IBM Security Secret Server
Version 10.7

Privilege Manager User Guide

Contents

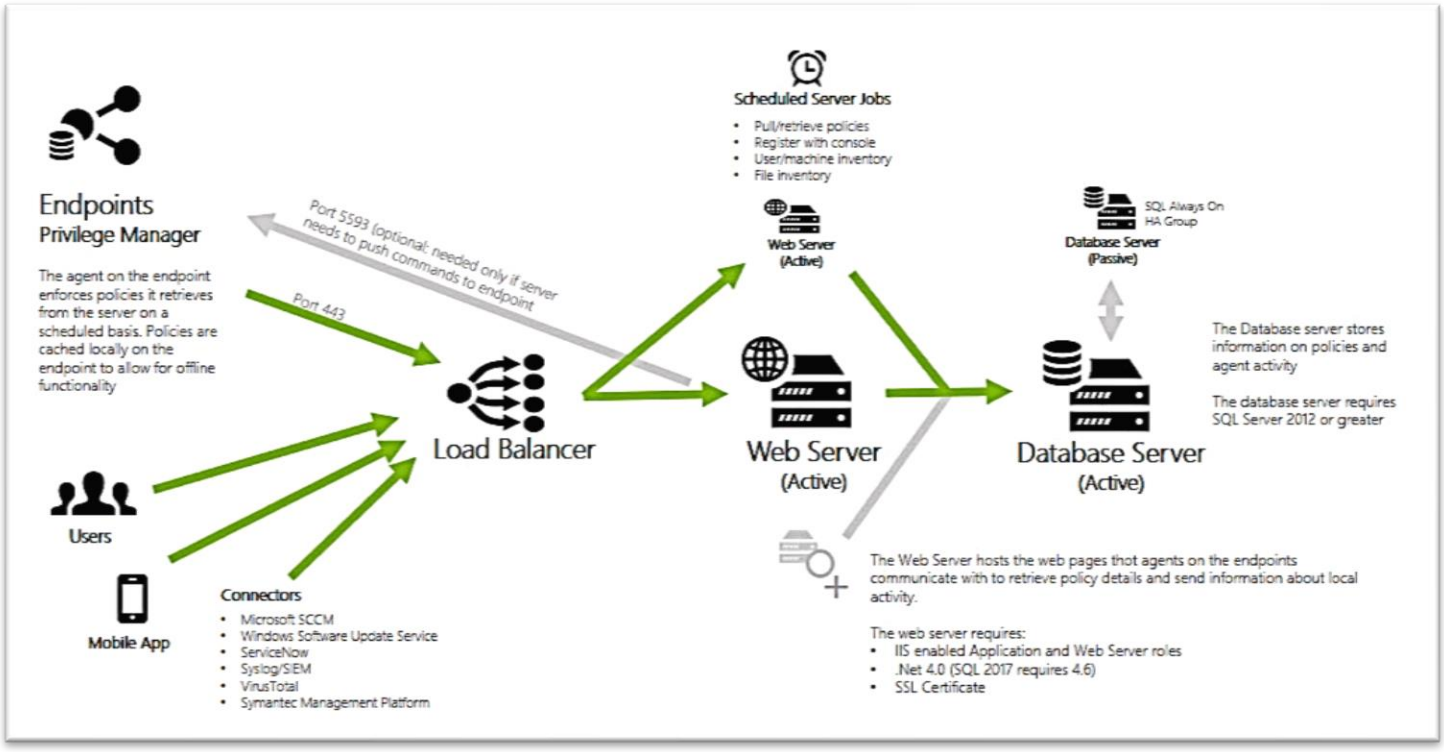
Preliminary Steps

Review System Requirements

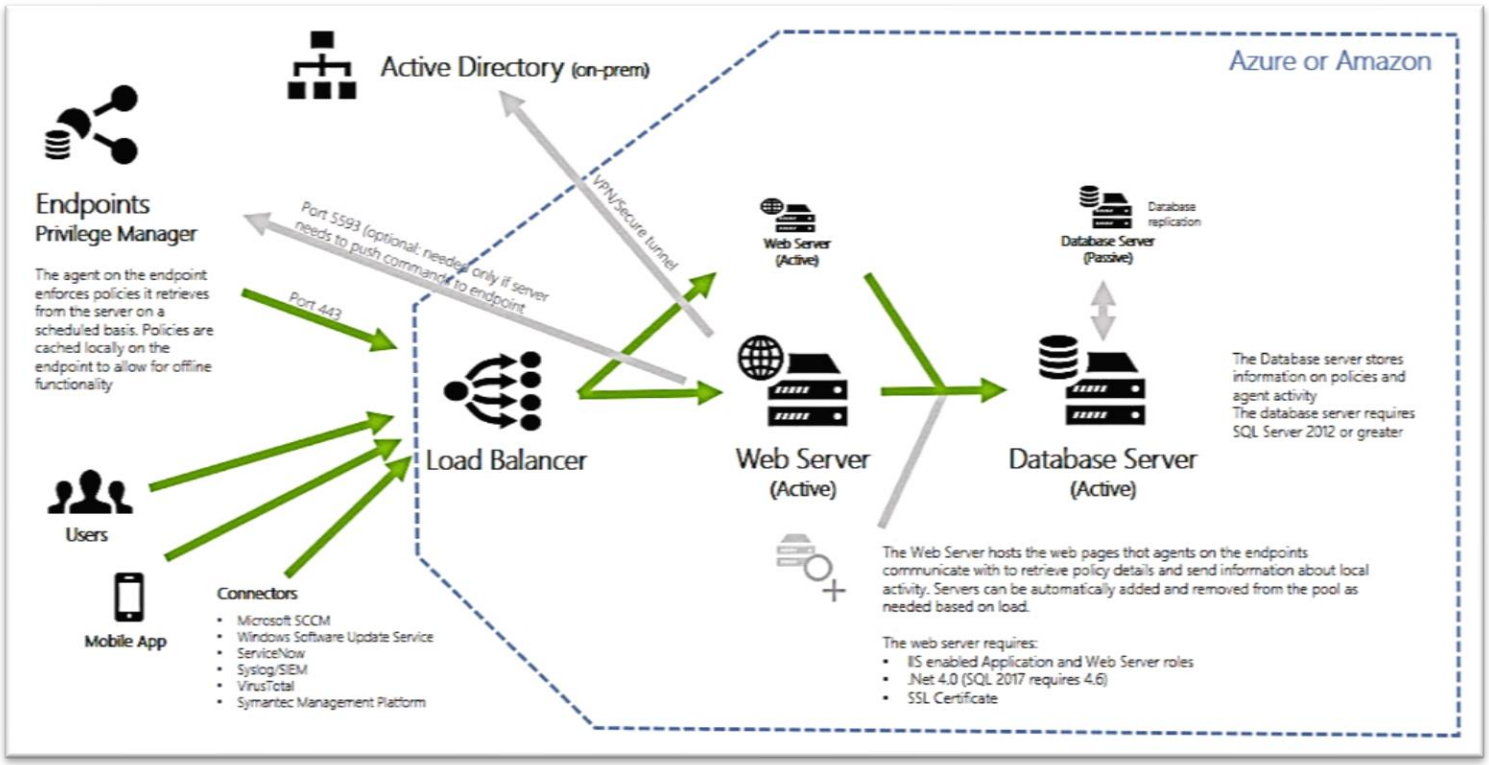
For a complete list of System Requirements for both proof-of-concept and Production Environments, see the System Requirements Guide for Privilege Manager.

System Architecture Diagrams

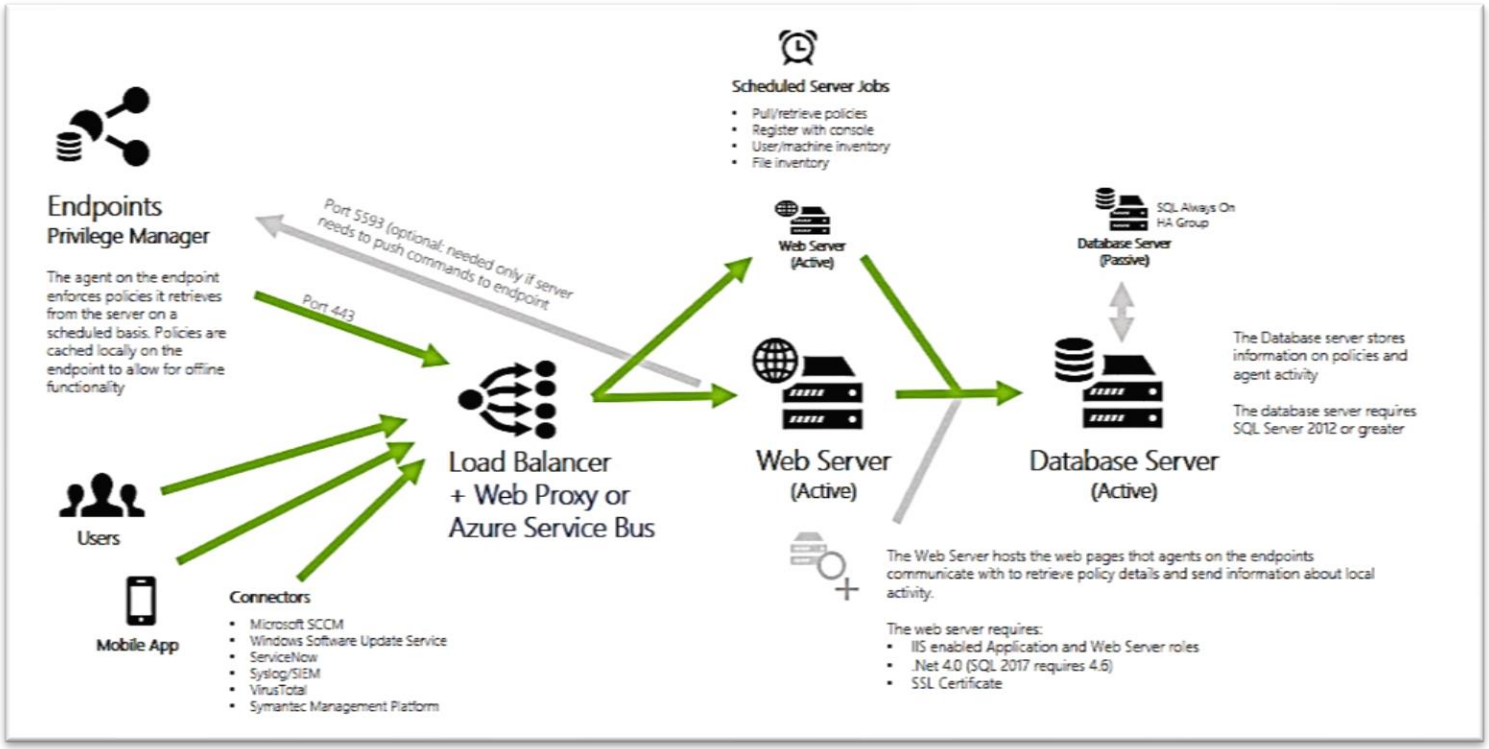
General Architecture



Cloud Architecture for Azure or Amazon AWS Hosting Environments



Proxy or Azure Service Bus Architecture for Environments Without Internet Access



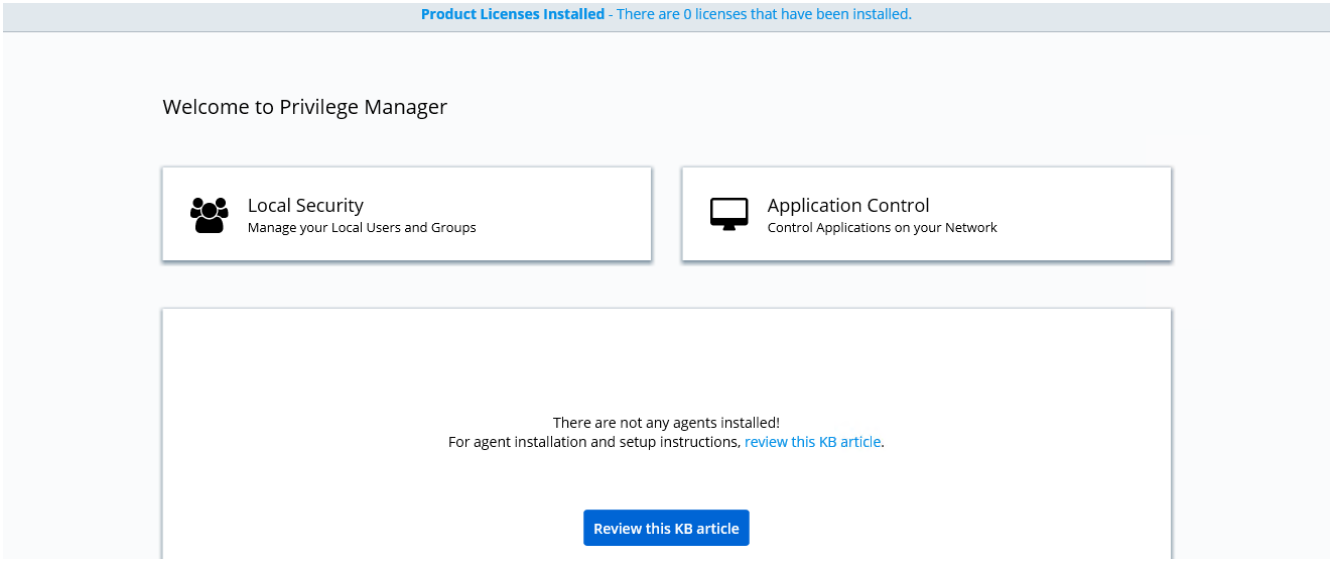
Port/Access Information

- Outbound access from the agent to the server is done **by default over port 443** (the standard port for HTTPS communication) but you can specify a different port if desired.
- The only port that the agent listens on is **port 5593**. This port is not required. For example, you can block this port and agents pulls information from the server on a set schedule.

Privilege Manager Installation

Install Privilege Manager following the directions that are outlined in the Installation Guide.
If any issues occur while you install Privilege Manager, check out the Troubleshooting Installation Guide.

By using the credentials that are configured in the **Create User** section (step 7 in Installation guide), ensure that you can log in to Privilege Manager and view the home screen. You might initially be logged in through Secret Server. If so, you can find Privilege Manager by navigating to **Tools > Privilege Manager**.



If you are accessing the homepage for the first time, you must install licenses. Click the top blue banner that says **Product Licenses Installed** to navigate to the **Licenses** page in Privilege Manager. Or go to **Admin > Licenses**.

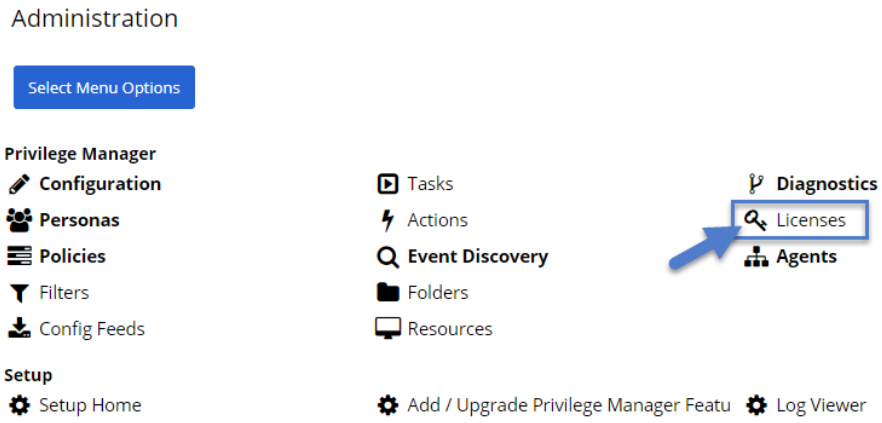
Licensing

Installing New Licenses

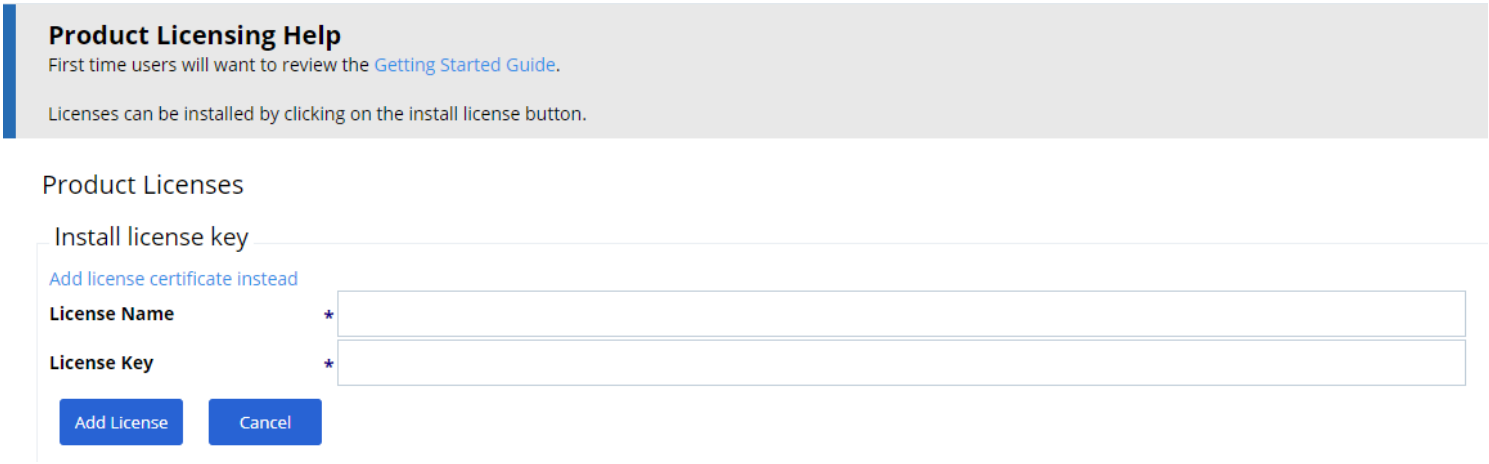
To install new Privilege Manager licenses, it depends on whether you A) choose to install Secret Server in tandem with Privilege Manager or if B) you perform a stand-alone installation.

Steps for stand-alone Privilege Manager Installation

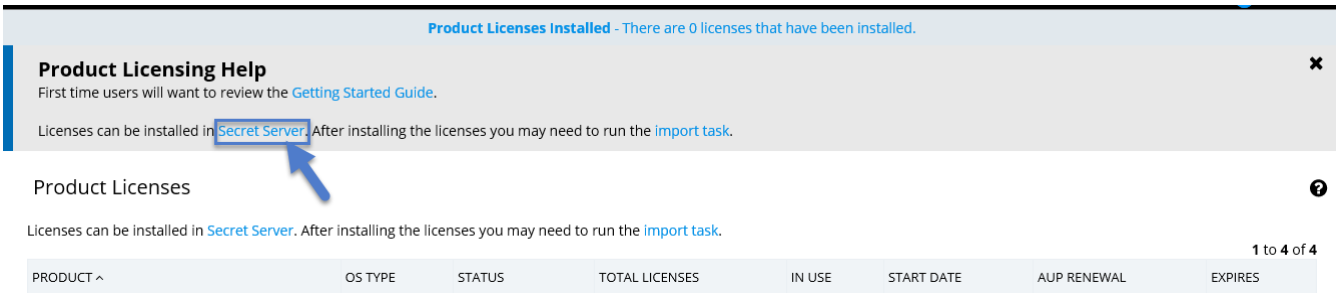
- To install licenses without Secret Server, navigate to **Admin > Licenses** or click the **Product Licenses Installed** link in the top banner.



- From the Privilege Manager Licenses page, click **Add License**, then enter your License Names and Keys one at a time, select **Add License** to finish.

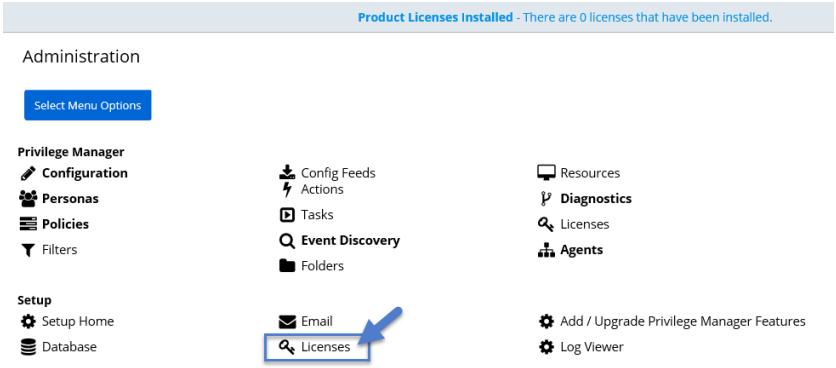


Steps for Combined Secret Server + Privilege Manager Installation

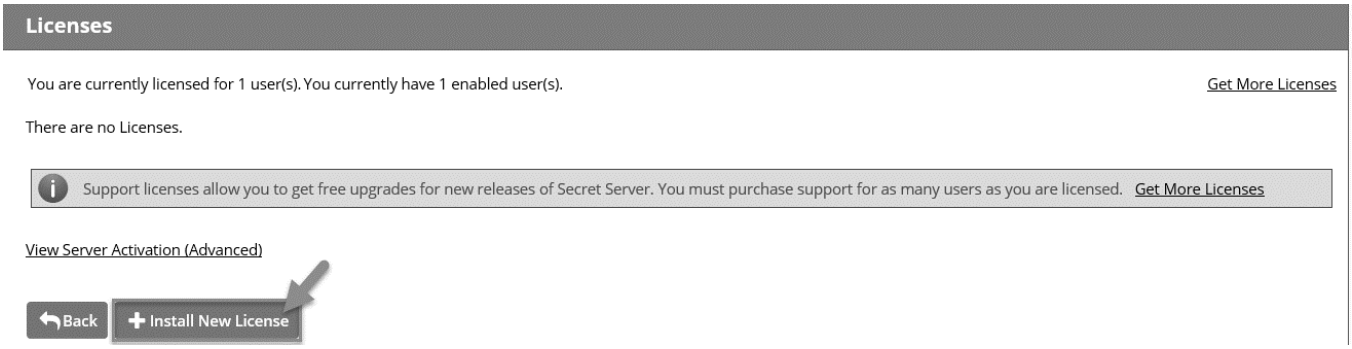


To install licenses with Secret Server on the same server as Privilege Manager, you must install licenses through the Secret Server UI and then import the new licenses into Privilege Manager.

- To access Secret Server's licensing page, either click the **Secret Server** link that is listed in the banner at the top of the Privilege Manager Licenses page or navigate to **Admin > Setup – Licenses** (as shown below).



- From Secret Server's License page, select **Install New License**.



- Enter your License Names and Keys individually or through the **Bulk Entry Mode**. Click **Save** or **Add Multiple Licenses** to save the License Keys. Installing these licenses in Secret Server will automatically import the licenses into Privilege Manager. Navigate back to the Privilege Manager License page to verify: **Tools > Privilege Manager > Admin > Privilege Manager–Licenses**.

If your license keys do not appear or you have too many keys that are listed, click the **import task** link and then **Run Task** to reset.

Converting from Trial Licenses

If you previously had evaluation licenses and purchased recently, you must install your new license keys for production with the same steps described earlier. Normal trial licenses offer 50 endpoint agents and expire 30 days after issue.

Expired Licenses

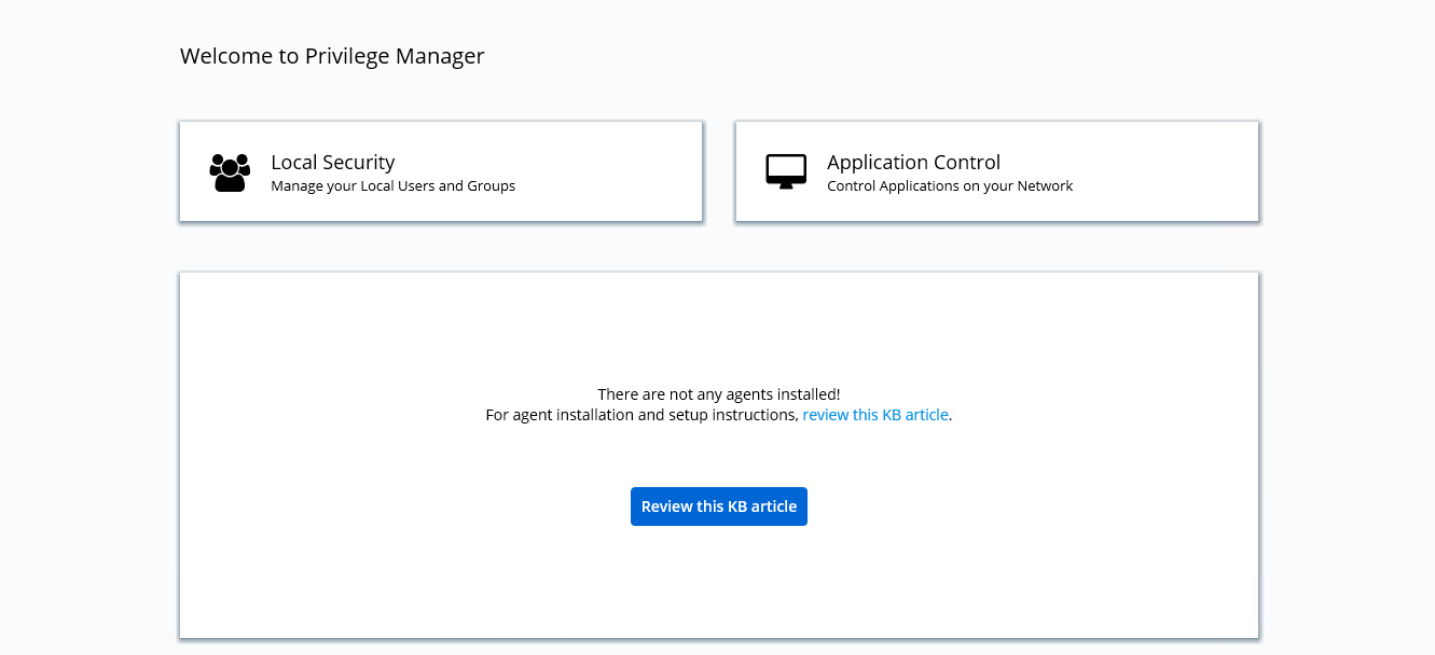
When your Privilege Manager licenses expire or exceed the licensed count, Privilege Manager reverts to a “Limited Mode,”. In Limited Mode, the server stops accepting data that is sent from agents. Additionally, new endpoints register but are not recorded. Endpoints that are identified are added to Computer Groups (Resource Targets), cannot collect application or user inventories, no password changes can occur, and so on.

Configured policies continue to run on endpoint computer but are not updated or edited. The server completely discards the data that agents send to Privilege Manager, and it is not stored.

Getting Started

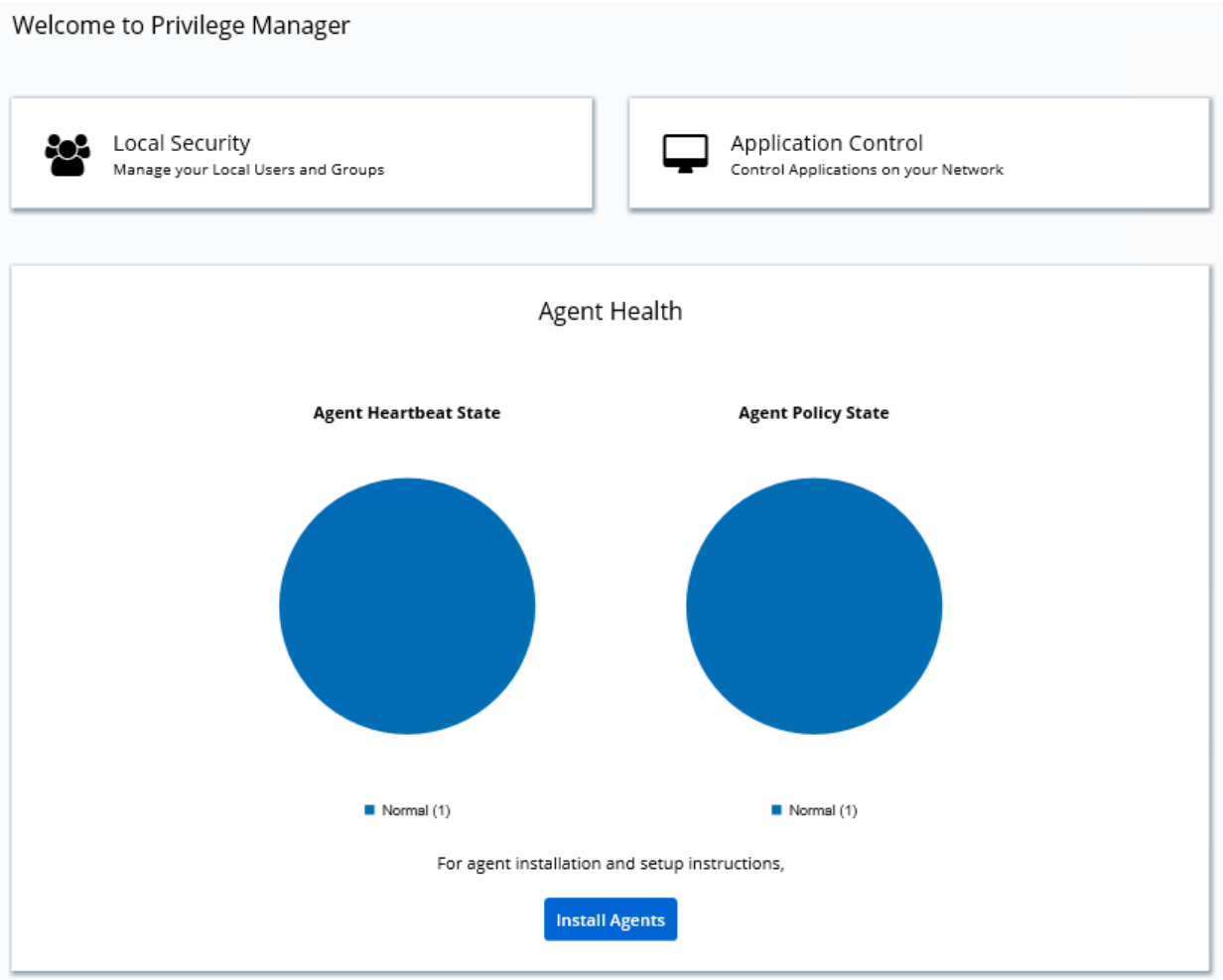
Home

Locate the Home screen of Privilege Manager by clicking **Home** in the top banner of any page inside of Privilege Manager. From this dashboard you can jump into either **Application Control** or **Local Security**, depending on what you want to do. You also are given a snapshot of your Agents' health. Before setting up Agents, your home page looks like this:



Agent Installation

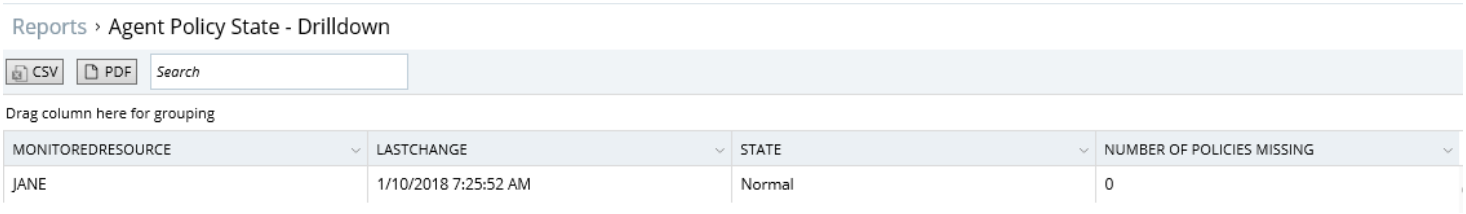
Download agent installers and follow steps for installing agents from for each of your endpoints https://ibm.biz/BdYBMe. When your agents are installed, you can verify the status of your Agents' Health from **Home**:



These two Agent Health dials describe your Agent Heartbeat State and the Policy State. Click the left **Agent Heartbeat State** dial and you see a report on a list of machines (the "MonitoredResource" column) where each registered agent is installed. Click the **Back** button or the **Home** tab to return.

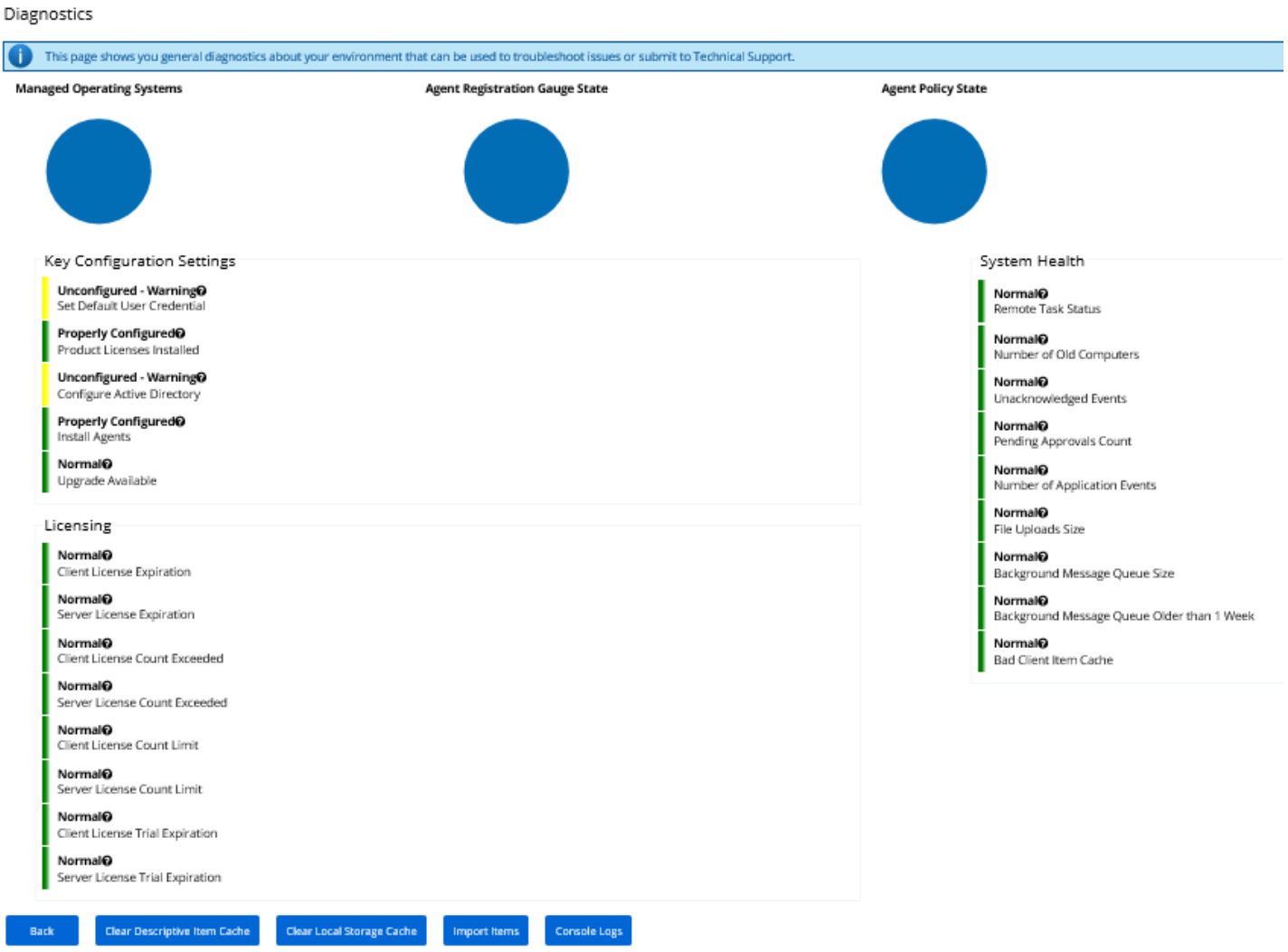
Clicking the **Agent Policy State** dial from the Home dashboard brings you to a report that links all your agent-

registered machines with the **Number of Policies Missing** from each agent. This page becomes invaluable after you have multiple policies running over different computer groups in your network.



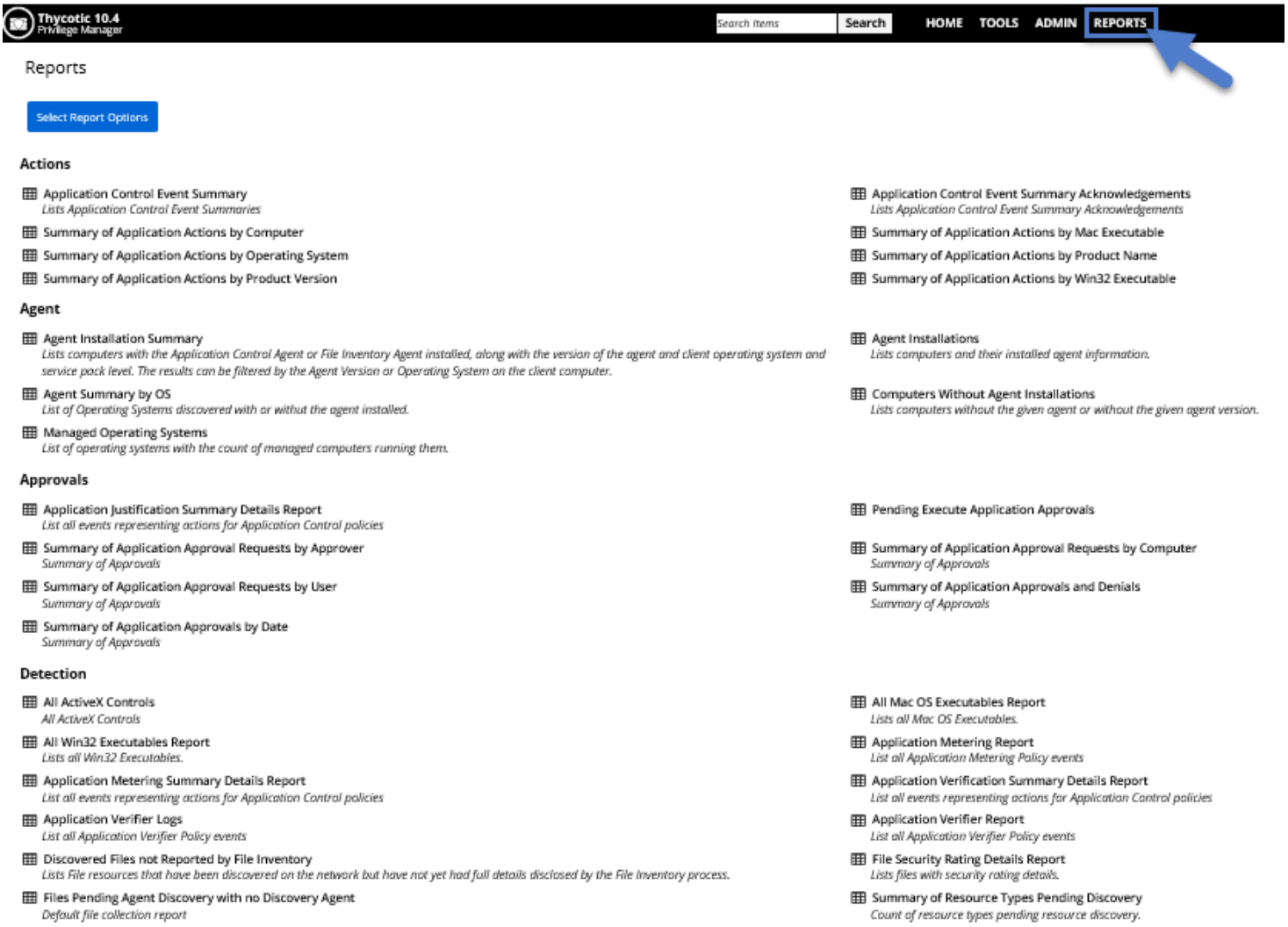
Diagnostics

Navigate to the **ADMIN** > **Diagnostics** page to view more comprehensive agent details. The Diagnostics page is also the go-to stop for full system health. Find Server **Console Logs** and other system level warnings or tips.



Reports

In the top menu, click the **Reports** tab for a list of relevant, ready for immediate use reports that span a spectrum of system activity and diagnostic information in Privilege Manager. Click the name of any of these reports to drilldown into details about your system.



Configuring Privilege Manager with Secret Server

If you are using both Privilege Manager and Secret Server, you can store Privilege Manager's local credentials in Secret Server. To configure Privilege Manager with Secret Server, follow the instructions that are listed here.

Active Directory Synchronization

Privilege Manager can synchronize with Active Directory to use OU computer lists, Security Groups, and User lists for use in policy definitions. Follow the instructions outlined here to set up Active Directory synchronization.

Least Privilege Overview

What is Least Privilege?

Least Privilege is a security-driven management philosophy that models a system where all employees are given the minimum level of access rights necessary to perform their job functions on endpoint machines. Privileged local admin or root accounts on endpoints give unfettered access to the entire endpoint and excess privileges can be used to access other computers, domain resources, and critical servers unless a least privilege security model is implemented. But implementing Least Privilege can be difficult for IT teams to enforce because plenty of daily, trusted activities that employees must perform require access to privileged credentials.

Privilege Manager's toolset is two-fold. First, **Local Security** discovers all existing accounts on endpoints and allows Privilege Manager Administrators to control the exact membership of machines in every local group. This ensures that correct admin and root accounts are permanently set across your network. Additionally, credentials are controlled by enforcing password rotation on those accounts.

Second, **Application Control** in Privilege Manager allows administrators to manage all application activity on endpoint machines. Applications requiring admin rights or root access can be automatically elevated if trusted, allowed applications can be whitelisted, and malicious applications can be blocked.

In other words, the key to keeping your organization's employees that are working both securely and effectively without notable disruptions to their work is by tailoring a robust, role-based **Application Control** system. Managing local administrator and root accounts through **Local Security** is the fastest way to lock down your network from malicious endpoint attacks that exploit administrator access.

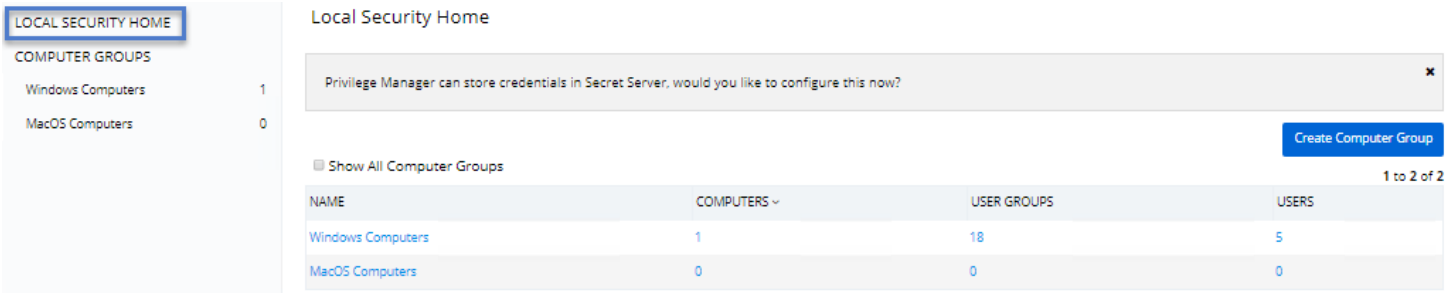
That's why IBM suggests a phased roll-out between the two sides of Privilege Manager's functionality. An example implementation strategy can proceed as follows:

1) **Application Control**: Set up Learning Mode policies on a group of test endpoints to learn about the applications already running on your endpoint machines
2) **Local Security**: Begin managing your Local User Accounts (only) and defining local Group Membership
3) **Application Control**: Tailor your policies so that they won't disrupt employee work (Elevate Trusted Applications) but will block known malicious applications. Implement these two baseline policies across endpoint agents
4) **Application Control**: Tailor new policies that are specific to employee roles. Create a "Request Access" system for any unknown applications that an employee attempts to run.
5) **Local Security**: After workflow is established between employees and the Privilege Manager Helpdesk for requests, widen the Local Security net to manage all local privileged accounts (ex: local admins) on endpoints.

Remember: Every Privilege Manager implementation is unique and can be tailored to achieve your organizational goals. The User Guide walks you through basic configurations for both Local Security and Application Control as the two Privilege Manager pillars for implementing Least Privilege. Use these configuration steps as a tutorial, reference, and guide for setting up a sandbox environment before you create your production rollout strategy. Feel free to flip around between sections.

Local Security Overview

From Privilege Manager's **Home** screen, click the left section that is called **Local Security** to enter the **Local Security Home**. From Local Security's navigation panel, you can click into existing Computer Groups to view all local groups and user accounts across the endpoints. The Local Security Home dashboard gives you a bird's eye view of the Computer Groups that exist in your system.



Computer Groups

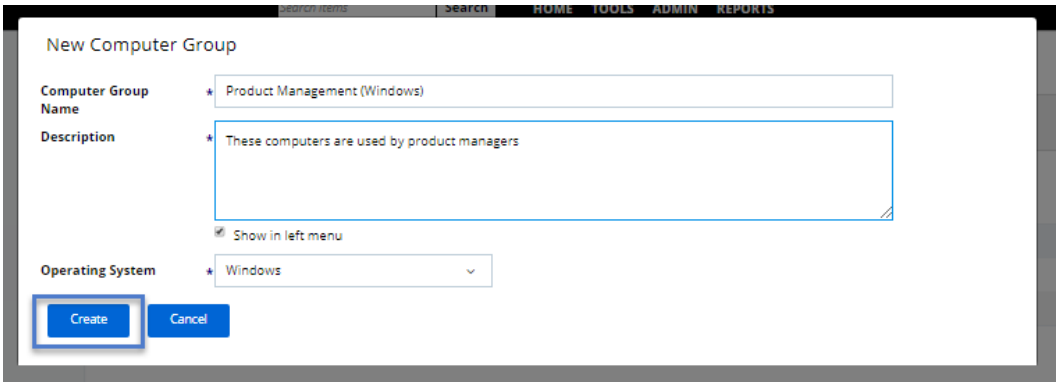
If you have agents that are already installed and registered, you see numbers that are automatically listed in **Local Security Home,** which is divided by Privilege Manager's two ready for immediate use computer groups that are listed as 1) **Windows Computers** and 2) **MacOS Computers**.

For example, in the screen capture above only one agent is registered with Privilege Manager. Local Security tells us that the agent is installed on a Windows computer (thus categorized in the **Windows Computers** group), that there are 18 local **User Groups,** and 5 local **Users** on the machine. Local Security automatically discovers this information upon every agent's registration with Privilege Manager.

If you have "Computer Groups" (also called Resource Targets) already configured for Application Control in Privilege Manager. Also ensure that those groups can also appear as Computer Groups in your Local Security navigation pane after you select the "Show All Computer Groups" check box. Select the first column of any row to use the target endpoints as a Computer Group and display it in the left navigation pane.

Create New Computer Group

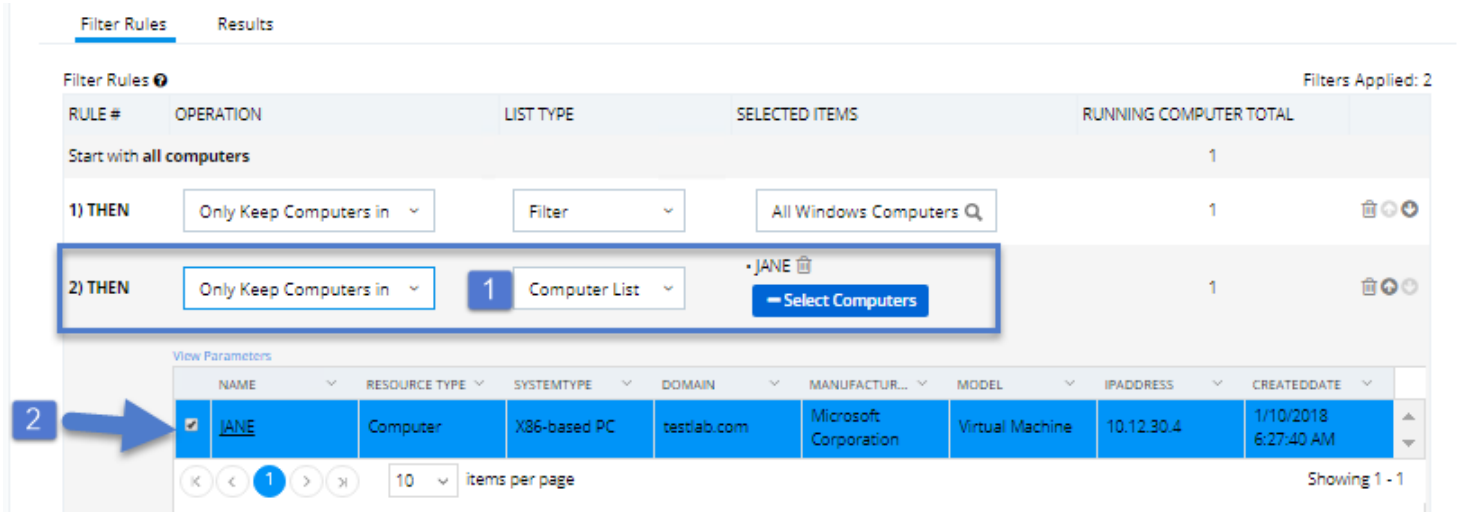
To add new computer groups that are tailored to your organization's environment, click **Create Computer Group** from the **Local Security Home** page. Enter a **Name** for your new group, a **Description**, and select the **Operating System (Windows versus Mac)** used by these computers.



To select the computers that you want to include within this group, you must create a **Filter** that targets the appropriate computers on your organization's network.

The default filter will begin with a rule that targets computers within the main OS Computer Group that was selected when you created the group, meaning it will target either all Windows or all Mac computers with registered agents.

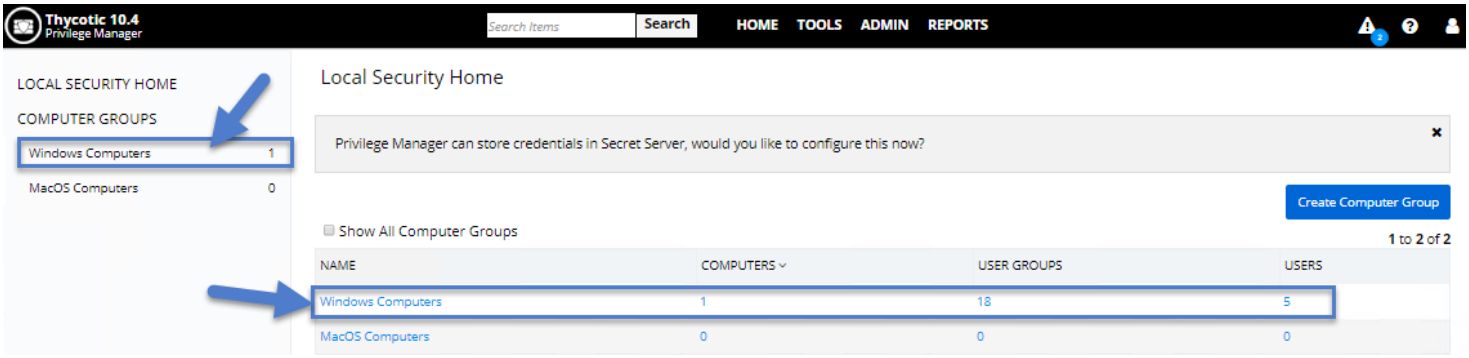
To narrow your group, click **Add Rule** then in the "List Type" column select **Computer List**. Click any specific computers from the provided list of registered computers, then click **Save**. You can collapse the computer list view by clicking **Select Computers** under the Selected Items area.



Local Groups

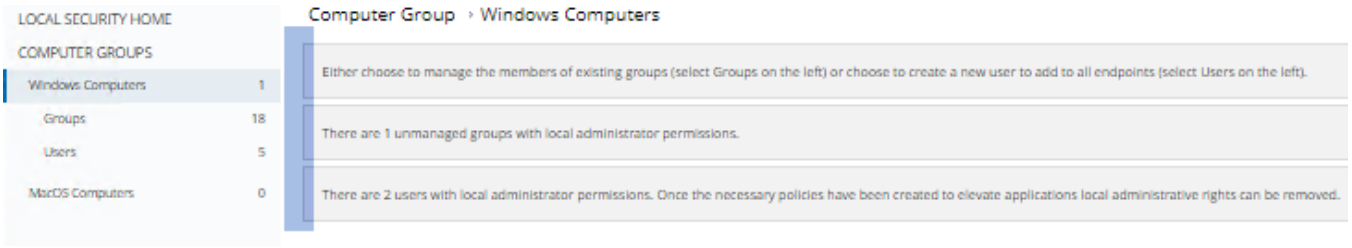
Every Computer Group is divided into **Groups** and **Users**. Both "Groups" and "Users" that are used in this context refer to local accounts on the computers that are included in the Computer Group.

To see more details about the Windows Computers Group, either click **Windows Computers** in the Local Security Home screen or in the left navigation pane:



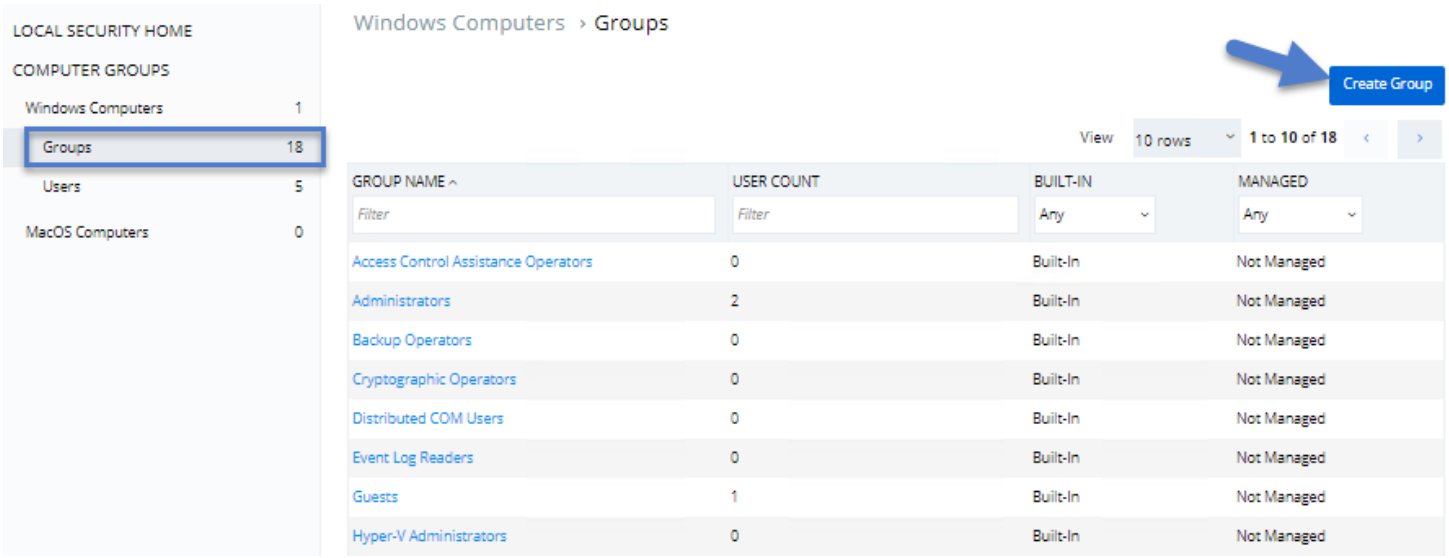
This **Computer Group's** page gives you pointers on what can be done with the users and local groups within this set of computers, and provide a high-level overview of the selected computer group based on **Local Users**, **Local Groups**, and the **number of computers** in the group.

Remember: When an agent registers, Local Security automatically discovers the local groups that exist on each machine.

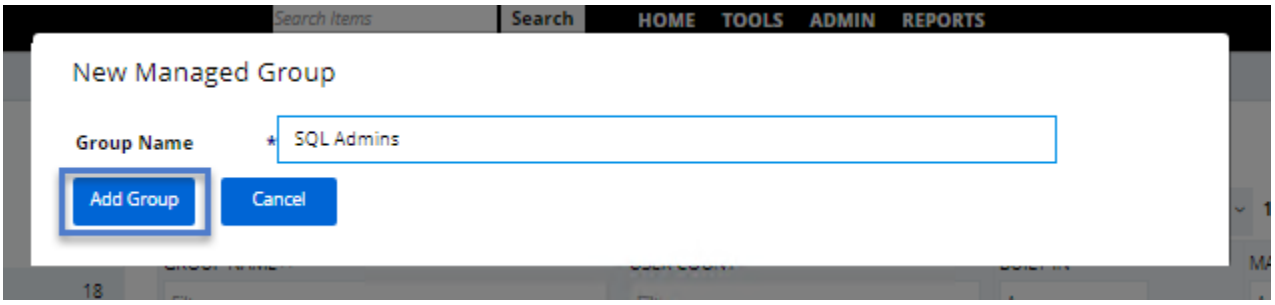


Create New Local Group

To create a new Group, select the **Groups** line item that is listed under the name of the intended Computer Group. At the right side of the page, click the **Create Group** button.



Enter a **Group Name** and click **Add Group.**

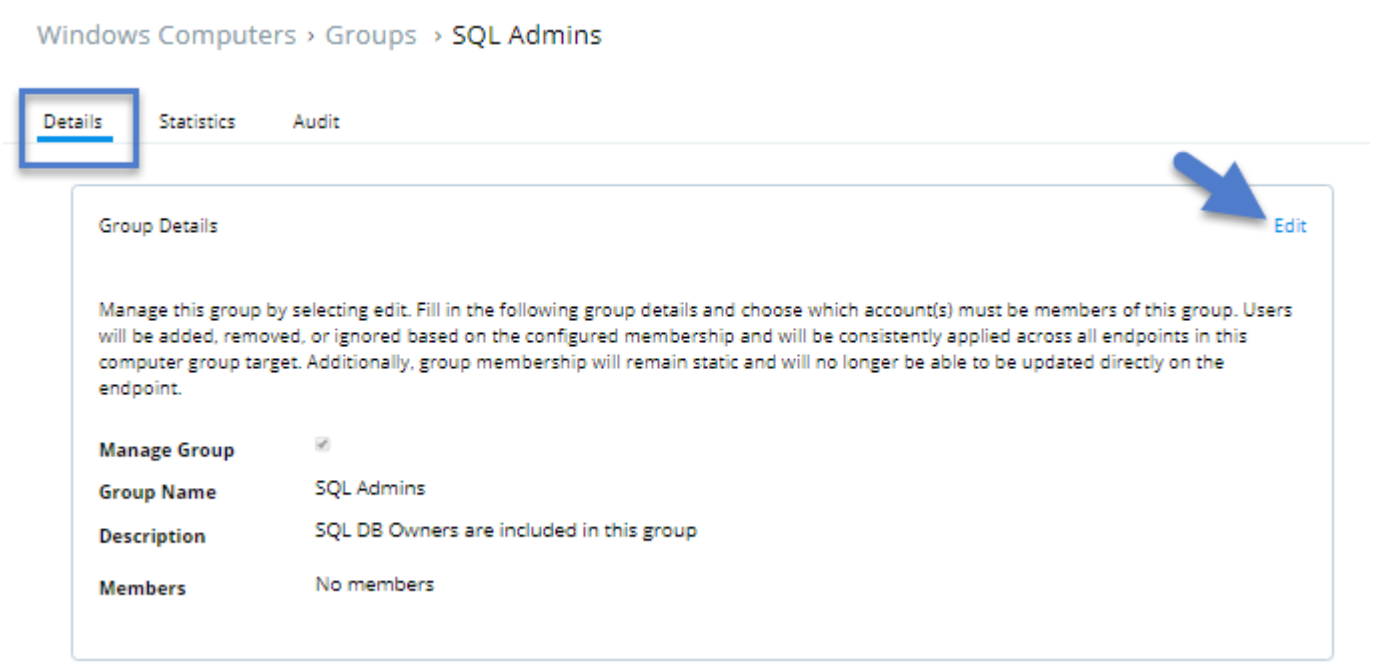


On your new group page, add a **Description** and select **Save Changes**. Privilege Manager prompts you with a **Confirm Navigation** box. Click **Yes**.

Details Tab

Add Members to Local Group

The Local Group Details' tab shows you the **Group Name**, **Description**, and **Members** that are part of this group. To edit your group details click **Edit** in the right corner.

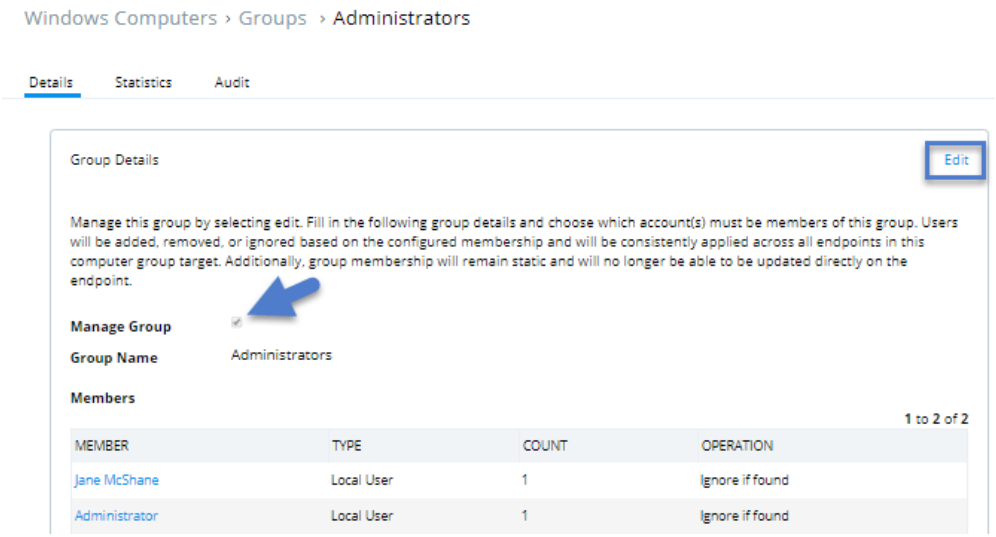


When editing, you can add members to the group by clicking the **Add Member** button. Select the type to add (*Domain User, Domain Group, Local User*) and then toggle the available options from the user list. To finish click **Add Member**, then **Save Changes**.

Manage Local Groups

Managing a local group means that you determine which accounts are in that group from the Local Security dashboard. In other words, if a group is being “managed,” the group membership remains static and will no longer be able to be updated directly on the endpoint.

If a local group is unmanaged you will see a toggle box next to **Manage Group** that is unchecked. To Manage the group, click **Edit** from the Details tab and then check the **Manage Group** box. Click **Save Changes**, and **Yes** to Confirm Navigation. Changes to these settings may take up to 15 minutes to update on your endpoints.

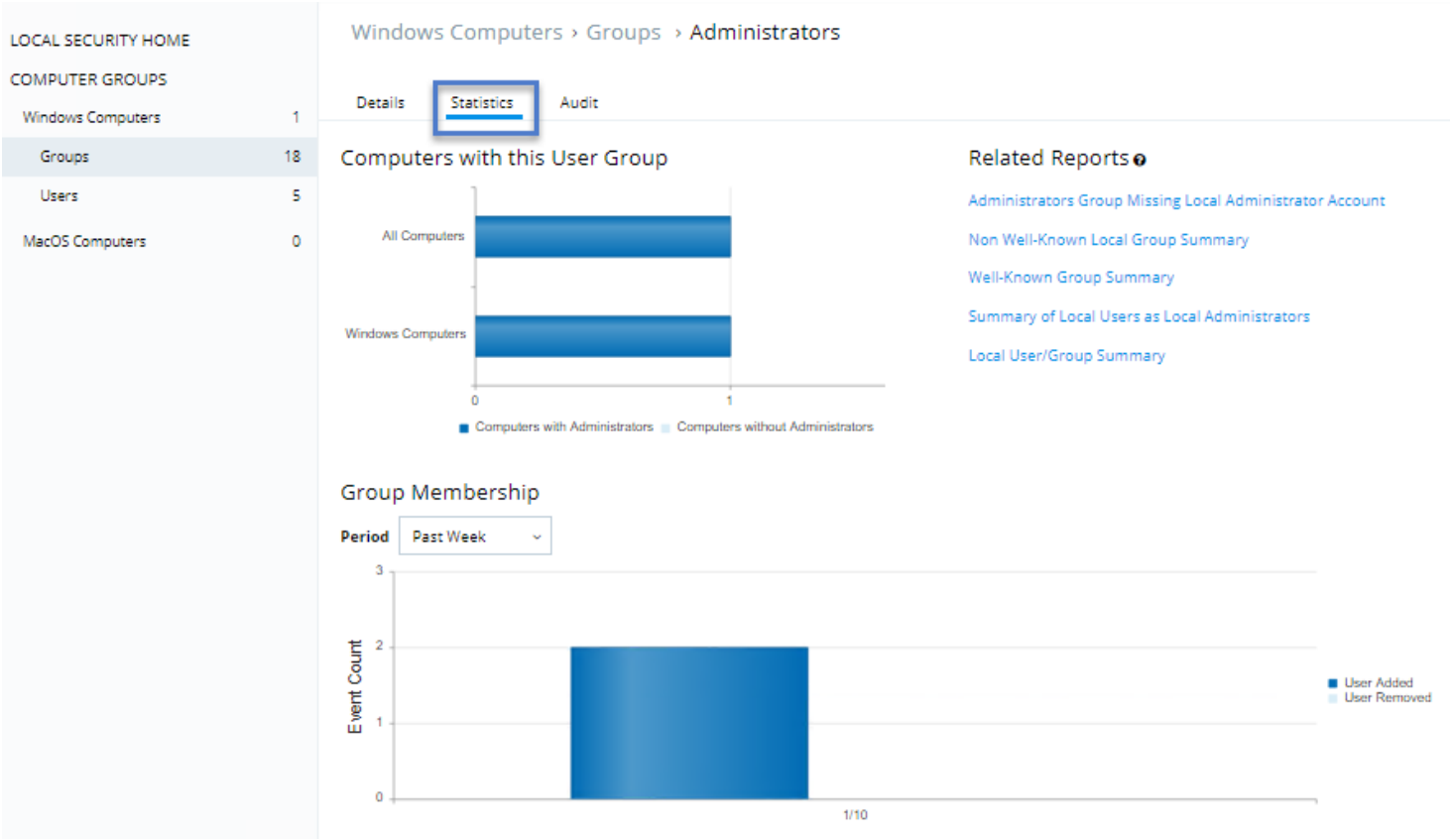


When managing a group, existing members and any that have been added to the policy will appear in the **Members** table. Choose the operation to perform upon the user if found on the endpoint. Options to **Ignore if found**, **Add if missing**, or **Remove if found** can be selected. The last row defines what action to take on all other users and groups. This ensures exact membership can be defined and any other users or groups can be automatically removed. By default, all other users and groups are ignored, keeping their membership intact so that this key operation does not occur automatically. Once saved, group membership is permanently defined. Updates that are made directly on the endpoint that break this policy is immediately reverted.

Statistics Tab

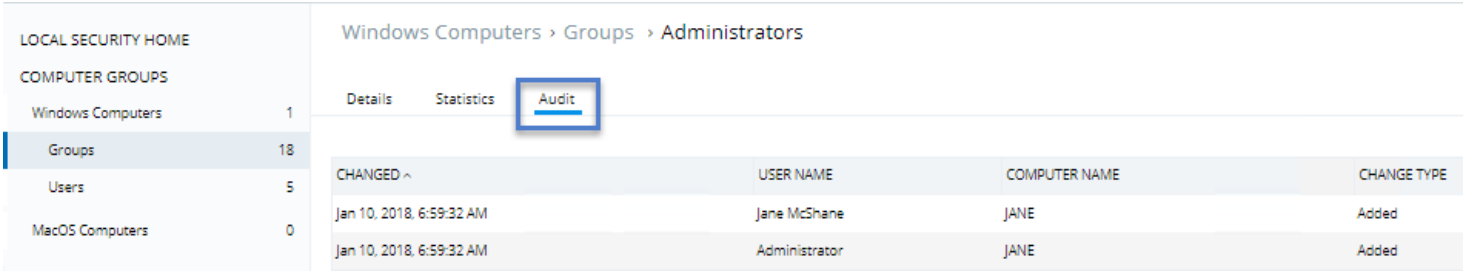
The Statistics’ tab for a local group highlights some quick visual statistics and links you to relevant reports based on key factors like how many computers from your network are included in this group and whether there have been changes that are made to the Group’s Membership within the specified period. Click these graphs to drill down into more details.

Note: The reports in the “Related Reports” sections are scoped to only include endpoints in the current computer group. To view reports across all computers, go to the Reports section of the product.



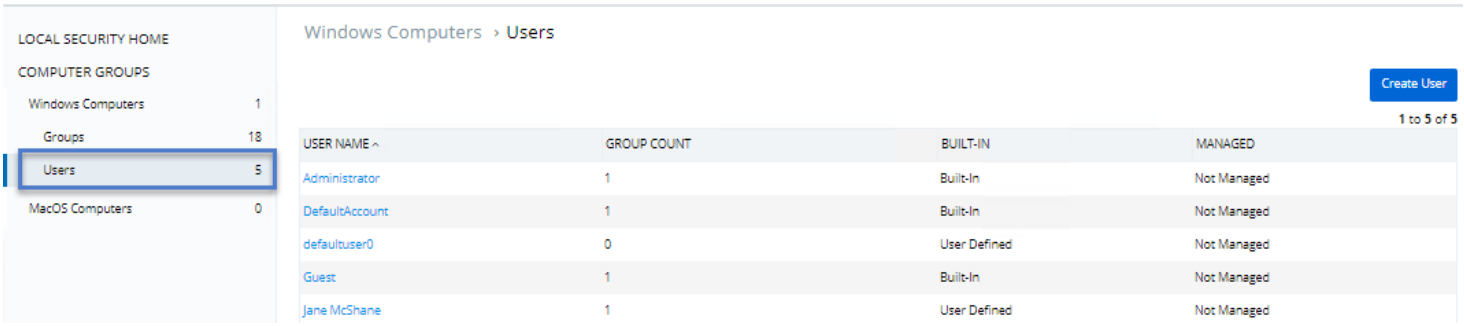
Audit Tab

The Audit tab is where you find an audit record of all membership additions and deletions that have been made to your local groups.



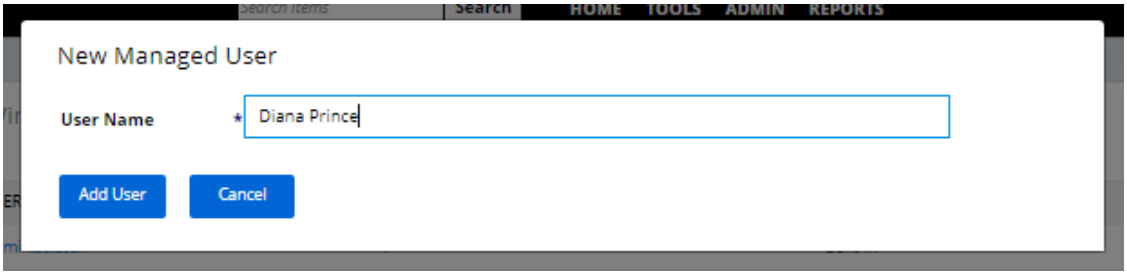
Local Users

The **Users'** page that is listed under your Computer Group shows a list of local users that exist within this Computer Group. The information that is highlighted by this table includes 1) how many groups each user account is a member of, 2) whether the user account was built in or user-defined, and 3) whether the account itself is "Managed." Managing local users in Local Security means that you are setting a password for the account and can rotate the password as wanted.



Create New Local User

To create a new local user, click the **Create User** button on the Users page, then give your user a name. Click **Add User**. This takes you to the **Details** tab for your new user account. To create a user through Local Security, it must be a managed user.



Details Tab

In Local Security, the most important thing to know about your user accounts is whether each is being managed. Managing a local user account means that you can rotate the account's password from Local Security's console in Privilege Manager.

Manage Local Users

To begin managing a user, select **Edit** in the **Account Details** box under the Details tab.

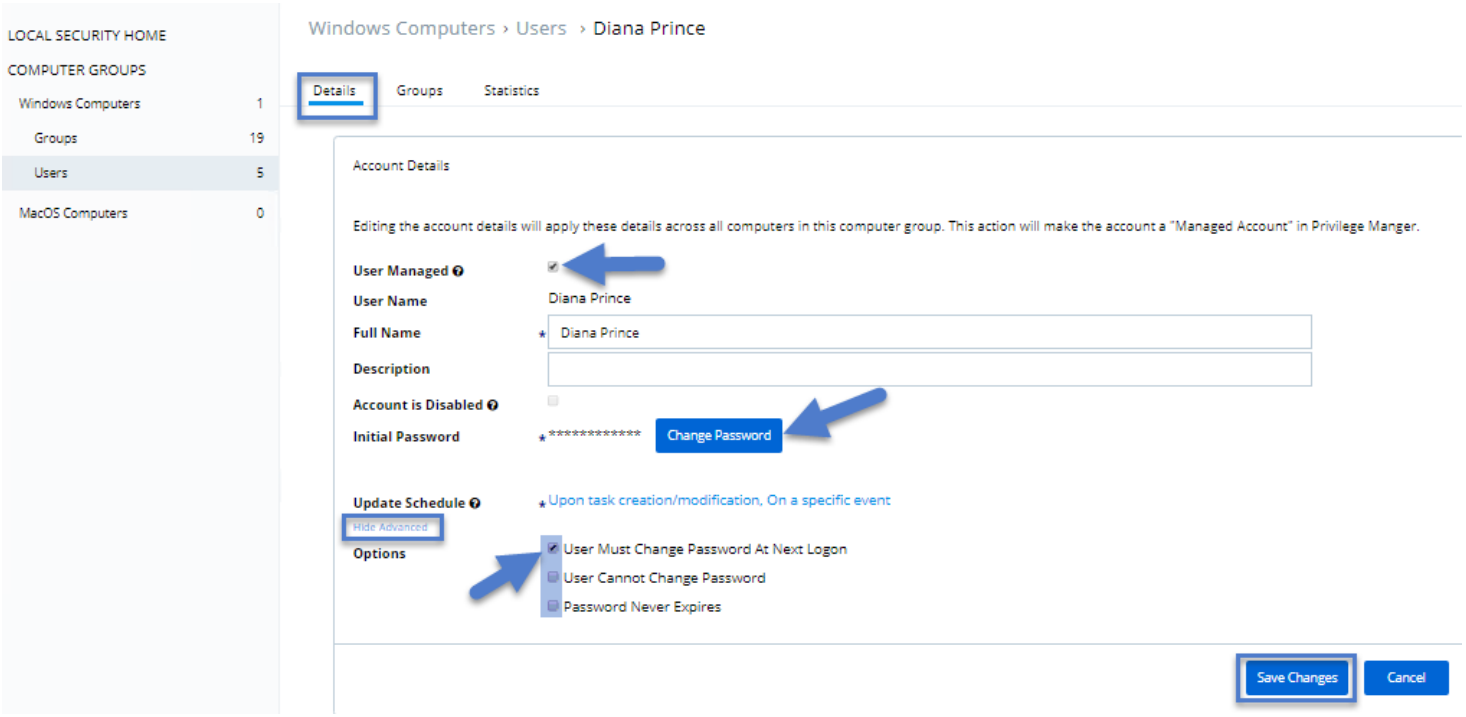
Click the box next to User Managed to begin. While editing a user you can change the account User Name, add details like the full name of the user or details, you might disable the account or update the schedule that pushes out modifications to endpoints.

The most important part of managing a user is setting a one-time password for the account. This means that any user of this account will no longer be able to access this account with their former password, effectively locking a user out of the account unless they contact the Privilege Manager Local Security Helpdesk.

To set a password for this account, enter a new password twice to confirm, then click **Save Password.** For advanced options, click **Show Advanced**. To save your changes, click **Save Changes**.

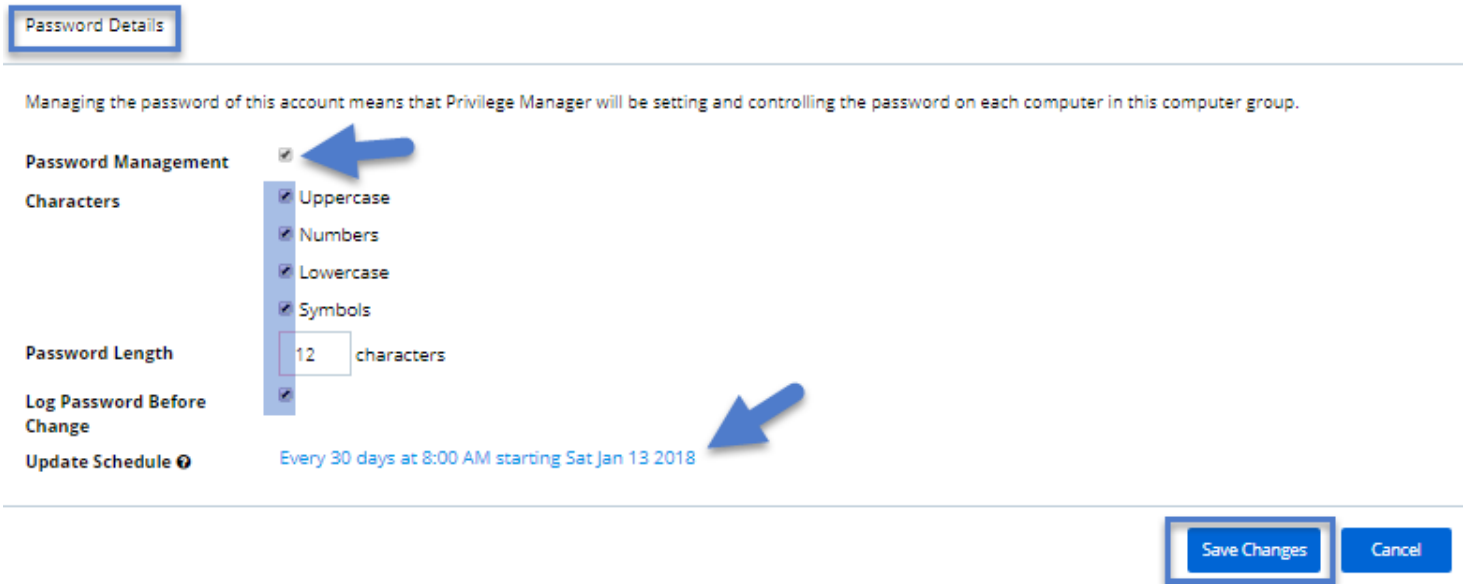
Note that settings for **Account is Disabled**, **User Must Change Password At Next Logon**, **User Cannot Change Password**, and **Password Never Expires** are all specific to Windows endpoints and will not be displayed for

Mac OS-based Computer Groups.



Randomize Local Account Passwords

The second box under the User Details tab is called **Password Details**. This option is generally used for privileged accounts that you want fully managed by Privilege Manager. To manage your password this way, select **Edit** in the Password Details box, then check the **Password Management** box and edit password length and strength rules. The password on this account will be rotated based on the **Update Schedule** details (click the details in blue to edit). **Save Changes** when complete. The password for the account on each endpoint in the Computer Group will be unique.



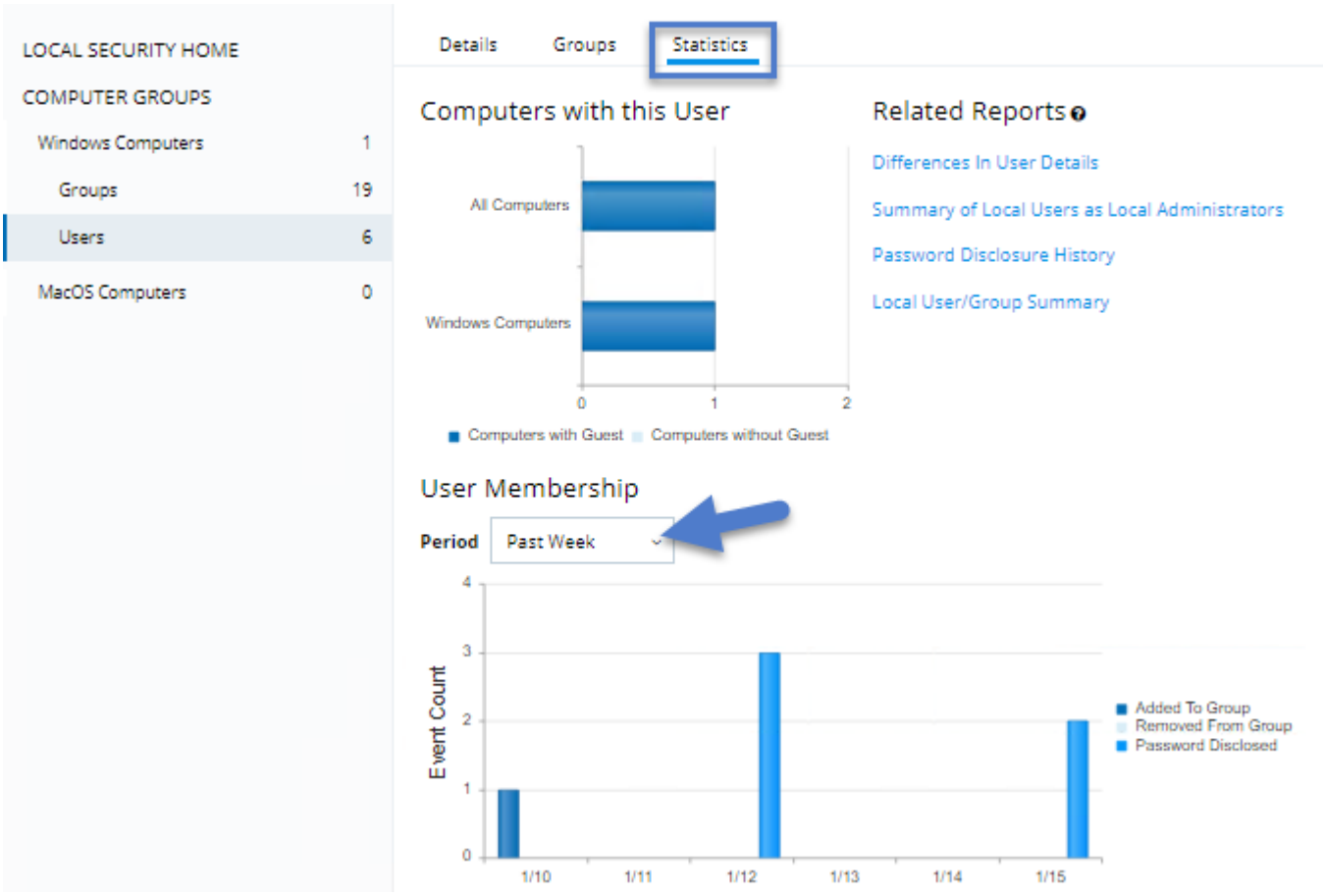
If the password is being managed, the **Update Schedule** determines when the new password is applied. Note, the **Account Details** of the user do NOT need to be managed in order to manage the password on a local account.

Groups Tab

The Groups tab for a Local Account tells you how many groups and computers the account is on. Clicking on a Group Name from this page will direct you back to the Details tab for that local group.

Statistics Tab

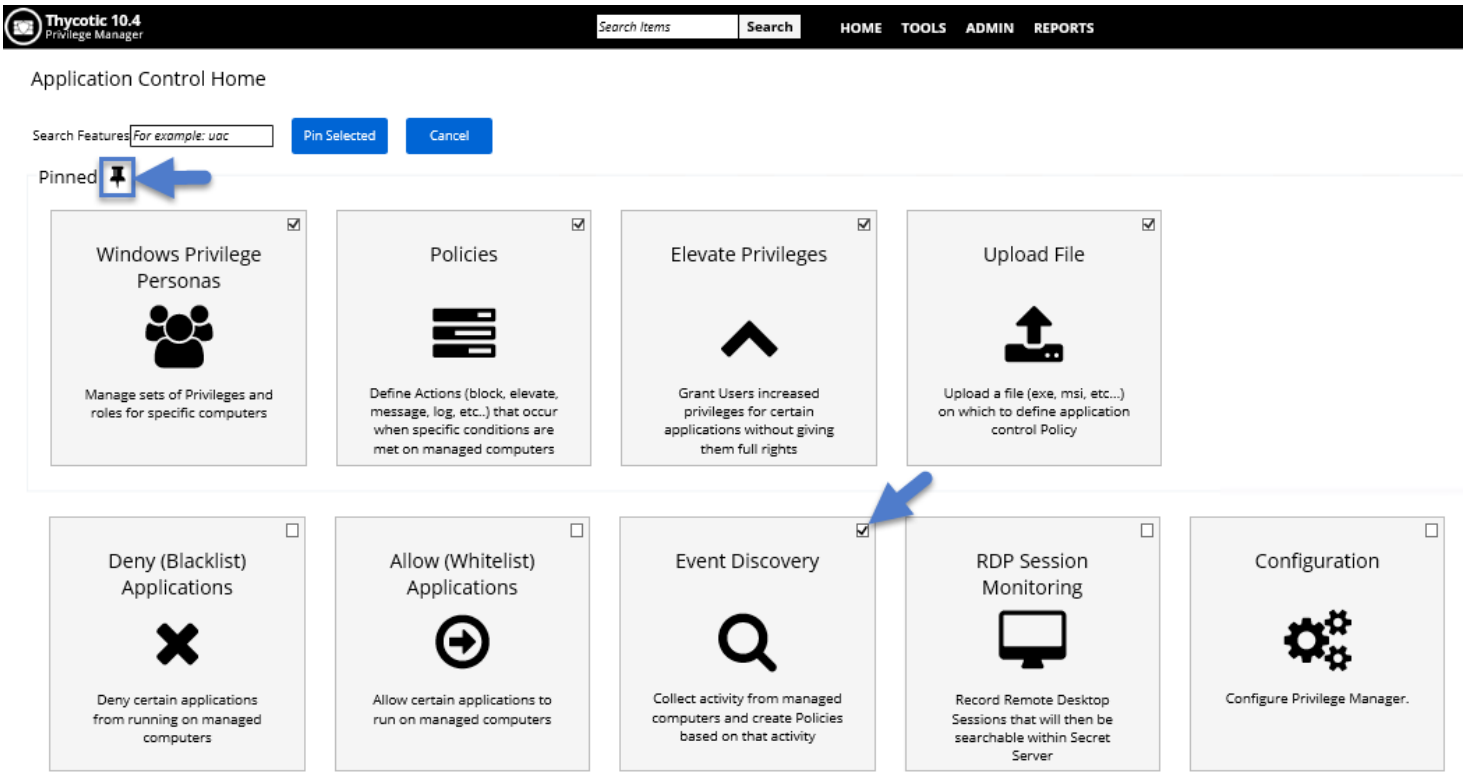
The Statistics' tab for a local user account highlights some quick visual statistics and links you to relevant reports based on key factors like how many computers from your network have this user account and whether there have been changes that are made to the User's Membership within the specified period. Click these graphs to drill down into more details.


LOCAL SECURITY HOME
COMPUTER GROUPS
Windows Computers 1
Groups 19
Users 6
MacOS Computers 0
Details
Groups
Statistics
Computers with this User
All Computers
Windows Computers
0
1
2
Computers with Guest
Computers without Guest
Related Reports
Differences In User Details
Summary of Local Users as Local Administrators
Password Disclosure History
Local User/Group Summary
User Membership
Period
Past Week
Event Count
4
3
2
1
0
1/10
1/11
1/12
1/13
1/14
1/15
Added To Group
Removed From Group
Password Disclosed

Application Control Overview

Dashboard

From Privilege Manager's **Home** click the right **Application Control** section to enter your Application Control **Dashboard**. Tiles provide shortcuts to the different components that are housed within Application Control. You can Pin tiles to the top of your screen to enhance navigation:



What is a Policy?

In Application Control, layered **Policies** create the backbone, or parameters, that dictate precisely how privileges are accessed across your network. They define what a user can run, and where. A policy is made up of customizable filters that apply an action to specific **Computer Groups**. In other words, each policy is defined by:

Filters What criteria needs to be met to apply this policy?

Targets Where should this policy be applied?

Actions What should happen to the applications this policy applies to? (that is, blocked, allowed, and so on)

During the creation of a Policy, you specify Actions and Targets, but Filters are created separately and then assigned to Policies.

Overview of the Configuration Process

This Setup Guide walks you through the specific steps you can take to configure a few popular example policies in Privilege Manager. While there are many different types of policies, the setup process must follow these basic steps:

1. **Collect File Data—**This enables Privilege Manager to recognize specific files and file types in your environment. The file data that you want to target with policies are called **Events**. All imported files can be viewed in the **Event Discovery > Files** page.

2. **Create Filters**—This step sorts important file data (Events) according to different criteria.

3. **Create Policies**—This step defines what 1) **Actions** to perform on applications and the 2) **Targets** (Locations) for those actions.

4. **Assign Filters to Policies**—This step directs a Policy's actions to the appropriate Events happening on your network. This step also allows a Policy to be **Enabled**, or activated.

5. **Order your Policies based on priority level**—Once your policies are created, the order they run across your network matters. See the **Policy Priority** section in this guide for more details.

Collecting File Data

Before Privilege Manager can do anything else for Application Control, it must be able to recognize files or file types in your environment like applications or executables that run. File data can be collected in several ways:

   a. **Event Discovery** – Discover active applications on your network by setting up **Learning Mode Policies**
   b. **File Upload** –Directly upload a specific file that you want to target
   c. **Remote File Inventory Task (Windows/MacOS)—**Scans endpoints directly and imports all file data (both active and inactive files) that exist on the targeted machine/s.

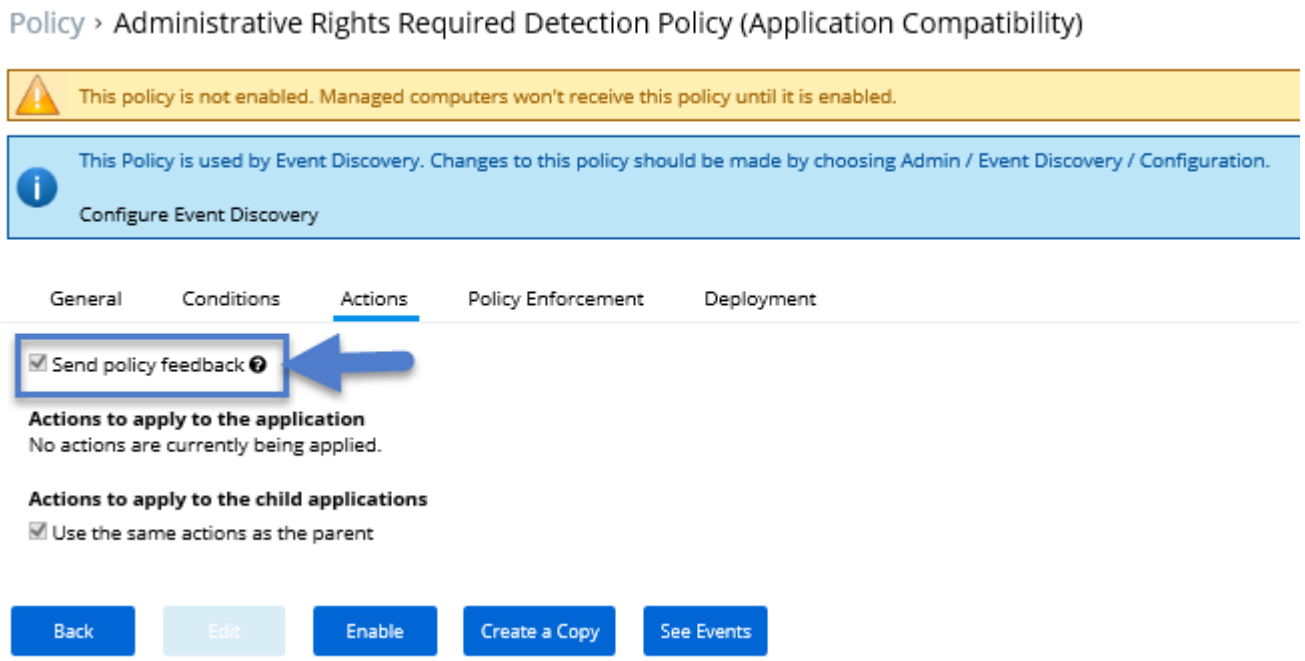
Event Discovery

Learning Mode Policies – Send Policy Feedback

At the most basic level, a **Learning Mode Policy** is a policy that takes no action, it exists only to gather data and you can use the data that it gathers for audits or for assigning actions to application events retrospectively. For trials and Proof of Concept (**PoC**) environments these can be pointed at specific endpoints in order to learn about events that are already happening, or in order to test-run specific applications that you want to quickly introduce into Privilege Manager.

Any Learning Mode Policy has the **Send Policy Feedback** selected under the Policy's **Actions** tab.

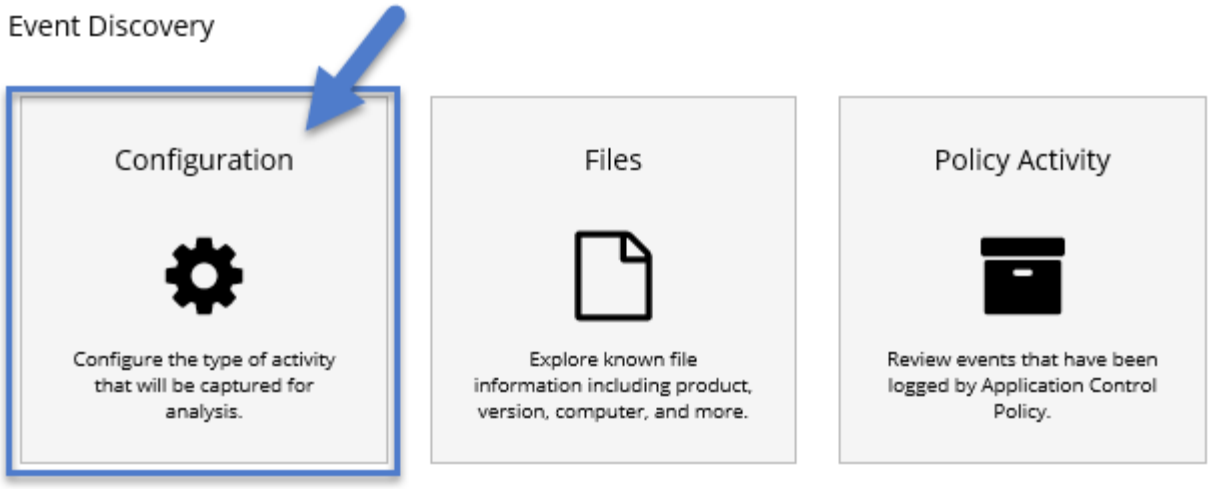
NOTE: Send Policy Feedback is generally disabled in production environments outside of specific auditing or data-collecting initiatives due to the large amount of data these policies can gather.



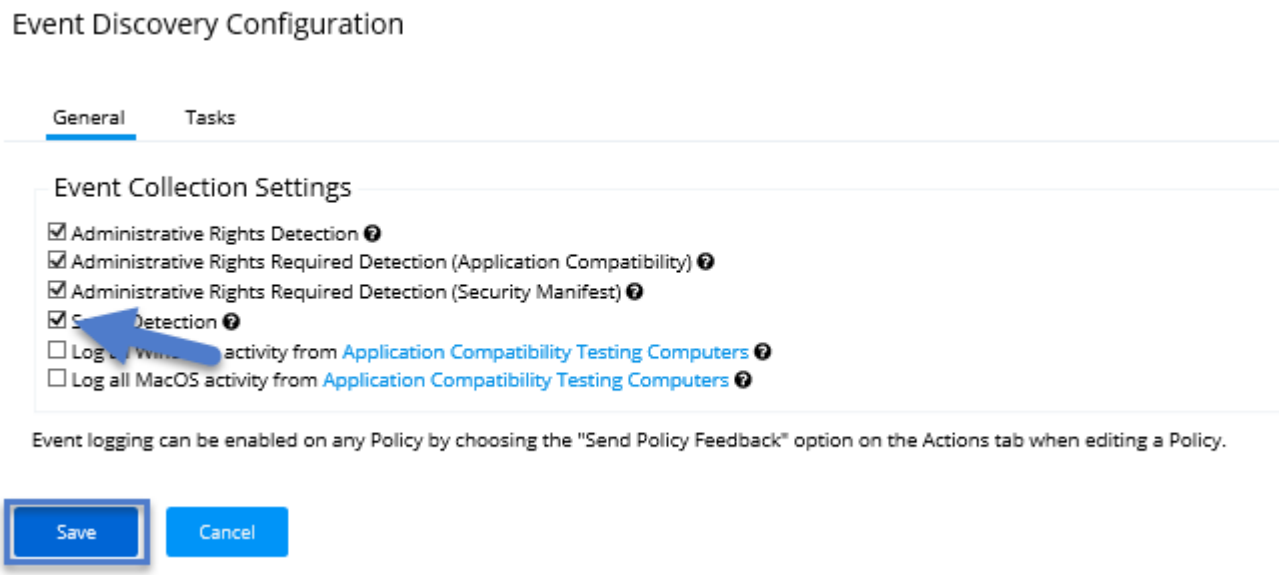
Discover Applications that Require Administrator Rights

The most influential applications are those that require administrator credentials to run. For setting up endpoints that are organized by **Least Privilege**, you can use a Learning Mode Policy to discover all events requiring Administrator rights.

1. From Application Control's Dashboard, navigate to **Event Discovery**. Next, click **Configuration**.



Here, you see a list of pre-configured policies:



2. Click **Edit** and check the boxes of the first four Collection Settings: **Administrative Rights Detection, Administrative Rights Required Detection (Application Compatibility)**, **Administrative Rights Required Detection (Security Manifest)**, and **Setup Detection.**

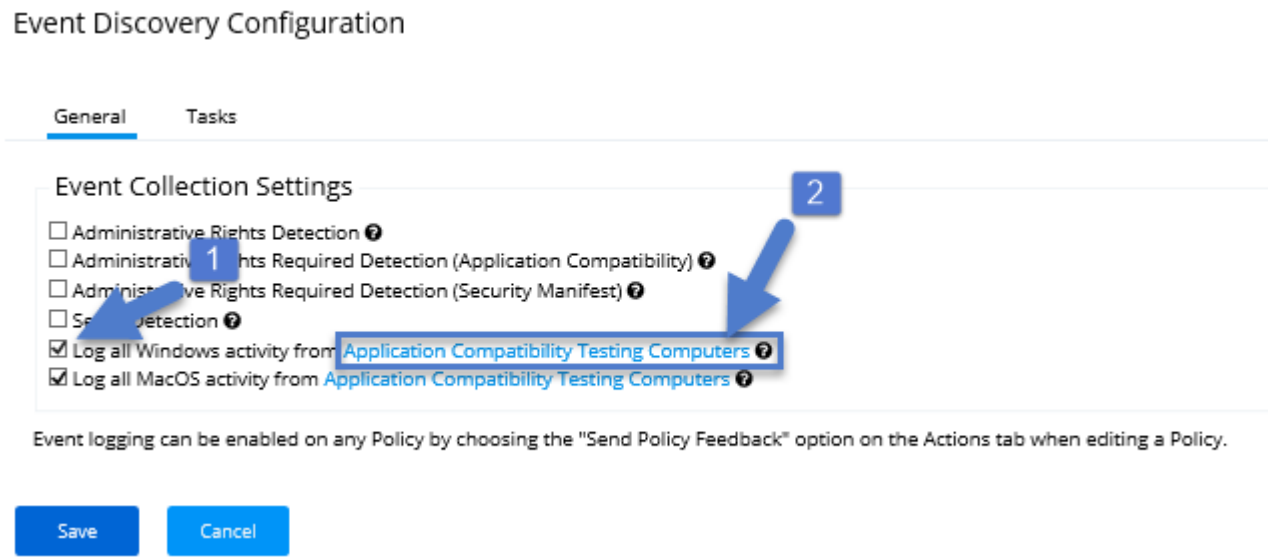
Click the **"?"** icons beside these options for explanations of each setting. Each Collection Setting that is listed here is a Policy that flags any event on endpoints that required a User Account Control (UAC) prompt.

Discover All Events on Test Endpoints

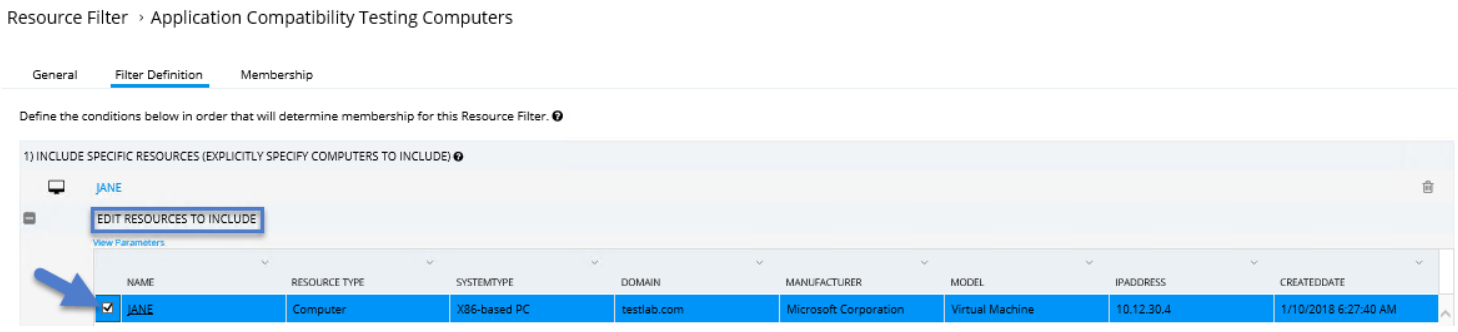
Another type of Learning Mode Policy discovers all events on targeted machines regardless of whether the application requires Administrator Rights. This policy is used in test environments to quickly target policies at untrusted/unwanted applications, but is not recommended for production settings.

1. From the **Event Discovery** > **Configuration** screen select **Edit** and check **Log all Windows/MacOS activity from Application Compatibility Testing Computers**.

2. Simply checking these boxes will not activate this policy. To begin collecting data, you must first specify target computers. To do so, click the text **Application Compatibility Testing Computers**



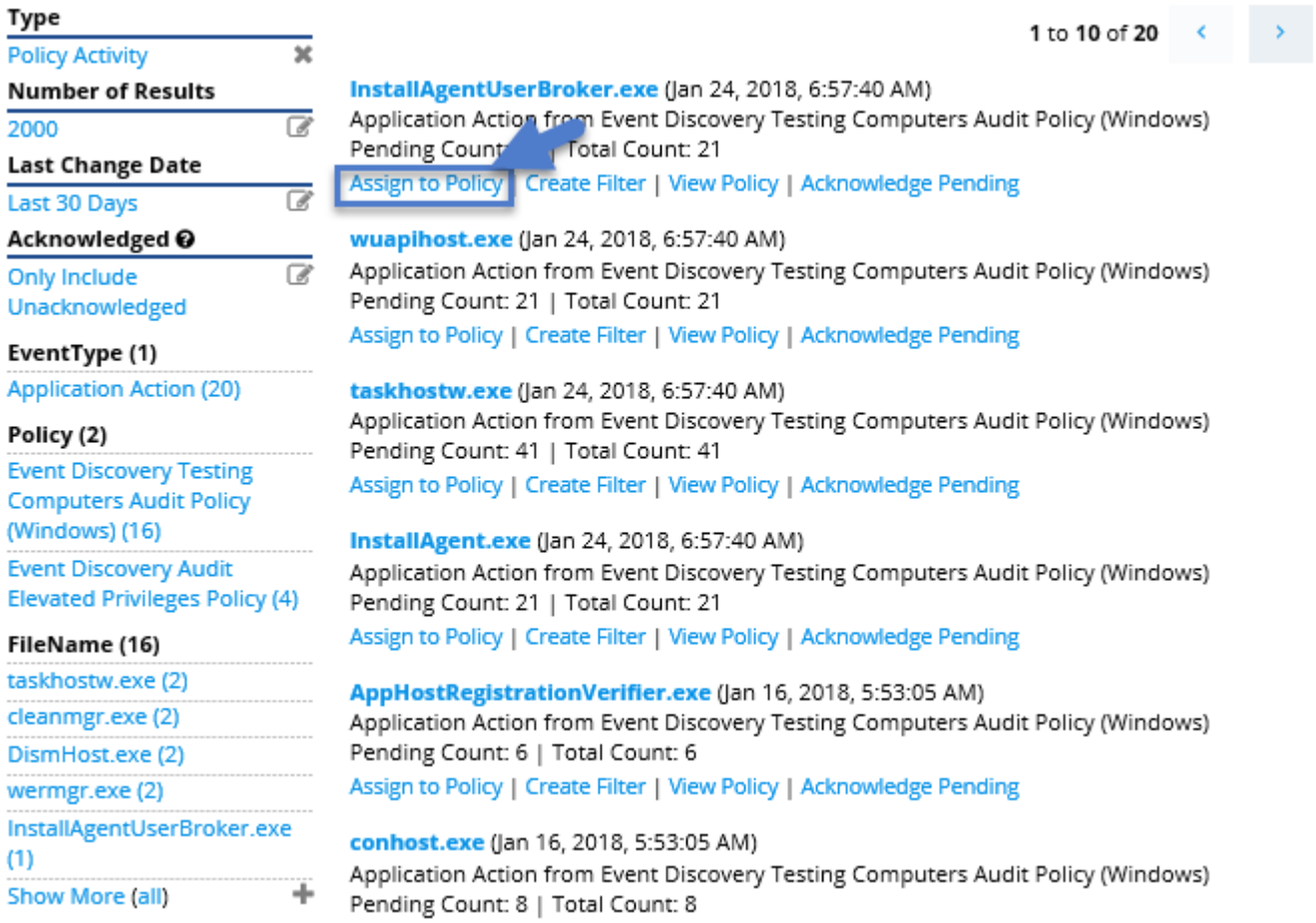
3. Under the **Filter Definition** tab, click **Edit**, then **Edit Resources to Include**. Here you can add specific **Resource Filters**, or target machines that your new policies run on.



4. When target computers are selected, click **Close**, then **Save.**

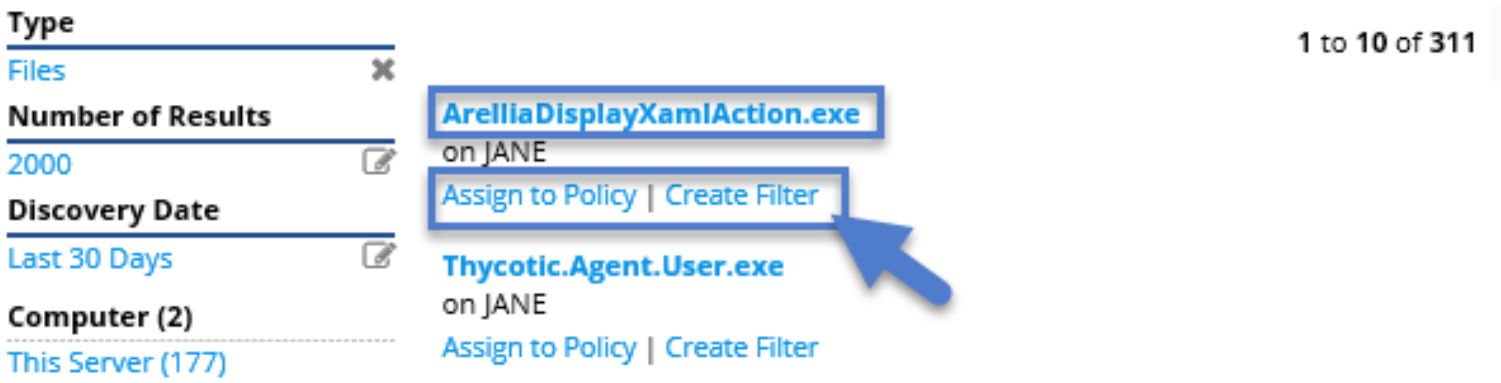
View Policy Results

To view all feedback, or event, sent from your existing policies with the “Send Policy Feedback” activity that is checked, navigate from Dashboard to **Event Discovery > Policy Activity**. Events are listed in the main section and on the left sidebar you can scope results for certain policies, computers, time frame, and so on. You can use this view to assign any events to policies by clicking **Assign to Policy** under the event listing.

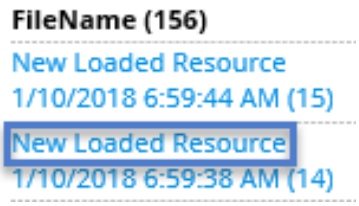


View Files

You can also quickly glean any new files that are found by Privilege Manager in the **Event Discovery > Files** Screen. Distinct from the Policy Events’ screen view, the Files page only shows files rather than displaying all events attached to current policies.

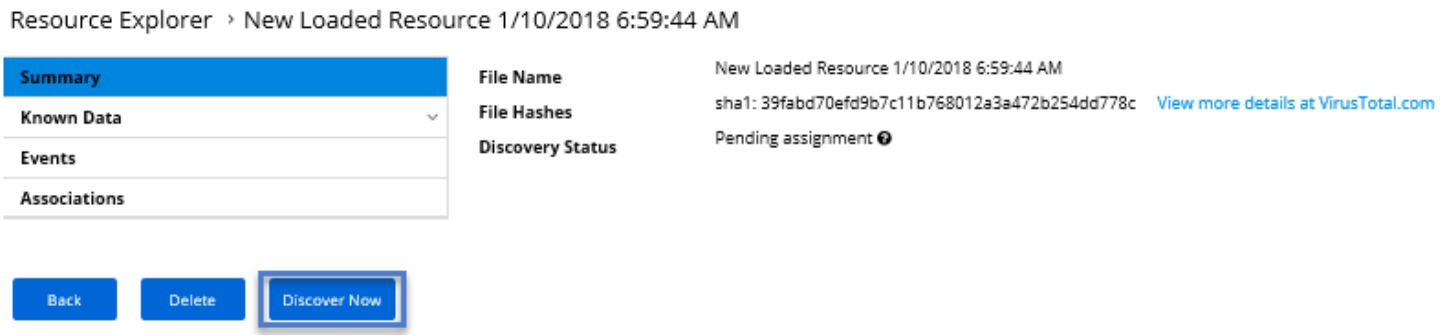


New Loaded Resource



At the beginning of your policy creation process, you see many new events that are labeled as "**New Loaded Resource.**" This is because importing files in Privilege Manager is not the same thing as discovering information about the files. Discovery of file details is done by scheduled policies by default, but if you want to discover file details immediately, do the following:

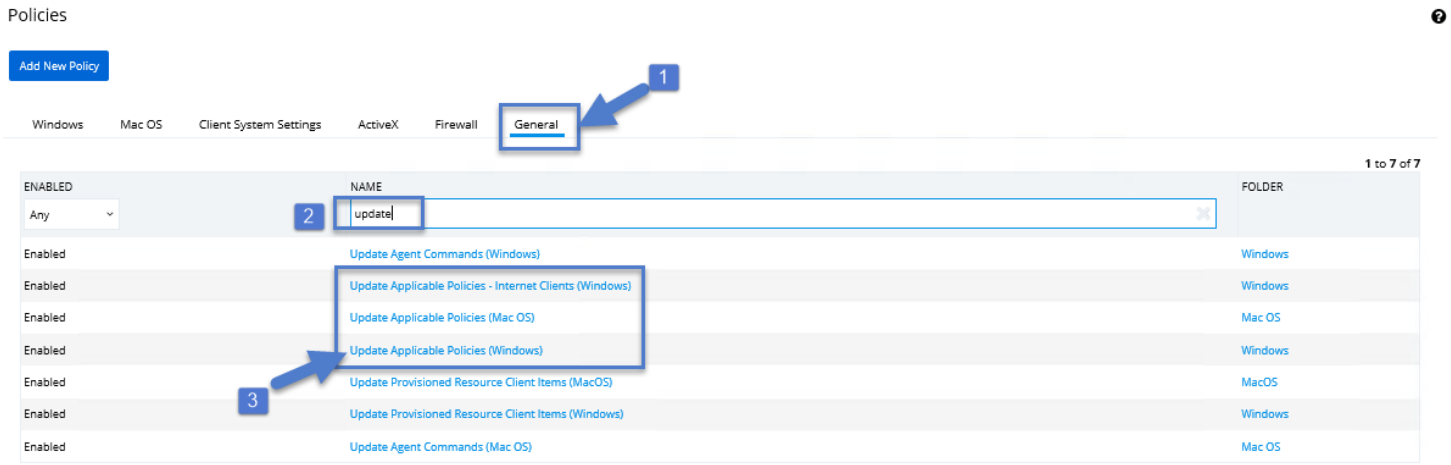
1. Navigate to **Event Discovery > Files** and click one of your **New Loaded Resource** files. Click **Discover Now**. This process might take a few minutes. If the file is not discovered, check to make sure that your endpoint target resource is running. Files might not be discovered if they have already been deleted in your system.



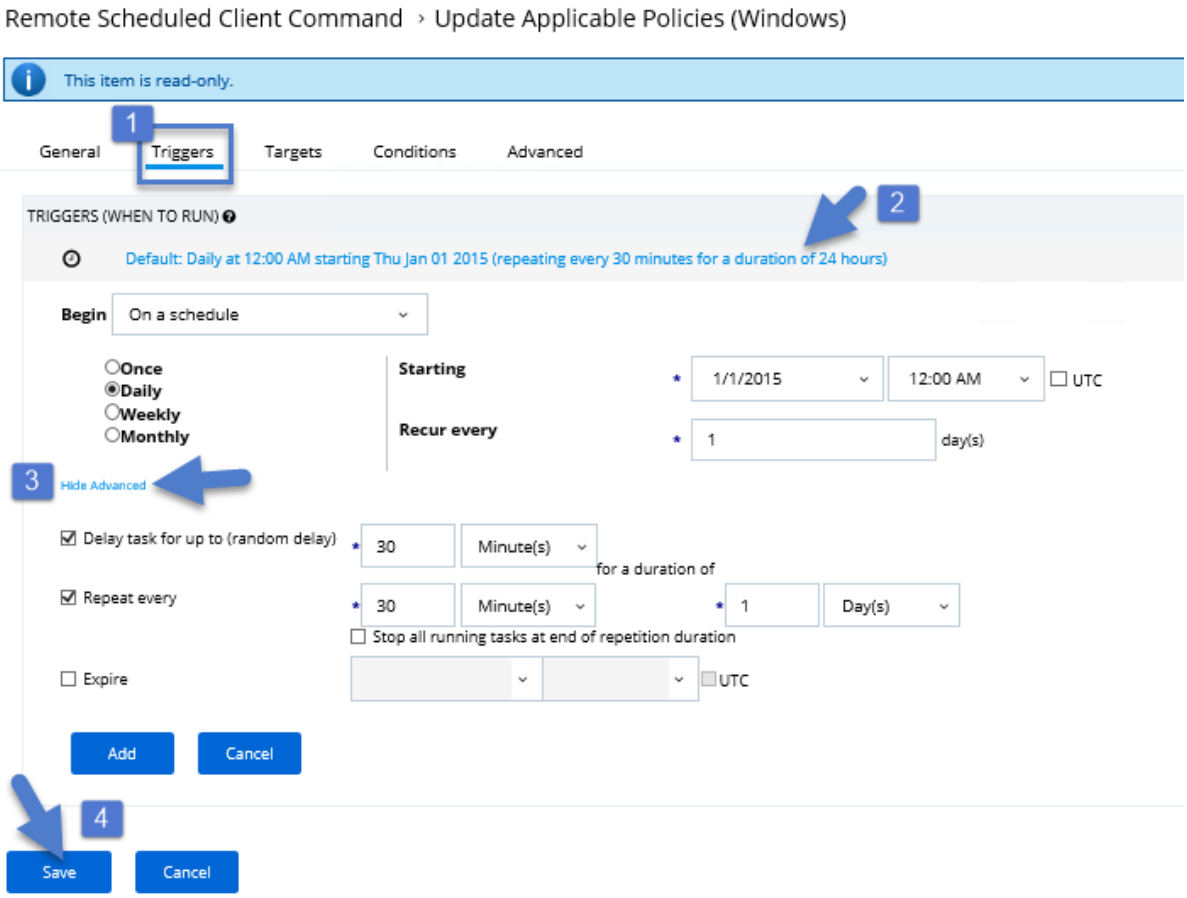
Sending Policies to Endpoints

After setting up your first policies, keep in mind that even after you enable them, **new policies are not immediately sent to target endpoints**. Instead, policies are updated on endpoints via the schedule that is defined by the **Update Applicable Policies** task.

1. Go to **Admin > Policies > General Tab** and search for the **Update Applicable Policies** task from your list of Scheduled tasks:



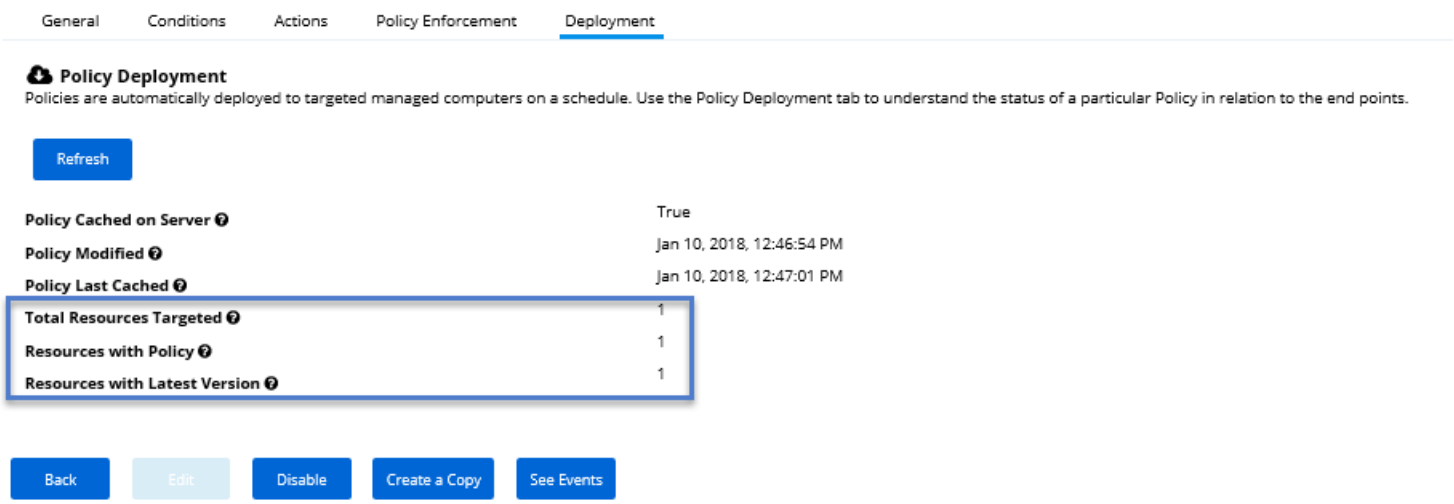
2. To edit the time scheduled that sets off this task, Click into the task, under the **Triggers** tab click the **Default: Daily** setting, then choose the **Show Advanced** link to adjust how often this task will be repeated.



In production environments having a delayed deployment schedule prevents performance issues when adjusting policies and rolling them out across many agents on your network. However, when setting up new policies you might want to immediately activate them on testing endpoints and verify that your configurations are working correctly. Remember to **Save** any changes you make to activate this schedule.

View Deployment Status

Within a Policy's Detail View, Navigate to the **Deployment** tab. This tells you how many computers the policy is already deployed on:



Update Policies on an Endpoint by using PowerShell

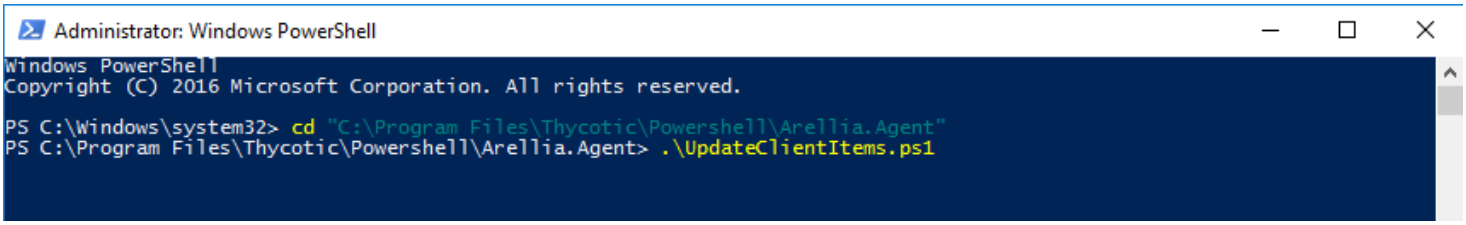
The fastest way to deploy or update your policies on a specific testing endpoint is by running a simple PowerShell script directly on your test machine where an Agent is installed.

1. **On your endpoint machine**, right-click on the **Windows Powershell** application and select **Run as Administrator**.

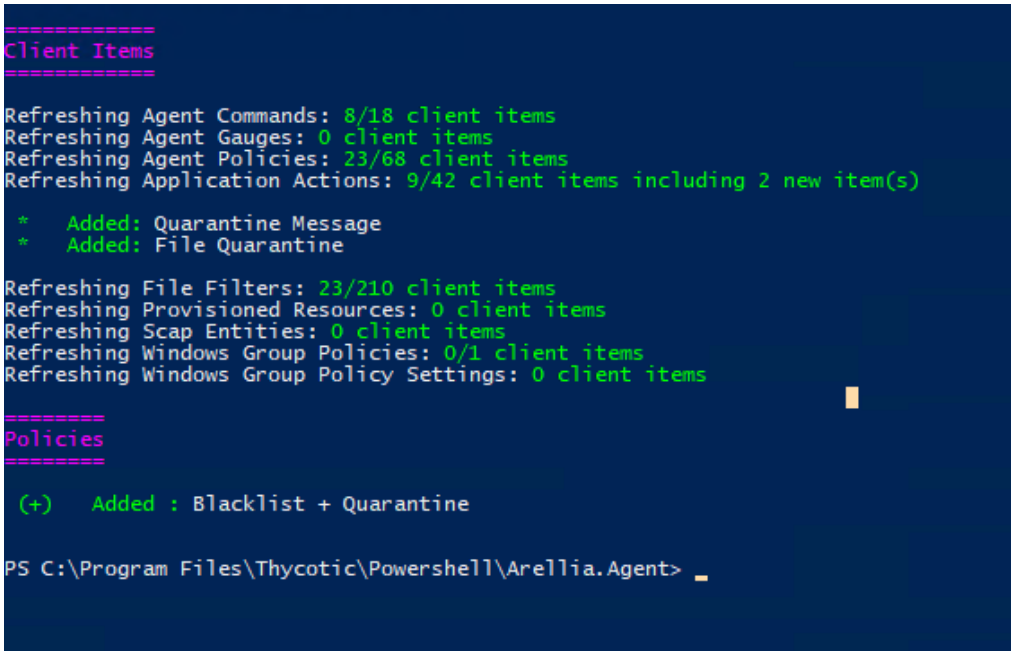
2. Navigate to the Agent directory by entering the following command and then **enter**:

cd "C:\Program Files\IBM\Powershell\Arellia.Agent"

Next type **UpdateClientItems.ps1,** then **enter**.



Your results look something like this:



In this example, we see that a new "**Blacklist + Quarantine**" policy was successfully added to the endpoint machine.

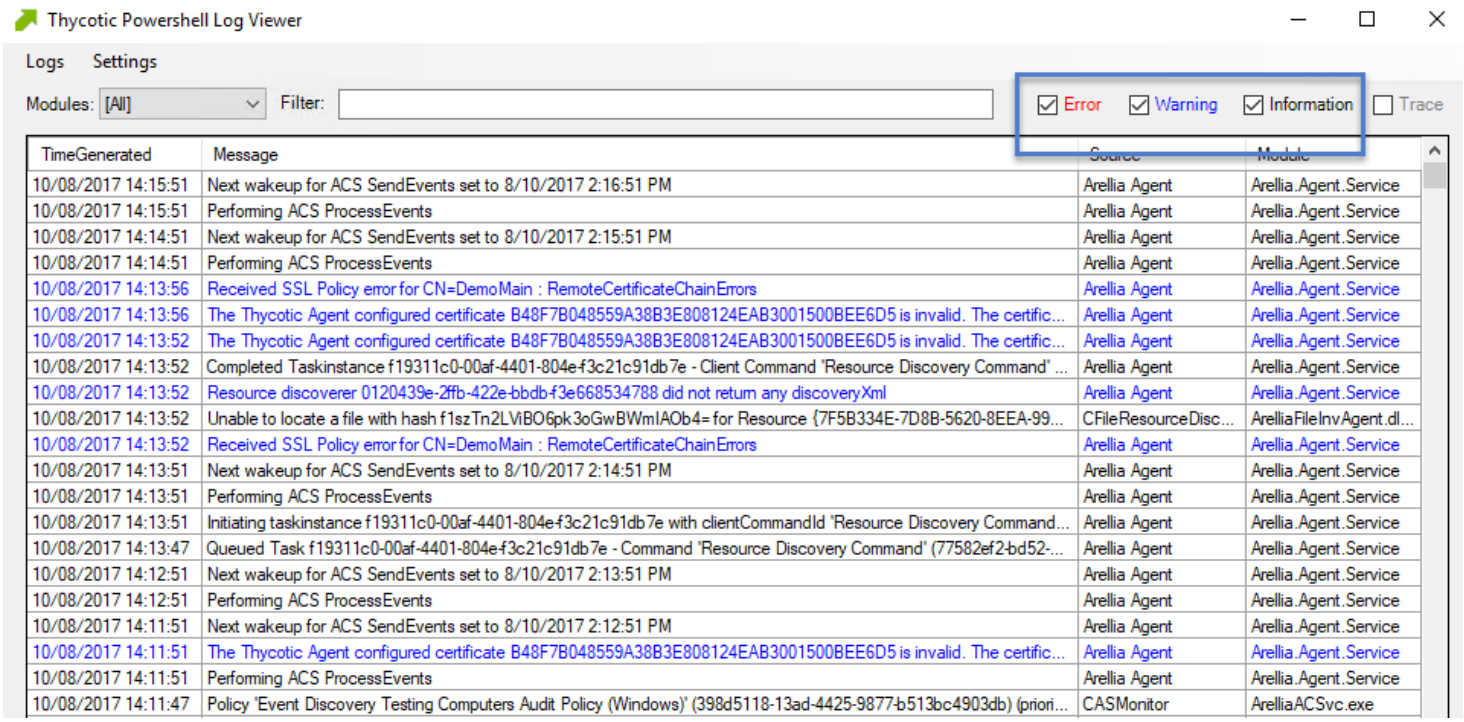
NOTE: If your policies are not immediately updated, wait a few minutes and try running the script again.

After you've updated your test endpoints, you can try running applications that are targeted by your policies to make sure that the policies are configured correctly. You will also see the policy's **Deployment** tab that is updated if refreshed.

Agent Event Log Viewer

Another helpful place to look when setting up new policies is your **Agent's Event Log Viewer**. On your endpoint machine, navigate to your Agent files. This is usually located in **C:\Program Files\IBM\Powershell\Arellia.Agent**. Right-click on **AgentLogViewer** and select **Run with Powershell**. This opens your Agent Event Log Viewer, which shows updates in real time as the agent communicates with the Privilege Manager server. For remote access, Agent logs are also viewable through the **Windows Event Viewer**.

Scroll all the way to the top of the page to see the most recent activity from your Agent. Clear the Information box on the upper right corner to narrow search results for any Errors and Warning messages that might be occurring. You can also double-click any line item for more detailed information about each event.



Now that you know how to update your endpoints and check to make sure that your policies are working, it's time to start building new policies!

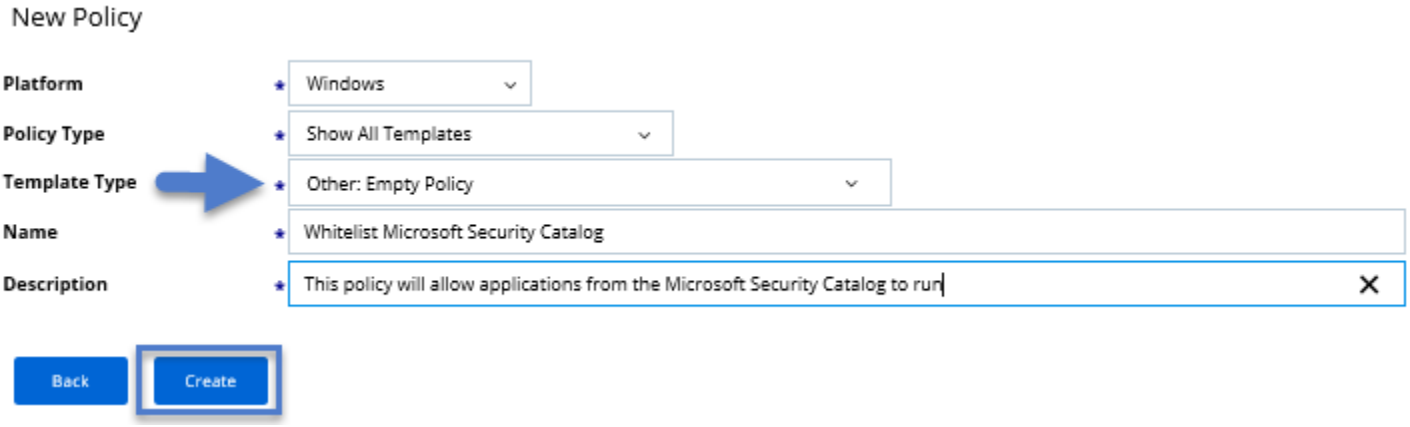
Whitelisting Policies

Whitelisting is a type of policy that allows applications to run on your endpoints. You can think of Whitelisting as a neutral policy type because it does not alter an application's default permissions, it merely signifies that the application is "known/trusted" and allowed to run. Although simple whitelisting follows normal, user-level credentials, whitelisted applications are also often paired with Elevation Policies outlined later in this guide.

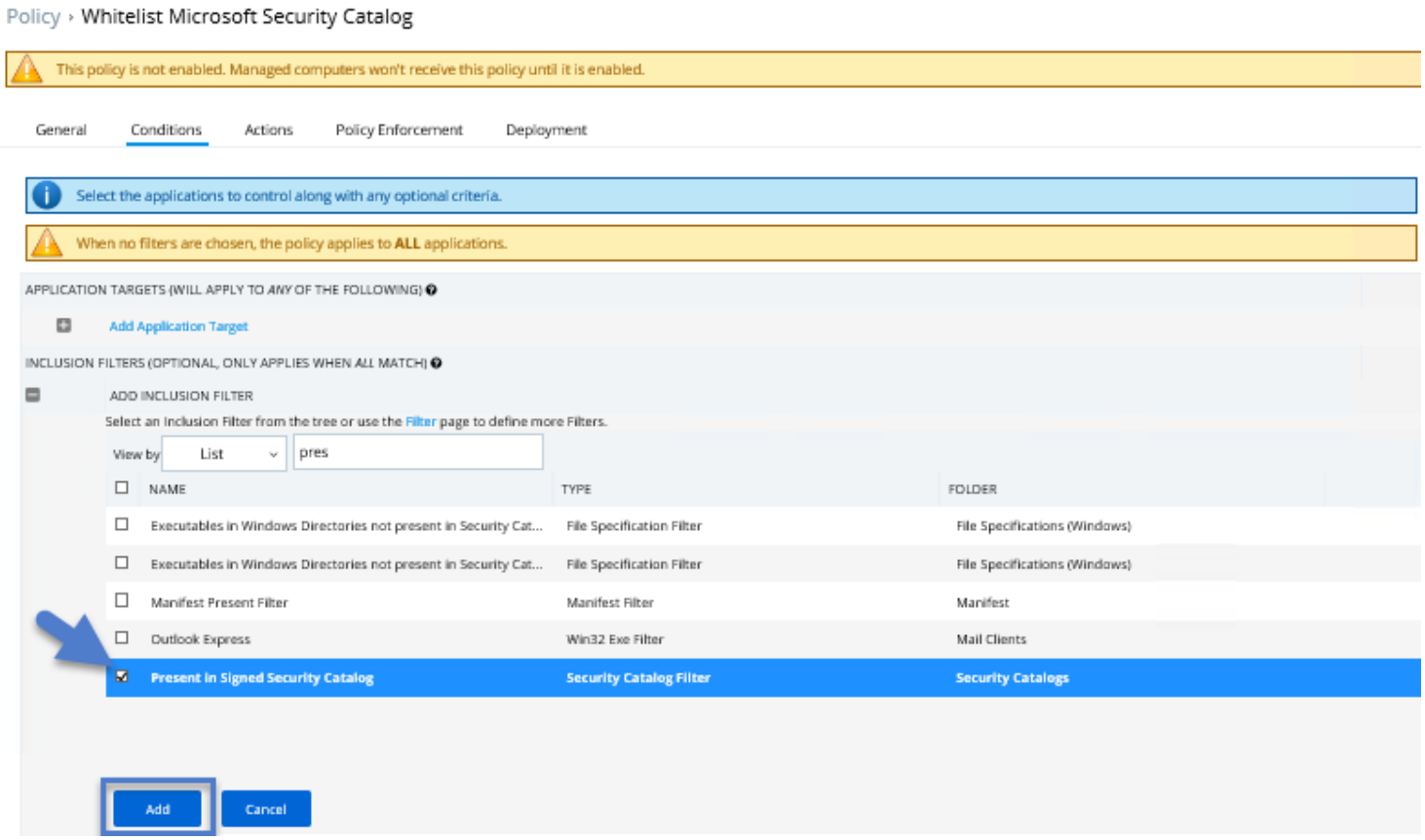
Example: Whitelist the Microsoft Security Catalog

This policy uses a built-in filter to whitelist Microsoft's **Signed Security Catalog**. This filter is often used to dynamically whitelist update items from Microsoft. Whitelisting these executables clears them so they are not affected by any other policy, (i.e. they are allowed to run).

1. Navigate to **Admin** > **Policies**, then click **Create a New Policy**.
2. Select **Windows** as a Platform, **Show All Templates** as a Policy Type, and **Other: Empty Policy** as a Template Type.
3. **Name** the policy and add a **Description**.



4. Click **Create**
5. Under the **Conditions** tab choose **Edit,** then **Add Inclusion Filter**. Type "**Present in Signed Security Catalog**" in the search bar to pull up the correct filter for this use case. Click **Add,** then **Save.**



6. Navigate to the **General** tab, **Edit**, and check the **Enabled** box to activate this policy. Click **Save**.

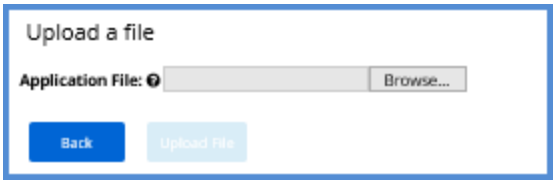
No action is required to add under the **Actions** tab, meaning that these items will be *Whitelisted* – i.e. they will be allowed to run with default permissions.

Example: Whitelist Google Applications with File Upload

In evaluation and production installations, proactive introduction of executables into Privilege Manager can be accomplished with a feature called **File Upload**. File Upload allows you to quickly introduce a file, then create a Filter and/or a Policy to govern the application. As example, here's how to introduce the Chrome Installer into Privilege Manager and use the file information to whitelist other Google applications.

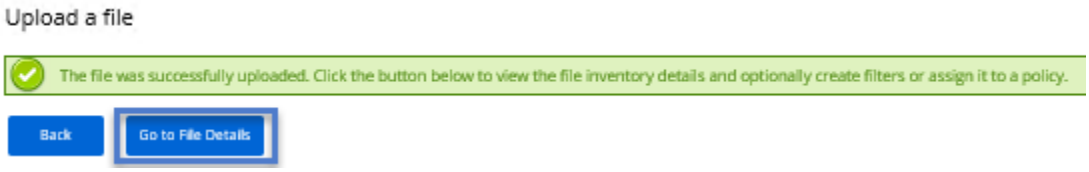
For this use-case you need to have access to downloaded Chrome installer files.

1. From the Privilege Manager home screen, navigate to **TOOLS** > **File Upload**.

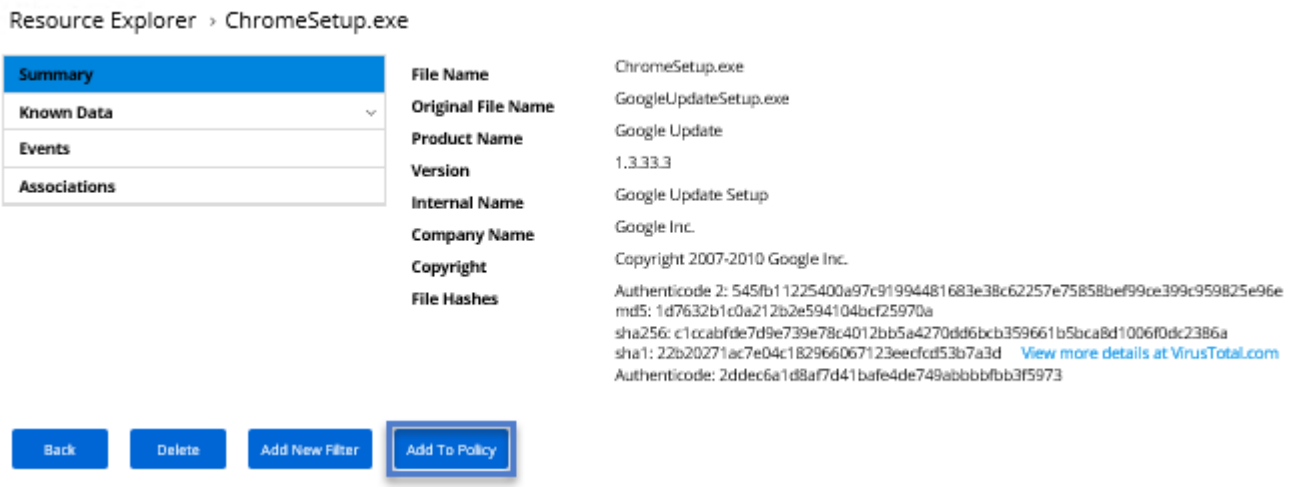


Click **Browse**, and select a file to upload. Click **Upload File.**

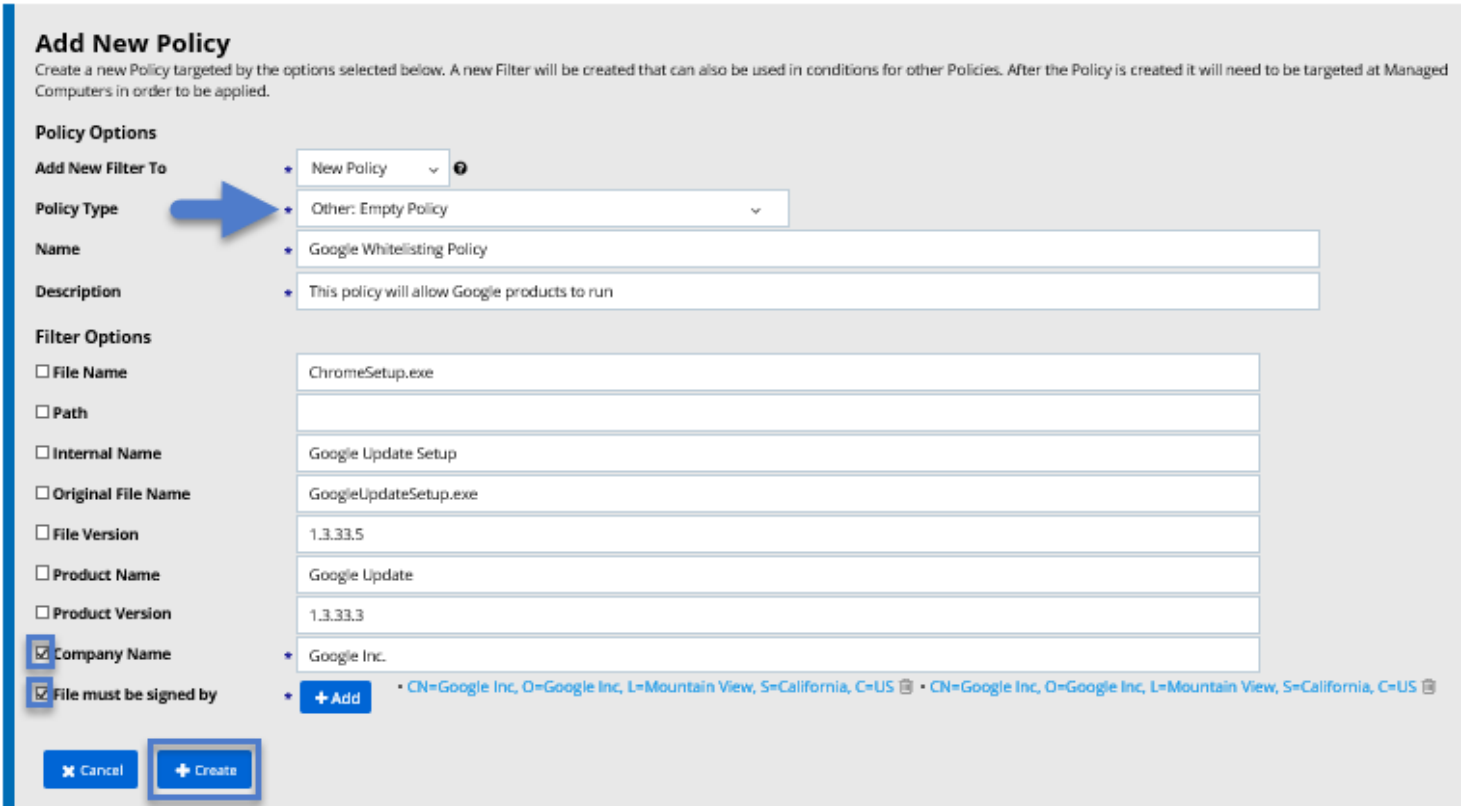
2. When the file successfully uploads, choose **Go to File Details**.



3. Click **Add to Policy.**



4. In the Add New Policy section that appears, select **Other: Empty Policy** as Policy Type, give it a **Name** and **Description**, and check the **Company Name** and **File Must be Signed By** Filters. Then, click **Create**.



5. This brings you to your new policy's detail view. Because this is a Whitelisting example, no extra Actions need to be assigned. Under the General tab, select **Edit**, check **Enabled,** then click **Save** to activate.

Blacklisting Policies

Blacklisting is a policy that denies applications from running on your endpoints based on application attributes, file hash, location, or certificates. This is a powerful type of policy and it might be used to block specific, known, and unwanted applications from running. A blacklist policy can target programs that prevent productivity for your end users or applications that are known malware. If malware, you can also add a quarantine action for your blacklist policy as outlined in the second example below.

Example: Blacklist iTunes with File Upload

As we've seen, there are multiple ways to introduce a new application into Privilege Manager before assigning a policy to it. For this example, we perform a File Upload for the iTunes installer to quickly Blacklist the iTunes program from running on target endpoints.

First, create the iTunes filter by using downloaded iTunes files:

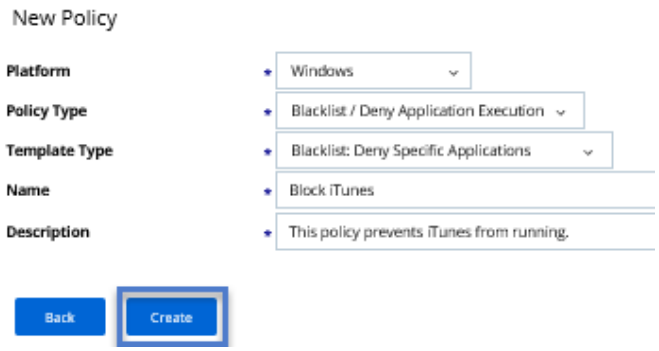
1. From Dashboard, select the **Upload File** tile. **Browse** to select file (that is, the iTunes installer), click **Upload File**.

2. When the file successfully uploads, choose **Go to File Details**.

3. Click **Add New Filter**. Check the Filter criteria you want to block like the **File Name**, the **Original File Name**, and the **Product Name**. Click **Create**

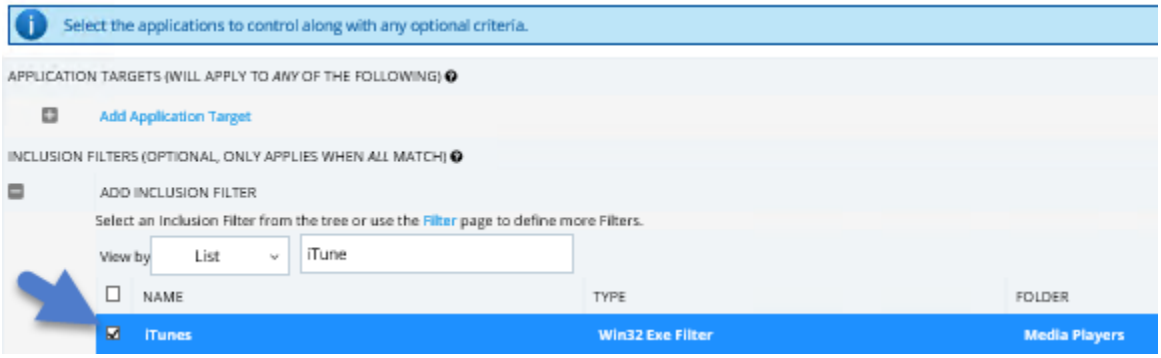
Next, create the iTunes Blacklist Policy:

4. Click the **Deny (Blacklist) Applications** tile on the Dashboard. Select a **Platform**, then **Blacklist: Deny Specific Applications**. Add **Name** and **Description**, click **Create**.



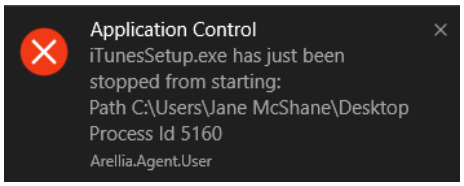
5. In the **Advanced Policy View** under the **Conditions** tab, select **Edit**, then **Add Inclusion Filter**.

6. Select your iTunes filter/s, click **Add**, then **Save**.



7. Under the **General** tab, **Edit**, check **Enabled**, then **Save** to activate this policy.

Under the **Actions** tab, do not change the settings, but notice it is set to **Deny Execute Message**. This produces a pop-up message to the user telling them this application execution is denied:



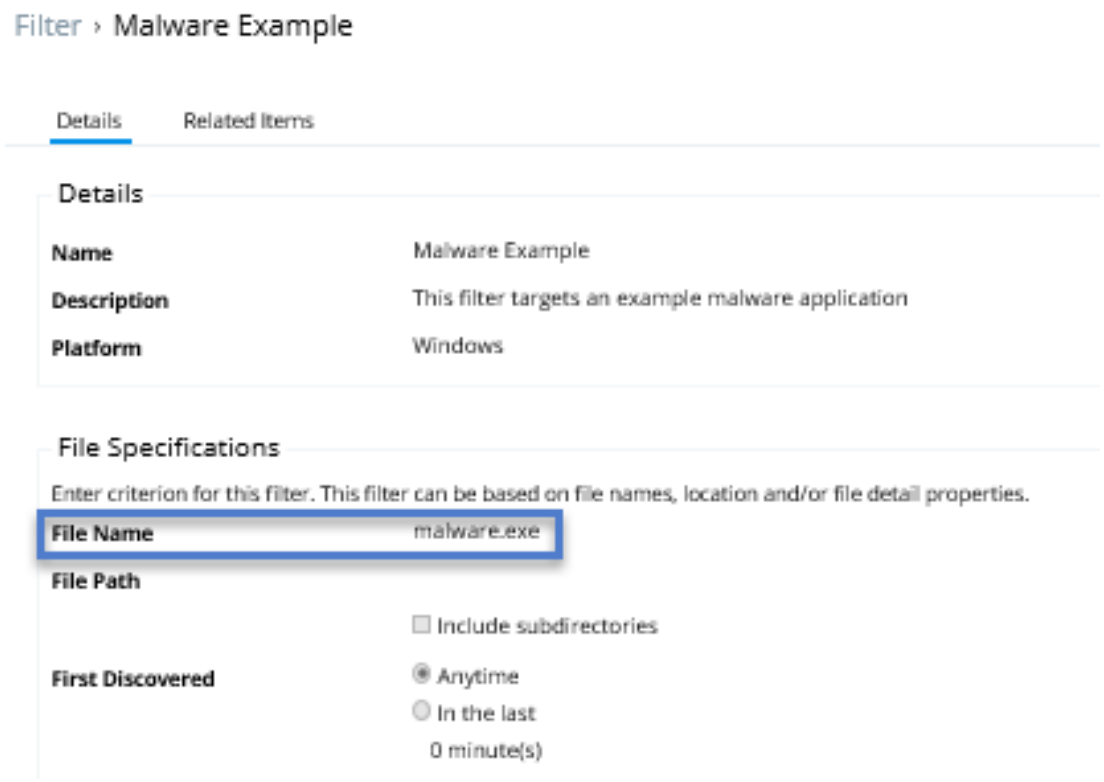
You can edit the policy further, if needed. Adjust the **Policy Priority** as needed. **Policy Priority** is discussed in detail later in this document.

Example: Quarantine Specified Malware

For known cases of malware or ransomware, you can use Privilege Manager to prevent specified applications from running and place them in a quarantine. For this example, target the generic executable "**malware.exe**," but you can do this with any File Name.

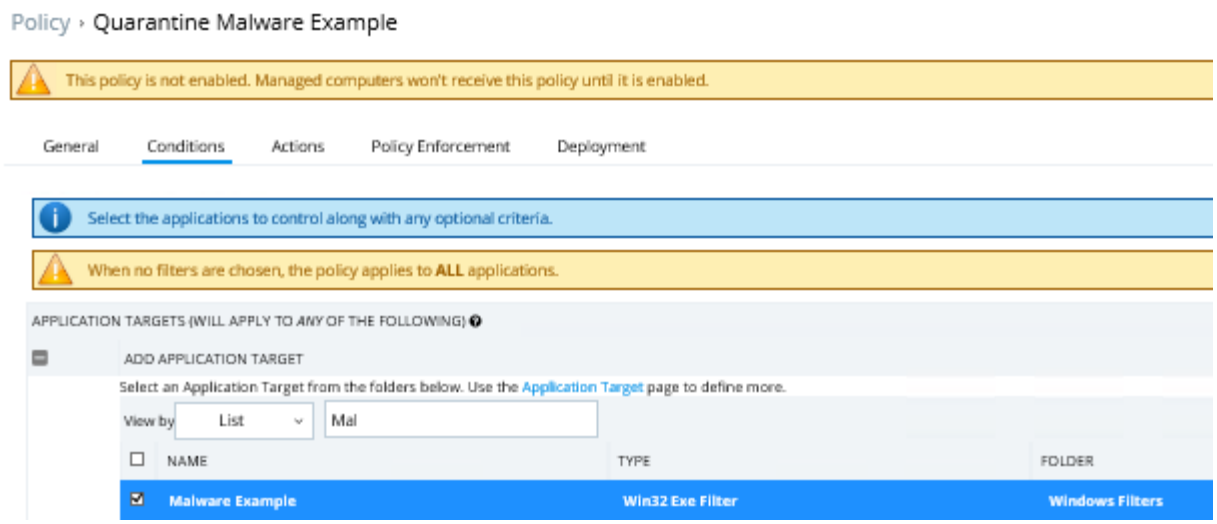
First, create your malware filter:

1. Choose the **Filters** Tile from the Dashboard or navigate to **ADMIN > Filters.** Click **Add Filter**. Select Windows as a platform and **Blank Win32 Executable Filter** as a Filter Type. Name your Filter **Malware Example** and add a description. Click **Create**.
2. **Edit**, and add the File Name **malware.exe**. Click **Save**.

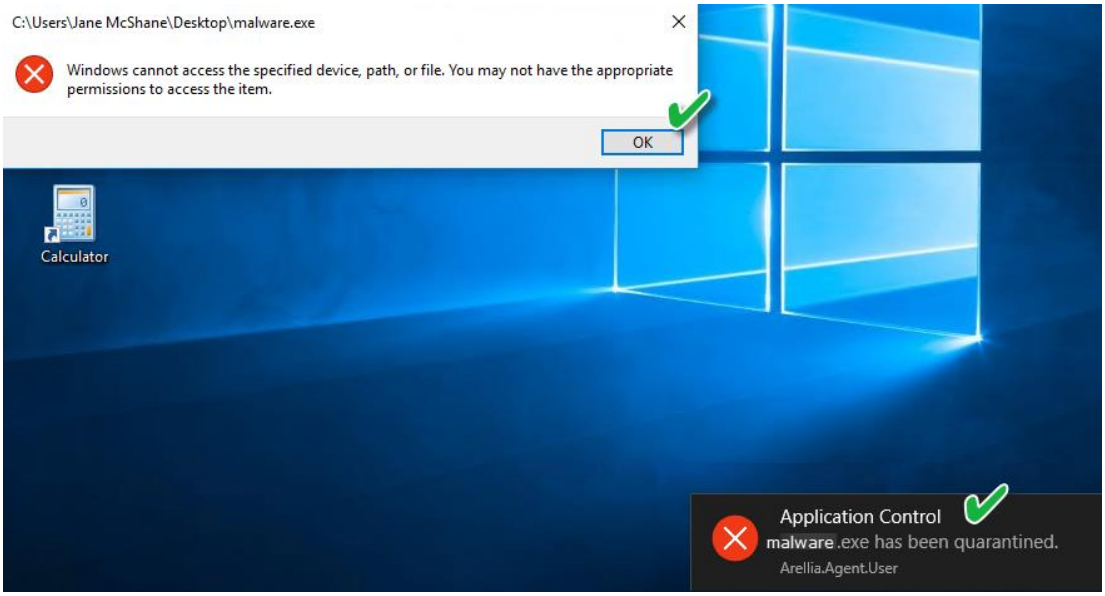


Next, create a Blacklist Policy that will quarantine this filter's target.

3. From the Dashboard click the **Policies** tile, then **Add New Policy**. Select **Windows** as a Platform, **Show All Templates**, then select **Blacklist: Quarantine Specific Applications** as a Template Type. Add a **Name** and **Description**, click **Create**.
4. Click **Edit** and the **Enabled** check box. Choose the **Advanced Policy View** button if possible.
5. Under the **Conditions** tab, **Edit** then **Add Application Target** and search for your **Malware Example** Filter. **Add** and then **Save** this policy.



6. Once this policy has been applied to your endpoint/s, any executable that is called malware.exe is automatically blocked and quarantined if prompted to run:



Elevation Policies

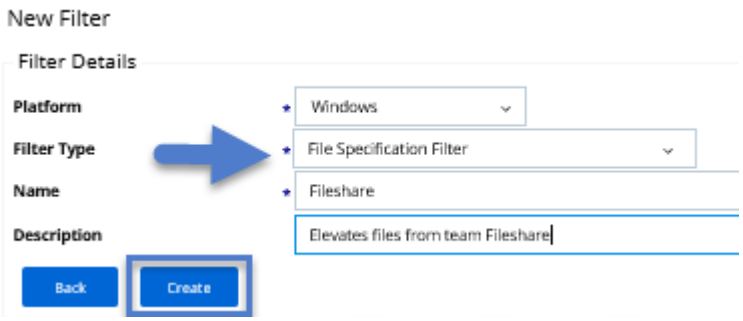
Distinct from Whitelisting policies where applications are simply allowed to run with default user level privileges, an **Elevation Policy** applies Administrator credentials to specified applications. This type of policy is often paired with Whitelisting to save IT Administrators time when many employees must perform trusted tasks that require Administrator credentials to complete, like installing a trusted application (Adobe) or device (printer).

Example: Applying Administrator Rights to a Network Share

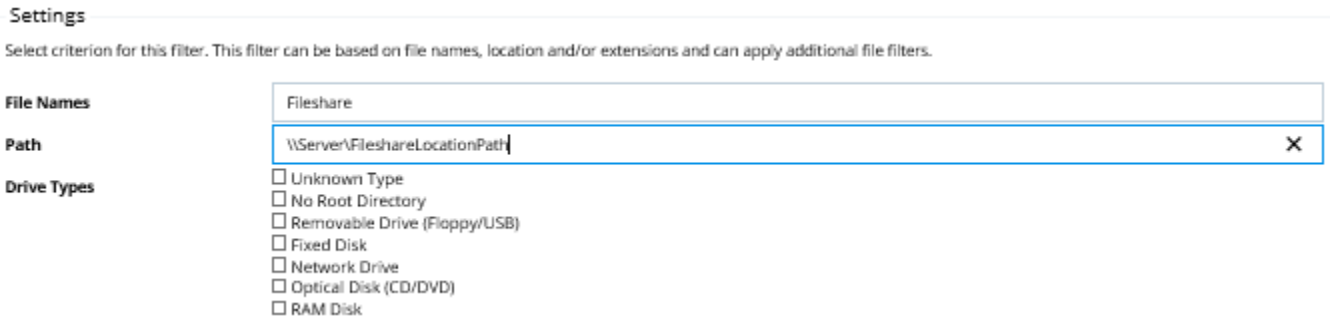
Many organizations put trusted installers on a network share that employees can use. Those installers can be elevated automatically from the shared network location by assigning an elevation policy to the network share location.

First, create a filter in Privilege Manager that points to your Shared File:

1. **Admin > Filters**, click **Add Filter**, select **Windows** as a Platform
2. In the Filter Type dropdown, choose **File Specification Filter**, add a **Name** and **Description**. Click **Create**



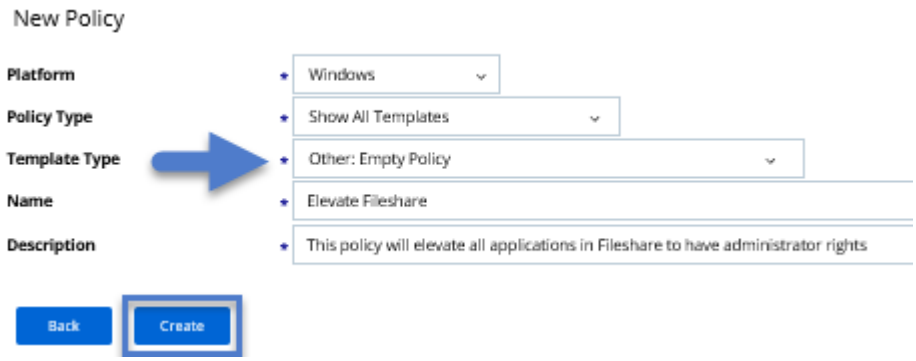
3. Under **Details**, Choose **Edit**, add the **Path** that points to your Fileshare folder, then **Save.**



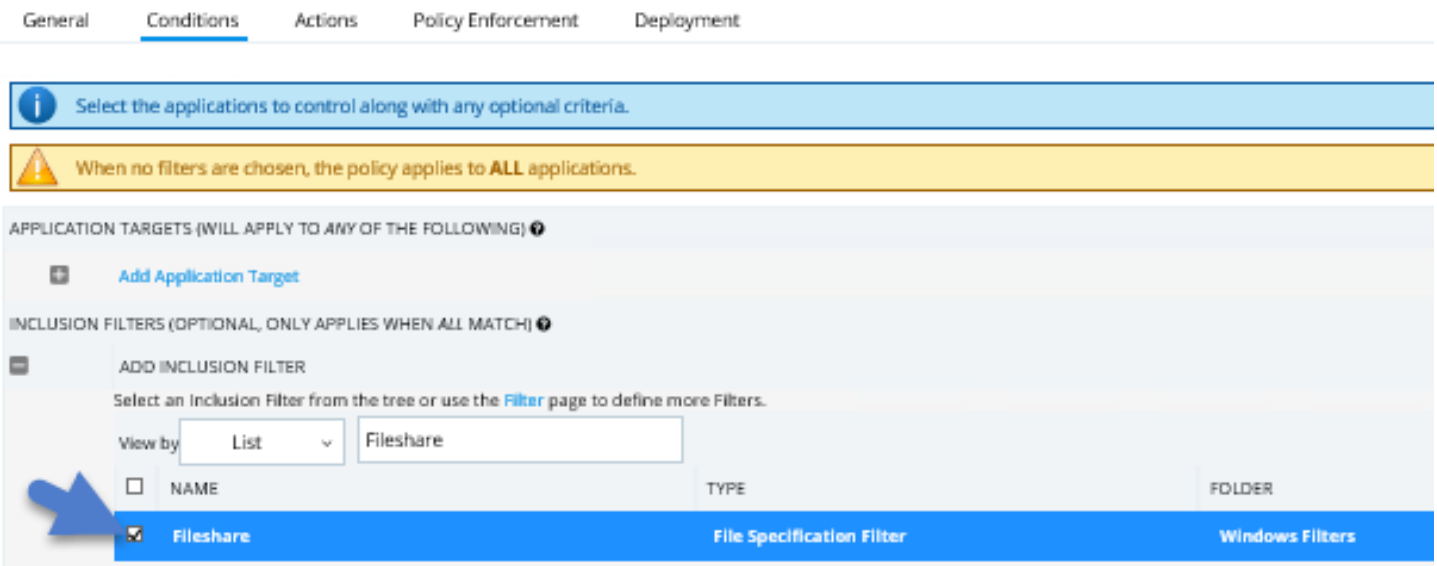
Second, create a New Policy:

4. Navigate to **Admin > Policies,** click **Add New Policy**

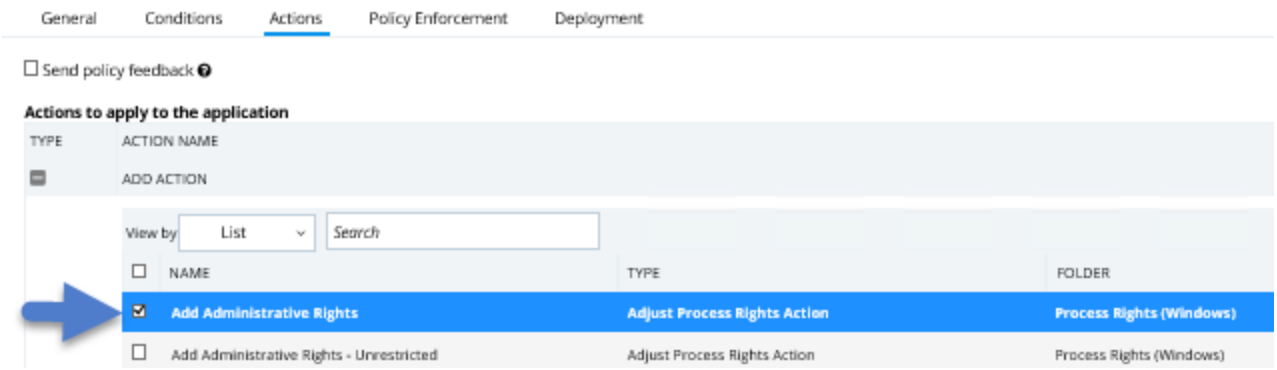
5. In the New Policy screen, select **Windows** as a Platform. Select **Show All Templates** as a Policy Type, then **Other: Empty Policy**.



6. Add a **Name** and **Description**, click **Create**.
7. Under the **Conditions** tab, click **Edit**
8. Click **Add Inclusion Filter.** In the Search bar, type in the **name of your new Filter** and select. Click **Add**, then **Save**.



9. Next, navigate to the **Actions** tab, choose **Edit**, then **Add Action**. Check the box for **Add Administrative Rights**.



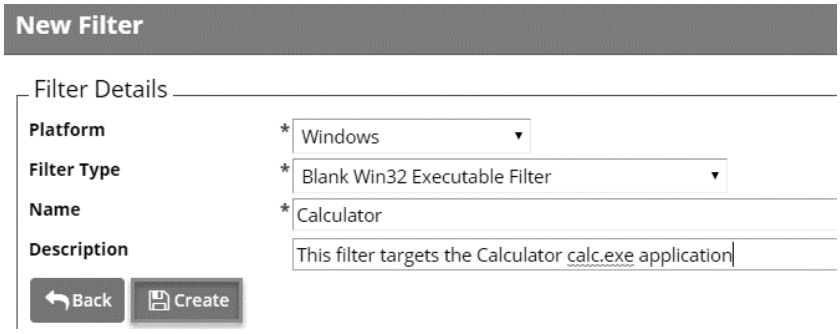
10. Click **Add**, then **Save**.
11. To activate your policy, click **Edit** under the **General** Tab and check the **Enable** box. Click **Save**.

Example: User Justification Required to Run

This policy type requires a user to provide a justification for why they need to run an application before elevating with administrator privileges. **User Justification** refers to the policy action. Since **Conditions** and **Actions** are independent, this action can be applied to any condition. In this use case, we will simply apply this action to a specific application.

First, create a filter that identifies the application.

1. Navigate to **Dashboard** > **Filters**, then click on **Add Filter**. In this use case, we target the Calculator application (*calc.exe*). Select **Windows** for your Platform, then **Blank Win32 Executable Filter**. Add **Name** and **Description**. Click **Create**.

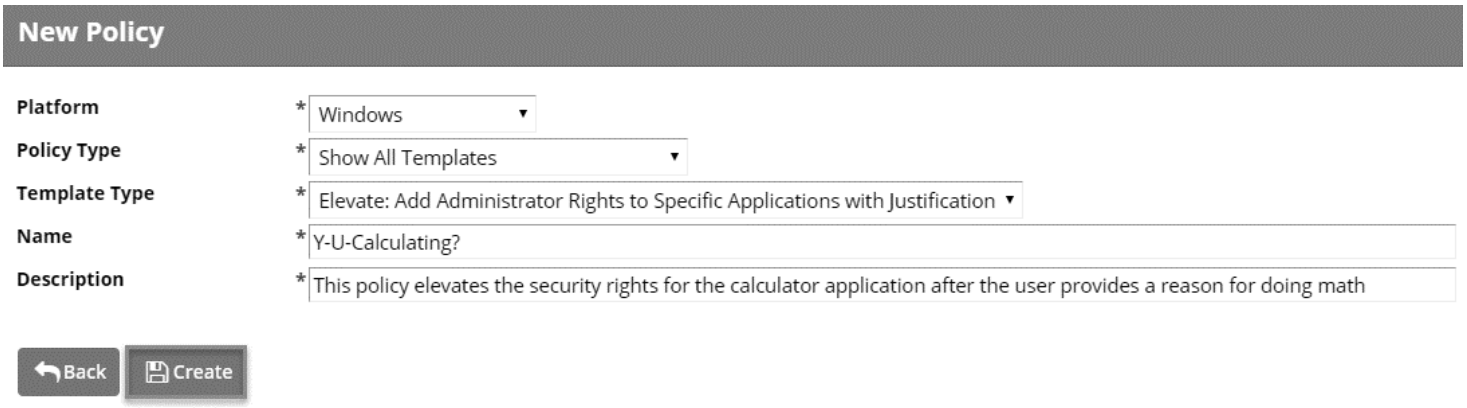


2. Click **Edit** at the bottom of the page. Enter *calc.exe* in the **File Name** field. Click **Save**.

This created a Condition filter that we can now use in the policy to govern the *calc.exe* executable. Next, we'll create the policy that requires justification.

3. Navigate to **Home** > **Policies**, then click **Add New Policy**.

4. Select **Windows** as a Platform, then **Show All Templates**. From the Template Type dropdown **select Elevate: Add Administrator Rights to Specific Applications with Justification**. Add a **Name** and **Description**. Click **Create.**



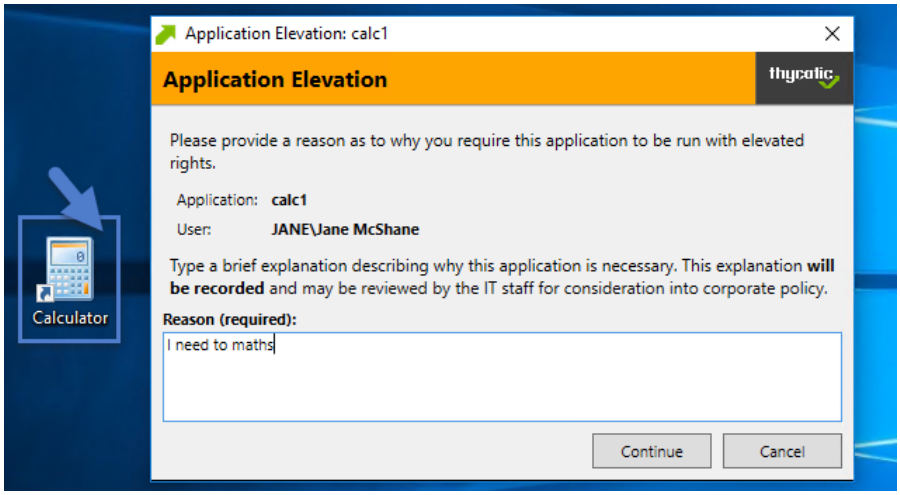
5. **Edit** and check the **Enabled** box and click the **Advanced Policy View** button (if in the Simple Policy View).

6. Select the **Conditions** tab. Select **Add Application Target** and search for the name of your Calculator filter. Select this filter and Click **Add**.

7. Click **Save**. This saves the policy to the policy list accessed from the Home screen – click **Policies** to view from the **Home** page. Once the policy is delivered to the endpoint agent, *calc.exe* will require the user to enter a justification reason for running this application. This policy will be applied to all users on all computers. See details on how to deliver policies to the endpoint in a later section.

To adjust this policy to apply to specific users or endpoints, click the **Advanced Policy View** in the policy's General tab, then click the **Conditions** tab to add Inclusion/Exclusion filters and Computer Groups.

8. The justification message the user will see as a result of this policy:



When the user adds a reason, and clicks the **Continue** button, the application is allowed to run. You can then view a user's provided reasons in Privilege Manager on the **Events Discovery > Policy Activity** page or under **Reports > Application Justification Summary Details Report**.

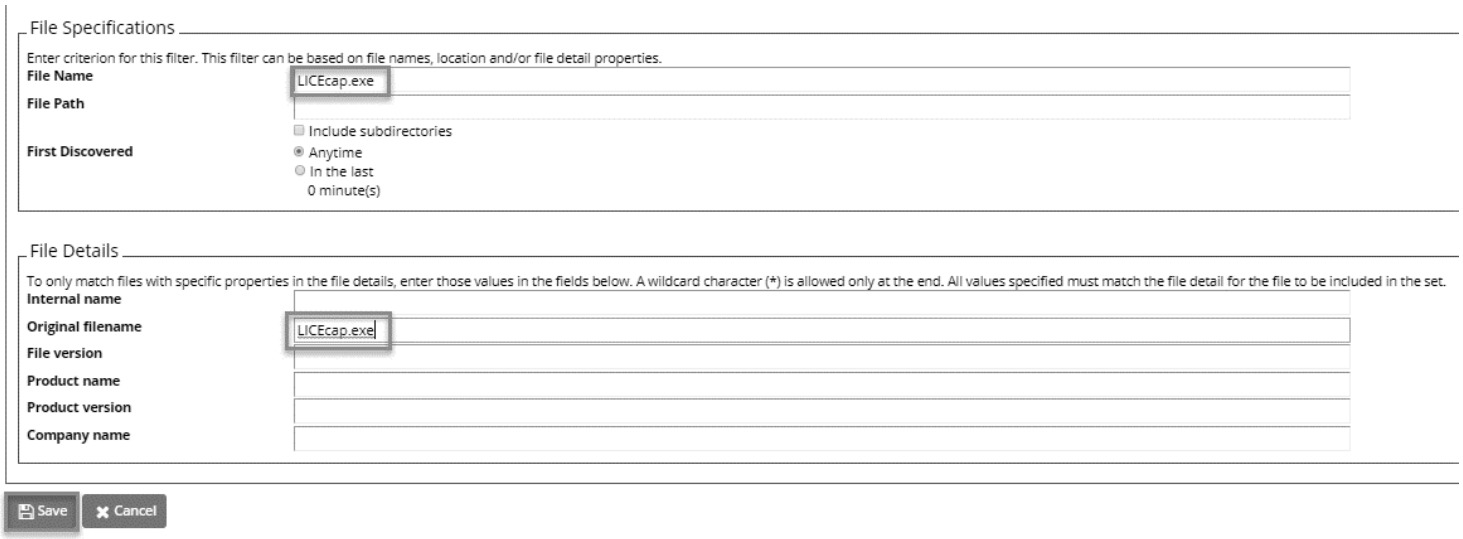
Example: Application Execution Requires Approval (Workflow)

This policy type requires a user to provide a justification reason as to why they need to run a process (installer or executable). Then, the reason is submitted to specified managers via Privilege Manager **Tools > Manage Approvals** for approval. There are several pieces to the Actions in this policy.
Because **Conditions** and **Actions** are independent, these actions for approval can be applied to any condition. In this use case, we apply this action to the LICEcap gif creator.

First, create a filter that identifies the process/executable on which Privilege Manager will act.

1. Like Step 1 in the previous example, Navigate to **Dashboard** > **Filters**, then click **Add Filter**. In this use case, we target the LICEcap application (*LICEcap.exe*). Select **Windows** for your Platform, then **Blank Win32 Executable Filter**. Add **Name** and **Description**. Click **Create**.

2. Click **Edit** at the bottom of the page. Enter *LICEcap.exe* in the **File Name** field under File Specifications as well as in the **Original filename** field under File Details. Click **Save**.



Next, create a workflow policy to assign to this filter:

3. Navigate to **Home** > **Policies**, then click **Add New Policy**.

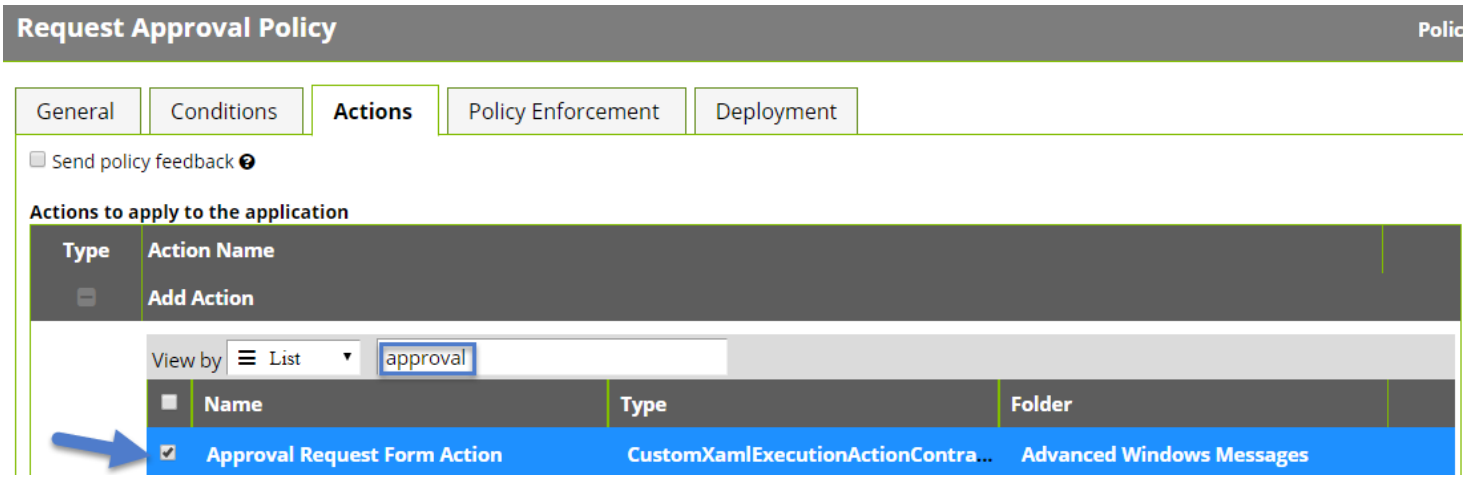
4. Select a platform, then **Show All Templates**. Select **Other: Empty Policy**. Name the policy **Request Approval Policy**, and add a description. Click **Create.**

5. **Edit**, and check the **Enabled** box.

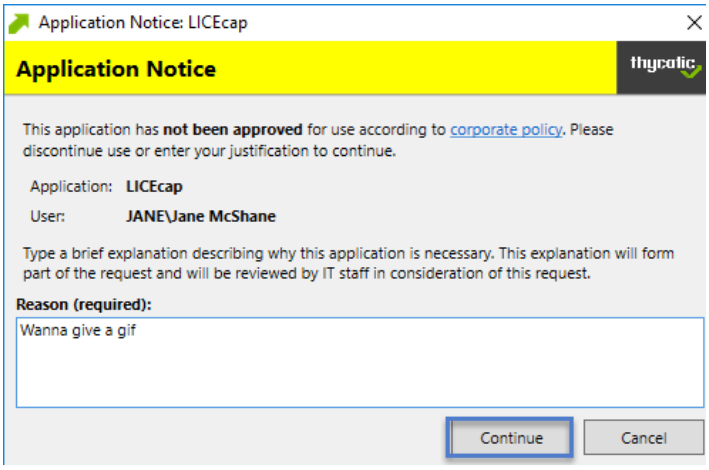
6. Select **Conditions**. Select **Add Application Target**. Search for the filter that is created in the previous steps (**LICEcap**). Select that filter and click **Add**.

7. Next, select the **Actions** tab.

Select **Add Action**. In the search field, type Approval, and locate **Approval Request Form Action**. Select this action and click **Add**.



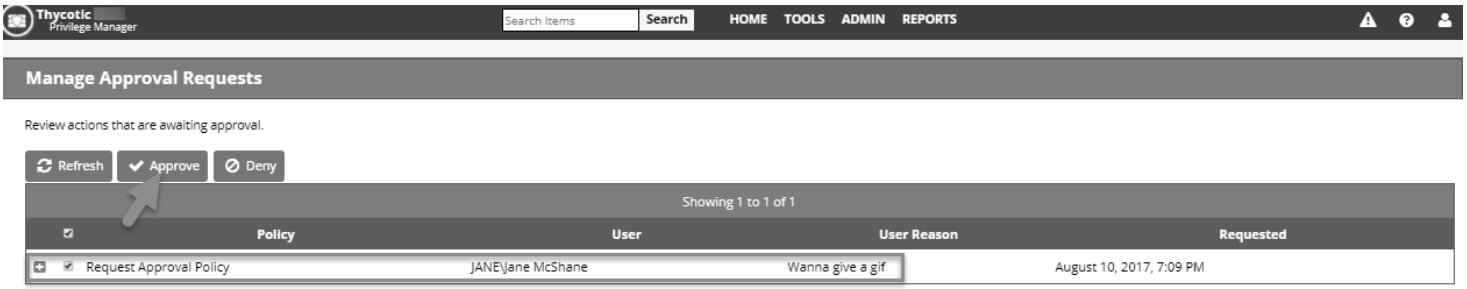
8. Click **Save**. This saves the policy to the policy list accessed from the Home screen – click **Policies** to view from the **Home** page. Once the policy is delivered to the endpoint agent *LICEcap.exe* requires the user to enter a justification reason for running this application:



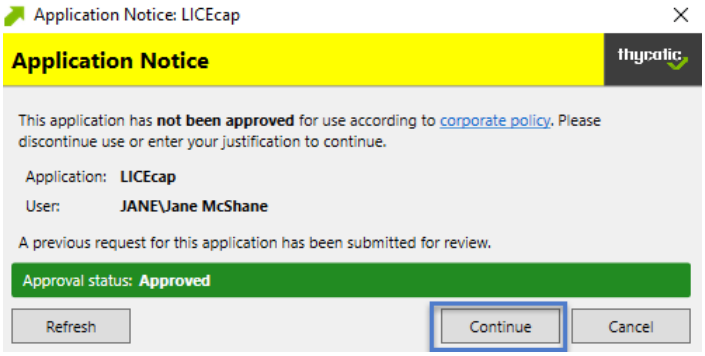
Once the reason is entered by the user, the user clicks **Continue** to forward to the request to Privilege Manager for approval. On their desktop, the Application Notice approval status is marked as **Pending.**

Finally, a privilege manager user approves this application request:

9. Return to the Privilege Manager Dashboard and navigate to **TOOLS** > **Manage Approvals**. Click the + left of the request to view the options for approval. Click **Approve**, then select One Time or an allotted time frame for access, and click **Approve**.



10. Now return to the desktop where the user initiated the executable, and you see the request has been approved. Click **Continue**, and the user is allowed to run that executable.



To adjust this policy to apply to specific users or endpoints, click the **Advanced Policy View** in the policy's General tab, then click the **Conditions** tab to add Inclusion/Exclusion filters and Computer Groups.

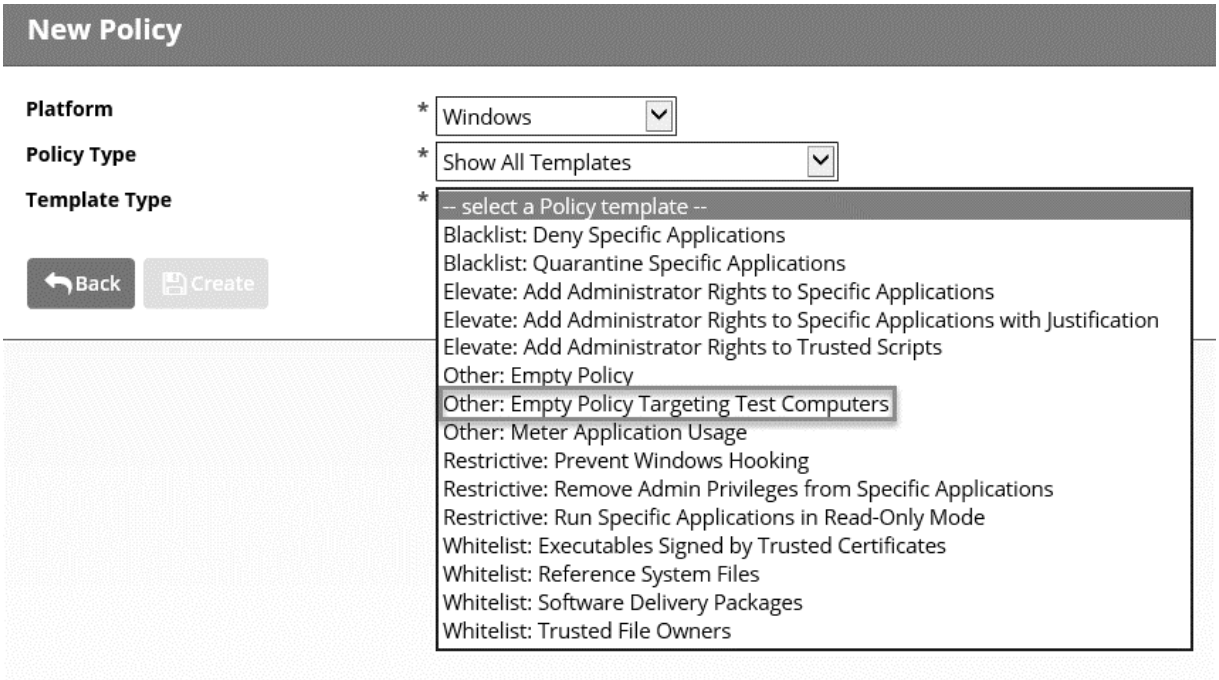
Greylisting Policies

Distinct from the policies that are already discussed is the category of Greylisting. Greylisting Policies apply to any unknown applications that attempt to run in your environment. It is important to discover unknown applications and determine whether to let them run or whether they are harmful. Greylisting provides a system for discovering the unknowns and adding an action that hinges on a reputation check.

Catch-All Policy

A useful **Learning Mode Policy** to set up in Production environments is called a Catch-All Policy. This type of policy gathers information on any executables in your environment that are not satisfied by other Privilege Manager policies.

1. Navigate to **Home** > New **Policy**, then select a platform
2. From **Policy Type** select **Show All Templates**
3. For POC and testing environments, Select **Other: Empty Policy Targeting Test Computers** from **Template Type** option

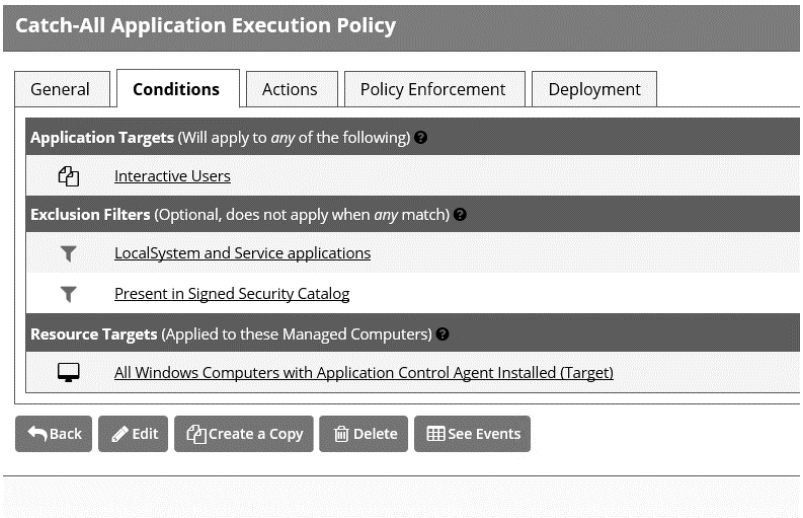


4. Name the policy **Catch-All Policy**, and add a description.

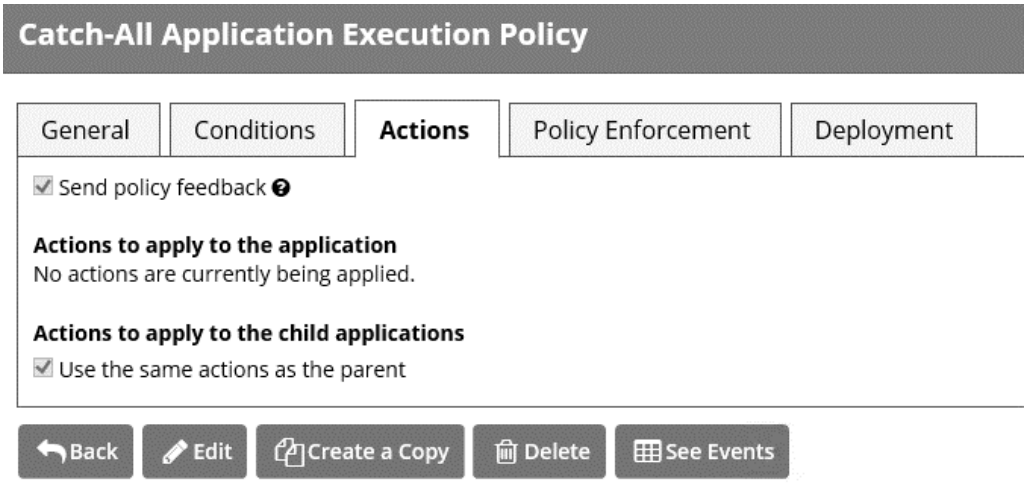
This policy catches all processes that are not caught by any defined policy above it. It should run at the highest policy priority (for example, 100).

5. Click **Create.**
6. To Enable this policy, you need to set up the Conditions, Actions, Policy Enforcement, and Deployment tabs. One version of a Catch-All Policy's settings are demonstrated by the following screen captures

Conditions:



Actions:



Policy Enforcement:

Reputation Checking Policies

Privilege Manager analyzes applications in real time. This unique feature allows for reputation analysis of any unknown applications that mitigate endpoint attacks from Ransomware, Zero-day attacks, Drive-by Downloads, and other unknown malicious software.

The greylist approach that is used here is that all applications that meet a general condition (for example, executed from a specific directory or directories) will be sent to VirusTotal for a reputation check. For this use case, we perform real-time reputation analysis of unknown applications by using VirusTotal.

First, you need to integrate Privilege Manager and VirusTotal by following the Integration steps that are listed in the Setting Up VirusTotal for Reputation Checking isss_gettingstarted.pdf section of this User Guide. That section walks you how to do the following:

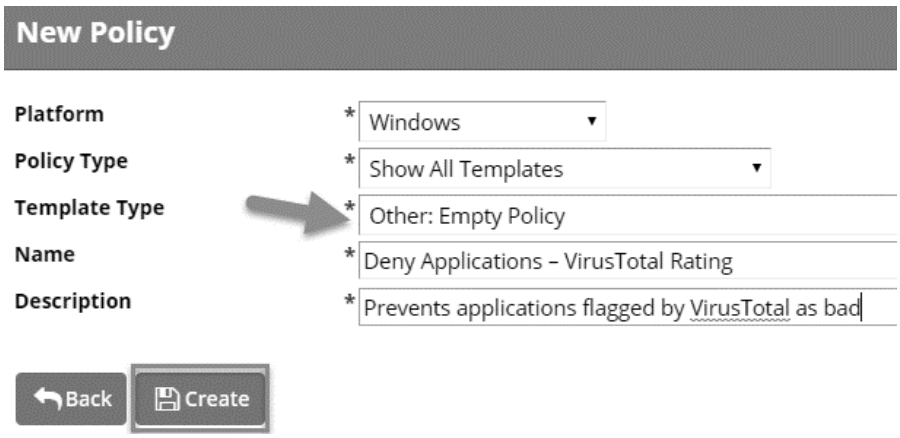
1. **Configure VirusTotal Ratings Provider**
2. **Install VirusTotal in Privilege Manager.**
3. **Create a Security Rating Filter for VirusTotal.**

Once the above steps are complete, follow these steps to create a Reputation Checking Policy:

1. After your Security Rating Filter for VirusTotal is created, Navigate to **Home** > **Policies**, then click **Add New Policy**.

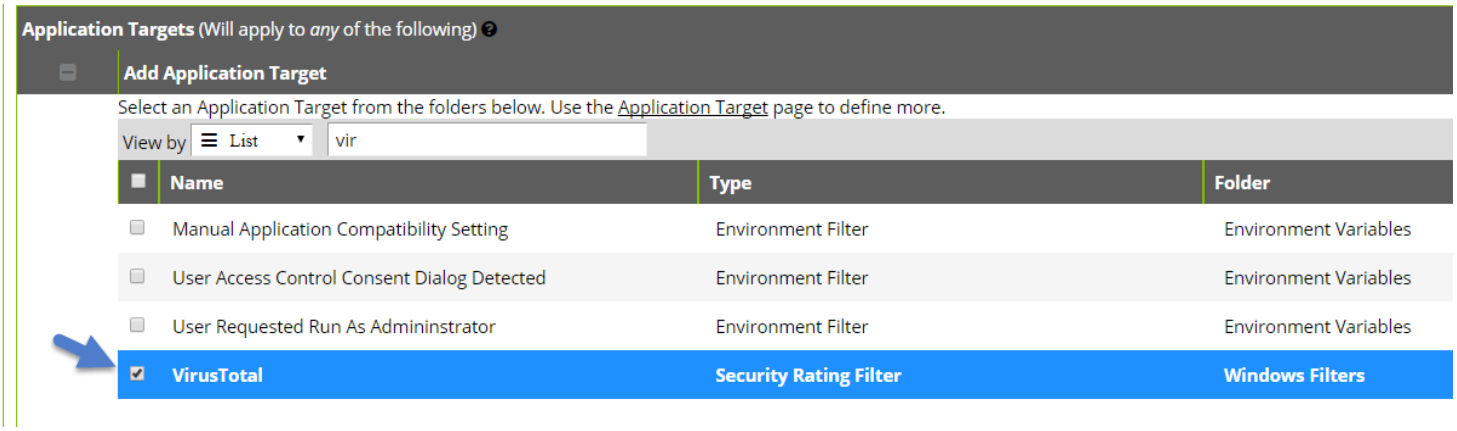
2. Select Windows as a Platform, **Show All Policies** as a Policy Type, then **Other: Empty Policy**.

Name the policy **Deny Applications – VirusTotal Rating**, and add a description **Prevents applications that are flagged by VirusTotal as bad**. Click **Create**.



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

Search for the filter that is created in the previous steps (VirusTotal). Select that filter and click **Add**.

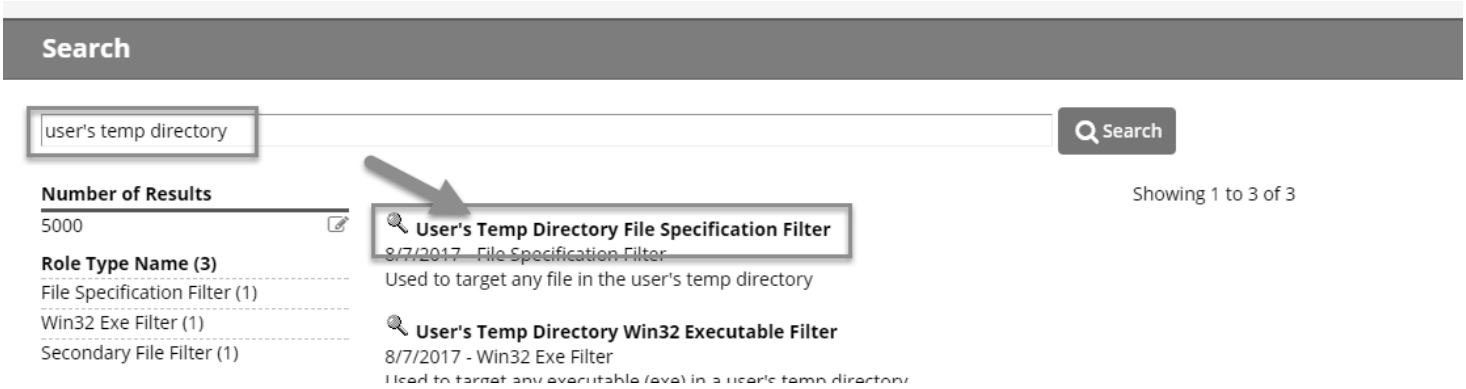


4. Next, select the **Actions** tab. Select **Add Action**. In the search field, type **Application Denied**, and locate **Application Denied Message Action**. Select this action and click **Add**.

This VirusTotal policy requires an extra step of creating a filter to be added as an Inclusion Filter under the Conditions tab. In this use case, we only want to send applications to VirusTotal for a reputation check that are in the user's Downloads and Temp directories.

Open another browser tab and open another Privilege Manager session so you can return to this policy in step 8 below.

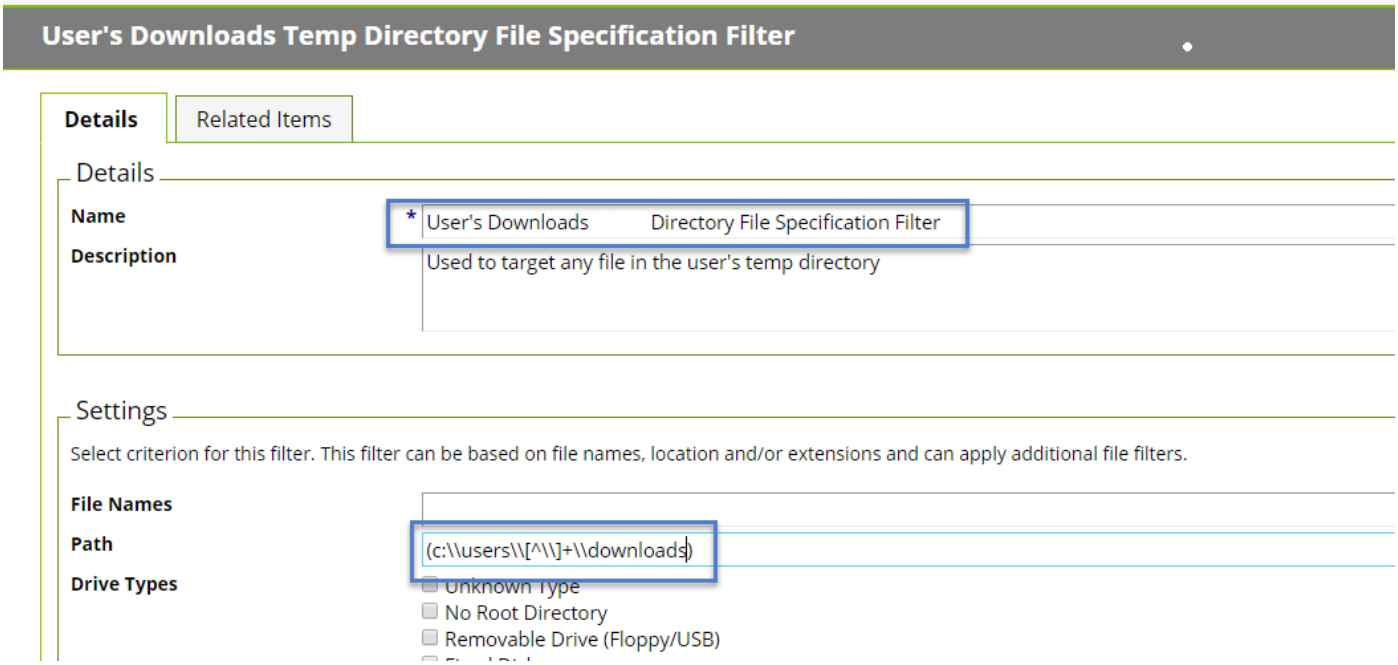
5. Start by searching for this policy in the Search Items that are filed at the top of the console page: **User's Temp Directory File Specification Filter**.



6. Select the filter **Users' Temp Directory File Specifications Filter**. Click **Create a Copy** at the bottom of the page. Name the new filter **User's Downloads Directory File Specification Filter**.

   Click **Create**.

7. Click **Edit**, and change the regular expression in the **Path** filed to the following: (c:\\users\\[^\\]+\\downloads). **Save** your changes.



Finally, combine the 2 filters into a single filter to target both directories:

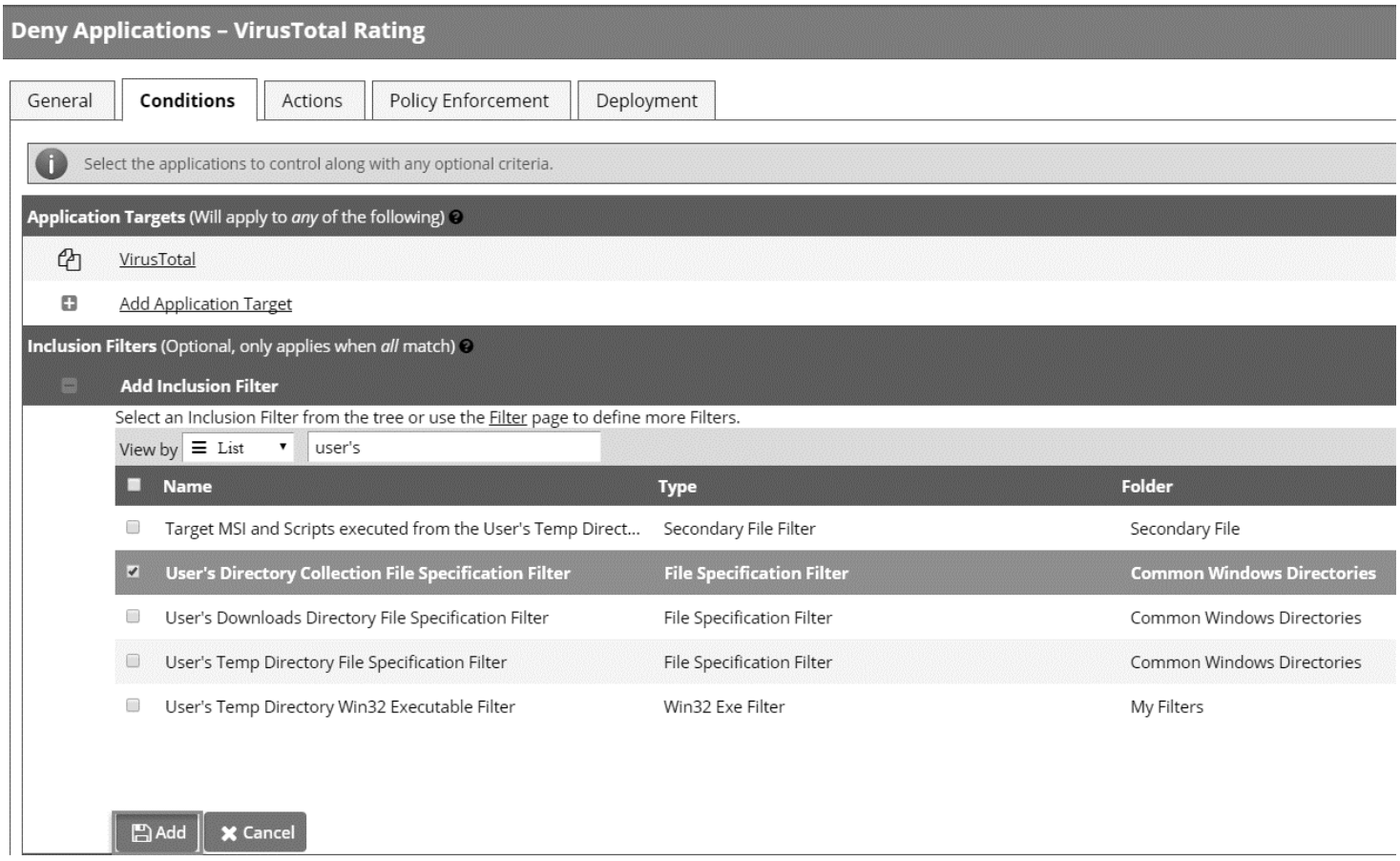
8. Click **Create a Copy** at the bottom of this filter's page, and name the new filter **User's Directory Collection File Specification Filter**. Click **Create**.
9. **Edit**, then **Clear** the entry in the **Path** field.

10. Click the **Add** button to the right of the **Include only filters** near the bottom of the page under Additional Filters (optional). Type User's to search for the filters that are identified and created in the previous steps:

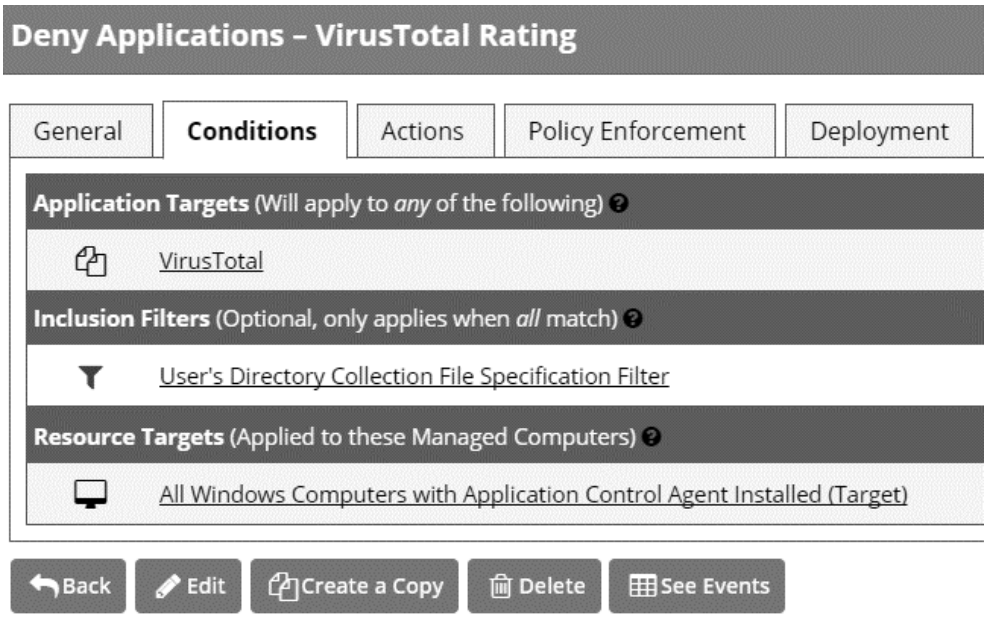
    - User's Downloads Directory File Specification Filter
    - User's Temp Directory File Specification Filter

    Click **Save**.

11. Now, add this new filter to the **Deny Applications – VirusTotal Rating** policy by clicking the Add Inclusion Filter under the **Conditions** tab.
12. Search for and add the filter just created named **User's Directory Collection File Specification Filter**. Click **Add**. **Save** changes.



To adjust this policy to apply to specific users or endpoints, click the **Advanced Policy View** in the policy's General tab, then click the **Conditions** tab to add Inclusion/Exclusion filters and Computer Groups.



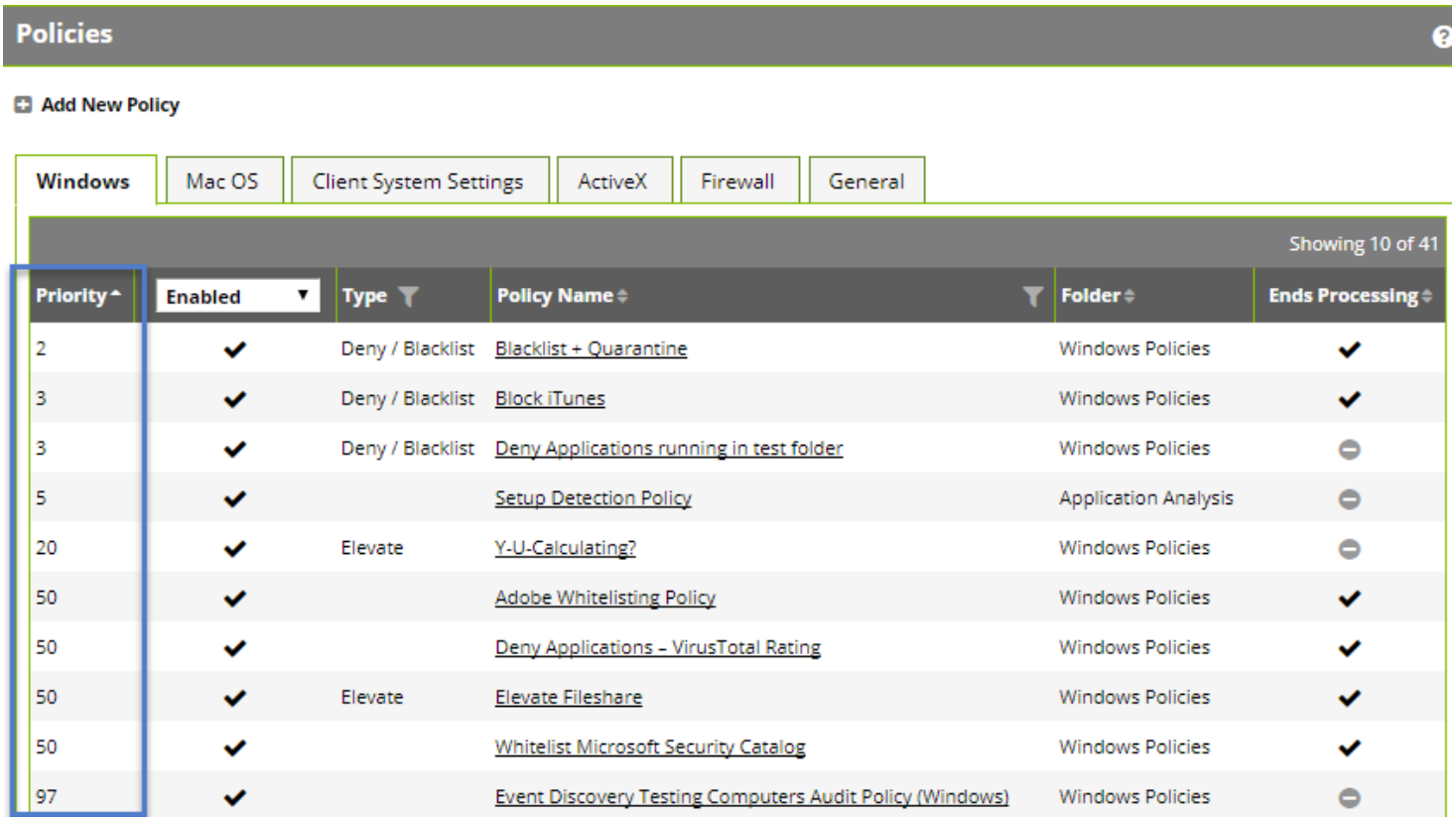
NOTE: This policy sends any application that is run from the user's Downloads or Temp directory to VirusTotal for a reputation check-in real time. If the application is graded with Bad from VirusTotal, the application will be denied.

To view a File Security Ratings report, from the main page go to **REPORTS** > **File Security Rating Details Report**. To see details of the applications in the report, click the file name in the **File** column.

Policy Priority

In Privilege Manager your Policies are evaluated in a certain order for each application that runs. It is important to have an awareness of all policies that are defined and the order in which they are called by the agent. If one policy blocks an application and ends execution before a second policy that was intended to elevate privileges, then only the block occurs.

The Policy Priority setting can be found on the **Policies** main screen in the left column. By default, policies are ordered according to their priority. You can edit this setting under the **General** tab after clicking into a policy.



Example: Why Policy Priority Matters

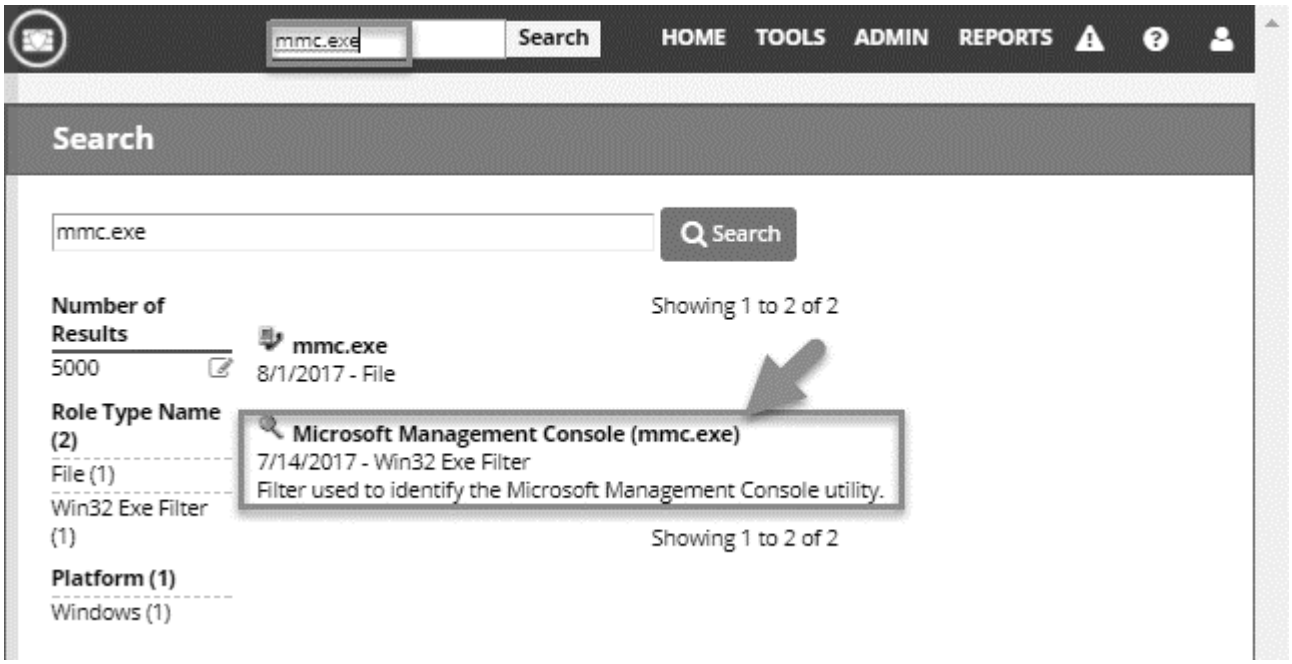
To illustrate the way policies are applied in order, this use case defines two policies to **1) block MMC.EXE**, but **2) allow a specific MMC Snap-in**.

Deny MMC.EXE Policy setup

First, we create a policy at a priority level of 50. This policy blocks the execution of MMC.EXE.

1. Privilege Manager provides a filter to identify the executable mmc.exe. This can be used in this policy to block mmc.exe.

Search for mmc.exe from the main screen search tool. Select the filter that is named **Microsoft Management Console (mmc.exe)**



Review how the Filter is set up. Note that both File Name and File Path parameters are used.

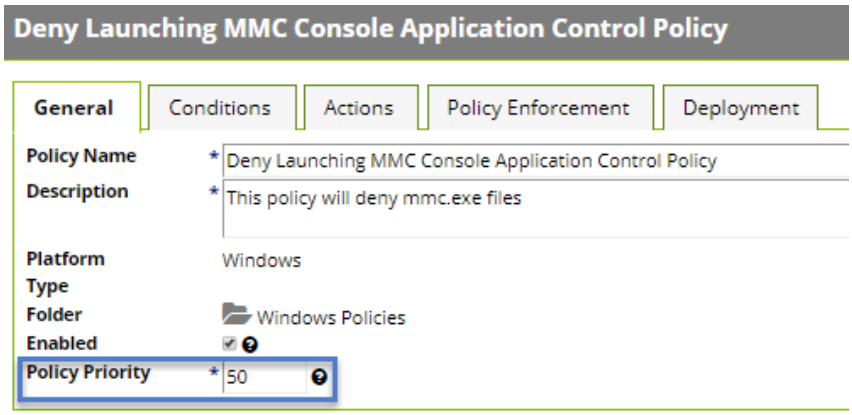
Next, create the deny mmc.exe policy.

2. From the home page, navigate to **ADMIN** > **Policies** > **Add New Policy**, Select Windows as a platform, **Show All Templates**, then **Other: Empty Policy** as the Template Type.

   Name the policy **Deny Launching MMC Console Application Control Policy**. Add a description. Click **Create**.

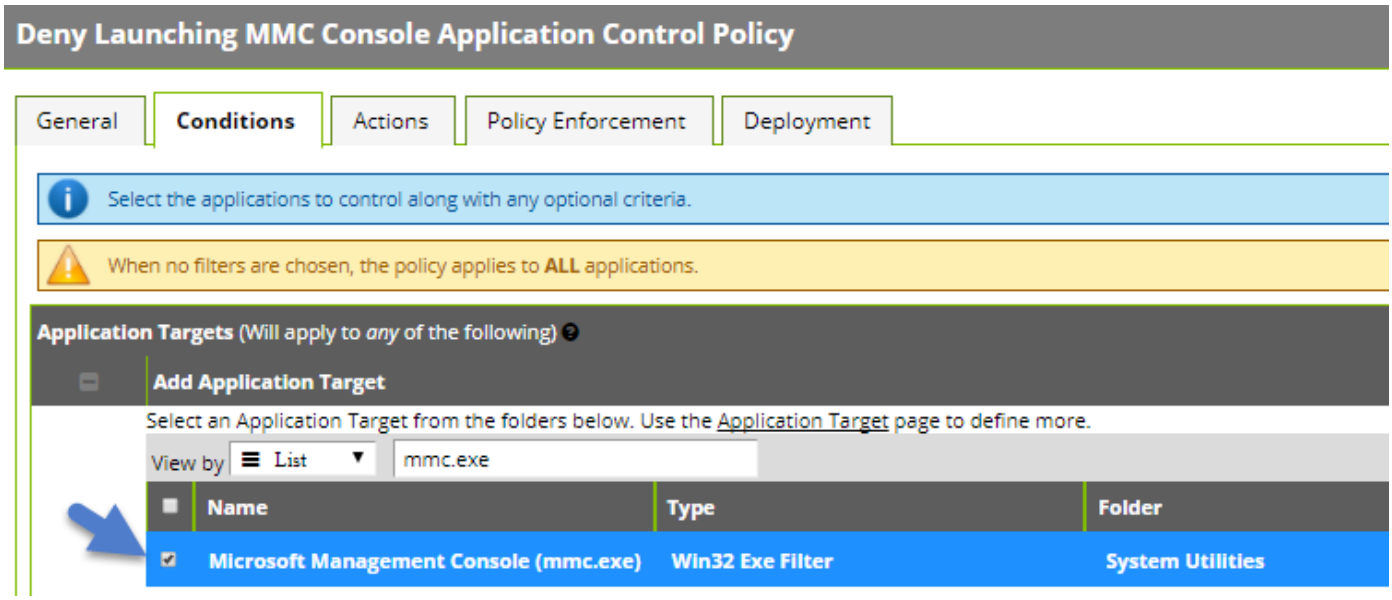
   Enable the policy by clicking the **Enabled** check box.

   Set the **Policy Priority** value to 50. (This level is not required, only defined for this use case.)

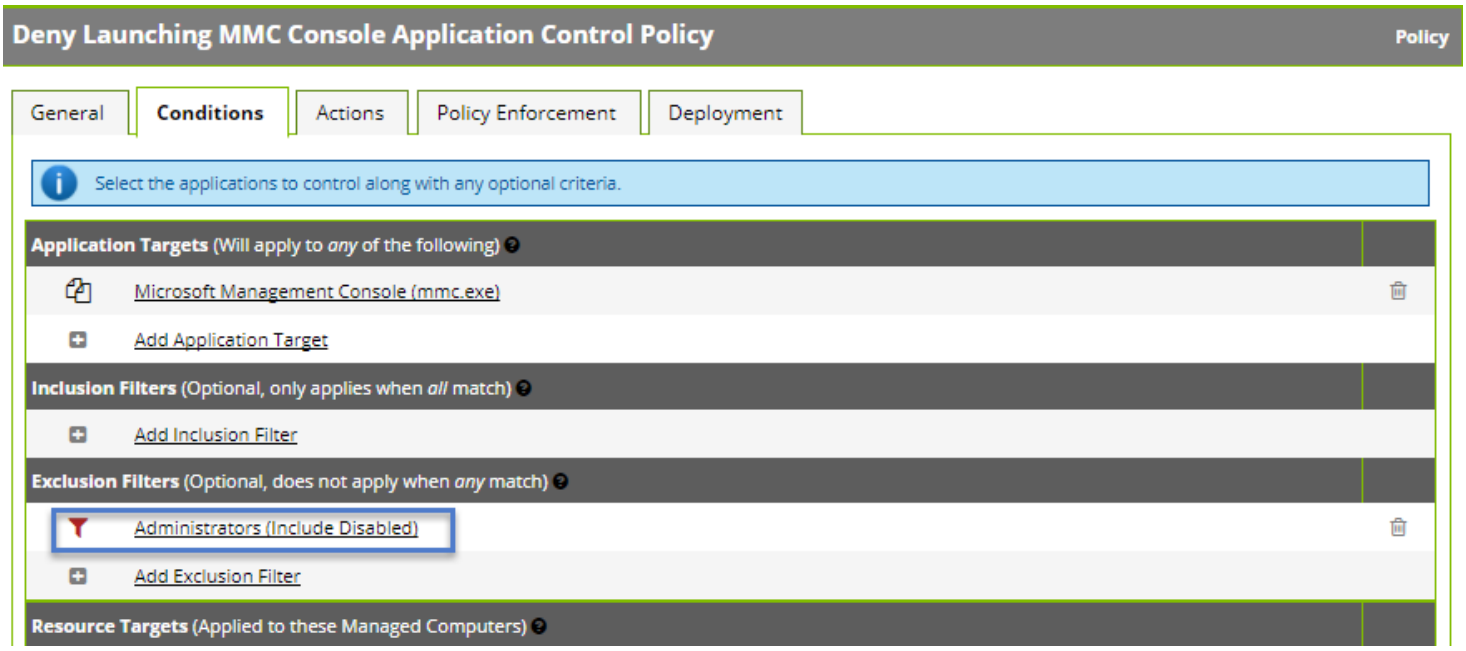


3. Click the **Conditions** tab.

Click **+ Add Application Target**. Search for the **MMC.EXE** filter that is mentioned above. Click **Add**.



4. You can also set an exception filter to not have this policy apply to Administrators. Search for and select the filer named **Administrators (Include Disabled)**. Click **Add**.

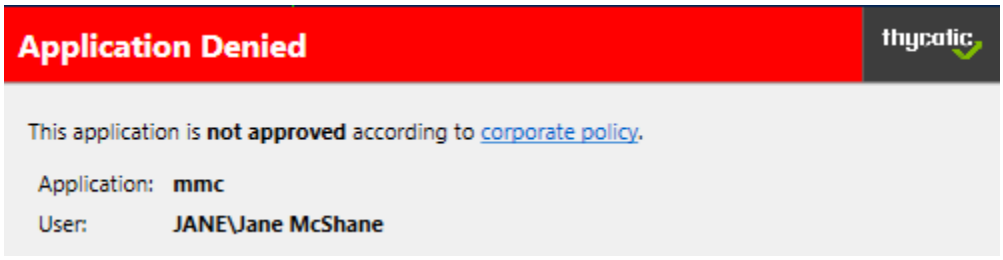


5. Click **Add Action** under the **Actions to apply to the application** section. Search for the **Application Denied Notification Action**. Click **Add**.

6. Click **Save**. This saves the policy to the policy list accessed from the Home screen – click **Policies** to view. Once the policy is delivered to the endpoint agent, mmc.exe will be denied execution for all users without administrator credentials on all target computers.

See details on how to deliver policies to the endpoint in the **Sending Policies to Endpoints** section.

7. Once the policy is delivered to the endpoint, test running mmc.exe to see the results.



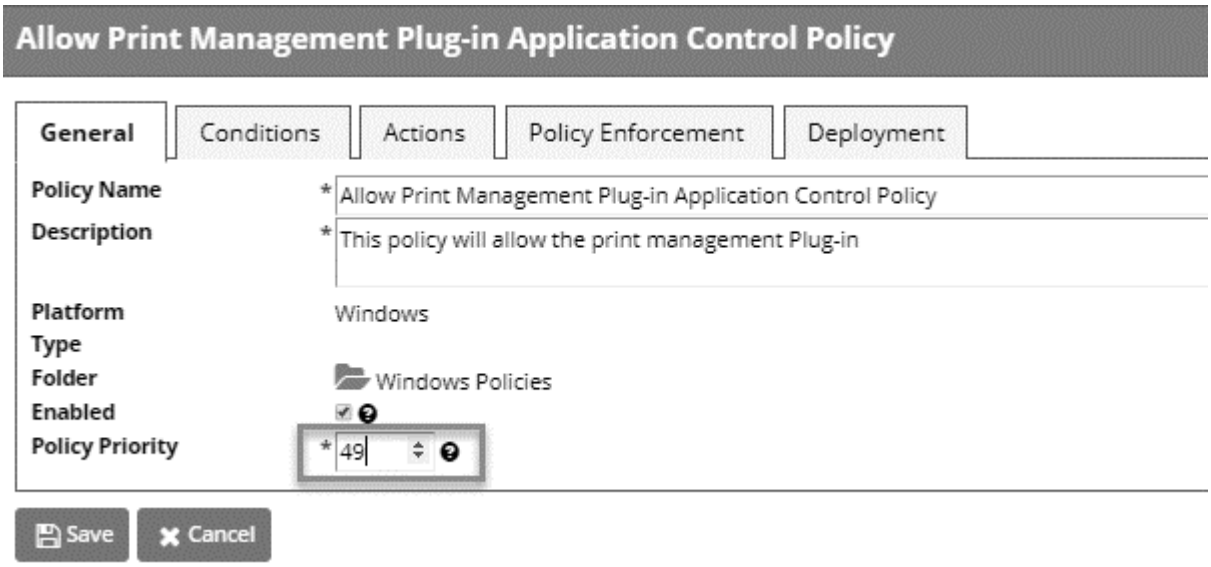
Allow specific MMC Snap-in

Next, we create a policy that has a priority of less than 50 and it allows specific MMC snap-ins. Having a priority less than 50 means this policy will be examined before the **Deny MMC Console Application Control Policy**.

8. As a short cut to this use case, start by making a copy of the policy we just created. Accomplish this on the General tab of the policy by clicking **Create a Copy**. Name the new policy **Allow Print Management Plug-in Application Control Policy**.

9. Enable the policy by clicking **Edit**, then the **Enabled** check box.

Set the Policy Priority value to ***less than 50***. (This level is not required, only defined for this use case.)



This means that this policy will be examined before the policy that blocks the mmc console. If the conditions are met, printmanagement.msc will run with elevation.

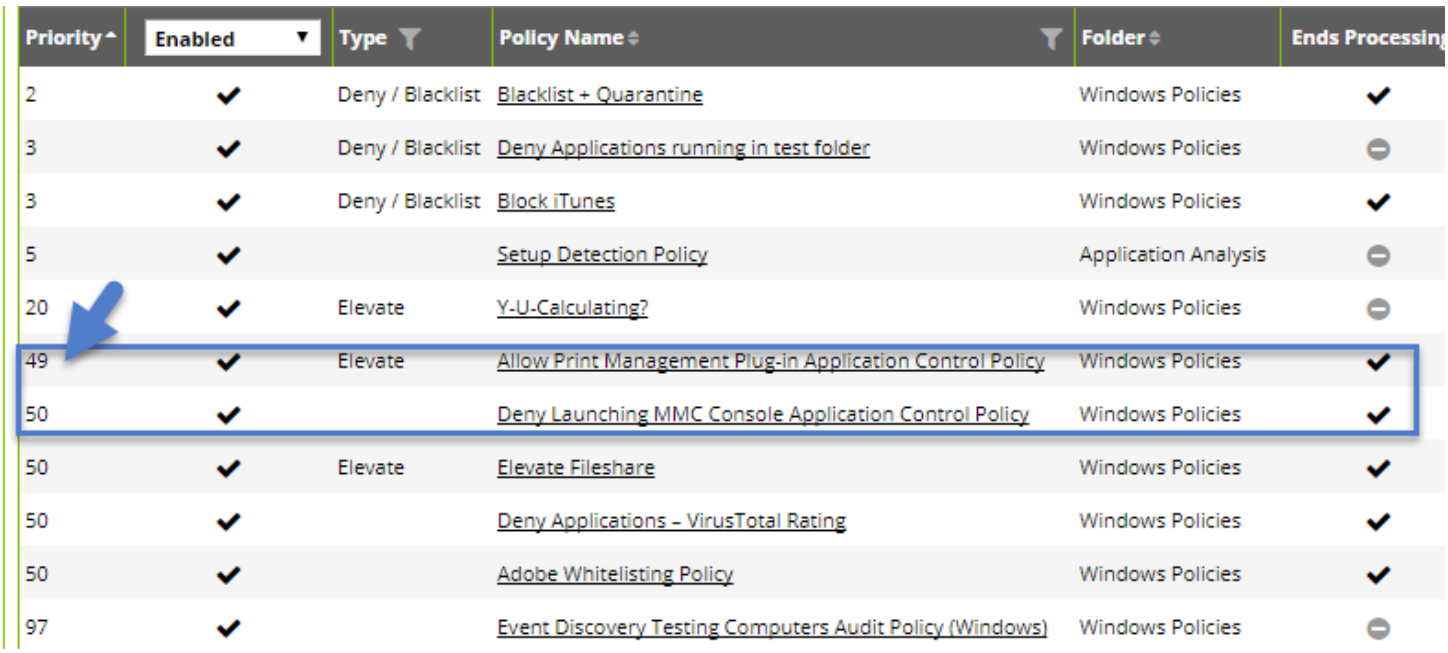
10. Click the **Conditions** tab. Do not remove the **Microsoft Management Console (mmc.exe)** filter under Application Targets.

11. Privilege Manager provides a filter to identify the MMC snap-in for Print Management. This can be used in this policy to elevate printmanagement.msc. Select **Add Inclusion Filter** and search for the **printmanagement.msc Commandline Filter**. Click **Add**, then **Save**.

    This filter identifies the mmc.exe file ONLY if the printmanagement.msc is run.

12. Click the Actions tab. Edit. Then, delete the existing Application Denied Notification Action by clicking **the trash can icon** on the right side. Click **Confirm Remove**.

13. Select **Add Action** under the **Actions to apply to the application** section. Search for and add **Add Administrative Rights** action. Click **Save**. You will now see your two policies in your Policies List:



Once this policy is delivered to the endpoint agent, printmanagement.msc will be elevated with administrative rights.

14. To test this use case:

    a. Run MMC.EXE from an endpoint where the user is not an administrator. This MMC.EXE execution is denied execution.

    b. Next, run printmanagement.msc from an endpoint where the user is not an administrator. This MMC snap-in will run with elevation.

However, if you change the **Policy Priority** of your "Allow Print Management Plug-in Application Control Policy" to be set at **Priority 51 rather than priority 49**, when you return to your endpoint and run printmanagement.msc, the application will be blocked despite your elevation policy. This is why it is crucial to keep the priority levels that are set for your policies in mind and adjust them to meet your intended system requirements.

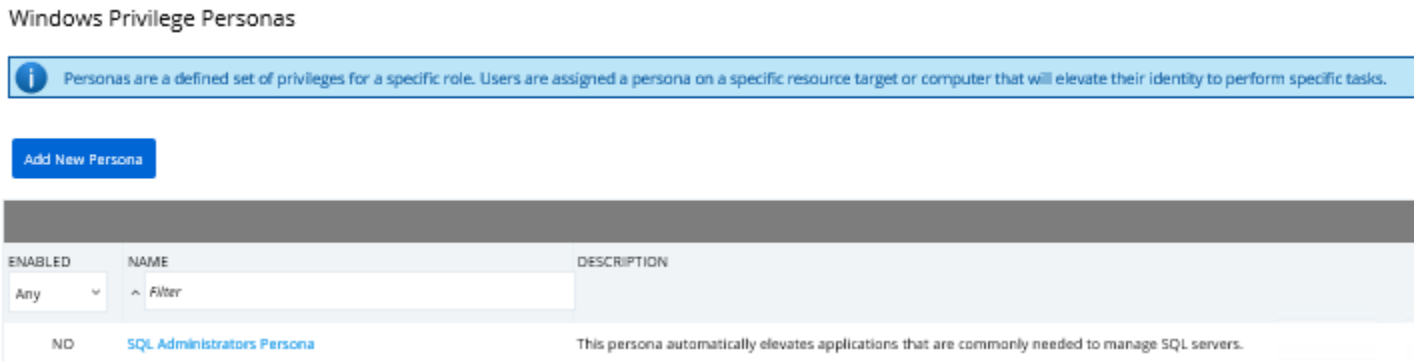
Personas

In Privilege Manager, Personas are collections of privileges for specific roles at an organization. You can assign Personas to users on a specific Computer Group to elevate their identity to perform specific tasks.

For example: A “SQL Administrator” Persona might be created that assigns rights to launch Certificate Manager and SQL Server Configuration Manager. Only users under this Persona would be allowed to run these applications on your network.

Viewing Your Personas

To see all your Personas, navigate to **Admin > Personas**. From the Windows Privilege Personas page, you can create new Personas and manage existing Personas.



Creating a Persona

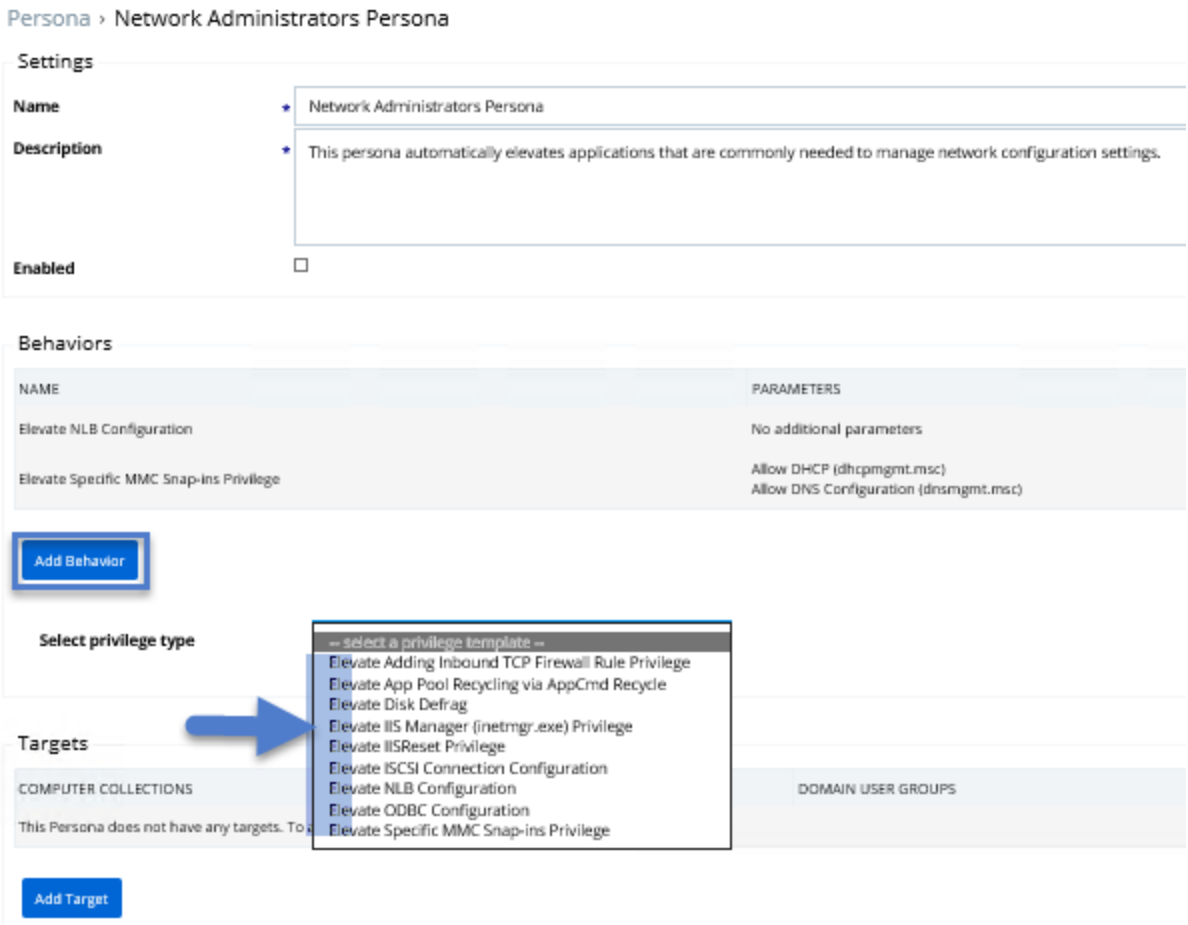
To create a Persona, click **Add New Persona** from the Personas page. You will be presented with a dropdown list of Persona Templates to choose from:

Custom Persona	Empty Persona
Network Administrators Persona	Elevate DHCP, DNS, and NLB Configuration
Security Administrators Persona	Elevate Local User and Groups and Group Policy Object Editor
SQL Administrators Persona	Elevate Certificate Manager, ODBC Configuration, and SQL Server Configuration Manager
Storage Administrators Persona	Elevate Disk Defrag, Disk Management, ISCSI Connection Configuration, Quota Management, Shared Folders, and Windows Backup

Web Administrators Persona	Elevate App Pool Recycling, Certificate Manager, IISReset, and adding TCP Firewall Rules

Select a Persona Template and then provide a Name and Description. Once you are ready to proceed, click **Create**.

If you selected any Persona Template other than Custom Persona, then you have pre-populated Behaviors that you can choose to delete or keep. Otherwise, you start with a blank Persona.



For Persona Settings, you can change the name, description, and whether the Persona will be enabled. For Persona Behaviors, you can click **Add Behavior** and choose which privilege you want to allow for this Persona. Finally, for Persona Targets you can choose which Active Directory Domain User Groups this Persona affects and on which Active Directory Organizational Units this Persona will apply.

Check the **Enabled** box and click **Save** to finish creating your Persona.

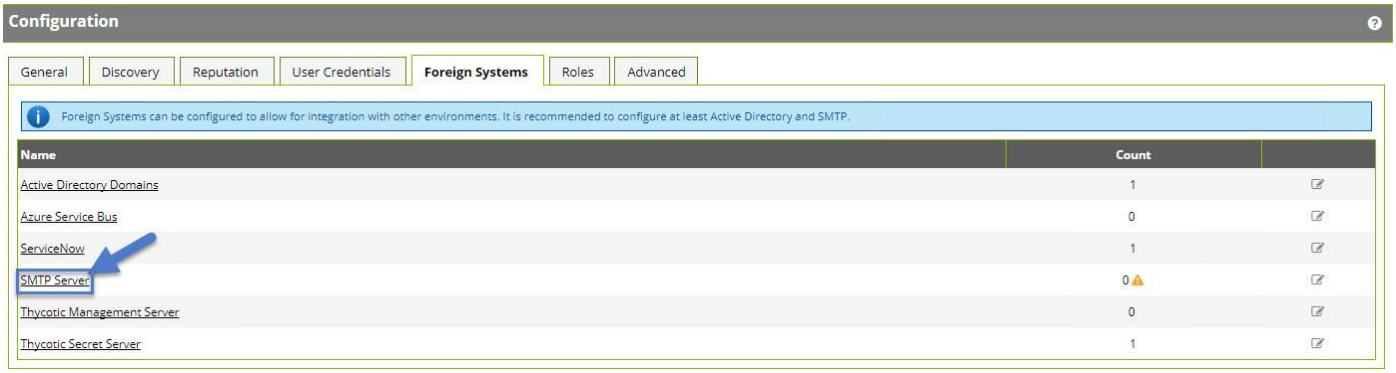
Integrations

Setting Up Email Server Connection (SMTP)

Simple Mail Transfer Protocol (SMTP) is the internet standard for email transmission. Often organizations use an SMTP Server—or a server that is specifically dedicated to transmitting email messages via TCP Port 25—and in order to send email alerts with Privilege Manager policies, you must ensure that your email server is connected to Privilege Manager.

To set up the connection, follow these steps:

1. Navigate to **Admin > Configuration > Foreign Systems** (tab)
2. Click **SMTP Server**, then **Add New.**



3. Add the **Name** of your SMTP Server and the **base Uri** (ex: smtp://[hostname];[port]), then **Create**

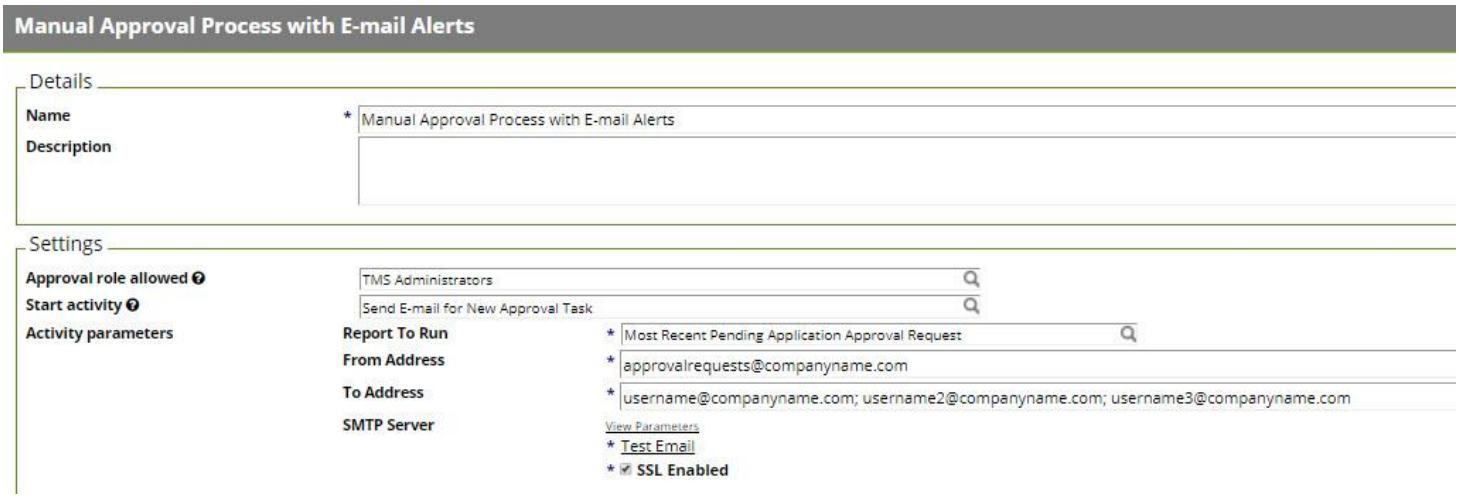
Next, in order to begin email alert notifications for a policy, you need to assign a Task for the job. This example sets up **Approval Requests with Email Alerts**,

Note: other types of email alerts can be created in **Admin > Tasks > Server Tasks > E-mail Tasks**, then **+Add New**.

To set up email alerts for Approval Requests:

1. Navigate to **Admin > Tasks > Automation tab**, then expand **Approvals** and select **Approval Processes**.
2. In the center section you will see options including **Manual Approval Process with E-mail Alerts** (If this option does not exist, click **Add New** to add it). Click this option and then **Edit**.

3. Enter the requested information. For the **Start Activity**, type **Send E-mail for New Approval Task**. For the **SMTP Server**, select the resource for the SMTP connection you created above. **Save**.



Setting Up VirusTotal for Reputation Checking

In order to perform real-time reputation checking for your greylisting policies,

"*VirusTotal aggregates many antivirus products and online scan engines to check for viruses that the user's own antivirus might have missed, or to verify against any false positives*.".

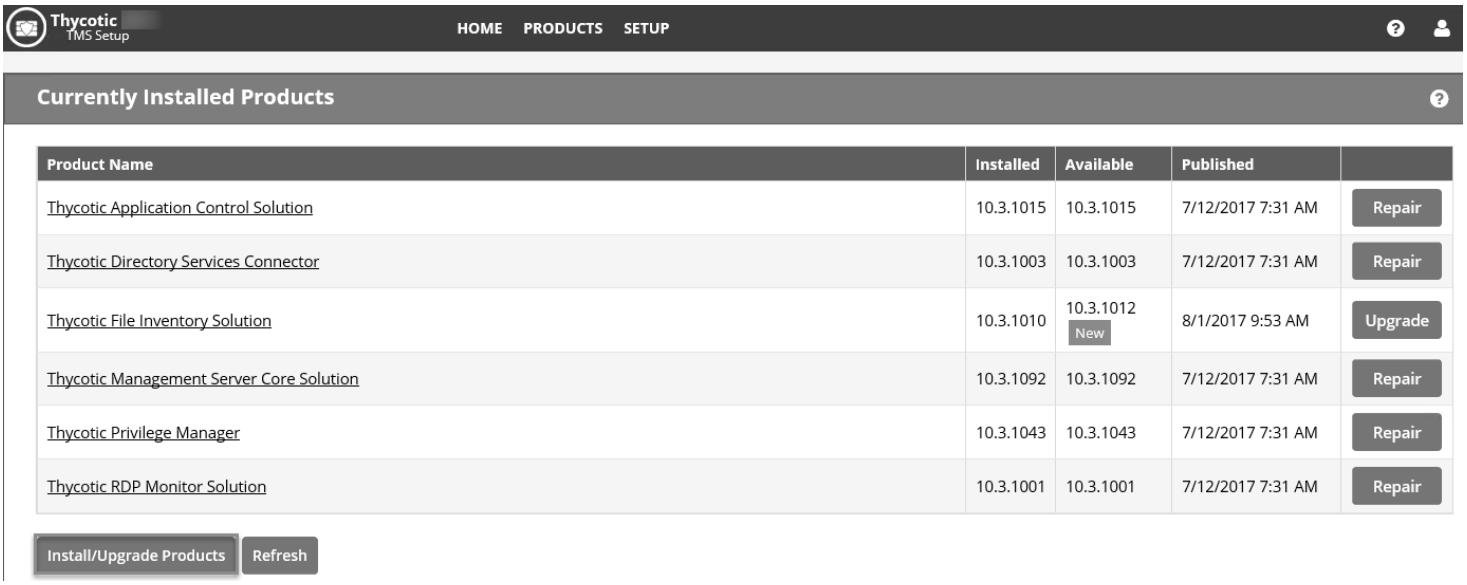
To use VirusTotal with Privilege Manager policies, signup at virustotal.com and secure an API key.

First, configure VirusTotal Ratings Provider:

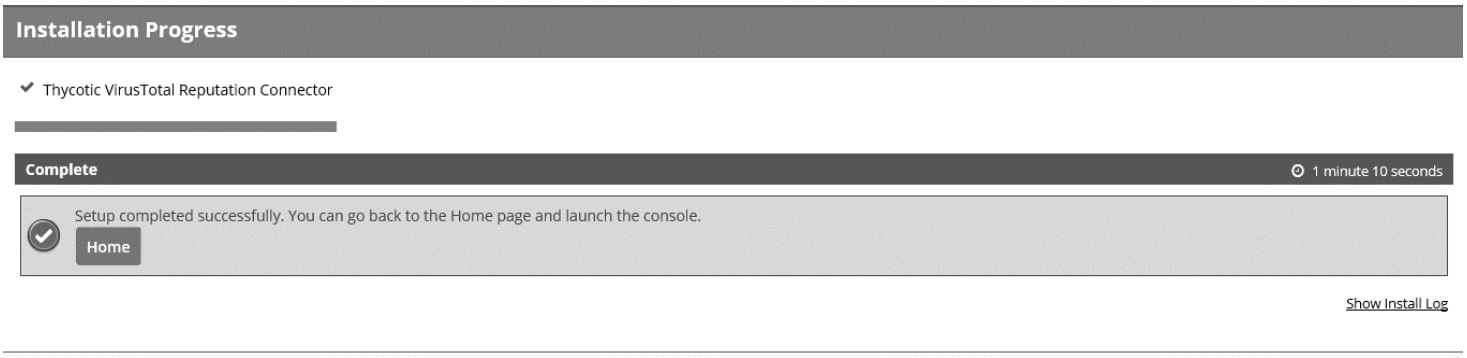
1. Sign up for a Free VirusTotal account at https://www.virustotal.com/ isss_gettingstarted.pdf , then sign in to VirusTotal and find your API key under your **Username > Settings > API Key**.

Second, Install VirusTotal in Privilege Manager. Note that you need outbound access on your server to install:

2. Open a browser on your Privilege Manager Web Server, browse to https://YourInstanceName/TMS/Setup/ isss_gettingstarted.pdf . On the Currently Installed Products screen, choose **Install/Upgrade Products**.

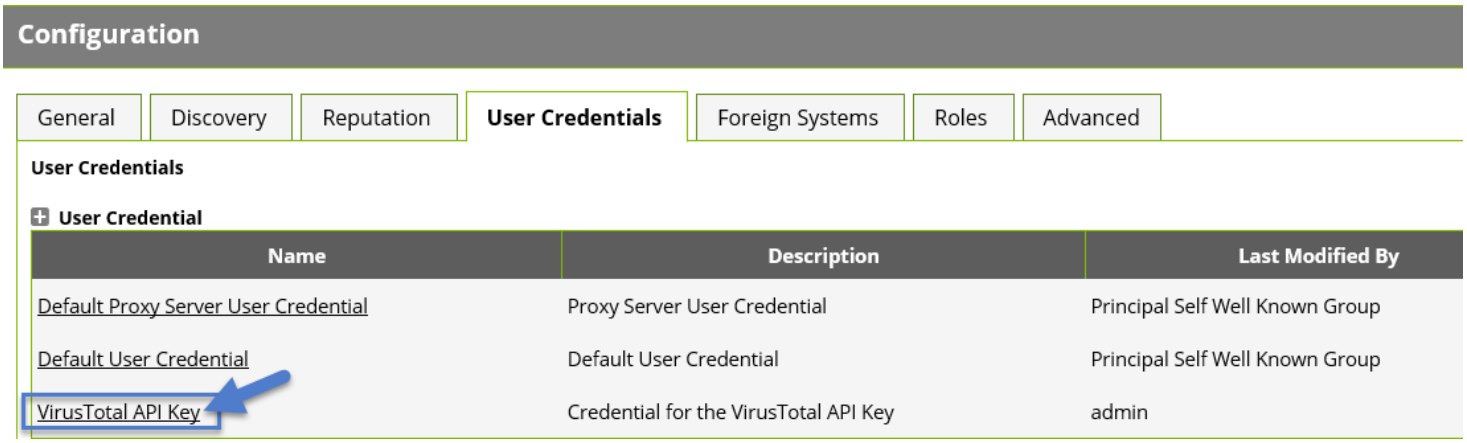


3. Check the VirusTotal Reputation Connector. Click **Install**. Then, **Accept** the End User License Agreement. You see your Installation Progress.

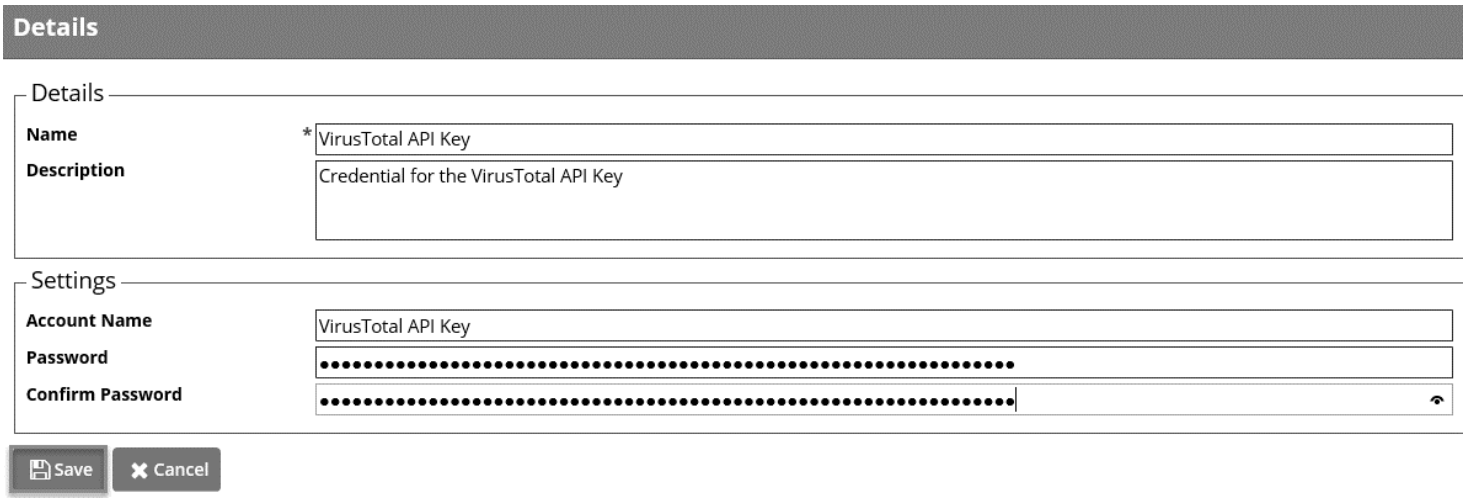


Troubleshooting: If the installation of VirusTotal initially fails, redirect to https://YourInstanceName/TMS/Setup/ and click the Repair button next to the VirusTotal Product.

4. Click the **Home** button. **Navigate to Products > Privilege Manager > Configuration > User Credentials**. Click the **+ User Credential** option, then **VirusTotal API Key**.

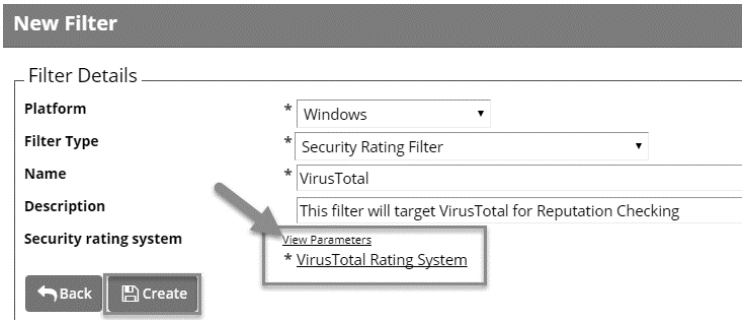


5. Click **Edit**. Set the Password to your **API key** provided by VirusTotal. **Save**.



Next, create a Security Rating Filter for VirusTotal:

6. Navigate to **Home > Filters**, the click **Add Filter**.
7. Select a platform, then **Security Rating Filter** as a Filter Type. Name the policy and add a description.
8. Next to Security Rating System, select **View Parameters** and then **VirusTotal as a Resource**. Click **Create.**



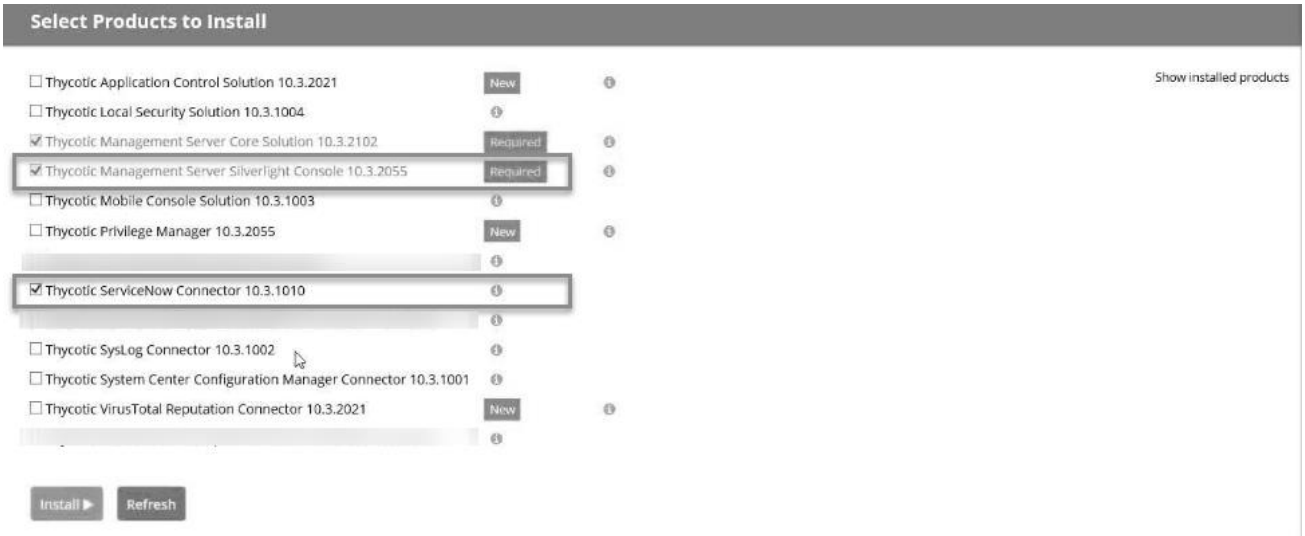
Setting Up ServiceNow Ticketing System

Many organization teams rely on their own ticketing systems like ServiceNow to facilitate workflow and approval requests. Follow the instructions below to set up a basic integration between Privilege Manager and ServiceNow. For more advanced tips on this process and how to tailor it to fit your environment see our Advanced ServiceNow Integration Guide here.

1. Verify **which ServiceNow User account you will use** for your integration with Privilege Manager. If you decide to create a new User account to manage your approval requests, make sure that it includes the roles: **Web Service Admin** and **Approval Admin**

2. Navigate to your Management Server Set up page at https://DomainName/TMS/Setup/ProductOptions/ShowProducts.

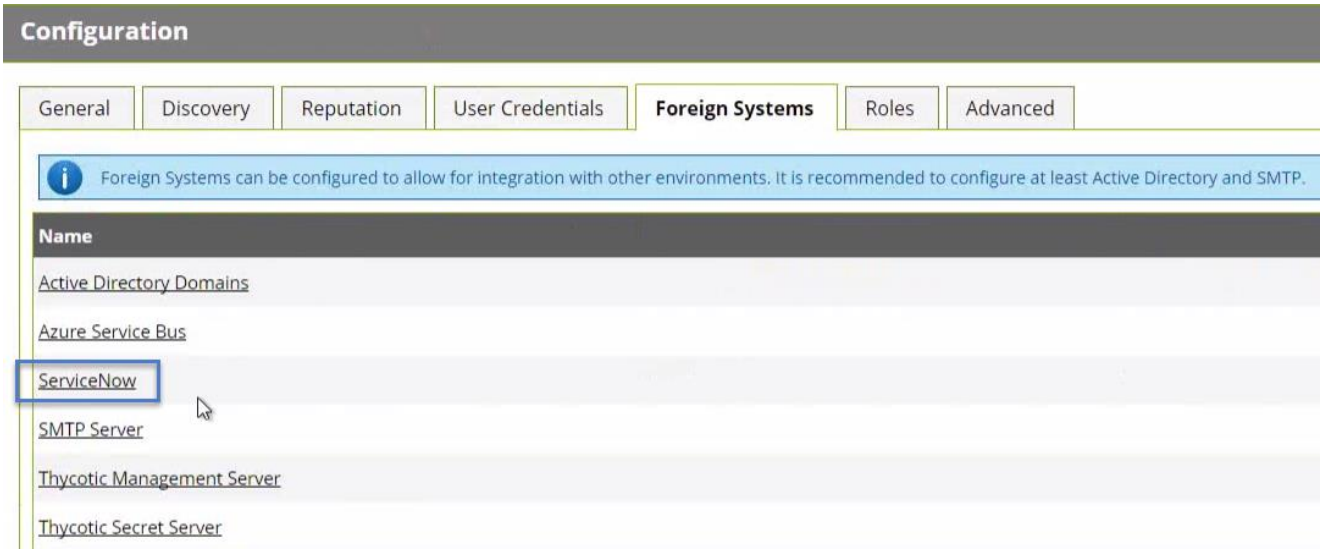
3. Install the **ServiceNow Connector** add-on and the **Management Server Silverlight Console**.

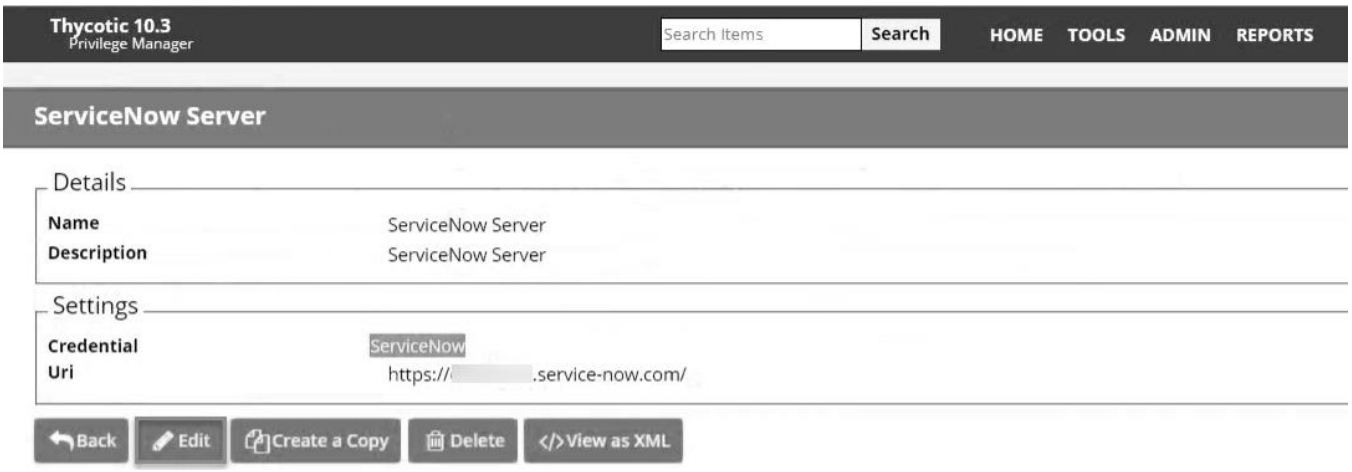


4. Navigate back to Privilege Manager's Dashboard (https://DomainName/TMS/PrivilegeManager) and then **Admin > Configuration > User Credentials** tab.

5. Create a new User Credential by clicking the **+User Credential** icon above the table, click into your New User Credential and **Edit** the **Name** (ServiceNow) and add a **Description**. Under Settings, provide the ServiceNow **Account Name** and **Password** that you use to run this integration and Approval Management (Step 1). Click **Save**, then **Back**.

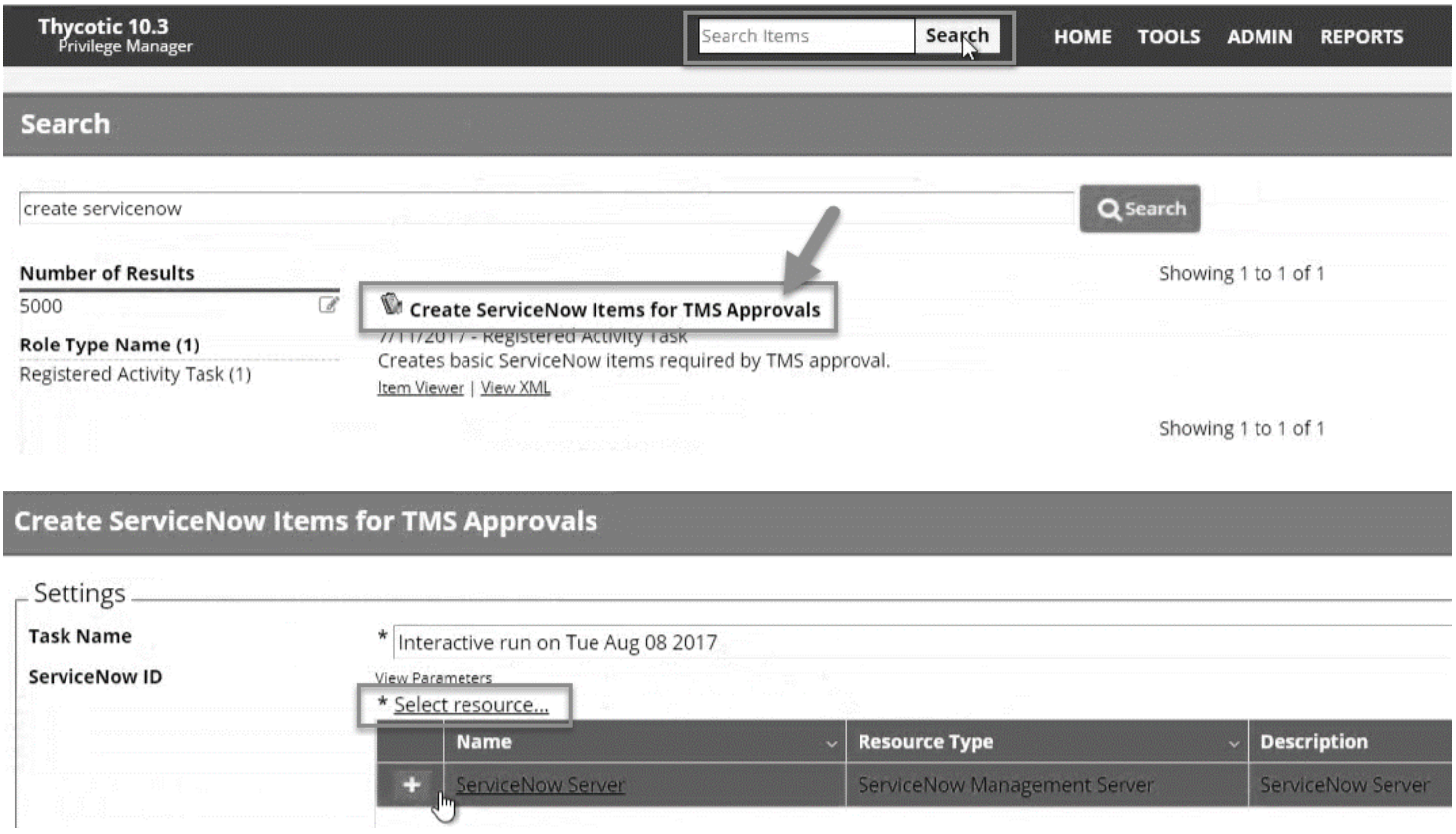
6. Next, under Configuration select the **Foreign Systems** tab. Click **ServiceNow**, then **Add New.** Add a **Name** (ServiceNow Server) and the **Base Uri** from your ServiceNow instance. Click **Create**.



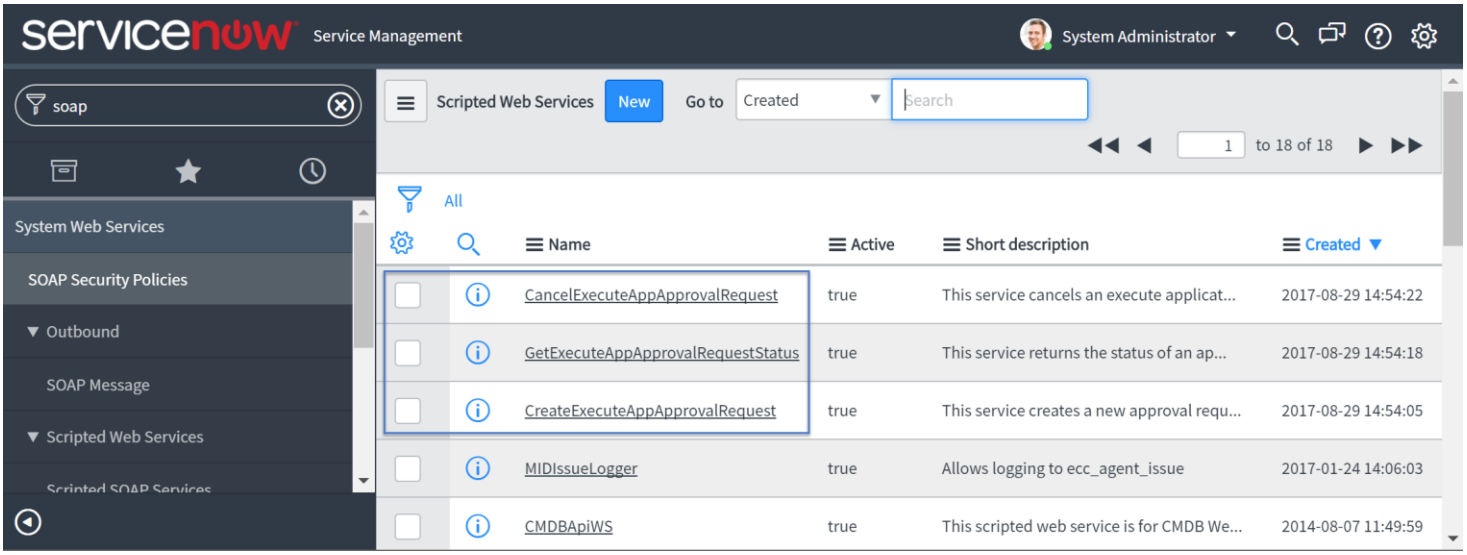


7. Next, in the Search Bar at the top of your Privilege Manager screen, search for "**Create ServiceNow Approval Request Items**" In your search results, click this task and then the **Run Task** button. Under Task Settings, click **Select resource** and add the ServiceNow Server that you created as a Foreign System in step 6. Then click **Run Task**.

Note: Clients with robust ServiceNow installations are welcome (and in fact encouraged) to alter their ServiceNow scripted web services for use with their own ServiceNow items and workflow rather than relying on this importing task. For more information on this, see our Advanced ServiceNow Integration Guide here.



8. The task you just ran creates several new items in your ServiceNow dashboard. Open **ServiceNow** and navigate to **Scripted Web Services > Scripted SOAP Services** to verify that these three new options are listed:
   1) **CancelExecuteAppApprovalRequest**,
   2) **CreateExecuteAppApprovalRequest**,
   3) **GetExecuteAppApprovalRequestStatus**



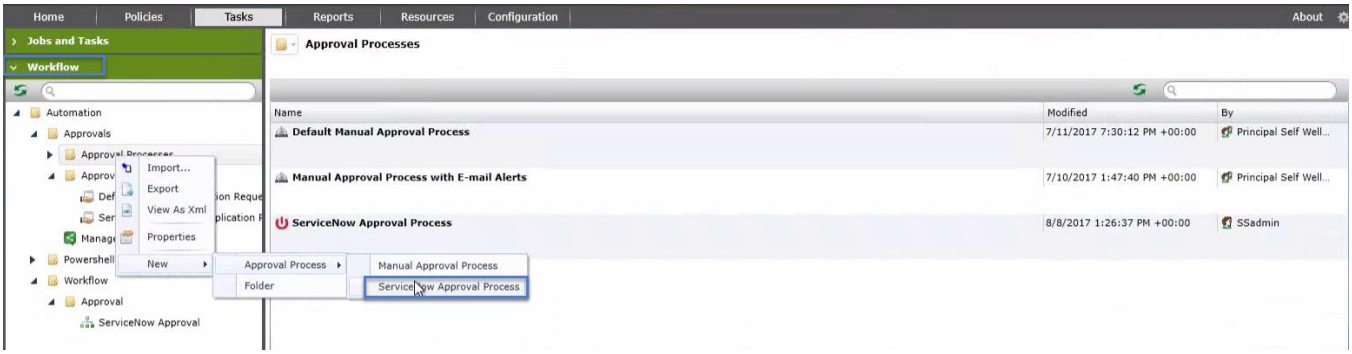
Now that you have successfully defined a SOAP endpoint that Privilege Manager knows how to call to initiate a ServiceNow request for approval.

Next, navigate to the **Management Server Silverlight Console** (installed in step 3):

9. Open an Internet Explorer Browser (not Edge) Go to https://DomainName/TMS/Setup and click **Security Manager Console**. If this is your first time opening Silverlight, you might need to follow the download prompt to install.

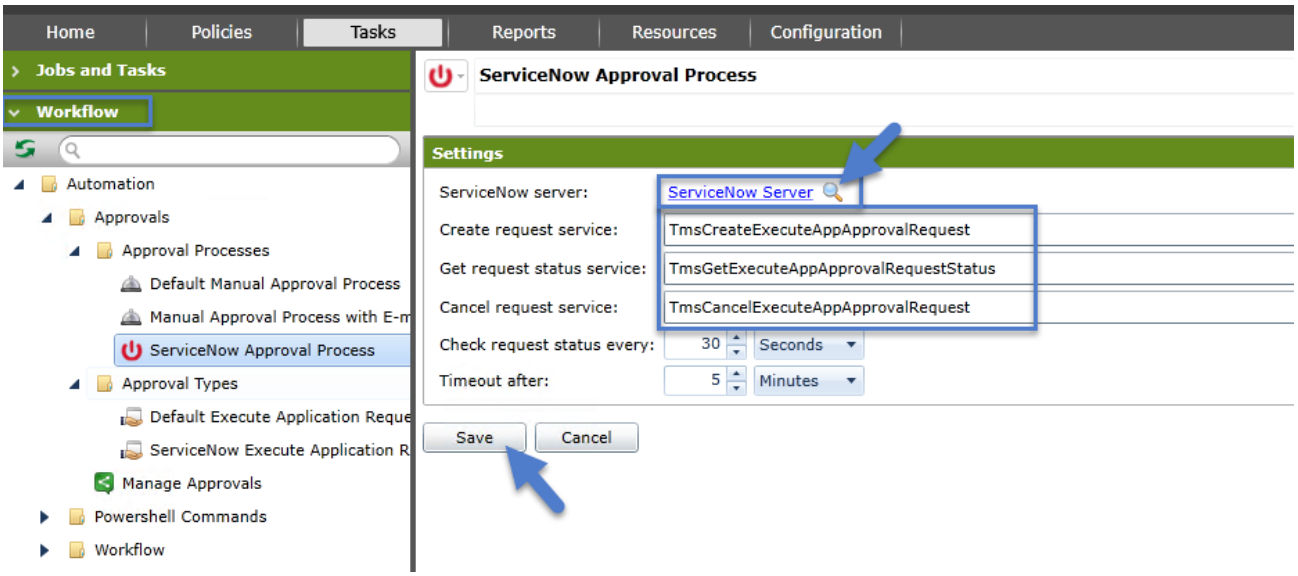
In the Silverlight Console you will first create a new **ServiceNow Approval Process**.

10. Click the **Tasks** tab, scroll to find Workflow in the left window, and expand the window. Navigate to **Automation > Approvals**, right click **Approval Processes**, then **New > Approval Process > ServiceNow Approval Process.**
    Your ServiceNow Approval Process will now appear under Approval Processes.



11. Click this process.

12. Next, click the **search icon** and select the name of your **ServiceNow Server** that you created in step 6.



13. Click **Request Item** and search for **Execute Application Workflow,** select this. It might take a few minutes to load.

14. Next to **Create request service**, type **CreateExecuteAppApprovalRequest**
    Next to **Get request status service**, type **GetExecuteAppApprovalRequestStatus**
    Next to **Cancel request service**, type **CancelExecuteAppApprovalRequest**

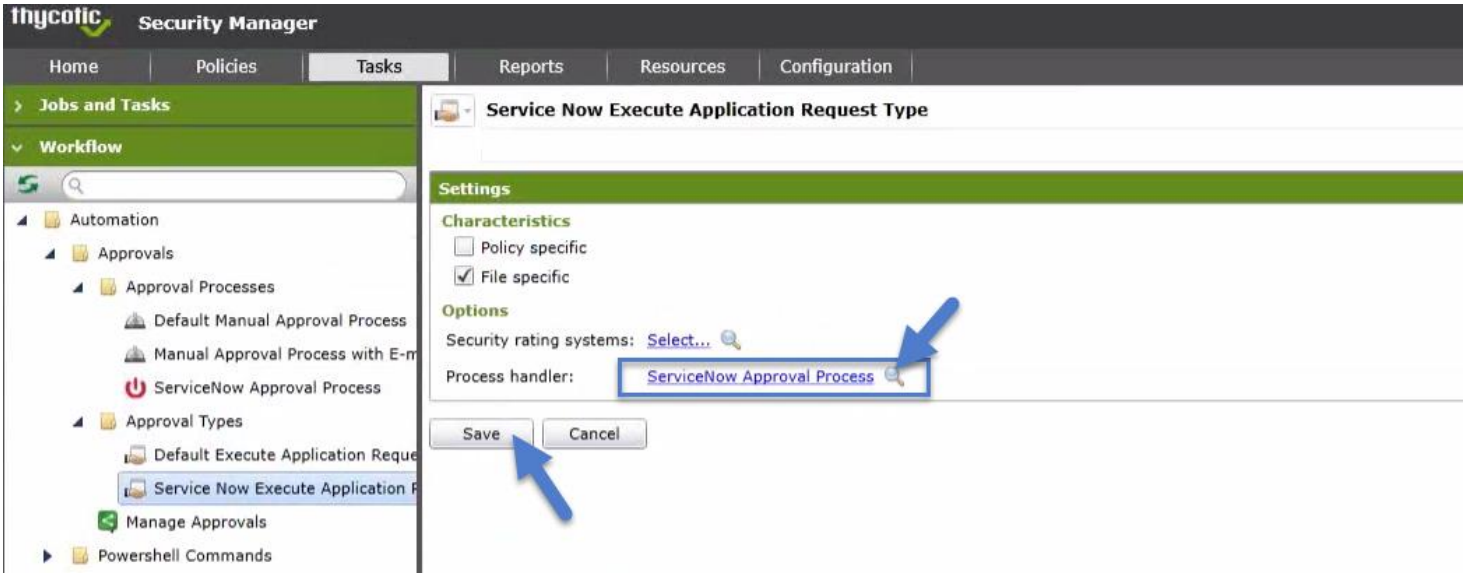
    Note that the names of these services must be the same in Privilege Manager and ServiceNow or the integration will break. Click **Save**.

Now, still under **Workflow** in your Silverlight **Tasks** tab,

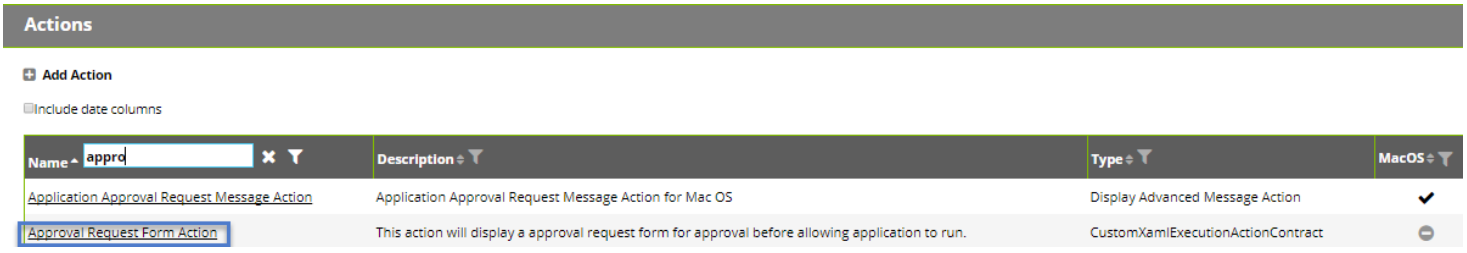
15. Navigate to **Automation > Approvals**, right click on **Approval Types** and then **New > Execute Application Approval Request**

16. Click **Service Now Execute Application Process** under **Approval Types.**

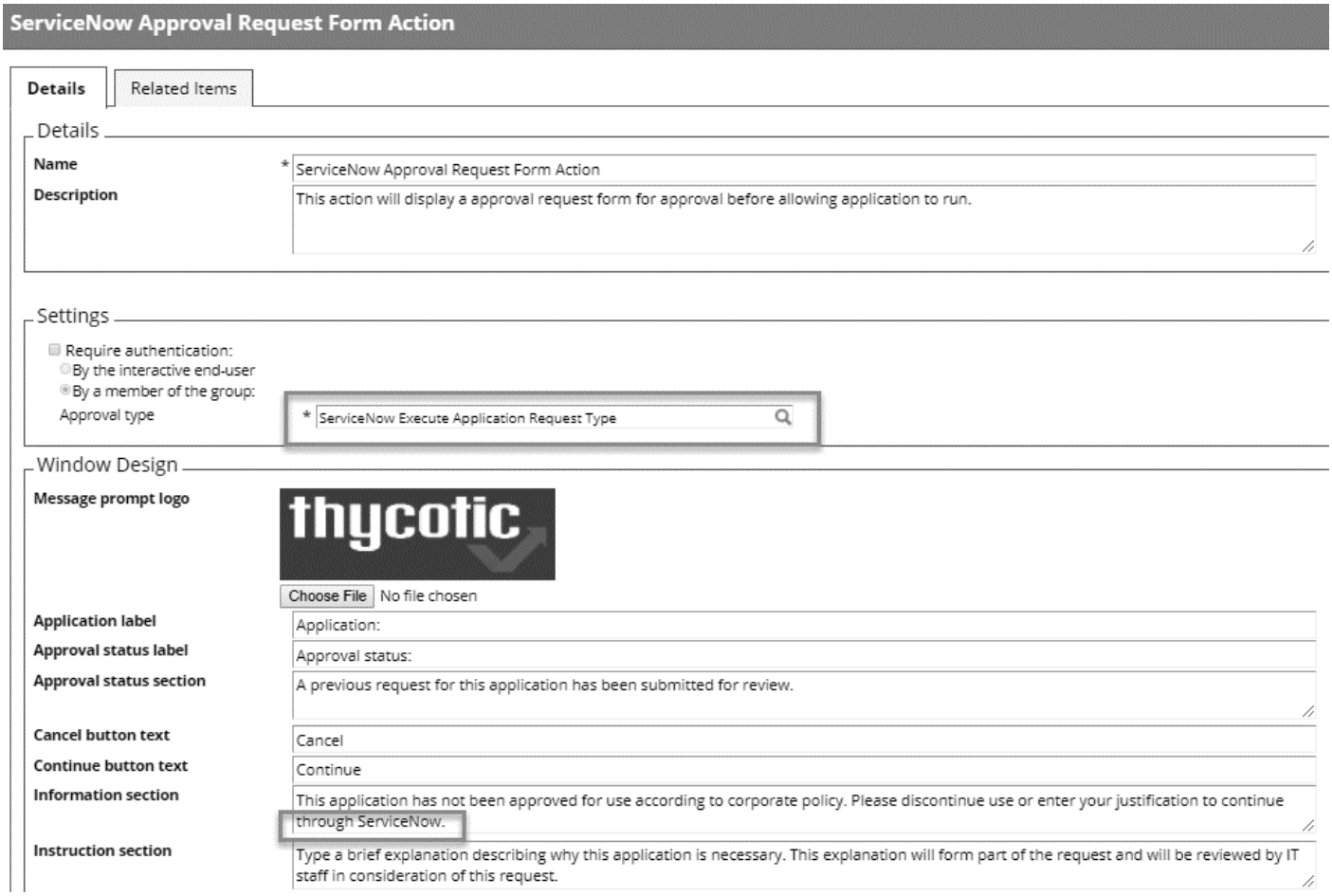
17. Select the **ServiceNow Approval Process** as your **Process Handler**. Click **Save**.



Lastly, you must **create an action and attach it to a policy** to manage what events you want sent to ServiceNow for approvals. To do this, navigate back to Privilege Manager (https://DomainName/TMS/PrivilegeManager):



18. In the Privilege Manager Dashboard, go to **Admin > Actions**. Search for **Approval Request Form Action**, click this, then **Create a Copy**.



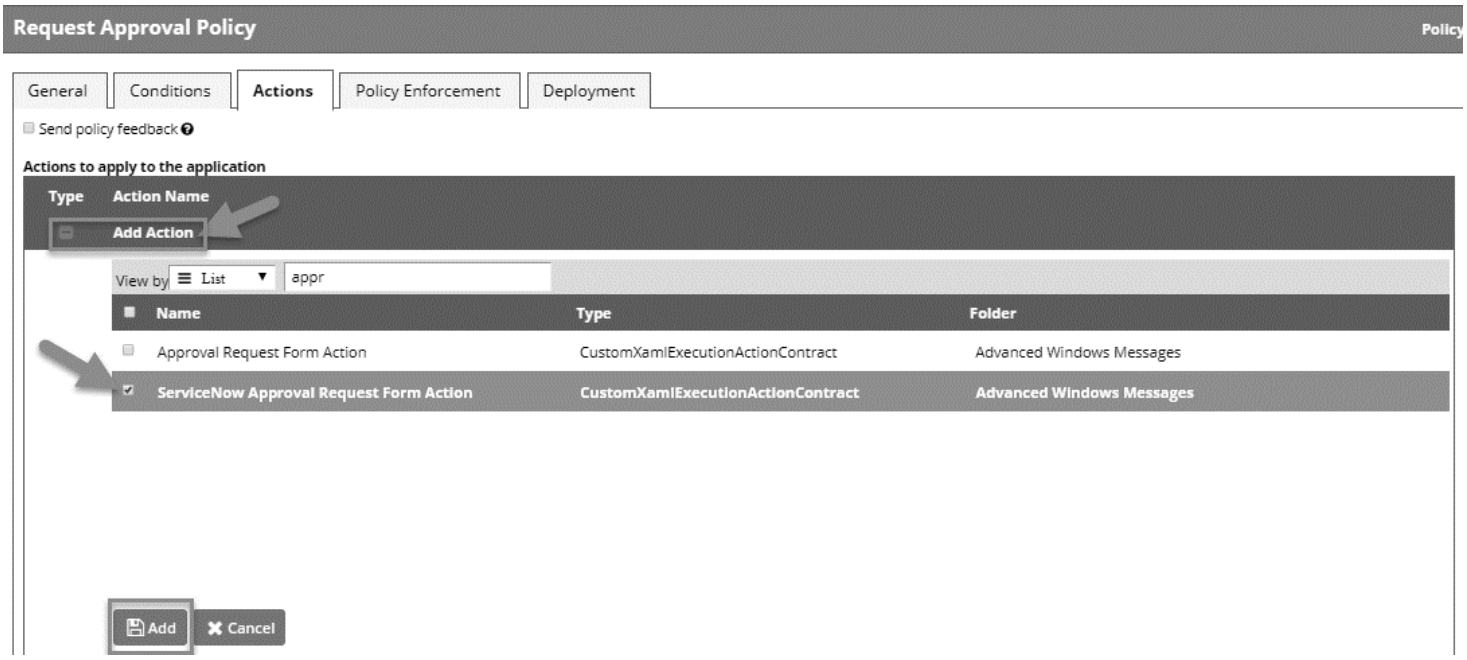
19. **Name** your new Action (ServiceNow Approval Request Form Action).

20. Click **Edit**. Next to Approval Type, search for **ServiceNow Execute Application Request Type**.

    You can also customize your Window Design and the **information Section** to specify "This application has not been approved for use according to corporate policy. Discontinue use or enter your justification **to continue through ServiceNow**," if desired. Click **Save**.

21. Next, navigate to **Policies > Create New** or find an existing policy that you want to use for ServiceNow Approvals.
    *If you need help creating a new policy, see the Privilege Manager User Guide.

22. On the Policy's detail view under the Actions tab, click **Edit** and **Add Action**. Search for the action you created (**ServiceNow Approval Request Form Action**). Click **Add**, then **Save**.

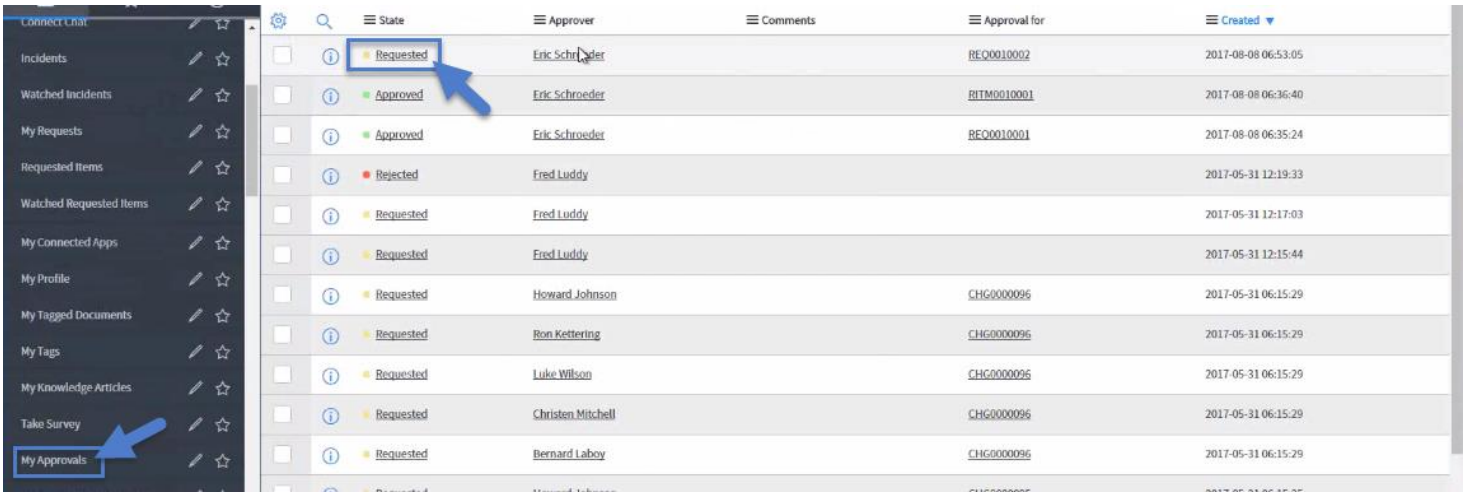


23. **Update your endpoints** by sending this new policy to target agents. Policies automatically update according to a schedule. For steps on how to do this immediately, see page 12 of the Privilege Manager User Guide.

Integration Workflow:

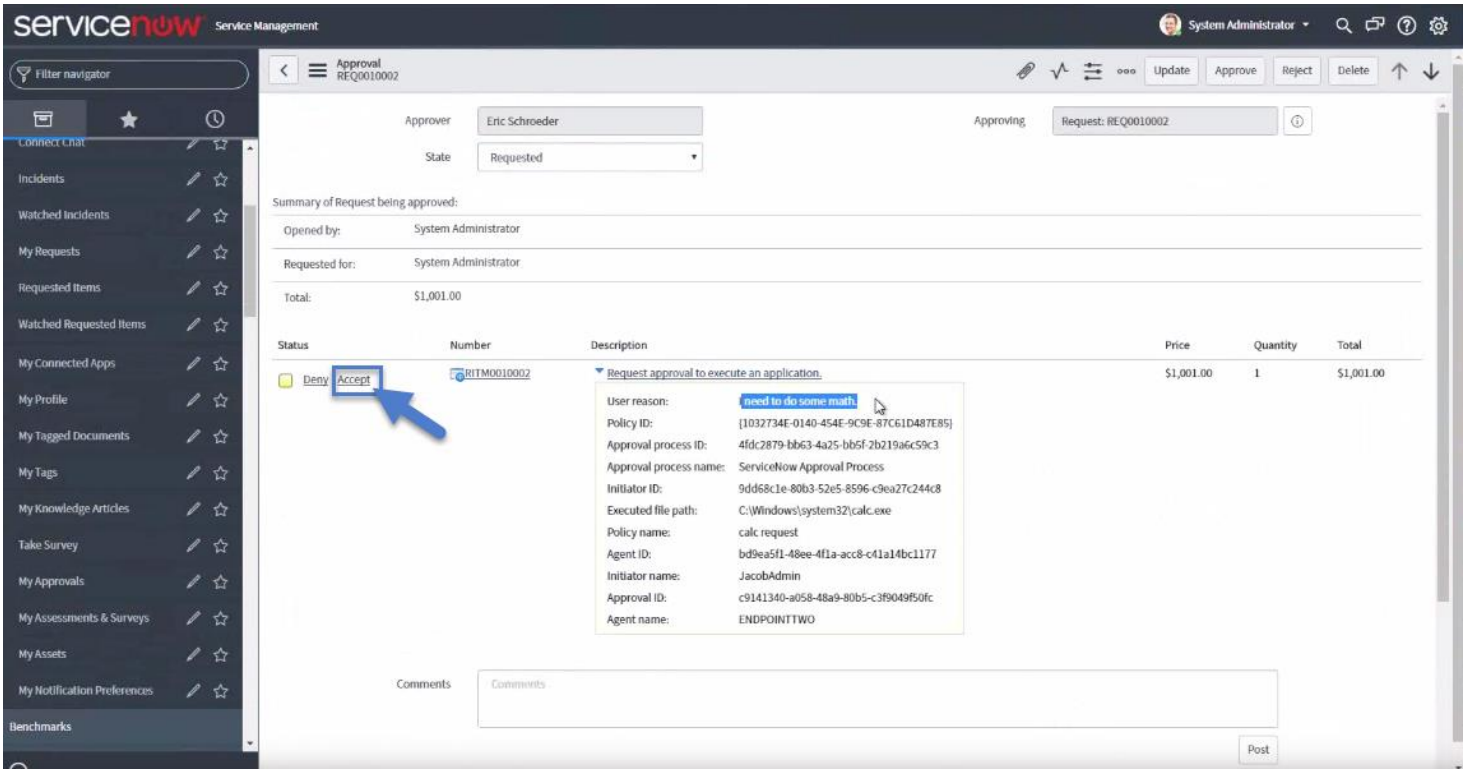
Now that you have a policy that is attached to your ServiceNow integrated Action, the requests from your policy is sent through ServiceNow for approval.

24. On your endpoint, complete the action that your policy targets for ServiceNow Approval. A justification window prompts you to explain your request. To approve these requests, open your ServiceNow Dashboard.

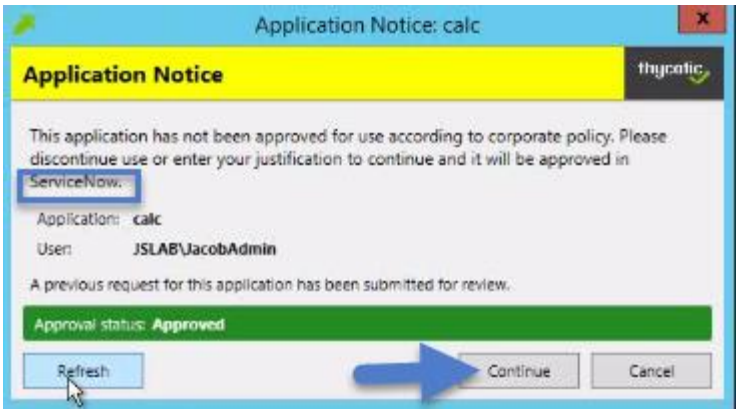


25. Go to **MyApprovals** in ServiceNow and you see your new requests. Click **Requested** for details.

26. In the Request page, you can view details of what action is being requested, and you can **Accept** the action.



27. On your endpoint, the pending justification window updates to an **Approved** status, and the user will be able to access their requested application.


Application Notice: calc
Application Notice
thycotic
This application has not been approved for use according to corporate policy. Please discontinue use or enter your justification to continue and it will be approved in ServiceNow.
Application: calc
User: JSLAB\JacobAdmin
A previous request for this application has been submitted for review.
Approval status: Approved
Refresh
Continue
Cancel

Troubleshooting

- If any issues occur while installing Privilege Manager, see Troubleshooting Installation.

Glossary of Terms

Action - An action is not required in a policy. A policy is designed, for example, to listen for specific application activity, and provide auditing information back to Privilege Manager. However, to apply controls to a process (executable), one defines an action in the policy. Some common actions include:

Adjust process rights, Add administrative rights, Remove administrative rights, Deny application execution, Require user justification – user provides a reason why they need to run the application, Application warning, Bypass UAC prompt, Require workflow approval – user needs approval to run an application, and so on.

Agent - An agent is installed on every endpoint in your network and will 1) Receive and apply defined policies to govern application/process execution on the endpoint, 2) Run tasks on the endpoint and feed audit and inventory data back to Privilege Manager.

Agent BaseUrl- The agent must be set to communicate directly with Privilege Manager. There exists a registry entry that is set upon agent installation – this registry key is called BaseUrl.

Agent Registration – The Privilege Manager agent completes a registration process when it initially contacts Privilege Manager following installation, but also at regular configurable intervals. So, registration occurs regularly.

Arellia – Arellia was the original name for Privilege Manager. Because of this, many file paths and back-end notations include the term Arellia or AMS instead of Privilege Manager or TMS.

Computer Groups – (also called **Resource Targets**) Specified sets of computers that meet certain criteria (for example, type of operating system, location of the computer, and so on) that are targeted by certain policies and scheduled tasks.

Condition – Policy Conditions contain one or more *filters* that defines what a policy is 'listening' for. If the *condition* is satisfied in a policy, then an *action* is applied.

Config Feeds – Config Feeds can be found on the ADMIN page access from the Privilege Manager main page. Configuration feeds allow IBM to deliver new components to Privilege Manager. Click through the options in the Config Feeds page, starting with the **Select Items** button, and download anything appropriate. After the item is downloaded, it is immediately available in Privilege Manager.

Dashboard – Dashboard is the term for the Privilege Manager's landing page, or Home screen.

Event – Any notable file data on your network that is targeted by Privilege Manager is called an Event.

Discovery – Discovery is a term that is used for any information that is scanned or "found" on a network and imported or used by the products.

Least Privilege –Least Privilege is a security strategy that is organized around best practices. When effectively implemented, an organization's employees can navigate their network system with the lowest level of privileges. Higher credentials are flexibly (and often automatically) granted or denied based on users and the tasks that are being performed. This dynamic strategy significantly reduces the threat of security breaches across an organization without interfering with daily operations.

Filter – The Policy Condition lists one or more filters. A filter is defined to identify many things about an executable or process, or 'situation' when an executable or process is initiated. Common Filters include:

File specifications, Network location, Directory location, Application reputation, Application digital certificate, Time of day, User context (what AD security group a user belongs), Download source, Drive type, File owner, Internet Zone, Security Catalogs, and so on.

- **Inclusion Filter/Exclusion Filter** – When a filter is placed in the **Inclusion Filters** or **Exclusion Filters** under the Conditions tab of a policy definition, it can be used to explicitly include or exclude what is defined in the filter about a policy. (For example, Exclusion: apply this policy only if the user is NOT an administrator; Inclusion: apply this policy only if the computer is on the company network; Inclusion: apply this policy only to applications signed by a specific company's digital certificate, and so on).

Persona - Personas manage sets of privileges that are assigned to users on specific Windows computers or Computer Groups. A Persona includes a set of pre-defined filters and provide an easy way to assign policies based on Computer Groups and users. Filter parameters in a Persona are limited and designed to be applied to Windows administrative users.

Policy – A set of conditions (Filters) that, when met, apply an *action* to managed resources (target computers).

- **Blacklisting** – Blacklisting is a type of policy that blocks an application from running based on a determined set of criteria.
- **Catch-All Policy** – A Catch-All policy is a type of Learning Mode policy that gathers information about any unknown events that happen in your network.
- **Elevation Policy** – An Elevation Policy allows specified applications to run with administrator credentials.
- **Greylisting** – Greylisting is a dynamic method of managing applications that might not be included on a whitelist or blacklist. Instead of trying to anticipate every executable user run, you can apply a flexible policy that includes actions or reputation checking for unknown applications.
- **Whitelisting** – Whitelisting is a type of policy that allows applications to run according to normal user credentials. This policy is often considered a neutral policy to specify trusted applications.

Policy Priority – Policies are evaluated in a certain order for each application that runs. If one policy blocks an application and ends execution before a second policy that was intended to elevate privileges, then only the block occurs. It is important to have an awareness of all policies that are defined and the order in which they are called by the agent.

RDP Monitor – The RDP Monitor is used to configure the Enhanced Session Monitoring feature in Secret Server. It is found in Privilege Manage because this feature uses the agent architecture that is defined by Privilege Manager, however this feature typically is not used in a Privilege Manager PoC.

Reputation Engine – Privilege Manager can call upon a reputation engine (for example, VirusTotal) in real time to check an application's public reputation. You can create a policy to check reputations in Privilege Manager through Greylisting policies. This type of policy can take application information and send it to the engine in real time and act on the application based on the returned reputation. For example, if the reputation engine returns a BAD grade, the application can be denied. It is suggested to apply this type of policy to specific directories where new or unknown applications might reside – like the Downloads, TEMP, or Desktop directory.

Resource Targets– (also called **Computer Groups**) Specified sets of computers that meet certain criteria (for example, type of operating system, location of the computer, and so on) that are targeted by certain policies and scheduled tasks.

Scheduled Tasks - A Privilege Manager policy that you define can be applied based on a schedule. These items run by using the Task Scheduler on each endpoint, and are only accessible by Privilege Manager administrators.

Secret Server – Secret Server is a product that many IT teams use to securely manage privileged accounts and passwords in an organization. Privilege Manager and Secret Server are separate products but often used together for a holistic approach to network security. The two products are highly integrated and some of the features cross between products. For example, the Secret Server license page houses Privilege Manager licenses, and Secret Server clients rely on Privilege Manager agent (RDP Monitor) when you use the advanced session recording feature.

Send Policy Feedback – Send Policy Feedback is a setting that can be enabled for any policy that sends information to Privilege Manager. This link is used in Learning Mode Policies and often valuable during testing, configuration, or auditing projects.

TMS – TMS is shorthand for **Management Server**. It is an umbrella term for the base application layer that Privilege Manager runs on top of.

VirusTotal – The VirusTotal reputation service is supported by Privilege Manager as a reputation engine. A free VirusTotal API key needs to be obtained to use VirusTotal in Privilege Manager. The free API has limits and might not be appropriate for a production environment that functions with over four requests per minute.