however, the Zoom QSS Cloudblade must be enabled to view the SD-WAN dashboard.
- You must be a Prisma SD-WAN greenfield tenant or tenant with a TSG ID.
- You must have an AIOps license to view the Zoom application activities.
- Consent for events and scopes used by Prisma SD-WAN must be allowed to complete the onboarding process.

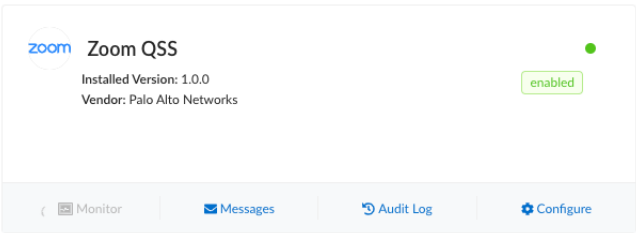
Configure the Zoom QSS CloudBlade in Prisma SD-WAN

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none"><input type="checkbox"/> Prisma SD-WAN license<input type="checkbox"/> Zoom QSS CloudBlade

To configure the Zoom QSS CloudBlade in Prisma SD-WAN:

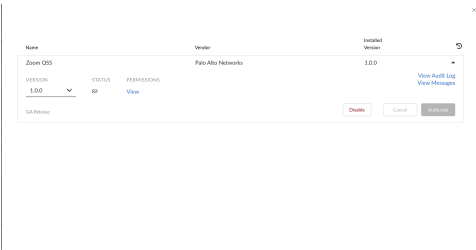
STEP 1 | From Strata Cloud Manager, go to **Manage > Prisma SD-WAN CloudBlades**.

STEP 2 | In CloudBlades, locate the **Zoom QSS CloudBlade** tile and select **Configure**.

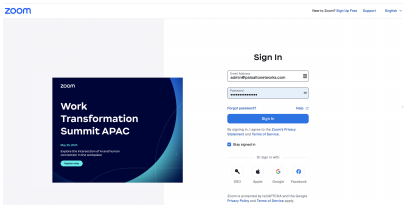


STEP 3 | Select **Authorize**.

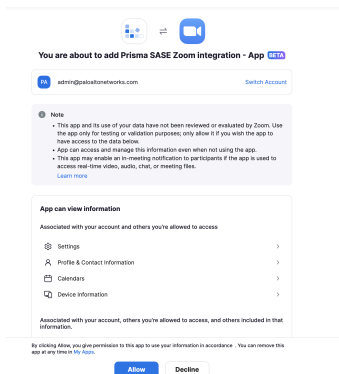
If the Zoom authorization is already done, the button on the configuration screen will be disabled.



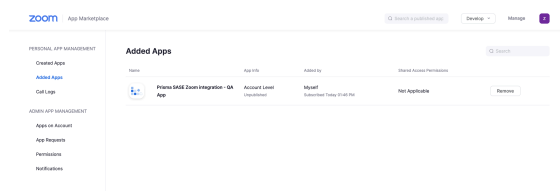
STEP 4 | Enter your Zoom credentials (Email Address and Password) in the Zoom sign in page.



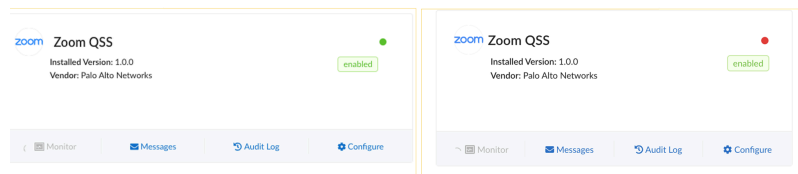
STEP 5 | Select **Allow** to add access permissions of the Prisma SASE Zoom Integration app.



STEP 6 | To verify if the CloudBlade is enabled, go to the Zoom marketplace to see if the **Prisma SASE Zoom Integration** app is published under **Added Apps**.

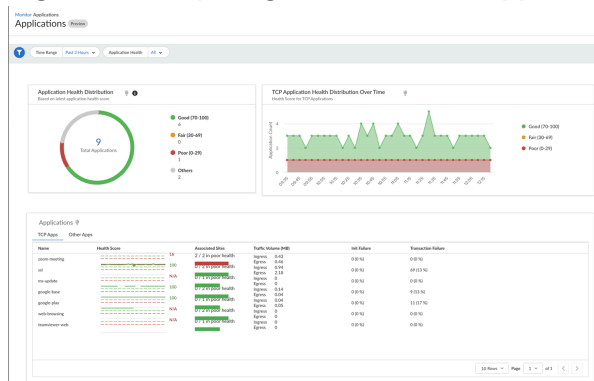


You will see a green indicator on the Zoom QSS CloudBlade tile upon successful authorization. A red indicator means the Zoom account is not authenticated properly, and needs to be re-authorized. When there is no indication, the CloudBlade is in a uninstalled state.



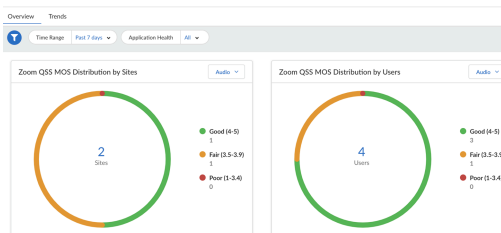
Access Zoom Application Experience Data

Prisma SD-WAN shows you the Zoom application experience data at an individual user level. You can navigate to this data from the following dashboards:

STEP 1 | Go to **Strata Cloud Manager > Activity Insights > SD-WAN Applications**.

The **Application** screen shows you the following widgets:

- **Application Health Distribution:** The distribution of good, fair, and poor applications for a given tenant.
- **Application Health Distribution Over Time:** The time series graph of application health distribution over time displays the good, fair, and poor applications for a given tenant. The time-series graph should be computed and refreshed based on the selected duration. For example, supported durations are 1 hour, 3 hours, one day, seven days, 30 days, and 90 days and the interval is 1 minute, 5 minutes, 1 hour, and one day, respectively.
- **Applications:** Lists all the applications details under **TCP Apps** such as Name, Health Score, Associated Sites, Traffic Volume, Init/Failure, and Transaction Failure.

STEP 2 | Select the zoom-meeting app from the list of apps. The **Overview** tab displays the Zoom QSS MOS distribution data for a site and for a user.

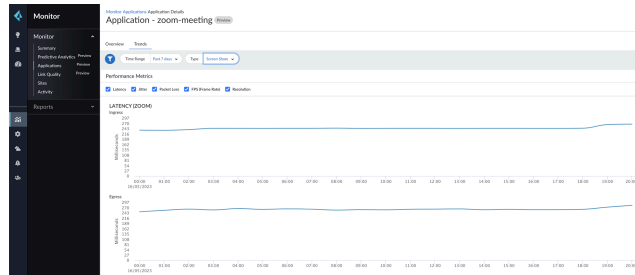
- **Zoom QSS MOS Distribution by Sites:** shows the Zoom MOS distribution of good, fair, and poor applications across sites. This application data can be filtered by audio, video, and screen share for a selected time period.
- **Zoom QSS MOS Distribution by Users:** shows the Zoom MOS distribution of good, fair, and poor applications across users. This application data can be filtered by audio, video, and screen share for a selected time period.
- **zoom-meeting Performance Details:** shows the zoom meeting performance and metrics per user for a selected time period. The **Users** tab lists a user's client IP address, user email, SD-WAN site, MOS count, latency, jitter, and packet loss percentage.

Zoom Meeting Performance Details						
Summary by Performance and metrics per users during the selected time range						
Client IP Address	User Email	SD-WAN Site	MOS Count	Latency (ms)	Jitter (ms)	Packet Loss (percentage)
192.168.1.100	john.doe@paloalto.com	-	Audio: 4.0 Video: 4.0 ScreenShare: 4.0	20.00 20.00 20.00	0.00 0.00 0.00	0.00 0.00 0.00
192.168.1.101	john.doe@paloalto.com	Site 1	Audio: 4.0 Video: 4.0 ScreenShare: 4.0	20.00 20.00 20.00	0.00 0.00 0.00	0.00 0.00 0.00
192.168.1.102	john.doe@paloalto.com	-	Audio: 4.0 Video: 4.0 ScreenShare: 4.0	20.00 20.00 20.00	0.00 0.00 0.00	0.00 0.00 0.00
192.168.1.103	john.doe@paloalto.com	Site 2	Audio: 4.0 Video: 4.0 ScreenShare: 4.0	20.00 20.00 20.00	0.00 0.00 0.00	0.00 0.00 0.00

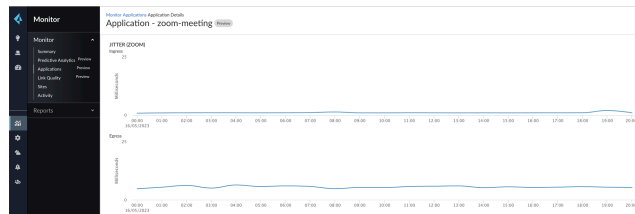
STEP 3 | Select the **Trends** tab to see the overall performance metrics against the network baseline app performance for audio, video, and screen share performance for a selected time frame.

The following graphs represent:

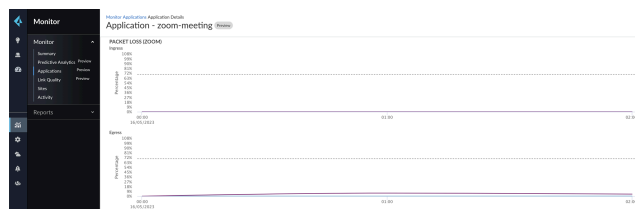
- **Latency (Zoom):** The latency used from the Zoom application in both the ingress and egress directions.



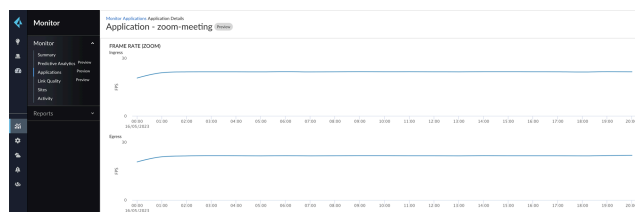
- **Jitter (Zoom):** The jitter used from the Zoom application in both the ingress and egress direction.



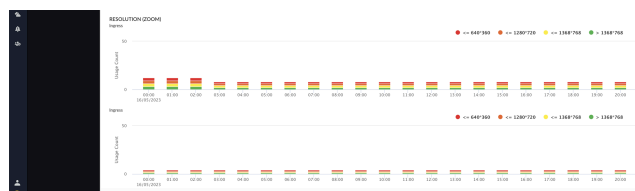
- **Packet Loss (Zoom):** The packet loss from the Zoom application in both the ingress and egress direction.



- **Frame Rate (Zoom):** The Frame rate (expressed in frames per second or FPS) at which consecutive images (frames) are captured or displayed from the Zoom application in both the ingress and egress directions.



- **Resolution (Zoom):** The resolution of the images (frames) are captured or displayed from the Zoom application across users in both the ingress and egress direction. The resolution markers depicted are color coded.





If the Zoom metrics is not visible for a period of time, recheck the QSS license status and reconfirm if the Zoom QSS CloudBlade is authorized successfully. If the issue still persists, contact the Palo Alto Networks support team.

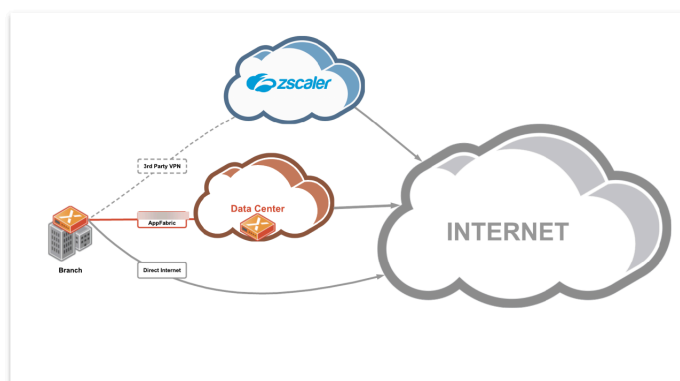
Zscaler Internet Access CloudBlade Integration

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license Zscaler Enforcement Nodes (ZEN) Integration CloudBlade

As enterprises rely on SaaS or Cloud-based delivery models for business-critical applications, there's a compelling need for per-application policy enforcement without increasing remote office infrastructure. Traditional hardware-router based approaches are limited by heavy-handed 'all or nothing' policies for direct-to-internet versus policy enforcement per-application. Additionally, because router-based approaches are packet-based versus application-session based, they fail to meet application session-symmetry requirements, causing network and security outages.

The integration of Prisma SD-WAN SD-WAN and Zscaler Internet Access (ZIA), allows customers to have a lightweight remote office hardware footprint, while still being able to provide a full suite of application-specific security policies.

To facilitate this integration, Prisma SD-WAN Release 5.1.1 and later provide CloudBlades to automatically integrate the Prisma SD-WAN Controller, Remote Prisma SD-WAN ION devices and Zscaler Enforcement Nodes (ZENs).



Prerequisites

The following items are required for configuring Prisma SD-WAN and Zscaler Internet Access integration:

Prisma SD-WAN

- An active Prisma SD-WAN subscription.
- Prisma SD-WAN AppFabric deployed at one or more locations.
- Physical and/or virtual ION devices running Release 5.1.9 or later.

Zscaler

- An active Zscaler Internet Access Instance (in any cloud).
- Administrator login credentials for this instance.
- A partner administrator account and partner key.

Plan the Zscaler CloudBlade Deployment

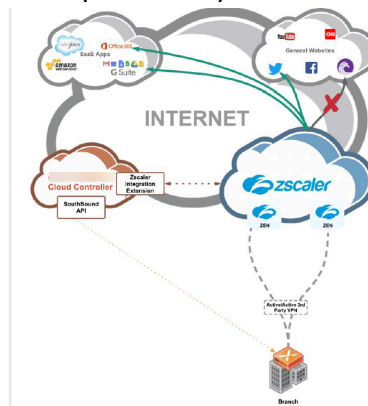
Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license Zscaler Enforcement Nodes (ZEN) Integration CloudBlade

The primary way to architecturally accomplish the Prisma SD-WAN and Zscaler Internet Access integration is through IPsec Standard VPNs and GRE tunnels from remote ION device endpoints to Zscaler. The Zscaler Integration CloudBlade automatically creates, manages, and maintains the IPsec and GRE Standard VPN tunnels.

Starting with release version 2.0.0, the Zscaler CloudBlade supports both IPsec and GRE tunnels. Zscaler Internet Access (ZIA) has launched APIs that can be used to build GRE tunnels to Zscaler nodes from branches that require high throughput. Each GRE tunnel can have up to 1 Gbps bandwidth.

The **AUTO-zscaler-GRE** tag is added to a site and circuit to create the GRE tunnels. The site tag is extended for sub-location, custom endpoint, and other options, while the circuit tag is a static tag. A single interface on the device supports both the IPsec tunnels (AUTO-zscaler tag) and GRE tunnels (AUTO-zscaler-GRE tag). If a circuit is tagged with both AUTO-zscaler and AUTO-zscaler-GRE tags on an interface, then both IPsec and GRE tunnels are established to the specific ZEN Nodes.

The Prisma SD-WAN interface must be configured and linked to Zscaler through a partner administrator account, and an SD-WAN partner key to facilitate this tag-based configuration.



Use the following steps to complete the integration:

- STEP 1 |** Create a partner administrator role, create a partner administrator account and assign the role, and generate an SD-WAN partner key from the Zscaler portal.
- STEP 2 |** Configure and install the Zscaler CloudBlade in the Prisma SD-WAN portal.
- STEP 3 |** Configure Prisma SD-WAN sites, and tag the circuit categories to denote which sites and circuit types are candidates for auto Standard VPN tunnel and GRE tunnel creation to Zscaler.

STEP 4 | Edit application network policy rules to send traffic to the Zscaler.



Prior to configuring the Zscaler CloudBlade in the Prisma SD-WAN portal, make sure that the user account you are logged in with has IP session lock disabled.

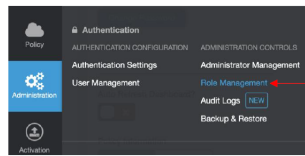
Acquire the Zscaler Information

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ Zscaler Enforcement Nodes (ZEN) Integration CloudBlade

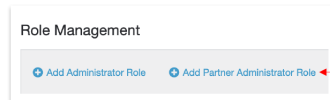
Before configuring Prisma SD-WAN to integrate with Zscaler, perform the following steps:

STEP 1 | Create a partner administrator role with full access controls for **Locations** and **VPN Credentials**. From version 2.0.0 onwards, you can also include access controls for options **Static IP** and **GRE Tunnels**.

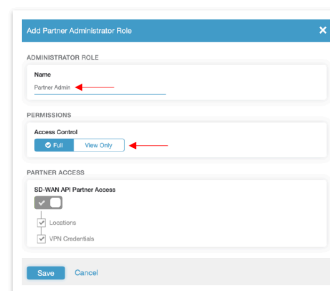
1. From **Administration**, click **Role Management**.



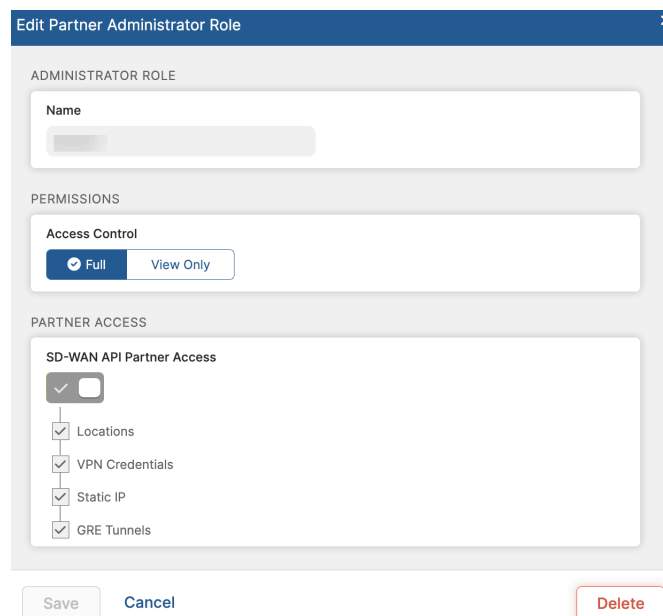
2. Click **Add Partner Administrator Role**.



3. On the **Add Partner Administrator Role** screen, select **Full** for **Access Control**. In the **Partner Access** section, select the **Locations** and **VPN Credentials** check boxes and click **Save**.

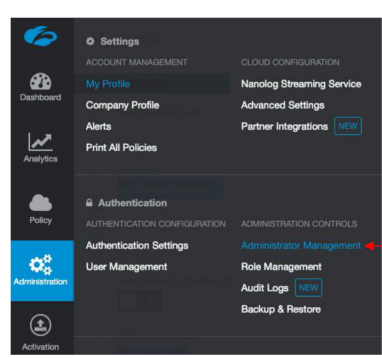


From version 2.0.0, in the **Partner Access** section, you can also select the options **Static IP** and **GRE Tunnels**.

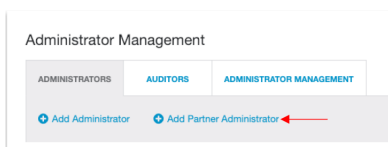


STEP 2 | Create a **partner administrator account** and assign the **Partner Admin** role created in Step 1.

1. From **Administration**, select **Administrator Management**.



2. On the **Administrator Management** screen, click **Add Partner Administrator**.

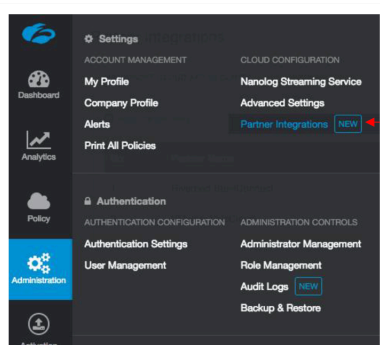


3. Select **Partner Admin** as the **Partner Role** and click **Save**.

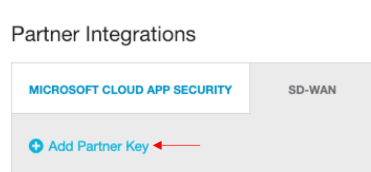
A screenshot of the 'Add Partner Administrator' form. The form is divided into two sections: 'ADMINISTRATOR' and 'SET PASSWORD'. In the 'ADMINISTRATOR' section, the 'Login ID' is 'api-test2', the 'Email' is 'api-test2@demo-cloudgenix.com', and the 'Name' is 'API Test User 2'. The 'Partner Role' dropdown is set to 'Partner Admin' and is highlighted with a red arrow. There is a 'Comments' text area below. In the 'SET PASSWORD' section, there are fields for 'Password' and 'Confirm Password'. At the bottom, there are 'Save' and 'Cancel' buttons.

STEP 3 | Generate an SD-WAN partner Key.

1. From **Administration**, select **Partner Integrations**.



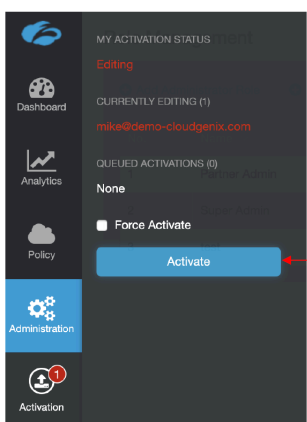
2. On the **SD-WAN** tab, click **Add Partner Key**.



3. The value of the **key** is displayed in the Key field. Copy this key, it will be needed during the configuration process.



STEP 4 | Activate pending changes on Zscaler by navigating to the **Activation** screen and clicking **Activate**.



If you wish to increase the Static IP and GRE tunnel limit to a desired number from the default value of 100, contact Zscaler support.

Create Security Zone and Security Policy for GRE Tunnels Creation

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license Zscaler Enforcement Nodes (ZEN) Integration CloudBlade

GRE tunnels created by the Zscaler Cloudblade must require a security policy (v1) or security policy set(v2) to be applied to the site for tunnel creation. The security policy and zone must be created and mapped to the site. The Cloudblade automatically places the servicelink GRE tunnel into the security zone. The CloudBlade typically creates two GRE tunnels, a Primary tunnel to Data center one and a Secondary GRE tunnel to Data center two.



If a policy or zone is removed later, the CloudBlade ignores all GRE operations performed on that site. This includes creating, updating or re-querying.

STEP 1 | Add a security zone.

1. In **Strata Cloud Manager**, go to **Manage > Policies > Security**.
2. Select **Security Zones** and add a **Security Zone**.

NGFW Security Zones

SECURITY STACKS			SECURITY SETS			SECURITY ZONES			SECURITY PREFIXES		
FILTER (By zone name)						TAGS					
▼						View All					
NAME						# SECURITY RULES USING THIS ZONE					
Test						0					
Test 2						0					
ZS GRE						1					

3. On the next screen, enter a name for the security zone and an optional description.
4. Click **Create**.

Add Security Zone

NAME

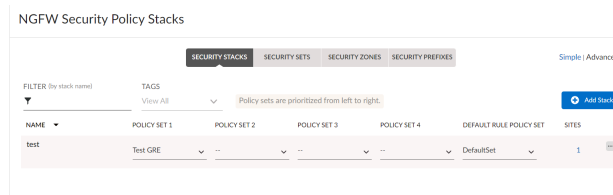
DESCRIPTION (optional)
Add a short description

256 character limit

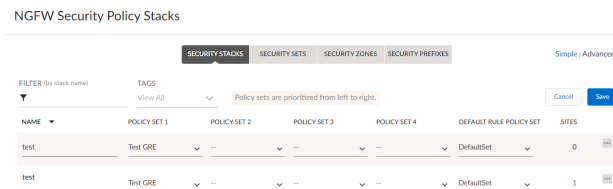
Cancel Create

STEP 2 | Add a security policy stack.

1. Select **Policies > Security** and add a Stack.

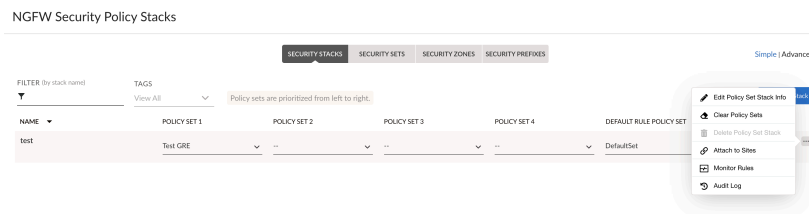


2. Enter a name for the Security stack, select the security policy zone created previously and **Save** the changes.



STEP 3 | Bind the security policy to the site.

1. Select the **Security Stack**.
2. From the ellipsis menu for a security policy, select **Attach to Sites**.



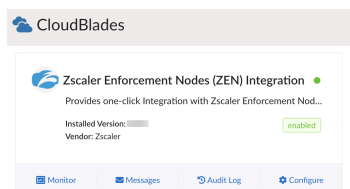
3. Select the site and click **Edit Selected**.
4. Review or edit your security policies and select **Save**.

Configure and Install the Zscaler Integration

Configure the Prisma SD-WAN CloudBlade to prepare the Prisma SD-WAN controller for integration.

STEP 1 | In **Strata Cloud Manager**, go to **Manage > Prisma SD-WAN > CloudBlades**.

STEP 2 | Locate the **Zscaler Enforcement Nodes (ZEN) Integration CloudBlade** tile in the CloudBlades page and click **Configure**. If this CloudBlade does not appear, contact Palo Alto support team.



STEP 3 | Enter the following information in the CloudBlade installation page.

1. From the **Version** list, select the required version.
2. For **Admin State**, retain **Enabled**, which is the default value.
3. For **API Key**, provide the SD-WAN key generated in the previous section.
4. For **Partner Admin Username** and **Partner Admin Password**, provide the partner administrator account details created in the previous section.
5. For **Zscaler cloud**, select the **Zscaler cloud** to which your subscription is attached (zscalerthree in the example below).



From version 2.1.0 onwards, the CloudBlade supports govcloud which supports only IPsec tunnels.

6. Specify the **IPsec Profile** name (case sensitive). The default is ZSCALER_IKEV2, which should be pre-provisioned along with the CloudBlade allocation. The tunnels to be created will be identified based on the tags created (AUTO-zscaler for IPsec and AUTO-zscaler-GRE for GRE; version 2.0.0 onwards).
7. If you select **Allow Interface Level Override** for the IPsec profile, it will allow administrators to change the IPsec profile referenced at the Standard VPN tunnel level without the CloudBlade overriding this change. This is typically useful in case of troubleshooting scenarios.
8. **(Optional)** Provide the **base URL**. If left blank, the base URL will be derived from the admin username domain.

STEP 4 | After you configure the settings, click **Install** (or **Save**, if the CloudBlade was previously installed).

The screenshot shows the configuration interface for Zscaler Enforcement Nodes (ZEN) Integration. At the top, it displays 'Zscaler Enforcement Nodes (ZEN) Integration' with a version of '2.0.0' and a status of 'PAUSED'. Below this, there are tabs for 'VERSION', 'STATUS', 'PERMISSIONS', and 'ADMIN STATE'. The 'ADMIN STATE' tab is selected, showing a 'Paused' status. The configuration fields include: 'PARTNER API KEY' (with an 'unmask' button), 'PARTNER ADMIN USERNAME' (with an 'unmask' button), 'PARTNER ADMIN PASSWORD' (with an 'unmask' button), 'ZSCALER CLOUD' (set to 'zscalerthree'), 'IPSEC PROFILE' (set to 'ZSCALER_IKEV2'), and a checked checkbox for 'ALLOW INTERFACE LEVEL OVERRIDE?'. At the bottom, there is a 'BASE URL (optional)' field and buttons for 'Unmask', 'Cancel', and 'Save'.

Configure IPsec and GRE in Prisma SD-WAN

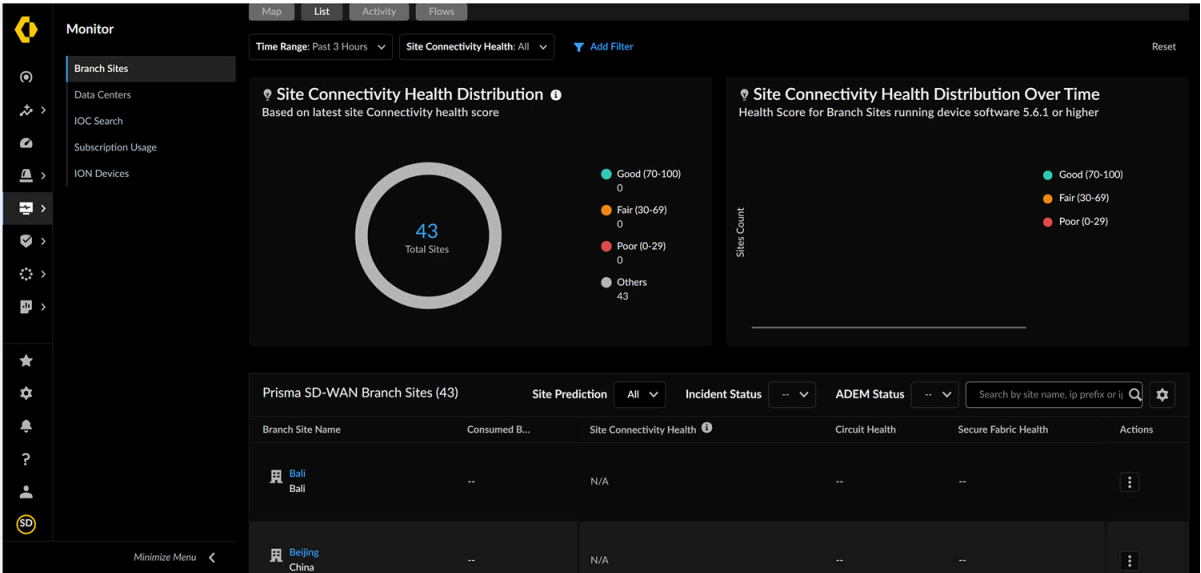
Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">Strata Cloud Manager	<ul style="list-style-type: none">Prisma SD-WAN licenseZscaler Enforcement Nodes (ZEN) Integration CloudBlade

This workflow simplifies the integration between Prisma SD-WAN and Zscaler by automating the creation, management, and maintenance of third-party IPsec VPN tunnels. By leveraging this one-touch integration, branch sites can seamlessly connect to Zscaler without manual configuration.

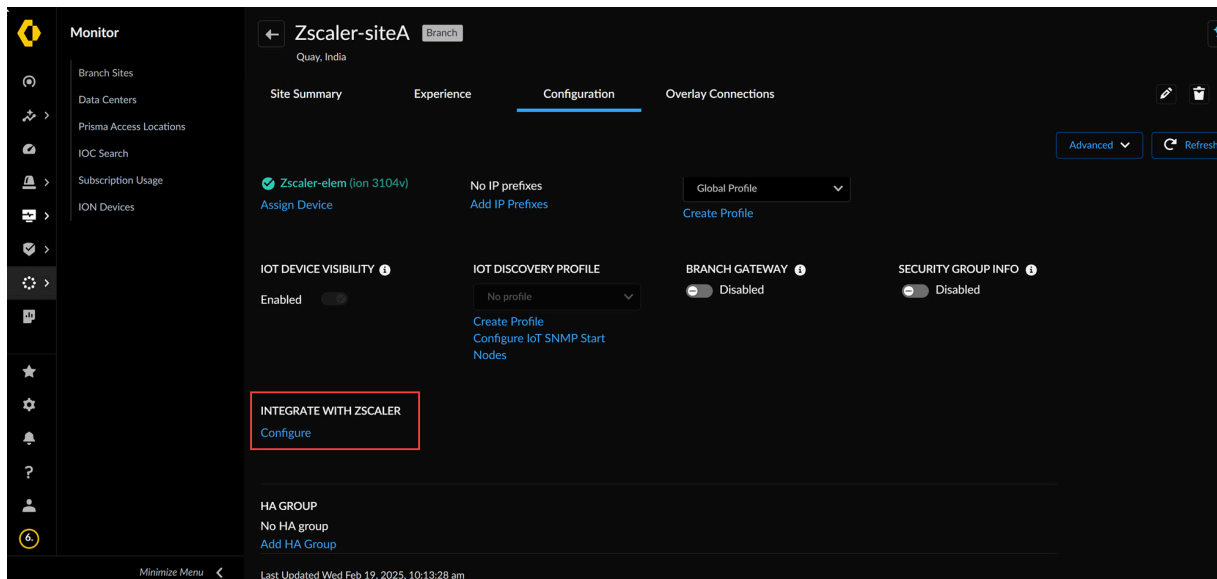
After the CloudBlade is configured, the next task is to configure Prisma SD-WAN sites, and tag the circuit categories to denote which sites and circuit types are candidates for auto Standard VPN tunnel and GRE tunnel creation to Zscaler.

STEP 1 | In **Strata Cloud Manager**, go to **Monitor > Prisma SD-WAN > Branch Sites**.

STEP 2 | Switch to **List View**, search for the required branch site, and open the site details page.



STEP 3 | Go to the **Configurations** tab and click **Configure** to initiate the Zscaler integration process.



The **Configure** button remains disabled if no [circuits](#) are attached or the CloudBlade is not enabled.

STEP 4 | On the **Connect to Zscaler** screen, select the tunnel type (**IPSec** or **GRE**) for configuration. To configure the **GRE Tunnel**, ensure that a **Security Zone** is associated with a Security Policy, and the Security Policy is bound to the site. Associating a Security Zone is mandatory for GRE tunnels. Go [here](#) to configure GRE endpoints for both primary and secondary tunnels.

STEP 5 | Select the preconfigured [Security Zone](#) and specify the Custom Endpoint for both primary and secondary tunnels (version 2.0.0 onwards).

The screenshot shows the 'Connect to ZScaler' configuration window, specifically Step 1: Tunnels & Gateways. The window has a dark theme. On the left, there is a sidebar with two steps: 'Step 1 Tunnels & Gateways' (active) and 'Step 2 Circuits'. The main content area is titled 'Pre-requisites' and includes a link to the 'Zscaler Internet Access CloudBlade Integration Guide'. Below this, the 'Tunnel Types' section asks the user to select the type of tunnel(s) to connect to ZScaler. There are two options: 'IPSec Tunnel' (unchecked) and 'GRE Tunnel' (checked). Below the tunnel types, there is a 'Security Zone (for GRE Tunnels only)' dropdown menu with the text 'Select Security Zone'. Below that, there is a 'Security Policy (for GRE Tunnels only)' field with the value '1732962950827019496'. A red error message box is displayed, stating: 'Security policy must be bound to the site for GRE tunnel configuration. Please bind a security policy to this site and then configure ZScaler integration.' At the bottom of the main content area, there is a section for 'Gateways, Sub-Locations and Endpoints' with an 'Optional' button. At the bottom right of the window, there are 'Cancel' and 'Next ->' buttons.



When using custom endpoints for GRE tunnels, ensure the IP addresses are listed among the closest data centers and belong to data centers in different locations.

STEP 6 | To [configure](#) the IPSec tunnel, set up a custom Standard VPN Endpoint if needed instead of the one managed by CloudBlade.

STEP 7 | Configure the Gateway, Sub-Locations, and Endpoints options.

- To configure the **Gateway** options at the parent location level, select the required settings to ensure all traffic from this location follows the configured options.

The screenshot shows the 'Connect to ZScaler' dialog box with the 'Gateway' tab selected. The 'IPSec Tunnel' option is checked, and 'GRE Tunnel' is unchecked. Under the 'Gateways, Sub-Locations and Endpoints' section, the following options are checked: 'Use XXF from Client Request', 'Enforce Firewall Control', 'Enforce IPS Control', 'Enforce Authentication', and 'Enable IP Surrogate'. The 'Idle time to disassociation' is set to 'Minutes' with a value of 1-43200. The 'Enforce Surrogate IP for Known Browsers' option is also checked, with a 'Refresh time for re-validation of Surrogacy' set to 'Minutes' with a value of 1-43200. The 'Optional' button is visible in the top right corner of the section. At the bottom right, there are 'Cancel' and 'Next →' buttons.

- To configure different gateway option settings for different sources of traffic from this site, define sub-locations by entering the sub-location name and IP address under the **Sub-Locations** tab.

The screenshot shows the 'Connect to ZScaler' dialog box with the 'Sub-Locations' tab selected. The 'IPSec Tunnel' option is checked, and 'GRE Tunnel' is unchecked. Under the 'Gateways, Sub-Locations and Endpoints' section, the 'Sub-Locations' tab is active. The 'Add Sub-Location' section contains a 'Sub-Location Name' field and an 'IP Address' field. A note below the IP Address field states: 'Each entry is either a single IP addr, CIDR or Range (eg: 10.10.33.0/24) or range (eg: 10.10.33.1 - 10.10.33.10)'. There is an 'Add IP Address' button at the bottom. The 'Optional' button is visible in the top right corner of the section. On the left side, there are steps: 'Step 1 Tunnels & Gateways' and 'Step 2 Circuits'. A 'Pre-requisites' link is also visible. At the bottom right, there are 'Cancel' and 'Next →' buttons.



You can enter multiple IP addresses for the sub-location. Each sub-location entry can be a single IP address, CIDR, or range.

Adding the first sub-location automatically creates a new sub-location called **Other**. All existing policy rules that reference the parent location will now apply to the other location. You must manually configure rules for traffic from this sub-location.

You can enable the following options in Gateways or Sub-Locations to customize configurations.

Gateway Option	Description
Enable XFF from Client Request	Use this option if the location employs proxy chaining to forward traffic to the service and you want Zscaler to utilize X-Forwarded-For (XFF) headers inserted by your on-premise proxy. When forwarding traffic to its destination, Zscaler removes the original XFF header and replaces it with the IP address of the client gateway (public IP) to prevent exposure of internal IP addresses.
Enforce Firewall Control	Activates the firewall at the specified location.
Enforce IPS Control	Enables user-to-device mapping when an internal IP can be differentiated from a public IP. This ensures user policies apply to cookie-incompatible traffic.

Gateway Option	Description
Enforce Authentication	Requires identification of individual user traffic using the configured authentication mechanism.
Enforce Caution	Enforces a caution policy action by displaying an end-user notification for unauthenticated traffic. If disabled, the action is treated as Allow .
Enforce AUP(Acceptable Use Policy)	Displays an Acceptable Use Policy (AUP) for unauthenticated traffic and requires users to accept it.
Enforce IP Surrogate	Enables user-to-device mapping for enforcing user policies when an internal IP can be distinguished from a public IP. This is essential for cookie-incompatible traffic.
Idle Time to Disassociation	If IP Surrogate is enabled, specifies the duration after a completed transaction before the service removes the IP-to-user mapping.
Enforce Surrogate IP for Known Browsers	If enabled, surrogate user identity is used for traffic from known browsers if an IP-user mapping exists. If disabled, traffic from known browsers will always be authenticated using the configured authentication mechanism.
Surrogate Identity Refresh Interval	Defines how long a surrogate user identity can be used before requiring revalidation via authentication. The refresh interval must be shorter than the DHCP lease time to prevent incorrect user policies from being applied.
Custom AUP Frequency	Specifies, in days, how often the Acceptable Use Policy is displayed to users.

Gateway Option	Description
Block Internet Access	Disables all internet access, including non-HTTP traffic, until the user accepts the Acceptable Use Policy.



By default, any changes to the IPSec and GRE configurations apply automatically to both the gateway and sub-locations.

- Specify the **Endpoints** from the drop-down if you need to use **Custom VPN Endpoints** for IPsec tunnels and GRE tunnels (primary and secondary) instead of those managed by the CloudBlade.

If using a custom endpoint, enter the preconfigured Standard VPN Endpoint name (case-sensitive) to be referenced when the CloudBlade configures the Standard VPN interfaces at this site. If no endpoint is specified, the CloudBlade will default to using the ZScaler Standard VPN endpoint, which includes a list of all ZEN node hostnames.

Gateways, Sub-Locations and Endpoints

Optional

Gateway

Sub-Locations

Endpoints

Endpoints

Specify the endpoint if there's a requirement to use a custom Standard VPN endpoint instead of the one, which the cloudblade manages and maintains.

Custom VPN Endpoints

IPSec Tunnel

Custom VPN Endpoint Name (optional)

Select a VPN Endpoint Name

☐ Allow interface level override

GRE Tunnel

Custom GRE Primary VPN Endpoint Name (optional)

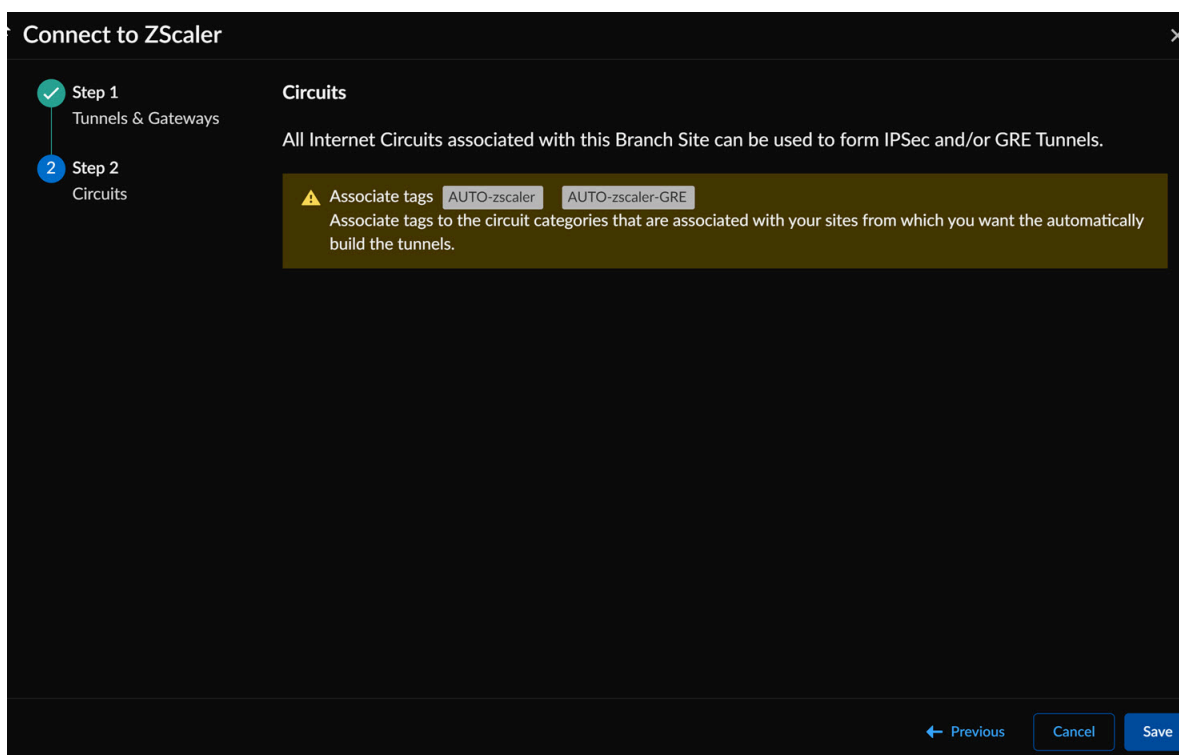
Select GRE Primary VPN Endpoint Name

Custom GRE Secondary VPN Endpoint Name (optional)

Select GRE Secondary VPN Endpoint Name

☐ Allow interface level override

If required, enable **Interface level override** for further customization.

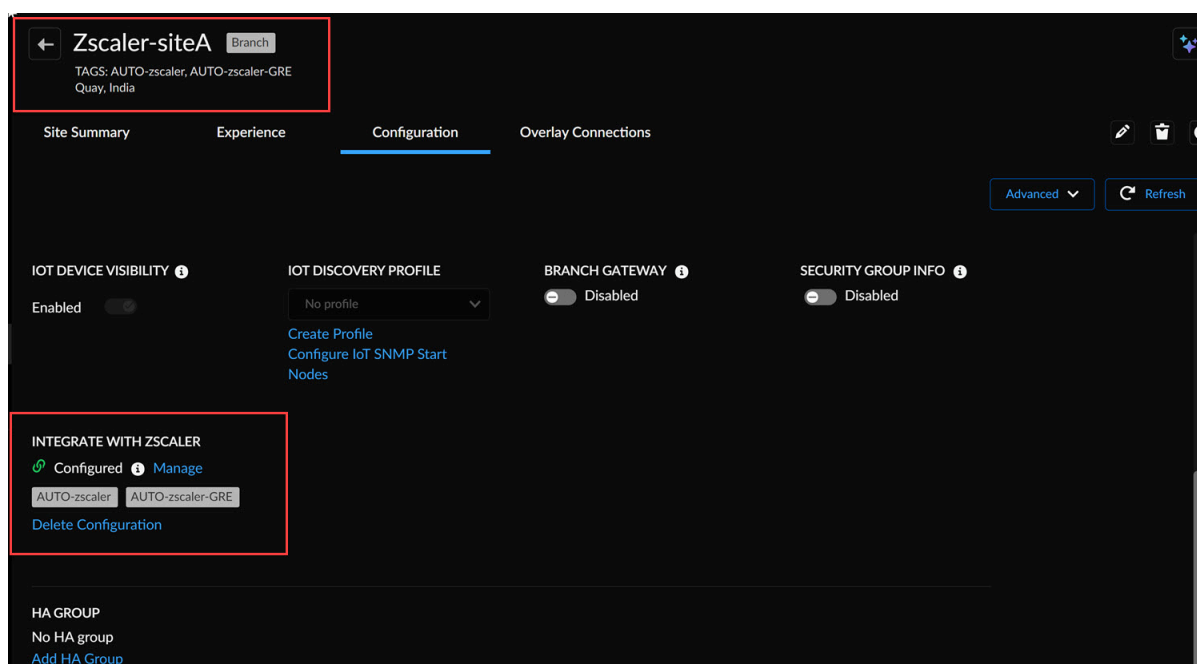
STEP 8 | Tag the circuit categories.

The 'Connect to ZScaler' dialog box shows a two-step process. Step 1, 'Tunnels & Gateways', is completed. Step 2, 'Circuits', is the current step. It contains a warning message: 'Associate tags AUTO-zscaler AUTO-zscaler-GRE. Associate tags to the circuit categories that are associated with your sites from which you want the automatically build the tunnels.' The dialog has 'Previous', 'Cancel', and 'Save' buttons at the bottom right.

Once the site is enabled for Zscaler, all Internet Circuits associated with this Branch Site can be used to form IPSec and/or GRE Tunnels. The IPSec and GRE configurations will be associated with the circuit categories to allow automatic tunnel formation.



You can validate the tunnel configuration by navigating to the Branch Site and confirming if the tags are configured correctly.



The 'Zscaler-siteA' configuration page shows the 'Configuration' tab selected. The page includes sections for 'IOT DEVICE VISIBILITY' (Enabled), 'IOT DISCOVERY PROFILE' (No profile), 'BRANCH GATEWAY' (Disabled), and 'SECURITY GROUP INFO' (Disabled). A red box highlights the 'INTEGRATE WITH ZSCALER' section, which shows 'Configured' status, 'Manage' button, and tags 'AUTO-zscaler' and 'AUTO-zscaler-GRE'. Below this is a 'Delete Configuration' link. Another red box highlights the site name and tags at the top left. The page also has 'Advanced' and 'Refresh' buttons at the top right.



- Select **Delete Configuration** (if required), and select the tunnel type (IPSec or GRE) to remove the Zscaler configuration from the branch site.
- Select **Manage** to edit any of the existing IPSec and GRE configurations.

Tag the Circuit Categories

Now that the site has been tagged as enabled for Zscaler, we need to tag the circuit categories that can be used to establish a Standard VPN or GRE tunnel to Zscaler.



This capability is useful if you want only specific types of circuits to be used for Zscaler integration or explicitly exclude certain circuit types. For example, a customer may not want to use their metered LTE circuit for Standard VPN establishment.

STEP 1 | In **Strata Cloud Manager**, go to **Manage > Resources > Circuit Categories**.

STEP 2 | Find the circuit categories that are associated with your sites from which you want the system to automatically build the tunnels. Edit the circuit category, and enter **AUTO-zscaler** and **AUTO-zscaler-GRE** (case sensitive) in the **Tags** field.

Edit Circuit Category "Ethernet Internet"

public-7

NAME

LABEL

Ethernet Internet

public-7

DESCRIPTION (optional)

General Internet connection with an Ethernet hand-off.

256 character limit

TAGS (optional)

AUTO-zscaler-GRE x

AUTO-zscaler x

4 tags max

☐ USE FOR CONTROLLER CONNECTIONS

☐ USE FOR APPLICATION REACHABILITY PROBES

☐ QOS

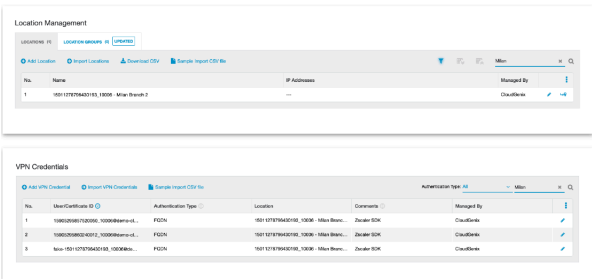
STEP 3 | Select **Update**.

Once this configuration is completed, Standard VPN IPsec/GRE tunnels connecting the Prisma SD-WAN ION device and Zscaler will begin the creation or onboarding process in the next integration cycle. It may take several integration cycles for the tunnels to appear and be active on the Prisma SD-WAN portal.

Validate the Zscaler Configuration

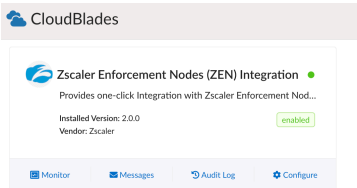
Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ Zscaler Enforcement Nodes (ZEN) Integration CloudBlade

The Zscaler CloudBlade will provision locations and unique VPN credentials per tunnel within Zscaler. Below is a sample output of the deployment for the Milan Branch 2 site from the Zscaler portal. This site has two circuits. Note that there is a third fake VPN credential which is never used, but is part of the initial location creation and onboarding process.



The status of the deployment and tunnels can be validated on the CloudBlades page as follows:

STEP 1 | On the **CloudBlades** screen, click **Monitor**.



STEP 2 | Select the **Stats** tab to see information on the Zscaler sites and status of the IPsec and GRE tunnels.

Monitoring

Stats	Summary	Details	Refresh Columns						
TOTAL ZSCALER SITES	SUCCESSFULLY DEPLOYED SITES	FAILED SITES	TOTAL 3RD PARTY VPNS	TOTAL IPSEC TUNNELS	IPSEC TUNNELS UP	IPSEC TUNNELS DOWN	TOTAL GRE TUNNELS	GRE TUNNELS UP	GRE TUNNELS DOWN
1	1	-	3	1	-	1	2	-	2

STEP 3 | Select the **Summary** tab to see an overview of all the connected sites, ZEN node endpoints, and name of the third-party endpoints.

Monitoring

StatsSummaryDetails

RefreshColumns

Site Name	Device Name	Circuit Name	Status	Zen Node Hostname & IP	3rd Party Endpoint Name	Creation Date	Last Updated
Chennai	T1S3_SPOKE1	eQA22760	up	maa2-vpn.zscalerthree.net 165.225.122.38	ZScaler	Sep 12, 2022 06:03:57pm	Sep 12, 2022 06:07:01pm
Chennai	T1S3_SPOKE1	eQA22760	down	165.225.120.33	Zscaler GRE Backup	Sep 12, 2022 06:04:28pm	Sep 12, 2022 06:06:30pm
Chennai	T1S3_SPOKE1	eQA22760	down	165.225.106.44	Zscaler GRE Primary	Sep 12, 2022 06:04:28pm	Sep 12, 2022 06:06:30pm

STEP 4 | Select the **Details** tab to view the deployment status and the configuration details. These details are helpful for troubleshooting.

Monitoring

StatsSummaryDetails

RefreshColumns

Site Name	Device Name	Circuit Name	3RD PARTY INTERFACE NAME	PARENT INTERFACE NAME	Deployment Status	Location Name	VPN Credential/IP
Chennai	T1S3_SPOKE1	eQA22760	sl-zscaler-16279671606970106	2	Success	16387995658550230_2760 - Chennai	1662986037514014296
Chennai	T1S3_SPOKE1	eQA22760	sl-zscaler-gre-backup-16279671606970106	2	Success	16387995658550230_2760 - Chennai	223.30.70.247
Chennai	T1S3_SPOKE1	eQA22760	sl-zscaler-gre-primary-16279671606970106	2	Success	16387995658550230_2760 - Chennai	223.30.70.247

Edit Application Network Policy Rules

Once the CloudBlade configures the appropriate Standard VPN objects within Prisma SD-WAN and Zscaler, the administrator can reference the path (Standard VPN) and service group (Zscaler) within application network policies. The ION devices will make intelligent per-app path selections using the network policies to chain multiple path options together in Active-Active and Active-Backup modes.

Example:

- Application A: Take **Standard VPN** direct to Zscaler.
- Application B: Take **Standard VPN** direct to Zscaler; Backup to **Direct Internet**.
- Application C: Go to Internet through Prisma SD-WAN; Backup to Standard VPN direct to Zscaler.
- Application D: Use only **Direct Internet**.

The Prisma SD-WAN Secure Application Fabric (AppFabric) enables granular controls for virtually unlimited number of policy permutations down to the sub-application level. Here are some of the most common examples of how traffic policy can be configured per application:

- Send all internet-bound traffic from a set of branches to a Zscaler datacenter. (Blanket Greylist)
- Send all internet-bound traffic from a set of branches to a Zscaler datacenter with the exception of specific known applications. (Greylist-Whitelist)
- Send all internet traffic direct to the internet except for certain applications needing additional inspection or security. (Whitelist-Greylist)

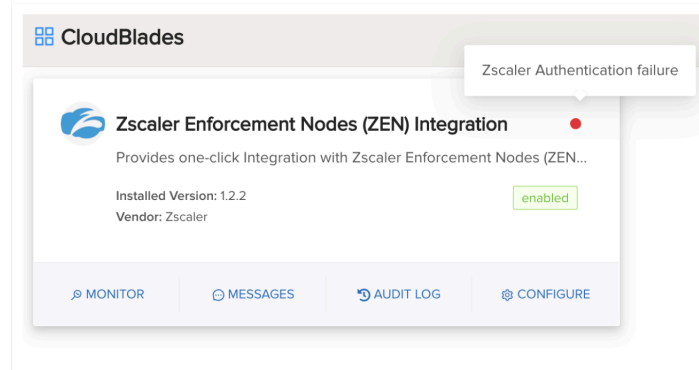
Troubleshoot Installation Scenarios

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Strata Cloud Manager 	<ul style="list-style-type: none"> Prisma SD-WAN license Zscaler Enforcement Nodes (ZEN) Integration CloudBlade

A few common scenarios administrators should be aware of when attempting to do the initial installation of the Zscaler CloudBlade.

Wrong API Key or Partner Admin Credentials

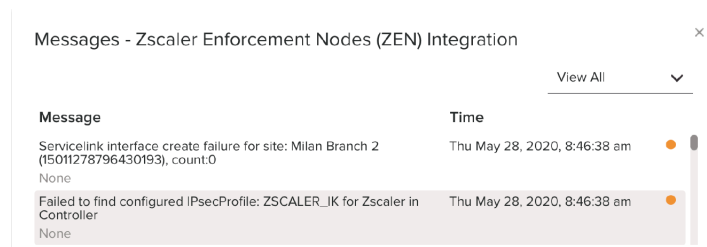
If an administrator incorrectly enters the API key or Partner Admin credentials, the system will alert the administrator by reporting the status on the CloudBlade page.



Prisma SD-WAN Standard VPNs not Created

There could be a scenario in which all user credentials, keys, and tokens are correct, and the Zscaler Location and VPN credential objects are also created. However, the Prisma SD-WAN VPNs are not created. This can be due to the pre-built IPsec profiles based on Zscaler's recommended best practices, which have not been allocated to your Prisma SD-WAN tenant. Another reason could be that the custom IPsec profile name specified in your CloudBlade configuration does not exist (or has a typo in it).

This condition can be validated by selecting the **Messages** link on the CloudBlade tile and looking for an error message similar to the one below.



To verify that these IPsec profiles exist, in **Strata Cloud manager**, navigate to **Manage > Prisma SD-WAN > Resources > Configuration Profiles > IPsec**, and check if the profiles shown in the example below are displayed. If these two profiles are not present, please contact Palo Alto support **OR** create your own IPsec profile in that name in your CloudBlade configuration.

Troubleshoot Standard VPNs

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Strata Cloud Manager	<ul style="list-style-type: none">❑ Prisma SD-WAN license❑ Zscaler Enforcement Nodes (ZEN) Integration CloudBlade

Start with the Zscaler Test Page to verify and troubleshoot client traffic to and through Zscaler Enforcement Nodes (ZENs). All application and path metrics will also be collected and reported, and all application monitoring alarms and alerts will be generated for Standard VPNs. To troubleshoot Standard VPNs, view Alerts and Alarms, Connectivity of Standard VPNs at the site level, and Activity charts to view possible issues with the VPN. In addition, device toolkit commands can be used to view Standard VPN stats, status, and summary.

Use the Zscaler Test Page

Zscaler provides a diagnostic page that allows for verification and troubleshooting of client traffic to and through Zscaler ZENs. To access the page from any client, open the link <http://ip.zscaler.com>.

For more details on this tool, refer to the Zscaler Knowledgebase article, [How can I check if a user's traffic is going to Zscaler?](#).

View Standard VPN at Site Level

To view the interface status at the site level, go to **Workflows > Prisma SD-WAN Setup > Branch Sites**.

Select a site, and under **Overlay Connections**, click **Standard VPN** to view the status of the Standard VPN.

View Alerts and Alarms

If a Standard VPN tunnel interface is down, an alarm will be raised, just like it would for any other interface within the system.

View Activity Charts

All activity charts can be filtered based on paths, including Standard VPNs.

In **Strata Cloud manager**, go to **Monitor > Branch Sites > Prisma SD-WAN**.

In the **Activity** tab, under **WAN**, select **Standard VPN**, use the filters to select the site connectivity, and time range to see the specific analytics for that path.

Zscaler Location Gateway Options

CloudBlade version 1.2.2 supports the following gateway options:

Options	Corresponding Prisma Access for NetworksTag
Use XFF from Client Request	Gateway Options: <True False>Sub Locations: Disabled
Enforce Zscaler App SSL Setting	Deprecated
Enable SSL Inspection	Deprecated
Enforce Firewall Control	<True False>
Enforce Authentication	<True False>
Enable IP Surrogate	<True False>Idle time: <val>Idle time metric: <minutes hours days>
Enable Surrogate IP for KnownBrowsers	<True False>Refresh time: <val>Refresh time metric: <minutes hours days>
Enable Caution	<True False>
Enable AUP	<True False>Frequency (days): <val>Block Internet Access: <True False>Force SSL Inspection: <True False>

Enable, Pause, Disable, and Uninstall the CloudBlade

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Prisma SD-WAN	<ul style="list-style-type: none">❑ Zscaler Enforcement Nodes (ZEN) Integration CloudBlade

After the CloudBlade is set up, operations can be done using the CloudBlade panel. These operations have various effects on the tunnels and configurations in Prisma SD-WAN and Zscaler.

- **Set the CloudBlade to Enabled**

Enabled is the standard expected mode of operation for the CloudBlade. The CloudBlade will run every 60 seconds, find any new Sites or Circuits with the appropriate tags, and configure the integration on Zscaler and Prisma SD-WAN. In addition, during this integration run, if any settings were previously modified manually on either Prisma SD-WAN or Zscaler (for example VPN credentials changed, or Location deleted in Zscaler), these will be reverted to the known good state automatically.

- **Set the CloudBlade to Paused**

Pausing the CloudBlade stops all future integration runs, but leaves any created objects intact. This stops any future objects from getting created but does NOT prevent removal of any unconfigured/untagged objects on either Prisma SD-WAN or Zscaler.

- **Set the CloudBlade to Disabled**

Disabling the CloudBlade tells the system to remove and delete all configurations created by the CloudBlade. This can cause communication interruptions if the policy isn't set to use other paths. The IPSec policies, IKE policies, and Prisma SD-WAN Endpoints and Service and DC groups aren't automatically deleted and must be removed manually.

- **Uninstalling the CloudBlade**

Uninstalling the CloudBlade removes the configuration for the CloudBlade, and immediately stops any changes by the CloudBlade. Uninstalling the CloudBlade doesn't automatically remove configuration from all sites and objects. The CloudBlade may be uninstalled and reinstalled to facilitate upgrades or downgrades to different versions without traffic interruption. To completely remove all items, set the CloudBlade to Disabled for 2-3 integration run periods (180 seconds) before uninstalling the CloudBlade.

