

IBM Security Secret Server

*Cylance Connector Guide*

IBM

# Contents

<b>Getting started.....</b>	<b>1</b>
<b>Configuring the connector.....</b>	<b>1</b>
<b>Creating a Cylance Security Rating filter .....</b>	<b>4</b>
<b>Creating a Cylance policy .....</b>	<b>7</b>

*Last modified: December 16, 2019*



# Getting started

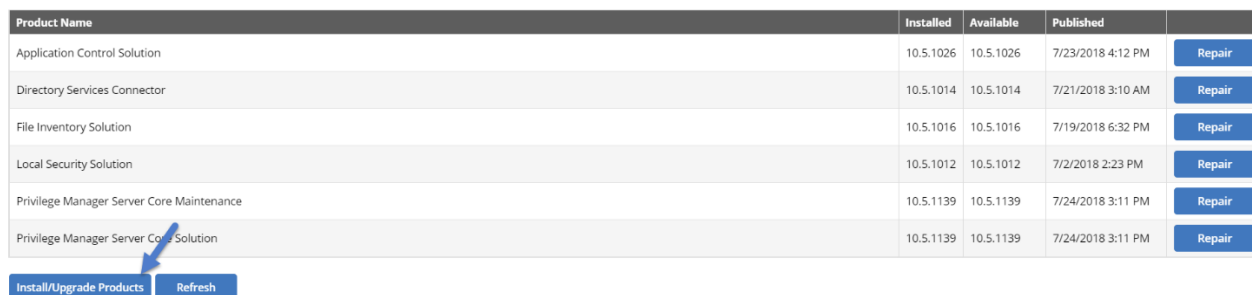
Cylance is an Artificial Intelligence Based Advanced Threat Prevention Solution for enterprise environments. Privilege Manager integrates with Cylance to help you proactively act on any unknown applications that run in your environment to prevent potential malware attacks.

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

Install/Upgrade Products Refresh

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.

- Browse to **Thycotic Privilege Manager > Admin > Configuration > Reputation** tab.
- For **Select Rating Provider**, select **Cylance Rating Provider**, then click **Edit**.

### Configuration

General    Discovery    **Reputation**    User Credentials    Foreign Systems    Roles    Advanced

**Select Rating Provider**    Cylance Rating Provider

---

**Credentials**

**Application Secret**    \*\*\*\*\*    Show

**Application ID**    \*\*\*\*\*    Show

---

**Settings**

**Tenant ID**   

**Region**   

**Edit**    ←

- Enter the required **Credentials** and **Settings** Details.  
Locate these details in your Cylance account. Log in at [protect.cylance.com](https://protect.cylance.com) under **Integrations > Custom Applications**.

CYLANCE    [Icons]

**Settings**

Application    User Management    Device Policy    Global List    Update    Certificates    **Integrations**

Custom Applications (2)

+ Add Application

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

**Demo Test**    Read | 6    Write | 4    Modify | 5    Delete | 0    [Edit] [Delete] [Refresh]

**Application ID:** 5d02556d-1464-4    Copy

**Application Secret:** \*\*\*\*\*    Copy

Regenerate Credentials

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

### Configuration

General   Discovery   **Reputation**   User Credentials   Foreign Systems   Roles   Advanced

Select Rating Provider   Cylance Rating Provider   ▾

---

Credentials

Application Secret ⓘ   ft   35c3


Application ID ⓘ   31   343

---

Settings

Tenant ID ⓘ   ba   54

Region ⓘ   North America   ▾

 **Save**   **Cancel**

# 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** \* -- select a filter type --

- Application Filters (Windows)**
  - Blank Win32 Executable Filter
  - Commandline Filter
  - Download Source Filter
  - Environment Filter
  - Network Location Filter
  - Parent Process Filter
  - Secondary File Filter
  - Security Rating Filter**
  - Signed File Filter
  - Time Of Day Filter
  - User Context Filter
- File Filters (Windows)**
  - Application Compatibility Filter
  - Application Manifest Filter
  - File Collection Security Catalog Filter
  - File Existence Filter
  - File Owner Filter
  - File Specification Filter

- 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

Navigation: < 1 > 10 Items per page Showing 1 - 2

[Close](#) [Clear](#)

[Back](#) [Create](#)



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

<b>Name</b>	* Test Cylance Security Rating Filter
<b>Description</b>	Test Cylance Security Rating Filter
<b>Platform</b>	Windows

### Settings

<b>Security Rating System</b>	* Cylance Rating System
<b>Rating Level</b>	* Unknown
<b>Timeout</b>	* Unknown second(s)
<b>Error Handling</b> On timeout, consider the result	* Error Condition
On failure, consider the result	* Error Condition

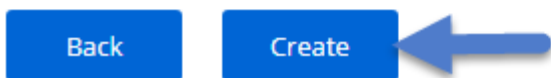


## Creating a Cylance policy

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

<b>Platform</b>	* Windows ▾
<b>Policy Type</b>	* Blacklist / Deny Application Execution ▾
<b>Template Type</b>	* Blacklist: Deny Specific Applications ▾
<b>Name</b>	* Test Deny Application Execution rated by Cylance
<b>Description</b>	* 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

General   **Conditions**   Actions   Policy Enforcement   Deployment

 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

<input type="checkbox"/>	NAME	TYPE	FOLDER
<input type="checkbox"/>	AppCmd for App Pool Recycling (appcmd.exe)	Win32 Exe Filter	System Utilities
<input type="checkbox"/>	Recycle App Pool Commandline	Commandline Filter	System Utility Arguments
<input checked="" type="checkbox"/>	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

General   Conditions   **Actions**   Policy Enforcement   Deployment

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

Simple Policy View   **Save**   Cancel