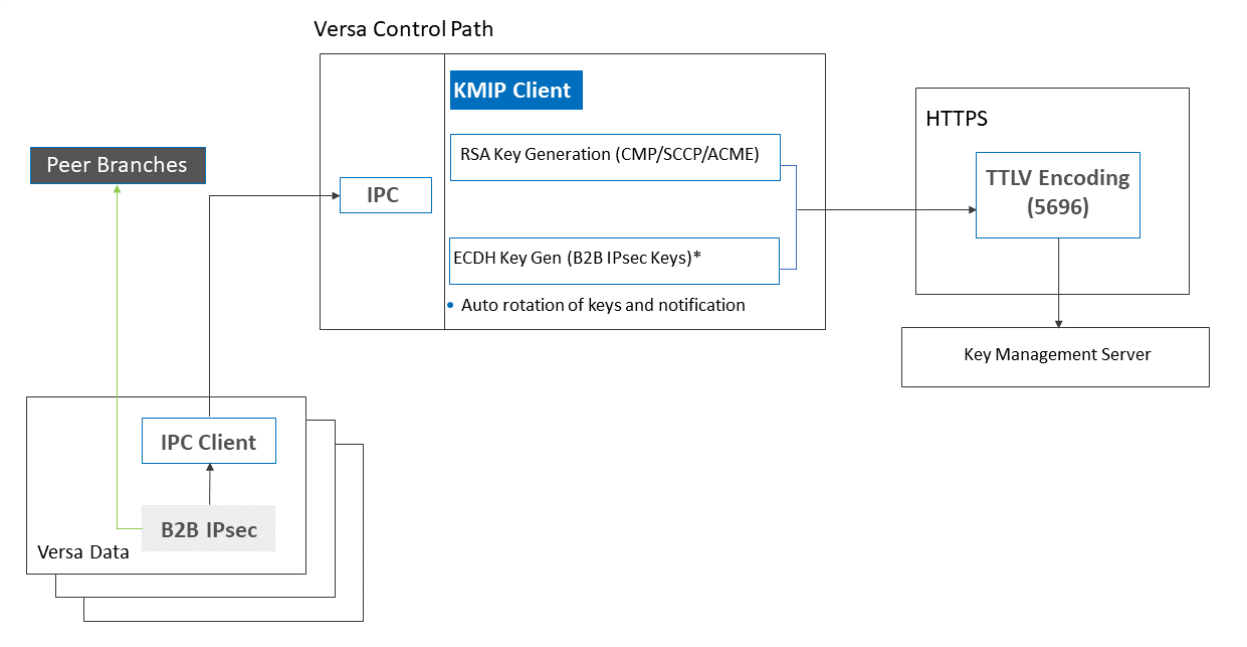
Configure a KMIP Client

For supported software information, click here.

The Key Management Interoperability Protocol (KMIP) is a client–server communication protocol that enables key management and cryptographic operations on a key management server (KMS). Cryptographic operations include managing the lifecycle of objects such as keys and performing cryptographic operations for these objects. KMIP simplifies cryptographic key management and allows you to store and maintain keys, certificates, and secret objects.

You can configure a Versa Operating System™ (VOS™) device to be a KMIP client.

The following figure illustrates how KMIP works on a Versa SD-WAN branch device that has been configured as a KMIP client. This figures shows that after you configure a Versa SD-WAN branch device to be a KMIP client, the KMIP client requests that an RSA key be created on the KMS for use in enrollment protocols such as SCEP, CMP, and ACME, and the client also requests the creation of an EC key to use for Diffie-Hellman operations in the SD-WAN secure data path.



On VOS devices, KMIP is handled by the certificate daemon.

The KMIP client interface securely connects with the KMS using TLS or HTTPS over port 5696, and sends HTTPS

requests to perform cryptographic operations on the KMS. To establish a TLS session to the KMS, the KMIP client must have a valid client certificate, private key, and certificate authority (CA) chain.

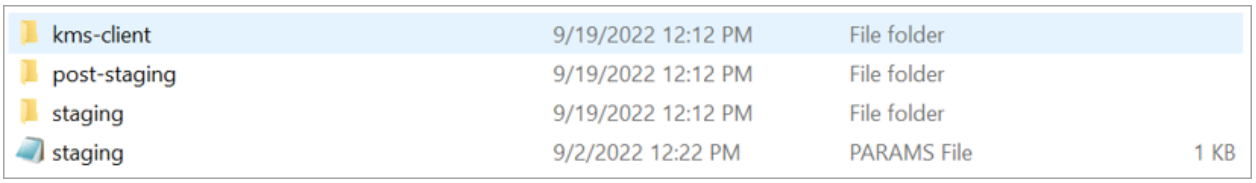
This article provides a configuration example for configuring a KMIP client. To configure a KMIP client, you perform zero-touch provisioning (ZTP) of a Versa SD-WAN branch device using the public key infrastructure (PKI) from a USB storage drive, you configure the Controller for KMIP traffic, and finally you configure a branch device to be a KMIP client.

Set Up a USB Storage Drive for PKI-Based ZTP

To perform PKI-based ZTP for VOS SD-WAN branch devices, you use a USB storage drive. Before you perform ZTP, you must create specific directories on the USB storage drive and copy the files to these directories that are required for the staging and post-staging processes.

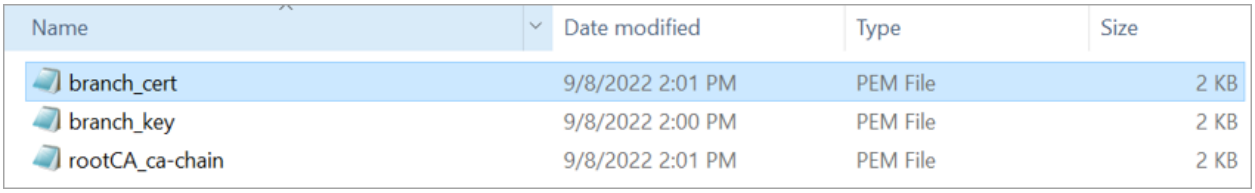
To set up the USB storage drive:

1. Create three directories on the USB, kms-client, post-staging, and staging. For example:



2. Access the CA certificate server or OpenSSL to generate a device certificate. For more information, see Create and Manage Certificates.
3. Copy the PKI key, device certificate, and CA chain files to the post-staging and staging directories, and copy the KMS certificate to each of the three folders. For these files, ensure the following:
   - Name of the device certificate file must end with _cert.pem.
   - Name of the key file must end with _key.pem.
   - Name of the CA chain must end with _ca-chain.pem.

   For example, here the kms-client folder contains the following files:



4. At the top level (root) of the USB drive, create a file named staging.params. This file contains input parameters for the staging.py script.
5. To check the staging.py script options supported in the current version of the VOS software, run the following CLI command:

```
$ vsh show-staging-params
```

For example:

```
$ vsh show-staging-params
static=10.230.55.12/16   (Static IP address of the branch)
gateway=10.230.0.1       (Gateway IP address of the branch)
controller=10.192.55.173 (WAN IP address of the controller for branch to connect for staging tunnel)
wan-port=0               (Interface link number)
auth-type=cert           (Staging mechanism - certificate or PSK)
```

Use the USB Storage Drive to Onboard a VOS Branch Device

If you have physical access to a VOS SD-WAN branch device, you can onboard the device by inserting the USB storage drive you set up in Set Up a USB Storage Drive for PKI-Based ZTP, above. When you insert the USB storage drive into the VOS branch device, the device automatically reads the staging.params file and configures itself based on the parameters specified in the file. For more information, see Use a USB Storage Drive To Activate a VOS Device.

You can perform ZTP using this USB storage drive for any VOS branch device that you want to onboard.

After you onboard a VOS branch device, to verify whether the PKI files have been imported to the device after ZTP:

1. To check that the PKI certificate has been imported, run the **show crypto pki certificates** CLI command. For example:

   ```
   admin@cli> show crypto pki certificates
   Possible completions:
   kms-client_branch_cert.pem - Certificate name
   ```

2. To check that the PKI private key file has been imported, run the **show crypto pki private-keys** CLI command. For example:

   ```
   admin@cli> show crypto pki private-keys
   Possible completions:
   kms-client_branch_key.pem - Private Key name
   ```

3. To check that the PKI CA chain file has imported, run the **show crypto pki ca-chains** CLI command. For example:

   ```
   admin@cli> show crypto pki ca-chains
   Possible completions:
   default                - Certificate Authority chain name
   kms-client_rootCA_ca-chain.pem - Certificate Authority chain name
   ```

Note that if the files have not been imported, the filenames are not displayed in the CLI output.

Configure the Controller Node for KMIP

After you onboard the SD-WAN branch devices, you configure the Controller node to handle KMIP traffic.

Before you configure the Controller node:

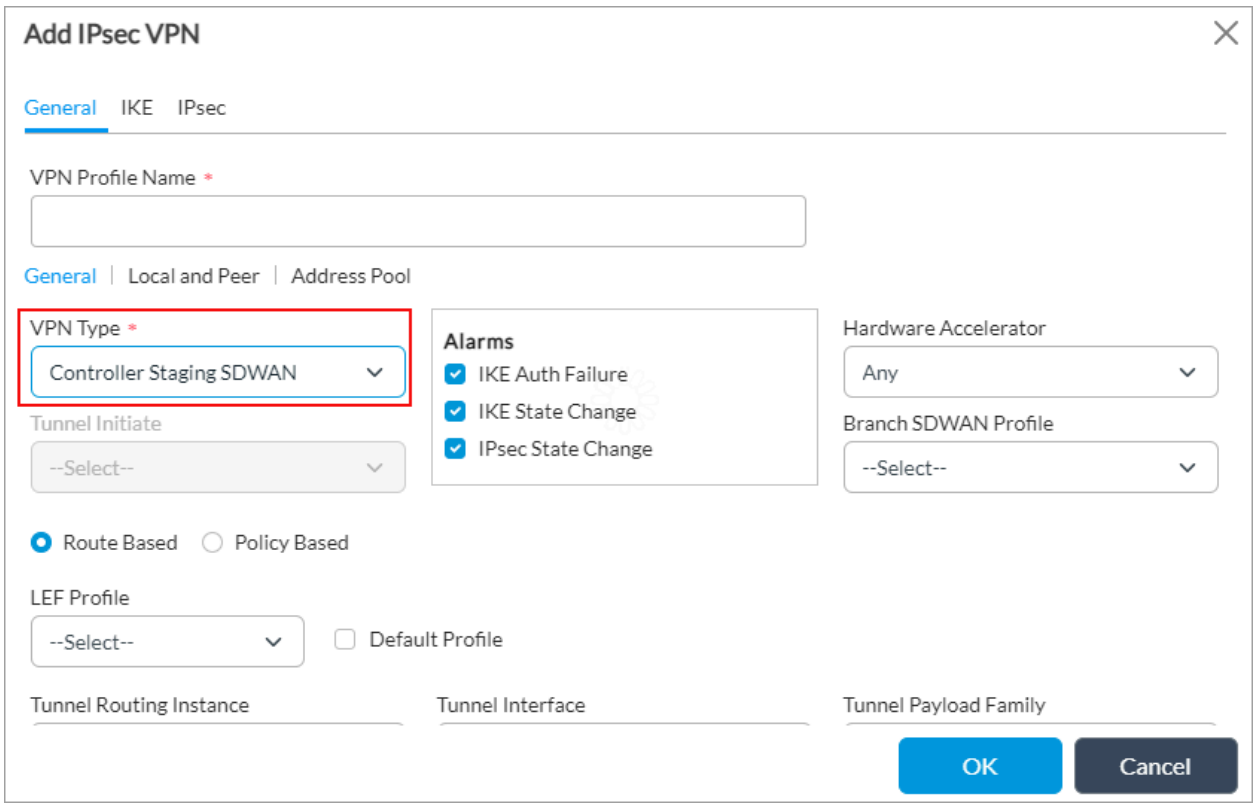
- Deploy the Controller node using a standard workflow. Note that you cannot onboard a Controller node using a USB storage drive. For more information, see Add a Controller Node.
- Ensure that the PKI certificate, key, and CA chain have been uploaded to the Controller node.

Configure an IPsec VPN Profile on the Controller Node

You configure an IPsec VPN profile on the Controller node so that it can create an IKE tunnel to use for staging.

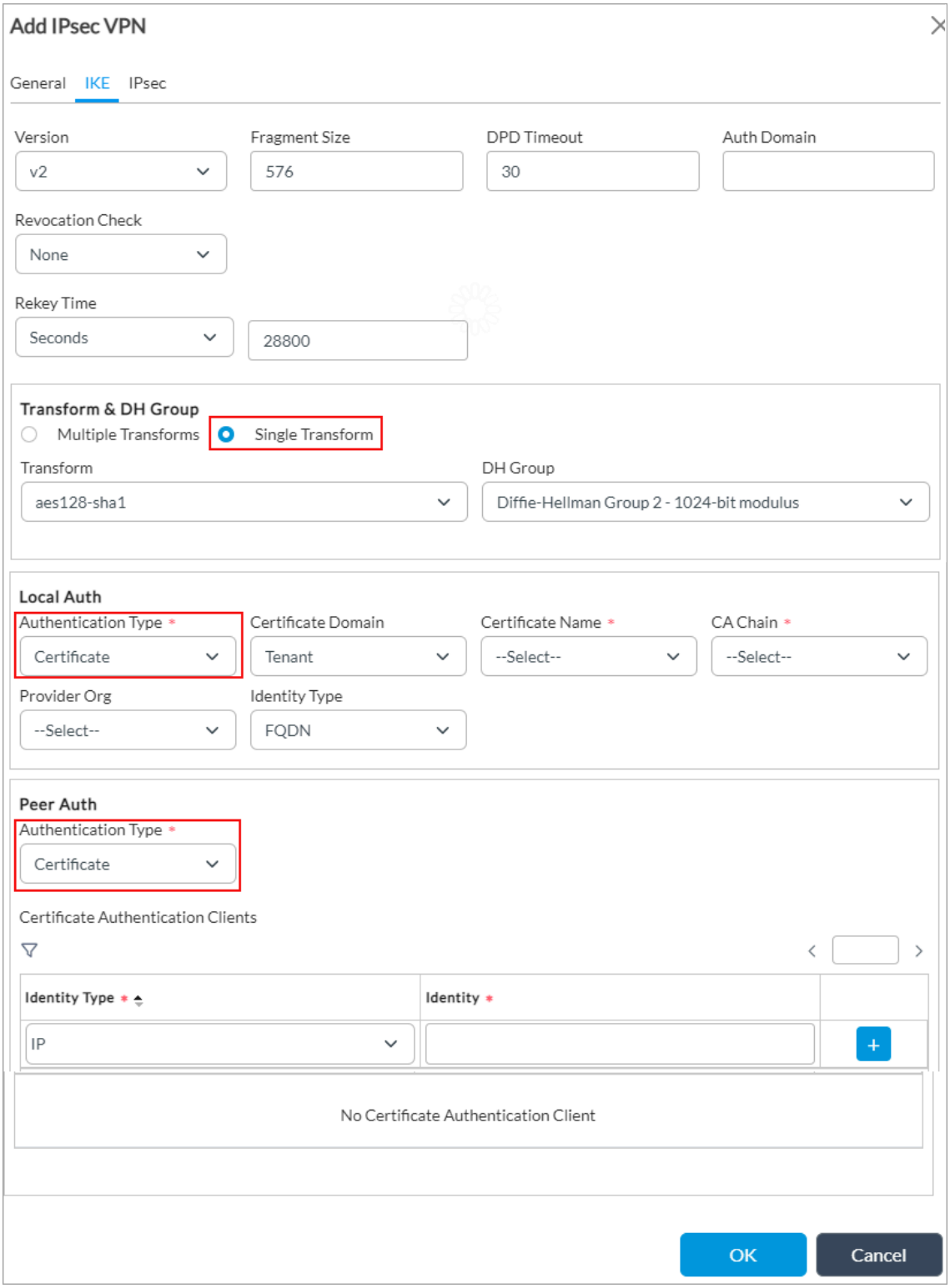
To configure an IPsec VPN profile:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select the Controller node in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > IPsec > VPN Profiles in the left menu bar.
4. Click the + Add to add an IPsec profile or select an existing profile to update it. The Add/Update IPsec VPN popup window displays.
5. Select the General tab, and then enter a name for the profile in the VPN Profile Name field.



Updated: Wed, 23 Oct 2024 08:26:50 GMT

6. Select the General tab in the horizontal menu, and then select Controller Staging SD-WAN in the VPN Type field.
7. Select the IKE tab.



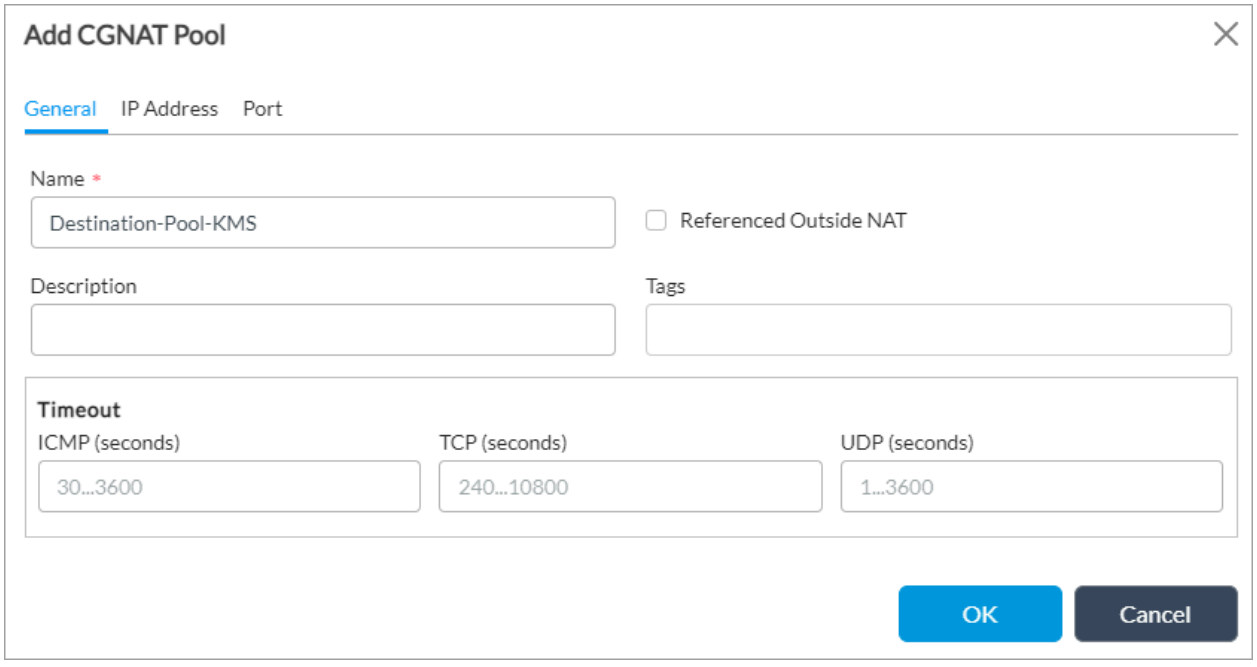
8. In the Transform & DH Group group of fields, click Single Transform.

9. In the Local Authentication group of fields, select Certificate in the Authentication Type field.
10. In the Certificate Name and CA Chain fields, elect the uploaded device certificate and CA chain.
11. In the Peer Authentication group of fields, select Certificate in the Authentication Type field.
12. For information about configuring other parameters, see Configure IPsec VPN Profiles.
13. Click OK.

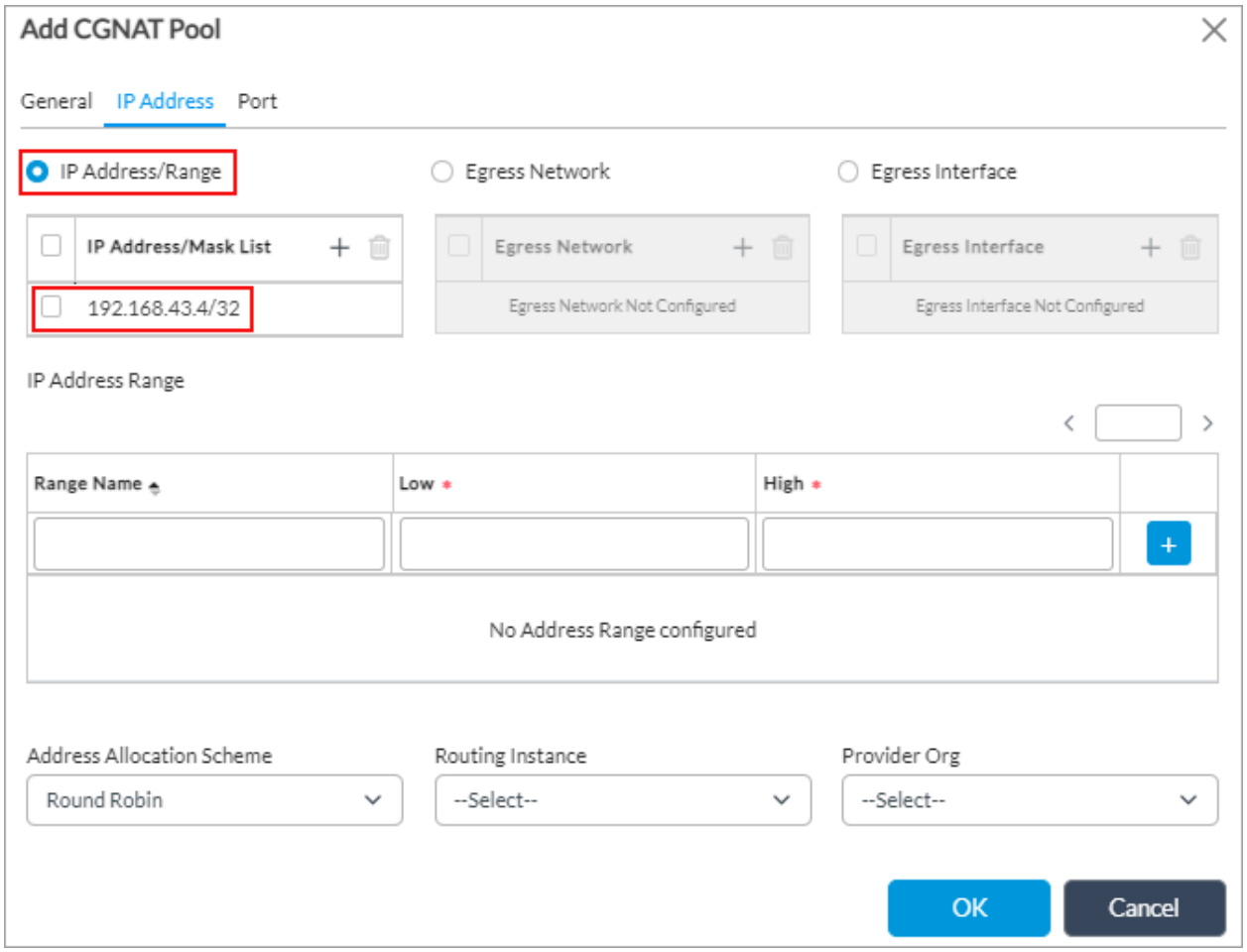
Configure a CGNAT Destination Address Pool

To configure CGNAT address pools to use for destination and source NAT KMIP traffic from the branch device to the Controller node:

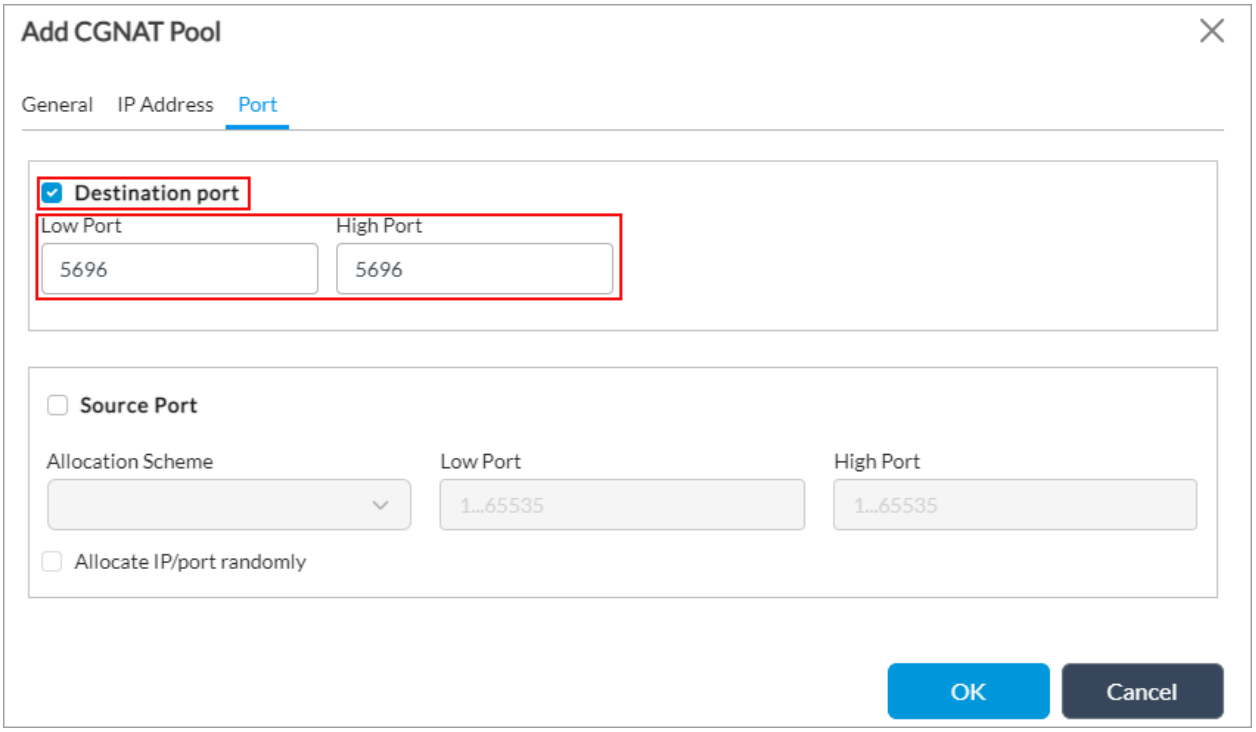
1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select the Controller node in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > CGNAT in the left menu bar. The Pools tab displays the CGNAT pools that are already configured.
4. Click + Add to add a pool. The Add CGNAT Pool popup window displays.
5. Select the General tab, and then enter a name for the destination address pool in the Name field.



6. Select the IP Address tab.



7. Click IP Address/Range, and then enter the IP address of the KMS server (here, 192.168.43.4) in the IP Address/Mask table.
8. Select the Port tab.

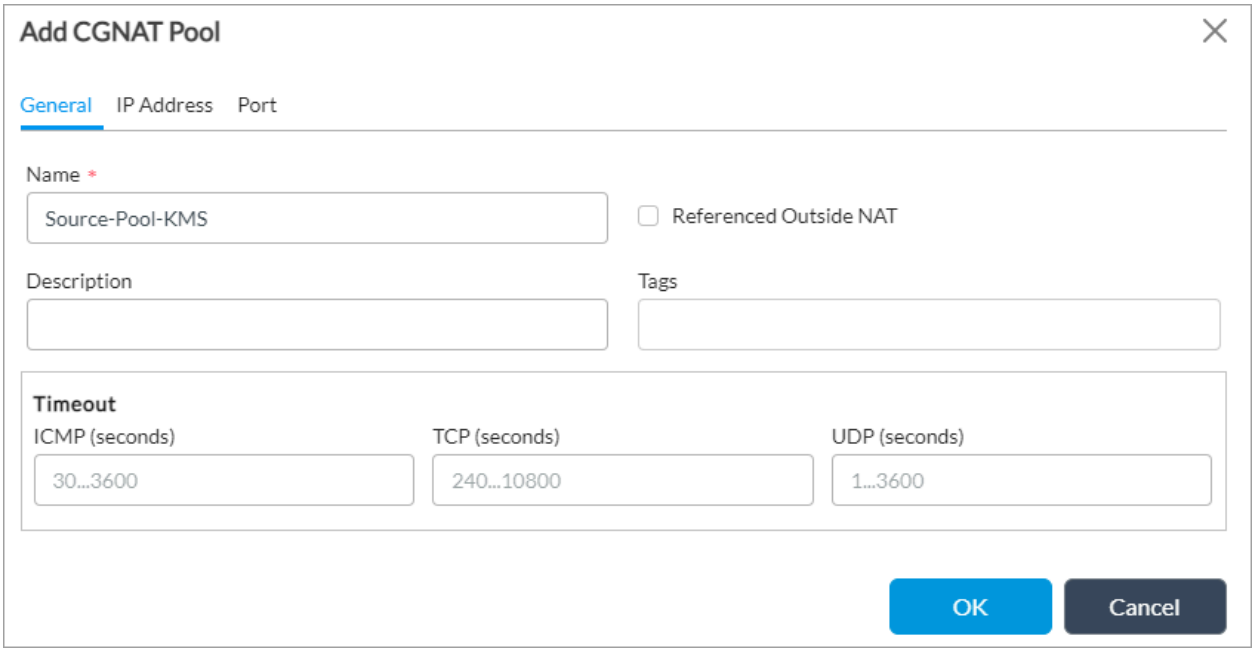


9. Click Destination Port, and the enter values in Low Port and High Port fields for the lowest and highest port numbers in the range. Enter 5696 for both port numbers.
10. For information about configuring other parameters, see Configure CGNAT Address Pools.
11. Click OK.

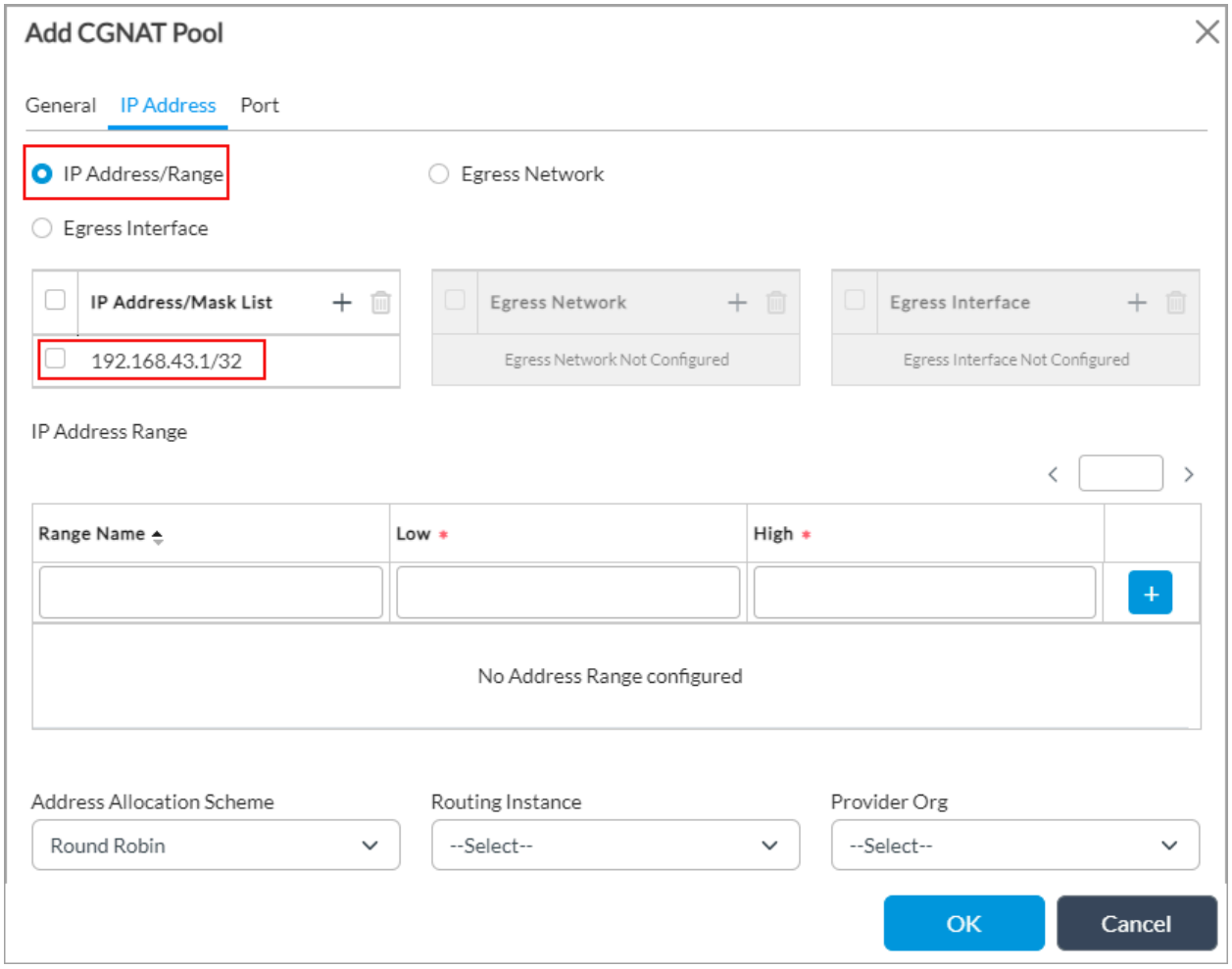
Configure a CGNAT Source Address Pool

To configure a CGNAT source address pool for NAT KMIP traffic from the branch device to the Controller node:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select the Controller node in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > CGNAT in the left menu bar. The Pools tab displays the CGNAT pools that are already configured.
4. Click + Add to add a pool. The Add CGNAT Pool popup window displays.
5. Select the General tab, and then enter a name for the source address pool in the Name field.

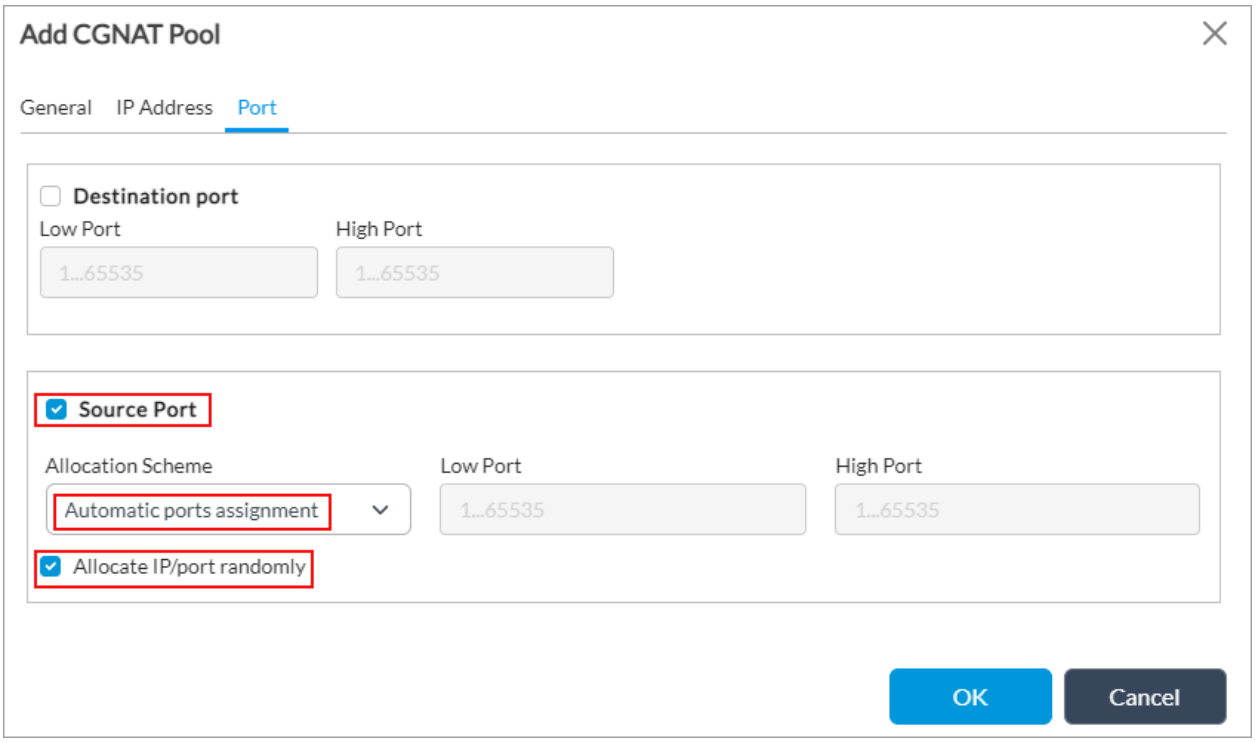


6. Select the IP Address tab.



7. Click IP Address/Range, and then enter the IP address of the KMS server (here, 192.168.43.1, which is the southbound IP address of the Controller node) in the IP Address/Mask table.
8. Select the Port tab.

Updated: Wed, 23 Oct 2024 08:26:50 GMT

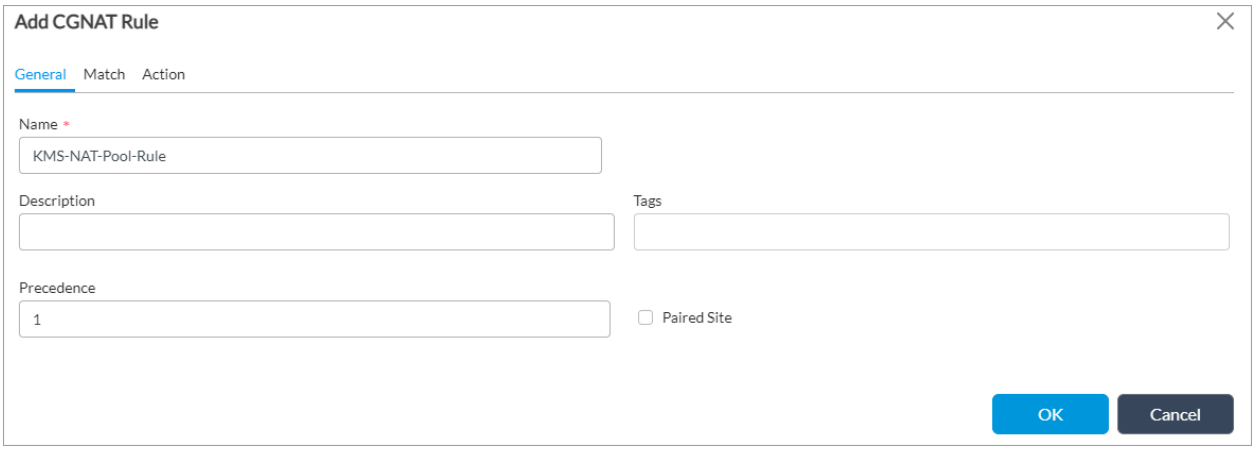


9. Click Source Port, and then select Automatic Port Assignment in the Allocation Scheme field.
10. Click Allocate IP/Port Randomly.
11. For information about configuring other parameters, see Configure CGNAT Address Pools.
12. Click OK.

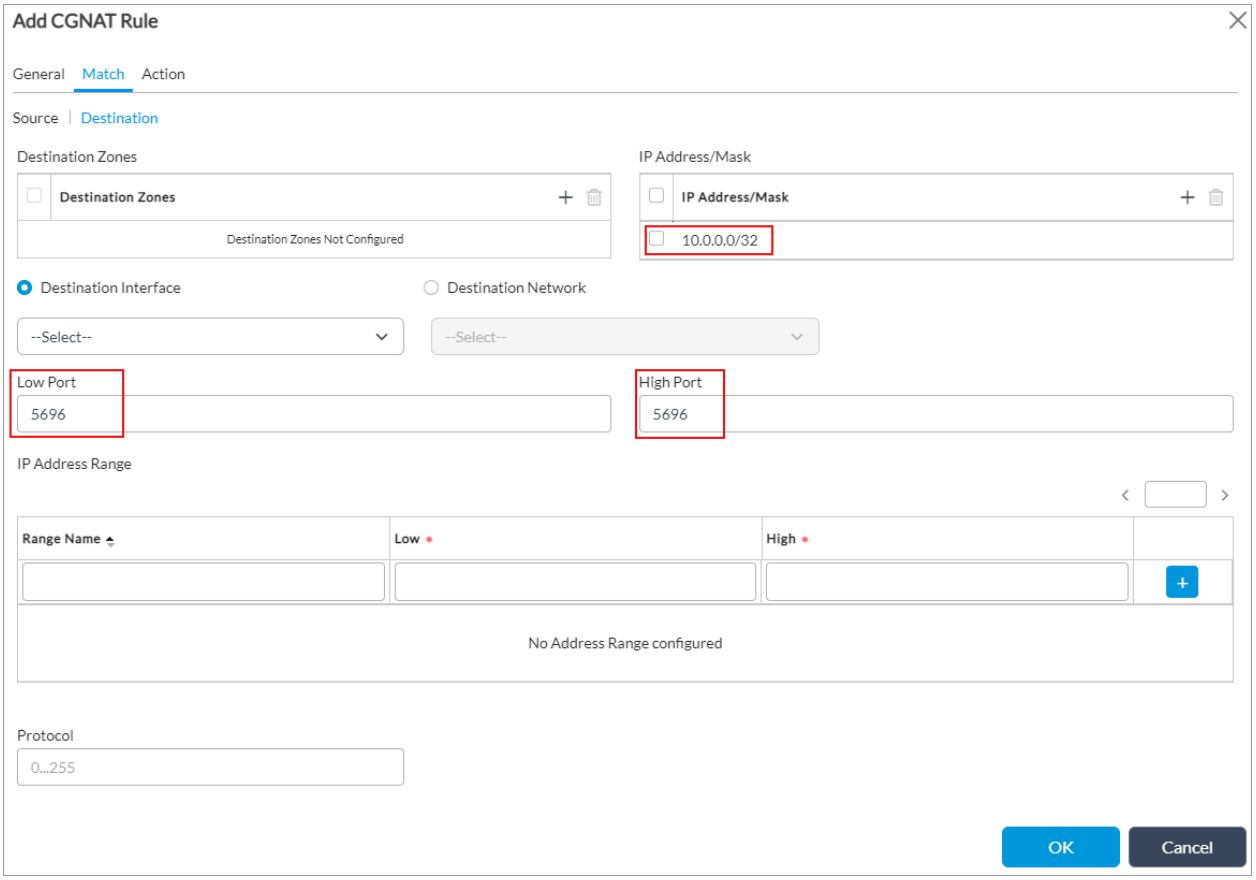
Configure a CGNAT Rule for the KMIP Connection

To configure a CGNAT rule for the KMIP connection between the Controller node and the branch device on which the KMIP client is configured:

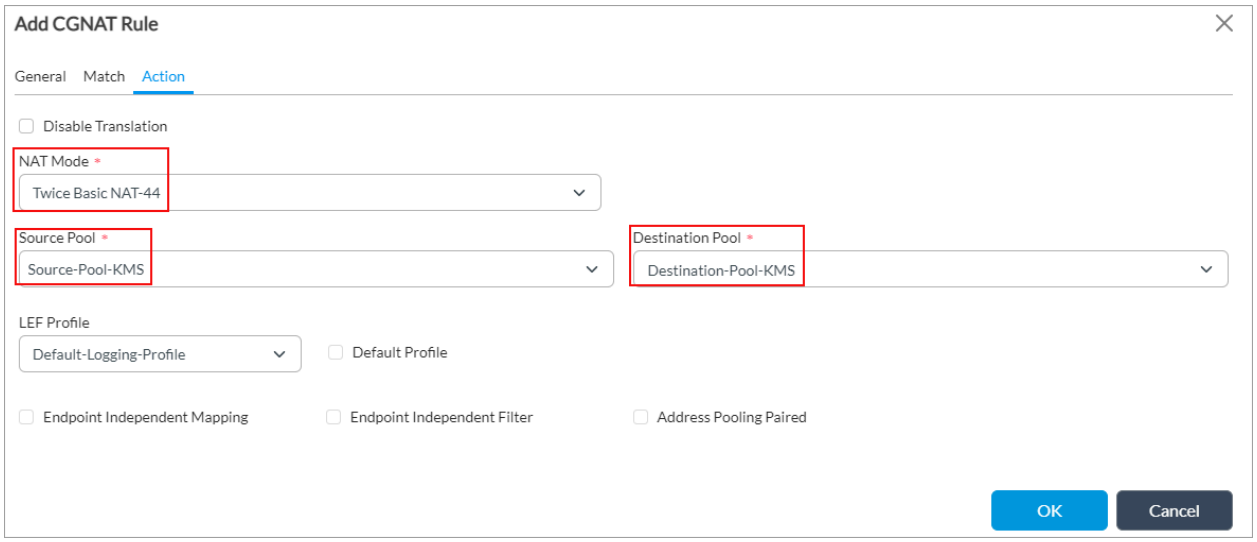
1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select the Controller node in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > CGNAT in the left menu bar.
4. Select the Rules tab in the horizontal menu bar. The main pane displays the rules that are already configured.
5. Click + Add to configure a rule. The Add CGNAT Rule popup window displays.
6. Select the General tab, and then enter a name for the rule in the Name field.



7. Select the Match tab.



8. Select the Destination tab and add the IP address of the organization control VR that is configured on the KMIP client. This is the address to use to connect to the KMS. Here, the address is 10.0.0.0/32.
9. Click Destination Interface, and then enter the value 5696 in the Low Port and High Port fields.
10. Select the Action tab.



11. In the NAT Mode field, select Twice NAPT-44.
12. In the Source Pool field, select the source CGNAT address pool you created in Configure a CGNAT Source Address Pool, above.
13. In the Destination Pool field, select the destination CGNAT address pool you created in Configure a CGNAT Destination Address Pool, above.
14. For information about configuring other parameters, see Configure CGNAT Rules.
15. Click OK.

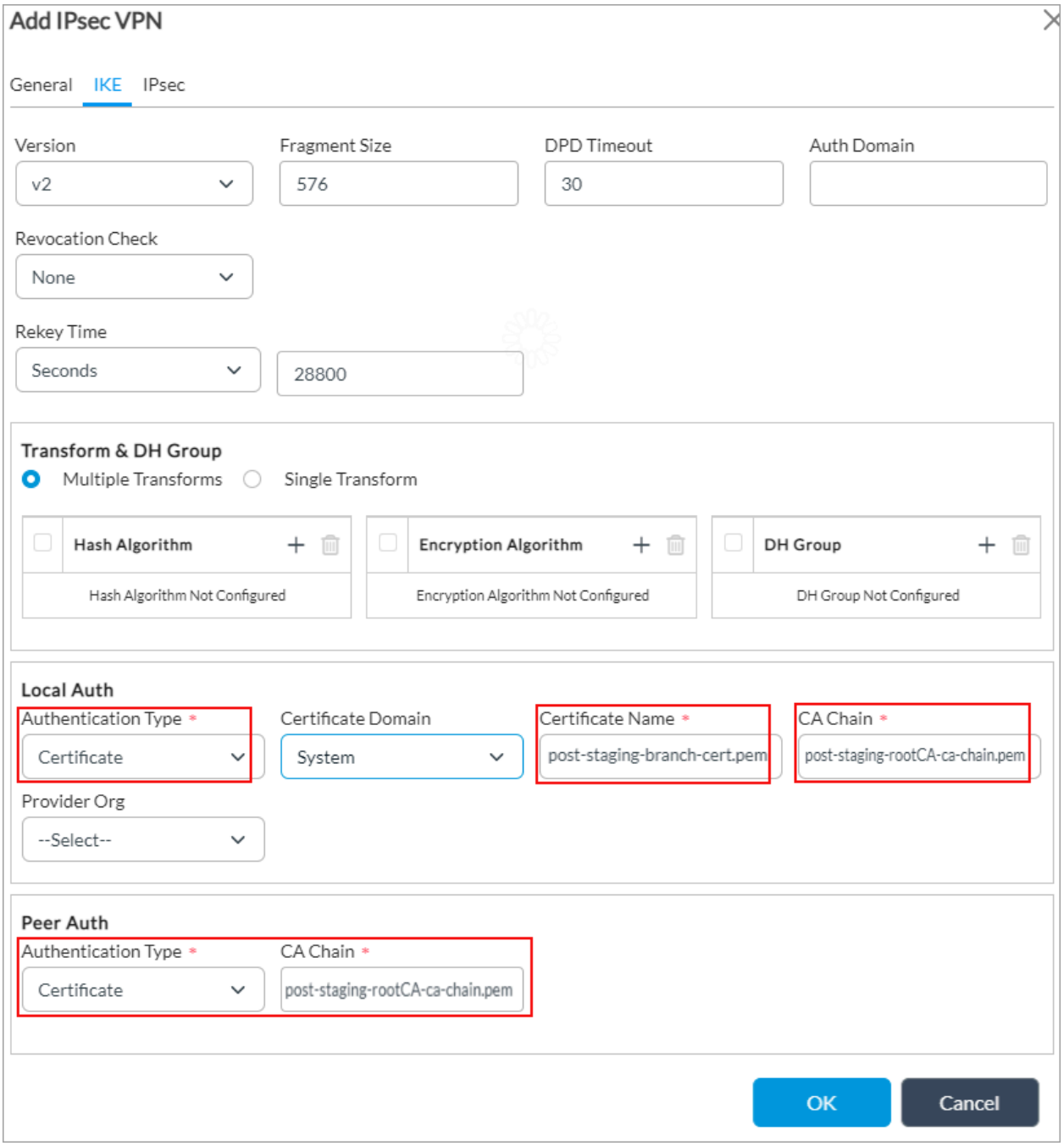
Configure the Branch Device for KMIP

You configure the post-staging template of the branch so that the branch to be a KMIP client. To do this, you configure an IPsec VPN profile, you configure a profile for the KMIP client server that hosts the certificates for the branch, and then you associate the KMIP client server profile with a branch SD-WAN profile.

Configure the Branch IPsec VPN Profile

To associate the branch device VPN profile with the PKI certificates for KMIP, configure an IPsec VPN profile on the branch:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select the branch device in the main pane. The view changes to Appliance view.
2. Select Services > IPsec > VPN Profiles in the left menu bar.
3. Click + Add icon to add an IPsec profile, or select an existing profile to update it. The Add/Update IPsec VPN popup window displays.

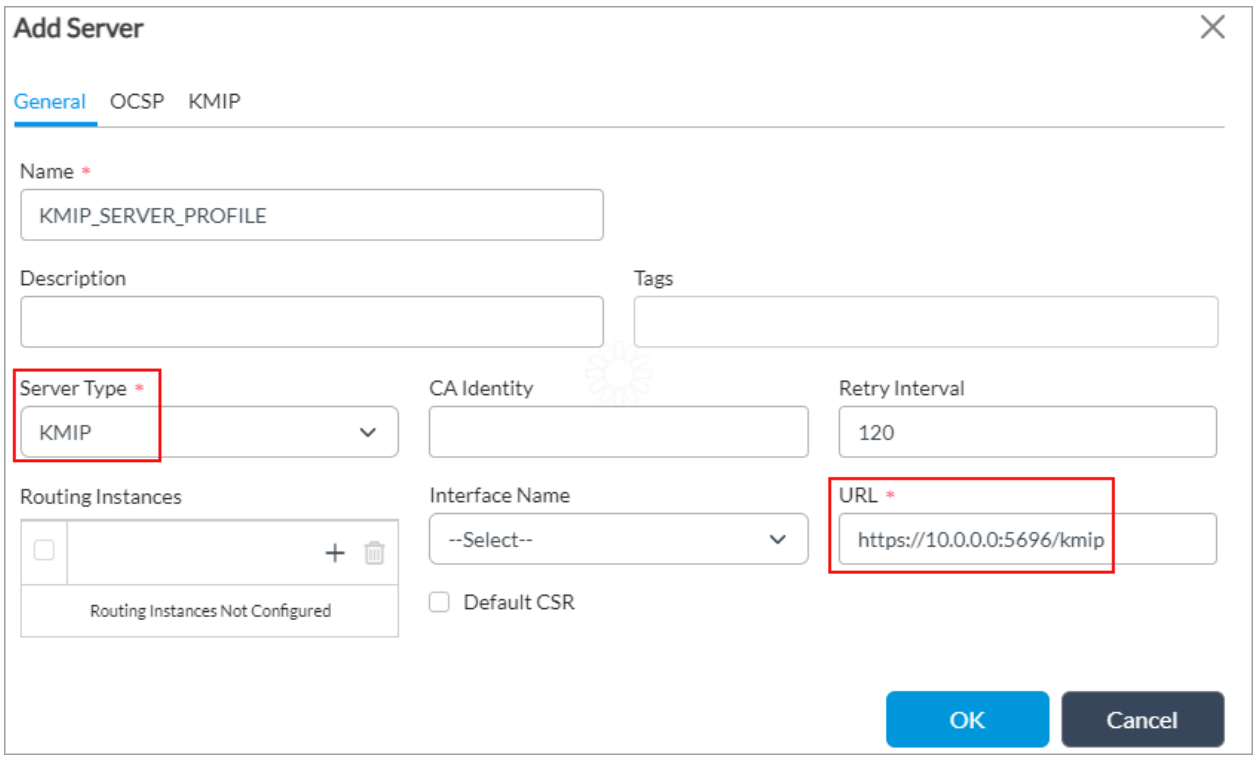


4. Select the IKE tab.
5. In the Local Authentication group of fields, select Certificate in the Authentication Type field.
6. In the Certificate Name and CA Chain fields, enter the names of the files containing the certificate and CA chain. You can parameterize the values if you use different certificates for different branches.
7. In the Peer Authentication group of fields, select Certificate in the Authentication Type field, and enter the name of the CA chain file in the CA Chain field.
8. For information about configuring other parameters, see Configure IPsec VPN Profiles.
9. Click OK.

Configure a KMIP Client Server Profile for the Branch

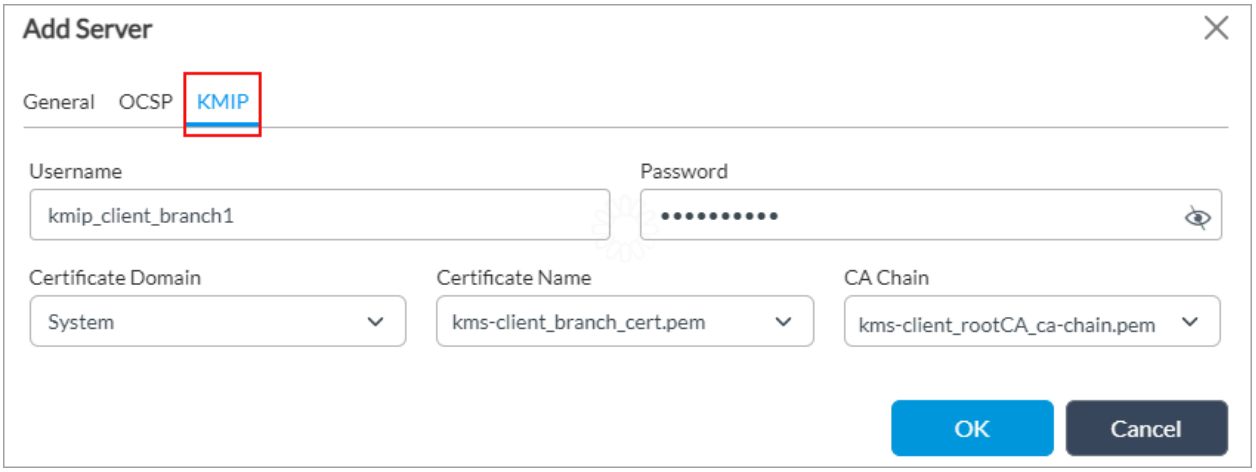
To configure a profile for the KMIP client server for that hosts the KMIP certificates for the branch:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select the branch device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > Certificate Manager in the left menu bar.
4. Select the Servers tab in the horizontal menu bar, and then click + Add icon. The Add Server popup window displays.



5. Select the General Tab.
6. In the Server Type field, select KMIP.
7. In the URL field, enter the URL of the KMIP server.

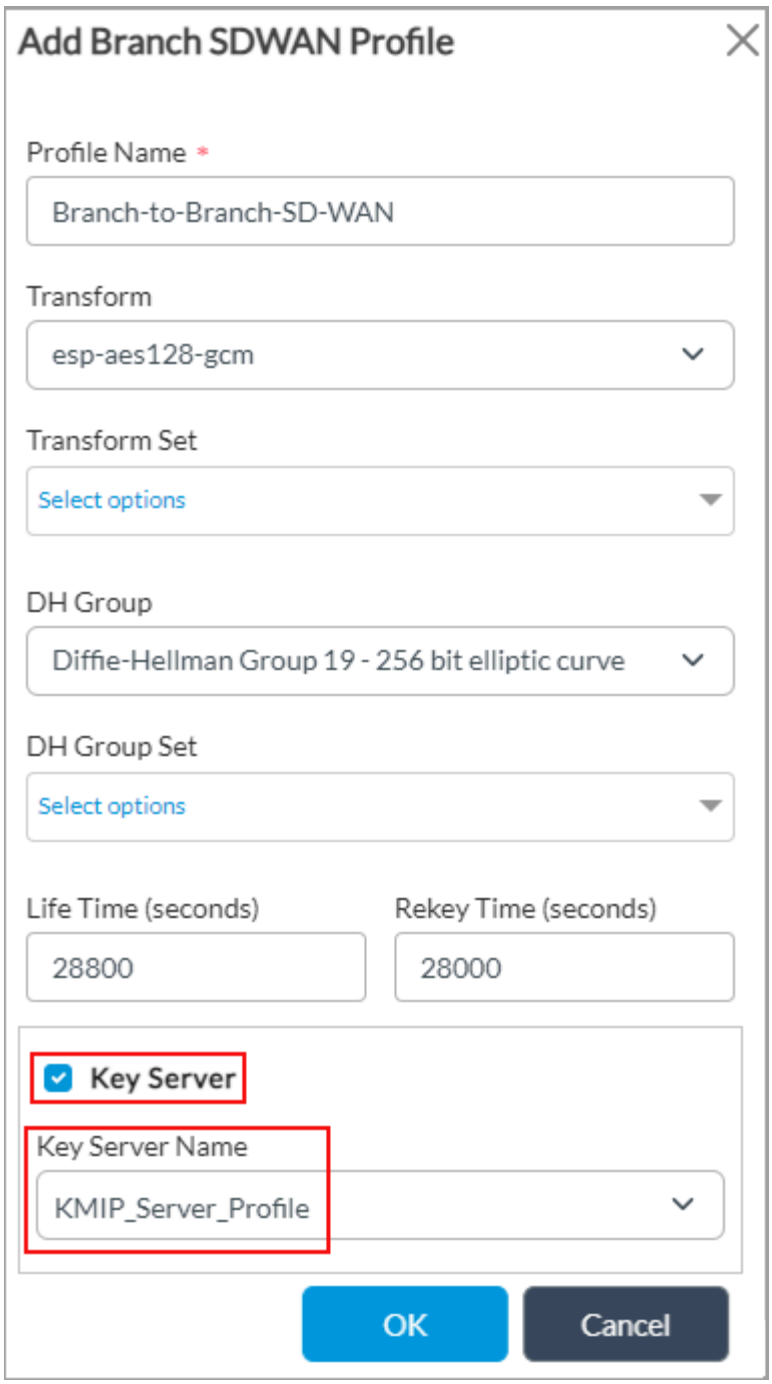
Updated: Wed, 23 Oct 2024 08:26:50 GMT



8. Select the KMIP tab.
9. In the KMIP group of fields, enter the username and password for the KMIP server.
10. In the Certificate Domain field, select System and then enter the names of the certificate and CA chain files.
11. For information about configuring other parameters, see Configure Certificate Servers.
12. Click OK.

Associate the KMIP Server Profile with a Branch SD-WAN Profile

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select the branch device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > IPsec > Branch SD-WAN Profile in the left menu bar.
4. Click + Add. The Add Branch SD-WAN Profile popup window displays.



5. In the Profile Name field, enter a name for the SD-WAN branch profile.
6. Click Key Server, and then, in the Key Server Name field, select the KMIP server profile you configured in Configure a KMIP Client Server Profile for the Branch, above.
7. For information about configuring other parameters, see Configure a Branch SD-WAN Profile.
8. Click OK.

Software Release Information

Releases 22.1.1 and later support all content described in this article.

Additional Information

Activate VOS Devices
Configure a Branch SD-WAN Profile
Configure Basic Features
Configure Certificate Servers
Configure CGNAT
Configure IPsec VPN Profiles