



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.

<) FORESCOUT.

Views

Search

▼ Apex Central Property Query (6)

Apex Properties Found (1)

1. Match Apex Properties Found

Condition Properties:

Agent domain:	+	EXCELLENT
Agent Product List:	+	SLF_PRODUCT_OFFICESCAN_CE
Agent isolation status:		Normal
Server ID:	+	[REDACTED] E59F
Agent capabilities:		Isolate Agent Relocate Agent Restore Isolated Agent Uninstall Agent
Agent ID:	+	[REDACTED] 6b8

Retrieve Apex Data

Endpoint Isolation

Trend Micro Apex Central

Isolate endpoint

Restore endpoint connectivity

Endpoint Isolated

OfficeScan has detected suspicious network connections originating from your endpoint. To prevent the risk from spreading, the Control Manager administrator has enforced measures that restrict you from accessing network resources.

OK

TREND MICRO | OfficeScan

6:11 PM
8/4/2020

Requirements



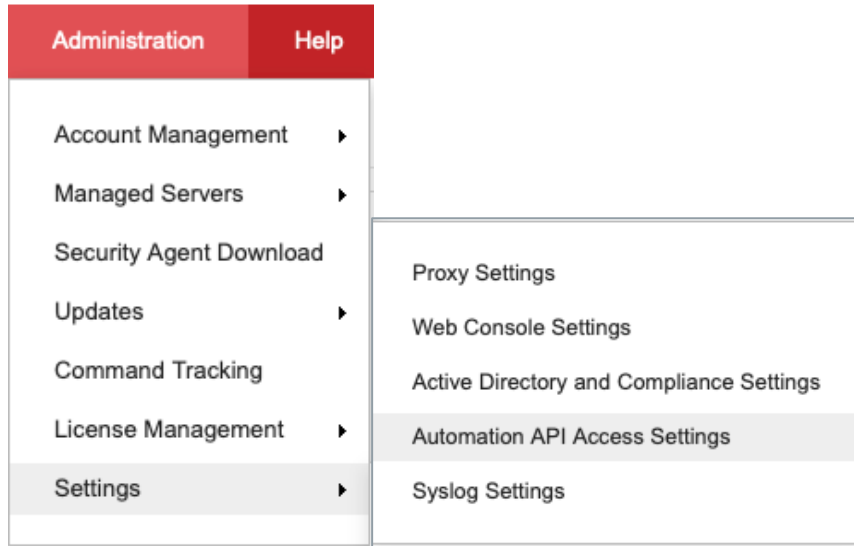
- eyeSight 8.1 or above
- eyeExtend Connect Module
- Valid license for both products
- Connect app for Trend Micro Apex



- 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 fore scout. Copy the Application ID and API key for later use.



The screenshot shows the 'Application Access Settings' form. It includes a checkbox to 'Enable application integration using Apex Central Automation APIs'. Below this, there are fields for 'Application name' (fore scout), 'Application ID' (B875), 'API key' (44FF), 'API type' (Isolate/Restore endpoint connections), and 'Communication time-out' (120 seconds). At the bottom are 'Save' and 'Cancel' buttons.

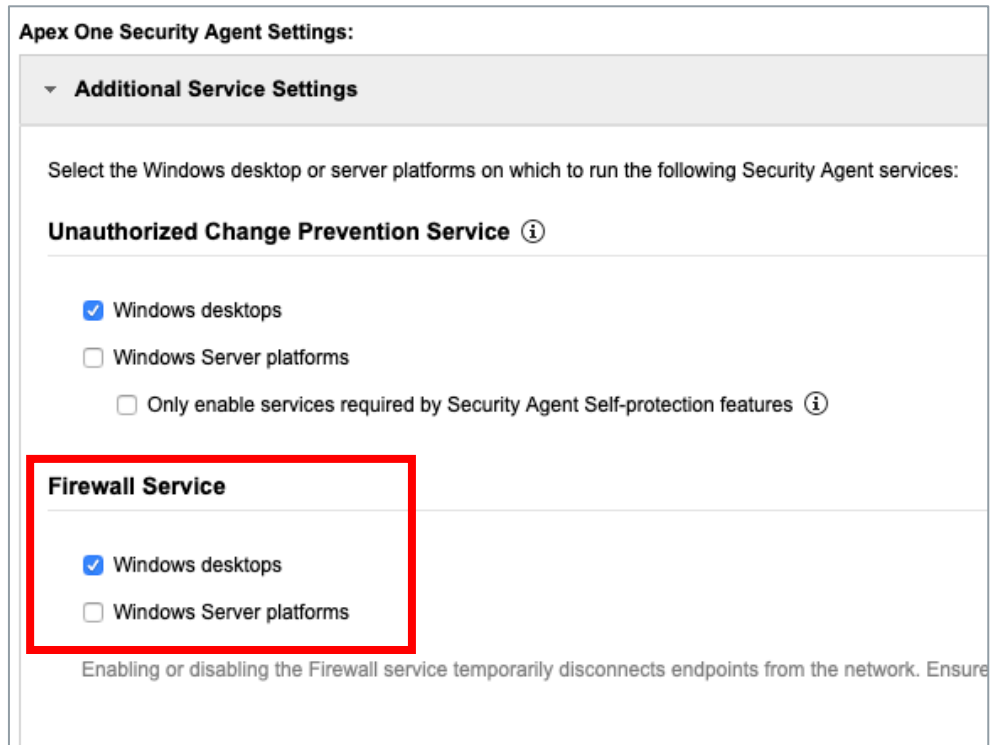
Enable Firewall for Endpoint Isolation (Optional)



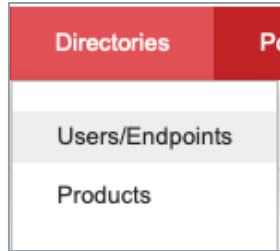
If not already configured, the Apex firewall service for endpoints will need to be enabled for isolation to work.

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

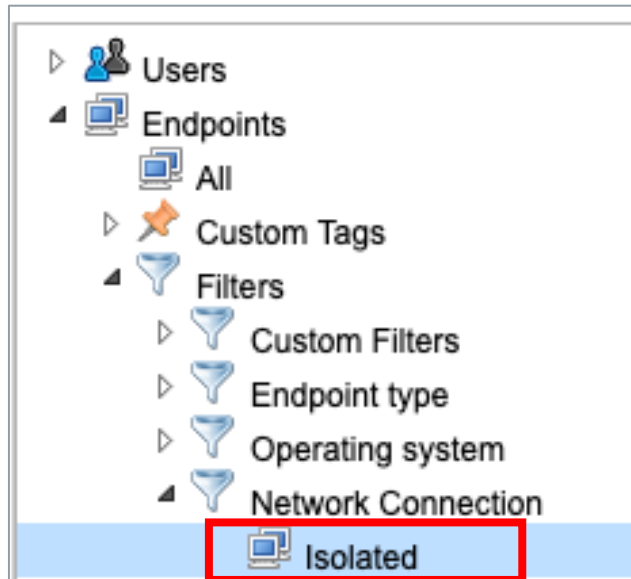
Make sure to take caution and understand the impact of changes you make in a production environment.



Add Exemptions for Isolation

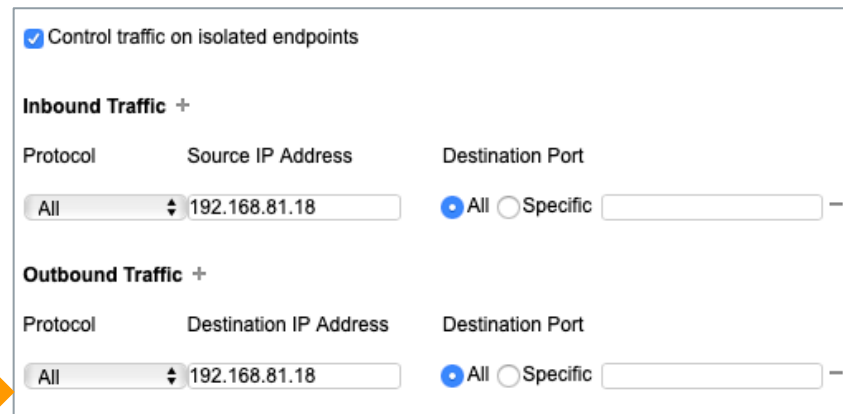
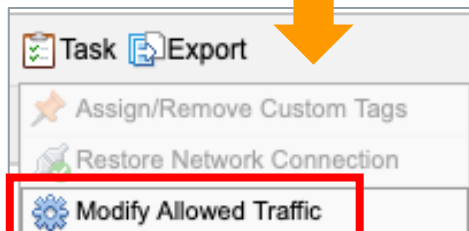


Traffic exceptions should be added to allow communication to and from Apex servers and Forescout the endpoint is isolated.



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

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

A screenshot of the 'Modify Allowed Traffic' configuration panel. At the top, there is a checkbox labeled 'Control traffic on isolated endpoints' which is checked. Below this, there are two sections: 'Inbound Traffic' and 'Outbound Traffic'. Each section has a table with columns for 'Protocol', 'Source IP Address' (for inbound) or 'Destination IP Address' (for outbound), and 'Destination Port'. In both sections, the 'Protocol' is set to 'All', the IP address is '192.168.81.18', and the 'Destination Port' is set to 'All' (selected with a radio button).

Protocol	Source IP Address	Destination Port
All	192.168.81.18	All

Protocol	Destination IP Address	Destination Port
All	192.168.81.18	All

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

FORESCOUT CONFIGURATION

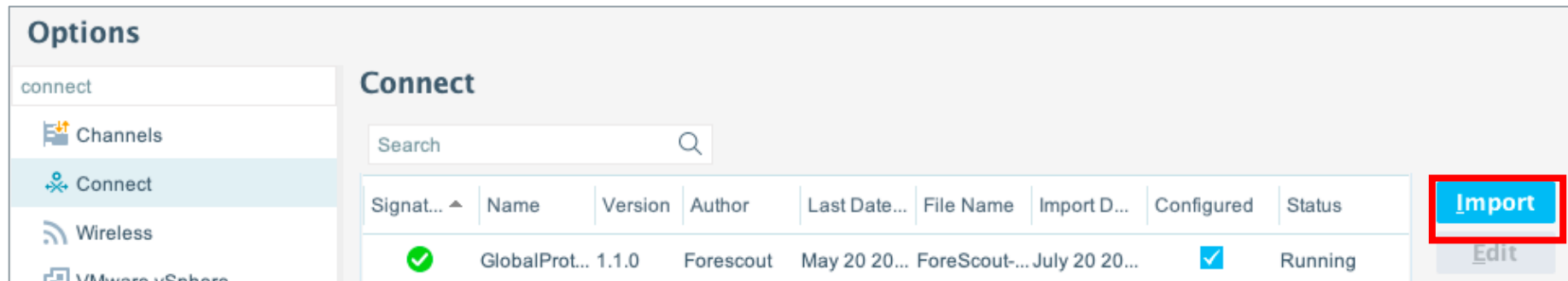
Upload the App to Connect Module

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.eyextend.connect.allow.unsigned.install=true  
[root@twtpfsvct01 python_logs]#
```

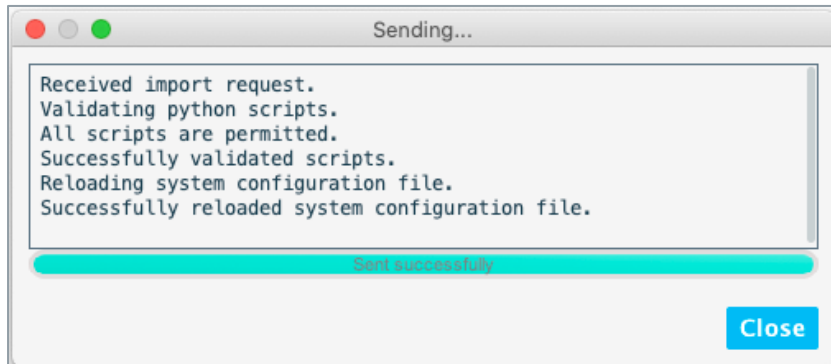
In the Forescout Console go to *Options* -> *Connect* and select Import to upload the apex.zip file.



The screenshot shows the Forescout Console interface. On the left, the 'Options' sidebar has 'Connect' selected. The main content area is titled 'Connect' and features a search bar and a table of installed applications. The table has columns for Signat..., Name, Version, Author, Last Date..., File Name, Import D..., Configured, and Status. One application is listed: 'GlobalProt...' with version '1.1.0', author 'Forescout', and status 'Running'. The 'Import' button is highlighted with a red box.

Signat...	Name	Version	Author	Last Date...	File Name	Import D...	Configured	Status
✓	GlobalProt...	1.1.0	Forescout	May 20 20...	ForeScout-...	July 20 20...	✓	Running

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.

Apex Central Connection

Apex Central server connection details

URL	<input type="text" value="https://192.168.81.18:443"/>
Application ID	<input type="text" value="8360F85D-487F-F55SA-3298F9f"/>
API Key	<input type="password" value="*****"/>
Verify API Key	<input type="password" value="*****"/>
Validate Server Certificate	<input type="checkbox"/>

Configure the Apex App

Proxy Server
Select a Proxy Server device to manage all communication between CounterACT and Apex Central.

Use Proxy Server ☐

Proxy Server

Proxy Server Port

Proxy Server Username

Proxy Server Password

Verify Proxy Server Password

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.

Apex Central Options

Desc

Number of API queries per unit time

Connect

Search

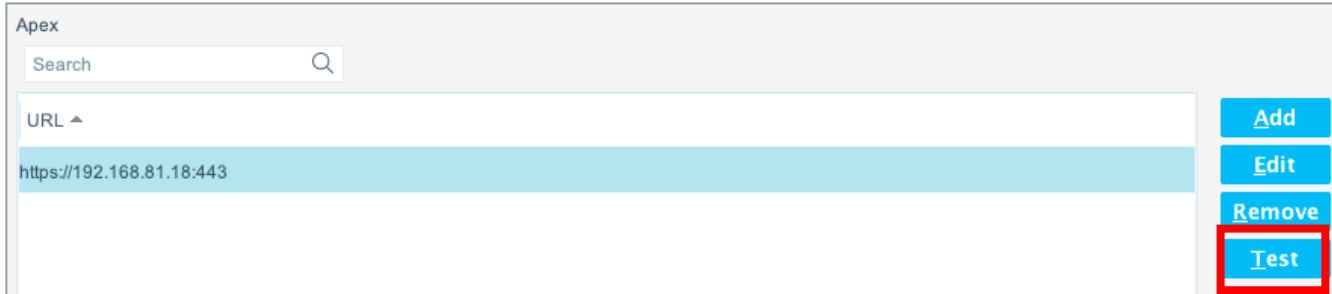
Signal...	Name	Version	Author	Last Dat...	File Name	Import D...	Configured	Status
⚠	Apex	1.0.0	Nick Cinco...	August 04 ...	apex.zip	August 04 ...	☑	Running
✓	GlobalProt...	1.1.0	Forescout	May 20 20...	ForeScout-...	July 20 20...	☑	Running

Import
Edit
Update
Remove
Start
Stop

Apply **Undo**

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

Configure the Apex App



Apex

Search

URL ^

https://192.168.81.18:443

Add

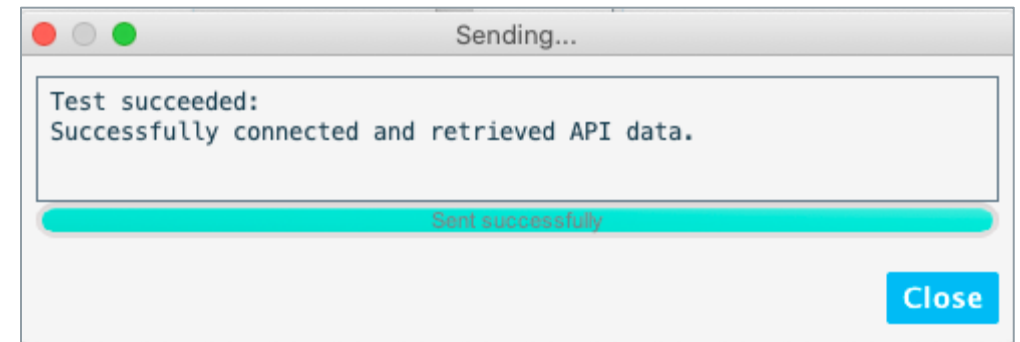
Edit

Remove

Test

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

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



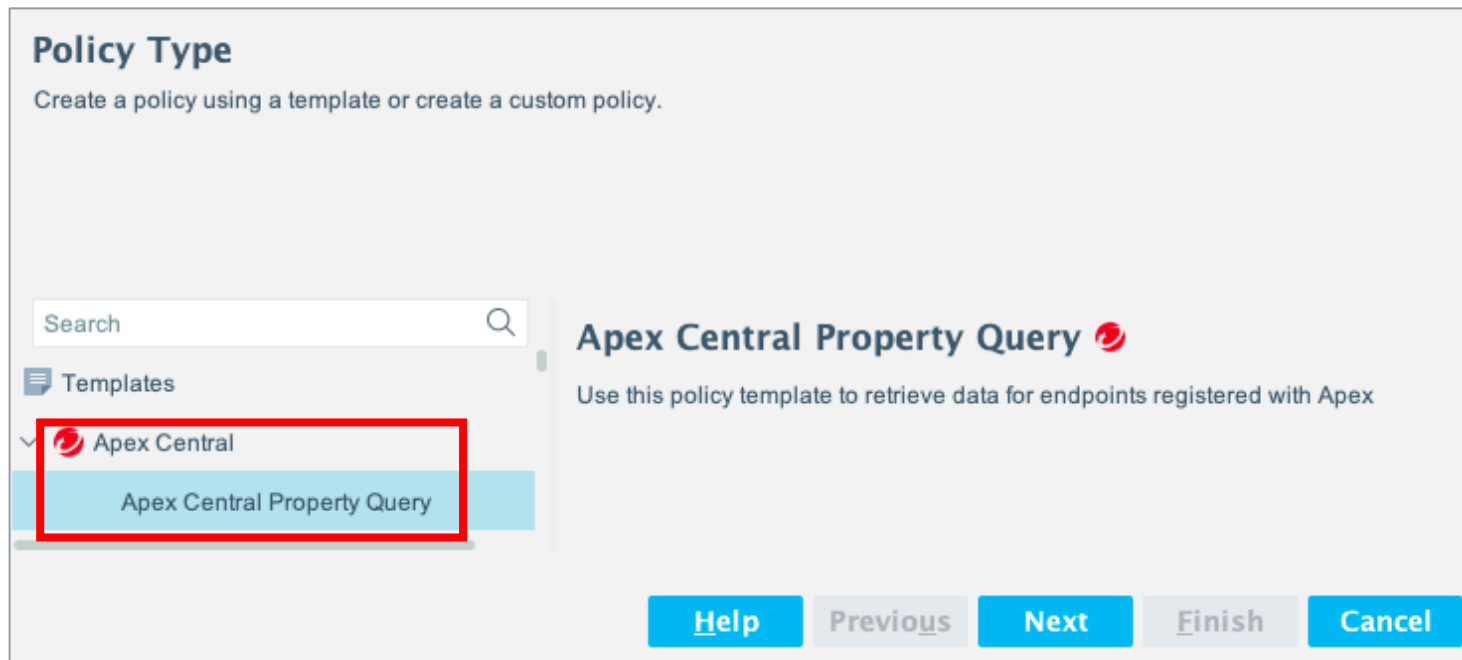
The Connect App for Apex should now be installed, and its properties and actions can be used in policy templates.

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



Policy Type
Create a policy using a template or create a custom policy.

Search

Templates

- ✓ Apex Central
 - Apex Central Property Query

Apex Central Property Query

Use this policy template to retrieve data for endpoints registered with Apex

Help Previous Next Finish Cancel

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.

Policy Manager

apex centr

☒ Show subfolder policies

Name	Category	Status	User Scope	Segments	Groups	Exceptions	Conditions	Actions
▼ Apex Central Property Query	None	⏸	Complete	In Scope			Operating Sy...	
Apex Properties Found							Agent capabil...	
No Apex properties found							No Conditions	

Add

Edit

Categorize

Dashboard Tag

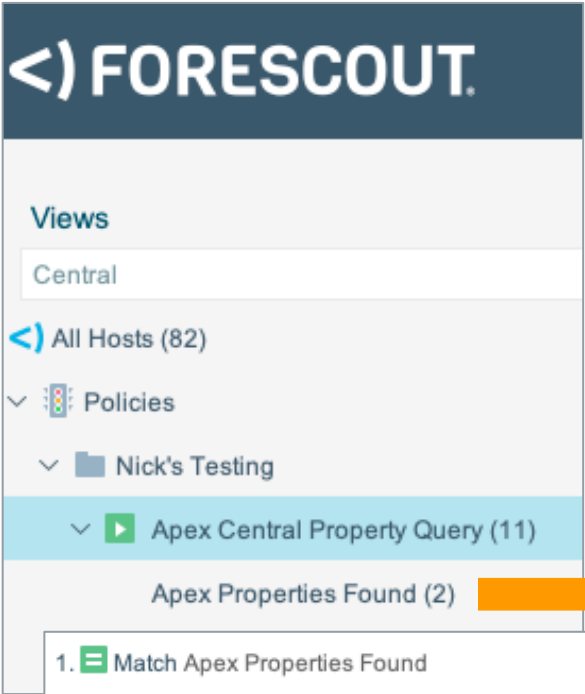
Remove

Duplicate

Move to

Apply

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.

1. Match Apex Properties Found

Condition Properties: Agent domain:	+	EXCELLENT
Agent Product List:	+	SLF_PRODUCT_OFFICESCAN_CE
Agent isolation status:		Normal
Server ID:	+	E59F
Agent capabilities:		Isolate Agent Relocate Agent Restore Isolated Agent Uninstall Agent
Agent ID:	+	6b8

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

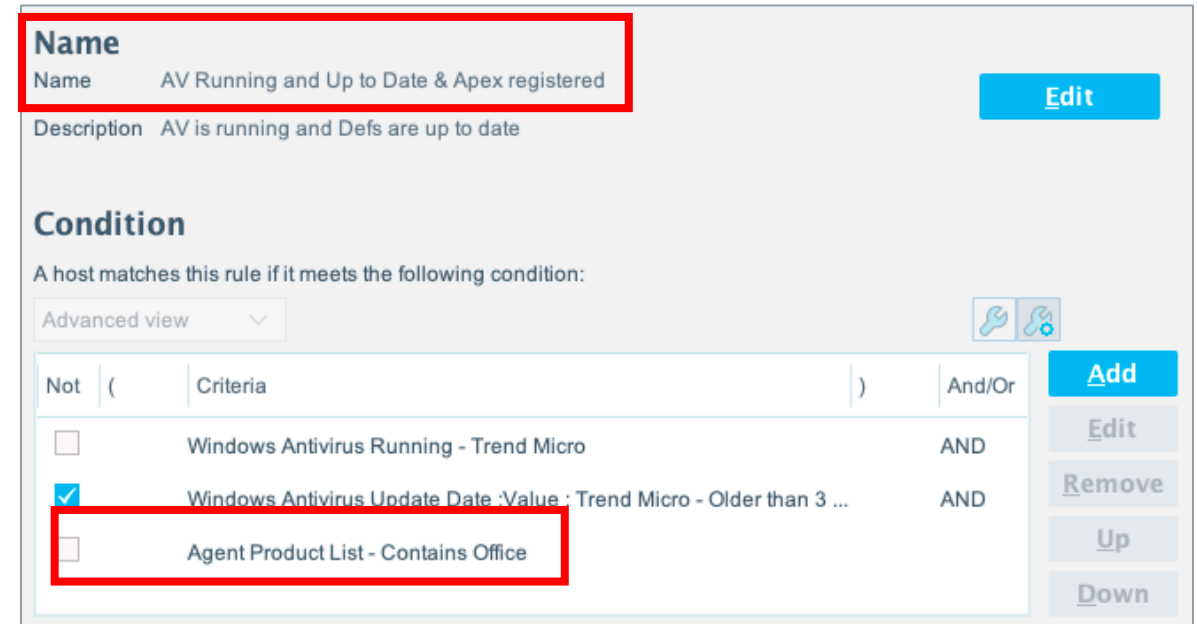
Enhance AntiVirus Compliance Policies



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.

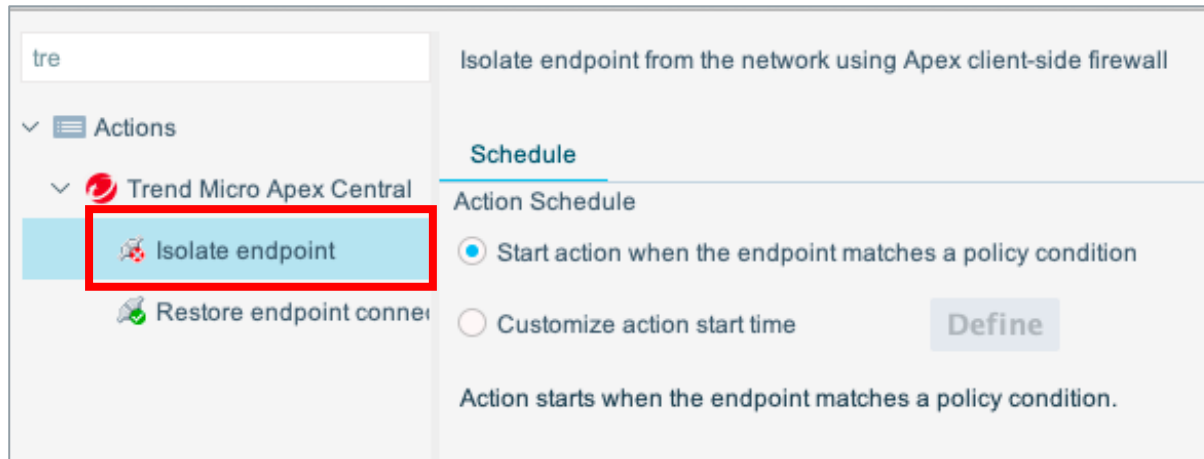
The easiest way to do this is to duplicate the compliant sub-rule for your antivirus policy and add a condition for Agent Product List -> Contains (AV product name).

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.

