

*<Plugin Vendor Name>* Plugin for Threat Exchange

## Instructions for using this plugin guide template

Please use this file as a template for future plugin config guides. Factors to consider are:

* A Table of Contents is not needed. These files are delivered in HMTL.
* A revision table is not needed. Revisions are tracked in our content management system.
* Style conventions are slightly different. View the steps in this file to see the conventions we use. Here’s the basics:
  + Bold is used for items in the UI that you click on.
  + Italic is used for special terms. Names of items in the UI are in Title Case, no style needed.
  + Monospace is used for code examples and things the user needs to enter in a text field in the UI.
* You can use this file to create new plugin guides. Some plugins have some commons flows, so reuse what’s common to reduce new content write.
* Remove all the green comments in this template. They are only there for guidance.
* Look at published versions at docs.netskope.com to see completed examples.
* Remove this page from the draft.

Describe the purpose of the guide.

Example:

This document explains how to configure CrowdStrike with Threat Exchange in the Netskope Cloud Exchange platform. This integration allows for sharing of event driven intelligence that has been identified by CrowdStrike EDR or Netskope.

### Requirements

To complete this configuration, you need: (examples shown)

* A Netskope tenant (or multiple, for example, production and development/test instances)
* No special license (Advanced Threat Protection is not needed)
* A Netskope Cloud Exchange tenant with a Threat Exchange module
* A CrowdStrike Falcon Prevent account.

### Workflow

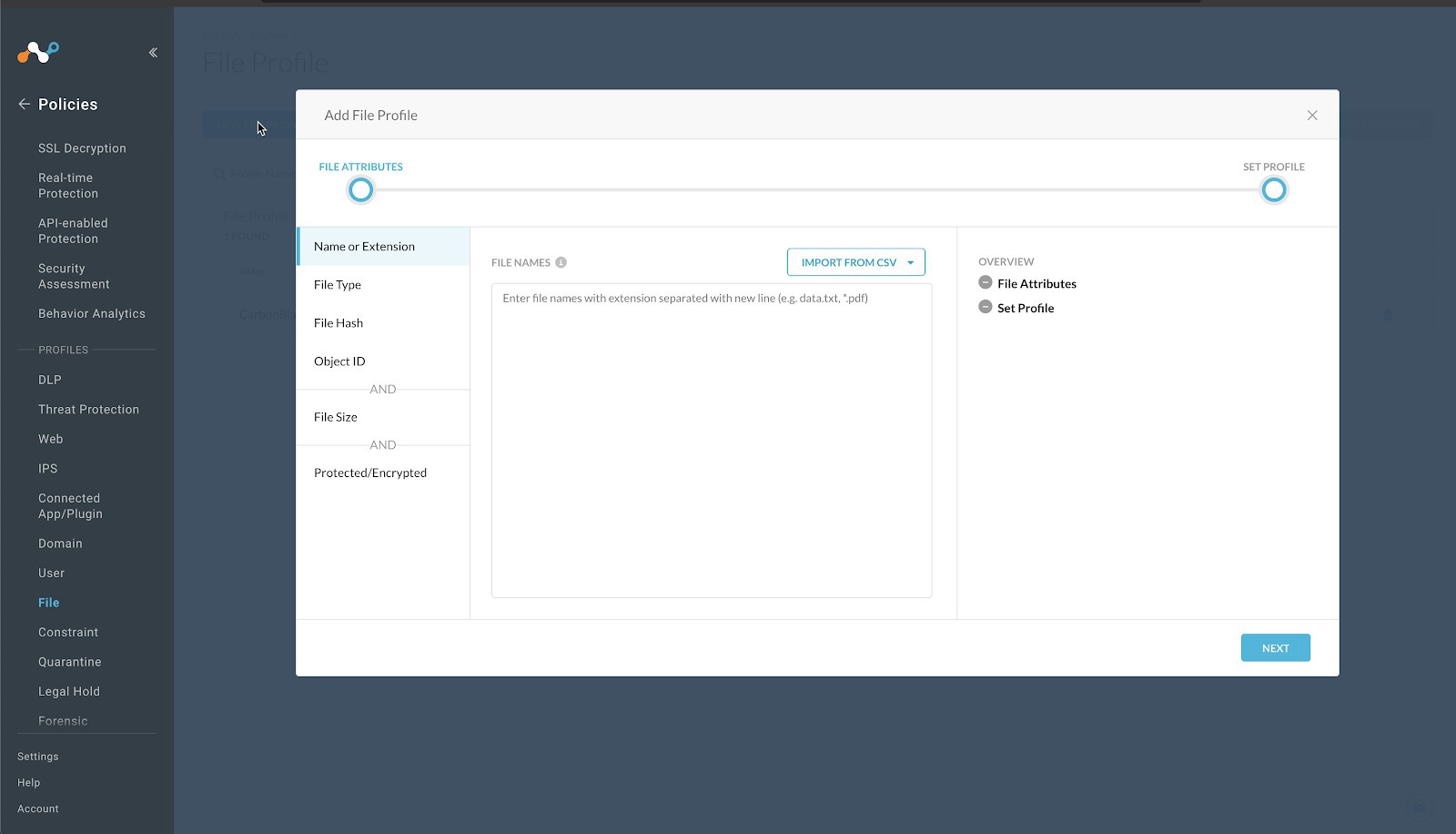
1. First thing they need to do.
2. Second thing they need to do.
3. Etc. etc., …
4. Testing/Validation
5. Troubleshooting (if known)

Here’s where I’ll add the video.

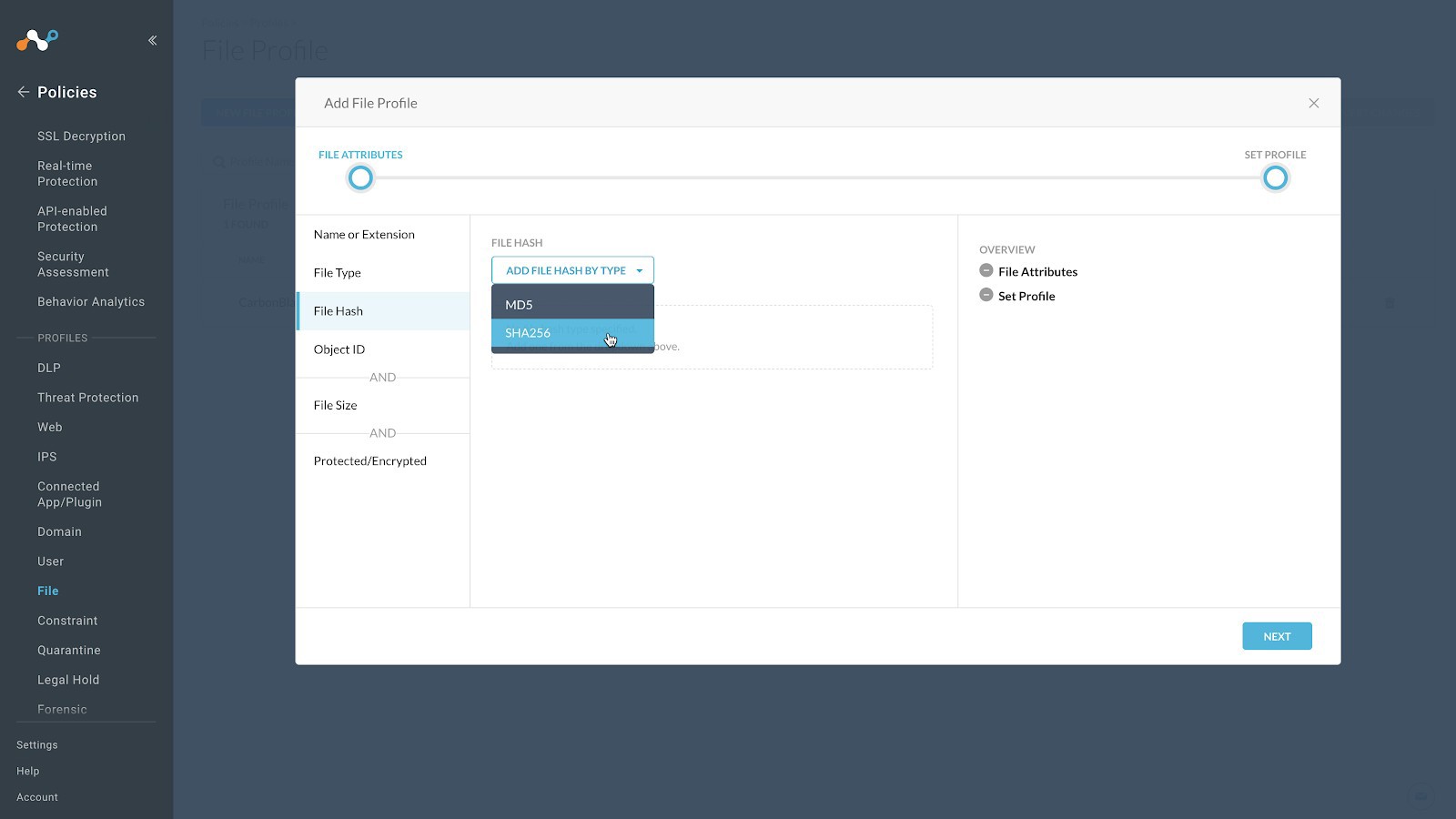
# First Thing to do in the Configuration

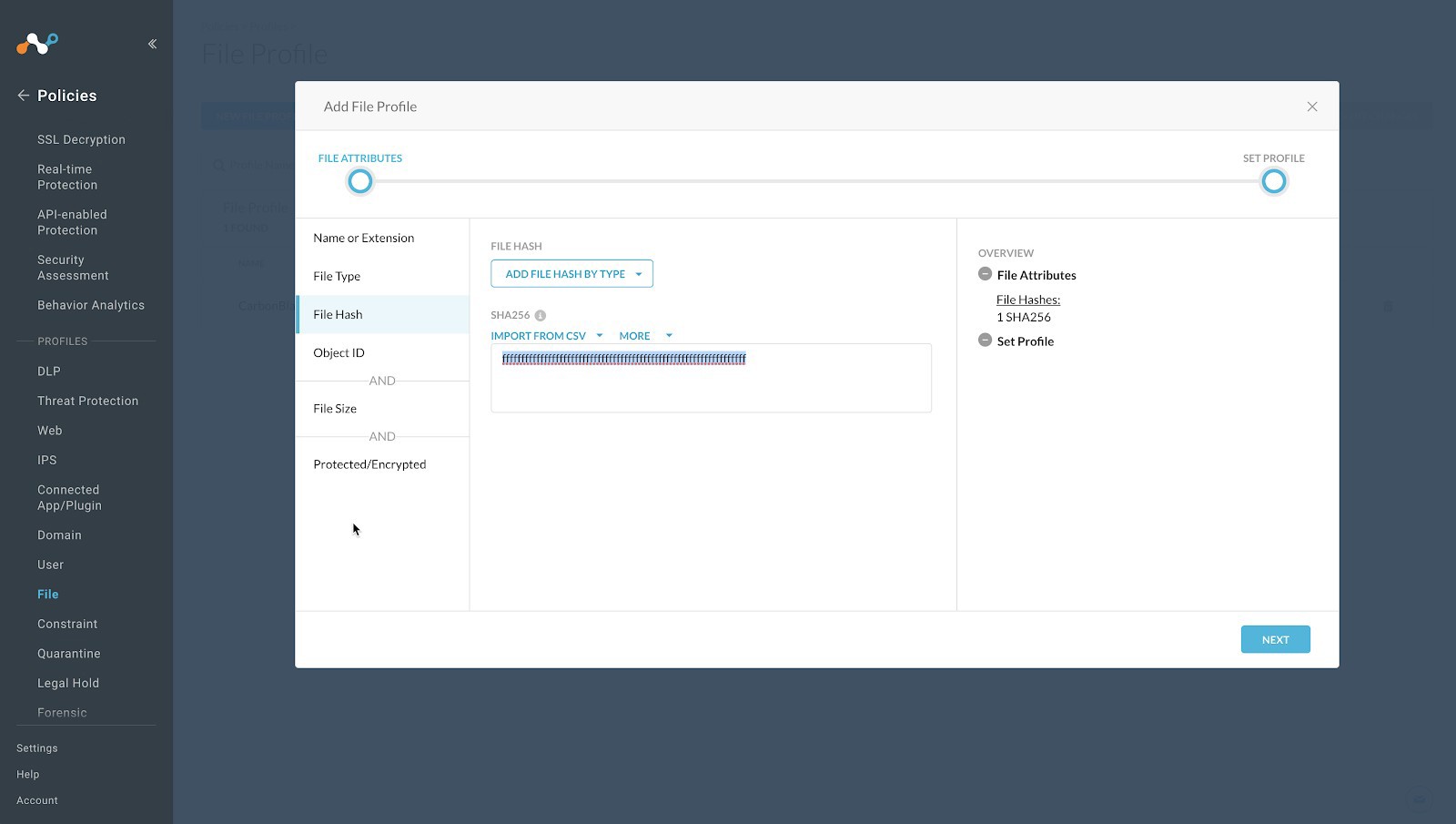
# Example Title: Create a Secure Web Gateway Custom File Profile

1. In the Netskope UI, go to **Policies** , select **File** , and click **New File Profile**.

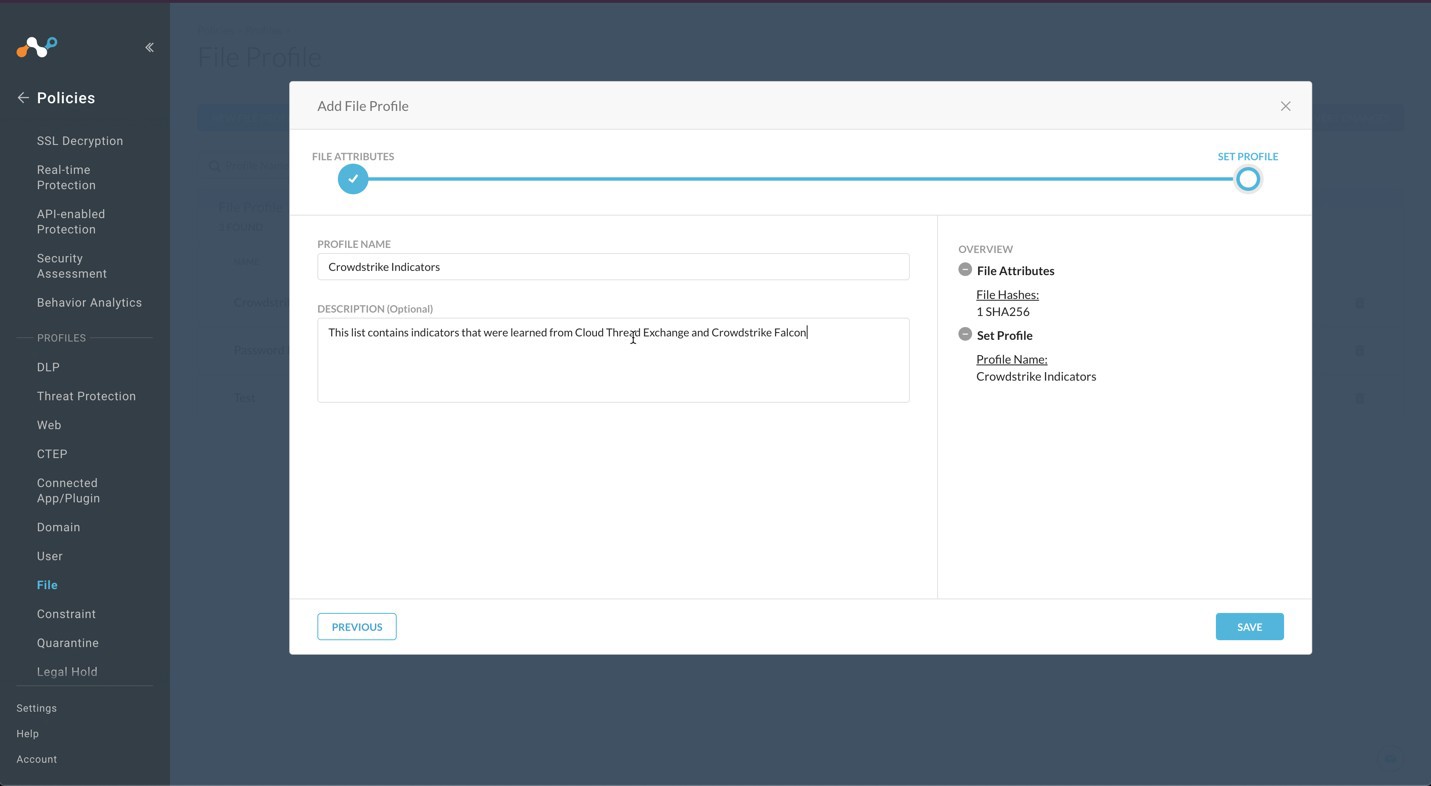


1. Click **File Hash** in the left panel, select **SHA256** from the File Hash dropdown list.



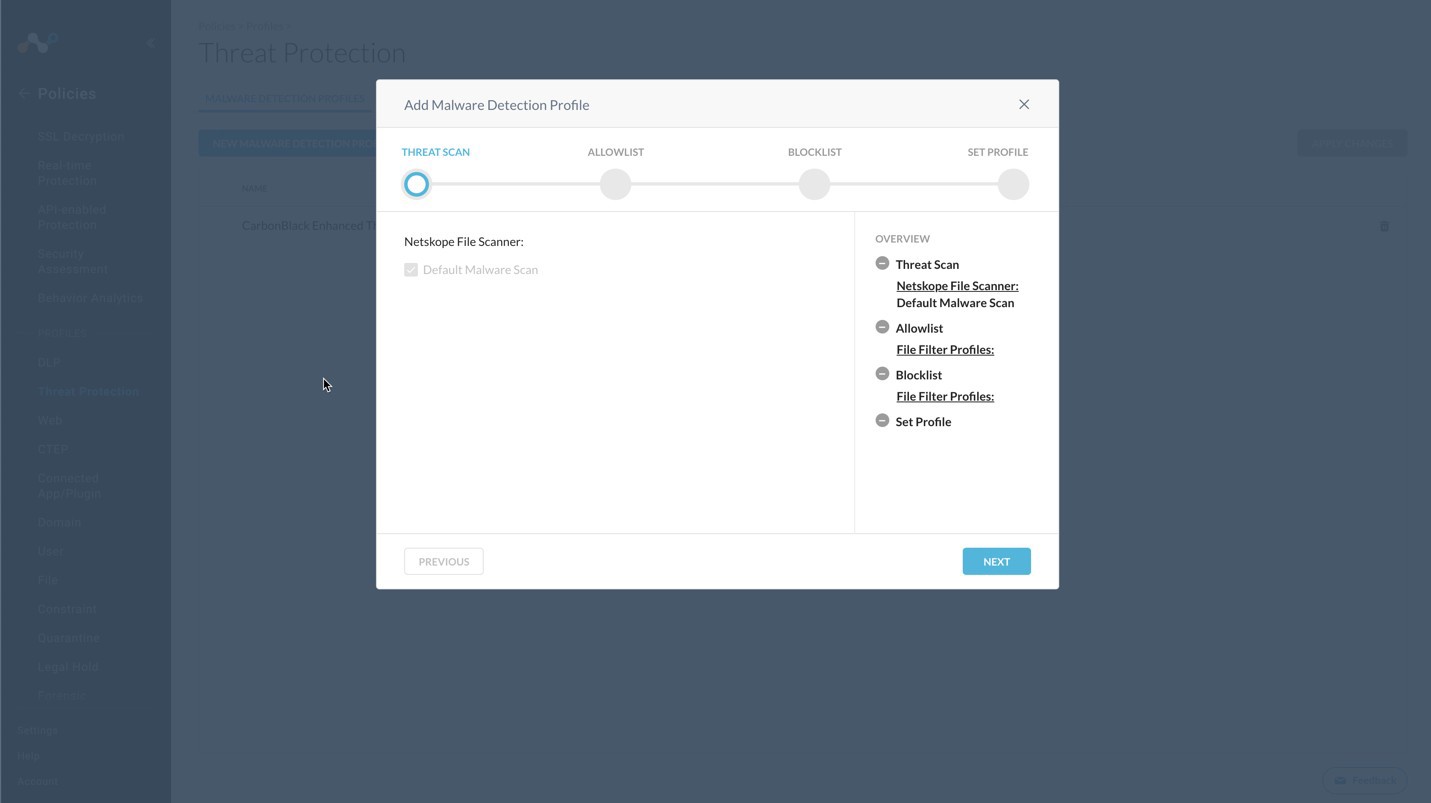
1. Enter a temporary value in the text field. Netskope does not support progressing without having a value in this field, and recommends entering a string of 64 characters that consists of the character f. For example, ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff. This will have a very low possibility of matching a valid file format.

#### Click Next.

1. Enter a Profile Name and a Description. We recommend not having blank spaces in your profile name; use underscores for spaces.
2. Click **Save**.
3. To publish this profile into the tenant, click **Apply Changes** in the top right.

# Second Thing to do in the Configuration

# Example Title: Create a Malware Detection Profile for CrowdStrike

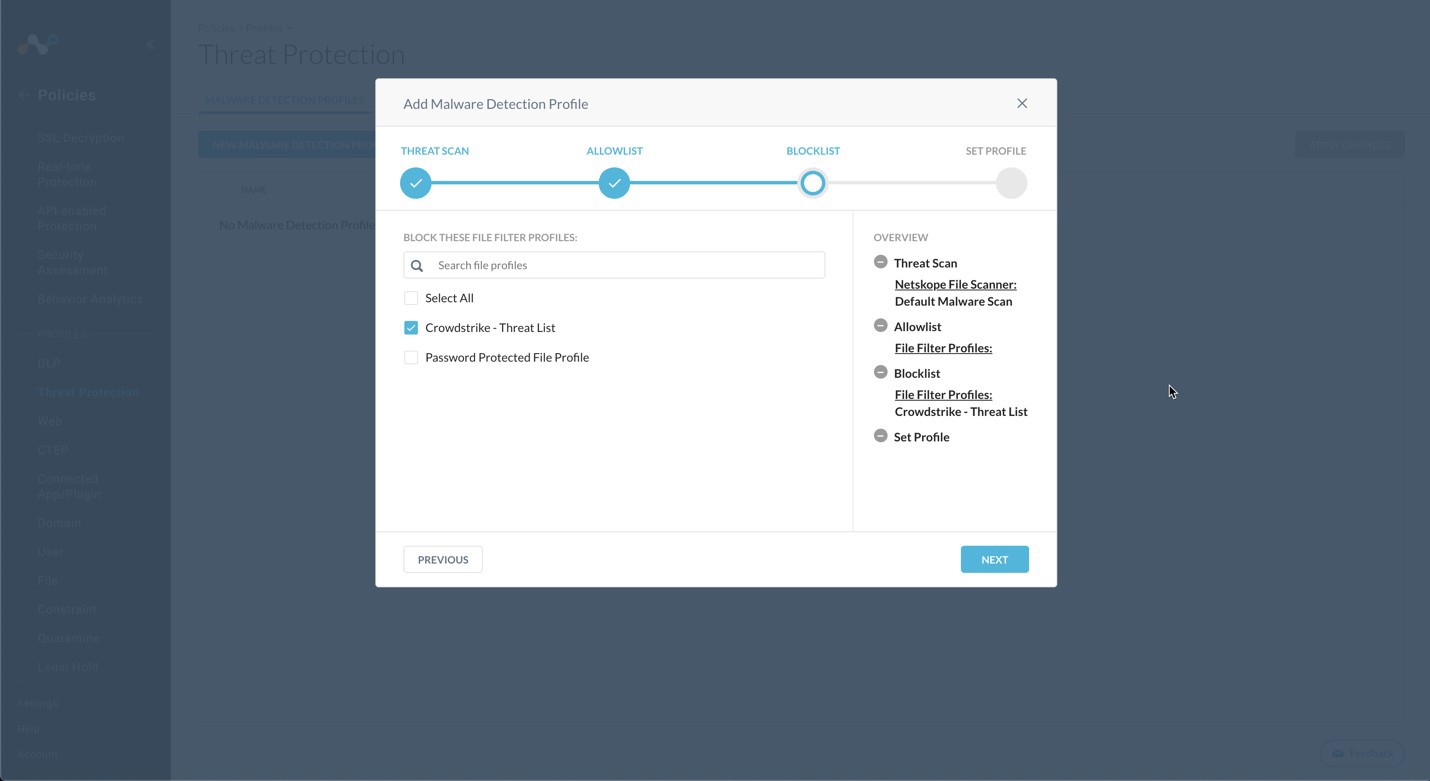
1. In the Netskope UI, go to **Policies**, select **Threat Protection** , and click **New Malware Detection Profile**.
2. Click **Next**.



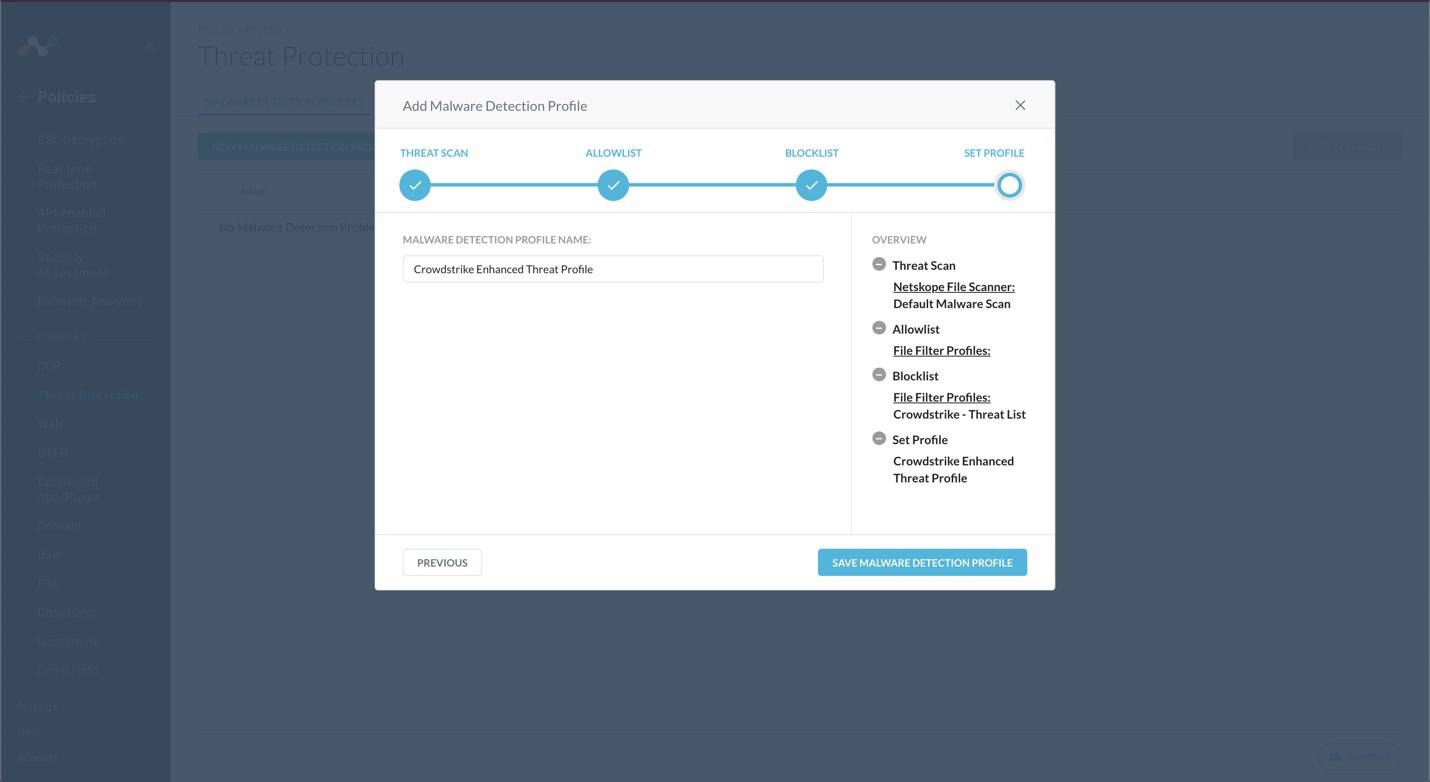
**NOTE**

For this configuration example, we will be using the intelligence for this list as a block list. Netskope does support inclusion of both allow and block lists in the threat profiles.

1. Click **Next** again.
2. Select the File Profile you created in the previous section and click **Next**.



1. Enter a Malware Detection Profile name and click **Save Malware Detection Profile**.



1. To publish this profile in the tenant, click **Apply Changes** in the top right.

# Third Thing to do in the Configuration

# Example Title: Create a Real-time Threat Protection Policy for CrowdStrike

These instructions apply to the new Real-time Protection policy workflow.

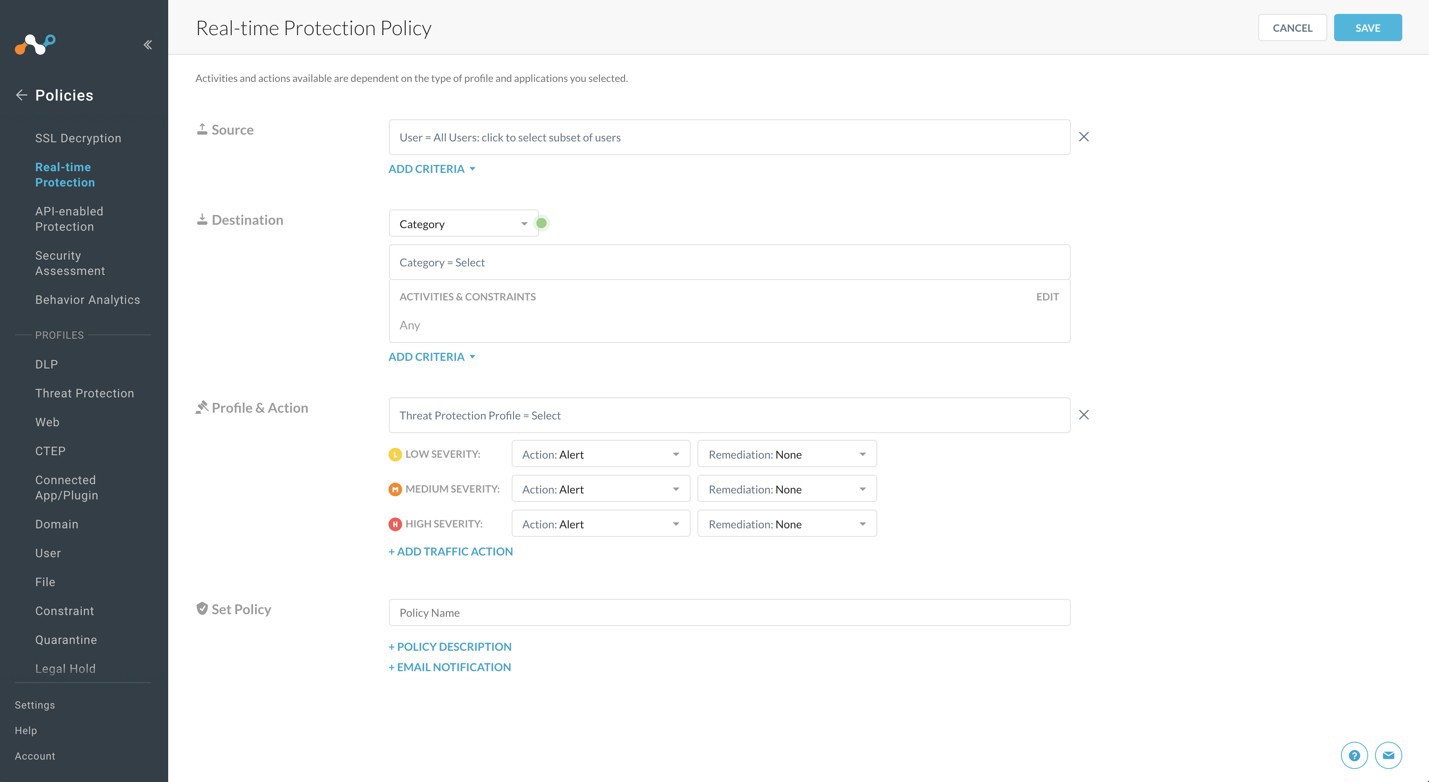
1. In the Netskope tenant, go to **Policies** and click **Real-time Protection**.

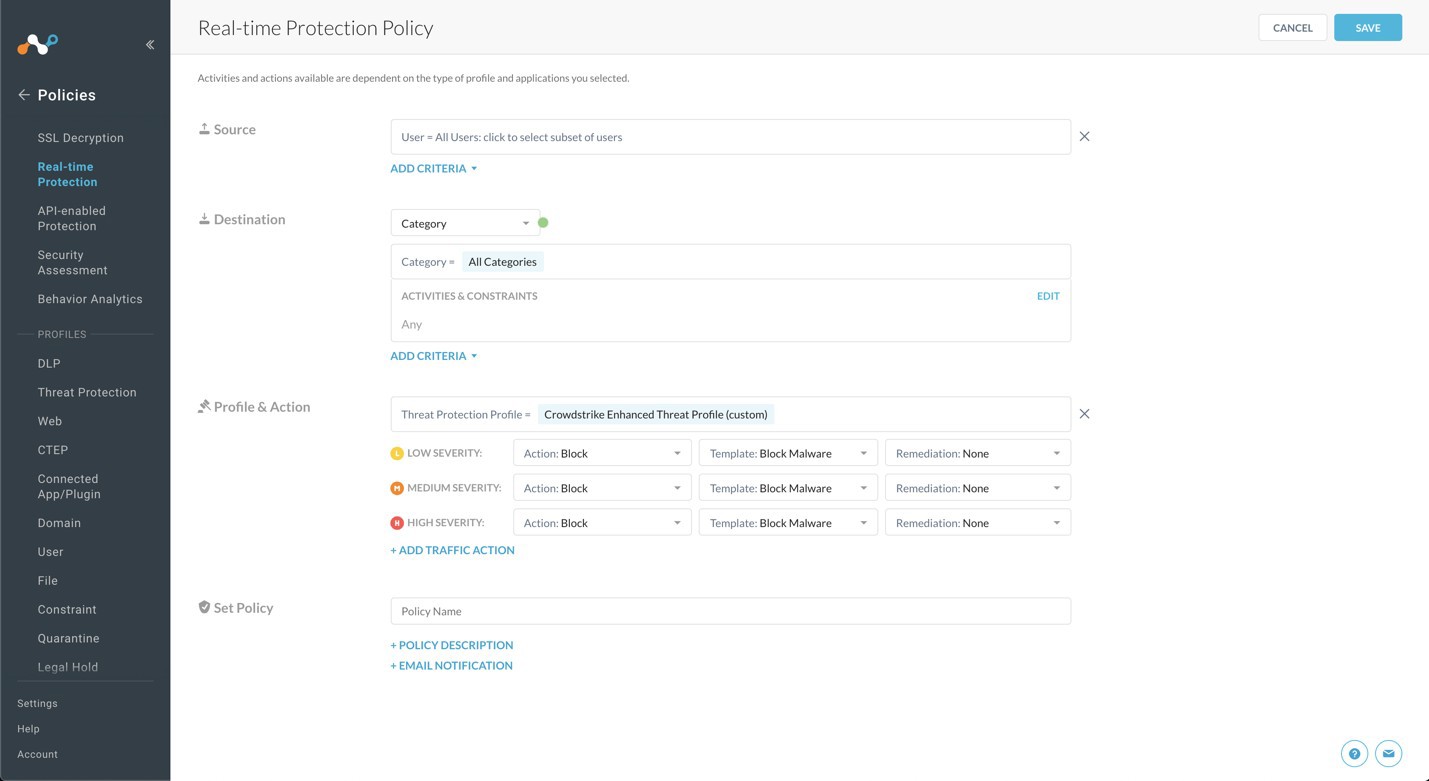


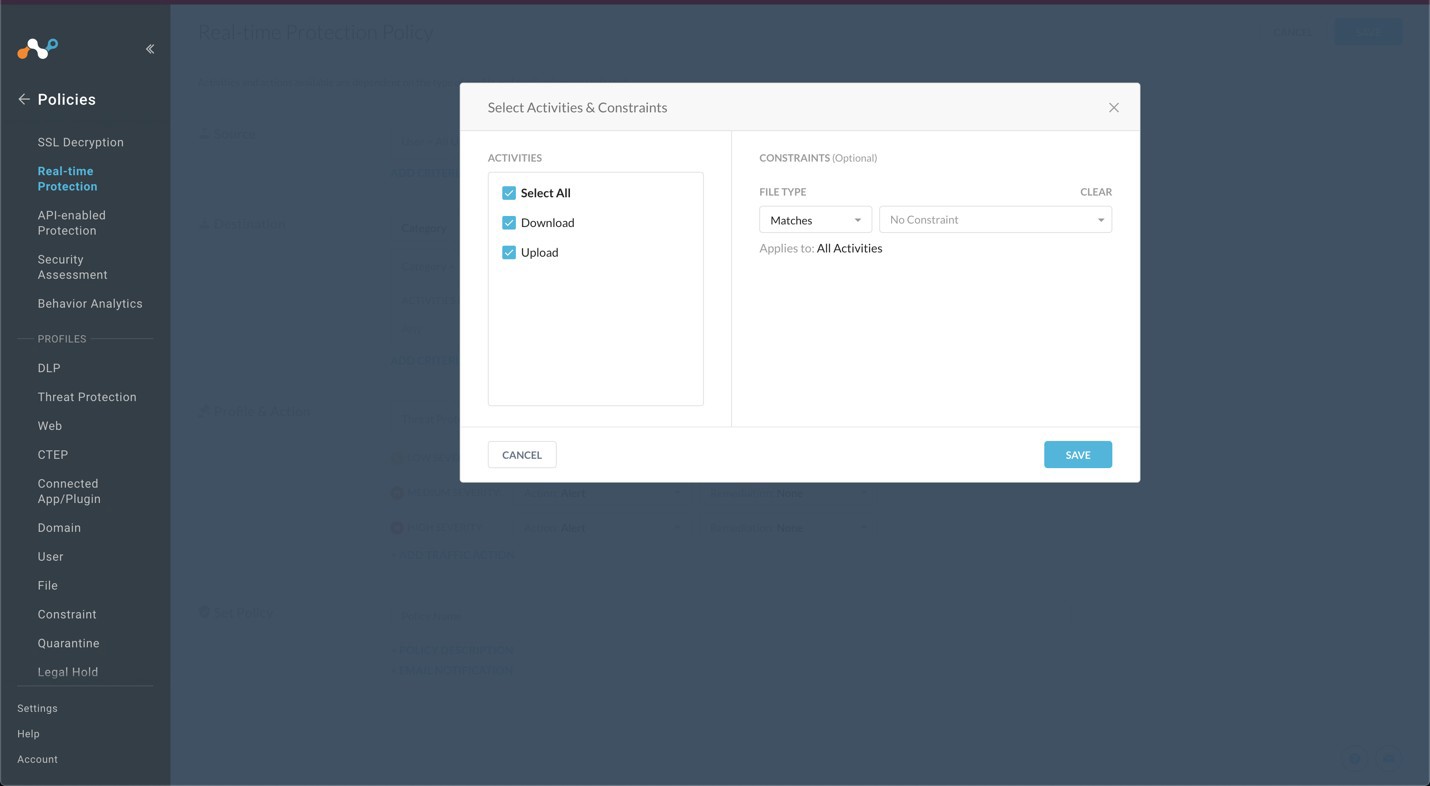
**NOTE**

The policy configured here is just an example. Modify as appropriate for your organization.

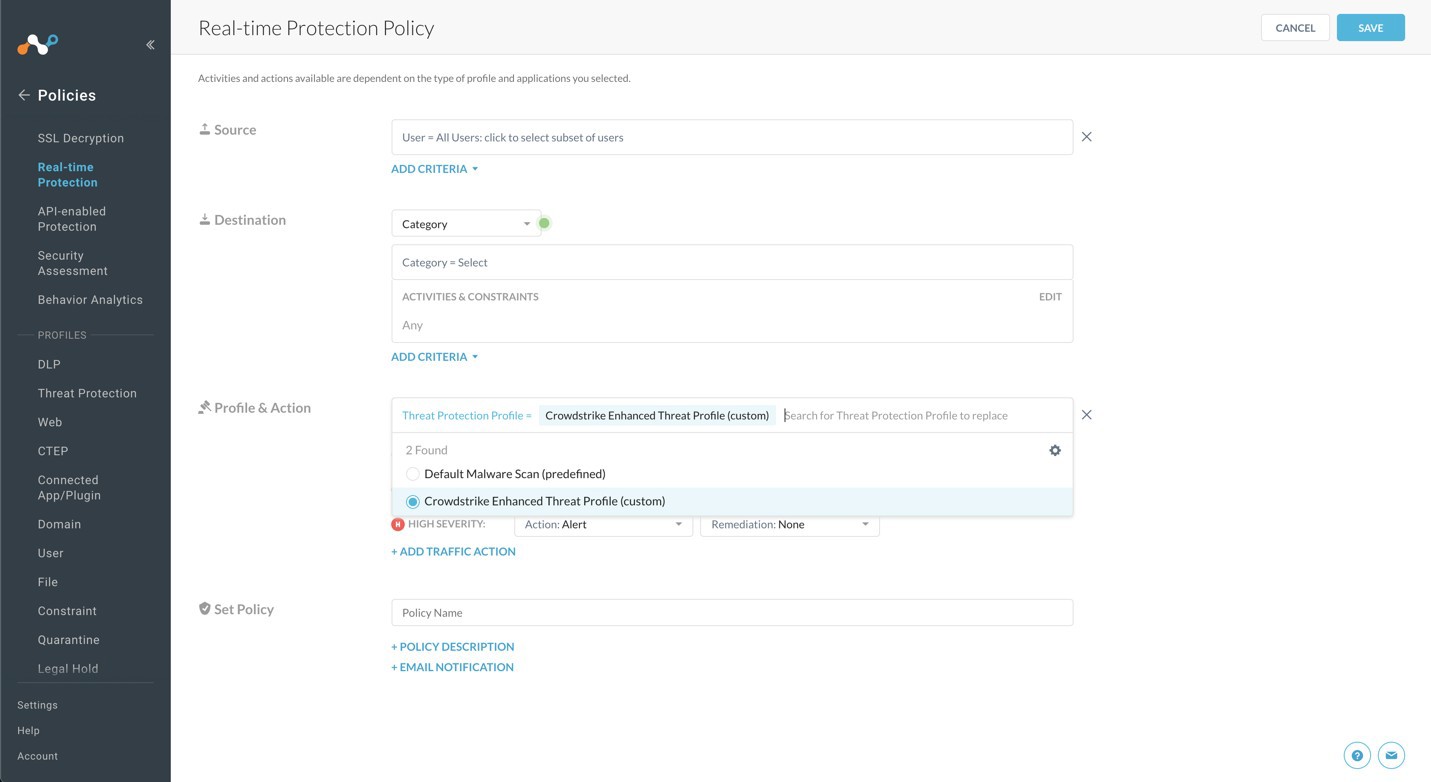
1. Click **New Policy** and select **Threat Protection**.



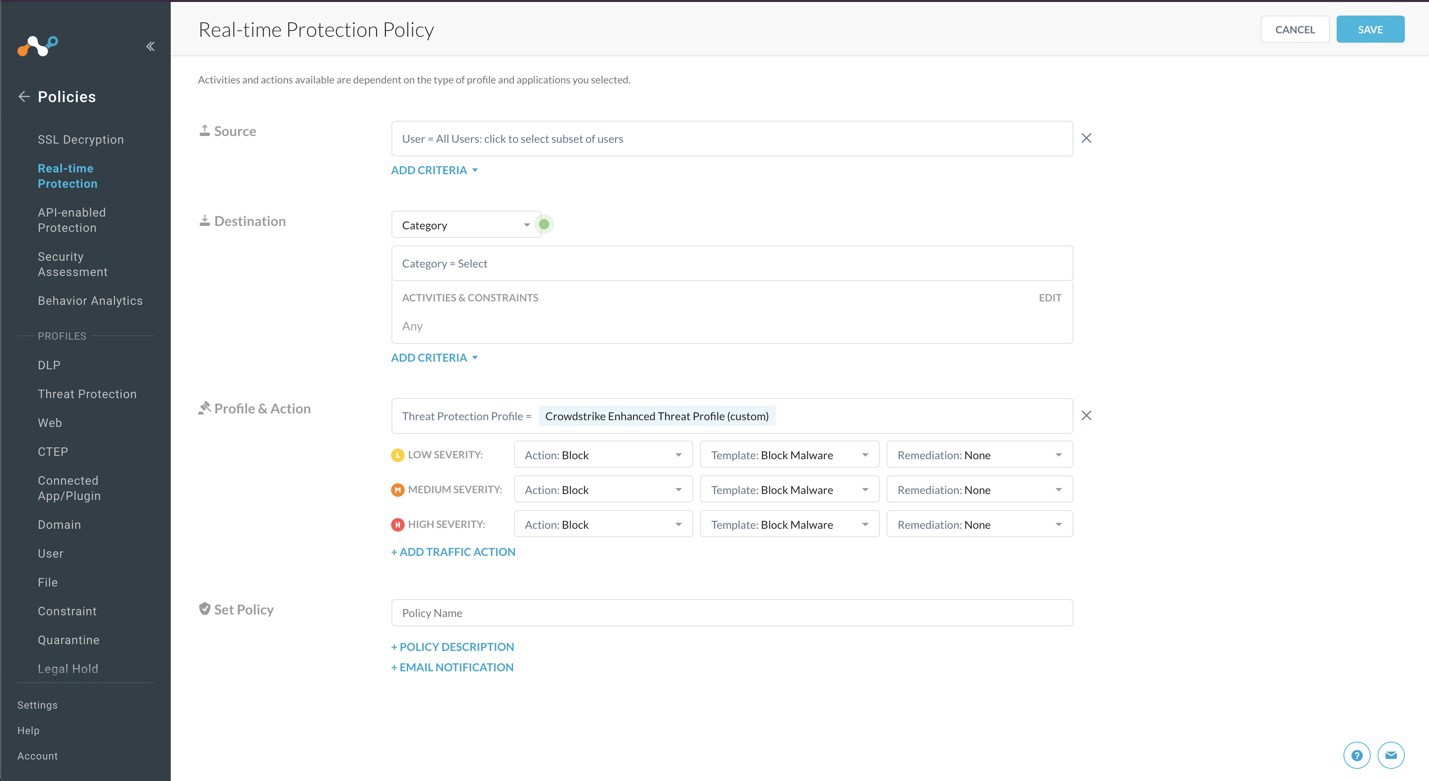
1. For *Source*, leave the default (User = All Users)
2. For *Destination*: select **Category**
3. The Category section expands and allows you to search and select categories. Click **Select All**. When finished, click outside of the Category section.
4. When the Activities & Constraints section opens, click **Edit**.
5. Select **Upload** and **Download**, and then click **Save**.



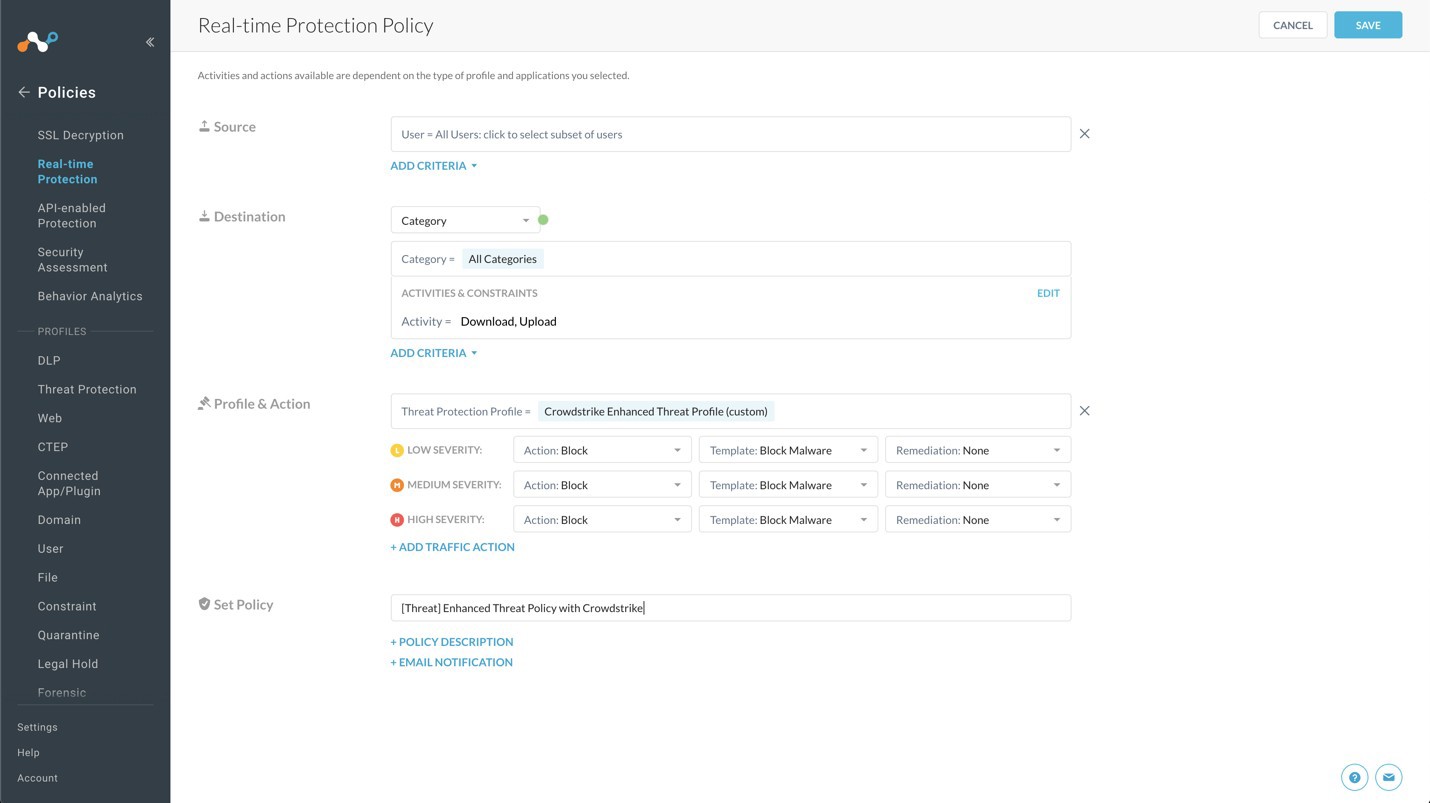
1. For *Profile & Action*, click in the text field.
2. Select the Malware Detection profile you created in the previous section.



1. For the Severity Levels, change all the Actions settings from Action: Alert to Action: Block.



1. Select a template to choose which block message is sent to the user.
2. For *Set Policy*, enter a descriptive Policy Name.



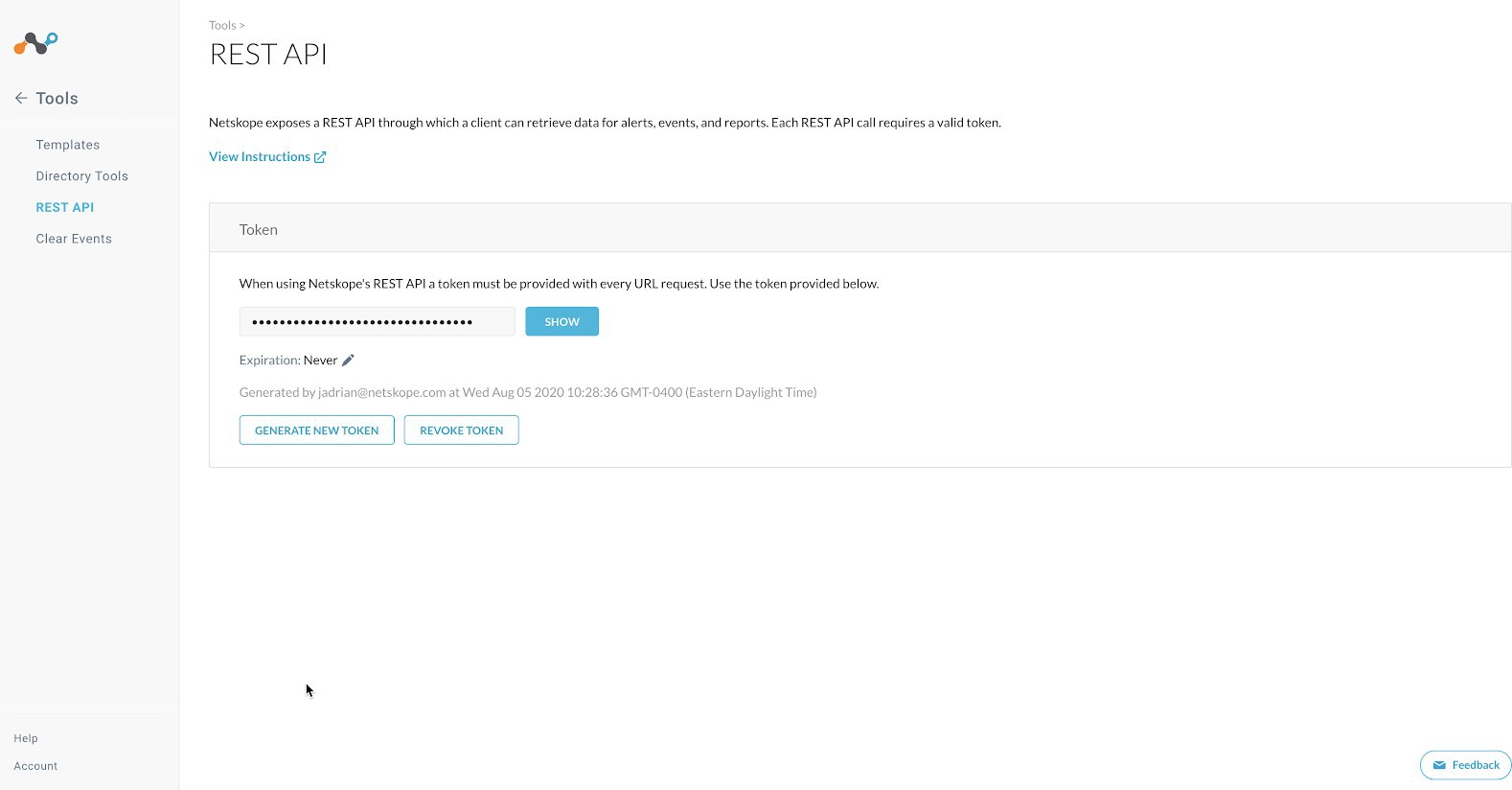
1. Click **Save** in the top right to save the policy.
2. Choose the **To the top** option when it appears. (Or appropriate location in your security policy)
3. To publish this policy into the tenant, select **Apply Changes** in the top right.

# Etc., For However Many Configurations are Needed

# Example Title: Get the Netskope API Token

The Netskope API token is needed to configure the Netskope Plugin for Cloud Exchange, so copy the token before proceeding.

1. In the Netskope UI, go to **Settings** on the bottom of the left nav panel.
2. Select **Tools** and then **REST API**



1. Click **Show** to view the token string; save the token for later use.
2. If you do not have a token, click **Generate New Token.**



**NOTE**

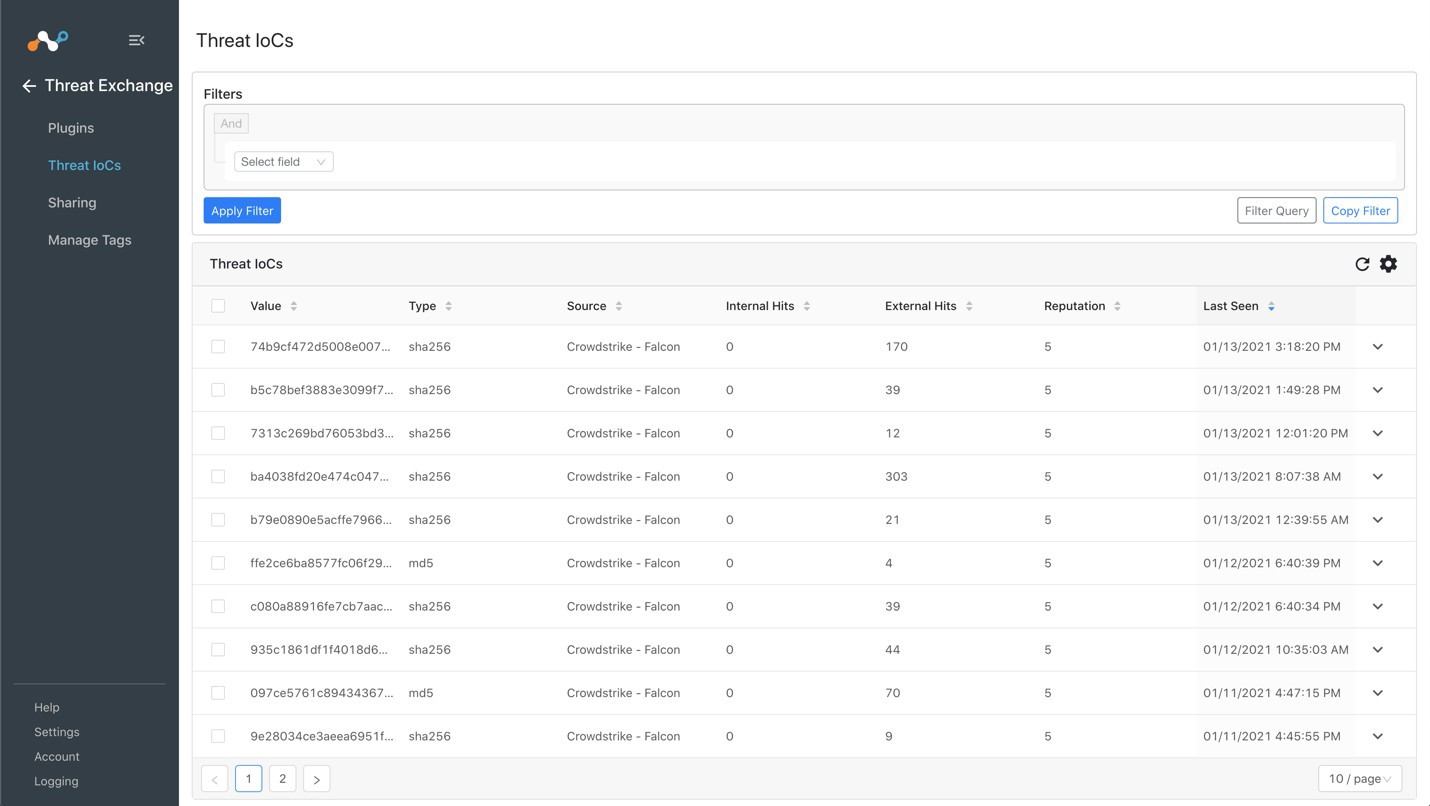
Netskope only supports a single token at writing this guide. Be aware if you generate a new token, there could be an impact to any automation that is using the existing token.

# Test the Configuration

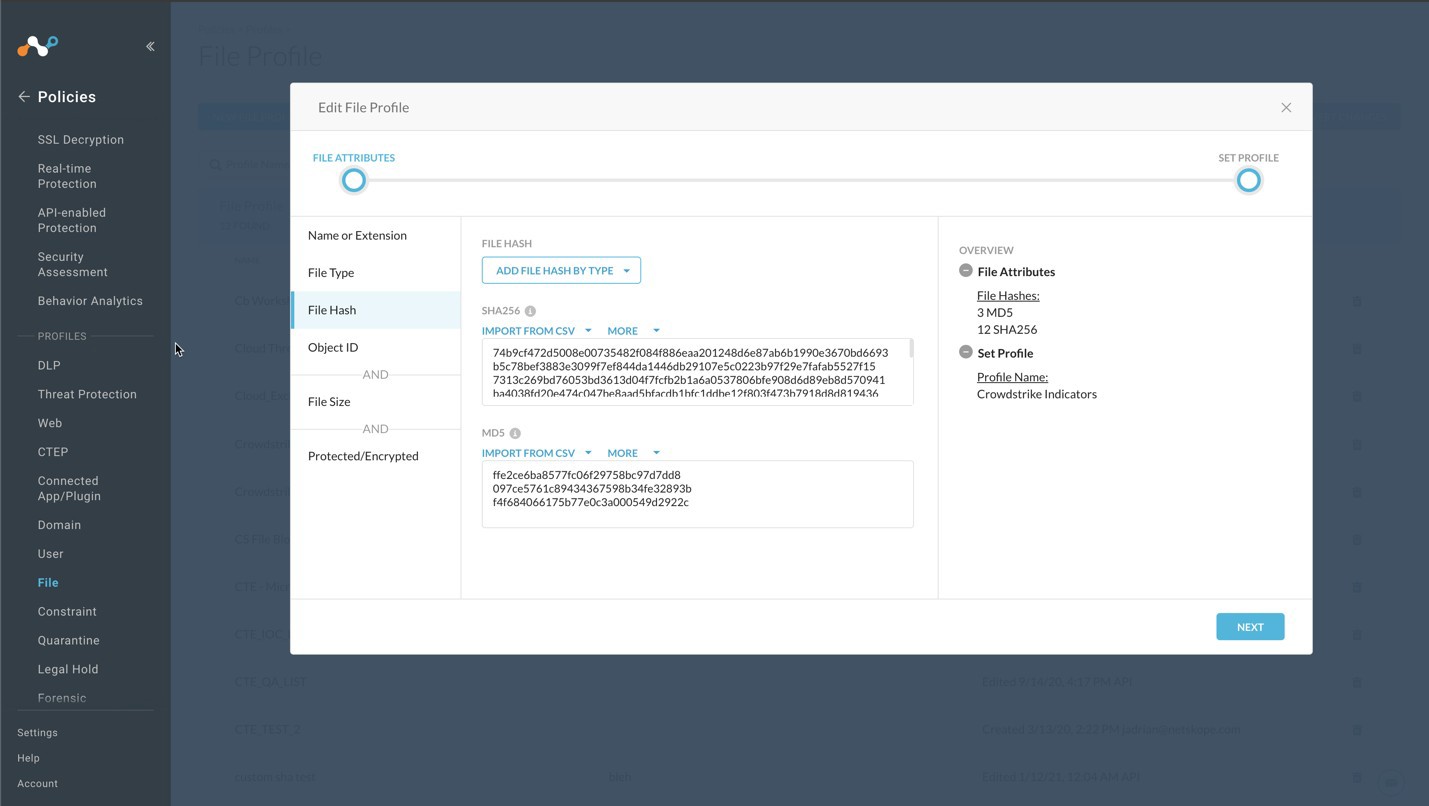
# Example Title: Validate the Plugins

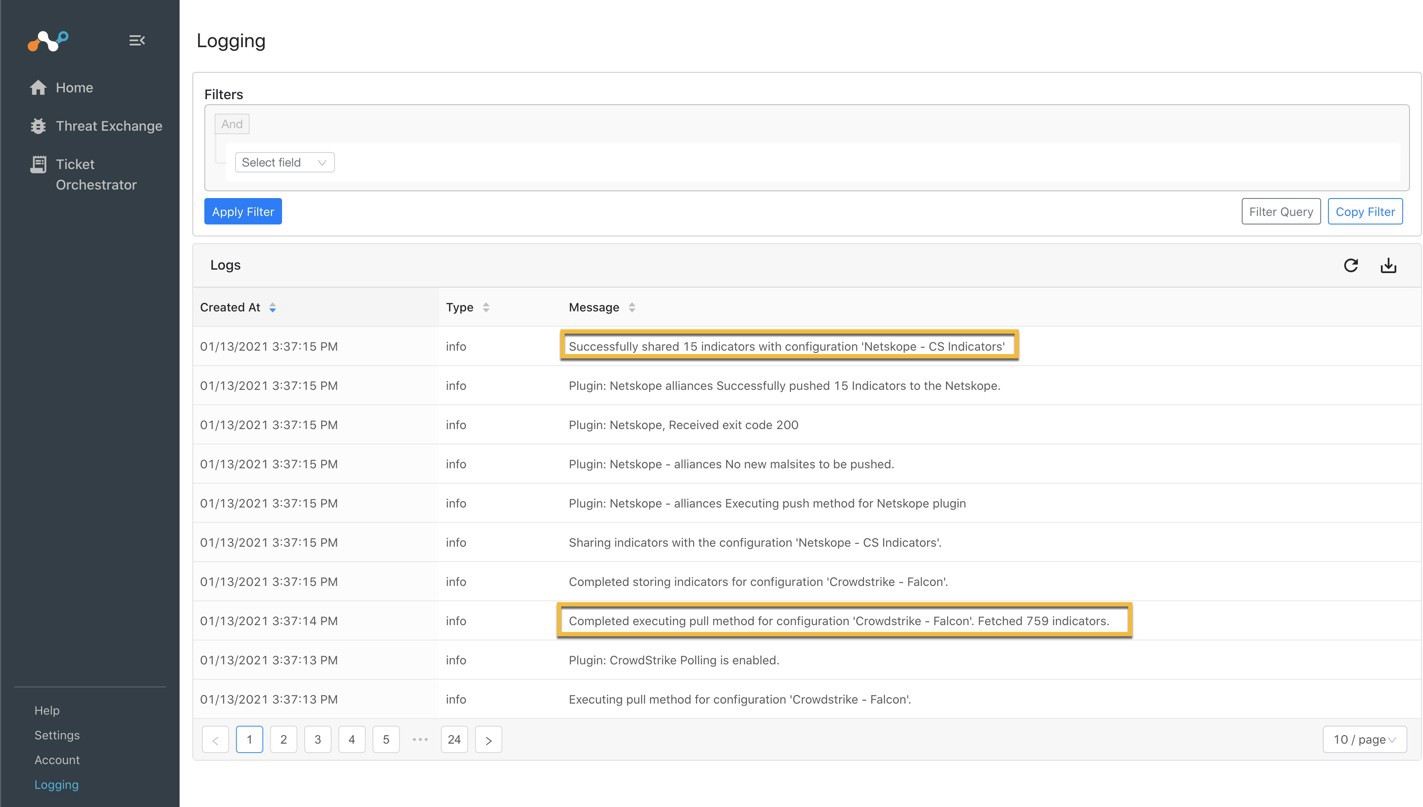
In order to validate the configuration you must have Netskope Alerts and/or CrowdStrike Detections. These will be queried based on the polling interval previously configured in the plugins.

1. Go to **Threat Exchange** and select **Threat IoCs**.

You should see records from your respective plugins. You can filter based on Source values to check both the Netskope and CrowdStrike plugins.

1. In the Netskope UI, go to **Policies > File**, select your custom File Profile, and click **File Hash.**



1. If data is not being brokered between the platforms, you can look at the audit logs in Cloud Exchange. In Cloud Exchange, select **Logging** in the left nav panel. Look through the logs for errors.