POLICY SUPERVISOR PROJECT

Getting Started & User Guide

April 2023

Table of Contents

Policy Supervisor Overview

Policy Supervisor is an online tool that enables operators of F5 WAF technologies to easily convert policy files between BIG-IP AWAF, F5 Distributed Cloud WAF, and NGINX App Protect formats. In the process we're using an intermediate JSON-based common declarative format called CDP (Common Declarative Policy).

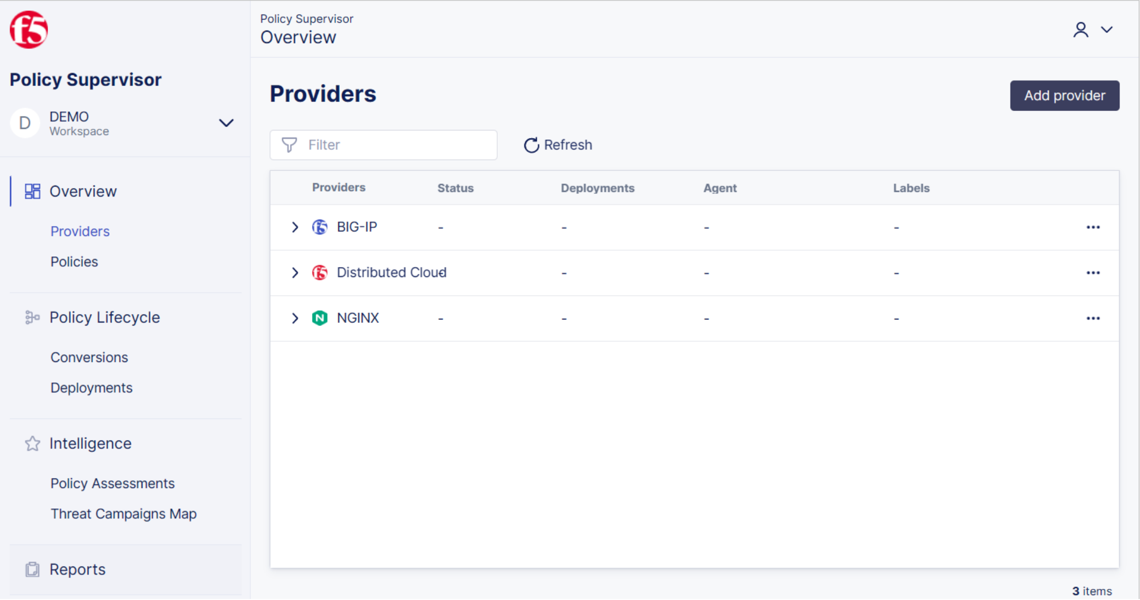
After a policy is converted to CDP, it can then be deployed to any supported WAF Solution, which is referred to as a Provider in Policy Supervisor lingo. Please refer to the GitHub repo for the Policy Supervisor Tutorial for currently supported Provider types.

Policy Supervisor provides a graphical interface for visual policy creation, editing and management for traditional SecOps and DevSecOps personas.

Getting Started

Go to the Policy Supervisor host site https://policysupervisor.io and log in using your organization Azure Active Directory (AAD) account, or your personal Microsoft account.

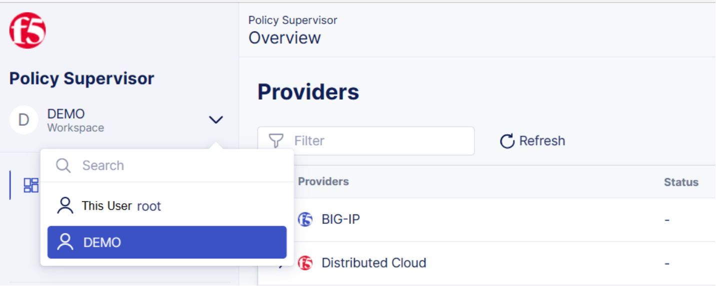
When you log in, your account is automatically created so you don't need to request account creation from an administrator or super user.



Providers	Status	Deployments	Agent	Labels
BIG-IP	-	-	-	-
Distributed Cloud		-	-	-
NGINX	-	-	-	-

Workspaces

Your default workspace is your Azure/Microsoft account name followed by *root*. Only you can view this personal workspace and make updates. Any other workspaces are accessible by invitation only; therefore, you will only see your own workspace, and those that you were invited to.



Providers	Status
BIG-IP	-
Distributed Cloud	-

Providers

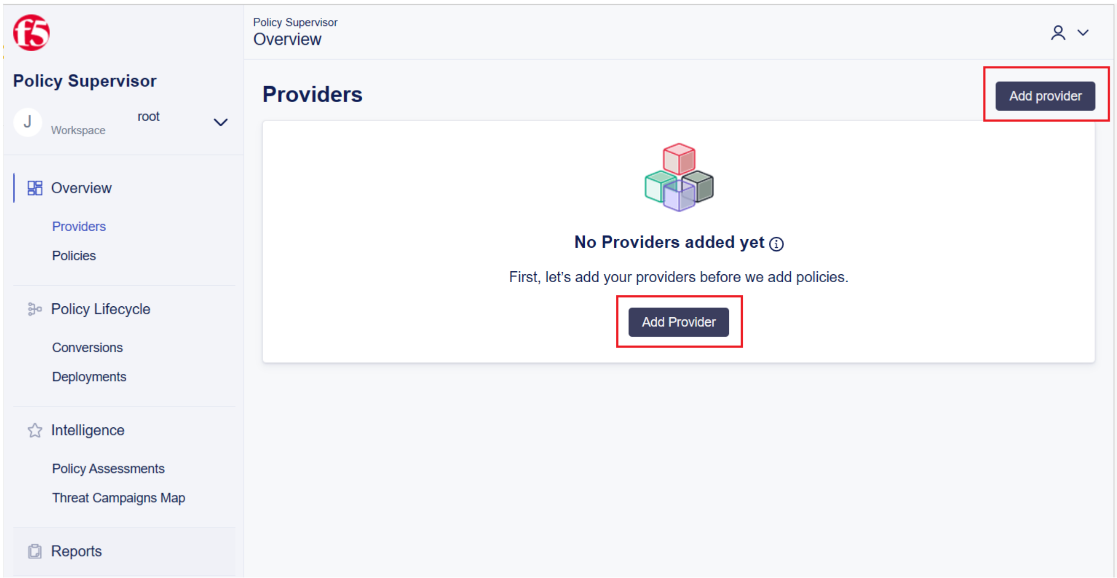
A Provider is a generic name used by Policy Supervisor to indicate an F5 Web App Firewall. The supported Provider types are: F5 Distributed Cloud WAF, BIG-IP Advanced WAF (AWAF), and NGINX Application Protection (NAP). Add and connect providers in Policy Supervisor to enable the deployment of your configuration policies across endpoints and load balancers for complete WAF protection.

Adding a BIG-IP Provider

When you add a BIG-IP instance as a provider, you must first set up an agent and associated secret on the private network to enable a secure connection between the BIG-IP instance and Policy Supervisor. For more information, see the following section: Adding and Configuring an Agent: BIG-IP and NGINX.

When you have installed your agent on the Linux machine/VM located on the same network as the BIG-IP instance, you can complete the setup in Policy Supervisor as follows:

1. On the *Overview* > *Providers* page, click **Add Provider**. If this is the first provider being added, there are two Add Provider buttons on the screen.



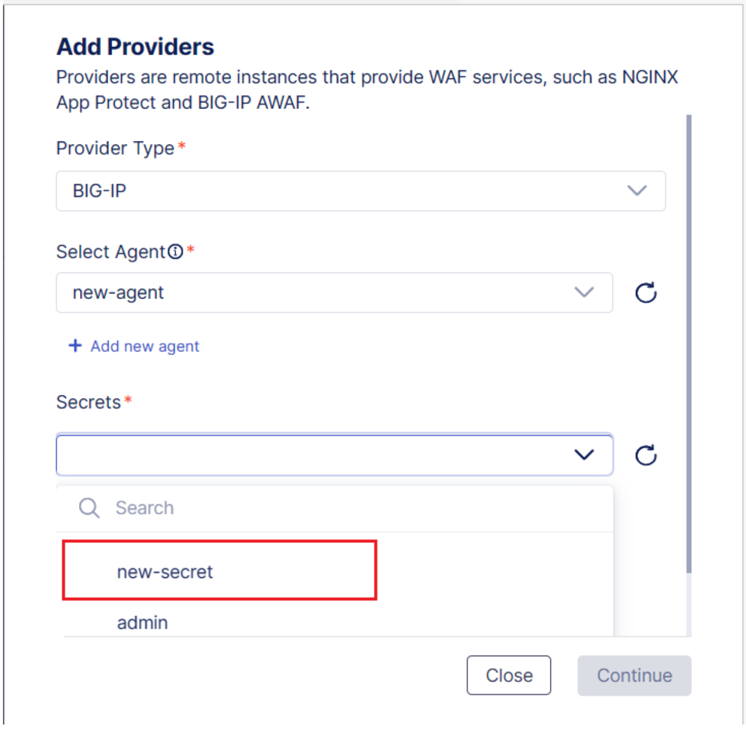
No Providers added yet ⓘ

First, let's add your providers before we add policies.

2. On the resultant *Add Providers* pane, in the *Provider Type* drop-down, choose **BIG-IP**.

3. In the *Select Agent* field, choose the agent that will be used to connect to the BIG-IP provider. Either select an existing agent or create a new one as described in Adding and Configuring an Agent: BIG-IP and NGINX.

4. The *Secrets* field is then displayed. From the *Secrets* drop-down list, choose the secret to use and click **Continue**.



Add Providers

Providers are remote instances that provide WAF services, such as NGINX App Protect and BIG-IP AWAF.

Provider Type*

BIG-IP

Select Agent ⓘ *

new-agent

+ Add new agent

Secrets*

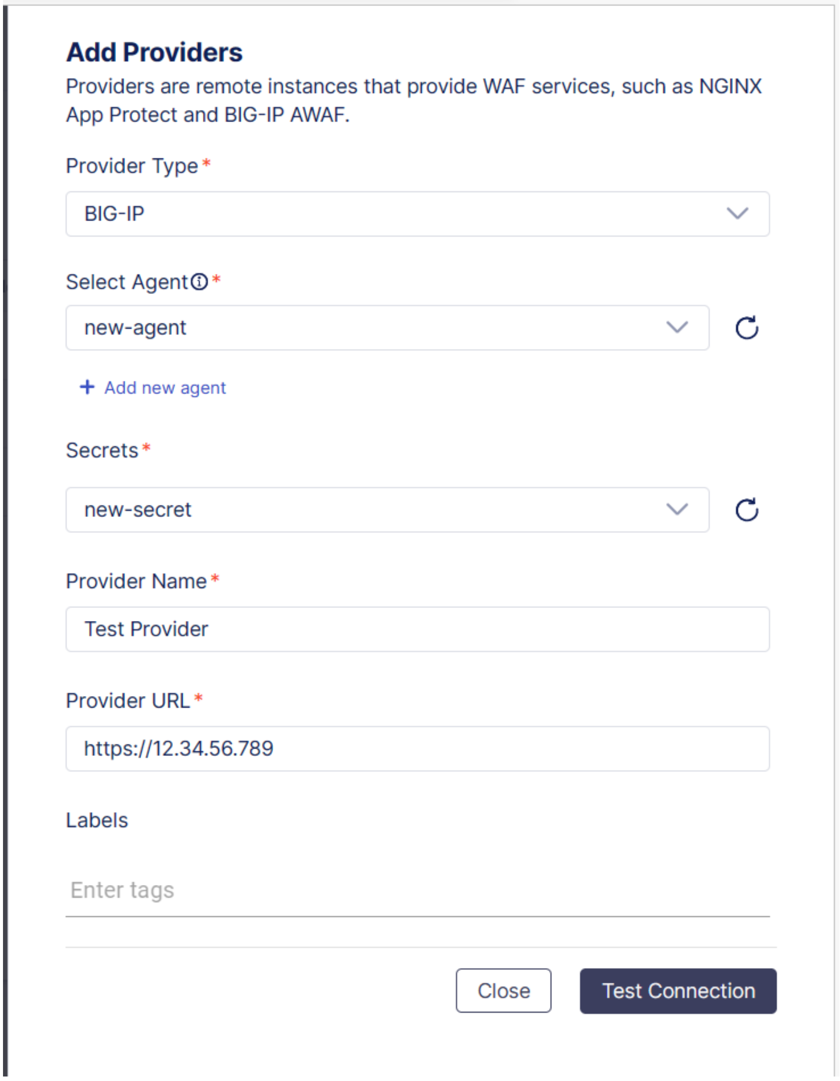
Search

new-secret

admin

Note: An agent can have more than one secret associated with it, and all secrets are displayed in the *Secrets* drop-down list.

5. In the *Provider Name* field, enter a name for this provider, and then in the *Provider URL* field, enter the URL where the BIG-IP provider instance is located.



Add Providers

Providers are remote instances that provide WAF services, such as NGINX App Protect and BIG-IP AWAF.

Provider Type * BIG-IP

Select Agent * new-agent

Secrets * new-secret

Provider Name * Test Provider

Provider URL * https://12.34.56.789

Labels

Note: Ensure that you enter the full URL description, including *https://*

6. In the *Labels* field, optionally add some label tags if you would like to have user-generated text that can be used to search for and organize your providers.

7. Click **Test Connection** and wait for the connection processes to complete between Policy Supervisor and the provider.

8. When the connection has completed, a *Success* message is displayed showing the connection details. From here you can add another provider or return to the *Providers Overview* page.

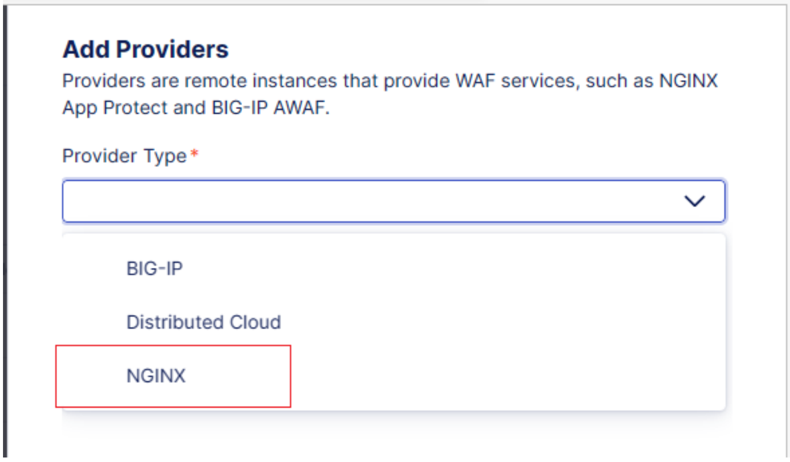
Adding an NGINX Provider

When you add an NGINX instance as a provider, you must first set up an agent and associated secret on the private network to enable Policy Supervisor to securely connect to the NGINX instance. For more information, see the following section: Adding and Configuring an Agent: BIG-IP and NGINX.

When you have installed your agent on the Linux machine/VM located on the same network as the NGINX instance, you can complete the setup in Policy Supervisor as follows:

1. On the *Providers* page, click **Add Provider**. If this is the first provider across all provider types being added, there are two Add Provider buttons on the screen.

2. On the resultant *Add Providers* pane, in the *Provider Type* drop-down, choose NGINX.



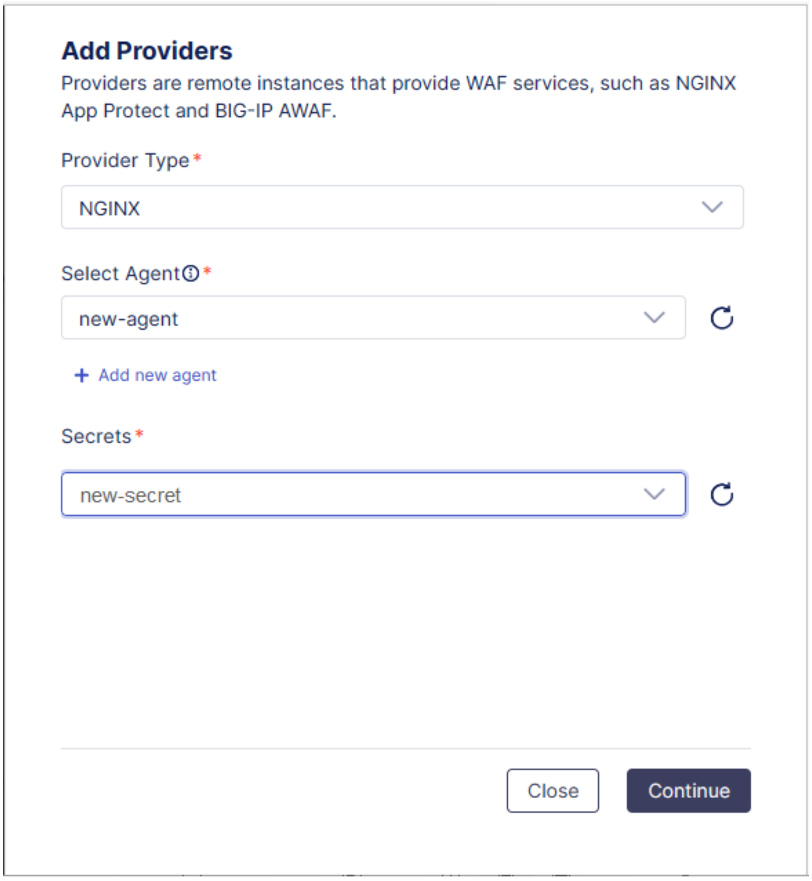
Add Providers

Providers are remote instances that provide WAF services, such as NGINX App Protect and BIG-IP AWAF.

Provider Type *

3. In the *Select Agent* field, choose the agent that will be used to securely connect to the NGINX provider. Either select an existing agent or create a new one as described in [Adding and Configuring an Agent: BIG-IP and NGINX](#).

4. The *Secrets* field is then displayed. From the *Secrets* drop-down list, choose the secret to use and click **Continue**.



Add Providers

Providers are remote instances that provide WAF services, such as NGINX App Protect and BIG-IP AWAF.

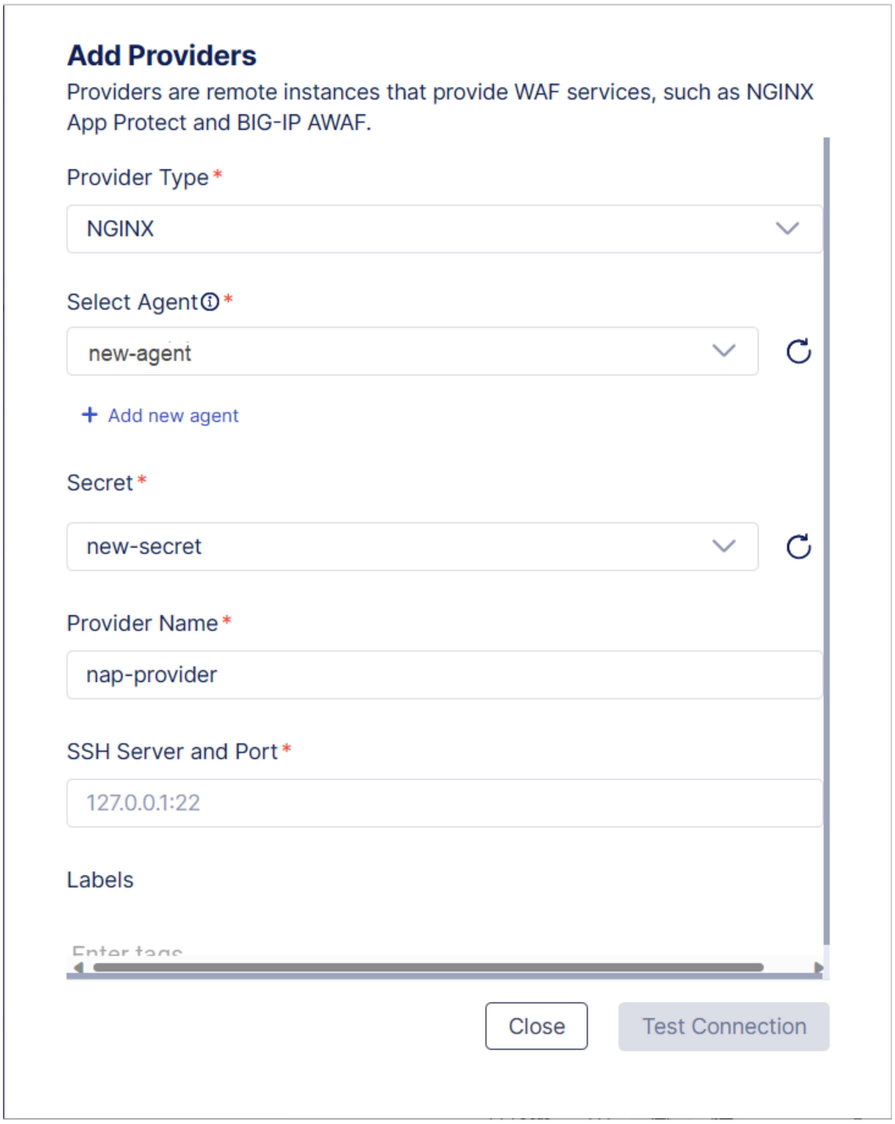
Provider Type *: NGINX

Select Agent *: new-agent

Secrets *: new-secret

5. The remaining fields are then displayed. In the *Provider Name* field, enter a name for this provider.

6. In the *SSH Server and Port* field, enter the IP address of the Nginx instance, and the ssh port number in the following format: `<ssh_server_ip>:<ssh_port>`



Add Providers

Providers are remote instances that provide WAF services, such as NGINX App Protect and BIG-IP AWAF.

Provider Type *: NGINX

Select Agent *: new-agent

Secret *: new-secret

Provider Name *: nap-provider

SSH Server and Port *: 127.0.0.1:22

Labels: Enter tags

Note: The *SSH Server and Port* field contains placeholder text with an example of the required data format.

7. In the *Labels* field, optionally add some label tags if you would like to have user-generated text that can be used to search for and organize your providers.

8. Click **Test Connection** and wait for the connection processes to complete between Policy Supervisor and the provider.

9. When the connection has completed, a *Success* message is displayed showing the connection details. From here you can add another provider or return to the *Providers Overview* page.

Adding a Distributed Cloud Provider

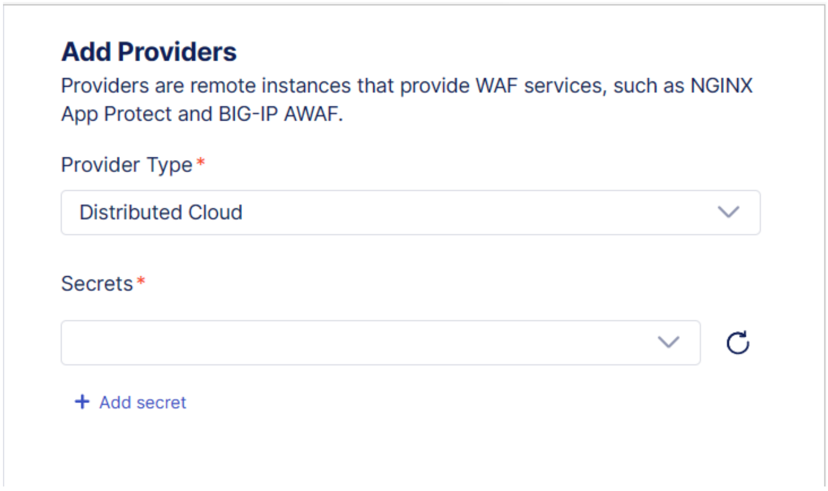
When you add a provider of type Distributed Cloud, you are setting up a connection to a Distributed Cloud namespace, to which you can then deploy policy files and configurations. Distributed Cloud namespaces are on a more open internet platform; therefore, you connect to Policy Supervisor via a global agent and secret to begin communication.

Unlike the other two provider types, you don't need to install an agent behind a private network for a Distributed Cloud instance. The agent for Distributed Cloud is stored on the Policy Supervisor system, and you set up an API credential and secret for connecting to the platform. For information on generating the API Token credential, see the following section: Generating a Distributed Cloud API Token credential.

To add a Distributed Cloud provider, complete the following steps.

1. On the *Providers* page, click **Add Provider**. If this is the first provider across all provider types being added, there are two Add Provider buttons on the screen.

2. On the *Add Providers* pane, click the *Provider Type* drop-down and choose **Distributed Cloud** from the list.



Add Providers

Providers are remote instances that provide WAF services, such as NGINX App Protect and BIG-IP AWAF.

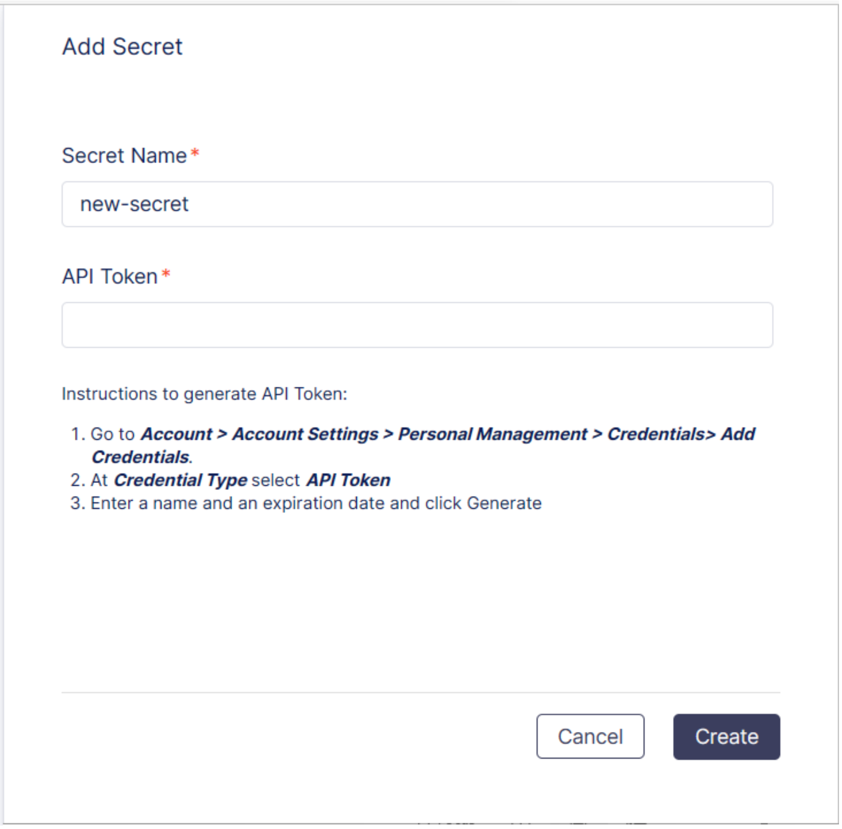
Provider Type*

Distributed Cloud

Secrets*

3. Select a secret from the Secrets drop-down list or add a new secret. To add a new secret, click **+ Add secret,** which opens the *Add Secret* pane.

4. Enter a name for this secret in the *Secret Name* field.



Add Secret

Secret Name*

new-secret

API Token*

Instructions to generate API Token:

1. Go to ***Account > Account Settings > Personal Management > Credentials> Add Credentials***.
2. At ***Credential Type*** select ***API Token***
3. Enter a name and an expiration date and click Generate

5. In the *API Token* field, enter the generated token from your account in the Distributed Cloud console, as described in Generating a Distributed Cloud API Token credential.

6. Once you have entered the API Token, click **Create**.

7. When you return to the *Add Providers* pane, choose your new secret from the *Secrets* drop-down list, and click **Continue**.
   Note: Click the *Refresh* button to update the Secrets list with the new secret.

8. Add a name for this provider instance, and enter the URL for your F5 Distributed Cloud tenant, typically in the following format:
   https://your_tenant.console.ves.volterra.io/

9. In the *Labels* field, optionally add some label tags if you would like to have user-generated text that can be used to search for and organize your Providers.

10. Click **Test Connection** and wait for the connection processes to complete between Policy Supervisor and the provider.

11. When the connection has completed, a *Success* message is displayed showing the connection details. From here you can add another provider or return to the *Providers Overview* page.

Adding and Configuring an Agent: BIG-IP and NGINX

Before you can add a BIG-IP or NGINX provider instance in Policy Supervisor, you must set up an "Agent" on the private network where the provider is running to ensure a secure connection between Policy Supervisor and the provider.

- Ensure you have a machine or VM with Linux OS with an outbound connection located on the same network as the BIG-IP or NGINX instance that you'd like to use as a Provider in Policy Supervisor.
- The Policy Supervisor "Agent" is a Linux binary that is first installed on this machine/VM and is registered using a unique token generated in the Policy Supervisor UI for your Policy Supervisor workspace only.
- The Agent is used to create "Secrets", which are stored in your environment only and are not transmitted outside of your network.
- These secrets are used to connect to your BIG-IP AWAF or NGINX NAP instance to execute various policy-related functions within a Docker container environment on that machine/VM.
- Ensure that Docker and wget are installed on your Linux machine/VM.

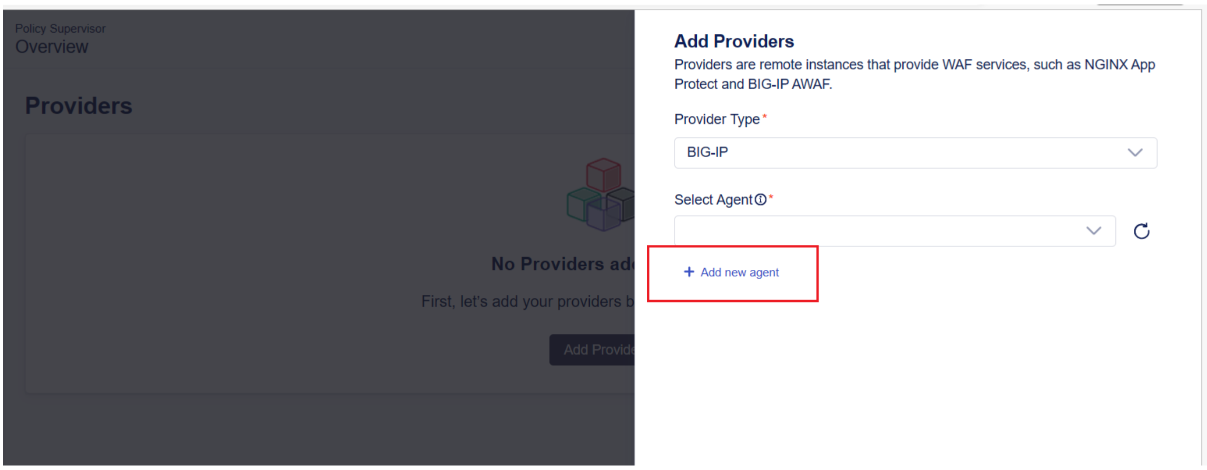
Adding and configuring an agent consists of the following sections:

- Download the agent-installer package
- Run the installer and configure the agent
- Set up the agent options

Download the agent-installer package

To download the installer package, complete the following steps:

1. On the **Add Providers** pane on Policy Supervisor, having selected the provider type of *BIG-IP* or *NGINX*, in the *Select Agent* section click **+ Add new agent**.



Add Providers

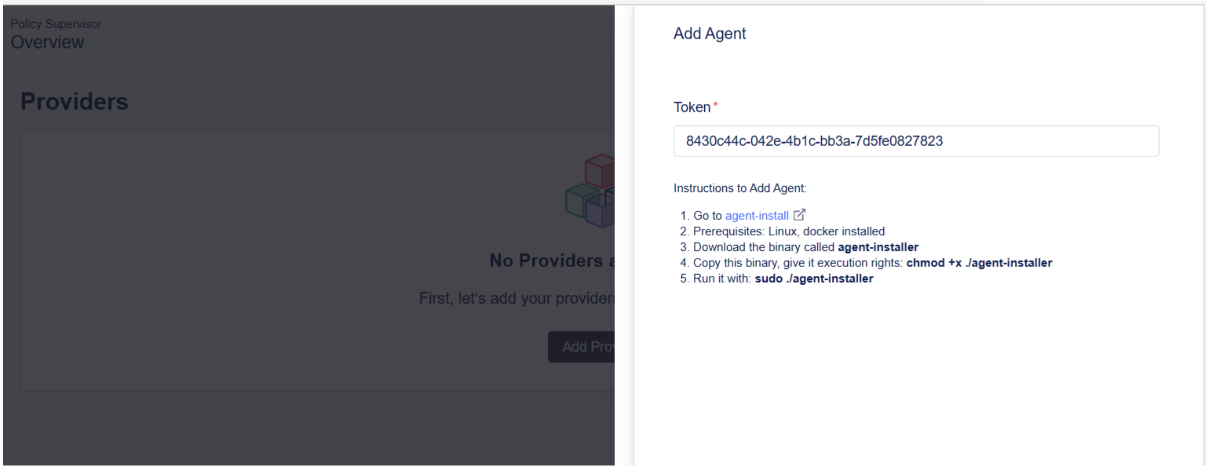
Providers are remote instances that provide WAF services, such as NGINX App Protect and BIG-IP AWAF.

Provider Type *

BIG-IP

Select Agent *

2. An *Add Agent* pane slides out, with a token generated as a long text string. Copy and paste the Token to a text file to be used later.



Add Agent

Token *

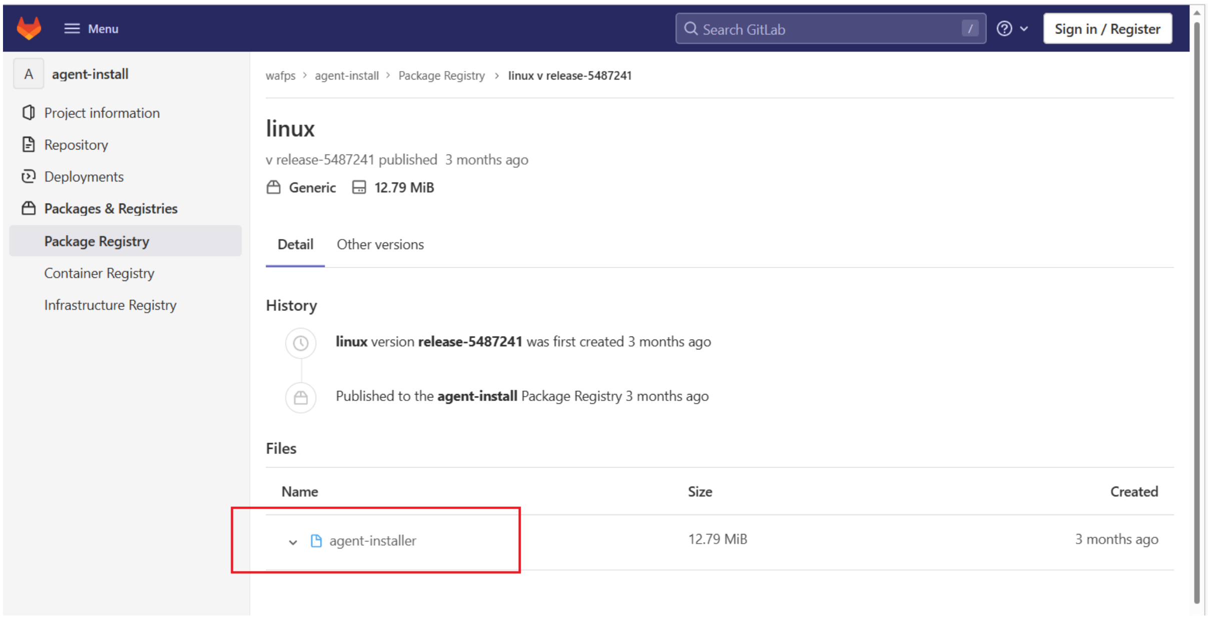
8430c44c-042e-4b1c-bb3a-7d5fe0827823

Instructions to Add Agent:

1. Go to agent-install
2. Prerequisites: Linux, docker installed
3. Download the binary called **agent-installer**
4. Copy this binary, give it execution rights: **chmod +x ./agent-installer**
5. Run it with: **sudo ./agent-installer**

3. In the *Add Agent* pane, click the **agent-install** link to open the GitLab repository.

4. On the *gitlab.policysupervisor.io* site, right-click on the **agent-installer** file name and select **Copy Link**.



linux

v release-5487241 published 3 months ago

Generic 12.79 MiB

History

linux version **release-5487241** was first created 3 months ago

Published to the **agent-install** Package Registry 3 months ago

Files

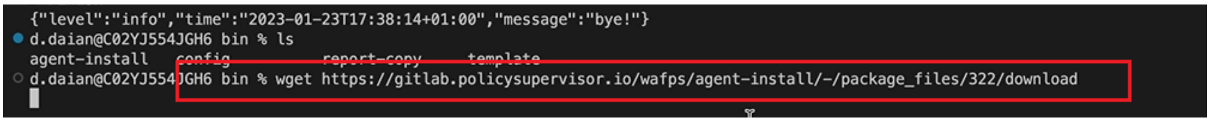
Name	Size	Created
agent-installer	12.79 MiB	3 months ago

The following URL is copied to your clipboard: *https://gitlab.policysupervisor.io/wafps/agent-install/-/package_files/322/download*

5. Go to your Linux machine (navigate to it on an AWS virtual machine, or through puTTy for example), which is on the same network as your BIG-IP or NGINX instance.

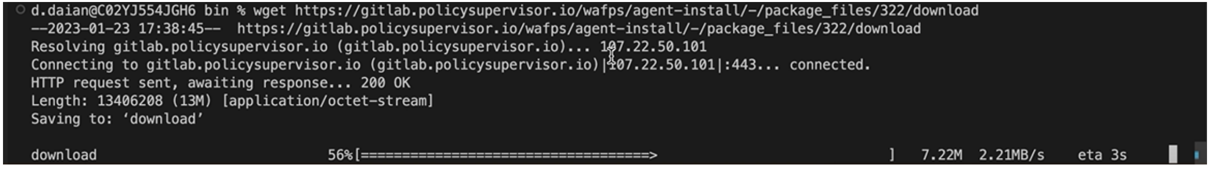
6. Download the installer via the command line by using the `wget` command and the GitLab URL:

```
wget https://gitlab.policysupervisor.io/wafps/agent-install/-
/package_files/322/download
```



```
{"level":"info","time":"2023-01-23T17:38:14+01:00","message":"bye!"}
d.daian@C02YJ554JGH6 bin % ls
agent-install   config          report-copy     template
d.daian@C02YJ554JGH6 bin % wget https://gitlab.policysupervisor.io/wafps/agent-install/-/package_files/322/download
```

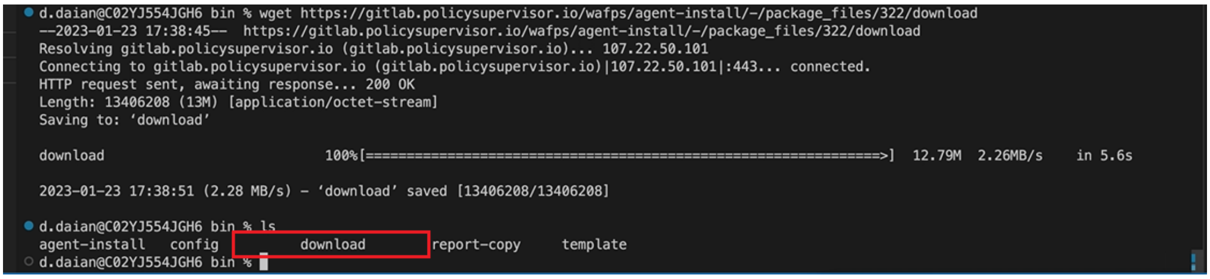
7. Wait for the package to download.



```
d.daian@C02YJ554JGH6 bin % wget https://gitlab.policysupervisor.io/wafps/agent-install/-/package_files/322/download
--2023-01-23 17:38:45--  https://gitlab.policysupervisor.io/wafps/agent-install/-/package_files/322/download
Resolving gitlab.policysupervisor.io (gitlab.policysupervisor.io)... 107.22.50.101
Connecting to gitlab.policysupervisor.io (gitlab.policysupervisor.io)|107.22.50.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13406208 (13M) [application/octet-stream]
Saving to: ‘download’

download                     56%[==================================>                          ]   7.22M  2.21MB/s    eta 3s
```

8. When the package is downloaded, use the `ls` command to show the downloaded package, which is shown as `download`.



```
d.daian@C02YJ554JGH6 bin % wget https://gitlab.policysupervisor.io/wafps/agent-install/-/package_files/322/download
--2023-01-23 17:38:45--  https://gitlab.policysupervisor.io/wafps/agent-install/-/package_files/322/download
Resolving gitlab.policysupervisor.io (gitlab.policysupervisor.io)... 107.22.50.101
Connecting to gitlab.policysupervisor.io (gitlab.policysupervisor.io)|107.22.50.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13406208 (13M) [application/octet-stream]
Saving to: ‘download’

download                    100%[==================================================================>]  12.79M  2.26MB/s    in 5.6s

2023-01-23 17:38:51 (2.28 MB/s) - ‘download’ saved [13406208/13406208]

d.daian@C02YJ554JGH6 bin % ls
agent-install   config          download        report-copy     template
d.daian@C02YJ554JGH6 bin %
```

You will rename it from `download` in the next section.

Run the installer and configure the agent

When the package has downloaded, use the following commands to run the agent installation.

1. Rename the downloaded package from `download` to `agent-installer` by using the following command:

   ```
   mv download agent-installer
   ```

   List the directory contents again, and verify that the package is now displayed as `agent-installer`

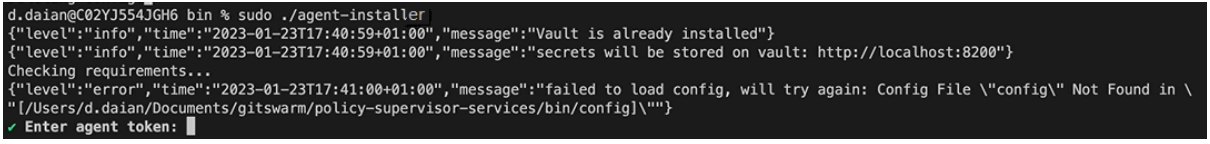
2. Next, give the installer package execution rights to enable it to run:

   ```
   chmod +x ./agent-installer
   ```

3. Then, go ahead and run the agent installer by using the following command:

   ```
   sudo ./agent-installer
   ```

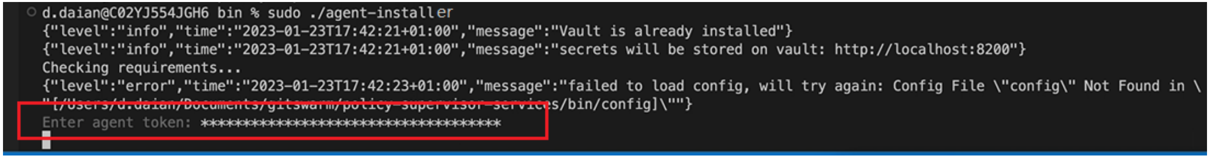
   Some messages are displayed while the agent installer is running.



```
d.daian@C02YJ554JGH6 bin % sudo ./agent-installer
{"level":"info","time":"2023-01-23T17:40:59+01:00","message":"Vault is already installed"}
{"level":"info","time":"2023-01-23T17:40:59+01:00","message":"secrets will be stored on vault: http://localhost:8200"}
Checking requirements...
{"level":"error","time":"2023-01-23T17:41:00+01:00","message":"failed to load config, will try again: Config File \"config\" Not Found in \
"[/Users/d.daian/Documents/gitswarm/policy-supervisor-services/bin/config]\""}
✓ Enter agent token:
```

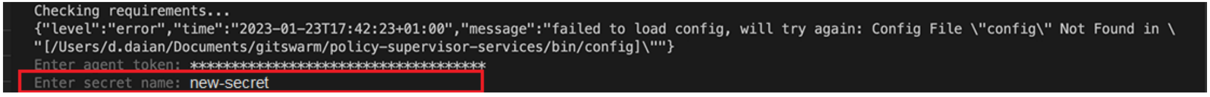
4. You are then prompted to enter the agent token.
   Note: This step is only required when running the installer for the first time.

Copy the agent token from the *Add Agent* screen on Policy Supervisor, or the text file where you pasted it previously, and paste it here.



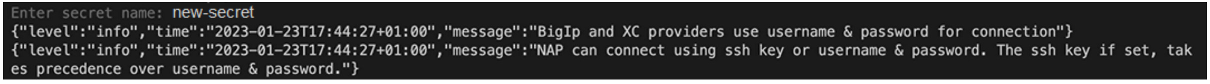
```
○ d.daian@C02YJ554JGH6 bin % sudo ./agent-installer
  {"level":"info","time":"2023-01-23T17:42:21+01:00","message":"Vault is already installed"}
  {"level":"info","time":"2023-01-23T17:42:21+01:00","message":"secrets will be stored on vault: http://localhost:8200"}
  Checking requirements...
  {"level":"error","time":"2023-01-23T17:42:23+01:00","message":"failed to load config, will try again: Config File \"config\" Not Found in \
  "[/Users/d.daian/Documents/gitswarm/policy-supervisor-services/bin/config]\""}
  Enter agent token: ************************************
```

5. Create the secret that will store the credentials to connect to the provider. Enter a name for the secret, which must be a unique secret name that hasn't been used before.



```
Checking requirements...
{"level":"error","time":"2023-01-23T17:42:23+01:00","message":"failed to load config, will try again: Config File \"config\" Not Found in \
"[/Users/d.daian/Documents/gitswarm/policy-supervisor-services/bin/config]\""}
Enter agent token: ************************************
Enter secret name: new-secret
```

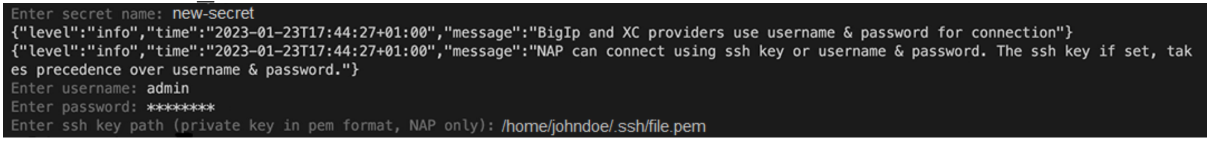
6. Informational messages are displayed for the connection and authentication methods to different providers.



```
Enter secret name: new-secret
{"level":"info","time":"2023-01-23T17:44:27+01:00","message":"BigIp and XC providers use username & password for connection"}
{"level":"info","time":"2023-01-23T17:44:27+01:00","message":"NAP can connect using ssh key or username & password. The ssh key if set, tak
es precedence over username & password."}
```

Note: For NGINX, you must have generated an ssh public and private key, with the public key placed on your remote Nginx App Protect instance. The private key is located on the Linux machine/VM where you are creating the agent. All ssh key and certificate details are normally stored in `.pem` format on the Linux machine. In the next step, you enter the path to this `.pem` file, so that it will be used when connecting Policy Supervisor to the NGINX instance.

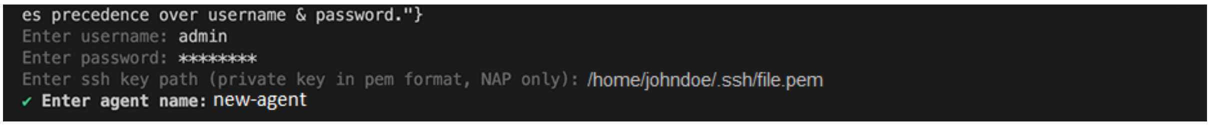
7. Enter the username and password that will be stored in the secret, and for NGINX, the path to the `.pem` file containing the ssh key details, for example, `/home/<your_name>/.ssh/file.pem`



```
Enter secret name: new-secret
{"level":"info","time":"2023-01-23T17:44:27+01:00","message":"BigIp and XC providers use username & password for connection"}
{"level":"info","time":"2023-01-23T17:44:27+01:00","message":"NAP can connect using ssh key or username & password. The ssh key if set, tak
es precedence over username & password."}
Enter username: admin
Enter password: ********
Enter ssh key path (private key in pem format, NAP only): /home/johndoe/.ssh/file.pem
```

Note: The username and password you enter here are the credentials that you use when you are logging in to the BIG-IP Configuration Utility.

8. You can then assign the name for the agent, which is the name that will be displayed when selecting it in the *Add Provider* screen.



```
es precedence over username & password."}
Enter username: admin
Enter password: ********
Enter ssh key path (private key in pem format, NAP only): /home/johndoe/.ssh/file.pem
✓ Enter agent name: new-agent
```

9. When you assign the agent name, the installation continues.

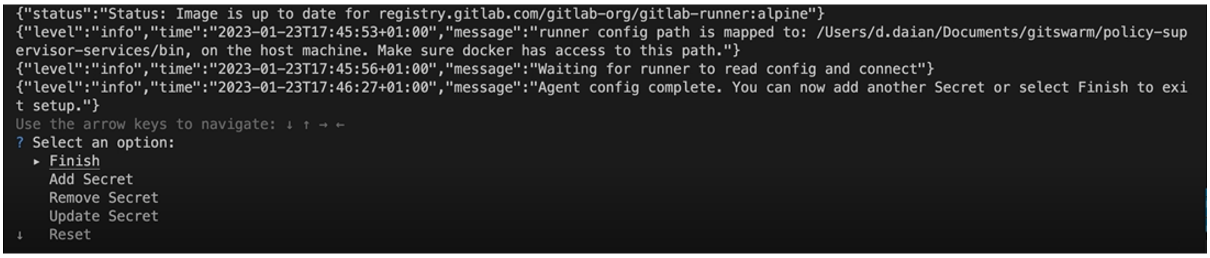
   When the installation is completed, you are then provided with some additional setup options for the agent.

Complete the setup and agent options

When you have downloaded and run the *agent-installer*, there are some additional setup options to complete for the agent installation.

1. The following setup options are displayed:

   ```
   Finish
   Add Secret
   Remove Secret
   Update Secret
   Reset
   View
   ```

   ```
   {"status":"Status: Image is up to date for registry.gitlab.com/gitlab-org/gitlab-runner:alpine"}
   {"level":"info","time":"2023-01-23T17:45:53+01:00","message":"runner config path is mapped to: /Users/d.daian/Documents/gitswarm/policy-sup
   ervisor-services/bin, on the host machine. Make sure docker has access to this path."}
   {"level":"info","time":"2023-01-23T17:45:56+01:00","message":"Waiting for runner to read config and connect"}
   {"level":"info","time":"2023-01-23T17:46:27+01:00","message":"Agent config complete. You can now add another Secret or select Finish to exi
   t setup."}
   Use the arrow keys to navigate: ↓ ↑ → ←
   ? Select an option:
     ▸ Finish
       Add Secret
       Remove Secret
       Update Secret
   ↓   Reset
   ```

2. Use the arrow keys to navigate and select each option:

   `Finish` – completes the agent installation and exits the process.

   `Add Secret` – allows you to add another secret to the agent, whereby you would enter an additional secret name, with another username and password.

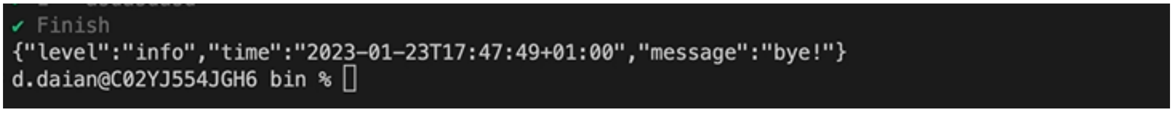
   `Remove Secret` – displays the existing secrets for this agent, and enables you to select one and remove it.

   `Update Secret` - displays the existing secrets for this agent, and enables you to select one and update it. For example, change the secret name, username, and/or password.

   `Reset` – removes the agent completely.

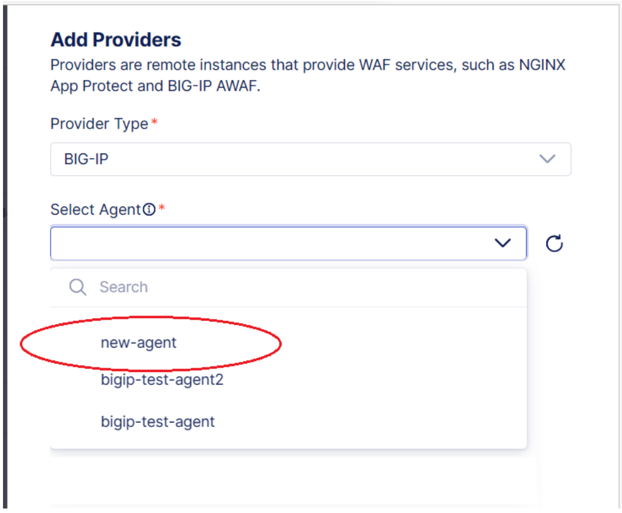
   `View` - this shows the name and workspace from Policy Supervisor for this agent, for example 'Firstname Surname - C Workspace test'.

3. When you select `Finish` on the list of options, the agent installation is completed.

   ```
   ✔ Finish
   {"level":"info","time":"2023-01-23T17:47:49+01:00","message":"bye!"}
   d.daian@C02YJ554JGH6 bin % ▯
   ```

4. Your agent will now be available for selection in the *Select Agent* drop-down list when you add a provider in Policy Supervisor, and the associated secrets in the *Secrets* drop-down list.



Add Providers

Providers are remote instances that provide WAF services, such as NGINX App Protect and BIG-IP AWAF.

Provider Type *

BIG-IP

Select Agent ⓘ *

Search

new-agent

bigip-test-agent2

bigip-test-agent

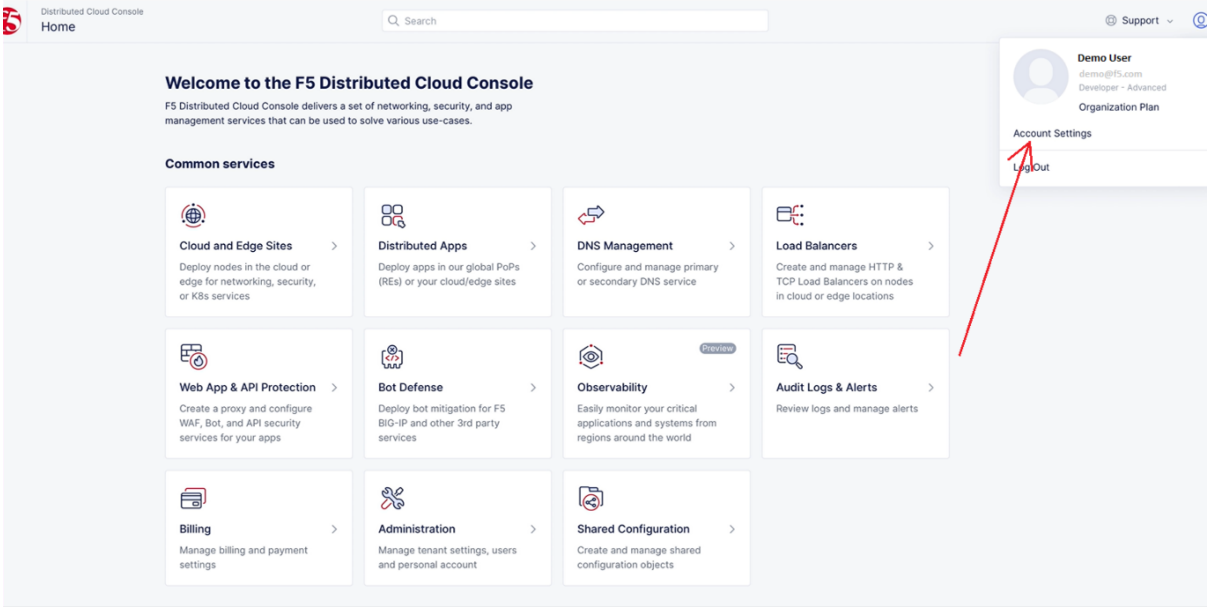
Generating a Distributed Cloud API Token credential

Distributed Cloud providers are on an open internet connection; therefore, they don't need an agent installed and configured on a private network. However, there is a requirement to set up a secret before you can connect to a Distributed Cloud provider in Policy Supervisor.

As part of the secret setup, you must first generate an API Token credential in the Distributed Cloud console. To generate this token credential, complete the following steps.

1. Log on to the *F5 Distributed Cloud UI*.

2. Go to your *User Account* menu and click **Account Settings**.



Welcome to the F5 Distributed Cloud Console

F5 Distributed Cloud Console delivers a set of networking, security, and app management services that can be used to solve various use-cases.

Common services

Cloud and Edge Sites: Deploy nodes in the cloud or edge for networking, security, or K8s services

Distributed Apps: Deploy apps in our global PoPs (REs) or your cloud/edge sites

DNS Management: Configure and manage primary or secondary DNS service

Load Balancers: Create and manage HTTP & TCP Load Balancers on nodes in cloud or edge locations

Web App & API Protection: Create a proxy and configure WAF, Bot, and API security services for your apps

Bot Defense: Deploy bot mitigation for F5 BIG-IP and other 3rd party services

Observability (Preview): Easily monitor your critical applications and systems from regions around the world

Audit Logs & Alerts: Review logs and manage alerts

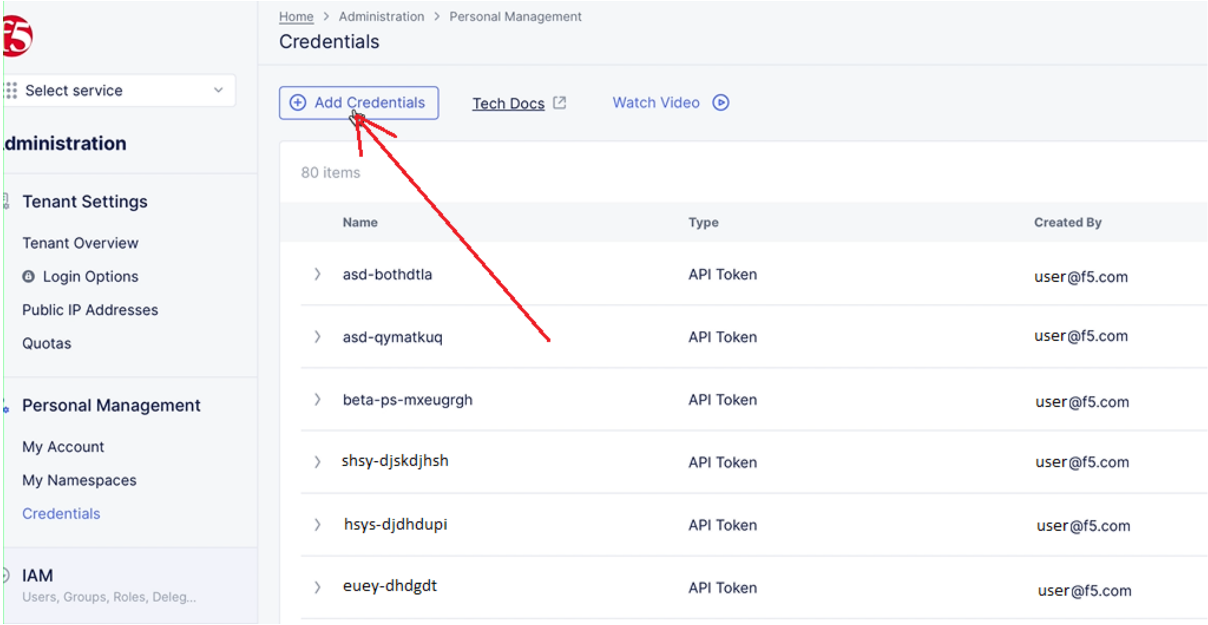
Billing: Manage billing and payment settings

Administration: Manage tenant settings, users and personal account

Shared Configuration: Create and manage shared configuration objects

3. On the *My Account* page, go to the left-hand Administration menu > *Personal Management*, and click **Credentials**.

4. On the *Credentials* page, click the **Add Credentials** button.



Home > Administration > Personal Management

Credentials

Select service

dministration

Tenant Settings

Tenant Overview

Login Options

Public IP Addresses

Quotas

Personal Management

My Account

My Namespaces

Credentials

IAM

Users, Groups, Roles, Deleg...

⊕ Add Credentials   Tech Docs   Watch Video

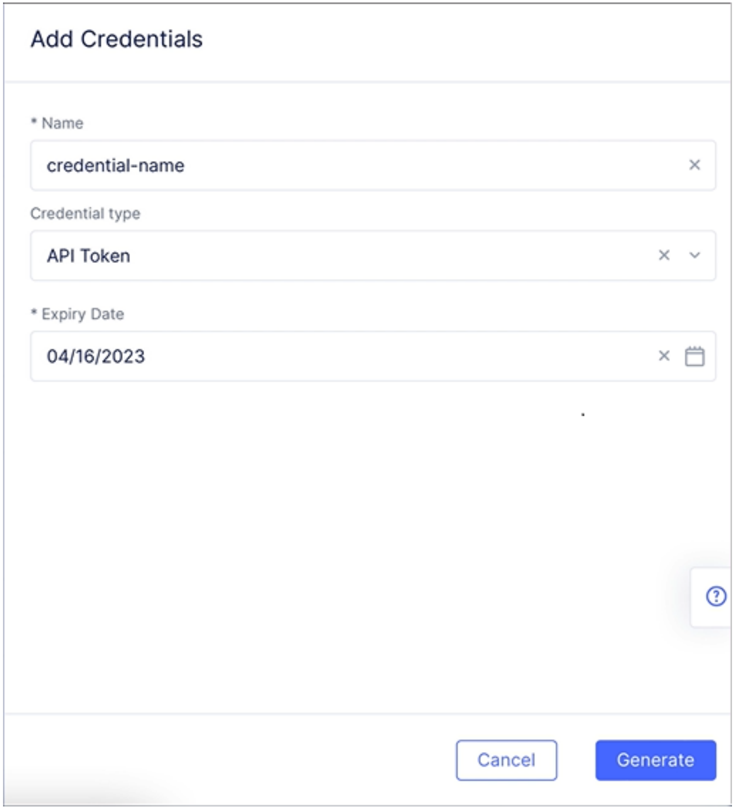
80 items

Name	Type	Created By
asd-bothdtla	API Token	user@f5.com
asd-qymatkuq	API Token	user@f5.com
beta-ps-mxeugrgh	API Token	user@f5.com
shsy-djskdjhsh	API Token	user@f5.com
hsys-djdhdupi	API Token	user@f5.com
euey-dhdgdt	API Token	user@f5.com

The *Add Credentials* pane slides out with fields and details to be completed.

5. Enter a *Name* for the credential and choose *API Token* as the authentication type to be generated, along with an *Expiry Date*.
 - Credential Name
 - Choose API Token
 - Expiry date

6. With *Name*, *Credential type*, and *Expiry Date* selected, click **Generate**.



Add Credentials

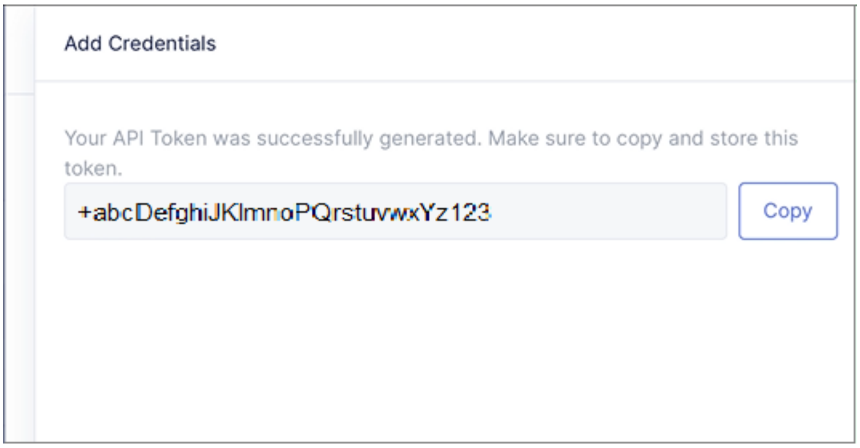
* Name: credential-name

Credential type: API Token

* Expiry Date: 04/16/2023

Cancel   Generate

7. The API token is generated, which you can copy to the clipboard for using in the *Add Provider* setup in Policy Supervisor.



Add Credentials

Your API Token was successfully generated. Make sure to copy and store this token.

+abcDefghiJKlmnoPQrstuvwxYz123

8. Click **close** on the *API token* pane to return to the *Credentials* page.

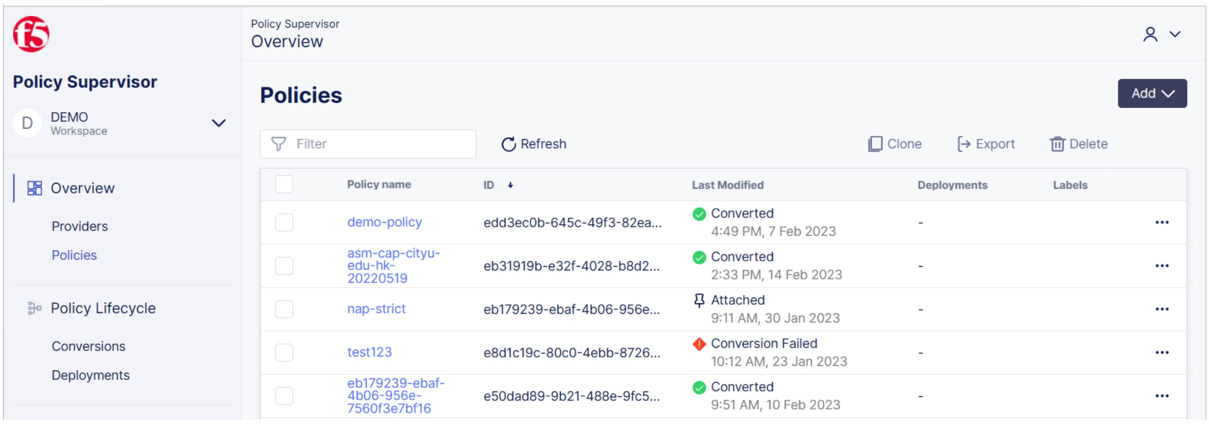
Deleting a provider

You can disconnect from an existing provider and remove it from Policy Supervisor if required. To delete a provider, complete the following steps:

1. On the *Providers* page, click the *Action menu* **(…)** for the provider you want to delete.
2. From the *Action menu*, choose **Delete**.
3. The connection is stopped, and the provider is removed from the *Providers* page.

Policies

The Policies page displays the existing policies that you are working with in Policy Supervisor and enables you to import and add new policies that you can edit and deploy.



□	Policy name	ID	Last Modified	Deployments	Labels	
□	demo-policy	edd3ec0b-645c-49f3-82ea...	Converted 4:49 PM, 7 Feb 2023	-		•••
□	asm-cap-cityu-edu-hk-20220519	eb31919b-e32f-4028-b8d2...	Converted 2:33 PM, 14 Feb 2023	-		•••
□	nap-strict	eb179239-ebaf-4b06-956e...	Attached 9:11 AM, 30 Jan 2023	-		•••
□	test123	e8d1c19c-80c0-4ebb-8726...	Conversion Failed 10:12 AM, 23 Jan 2023	-		•••
□	eb179239-ebaf-4b06-956e-7560f3e7bf16	e50dad89-9b21-488e-9fc5...	Converted 9:51 AM, 10 Feb 2023	-		•••

To add policies to Policy Supervisor, you have the following options:

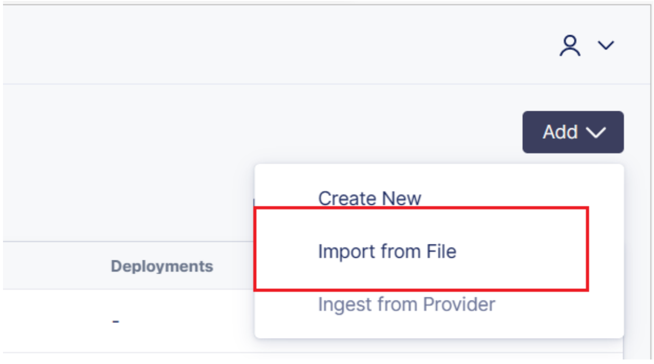
- **Import** a policy from file.
- **Ingest** directly from provider.
- **Create** a new policy.

Importing a Policy from File (BIG-IP, NGINX)

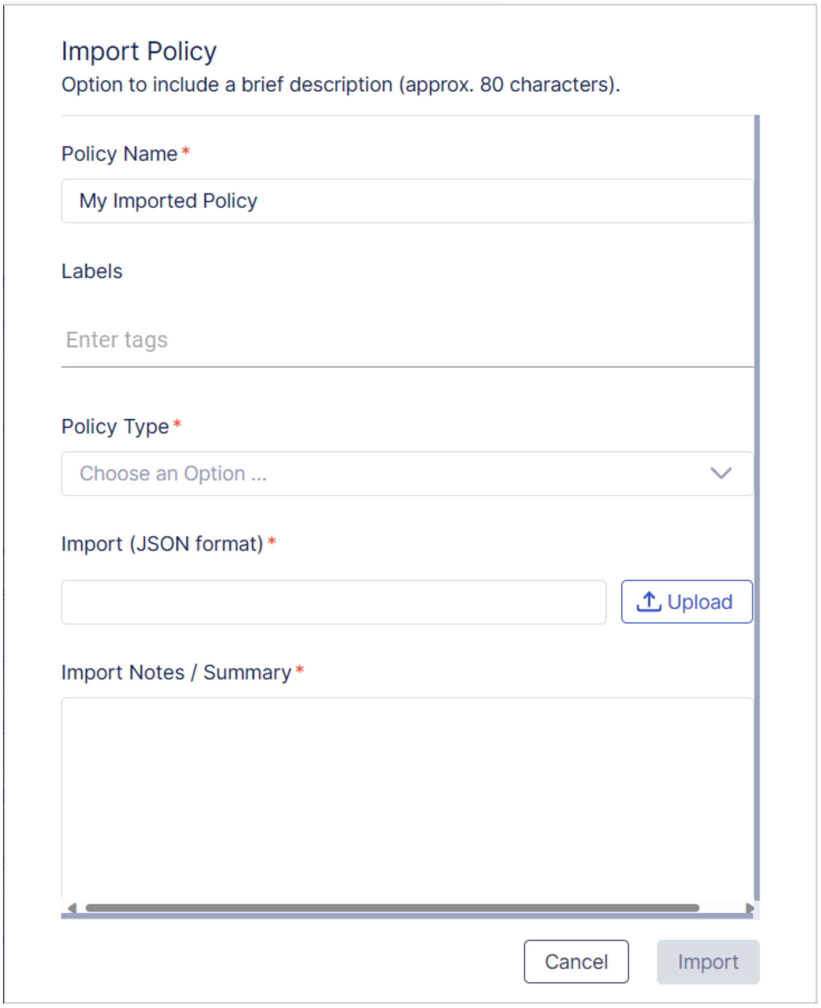
If you have exported policy files from your provider interface such as BIG-IP or NGINX into .JSON format, you can import them to Policy Supervisor for conversion and deployment.

To import a policy from file, complete the following steps:

1. In the top-right corner of the *Policies* page, click the **Add** button and choose *Import from File*.



2. On the *Import Policy* pane, in the *Policy Name* field, enter the name that you want to display for the policy.



Import Policy

Option to include a brief description (approx. 80 characters).

Policy Name *

My Imported Policy

Labels

Enter tags

Policy Type *

Choose an Option ...

Import (JSON format) *

Import Notes / Summary *

3. In the *Policy Type* field, choose **BIG-IP** or **NGINX** from the drop-down list.
   Note: Distributed Cloud policy type isn't supported for file import in the current release.

4. Upload the JSON export of the AWAF or NAP policy by clicking the **Upload** button and browsing to the file on your computer.

5. Add some descriptive notes about the policy in the *Import Notes/Summary* field and click **Import**.
   Note: The text that you enter in the Import Notes/Summary field is used as the name of the Report that is created for the conversion on the Reports page.

6. The files are imported and the conversion to CDP format completes. A conversion summary report displays the policy settings (configurations) that have been successfully converted, partially converted, or not supported. For more information on these details, see Reports.

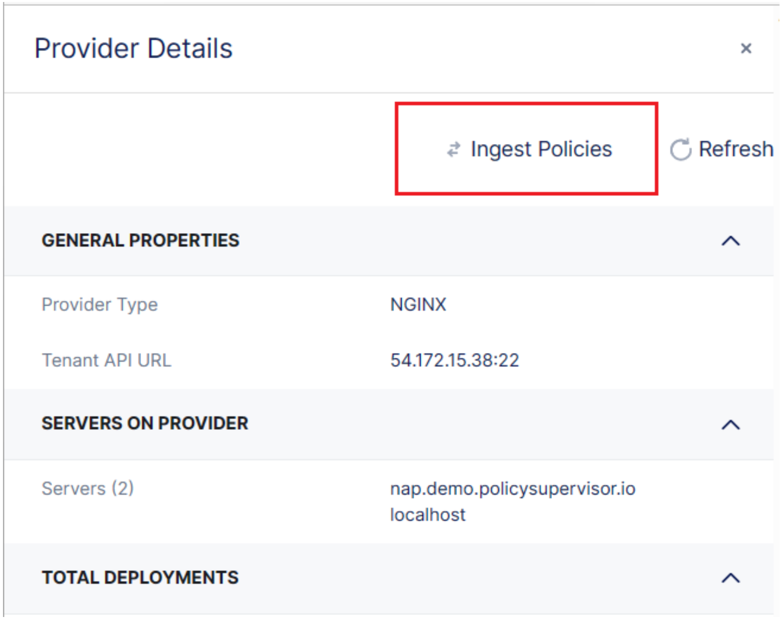
7. At the bottom of the *Conversion Completed* pane, click the **Edit Policy** button to view the imported policy in the Editor. Here you can review and make updates to the imported policy if necessary.

Ingesting a Policy from a Provider (BIG-IP, NGINX)

You can ingest a policy directly from a connected BIG-IP or NGINX provider for conversion and deployment to another provider type.

To ingest a policy from a provider, complete the following steps:

1. On the *Providers* page, click on a provider name to display the *Provider Details* pane and click **Ingest Policies**.



Provider Details

GENERAL PROPERTIES

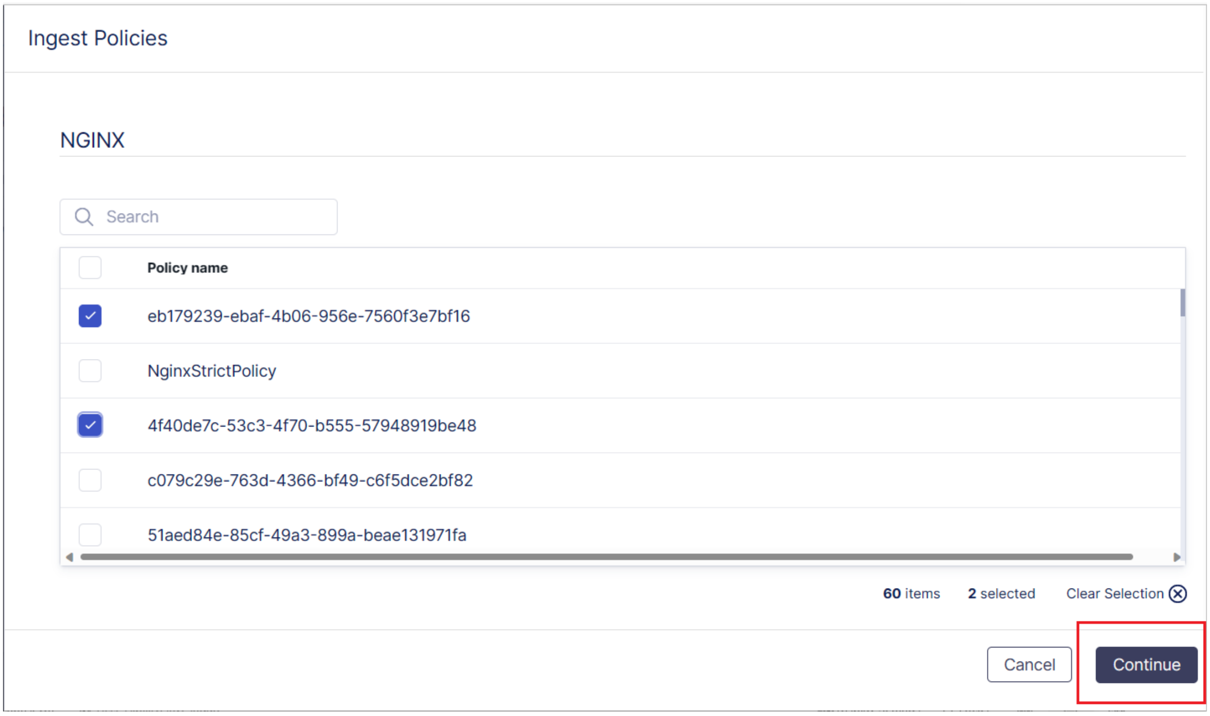
Provider Type	NGINX
Tenant API URL	54.172.15.38:22

SERVERS ON PROVIDER

Servers (2)	nap.demo.policysupervisor.io localhost

TOTAL DEPLOYMENTS

2. On the *Ingest Policies* pane, select one or more policies from the list and click **Continue**.



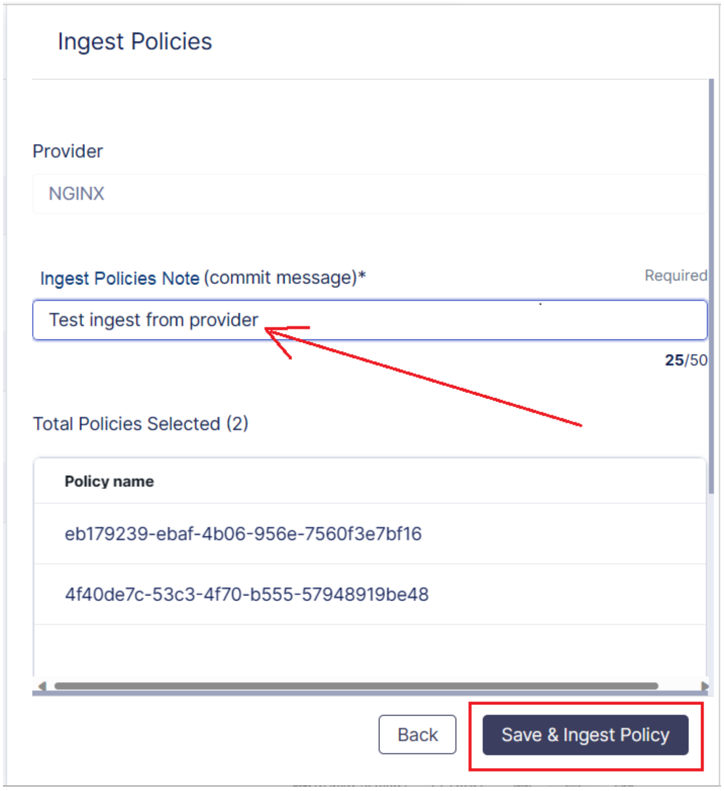
Ingest Policies

NGINX

☐	Policy name
☑	eb179239-ebaf-4b06-956e-7560f3e7bf16
☐	NginxStrictPolicy
☑	4f40de7c-53c3-4f70-b555-57948919be48
☐	c079c29e-763d-4366-bf49-c6f5dce2bf82
☐	51aed84e-85cf-49a3-899a-beae131971fa

60 items **2** selected

3. In the *Ingest Policies Note* field, enter a commit message, and then click **Save & Ingest Policy**.



Ingest Policies

Provider

NGINX

Ingest Policies Note (commit message)* Required

Test ingest from provider

25/50

Total Policies Selected (2)

Policy name
eb179239-ebaf-4b06-956e-7560f3e7bf16
4f40de7c-53c3-4f70-b555-57948919be48

A status page is displayed while connecting to the provider and ingesting the policies.

4. When the policies have been successfully ingested, a *Success* page is displayed with the following options:

- **Ingest Policy report saved as**: *Commit message*; click this commit message text to open

the *Reports* page in a new window.
- **Policies Overview**; click to return to the *Policies* page.
- **View Full Report**; click to open the report details of the ingest and conversion. For more information on report details, see Reports.

Creating a New Policy from Template

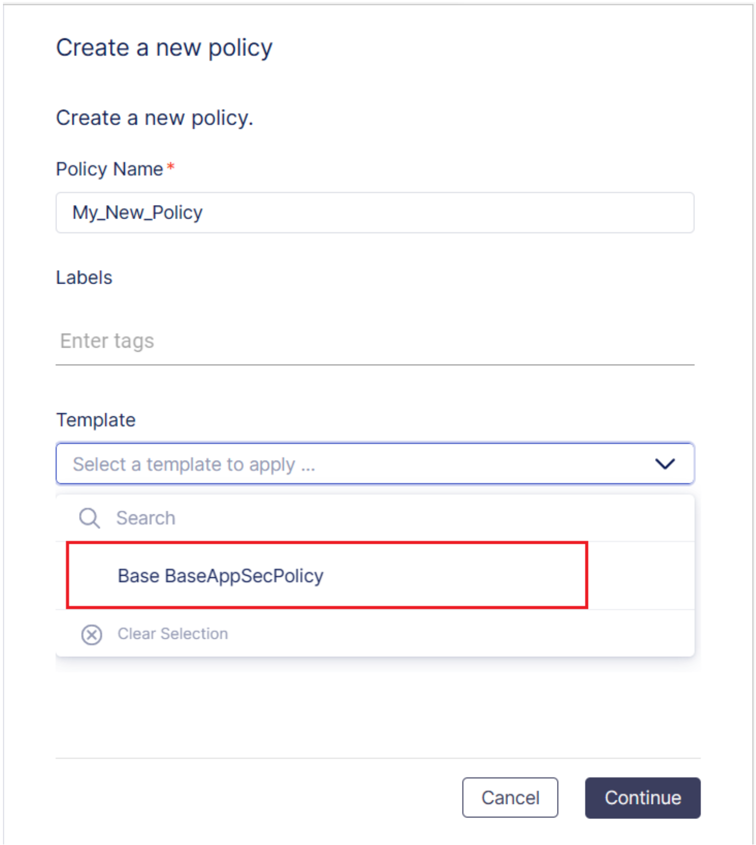
You can create a policy directly in the Policy editor, using the CDP file template to structure the content correctly.

To create a new policy, complete the following steps:

1. In the top-right corner of the *Policies* page, click the **Add** button and choose **Create New**.

2. On the *Create a new policy* pane, enter a name for the new policy.
   Note: The policy name can't contain any spaces.

3. Click the *Template* field and select the template from the drop-down list.



Create a new policy

Create a new policy.

Policy Name*

My_New_Policy

Labels

Enter tags

Template

Select a template to apply ...

4. Add optional tags in the *Labels* field, then click **Continue**.

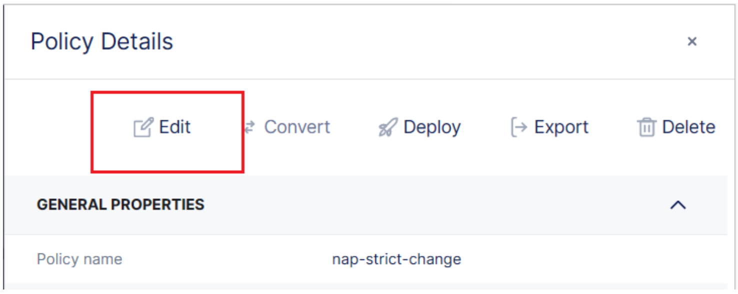
5. The policy editor is displayed in the CDP template format, enabling you to update any configuration details, or copy and paste a valid JSON policy in CDP format.

6. To save the new policy, click **Save**. The policy is then displayed on the *Policies* page.

Working in the Policy Editor

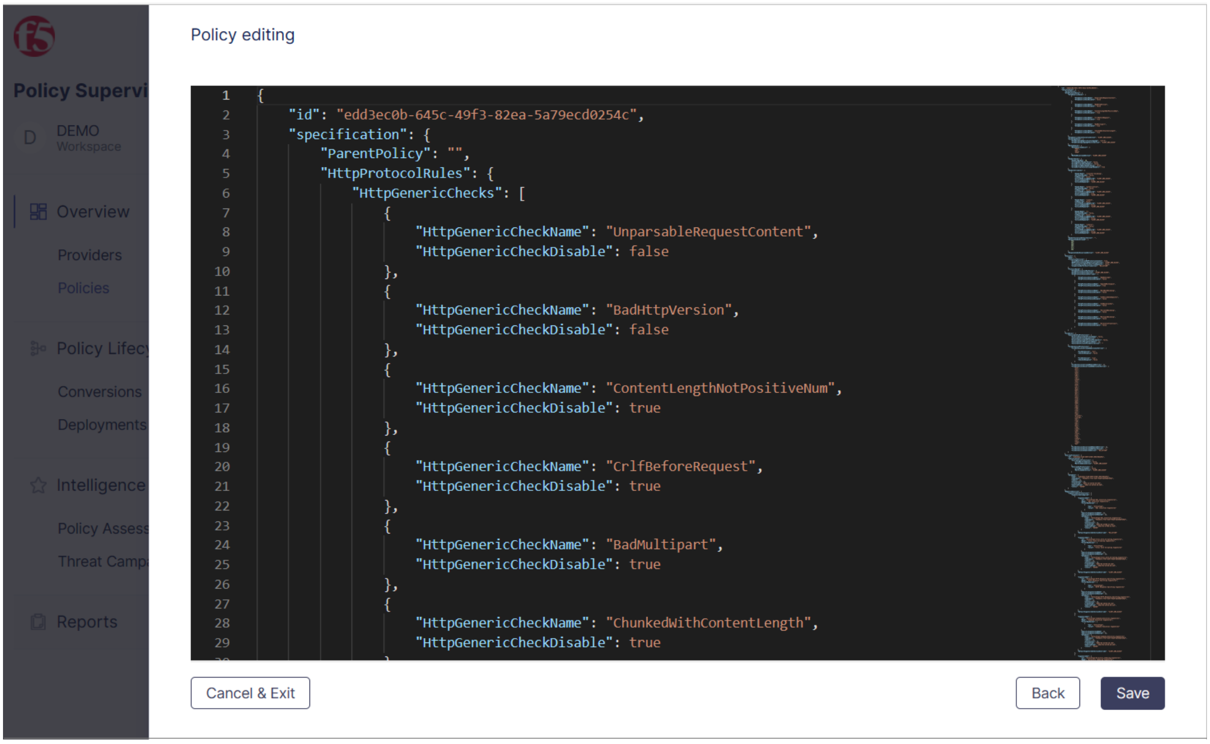
When you import a policy or create a new one, you can make changes to the configurations and settings of the policy in the Policy Editor.

On the *Policies* page, click on a **Policy name** to open the *Policy Details* pane. In the Policy Details pane, click **Edit**.



Policy name nap-strict-change

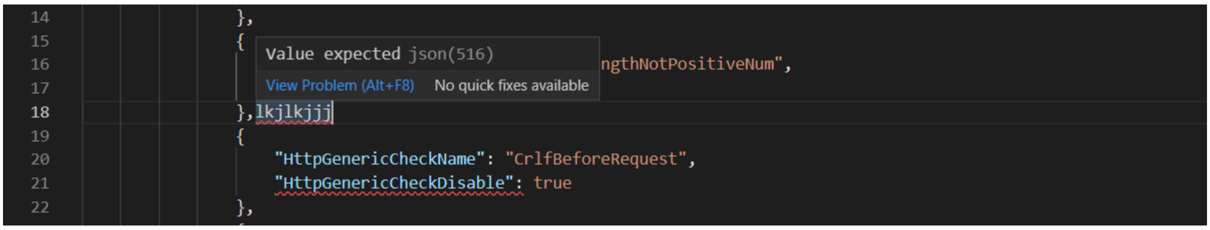
The policy will open in the Policy Editor, enabling you to check the content and make updates if necessary.



```
{
    "id": "edd3ec0b-645c-49f3-82ea-5a79ecd0254c",
    "specification": {
        "ParentPolicy": "",
        "HttpProtocolRules": {
            "HttpGenericChecks": [
                {
                    "HttpGenericCheckName": "UnparsableRequestContent",
                    "HttpGenericCheckDisable": false
                },
                {
                    "HttpGenericCheckName": "BadHttpVersion",
                    "HttpGenericCheckDisable": false
                },
                {
                    "HttpGenericCheckName": "ContentLengthNotPositiveNum",
                    "HttpGenericCheckDisable": true
                },
                {
                    "HttpGenericCheckName": "CrlfBeforeRequest",
                    "HttpGenericCheckDisable": true
                },
                {
                    "HttpGenericCheckName": "BadMultipart",
                    "HttpGenericCheckDisable": true
                },
                {
                    "HttpGenericCheckName": "ChunkedWithContentLength",
                    "HttpGenericCheckDisable": true
```

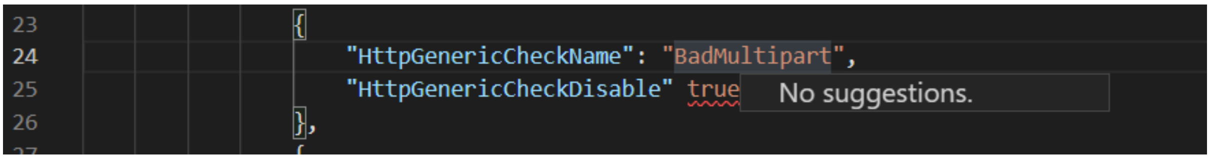
Syntax validation

The policy is displayed in Common Declarative Policy (CDP) format by default in the Policy Editor. When you work on a new policy or make changes to an existing one, your updates are checked automatically using real-time syntax validation.



```
        },
        {
          Value expected json(516)              ngthNotPositiveNum",
          View Problem (Alt+F8)    No quick fixes available
        },lkjlkjjj
        {
          "HttpGenericCheckName": "CrlfBeforeRequest",
          "HttpGenericCheckDisable": true
        },
```

You can check for any information that might be available to further clarify the syntax error with a keypress of `ctrl` and `space`. If there is additional information available a message is displayed, otherwise it shows “No suggestions”.



```
        {
          "HttpGenericCheckName": "BadMultipart",
          "HttpGenericCheckDisable" true   No suggestions.
        },
```

References/Policy IDs

To enable the sharing of certain objects within policies such as Trust Lists and Overlay Protocols, you can add references within a protocol configuration, and this allows the object to be shared by multiple policies.

Every policy must have a Policy ID name/value pair, and this provides the ability to reference the ID from other policies.

Each reference object is given an auto-generated ID, and each policy in a workspace needs a unique name. If a policy that was converted to support references has a name conflict, a new name will be generated by appending a unique string at the end of the policy name.

An overlay protocol has an ID associated with it, enabling the sharing of this item in another policy. **Note**: When a reference is being reused in another policy, these policies must be within the same workspace.

Deleting a Policy

If you no longer need a policy, or it has become corrupt/invalid, you can delete it from Policy Supervisor if required. To delete a policy, complete the following steps:

1. On the *Policies* page, click the **Action menu (…)** for the policy you want to delete.

2. From the menu, choose **Delete**.
   A confirmation dialog box is displayed asking you to confirm that you want to proceed.

3. Click **Delete** on the confirmation dialog. The policy is deleted and is removed from the *Policies* page.

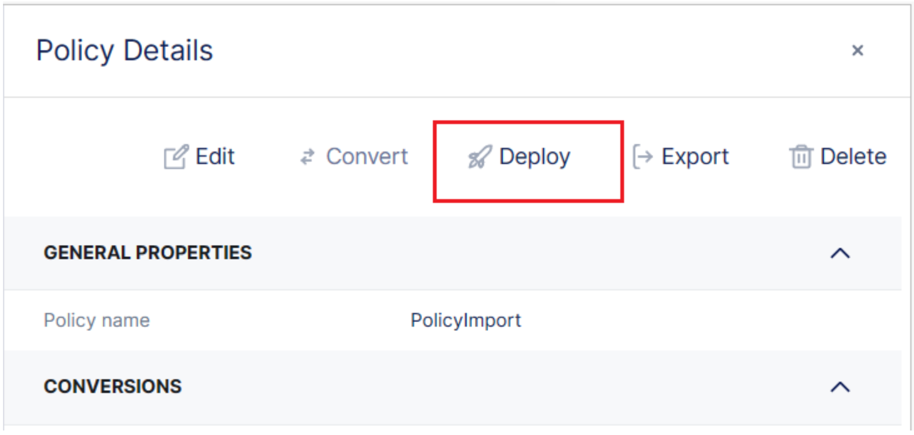
Policy Conversion and Deployment

Valid policies can be deployed from the *Policies* page and attached to BIG-IP, NGINX, and Distributed Cloud providers. When you run the deployment function, the policy is first converted to the target provider type format. If successfully converted, the policy is then deployed and attached to the provider. A report is generated after each conversion.

Deploying a policy: Conversion process

To run the deployment process beginning with the conversion, complete the following steps:

1. On the *Policies* page, select the *Policy name*, and on the *Policy Details* pane, click the **Deploy** button.



Policy Details

GENERAL PROPERTIES

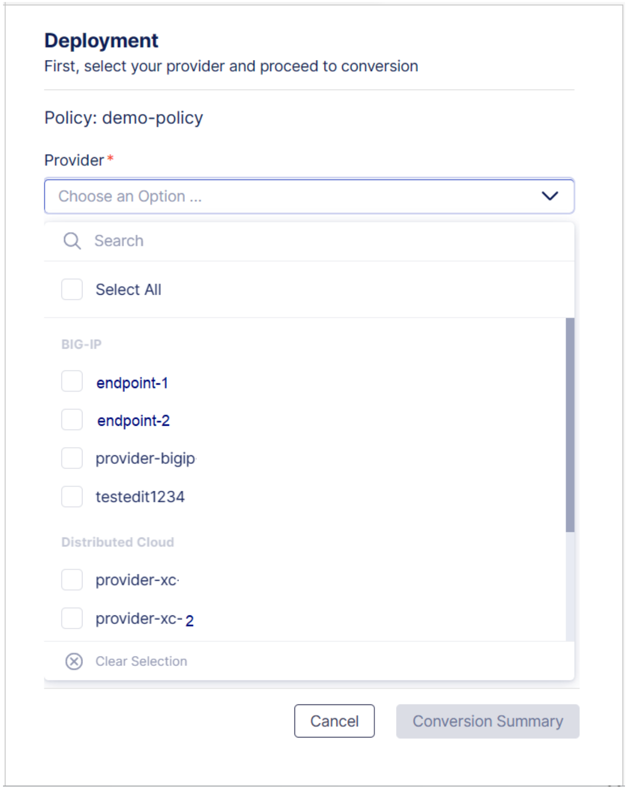
Policy name	PolicyImport

CONVERSIONS

Alternatively, click the **action menu (...)** for the policy and choose **Deploy**.

2. From the resultant *Deployment* page, click the *Provider* drop-down menu.

3. Each virtual server and namespace are shown for the BIG-IP, Distributed Cloud, and NGINX providers respectively. You can select the endpoints that you want to deploy the policy to or *Select All*.



Deployment

First, select your provider and proceed to conversion

Policy: demo-policy

Provider *

Choose an Option ...

□ Select All

BIG-IP

□ endpoint-1

□ endpoint-2

□ provider-bigip

□ testedit1234

Distributed Cloud

□ provider-xc·

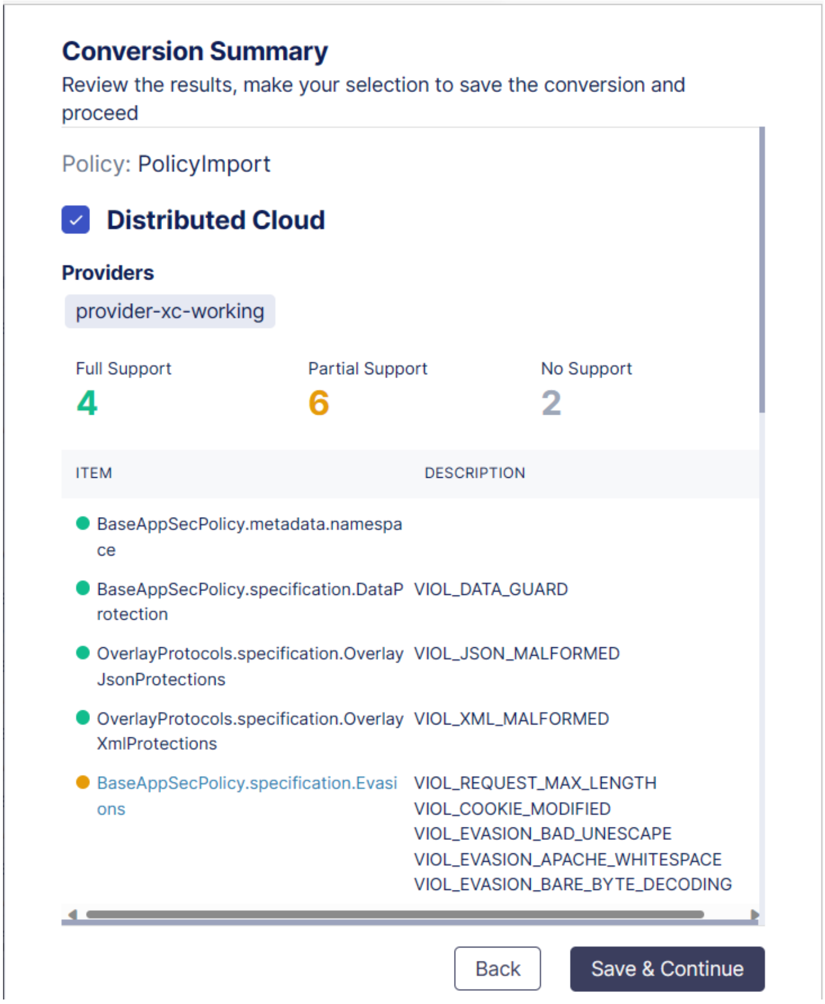
□ provider-xc- 2

4. When you have selected the provider endpoints, click outside the drop-down to close the list. The selected endpoints are displayed as items in the *Provider* field.

5. In the *Deployment Note/Summary* field, enter a commit message for the deployment. **Note**: The text that you enter in the Import Notes/Summary field is used as the name of the report that is created for the deployment on the Reports page.

6. Click **Conversion Summary** to start the conversion process. If you have selected two provider types, it will do the conversion for both. For example, from CDP to AWAF format, and from CDP to Distributed Cloud WAF.

7. On the *Conversion Summary* page, it shows the results for the conversion to the selected provider type. A report is displayed for the conversions, showing the numbers of configuration items that were converted with *Full Support*, *Partial support*, and *No Support*.



Conversion Summary

Review the results, make your selection to save the conversion and proceed

Policy: PolicyImport

☑ **Distributed Cloud**

Providers

provider-xc-working

Full Support	Partial Support	No Support
4	6	2

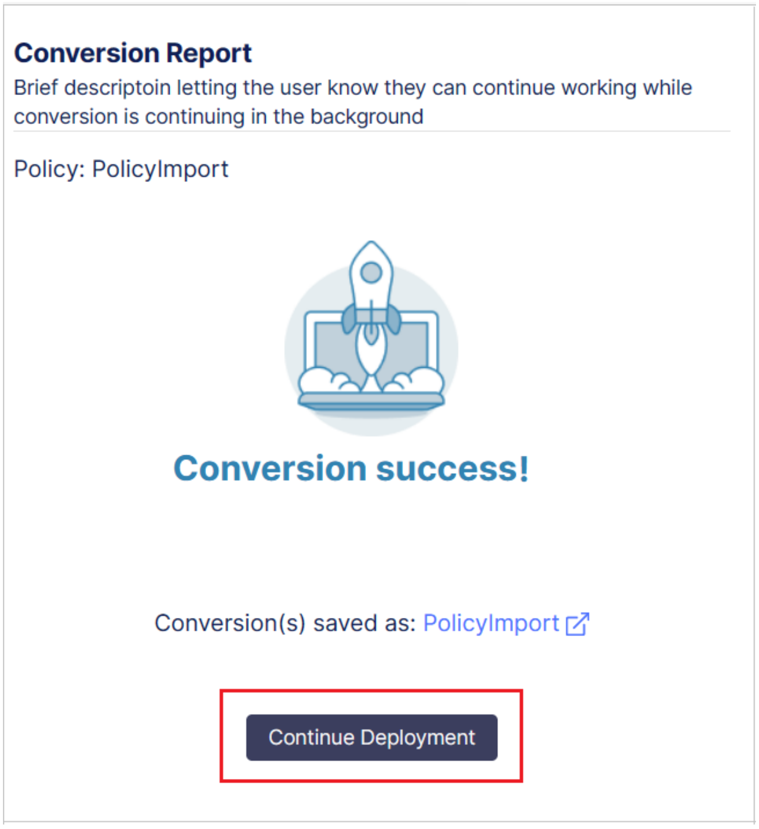
ITEM	DESCRIPTION
● BaseAppSecPolicy.metadata.namespace	
● BaseAppSecPolicy.specification.DataProtection	VIOL_DATA_GUARD
● OverlayProtocols.specification.OverlayJsonProtections	VIOL_JSON_MALFORMED
● OverlayProtocols.specification.OverlayXmlProtections	VIOL_XML_MALFORMED
● BaseAppSecPolicy.specification.Evasions	VIOL_REQUEST_MAX_LENGTH VIOL_COOKIE_MODIFIED VIOL_EVASION_BAD_UNESCAPE VIOL_EVASION_APACHE_WHITESPACE VIOL_EVASION_BARE_BYTE_DECODING

8. Click **Save & Continue** to proceed with the Deployment.

Deploying a policy: Deployment of successful conversion

Upon successful conversion of a policy, continue with the Deployment as follows:

1. On the *Conversion Success* screen, click **Continue Deployment**.



Conversion Report

Brief descriptoin letting the user know they can continue working while conversion is continuing in the background

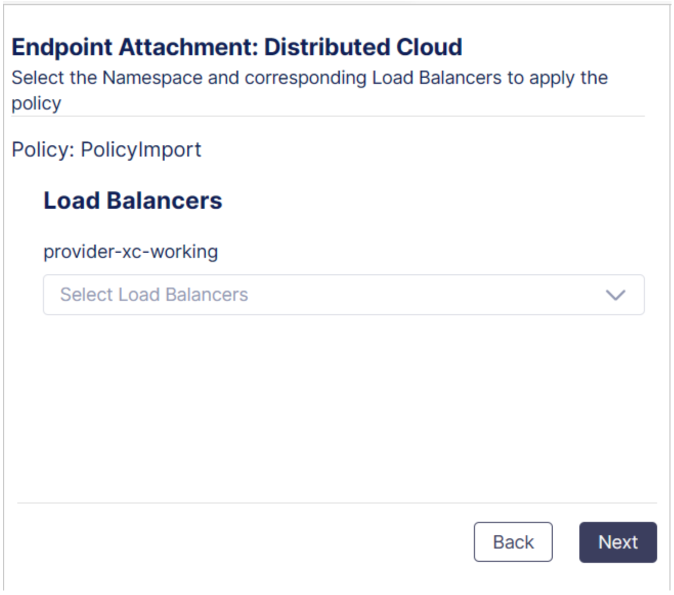
Policy: PolicyImport

Conversion success!

Conversion(s) saved as: PolicyImport

2. The Endpoint Attachment screen will be displayed for the provider type you are deploying to: *Distributed Cloud*, *BIG-IP*, *NGINX*.

3. For *Endpoint Attachment: Distributed Cloud*, click the **Load Balancers** drop-down for the provider, select the load balancer to deploy to and click **Next**.



Endpoint Attachment: Distributed Cloud

Select the Namespace and corresponding Load Balancers to apply the policy

Policy: PolicyImport

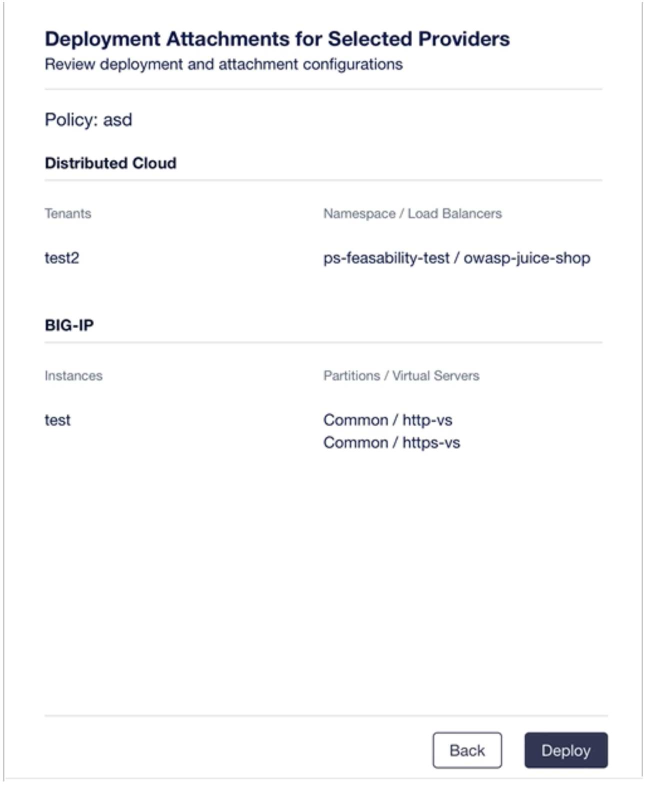
Load Balancers

provider-xc-working

Select Load Balancers

4. For *Endpoint Attachment: BIG-IP*, select the partition and corresponding virtual servers to attach the policy to.

5. On the Deployment Attachments for Selected Providers page, review the tenants and load balancers, and the partitions and virtual servers that you are deploying to, then click **Deploy**.



Deployment Attachments for Selected Providers
Review deployment and attachment configurations

Policy: asd

Distributed Cloud

Tenants	Namespace / Load Balancers
test2	ps-feasability-test / owasp-juice-shop

BIG-IP

Instances	Partitions / Virtual Servers
test	Common / http-vs Common / https-vs

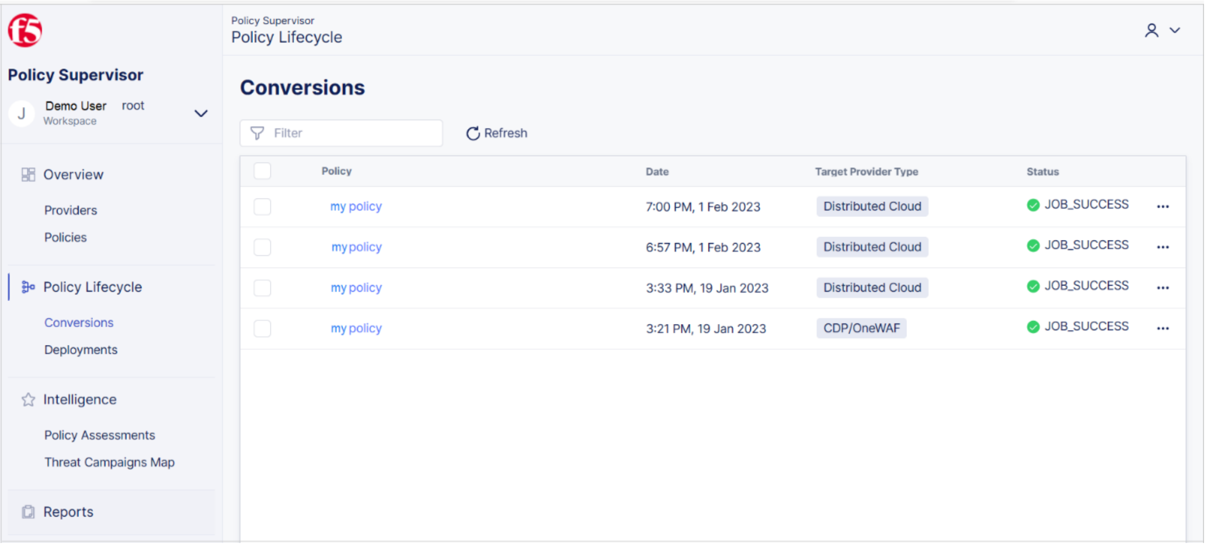
6. A successful deployment is displayed on the *Deployment Completed* page. From here you can click the following options:
   - **Back to Overview**: Returns you to the *Policies* page.
   - **View Report**: Takes you to the *Deployment report*.
   - **Deployment saved as** [policy name]: Takes you to the *Deployments* page for that policy.

Policy Lifecycle

The *Policy Lifecycle* page displays details of the conversions and deployments that have taken place in Policy Supervisor.

Conversions

The *Conversions* page provides a list of all conversions that have taken place for each policy. This includes conversions on imported files to CDP, and subsequent conversions for different provider types.



Policy	Date	Target Provider Type	Status
my policy	7:00 PM, 1 Feb 2023	Distributed Cloud	JOB_SUCCESS
my policy	6:57 PM, 1 Feb 2023	Distributed Cloud	JOB_SUCCESS
my policy	3:33 PM, 19 Jan 2023	Distributed Cloud	JOB_SUCCESS
my policy	3:21 PM, 19 Jan 2023	CDP/OneWAF	JOB_SUCCESS

Each conversion is listed with its *Policy name*, *Date*, *Target Provider Type*, and *Status* of the conversion.

From the **Actions (…) menu** for any conversion that is listed, you can *view the logs* of the conversion, as well as *download the policy* that was converted.

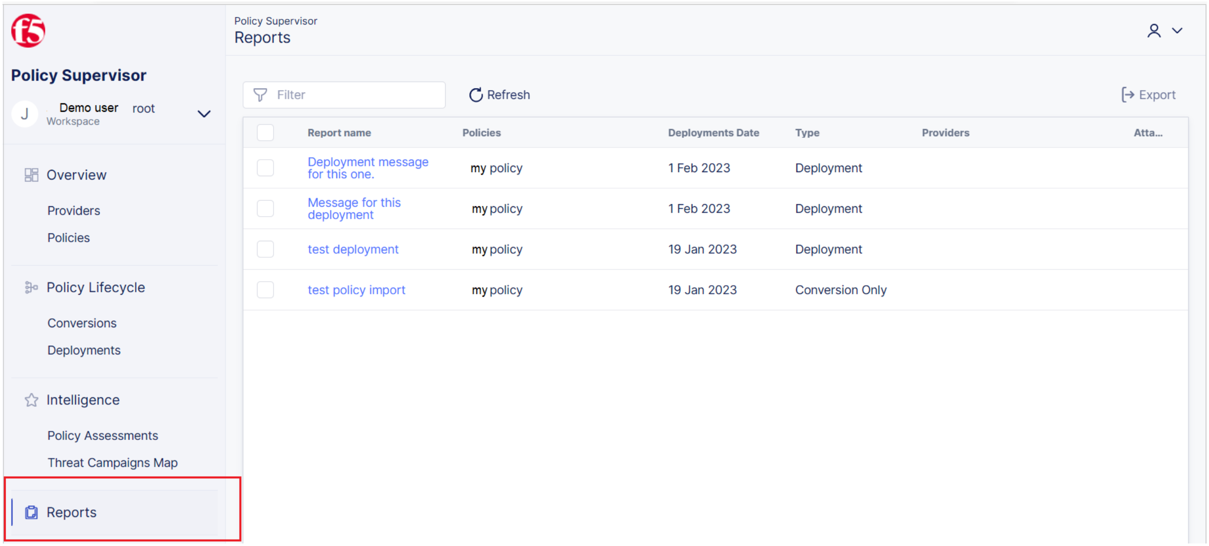
Deployments

The Deployments page lists all the policy deployments along with the following information for each deployment: *Policy name*, *Deployment Date*, *Status*, *Provider*, and *number of attachments*.

To view the log files for any deployment, click the **Actions menu** > **View logs**. The log file is downloaded and saved with a file name composed of the policy and provider names.

Reports

On the Reports page, the report for each conversion and deployment that has taken place is listed with details for each one.



Report name	Policies	Deployments Date	Type	Providers	Atta...
Deployment message for this one.	my policy	1 Feb 2023	Deployment		
Message for this deployment	my policy	1 Feb 2023	Deployment		
test deployment	my policy	19 Jan 2023	Deployment		
test policy import	my policy	19 Jan 2023	Conversion Only		

The Report name is taken from the deployment or commit message text that you provided when creating the conversion or deployment.

To see the details of a report, click the *Report name*, and the *Report details pane* slides out.

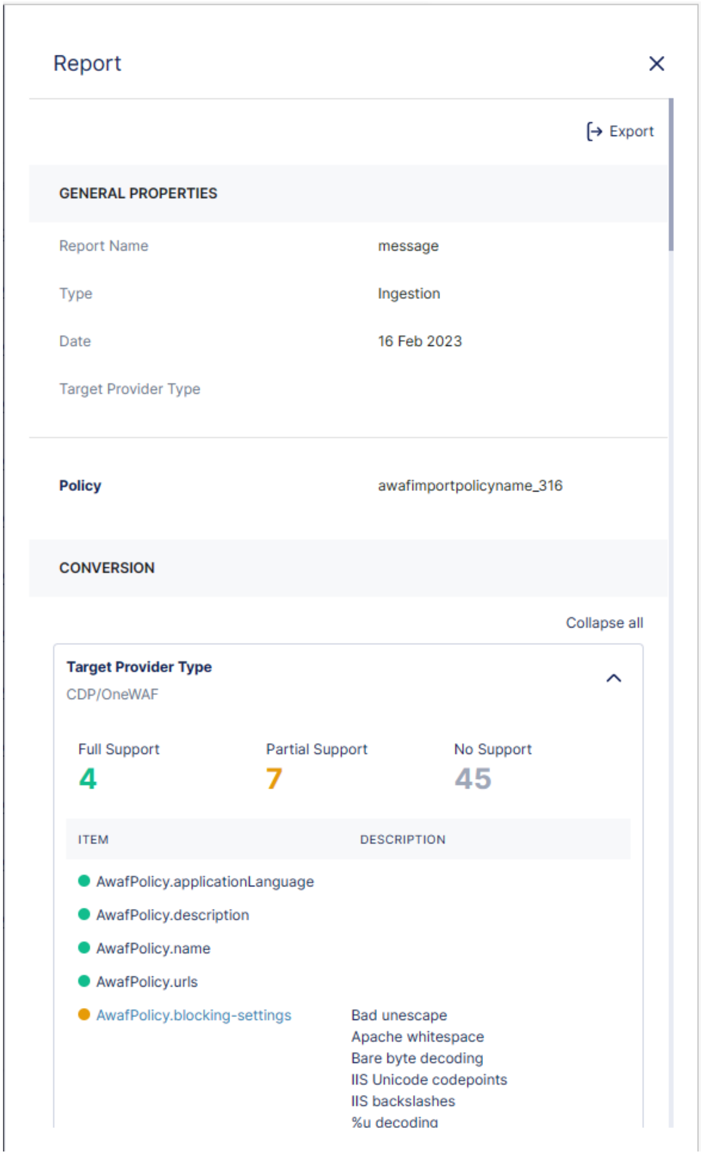
Report Details

The Report details pane contains a **General Properties** section, a **Conversion** section, and a **Deployment** section if applicable. The General Properties section displays information such as the *Report Name*, *type* of report, and the *policies* converted/deployed.

Conversion Reports

For conversion reports, the Conversion section displays the **Target Provider Type**. This will be CDP in the case of a policy ingestion/import from file.

To see the details of the conversion, expand the **Target Provider Type** section.



Report

GENERAL PROPERTIES

Report Name	message
Type	Ingestion
Date	16 Feb 2023
Target Provider Type	
Policy	awafimportpolicyname_316

CONVERSION

Target Provider Type
CDP/OneWAF

Full Support	Partial Support	No Support
4	7	45

ITEM	DESCRIPTION
● AwafPolicy.applicationLanguage	
● AwafPolicy.description	
● AwafPolicy.name	
● AwafPolicy.urls	
● AwafPolicy.blocking-settings	Bad unescape Apache whitespace Bare byte decoding IIS Unicode codepoints IIS backslashes %u decoding

The details of the policy items that have been converted are displayed in the following three states:

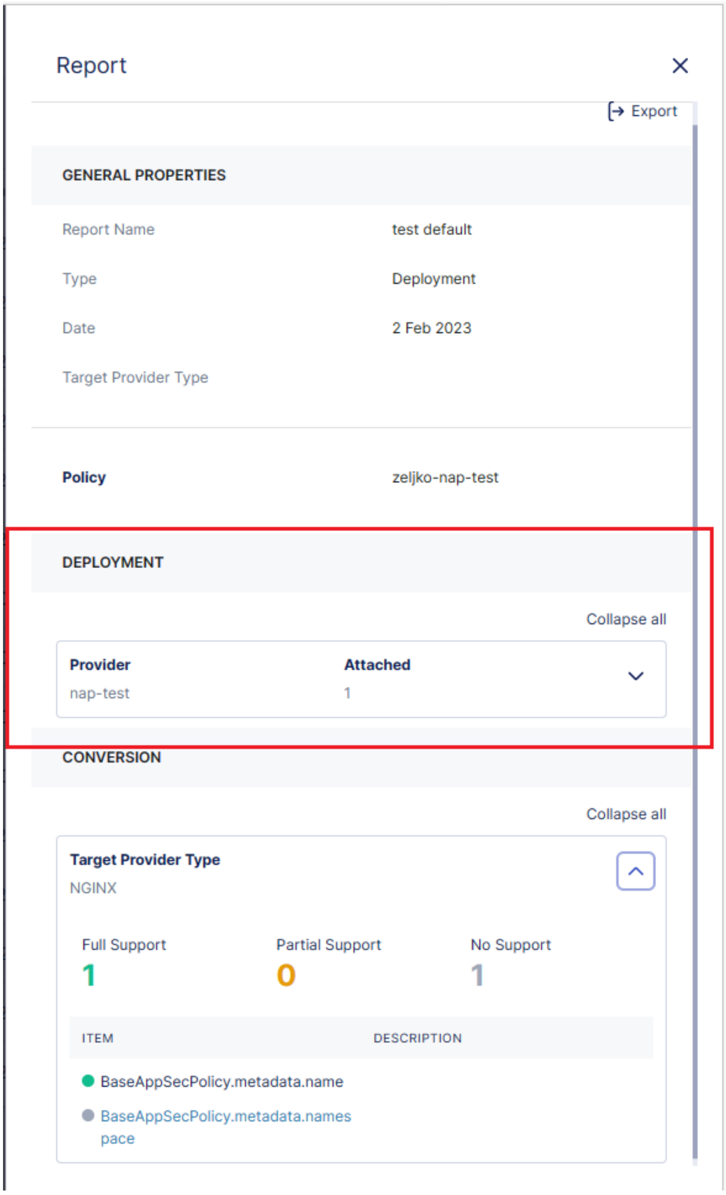
- *Full Support*: the settings converted fully from the source provider format to CDP.
- *Partial Support*: some settings in the category have been converted fully, some others have not been converted. This may happen either: A) because CDP may not have a corresponding

configuration or setting, or B) this feature is not yet supported by the Policy Supervisor converter.

- *No Support*: this group of features is not yet supported by the Policy Supervisor converter.

Deployment Reports

For Deployment reports, the provider *type*, *attachments*, and items that were deployed during the process are displayed. The **Deployment** section shows the *Providers* that the policies were deployed to, along with the number of attachments to namespaces/virtual servers.


Report

Export

GENERAL PROPERTIES

Report Name	test default
Type	Deployment
Date	2 Feb 2023
Target Provider Type	

Policy	zeljko-nap-test

DEPLOYMENT

Collapse all

Provider	Attached
nap-test	1

CONVERSION

Collapse all

Target Provider Type

NGINX

Full Support	Partial Support	No Support
1	0	1

ITEM	DESCRIPTION
● BaseAppSecPolicy.metadata.name	
● BaseAppSecPolicy.metadata.namespace	

Deployment reports also have a **Conversion** section with details of the conversion to the target provider type.

For reports that have multiple policies, you can click each **Target Provider Type** section to expand the details of that conversion.

For Questions, Comments or Issues please utilize the “Create a New Issue” under the project on GitHub for the Policy Supervisor Tutorial or email the alias: policysupervisor@f5.com.