

Configure IPsec VPN Profiles



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

For staging and post-staging servers, you configure IPsec VPN profiles to define the properties of the IPsec and IKE tunnels between tenants (organizations) and SD-WAN network devices. For IKE, these properties include how often to regenerate the IKE key (rekey timer), the encryption transformations, and authentication and certificate information. For IPsec, these properties include the anti-replay detection, how often to regenerate the IPsec key (rekey timer), and the encryption transformations.

For a provider tenant, you configure a staging IPsec VPN profile for the IPsec/IKE tunnel that the tenant uses to communicate with the staging server. In a multitenant topology, the staging server IPsec VPN profile is associated with the parent organization.

For a provider or customer tenant, you configure a post-staging IPsec VPN profile for the IPsec/IKE tunnel that the tenant branch uses to connect, through a Controller node, with a Director node. The Director node uses this connection to deploy templates to the branch.

This article describes how configure VPN profiles for IPsec to use for staging and post-staging, to enable communication with the staging and post-staging servers.

In the configuration of IKE tunnels, you can configure preshared key (PSK) authentication for the tunnel. The PSK can contain letters, numbers, and some special characters. The following table list the special characters that are and are not allowed in the PSK.

Special Character	Description	Allowed in PSK
"	Quotation mark	No
>	Close angle bracket (greater-than sign)	No
<	Open angle bracket (less-than sign)	No
#	Hash (pound) sign (octothorpe)	No
\	Backslash	No
{	Open brace	No


Special Character	Description	Allowed in PSK
}	Close brace	No
~	Tilde	Yes
!	Exclamation point (bang)	Yes
\$	Dollar sign	Yes
%	Percent sign	Yes
^	Circumflex (caret)	Yes
&	Ampersand (and sign)	Yes
*	Asterisk (star)	Yes
(Open parenthesis	Yes
)	Close parenthesis	Yes
_	Underscore	Yes
+	Plus sign	Yes
[Open bracket	Yes
]	Close bracket	Yes
	Vertical bar (pipe)	Yes
:	Colon	Yes
;	Semicolon	Yes
?	Question mark	Yes
`	Accent grave (backward tick)	Yes
'	Apostrophe (single quotation mark)	Yes
-	Hyphen (dash)	Yes
=	Equal sign	Yes
,	Comma	Yes
.	Period	Yes

Special Character	Description	Allowed in PSK
/	Forward slash	Yes
@	At sign	Yes

When you change the IKE and IPsec configuration parameters or when you renew or change a certificate, the changes are effective immediately, and the result is that the affected IPsec/IKE tunnel is torn down (that is, the tunnel flaps). For Releases 22.1.3 and later, when you renew or change certificates or when you change a few of the IKE and IPsec parameters, the change is delayed. For the following parameters, the changes take effect only after the IPsec/IKE security association (SA) negotiation or rekeying completes:

- IKE rekey time
- IKE dead-peer detection (DPD) timeout
- IKE fragmentation
- IPsec anti-replay
- IPsec fragmentation
- IPsec rekey time
- IPsec rekey volume
- IPsec keepalive timeout

To configure an IPsec VPN profile:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
 - d. Select an organization (tenant).
2. Select the Configuration tab in the top menu bar.
3. Select Services  > IPsec > VPN Profiles in the left menu bar. The main pane displays the organizations associated with the Controller node.

VERSA NETWORKS

Director View | **Appliance View** | Template View | Controller-1

Administrator

Monitor | Analytics | **Configuration** | Administration

Versa

You are currently in Appliance View

Build

Networking | Services | Objects & Connectors | Others

> ADC

> Next Gen Firewall

> IPsec

VPN Profiles

Branch SDWAN Profile

> SDWAN

> Layer 2 SDWAN

Web Proxy

Captive Portal

Search

+ Add Delete Clone

VPN PROFILE	VPN TYPE	LOCAL IP/INTERFACE/H	PEER IP/FQDN/HOSTNA	LOCAL AUTH INFO		
				AUTH TYPE	AUTH INFO	AU
<input type="checkbox"/> Versa-PostStaging	controller-sdwan	vti-0/2.0		psk	id-type = email key = zSs/UU2Zgm... id-string = Controll...	psk
<input type="checkbox"/> WAN-0009-Contro...	controller-staging-s...	vni-0/1.0		psk	id-type = email key = zSs/UU2Zgm... id-string = Controll...	psk

Rows per page 25 Showing 1 - 2 of 2

4. Click the **+** Add icon. The Add IPsec VPN popup window displays. Select the upper General tab, and then enter information for the following field.

Add IPsec VPN

General | IKE | IPsec

VPN Profile Name *

Controller-1-Profile

General | Local and Peer | Address Pool

VPN Type *

Branch SDWAN

Tunnel Initiate

Automatic

Alarms

☒ IKE Auth Failure

☒ IKE State Change

☒ IPsec State Change

Hardware Accelerator

--Select--

Branch SDWAN Profile

b2b-sdwan

☒ Route Based ☐ Policy Based

LEF Profile

--Select--

☐ Default Profile

Tunnel Routing Instance

Versa-Control-VR

Tunnel Interface *

ptvi513

Tunnel Payload Family

--Select--

OK Cancel

Field	Description
VPN Profile Name	Enter a name for the VPN profile.

5. Select the General tab below the VPN Profile Name field, and enter information for the following fields.

Field	Description
VPN Type	<p>Select a VPN type:</p> <ul style="list-style-type: none"> ◦ Branch SD-WAN—Select for a post-staging IPsec VPN profile for a branch. ◦ Branch Staging SD-WAN—Select for a staging IPsec VPN profile for a branch. ◦ Controller SD-WAN—Select for a post-staging IPsec VPN profile for a Controller node. ◦ Controller Staging SD-WAN—Select for a staging IPsec VPN profile for a Controller node. ◦ Remote Access Client ◦ Remote Access Server—Currently, this option is not supported. ◦ Site to Site
Tunnel Initiate	<p>Select how to initiate creation of the child SA:</p> <ul style="list-style-type: none"> ◦ Automatic—Initiate automatically. ◦ Responder Only—(For Releases 21.2.1 and later.) Initiate for responder. ◦ Traffic—Initiate when traffic is seen.
Alarms (Group of Fields)	
◦ IKE Authentication Failure	Click to generate an alarm when IKE authentication fails.
◦ IKE State Change	Click to generate an alarm when the IKE state changes.
◦ IPsec State Change	Click to generate an alarm when the IPsec state changes.
Hardware Accelerator	<p>Select the hardware accelerator to use:</p> <ul style="list-style-type: none"> ◦ Any ◦ Nitrox ◦ None ◦ QAT
Branch SD-WAN Profile	For a Branch SD-WAN VPN type, select the branch SD-WAN profile to associate with the VPN. For more

	information, see Configure a Branch SD-WAN Profile .
Route Based	Click to select a VPN through which traffic is tunneled by performing a route lookup for a route that points to a tunnel interface.
◦ LEF Profile	Select a LEF profile to use for logging. Note that this field is not displayed if you select Remote Access Type in the VPN Type field.
◦ Default Profile	Click to use the default LEF profile for logging. Note that this field is disabled if you select a profile in the LEF Profile field.
◦ RAS ID	For the VPN type Remote Access Server, enter the name identifier of the remote access server to associate with the VPN profile. Currently, this option is not supported.
◦ Tunnel Routing Instance	Select the tunnel routing instance to use to reach the staging server.
◦ Tunnel Interface	Select the tunnel interface to use to reach the staging server.
◦ Tunnel Payload Family	(For Releases 22.1.1 and later.) Select the tunnel payload family: <ul style="list-style-type: none"> ◦ IPv4 family ◦ IPv6 family ◦ IPv4 and IPv6 family
Policy Based	Click to select a VPN through which traffic is tunneled based on rules or policies negotiated with the peer.

6. Select the Local and Peer tab, and enter information for the following fields.

Add IPsec VPN

General

IKE

IPsec

VPN Profile Name *

mgnt

General

Local and Peer

Address Pool

Routing Instance *

--Select--

Peer

Peer FQDN

+

Peer FQDN Not Configured

Peer IP

+

Peer IP Not Configured

Peer Hostname

Local

Local IP

Local Interface

--Select--

Hostname

Interface List

INTERFACE LIST

+

Interface List Not Configured

OK



Cancel

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_IPsec...

Updated: Wed, 23 Oct 2024 08:24:41 GMT

Copyright © 2024, Versa Networks, Inc.

8

Field	Description
Routing Instance	Select the routing instance routing instance through which IPsec peer is reachable.
Peer (Group of Fields)	Select one of the options to specify peer FQDN, IP address, or hostname.
◦ Peer FQDN	Click to enter the peer FQDN by clicking the  Add icon.
◦ Peer IP	Click to enter the peer IP address by clicking the  Add icon.
◦ Peer Hostname	Click to enter the peer hostname.
Local (Group of Fields)	Select one of the options to specify local IP address, interface, or hostname.
◦ Local IP	Click to enter the local IP address.
◦ Local Interface	Click to select a local interface from the drop-down list.
◦ Hostname	Click to enter the local hostname.
◦ Interface List	Currently, this option is not supported.

7. Select the Address Pool tab, and enter information for the following fields.

GeneralIKEIPsec

VPN Profile Name *

GeneralLocal and PeerAddress Pool

Address From *

⚙

Address To *

⚙

Mask *

⚙

IPAM Address

--Select--

ACCESSIBLE SUBNETS *

+

🗑

Accessible Subnets Not Configured

Server Name

⚙

30

NAMESERVER IPV4/IPV6 ADDRESSES *

+

🗑

Nameserver IPv4/IPv6 Addresses Not Configured

DOMAIN NAMES *

+

🗑

Domain Names Not Configured

OK




Cancel

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_IPsec...

Updated: Wed, 23 Oct 2024 08:24:41 GMT

Copyright © 2024, Versa Networks, Inc.

10

Field	Description
Address From	Enter the lowest IPv4 or IPv6 address in the address pool.
Address To	Enter the highest IPv4 or IPv6 address in the address pool.
Mask	Enter the subnet mask for the tunnel IP address range, for example, 255.255.255.0.
IPAM Address	(For Releases 22.1.3 and later.) Select the IP address of an IP address management (IPAM) service.
Accessible Subnets	Click the  Add icon, and enter the IPv4 or IPv6 addresses and subnets masks for the accessible subnets. Authenticated remote users can access the subnets specified in this address range.
DNS (Group of Fields)	(For Releases 22.1.3 and later.)
◦ Server Name	Enter the name of the DNS server.
◦ Name Server IPv4/IPv6 Addresses	Click the  Add icon, and then enter the IPv4 or IPv6 addresses of the DNS name servers. You can configure up to two DNS server IP addresses. These addresses are sent to remote access clients (RACs) during IKE negotiation for address resolution of the domain names.
◦ Domain Names	Click the  Add icon and enter the domain name of the DNS name server.

8. Select the IKE tab, and enter information for the following fields.

Add IPsec VPN
✕

General
IKE
IPsec

Version
v2

Fragment Size
576

DPD Timeout
30

Auth Domain

Revocation Check
None

Rekey Time
Seconds
28800

Transform & DH Group

Multiple Transforms
Single Transform

HASH ALGORITHM
+

ENCRYPTION ALGORITHM
+

DH GROUP
+

Local Auth

Authentication Type *
Certificate

Certificate Domain
Tenant

Certificate Name *
--Select--

CA Chain *
--Select--


Provider Org
--Select--



Peer Auth

Authentication Type *
Certificate

CA Chain *

OK
Cancel

Field	Description
Version	Select v2.
Fragment Size	<p>(For Releases 22.1.1 and later.) Enter the maximum frame size for an IKE packet. Packets larger than this size are fragmented, and as a result they might be dropped.</p> <p><i>Range:</i> 576 through 1280 bytes</p> <p><i>Default:</i> 576 bytes</p>
DPD Timeout	<p>Enter how long to wait for traffic from the destination peer on the tunnel before sending a dead-peer-detection (DPD) request packet.</p> <p><i>Range:</i> 10 through 180 seconds</p> <p><i>Default:</i> 30 seconds</p>
Authentication Domain	Enter the name of the authentication domain.
Revocation Check	<p>Select the method to use to check for revoked certificates:</p> <ul style="list-style-type: none"> ◦ None—Do not check for revoked certificates. ◦ OSCP—Use the Online Certificate Status Protocol.
Rekey Time	<p>Enter how often to regenerate the IKE key.</p> <p><i>Range:</i> 3600 through 28800 seconds (1 through 8 hours)</p> <p><i>Default:</i> 28800 seconds</p>
Transform & DH Group (Group of Fields)	
◦ Multiple Transforms	Click to specify hash algorithms, encryption algorithms, and Diffie-Hellman groups.
◦ Hash Algorithm	Click the  Add icon, and select the hash algorithms to use:

	<ul style="list-style-type: none"> ◦ MD5—MD5 Message Digest Algorithm ◦ SHA-1—Secure Hash Algorithm 1 with 160-bit digest. This is the default. ◦ SHA-256—Secure Hash Algorithm 2 with 256-bit digest ◦ SHA-384—Secure Hash Algorithm 2 with 384-bit digest ◦ SHA-512—Secure Hash Algorithm 2 with 512-bit digest <p><i>Default:</i> SHA-1</p>
<ul style="list-style-type: none"> ◦ Encryption Algorithm 	<p>Click the  Add icon, and select the encryption algorithms to use:</p> <ul style="list-style-type: none"> ◦ 3DES—Triple DES encryption algorithm ◦ AES 128—AES CBC Encryption Algorithm This is the default. ◦ AES 128-GCM—(For Releases 22.1.1 and later.) AES Encryption Algorithm with 128-bit key. This algorithm is supported for IKEv2 only. ◦ AES 256—AES CBC Encryption Algorithm with 256-bit key ◦ AES 256-GCM—(For Releases 22.1.1 and later.) AES Encryption Algorithm with 256-bit key. This algorithm is supported for IKEv2 only. <p><i>Default:</i> AES 128</p>
<ul style="list-style-type: none"> ◦ DH Group 	<p>Click the  Add icon, and select the Diffie-Hellman groups to use. Select the Diffie-Hellman group to use:</p> <ul style="list-style-type: none"> ◦ Diffie-Hellman Group 1—768-bit modulus ◦ Diffie-Hellman Group 2—1024-bit modulus. This is the default. ◦ Diffie-Hellman Group 5—1536-bit modulus ◦ Diffie-Hellman Group 14—2048-bit modulus ◦ Diffie-Hellman Group 15—3072-bit modulus ◦ Diffie-Hellman Group 16—4096-bit modulus ◦ Diffie-Hellman Group 19—256-bit elliptic curve ◦ Diffie-Hellman Group 20—384-bit elliptic curve ◦ Diffie-Hellman Group 21—521-bit elliptic curve

	<ul style="list-style-type: none"> ◦ Diffie-Hellman Group 25—192-bit elliptic curve ◦ Diffie-Hellman Group 26—224-bit elliptic curve <p>No PFS</p> <p><i>Default:</i> Diffie-Hellman Group 2—1024-bit modulus</p>
◦ Single Transform	Click to specify the transform and Diffie-Hellman group.
◦ Transform	<p>Select the transform type to use:</p> <ul style="list-style-type: none"> ◦ 3DES encryption and MD5 hashing ◦ 3DES encryption and SHA-1 hashing ◦ AES 128-bit encryption and MD5 hashing ◦ AES 128-bit encryption and SHA-1 hashing ◦ AES 128-bit encryption and SHA-256 hashing ◦ AES 128-bit encryption and SHA-384 hashing ◦ AES 128-bit encryption and SHA-512 hashing ◦ AES 256-bit encryption and MD5 hashing ◦ AES 256-bit encryption and SHA-1 hashing ◦ AES 256-bit encryption and SHA-256 hashing ◦ AES 256-bit encryption and SHA-384 hashing ◦ AES 256-bit encryption and SHA-512 hashing
◦ DH Group	<p>Select the Diffie-Hellman group to use:</p> <ul style="list-style-type: none"> ◦ Diffie-Hellman Group 1—768-bit modulus ◦ Diffie-Hellman Group 2—1024-bit modulus ◦ Diffie-Hellman Group 5—1536-bit modulus ◦ Diffie-Hellman Group 14—2048-bit modulus ◦ Diffie-Hellman Group 15—3072-bit modulus ◦ Diffie-Hellman Group 16—4096-bit modulus ◦ Diffie-Hellman Group 19—256-bit elliptic curve ◦ Diffie-Hellman Group 20—384-bit elliptic curve ◦ Diffie-Hellman Group 21—521-bit elliptic curve ◦ Diffie-Hellman Group 25—192-bit elliptic curve ◦ Diffie-Hellman Group 26—224-bit elliptic curve ◦ No PFS

Local Authentication (Group of Fields)	Select the local authentication type.
<ul style="list-style-type: none"> ◦ Certificate 	<div data-bbox="863 319 1624 537"> <p>Local Auth</p> <p>Authentication Type * Certificate Domain Certificate Name * CA Chain *</p> <p>Provider Org Identity Type</p> </div> <p>Use certificate authentication. This is the default authentication type. Enter information for the following fields:</p> <ul style="list-style-type: none"> ◦ Certificate Domain—Select the domain to which the certificate applies: <ul style="list-style-type: none"> ▪ System ▪ Tenant ◦ Certificate Name (Required)—Select the certificate name. ◦ CA Chain (Required)—Select the CA chain. ◦ Provider Organization—Select the name of the provider organization. ◦ Identity Type—Select the type of identity to use for authentication: <ul style="list-style-type: none"> ▪ Email ▪ FQDN (default) ▪ IP ◦ Identity—If you select a value in the Identity Type field, enter the email address, FQDN, or IP address.
<ul style="list-style-type: none"> ◦ PSK 	<div data-bbox="863 1488 1624 1633"> <p>Local Auth</p> <p>Authentication Type * Shared Key * Identity Type * Identity *</p> </div> <p>Use a preshared key for authentication. Enter information for the following fields:</p> <ul style="list-style-type: none"> ◦ Shared Key—Enter the preshared key (PSK) to

	<p>use to create a tunnel. The PSK cannot include any of the following five special characters: " < > # /.</p> <ul style="list-style-type: none"> ◦ Identity Type—Select the type of identity to use for authentication: <ul style="list-style-type: none"> ▪ Email ▪ FQDN (default) ▪ IP ◦ Identity—Enter the email address, FQDN, or IP address. 				
Peer Authentication (Group of Fields)	Select the authentication type for the peer.				
<ul style="list-style-type: none"> ◦ Certificate 	<div> <div> <div>Peer Auth</div> <div>Authentication Type *</div> <div>Certificate ▾</div> </div> <div> <div>Certificate Authentication Clients</div> <div>▽</div> <table> <tr> <td>Identity Type * ▾</td> <td>Identity *</td> </tr> <tr> <td>IP ▾</td> <td></td> </tr> </table> <div>No Certificate Authentication Client</div> </div> </div> <p>Use certificate authentication. This is the default authentication type. Enter information for the following fields:</p> <ul style="list-style-type: none"> ◦ Identity Type (Required)—Select the type of identity to use for authentication: <ul style="list-style-type: none"> ▪ Email ▪ FQDN (default) ▪ IP ◦ Identity (Required)—Enter the email address, FQDN, or IP address. 	Identity Type * ▾	Identity *	IP ▾	
Identity Type * ▾	Identity *				
IP ▾					

<ul style="list-style-type: none"> ◦ EAP 	<div data-bbox="865 212 1563 375"> <p>Peer Auth</p> <p>Authentication Type * EAP Type * Authentication Profile</p> <p>EAP MSCHAPv2 --Select--</p> </div> <p>Use the Extensible Authentication Protocol for authentication. Note that this option is available only when you select Remote Access Server in the VPN Type field in the General tab. Enter information for the following fields:</p> <ul style="list-style-type: none"> ◦ EAP Type (Required)—Select the EAP type: <ul style="list-style-type: none"> ▪ MD5 ▪ MSCHAPv2 ▪ (For Releases 22.1.1 and later.) TLS ◦ Authentication Profile—Select an authentication profile to associate with EAP.
<ul style="list-style-type: none"> ◦ PSK 	<div data-bbox="865 976 1624 1394"> <p>Peer Auth</p> <p>Authentication Type *</p> <p>PSK</p> <p>Remote Clients</p> <p>Identity Type * Identity * key *</p> <p>IP</p> <p>No Remote Clients configured</p> </div> <p>Use a preshared key for authentication. Enter information for the following fields:</p> <ul style="list-style-type: none"> ◦ Identity Type (Required)—Select the type of identity to use for authentication: <ul style="list-style-type: none"> ▪ Email ▪ FQDN (default) ▪ IP ◦ Identity (Required)—Enter the email address, FQDN, or IP address.

	<ul style="list-style-type: none"> ◦ Key (Required)—Enter the preshared key (PSK) to use to create a tunnel. The PSK cannot include any of the following five special characters: " < > # /.
--	---

9. Select the IPsec tab and enter information for the following fields.

Add IPsec VPN

General
IKE
IPsec

Mode
Tunnel

Anti Replay
enable

Fragmentation
pre-fragmentation

Force-NAT-T Configuration
Disable

Hello Interval
10

IPsec Rekey Time
Seconds

28800

IPsec Rekey Volume
MB

Transform

☒ Multiple Transforms
☐ Single Transform




☐ HASH ALGORITHM
+

☐ ENCRYPTION ALGORITHM
+

☐ PERFECT FORWARD SECRECY GROUF
+

OK
Cancel

Field	Description
Mode	Select Tunnel.
Anti-replay	Select Enable to use anti-replay detection. Select Disable to not use anti-replay detection.
Fragmentation	Select the fragmentation type: <ul style="list-style-type: none"> ◦ Prefragmentation ◦ Post-fragmentation
Force-NAT-T Configuration	Select Enable to force the tunnel to use NAT traversal. use the force-NAT-T configuration. Select Disable to not use NAT traversal.
Hello Interval	(For Releases 22.1.1 and later.) Enter the hello interval timeout. Note that in previous releases, this field was called Keepalive Timeout. <i>Range:</i> 3 through 30 seconds
IPsec Rekey Time	Select the time units for how often to regenerate the IPsec key, and then enter the time interval: <ul style="list-style-type: none"> ◦ Hours ◦ Minutes ◦ Seconds
IPsec Rekey Volume	Select the IPsec rekey volume units, in MB, GB, or TB, and then enter a value for how much data can be transmitted using a given IPsec key.
Transform (Group of Fields)	
<ul style="list-style-type: none"> ◦ Multiple Transforms 	Click to configure multiple transforms.

<ul style="list-style-type: none"> ◦ Hash Algorithm 	<p>Click the  Add icon, and select the hash algorithms to use:</p> <ul style="list-style-type: none"> ◦ MD5—MD5 Message Digest Algorithm ◦ SHA-1—Secure Hash Algorithm 1 with 160-bit digest. This is the default. ◦ SHA-256—Secure Hash Algorithm 2 with 256-bit digest ◦ SHA-384—Secure Hash Algorithm 2 with 384-bit digest ◦ SHA-512—Secure Hash Algorithm 2 with 512-bit digest ◦ XCBC—Extended Cypher Block Chaining <p><i>Default:</i> SHA-1</p>
<ul style="list-style-type: none"> ◦ Encryption Algorithm 	<p>Click the  Add icon, and select the encryption algorithm to use:</p> <ul style="list-style-type: none"> ◦ 3DES—Triple DES encryption algorithm ◦ AES128—AES CBC encryption algorithm with 128-bit key ◦ AES128-CTR—AES counter mode encryption algorithm with 128-bit key ◦ AES128-GCM—AES GCM encryption algorithm with 128-bit key ◦ AES256—AES CBC encryption algorithm with 256-bit key ◦ AES256-GCM—AES GCM encryption algorithm with 128-bit key ◦ Null
<ul style="list-style-type: none"> ◦ Perfect Forward Secrecy Group 	<p>Click the  Add icon, and select the Diffie-Hellman groups to use for PFS:</p> <ul style="list-style-type: none"> ◦ Diffie-Hellman Group 1—768-bit modulus ◦ Diffie-Hellman Group 2—1024-bit modulus

	<ul style="list-style-type: none"> ◦ Diffie-Hellman Group 5—1536-bit modulus ◦ Diffie-Hellman Group 14—2048-bit modulus ◦ Diffie-Hellman Group 15—3072-bit modulus ◦ Diffie-Hellman Group 16—4096-bit modulus ◦ Diffie-Hellman Group 19—256-bit elliptic curve ◦ Diffie-Hellman Group 20—384-bit elliptic curve ◦ Diffie-Hellman Group 21—521-bit elliptic curve ◦ No PFS. This is the default. <p><i>Default:</i> No PFS</p>
◦ Single Transform	Click to configure a single transform.
◦ Transform	<p>Select the transform type to use:</p> <ul style="list-style-type: none"> ◦ ESP-3DES-MD5 ◦ ESP-3DES-SHA1 ◦ ESP-AES128-CTR-SHA1 ◦ ESP-AES128-CTR-XCBC ◦ ESP-AES128-GCM ◦ ESP-AES128-MD5 ◦ ESP-AES128-SHA1 ◦ ESP-AES128-SHA256 ◦ ESP-AES128-SHA384 ◦ ESP-AES128-SHA512 ◦ ESP-AES256-GCM ◦ ESP-AES256-MD5 ◦ ESP-AES256-SHA256 ◦ ESP-AES256-SHA384 ◦ ESP-AES256-SHA512 ◦ ESP-NUL-MD5 <p><i>Default:</i> ESP-AES128-SHA1</p>
◦ Perfect Forward Secrecy Group	<p>Select the Diffie-Hellman group to use for PFS:</p> <ul style="list-style-type: none"> ◦ Diffie-Hellman Group 1—768-bit modulus ◦ Diffie-Hellman Group 2—1024-bit modulus ◦ Diffie-Hellman Group 5—1536-bit modulus

	<ul style="list-style-type: none"> ◦ Diffie-Hellman Group 14—2048-bit modulus ◦ Diffie-Hellman Group 15—3072-bit modulus ◦ Diffie-Hellman Group 16—4096-bit modulus ◦ Diffie-Hellman Group 19—256-bit elliptic curve ◦ Diffie-Hellman Group 20—384-bit elliptic curve ◦ Diffie-Hellman Group 21—521-bit elliptic curve ◦ Diffie-Hellman Group 25—192-bit elliptic curve ◦ Diffie-Hellman Group 26—224-bit elliptic curve ◦ No PFS. This is the default. <p><i>Default:</i> No PFS</p>
--	--

10. Click OK.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 22.1.1 adds support for the Fragment Size field for IKE; allows you to configure AES 128-GCM and AES 256-GCM encryption for IKE.
- In Release 22.1.3, when you change IPsec and IKE configuration parameters or when a certificate is renewed, the affected IPsec/IKE tunnel is not torn down; add IPAM address and DNS fields when configuring address pools.

Additional Information

[Configure Basic Features](#)

[Configure a Branch SD-WAN Profile](#)

[Configure a KMIP Client](#)

[Configure Versa Secure Access Service](#)

[Configure VOS Device Alarms](#)

[Overview of Configuration Templates](#)

[Troubleshoot IKE and IPsec](#)