FORESCOUT

BETA

TREND MICRO APEX CENTRAL

Forescout eyeExtend Connect app Integration

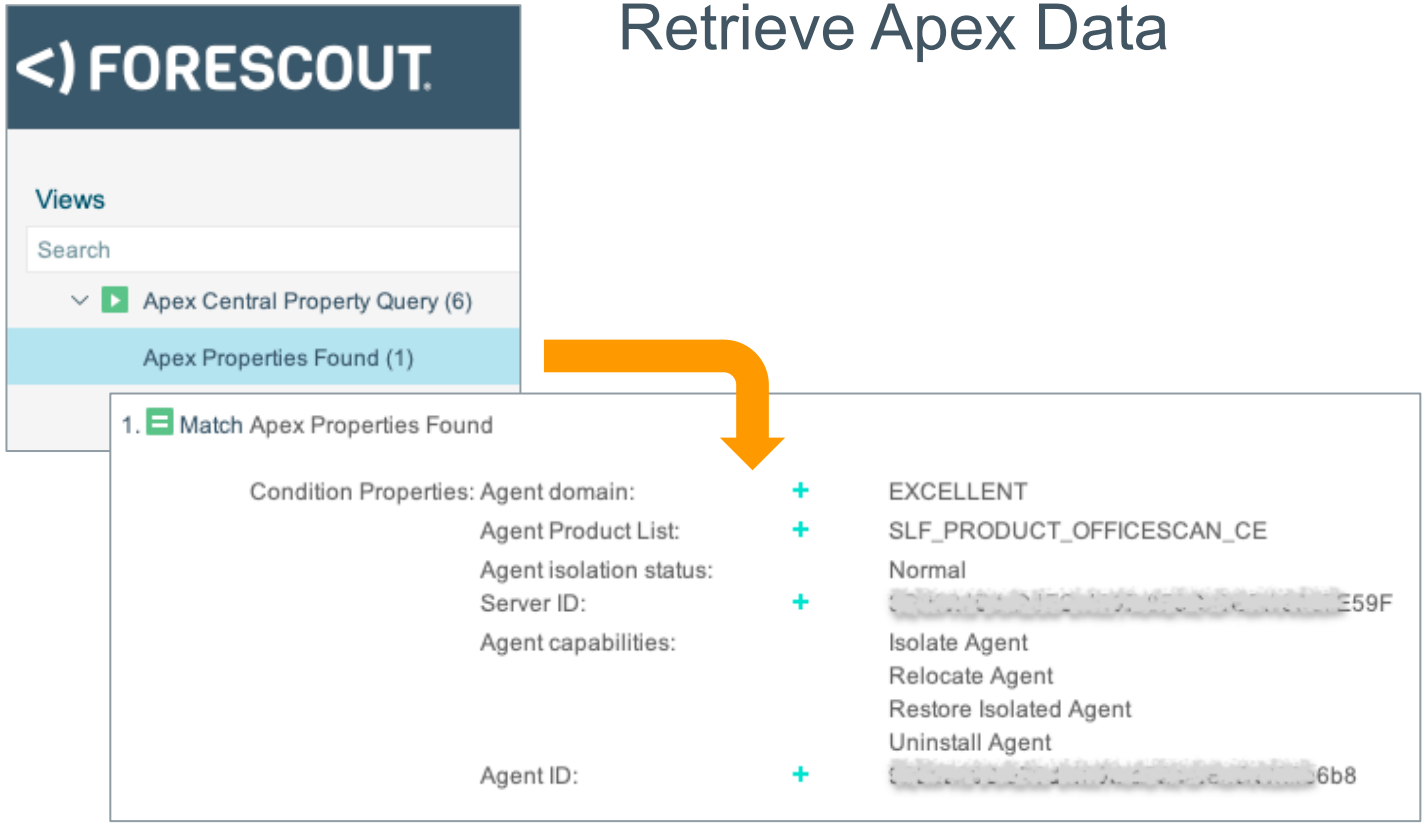
Author: Nick Cincotta
Date: August 2020

Capabilities

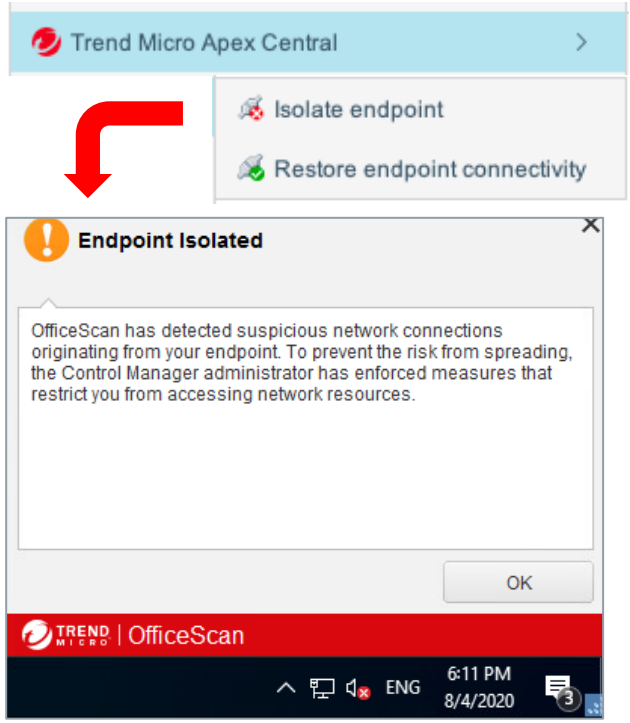
The eyeExtend Connect app for Trend Micro Apex can be used to:

- Retrieve endpoint information from Apex server to use in policies.
- Send commands to Apex to isolate the endpoint from the network.

Retrieve Apex Data



Endpoint Isolation



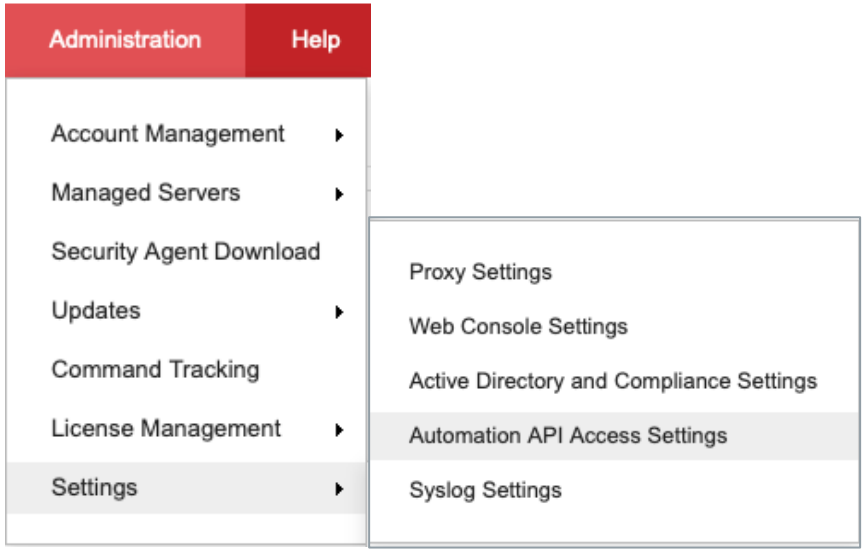
Requirements

- eyeSight 8.1 or above
- eyeExtend Connect Module
- Valid license for both products
- Connect app for Trend Micro Apex

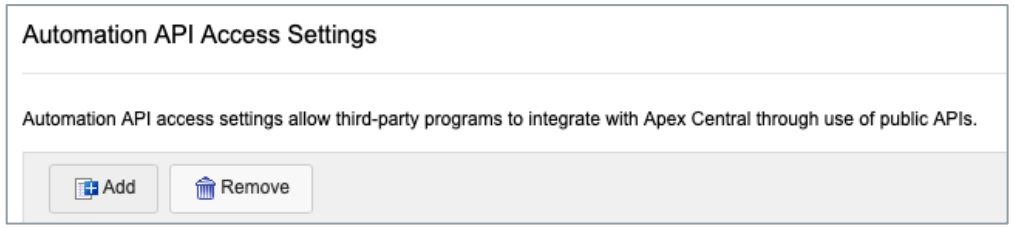
- Apex Central (Tested on version 2019)
- Automation API enabled

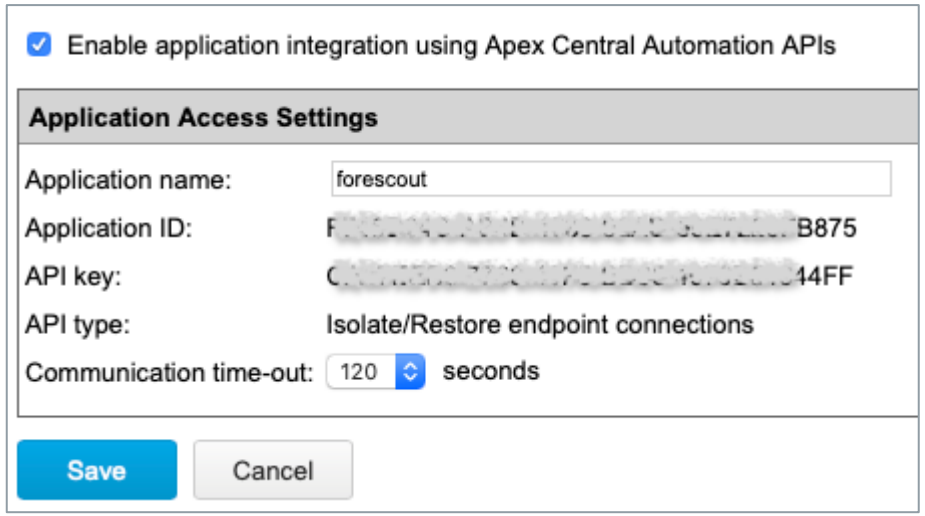
APEX CENTRAL CONFIGURATION

Enable Automation API



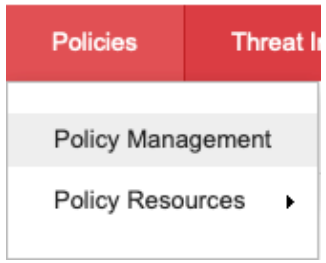
In the Apex Central management portal go to: *Administration -> Settings -> Automation API Access Settings*.

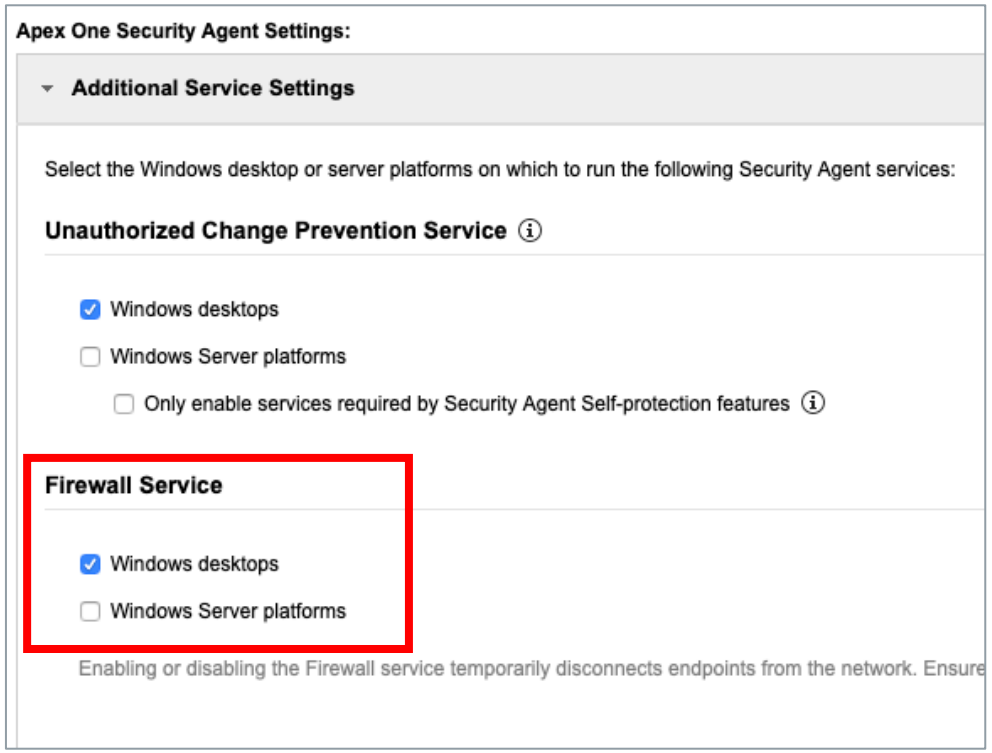




Add a new program and name it forescout. Copy the Application ID and API key for later use.

Enable Firewall for Endpoint Isolation (Optional)



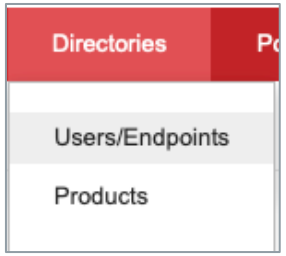


If not already configured, the Apex firewall service for endpoints will need to be enabled for isolation to work.

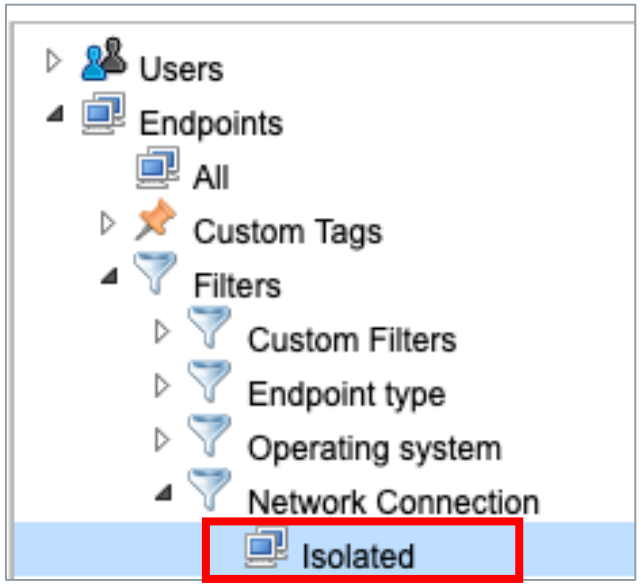
Go to Policies -> Policy Management and select your policy. Then under Additional Service Settings enable Firewall Service.

Make sure to take caution and understand the impact of changes you make in a production environment.

Add Exemptions for Isolation

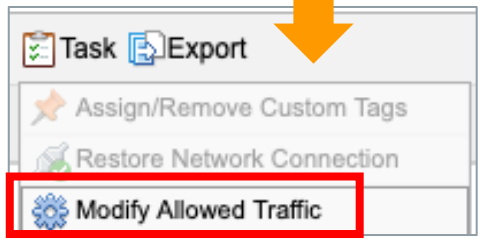


Traffic exceptions should be added to allow communication to and from Apex servers and Forescout the endpoint is isolated.



Select *Directories -> Users/Endpoints* Then click the *Isolated* field under *Filters -> Network Connection*.

On the panel on the right select *Task -> Modify Allowed Traffic.*



Here you can add specific ports if necessary or simply allow all traffic inbound and outbound from Forescout appliances and Apex servers.

FORESCOUT CONFIGURATION

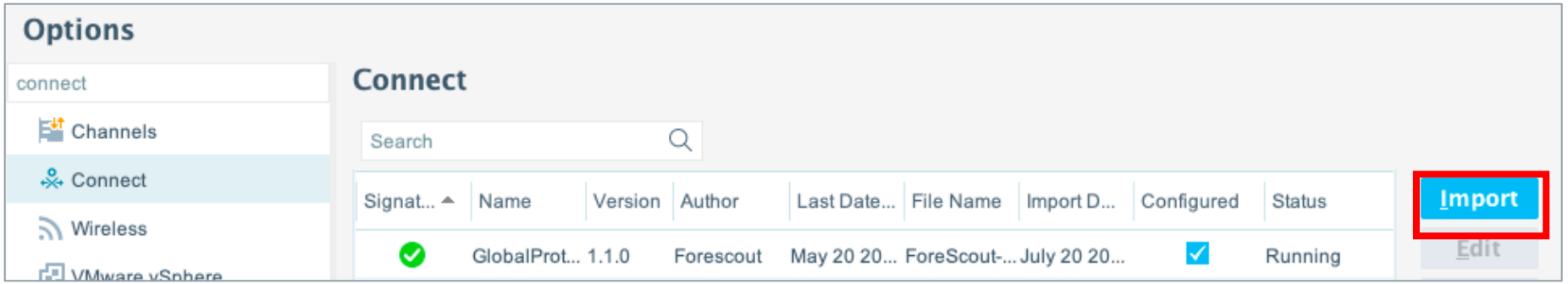
Upload the App to Connect Module

For the current Beta release for this app it requires that the use of unsigned apps be enabled for the eyeExtend Connect module.

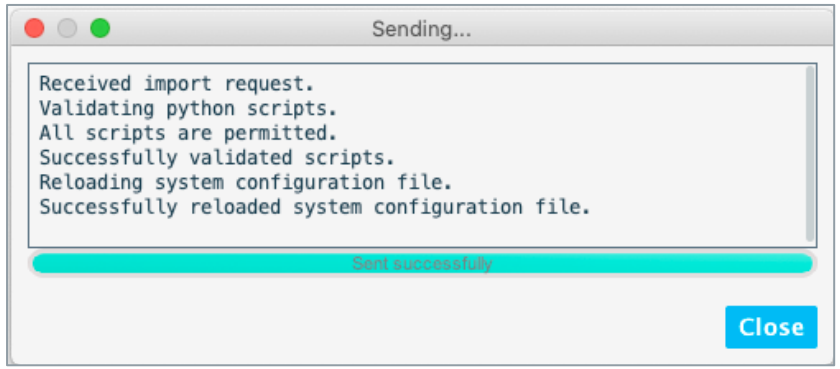
SSH to the Enterprise Manager or Stand-alone appliance and login as cliadmin. Enter the command *fstool allow_unsigned_connect_app_install true*

```
[root@twtpfsvct01 python_logs]# fstool allow_unsigned_connect_app_install true
fs.eyeextend.connect.allow.unsigned.install=true
[root@twtpfsvct01 python_logs]#
```

In the Forescout Console go to *Options* -> *Connect* and select Import to upload the apex.zip file.



Configure the Apex App



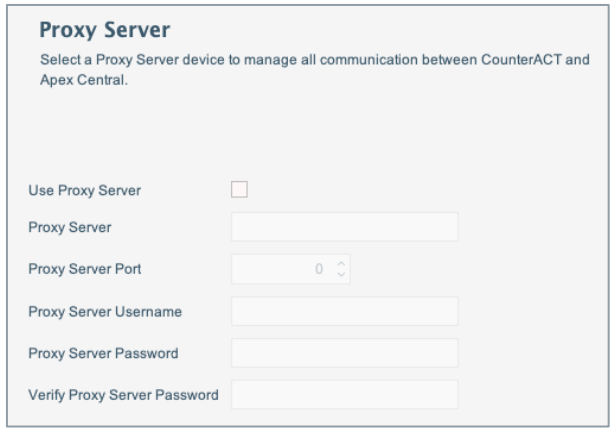
After the app loads successfully you can configure the Apex App.

Click the Add button to begin the configuration.

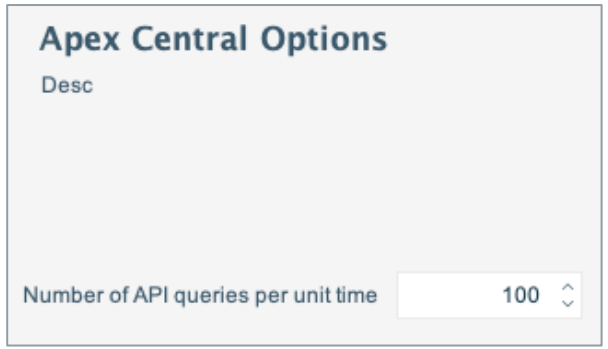
Provide the URL of the Apex Central server as well as Application ID and API Key from the earlier step.

The Validate Server Certificate option can remain unchecked if not necessary.

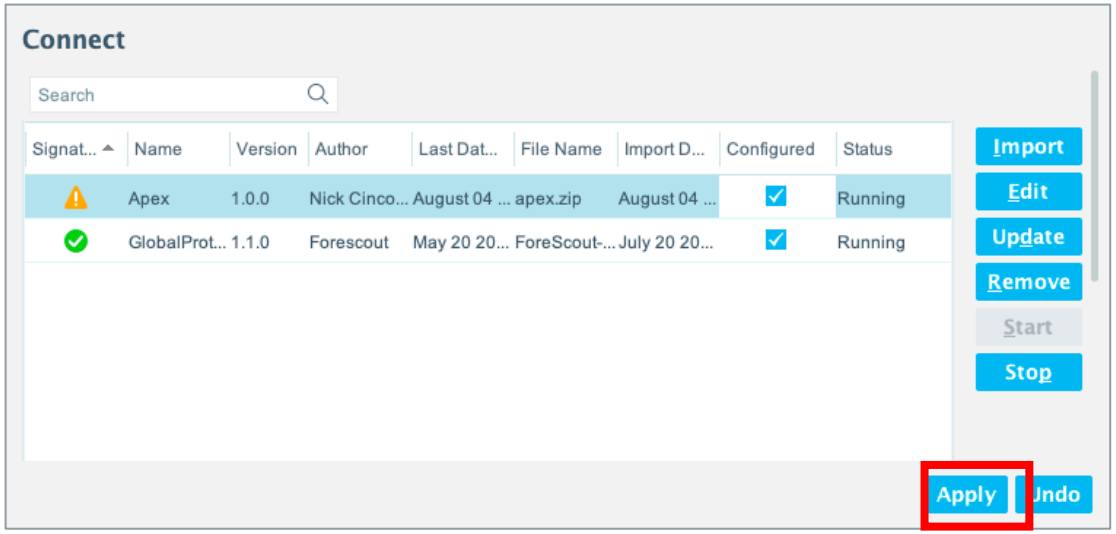
Configure the Apex App



If a proxy server needs to be configured for communication between Forescout and Apex Central, configure the settings here.



Set the number of API queries per minute or leave the default. Click Finish when done.

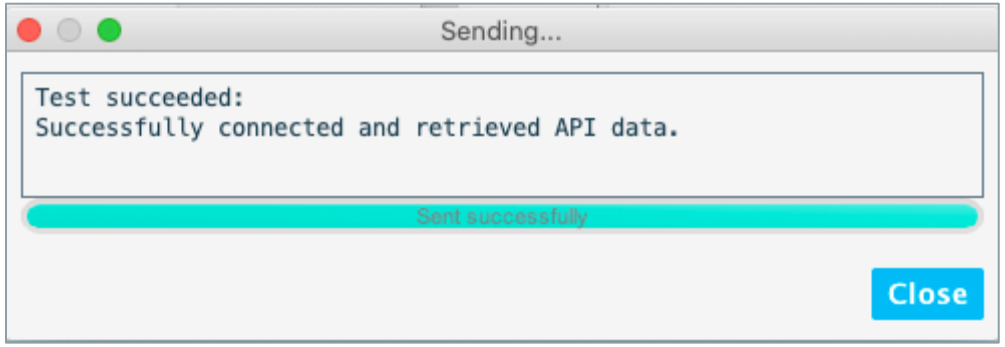


Click OK and back at the main screen you should now see the app loaded. Hit apply to save.

Configure the Apex App

Highlight the Apex app and click Edit. Then test to check the settings.

The test should complete successfully. Troubleshoot if there are any issues.



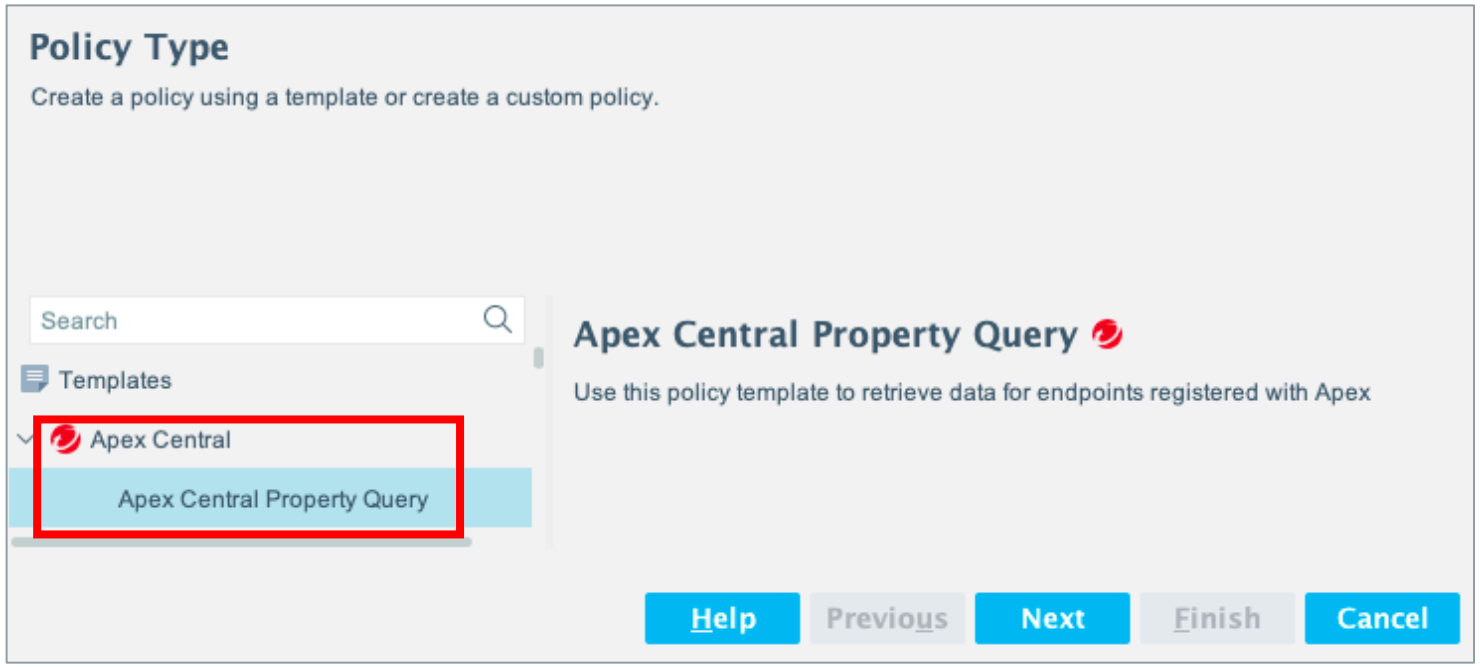
The Connect App for Apex should now be installed, and its properties and actions can be used in policy templates.

USING THE APP

Import the Apex Policy Template

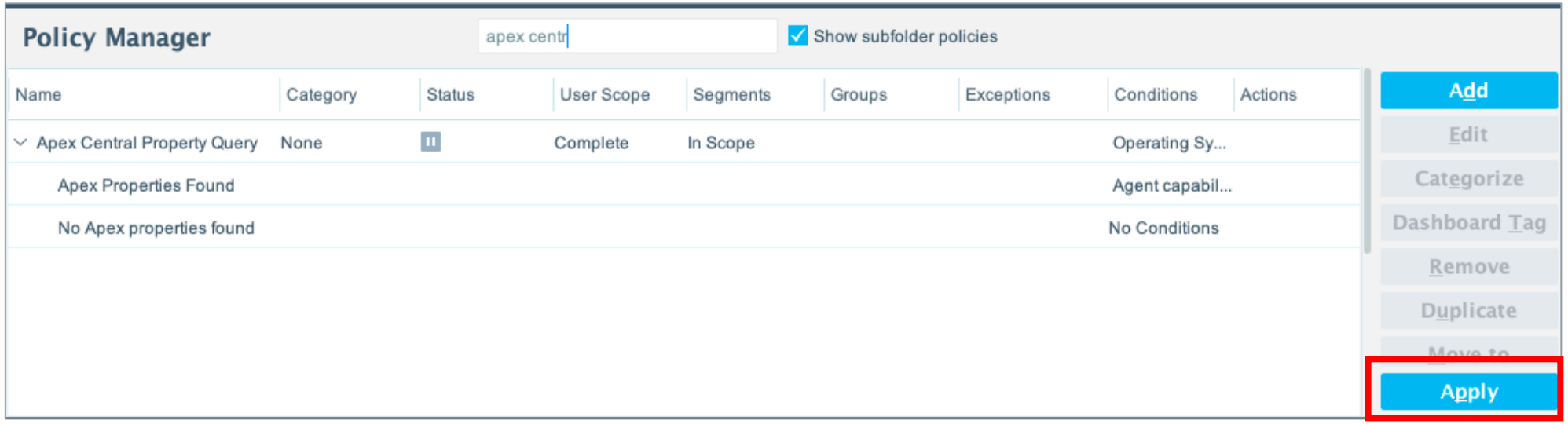
The quickest way to get started with retrieving Apex data for endpoints is to import the Apex policy template.

In the Forescout Console go to Policies and click Add. Select the Apex Central Property Query policy and click Next

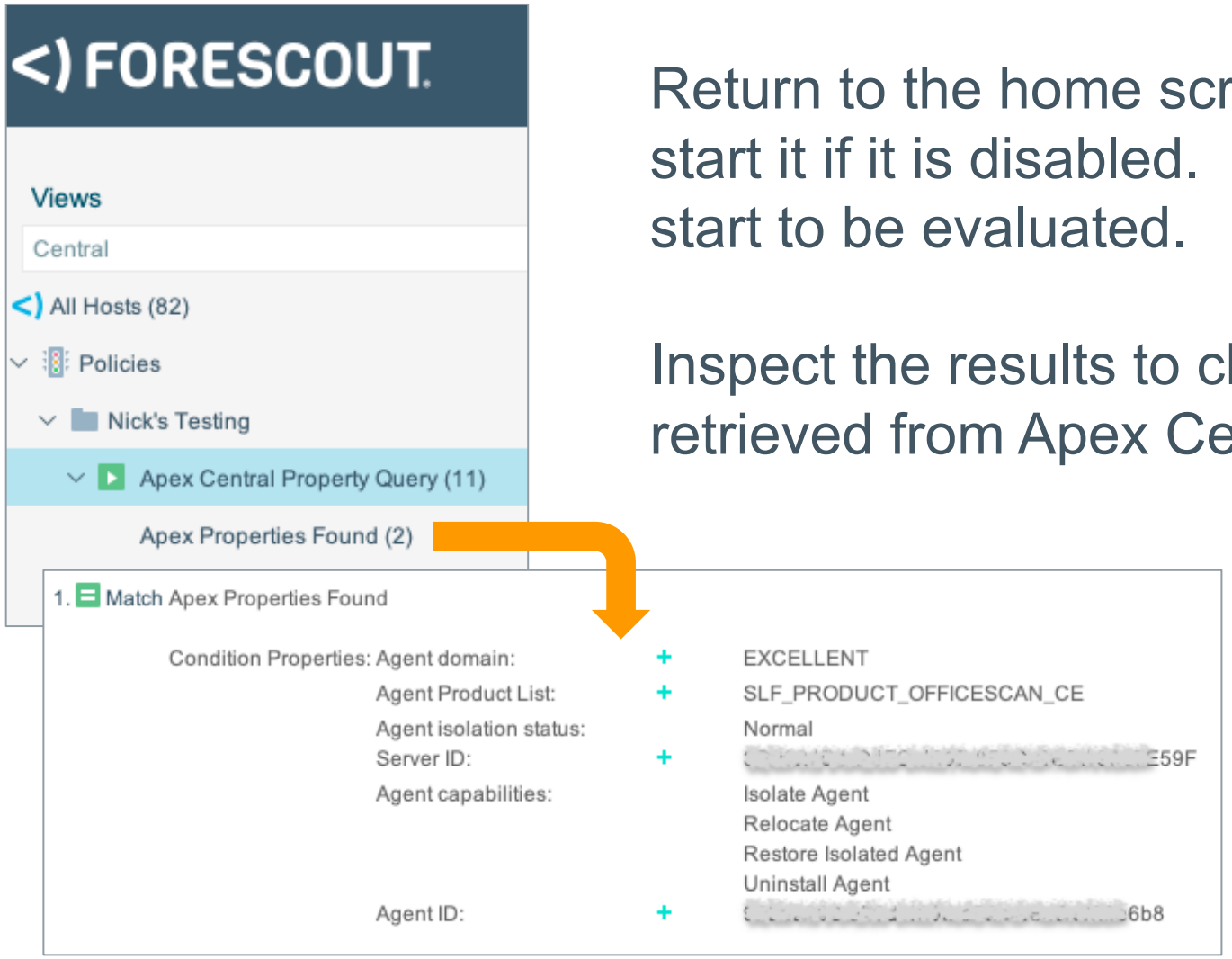


Configure the Apex Policy Template

Provide a policy name and set the scope. Select all other defaults and finish when complete. After the policy is configured be sure to hit apply to save the changes.



Configure the Apex Policy Template



Return to the home screen and find the policy and start it if it is disabled. Endpoints should immediately start to be evaluated.

Inspect the results to check the data that is being retrieved from Apex Central.

Apex Property List

This is the current list of all properties that can be retrieved from Apex Central via API. They can be used in custom compliance policies.

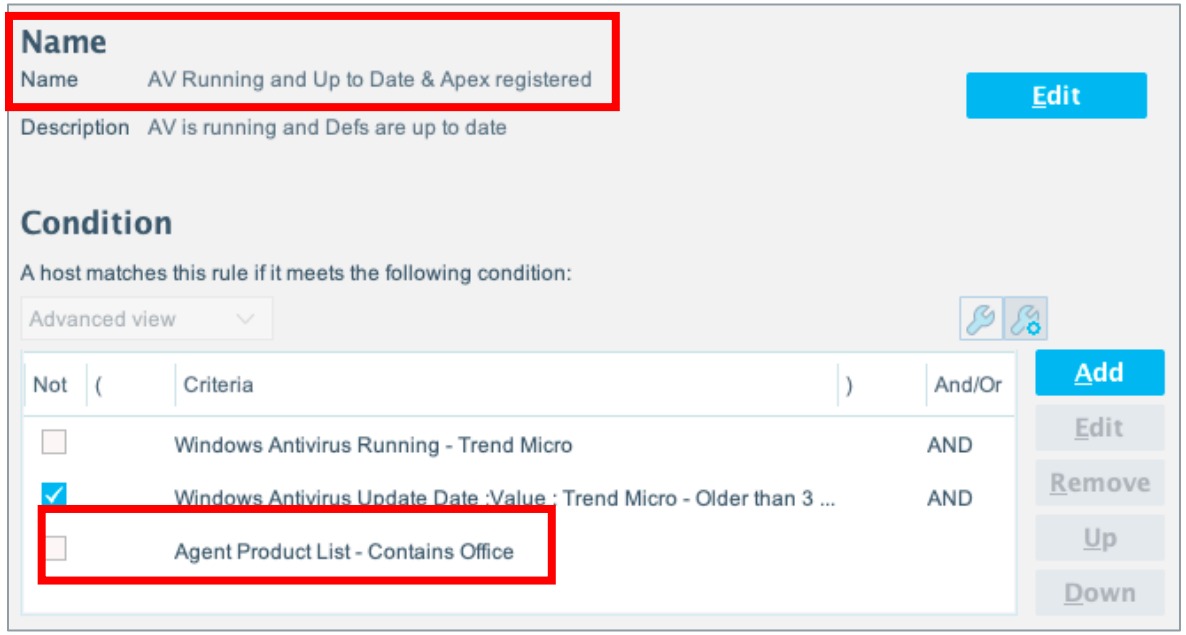
Property	Description
Agent Domain	The Active Directory domain the agent belongs to.
Agent Product List	Trend Micro products enabled for the endpoint.
Agent Isolation Status	Indicates the agent isolation status.
Server ID	The GUID of the Apex server managing the agent.
Agent Capabilities	Lists the API actions that can be performed on the agent.
Agent ID	The Apex GUID of the Security Agent

Enhance AntiVirus Compliance Policies

One use case for the properties retrieved from the Apex server is to enhance the capabilities of your AntiVirus compliance checking by not only checking the client-side settings but also ensuring that the device is registered with Apex server-side as well.

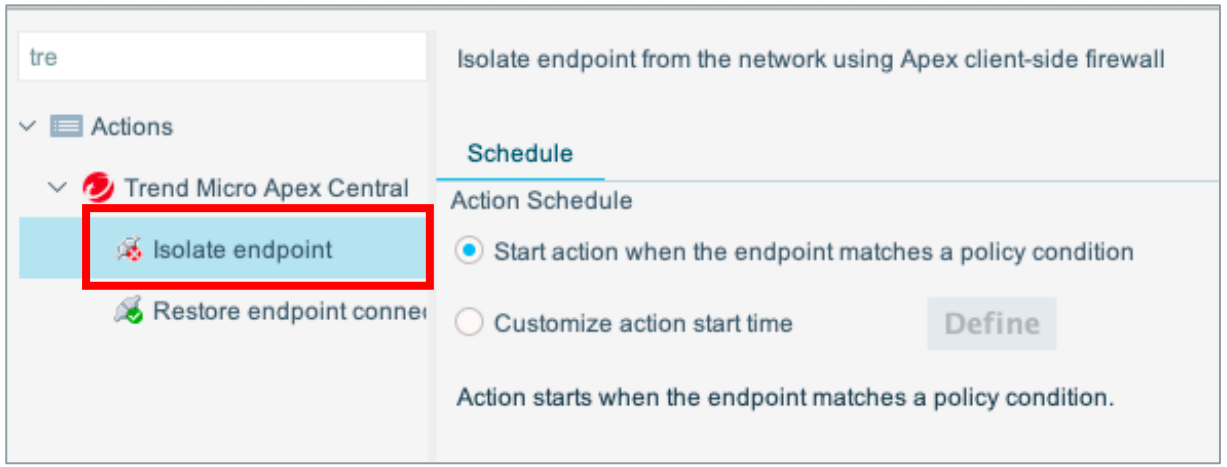
The easiest way to do this is to duplicate the compliant sub-rule for your antivirus policy and add a condition for Agent Product List -> Contains (AV product name).

Rename it to reflect that the endpoint is compliant and registered with Apex.



Endpoint Isolation

The app supports blocking network connectivity for endpoints by placing them in isolation through Apex Central. This action can be used wherever appropriate as a response to compliance failures and malicious behavior.



Simply select the Trend Micro Apex Central -> Isolate Endpoint action and apply it in your policy.

Apex will place targeted endpoints in network isolation and the user will receive notice. This works via the agent firewall blocking traffic. Once the action is removed network connectivity will be automatically restored.