IBM Security Verify Privilege On-Premises
Version 10.9

Cylance Connector Guide

IBM

Contents

Last modified: September 21, 2020

Getting started

Cylance is an Artificial Intelligence Based Advanced Threat Prevention Solution for enterprise environments. Privilege Manager integrates with Cylance to help you proactively act on any unknown applications that run in your environment to prevent potential malware attacks.

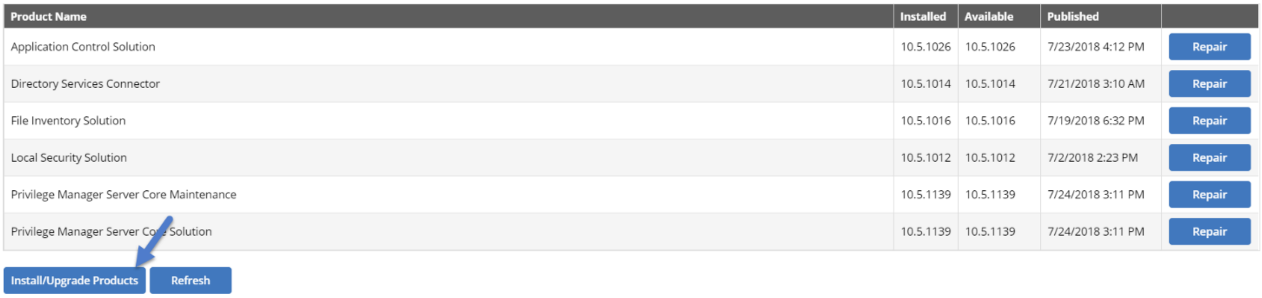
The following steps describe how to integrate Cylance with Privilege Manager and create an example policy to begin using Cylance intelligence in action across your environment.

Remember that while the Cylance integration provides insight into threat analysis, ultimately you can use Privilege Manager policies to act or react in whatever way makes most sense to your organization.

Configuring the connector

1. Open a browser on your Privilege Manager Web Server, browse to *https://[YourInstanceName]/TMS/Setup/*

2. On the Currently Installed Products screen, choose **Install/Upgrade Products**.



Product Name	Installed	Available	Published	
Application Control Solution	10.5.1026	10.5.1026	7/23/2018 4:12 PM	Repair
Directory Services Connector	10.5.1014	10.5.1014	7/21/2018 3:10 AM	Repair
File Inventory Solution	10.5.1016	10.5.1016	7/19/2018 6:32 PM	Repair
Local Security Solution	10.5.1012	10.5.1012	7/2/2018 2:23 PM	Repair
Privilege Manager Server Core Maintenance	10.5.1139	10.5.1139	7/24/2018 3:11 PM	Repair
Privilege Manager Server Core Solution	10.5.1139	10.5.1139	7/24/2018 3:11 PM	Repair

3. Install the connector.

    a. Select option **Thycotic Cylance Reputation Connector**.

    b. Click **Install** and **Accept** the End User License Agreement. You will see your Installation Progress.

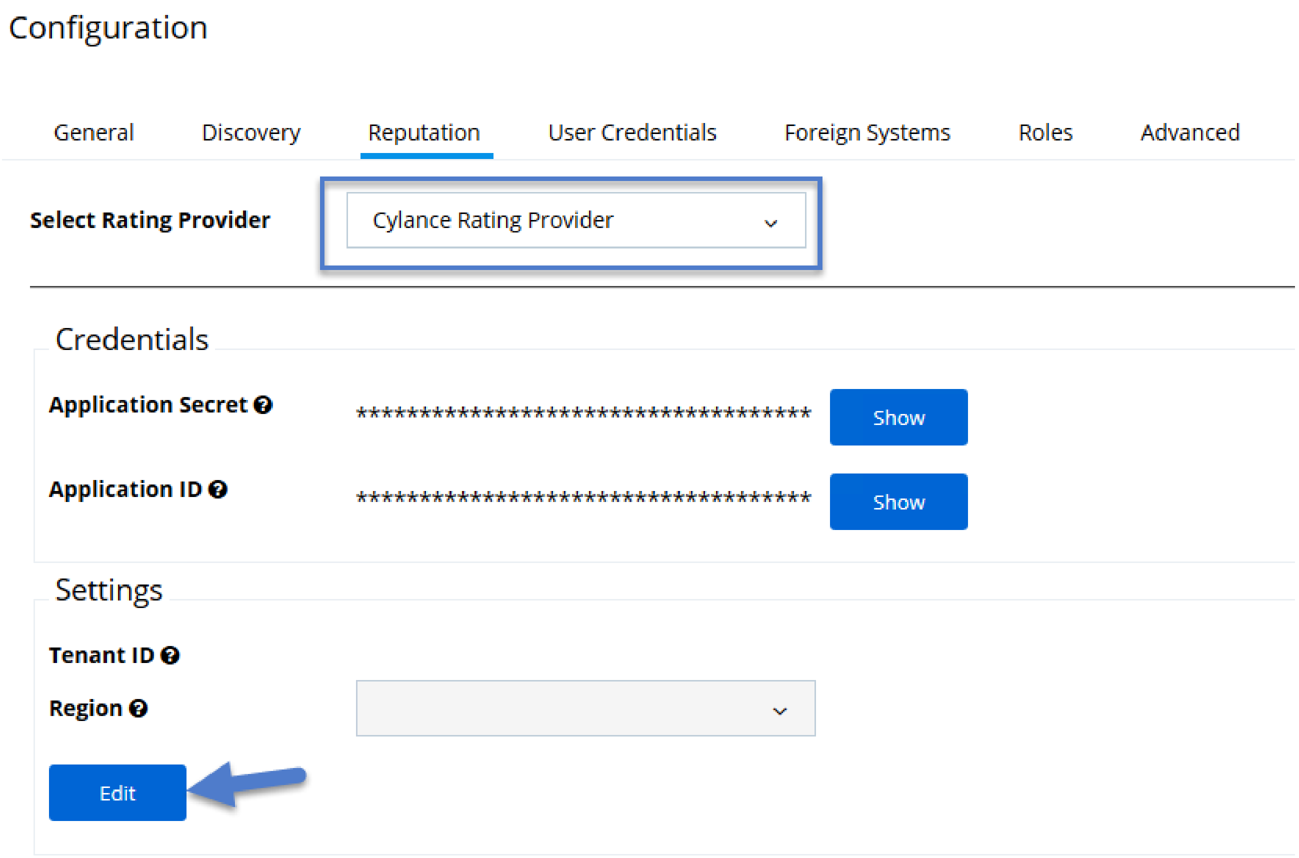
    c. Click “**Show install Logs**” to check for any errors.

    Note: If the installation of Cylance initially fails, redirect to `https://[YourInstanceName]/TMS/Setup/` and click **Repair**.

4. After installation completes, click the **Home** button.

5. Browse to **Thycotic Privilege Manager > Admin > Configuration > Reputation** tab.

6. For **Select Rating Provider**. select **Cylance Rating Provider**, then click **Edit**.



Configuration

Select Rating Provider Cylance Rating Provider

Credentials

Application Secret ***********************************

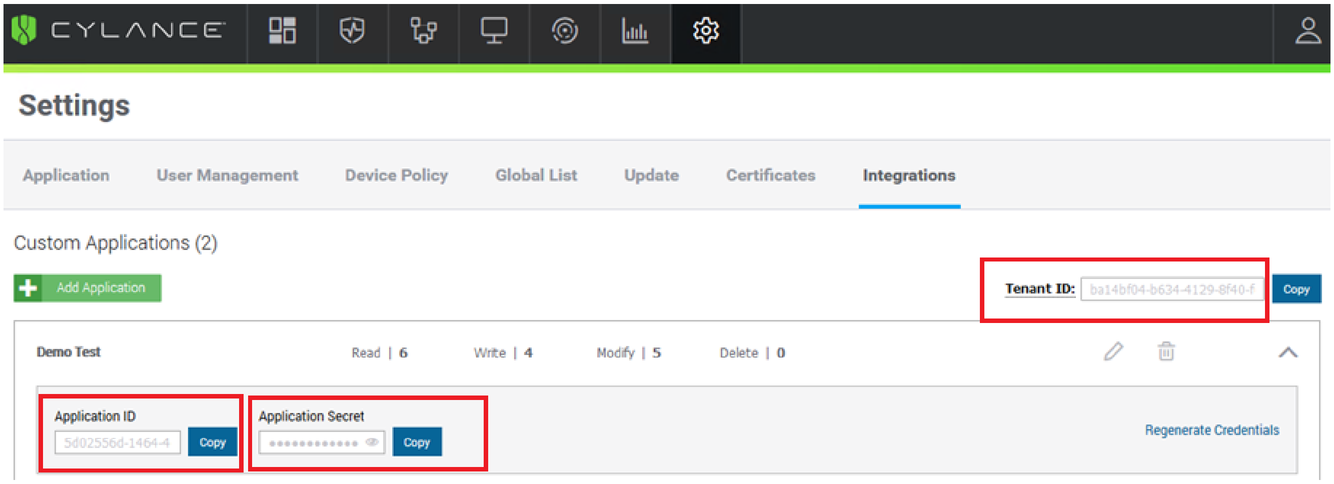
Application ID ***********************************

Settings

Tenant ID

Region

7. Enter the required **Credentials** and **Settings** Details.
   Locate these details in your Cylance account. Log in at protect.cylance.com under **Integrations > Custom Applications**.



Settings

Custom Applications (2)

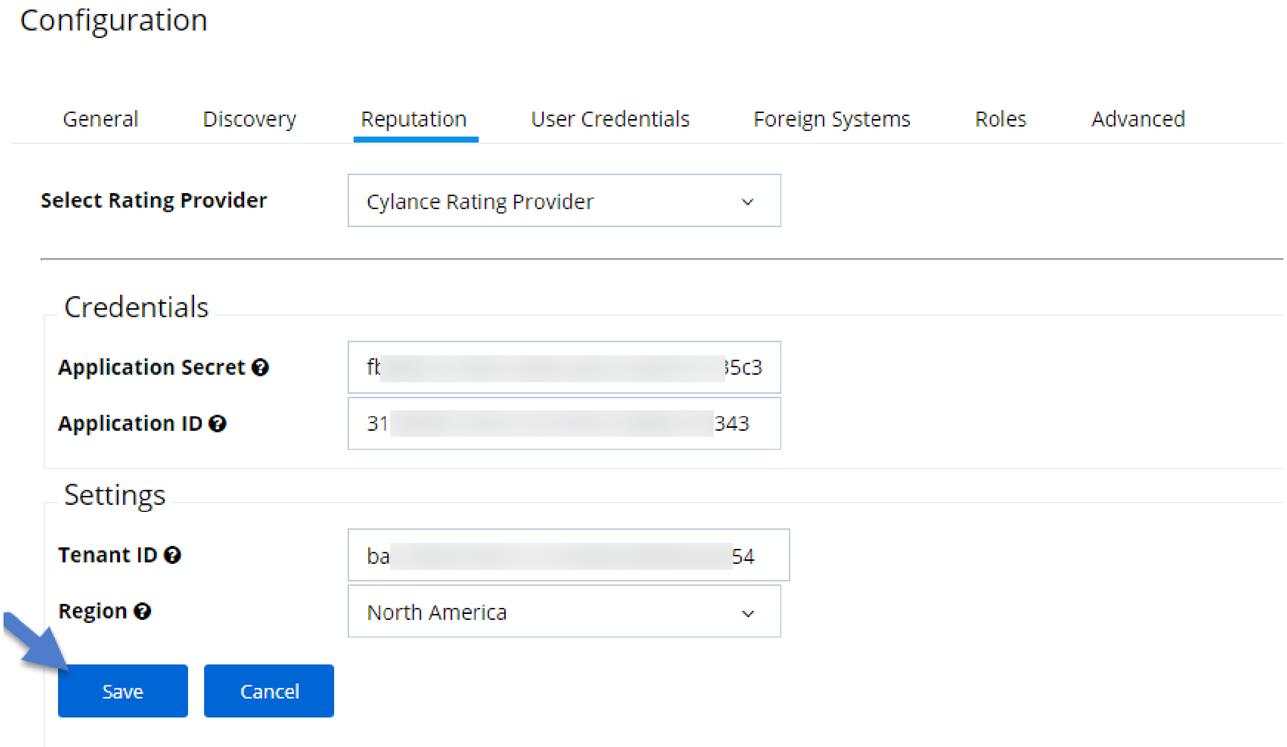
Tenant ID: ba14bf04-b634-4129-8f40-f

Demo Test Read | 6 Write | 4 Modify | 5 Delete | 0

Application ID 5d02556d-1464-4

Application Secret ••••••••••••

8. When required details are entered, click **Save**.



Select Rating Provider: Cylance Rating Provider

Credentials

Application Secret: f[redacted]5c3

Application ID: 31[redacted]343

Settings

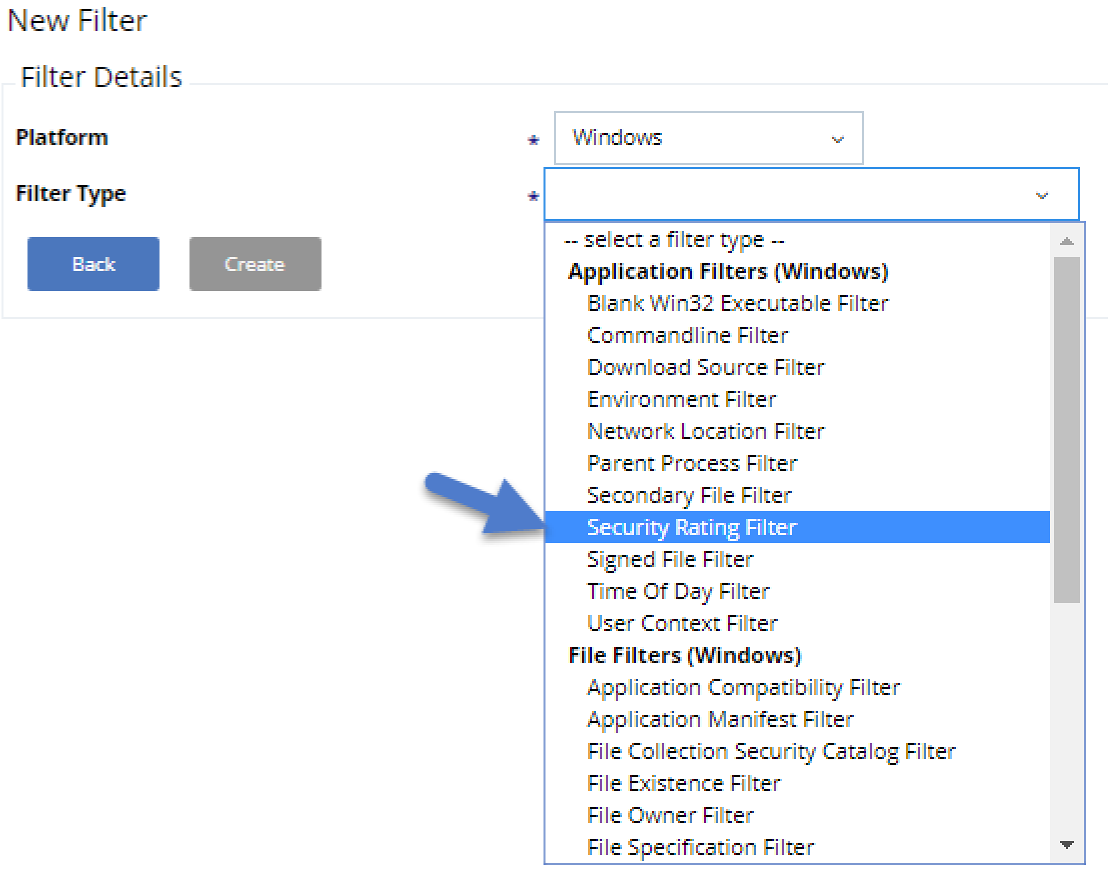
Tenant ID: ba[redacted]54

Region: North America

Creating a Cylance Security Rating filter

1. Next, in Privilege Manager navigate to **Admin > More > Filters**, then click **Add Filter**.

2. Select a platform, and for **Filter Type**, select **Security Rating Filter**. Name the policy and add a description.



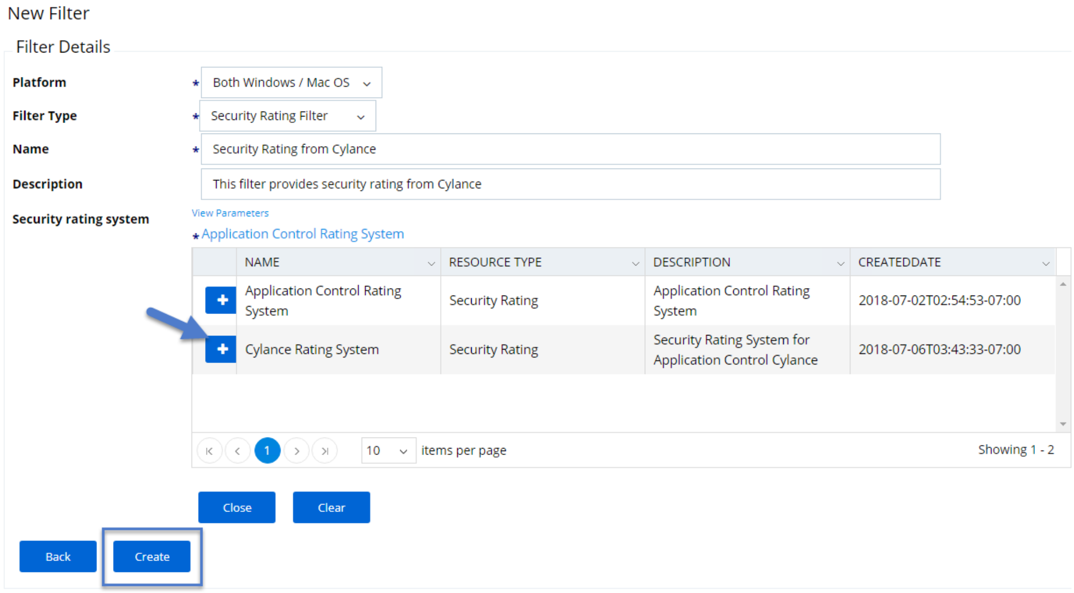
New Filter

Filter Details

Platform * Windows

Filter Type *

3. Next to Security Rating System, Click **Application Control Rating system**, then select **Cylance Rating System** from available options. Click **Create.**



New Filter

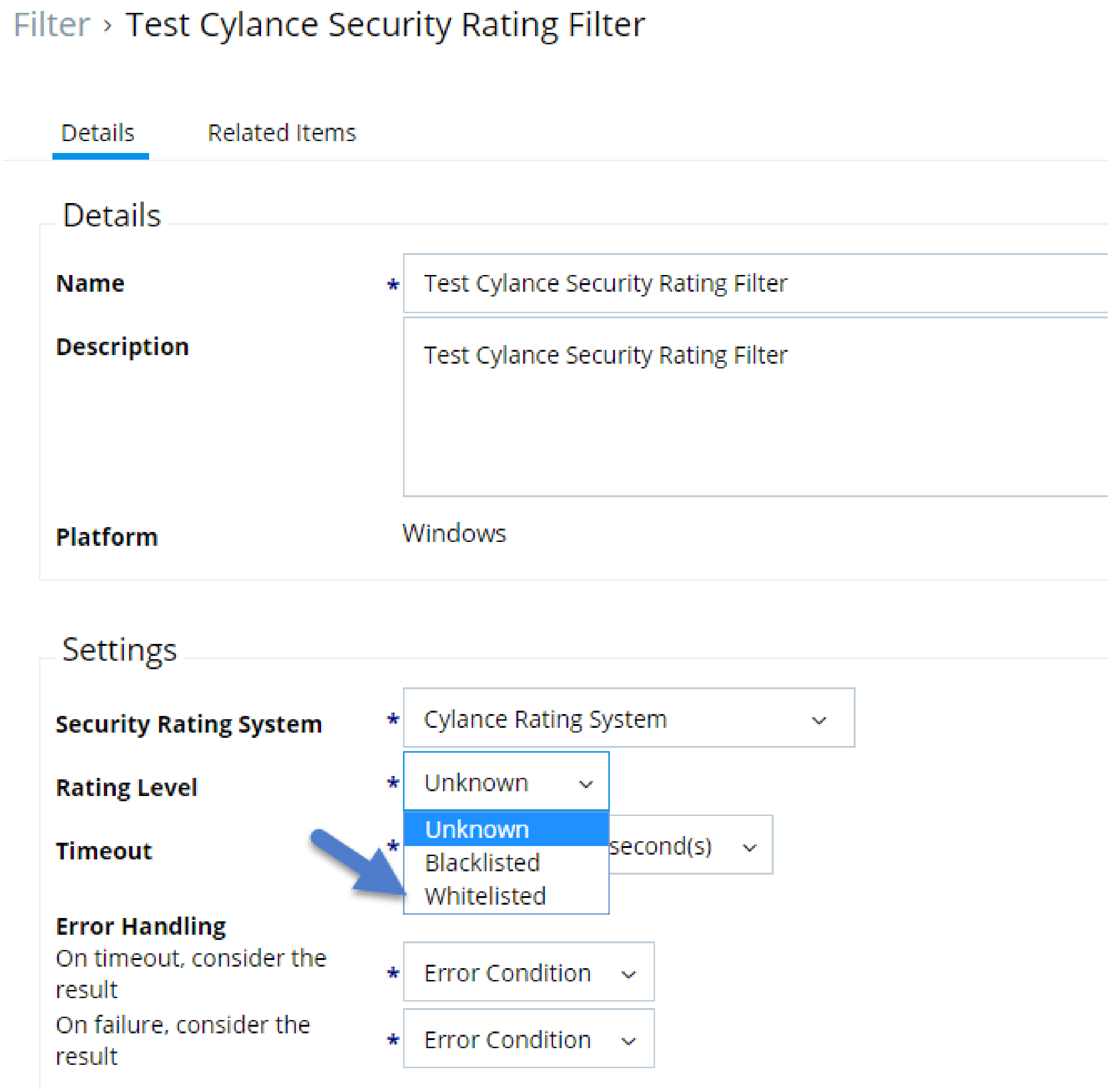
Filter Details

Platform	* Both Windows / Mac OS
Filter Type	* Security Rating Filter
Name	* Security Rating from Cylance
Description	This filter provides security rating from Cylance
Security rating system	View Parameters * Application Control Rating System

	NAME	RESOURCE TYPE	DESCRIPTION	CREATEDDATE
+	Application Control Rating System	Security Rating	Application Control Rating System	2018-07-02T02:54:53-07:00
+	Cylance Rating System	Security Rating	Security Rating System for Application Control Cylance	2018-07-06T03:43:33-07:00

4. After the filter is created, click **Edit**, select the **Rating Level**, and click **Save**

.



Filter › Test Cylance Security Rating Filter

Details | Related Items

Details

Name	* Test Cylance Security Rating Filter
Description	Test Cylance Security Rating Filter
Platform	Windows

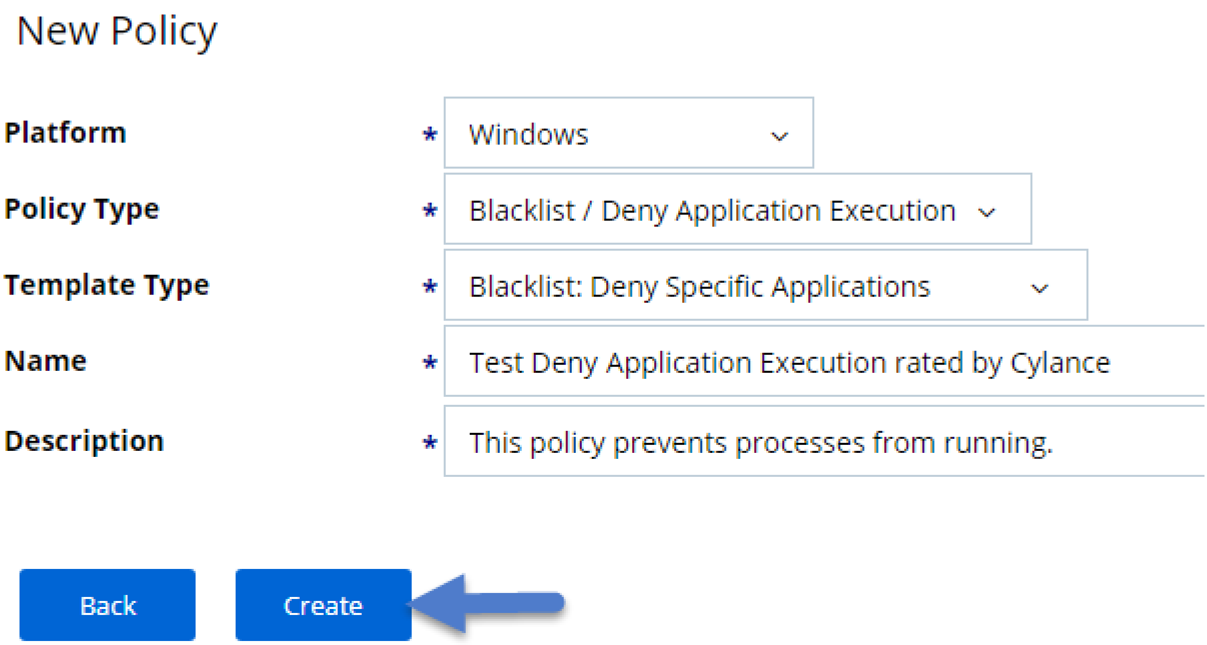
Settings

Security Rating System	* Cylance Rating System
Rating Level	* Unknown Unknown Blacklisted Whitelisted
Timeout	* second(s)
Error Handling	
On timeout, consider the result	* Error Condition
On failure, consider the result	* Error Condition

Creating a Cylance policy

1. After your Filter is created, Navigate to **Admin > Policies > Add New Policy**.

2. Select **Windows** as a Platform. Enter required details and click **Create**.



New Policy

Platform * Windows

Policy Type * Blacklist / Deny Application Execution

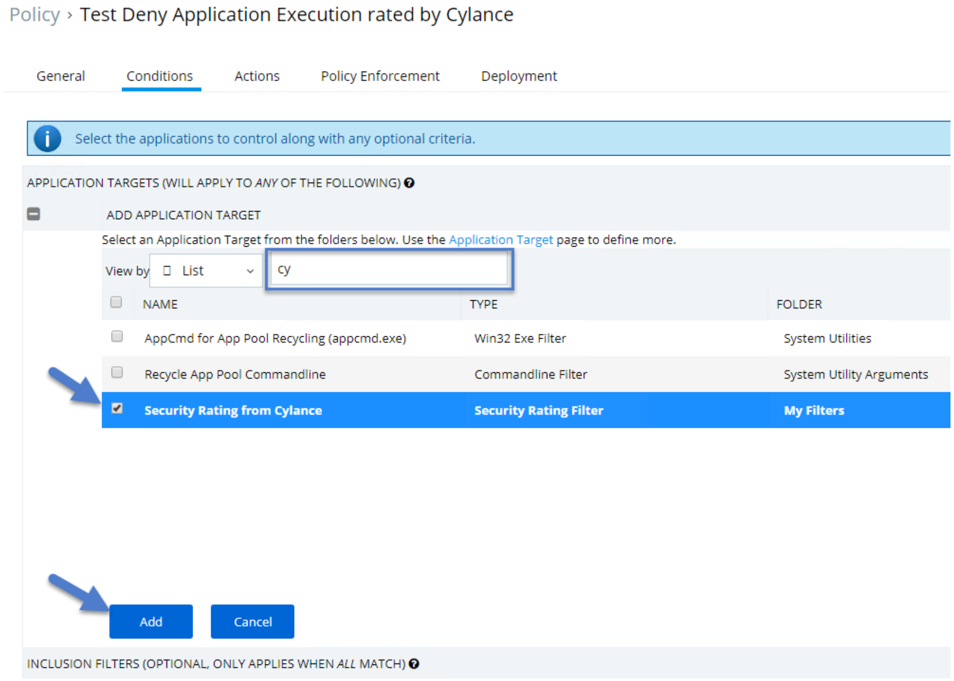
Template Type * Blacklist: Deny Specific Applications

Name * Test Deny Application Execution rated by Cylance

Description * This policy prevents processes from running.

3. Click **Edit** and check the **Enabled** box. Select the **Conditions** tab, and select **Add Application Target**.

4. Search for the Cylance filter created in the previous steps. Select that filter and click **Add**.



Policy › Test Deny Application Execution rated by Cylance

Select the applications to control along with any optional criteria.

APPLICATION TARGETS (WILL APPLY TO *ANY* OF THE FOLLOWING)

ADD APPLICATION TARGET

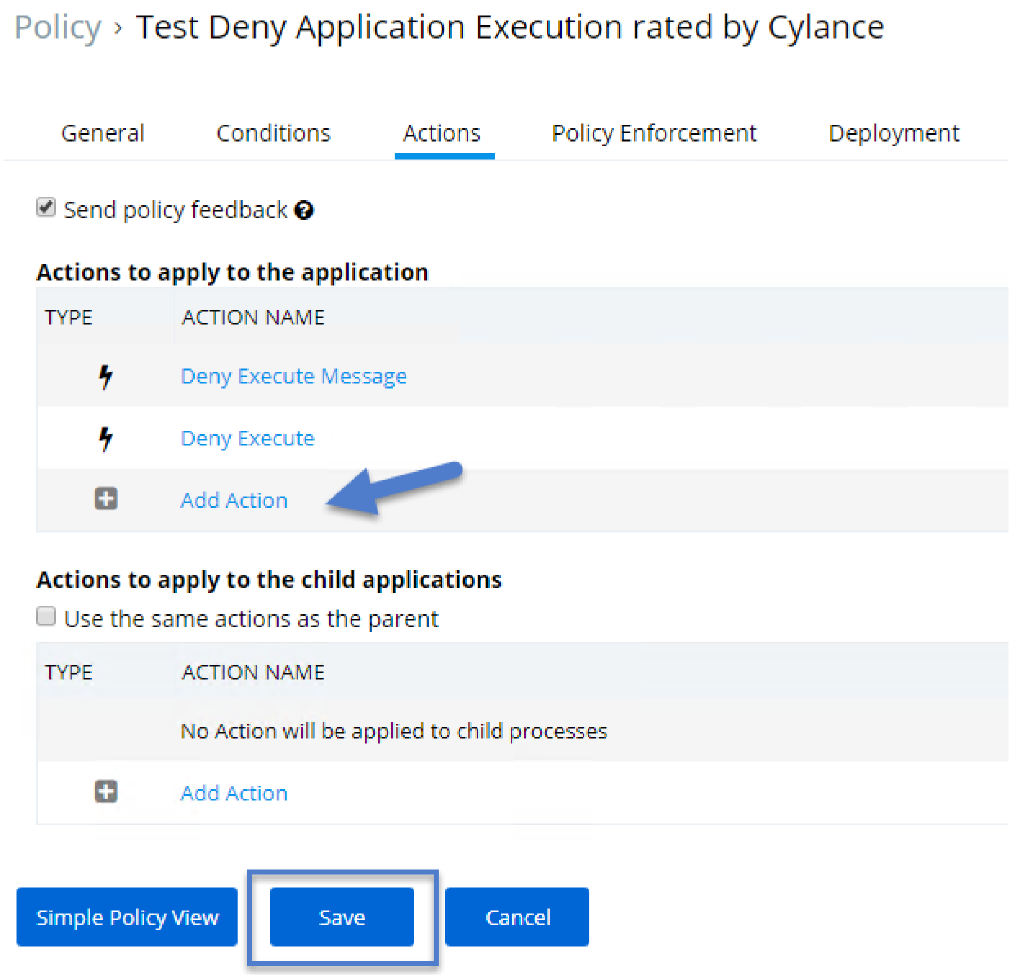
Select an Application Target from the folders below. Use the Application Target page to define more.

View by List: cy

	NAME	TYPE	FOLDER
□	AppCmd for App Pool Recycling (appcmd.exe)	Win32 Exe Filter	System Utilities
□	Recycle App Pool Commandline	Commandline Filter	System Utility Arguments
☑	Security Rating from Cylance	Security Rating Filter	My Filters

INCLUSION FILTERS (OPTIONAL, ONLY APPLIES WHEN *ALL* MATCH)

5. Select the **Actions** tab. Add an action to take. Click **Save**.



Policy › Test Deny Application Execution rated by Cylance

☑ Send policy feedback

Actions to apply to the application

TYPE	ACTION NAME
⚡	Deny Execute Message
⚡	Deny Execute
⊞	Add Action

Actions to apply to the child applications

□ Use the same actions as the parent

TYPE	ACTION NAME
	No Action will be applied to child processes
⊞	Add Action