

IBM Security Verify Privilege On-Premises  
Version 10.9

*Privilege Manager User Guide*

# Contents

<b>Preliminary Steps</b> .....	<b>1</b>
Review System Requirements.....	1
System Architecture Diagrams.....	1
General Architecture.....	1
Cloud Architecture for Azure or Amazon AWS Hosting Environments.....	2
Proxy or Azure Service Bus Architecture for Environments Without Internet Access.....	2
Port/Access Information.....	3
<b>Privilege Manager Installation</b> .....	<b>4</b>
<b>Licensing</b> .....	<b>5</b>
Installing New Licenses.....	5
Steps for stand-alone Privilege Manager Installation.....	5
Steps for Combined Privilege Vault + Privilege Manager Installation.....	6
Converting from Trial Licenses.....	7
Expired Licenses.....	7
<b>Getting Started</b> .....	<b>8</b>
Home.....	8
Agent Installation.....	9
Diagnostics.....	10
Reports.....	11
Configuring Privilege Manager with Privilege Vault.....	11
Active Directory Synchronization.....	12
<b>Least Privilege Overview</b> .....	<b>13</b>
What is Least Privilege?.....	13
<b>Local Security Overview</b> .....	<b>15</b>
Computer Groups.....	15
Create New Computer Group.....	15
Local Groups.....	16
Create New Local Group.....	17
Details Tab.....	18
Statistics Tab.....	19
Audit Tab.....	20
Local Users.....	20
Create New Local User.....	21
Details Tab.....	21
Groups Tab.....	23
Statistics Tab.....	23
<b>Application Control Overview</b> .....	<b>25</b>
Dashboard.....	25
What is a Policy?.....	25
Overview of the Configuration Process.....	26

Collecting File Data .....	26
<b>Event Discovery .....</b>	<b>27</b>
Learning Mode Policies – Send Policy Feedback .....	27
Discover Applications that Require Administrator Rights .....	27
Discover All Events on Test Endpoints .....	29
View Policy Results .....	30
View Files .....	30
New Loaded Resource .....	31
<b>Sending Policies to Endpoints .....</b>	<b>32</b>
View Deployment Status.....	33
Update Policies on an Endpoint by using PowerShell.....	34
Agent Event Log Viewer .....	35
<b>Whitelisting Policies.....</b>	<b>37</b>
Example: Whitelist the Microsoft Security Catalog.....	37
Example: Whitelist Google Applications with File Upload .....	38
<b>Blacklisting Policies .....</b>	<b>41</b>
Example: Blacklist iTunes with File Upload .....	41
Example: Quarantine Specified Malware .....	42
<b>Elevation Policies .....</b>	<b>45</b>
Example: Applying Administrator Rights to a Network Share .....	45
Example: User Justification Required to Run.....	47
Example: Application Execution Requires Approval (Workflow) .....	49
<b>Greylisting Policies.....</b>	<b>53</b>
Catch-All Policy .....	53
Reputation Checking Policies .....	55
<b>Policy Priority .....</b>	<b>60</b>
Example: Why Policy Priority Matters.....	60
<b>Personas .....</b>	<b>67</b>
Viewing Your Personas .....	67
Creating a Persona.....	67
<b>Integrations.....</b>	<b>69</b>
Setting Up Email Server Connection (SMTP) .....	69
Setting Up VirusTotal for Reputation Checking.....	70
Setting Up ServiceNow Ticketing System .....	73
<b>Troubleshooting .....</b>	<b>83</b>
<b>Glossary of Terms.....</b>	<b>84</b>

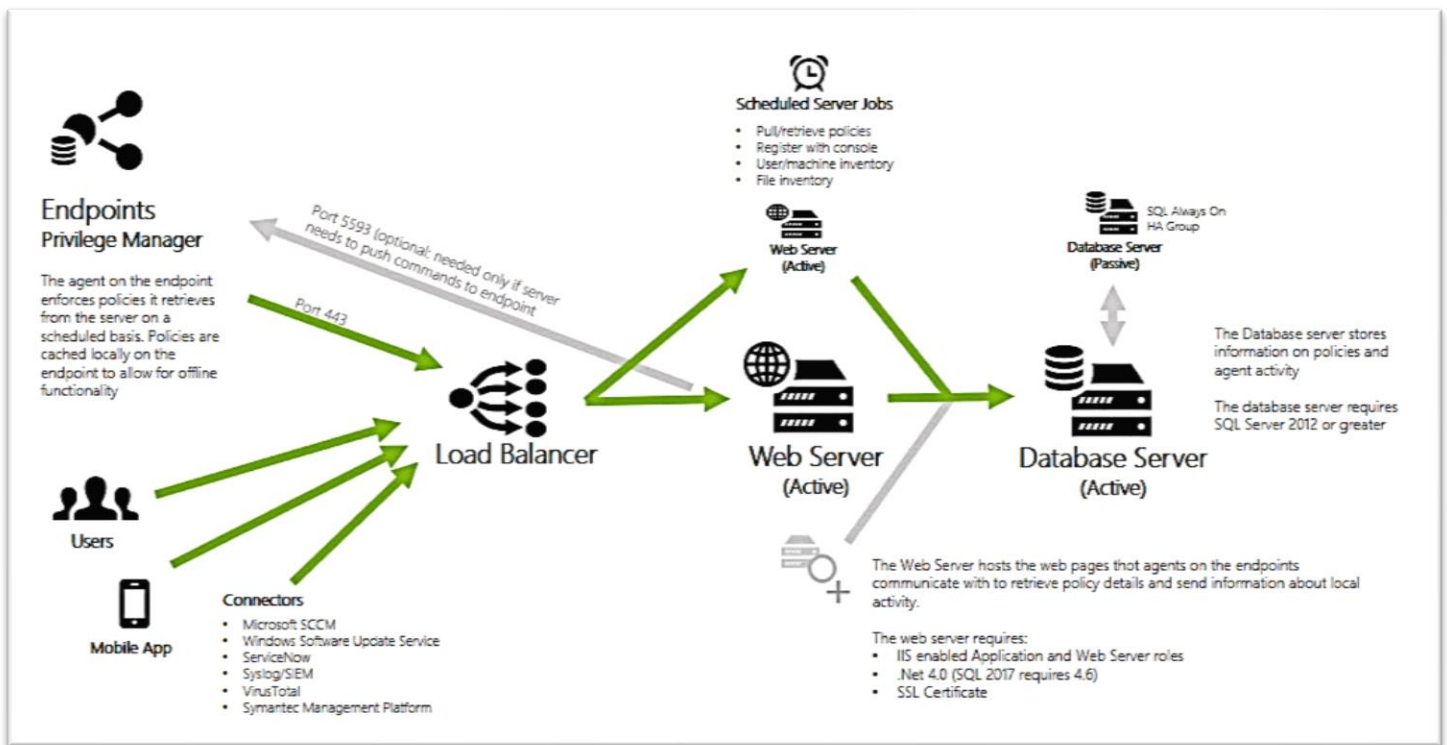
# Preliminary Steps

## Review System Requirements

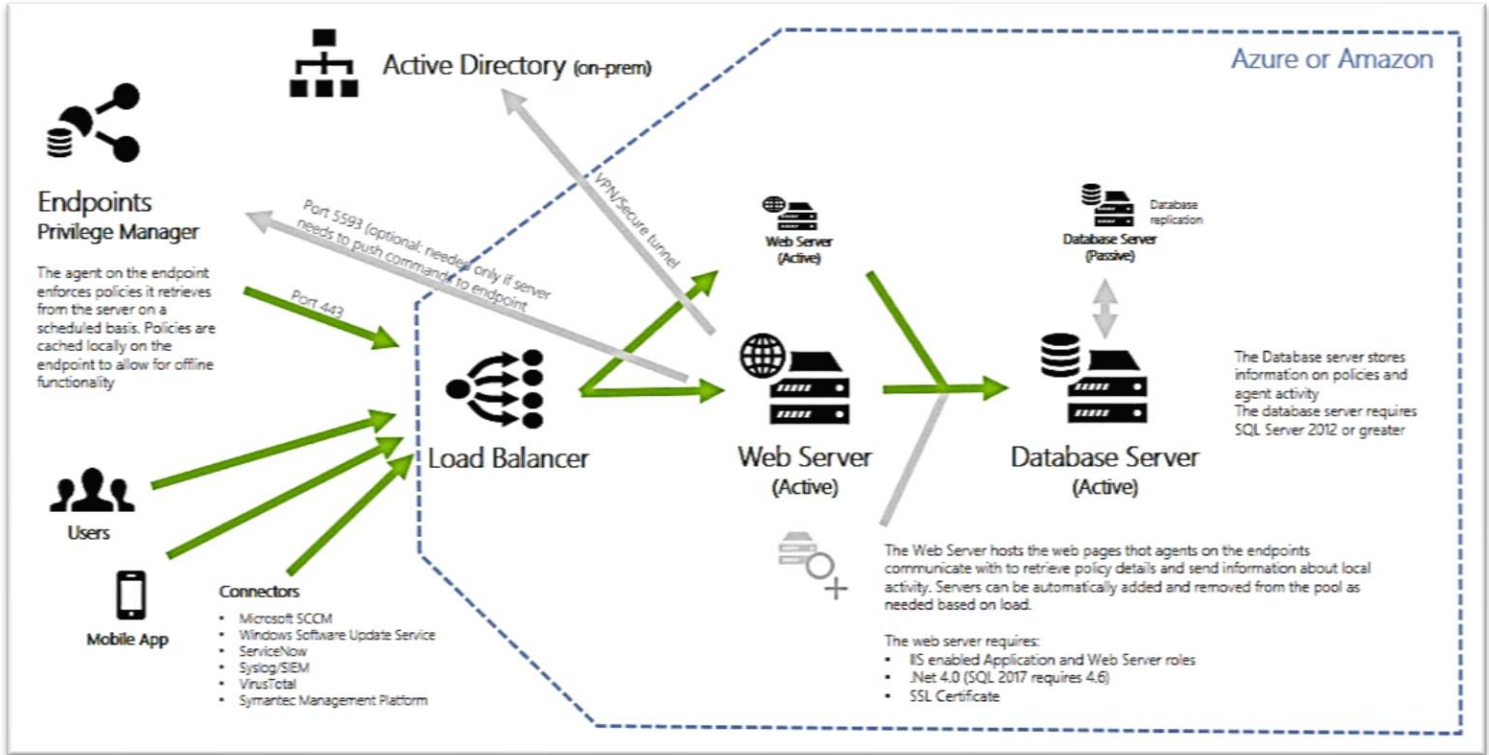
For a complete list of System Requirements for both proof-of-concept and Production Environments, see the [System Requirements Guide for Privilege Manager](#).

## System Architecture Diagrams

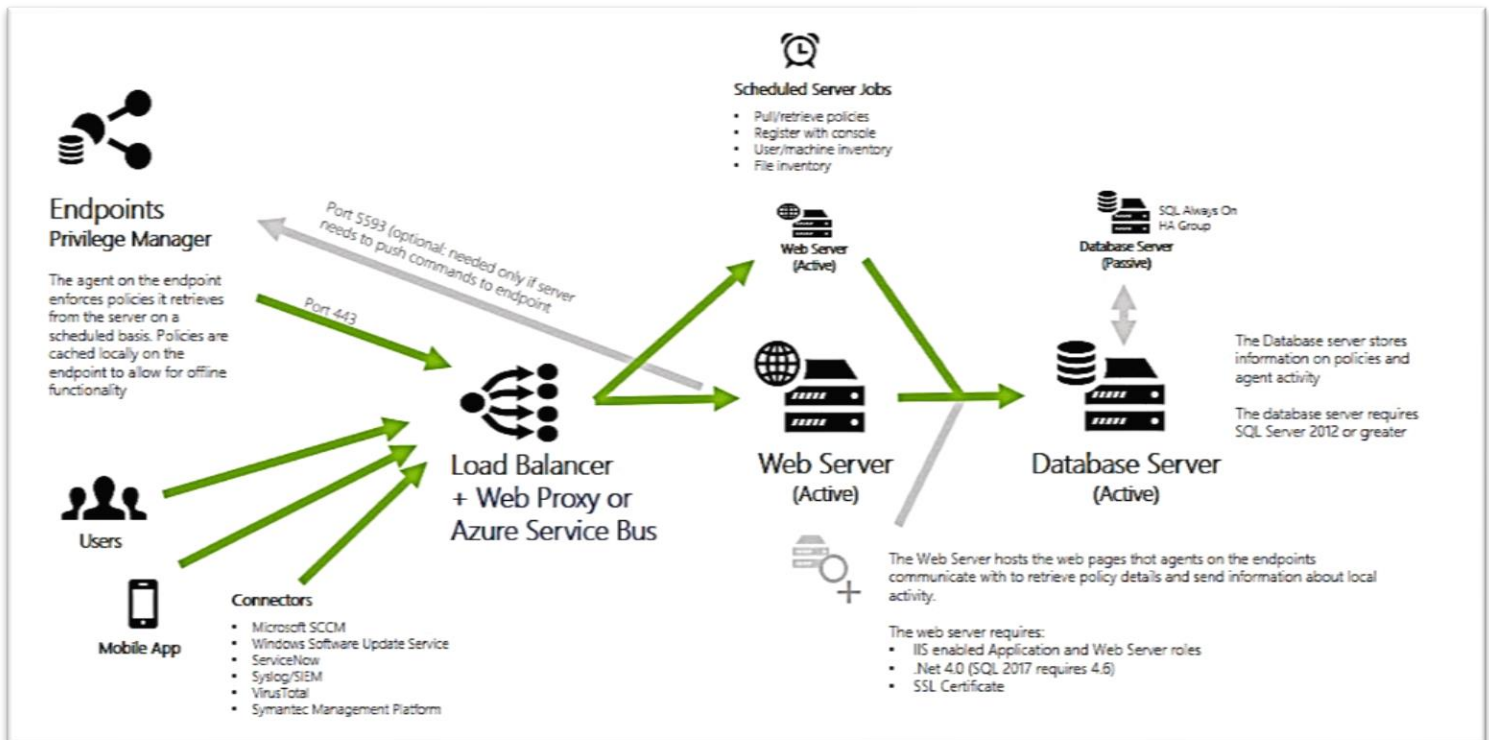
### General Architecture



## Cloud Architecture for Azure or Amazon AWS Hosting Environments



## Proxy or Azure Service Bus Architecture for Environments Without Internet Access



## Port/Access Information

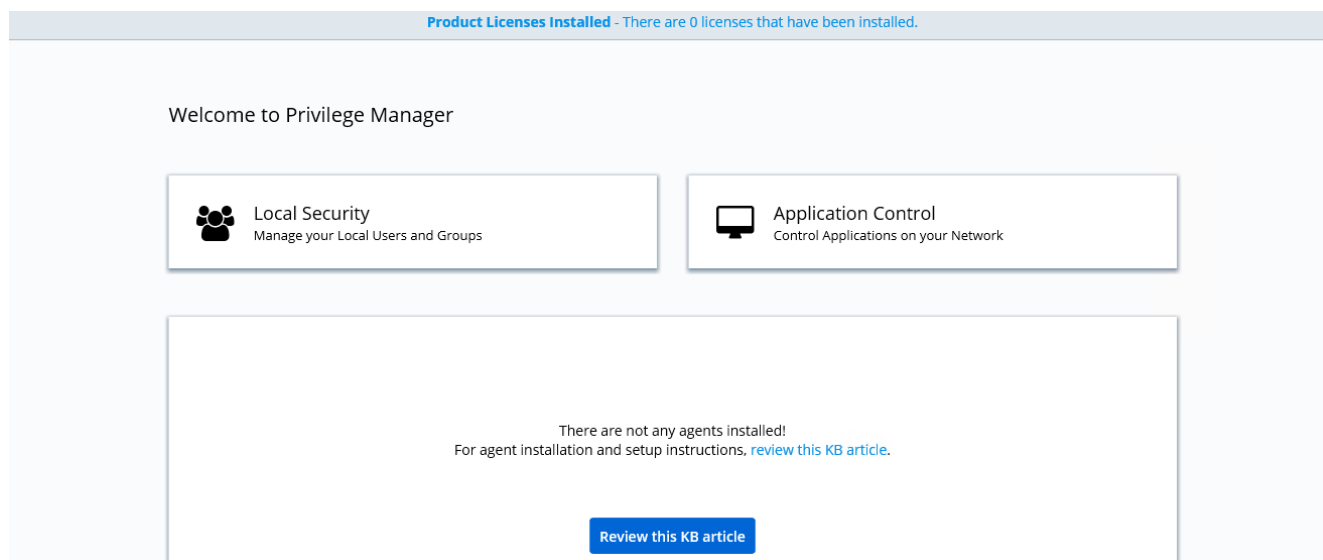
- Outbound access from the agent to the server is done **by default over port 443** (the standard port for HTTPS communication) but you can specify a different port if desired.
- The only port that the agent listens on is **port 5593**. This port is not required. For example, you can block this port 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 Privilege Vault. 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 Privilege Vault 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 Privilege Vault, navigate to **Admin > Licenses** or click the **Product Licenses Installed** link in the top banner.

Administration

Select Menu Options

Privilege Manager

Configuration

Personas

Policies

Filters

Config Feeds

Setup

Setup Home

Tasks

Actions

Event Discovery

Folders

Resources

Diagnostics

Licenses

Agents

Add / Upgrade Privilege Manager Featu Log Viewer

- 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.

### Product Licensing Help

First time users will want to review the [Getting Started Guide](#).

Licenses can be installed by clicking on the install license button.

Product Licenses

Install license key

[Add license certificate instead](#)

License Name \*

License Key \*

Add License

Cancel



## Steps for Combined Privilege Vault + Privilege Manager Installation

Product Licenses Installed - There are 0 licenses that have been installed.

**Product Licensing Help** ✕  
First time users will want to review the [Getting Started Guide](#).

Licenses can be installed in [Secret Server](#). After installing the licenses you may need to run the [import task](#).

Product Licenses ?

Licenses can be installed in [Secret Server](#). After installing the licenses you may need to run the [import task](#).

1 to 4 of 4

PRODUCT ^	OS TYPE	STATUS	TOTAL LICENSES	IN USE	START DATE	AUP RENEWAL	EXPIRES
-----------	---------	--------	----------------	--------	------------	-------------	---------

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

- To access Privilege Vault’s licensing page, either click the **Privilege Vault** 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).

Product Licenses Installed - There are 0 licenses that have been installed.

Administration

Select Menu Options

**Privilege Manager**

- Configuration
- Personas
- Policies
- Filters

**Setup**

- Setup Home
- Database
- Config Feeds
- Actions
- Tasks
- Event Discovery
- Folders
- Email
- Licenses
- Resources
- Diagnostics
- Licenses
- Agents
- Add / Upgrade Privilege Manager Features
- Log Viewer

- From Privilege Vault’s License page, select **Install New License**.

**Licenses**

You are currently licensed for 1 user(s). You currently have 1 enabled user(s). [Get More Licenses](#)

There are no Licenses.

i Support licenses allow you to get free upgrades for new releases of Secret Server. You must purchase support for as many users as you are licensed. [Get More Licenses](#)

[View Server Activation \(Advanced\)](#)

[Back](#) [+ 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 Privilege Vault 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

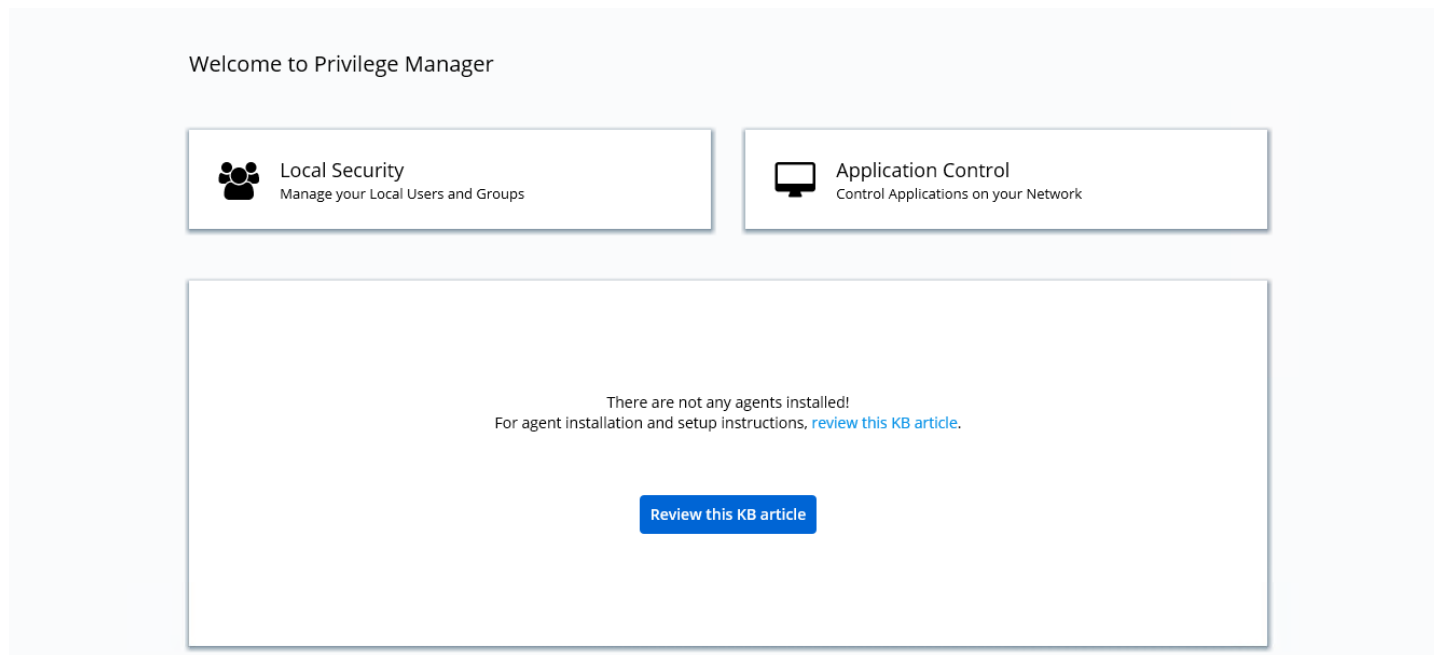
When your Privilege Manager licenses expire or exceed the licensed count, Privilege Manager reverts to a “Limited Mode.” In Limited Mode, the server stops accepting data that is sent from agents. Additionally, new endpoints register but are not recorded. Endpoints that are identified are added to Computer 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:

Welcome to Privilege Manager

The screenshot shows the 'Home' page of the Privilege Manager interface. At the top, there is a 'Welcome to Privilege Manager' message. Below this, there are two main navigation cards: 'Local Security' (Manage your Local Users and Groups) and 'Application Control' (Control Applications on your Network). The central focus is the 'Agent Health' section, which contains two large blue circular gauges. The left gauge is labeled 'Agent Heartbeat State' and the right is 'Agent Policy State'. Both gauges show a legend for 'Normal (1)'. Below the gauges, there is a text prompt 'For agent installation and setup instructions,' and a blue 'Install Agents' button.

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.

Reports > Agent Registration Gauge State - Drilldown

CSV PDF Search

Drag column here for grouping

MONITOREDRESOURCE	LASTCHANGE	STATE	MINUTES	PREVIOUSSTATE
JANE	1/10/2018 6:55:47 AM	Normal	18	

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.

Reports > Agent Policy State - Drilldown

Drag column here for grouping

MONITOREDRESOURCE	LASTCHANGE	STATE	NUMBER OF POLICIES MISSING
JANE	1/10/2018 7:25:52 AM	Normal	0

## 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.

### Diagnostics

*This page shows you general diagnostics about your environment that can be used to troubleshoot issues or submit to Technical Support.*

#### Managed Operating Systems



#### Agent Registration Gauge State



#### Agent Policy State



#### Key Configuration Settings

- Unconfigured - Warning**  
Set Default User Credential
- Properly Configured**  
Product Licenses Installed
- Unconfigured - Warning**  
Configure Active Directory
- Properly Configured**  
Install Agents
- Normal**  
Upgrade Available

#### Licensing


- Normal**  
Client License Expiration
- Normal**  
Server License Expiration
- Normal**  
Client License Count Exceeded
- Normal**  
Server License Count Exceeded
- Normal**  
Client License Count Limit
- Normal**  
Server License Count Limit
- Normal**  
Client License Trial Expiration
- Normal**  
Server License Trial Expiration

#### System Health

- Normal**  
Remote Task Status
- Normal**  
Number of Old Computers
- Normal**  
Unacknowledged Events
- Normal**  
Pending Approvals Count
- Normal**  
Number of Application Events
- Normal**  
File Uploads Size
- Normal**  
Background Message Queue Size
- Normal**  
Background Message Queue Older than 1 Week
- Normal**  
Bad Client Item Cache

# 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.



Thycotic 10.4 Privilege Manager

Search items Search HOME TOOLS ADMIN **REPORTS**

### Reports

Select Report Options

#### Actions

- Application Control Event Summary  
*Lists Application Control Event Summaries*
- Summary of Application Actions by Computer
- Summary of Application Actions by Operating System
- Summary of Application Actions by Product Version
- Application Control Event Summary Acknowledgements  
*Lists Application Control Event Summary Acknowledgements*
- Summary of Application Actions by Mac Executable
- Summary of Application Actions by Product Name
- Summary of Application Actions by Win32 Executable

#### Agent

- Agent Installation Summary  
*Lists computers with the Application Control Agent or File Inventory Agent installed, along with the version of the agent and client operating system and service pack level. The results can be filtered by the Agent Version or Operating System on the client computer.*
- Agent Summary by OS  
*List of Operating Systems discovered with or without the agent installed.*
- Managed Operating Systems  
*List of operating systems with the count of managed computers running them.*
- Agent Installations  
*Lists computers and their installed agent information.*
- Computers Without Agent Installations  
*Lists computers without the given agent or without the given agent version.*

#### Approvals

- Application Justification Summary Details Report  
*List all events representing actions for Application Control policies*
- Summary of Application Approval Requests by Approver  
*Summary of Approvals*
- Summary of Application Approval Requests by User  
*Summary of Approvals*
- Summary of Application Approvals by Date  
*Summary of Approvals*
- Pending Execute Application Approvals
- Summary of Application Approval Requests by Computer  
*Summary of Approvals*
- Summary of Application Approvals and Denials  
*Summary of Approvals*

#### Detection

- All ActiveX Controls  
*All ActiveX Controls*
- All Win32 Executables Report  
*Lists all Win32 Executables.*
- Application Metering Summary Details Report  
*List all events representing actions for Application Control policies*
- Application Verifier Logs  
*List all Application Verifier Policy events*
- Discovered Files not Reported by File Inventory  
*Lists File resources that have been discovered on the network but have not yet had full details disclosed by the File Inventory process.*
- Files Pending Agent Discovery with no Discovery Agent  
*Default file collection report*
- All Mac OS Executables Report  
*Lists all Mac OS Executables.*
- Application Metering Report  
*List all Application Metering Policy events*
- Application Verification Summary Details Report  
*List all events representing actions for Application Control policies*
- Application Verifier Report  
*List all Application Verifier Policy events*
- File Security Rating Details Report  
*Lists files with security rating details.*
- Summary of Resource Types Pending Discovery  
*Count of resource types pending resource discovery.*

## Configuring Privilege Manager with Privilege Vault

If you are using both Privilege Manager and Privilege Vault, you can store Privilege Manager’s local credentials in Privilege Vault. To configure Privilege Manager with Privilege Vault, 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.

NAME	COMPUTERS	USER GROUPS	USERS
Windows Computers	1	18	5
MacOS Computers	0	0	0

## 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.

RULE #	OPERATION	LIST TYPE	SELECTED ITEMS	RUNNING COMPUTER TOTAL
1)	Only Keep Computers in	Filter	All Windows Computers	1
2)	Only Keep Computers in	1 Computer List	JANE	1

NAME	RESOURCE TYPE	SYSTEMTYPE	DOMAIN	MANUFACTUR...	MODEL	IPADDRESS	CREATEDDATE
JANE	Computer	X86-based PC	testlab.com	Microsoft Corporation	Virtual Machine	10.12.30.4	1/10/2018 6:27:40 AM

## 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:

Thycotic 10.4 Privilege Manager

Search Items Search HOME TOOLS ADMIN REPORTS

LOCAL SECURITY HOME

COMPUTER GROUPS

- Windows Computers 1
- MacOS Computers 0

Local Security Home

Privilege Manager can store credentials in Secret Server, would you like to configure this now?

Show All Computer Groups 1 to 2 of 2

NAME	COMPUTERS	USER GROUPS	USERS
Windows Computers	1	18	5
MacOS Computers	0	0	0

Create Computer Group

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.

LOCAL SECURITY HOME

COMPUTER GROUPS

- Windows Computers 1
- Groups 18
- Users 5
- MacOS Computers 0

Computer Group > Windows Computers

Either choose to manage the members of existing groups (select Groups on the left) or choose to create a new user to add to all endpoints (select Users on the left).

There are 1 unmanaged groups with local administrator permissions.

There are 2 users with local administrator permissions. Once the necessary policies have been created to elevate applications local administrative rights can be removed.

## 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.

LOCAL SECURITY HOME

COMPUTER GROUPS

- Windows Computers 1
- Groups 18
- Users 5
- MacOS Computers 0

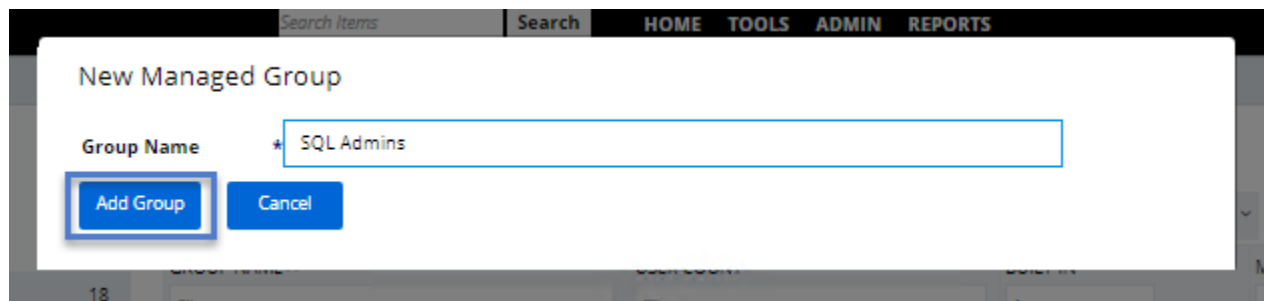
Windows Computers > Groups

View 10 rows 1 to 10 of 18

GROUP NAME	USER COUNT	BUILT-IN	MANAGED
Access Control Assistance Operators	0	Built-In	Not Managed
Administrators	2	Built-In	Not Managed
Backup Operators	0	Built-In	Not Managed
Cryptographic Operators	0	Built-In	Not Managed
Distributed COM Users	0	Built-In	Not Managed
Event Log Readers	0	Built-In	Not Managed
Guests	1	Built-In	Not Managed
Hyper-V Administrators	0	Built-In	Not Managed

Create Group

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

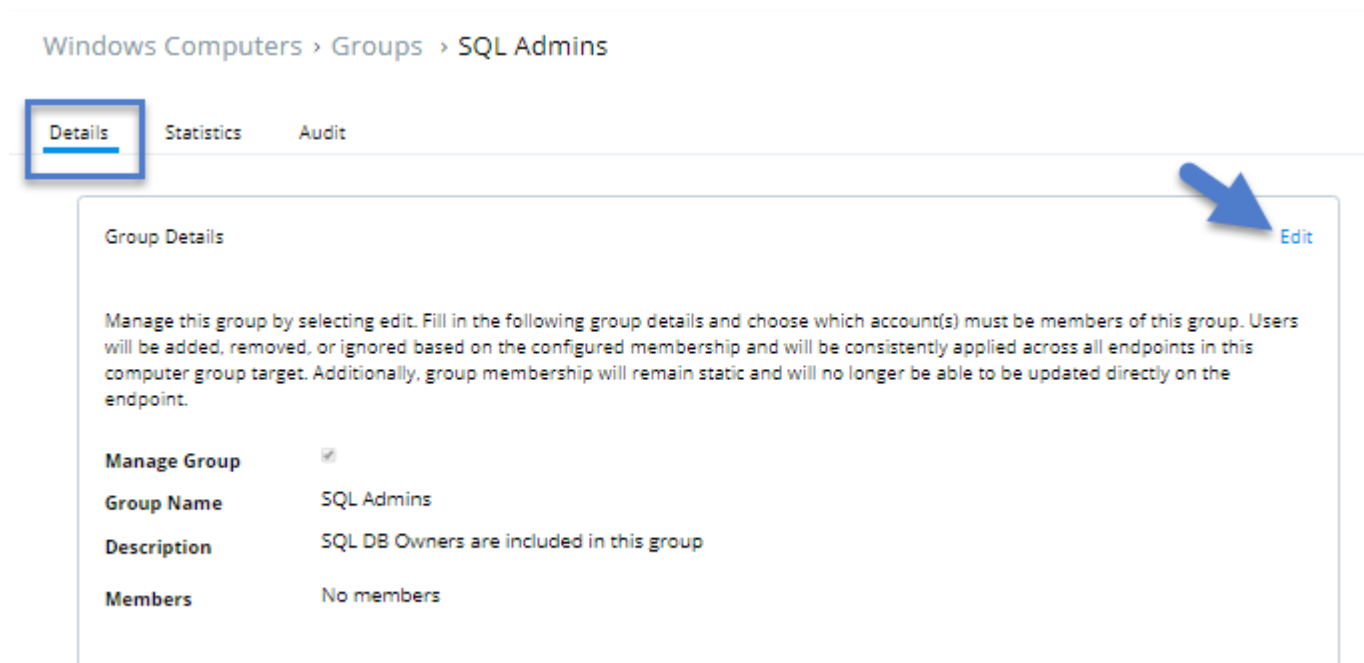


On your new group page, add a **Description** and select **Save Changes**. Privilege Manager prompts you with a **Confirm Navigation** box. Click **Yes**.

## 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.



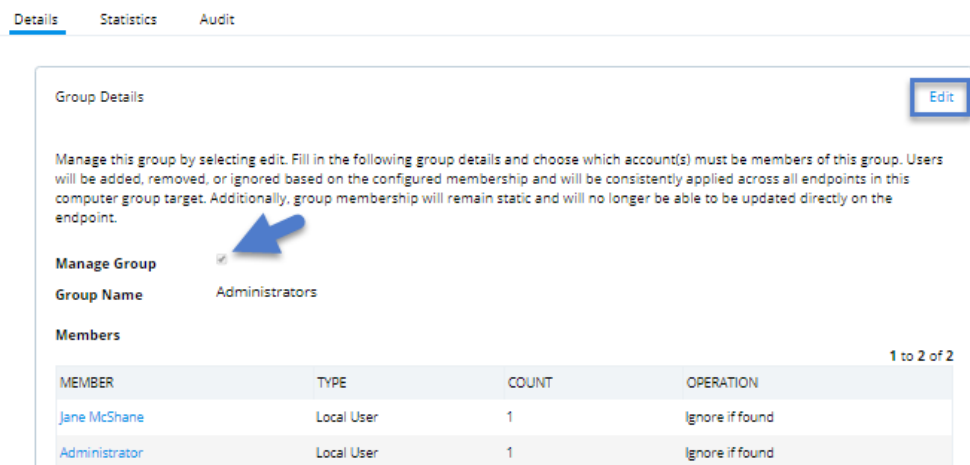
When editing, you can add members to the group by clicking the **Add Member** button. Select the type to add (*Domain User, Domain Group, Local User*) and then toggle the available options from the user list. To finish click **Add Member**, then **Save Changes**.

### 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.

Windows Computers > Groups > Administrators



Group Details Edit

Manage this group by selecting edit. Fill in the following group details and choose which account(s) must be members of this group. Users will be added, removed, or ignored based on the configured membership and will be consistently applied across all endpoints in this computer group target. Additionally, group membership will remain static and will no longer be able to be updated directly on the endpoint.

**Manage Group**

**Group Name** Administrators

**Members** 1 to 2 of 2

MEMBER	TYPE	COUNT	OPERATION
Jane McShane	Local User	1	Ignore if found
Administrator	Local User	1	Ignore if found

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.

LOCAL SECURITY HOME

COMPUTER GROUPS

- Windows Computers 1
- Groups 18**
- Users 5
- MacOS Computers 0

Windows Computers > Groups > Administrators

Details **Statistics** Audit

### Computers with this User Group

Related Reports

- Administrators Group Missing Local Administrator Account
- Non Well-Known Local Group Summary
- Well-Known Group Summary
- Summary of Local Users as Local Administrators
- Local User/Group Summary

### Group Membership

Period: Past Week

## 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 SECURITY HOME

COMPUTER GROUPS

- Windows Computers 1
- Groups 18**
- Users 5
- MacOS Computers 0

Windows Computers > Groups > Administrators

Details Statistics **Audit**

CHANGED ^	USER NAME	COMPUTER NAME	CHANGE TYPE
Jan 10, 2018, 6:59:32 AM	Jane McShane	JANE	Added
Jan 10, 2018, 6:59:32 AM	Administrator	JANE	Added

## 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.

LOCAL SECURITY HOME		Windows Computers > Users		
COMPUTER GROUPS		<a href="#">Create User</a>		
Windows Computers	1	1 to 5 of 5		
Groups	18			
<b>Users</b>	<b>5</b>			
MacOS Computers	0			

USER NAME ^	GROUP COUNT	BUILT-IN	MANAGED
Administrator	1	Built-in	Not Managed
DefaultAccount	1	Built-in	Not Managed
defaultuser0	0	User Defined	Not Managed
Guest	1	Built-in	Not Managed
Jane McShane	1	User Defined	Not Managed

## 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.

The screenshot shows a dialog box titled "New Managed User". It has a "User Name" field with the text "Diana Prince" entered. Below the field are two buttons: "Add User" and "Cancel".

## 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.


The screenshot shows the 'Users' tab for the 'Diana Prince' user in the Privilege Manager console. The left sidebar shows a tree view with 'Users' selected. The main content area is titled 'Windows Computers > Users > Diana Prince' and has three tabs: 'Details' (selected), 'Groups', and 'Statistics'. Below the tabs, there's a warning: 'Editing the account details will apply these details across all computers in this computer group. This action will make the account a "Managed Account" in Privilege Manger.' The 'Account Details' section includes: 'User Managed' (checked), 'User Name' (Diana Prince), 'Full Name' (Diana Prince), 'Description' (empty), 'Account is Disabled' (unchecked), and 'Initial Password' (masked with asterisks and a 'Change Password' button). The 'Update Schedule' section is expanded to show 'Options': 'User Must Change Password At Next Logon' (checked), 'User Cannot Change Password' (unchecked), and 'Password Never Expires' (unchecked). At the bottom right, there are 'Save Changes' and 'Cancel' buttons. Blue arrows point to the 'User Managed' checkbox, the 'Change Password' button, and the 'User Must Change Password At Next Logon' checkbox.

### 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.

## Password Details

Managing the password of this account means that Privilege Manager will be setting and controlling the password on each computer in this computer group.



**Password Management**  

**Characters**

- Uppercase
- Numbers
- Lowercase
- Symbols

**Password Length**  characters

**Log Password Before Change**

**Update Schedule**  Every 30 days at 8:00 AM starting Sat Jan 13 2018 

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
<b>Users</b>	<b>6</b>
MacOS Computers	0

Details   Groups   **Statistics**

### Computers with this User

Category	Computers with Guest	Computers without Guest
All Computers	1	1
Windows Computers	1	0

■ 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:

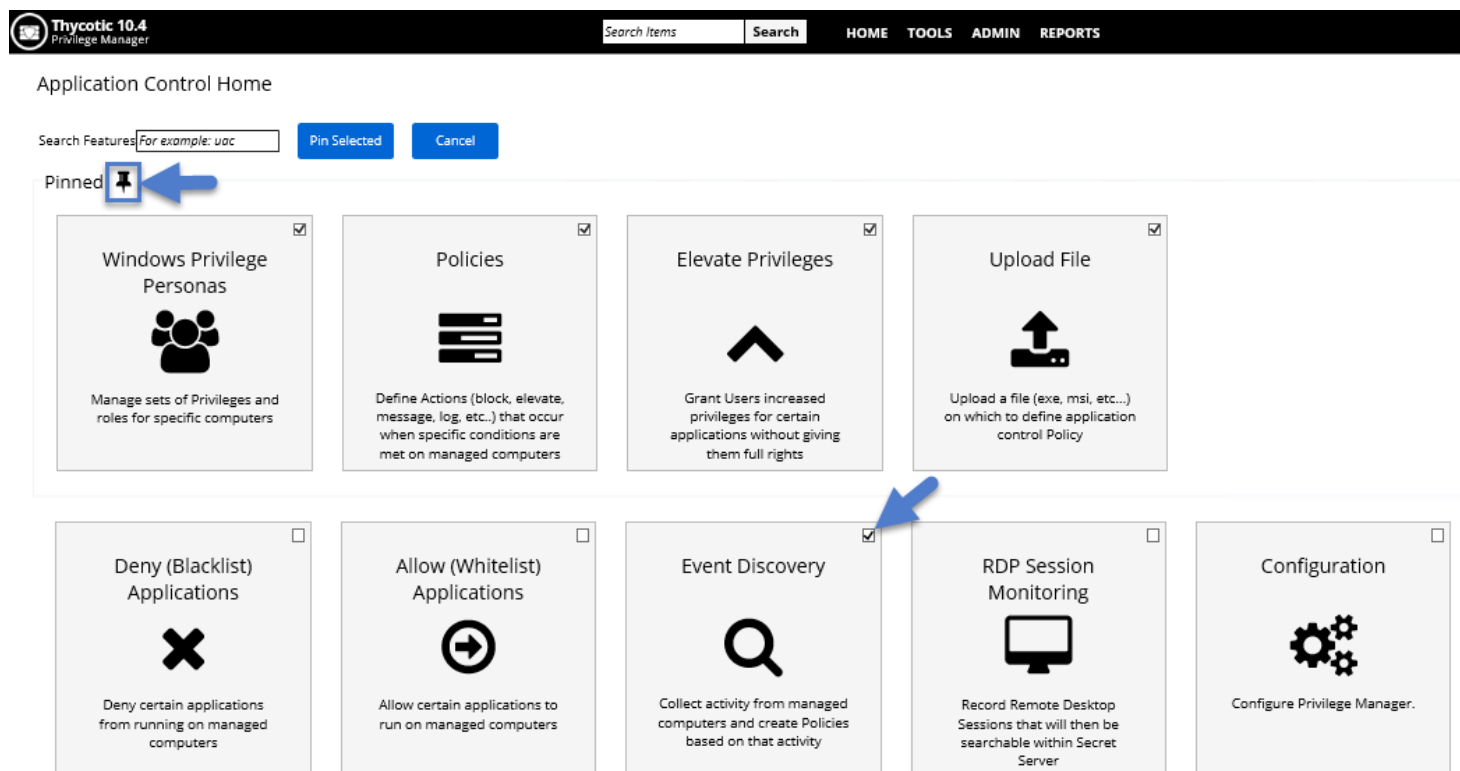
Date	Added To Group	Removed From Group	Password Disclosed
1/10	1	0	0
1/11	0	0	0
1/12	0	0	3
1/13	0	0	0
1/14	0	0	0
1/15	0	0	2

■ 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.

Policy > Administrative Rights Required Detection Policy (Application Compatibility)

 This policy is not enabled. Managed computers won't receive this policy until it is enabled.

 This Policy is used by Event Discovery. Changes to this policy should be made by choosing Admin / Event Discovery / Configuration.  
Configure Event Discovery

General    Conditions    **Actions**    Policy Enforcement    Deployment

Send policy feedback  

**Actions to apply to the application**  
No actions are currently being applied.

**Actions to apply to the child applications**  
 Use the same actions as the parent

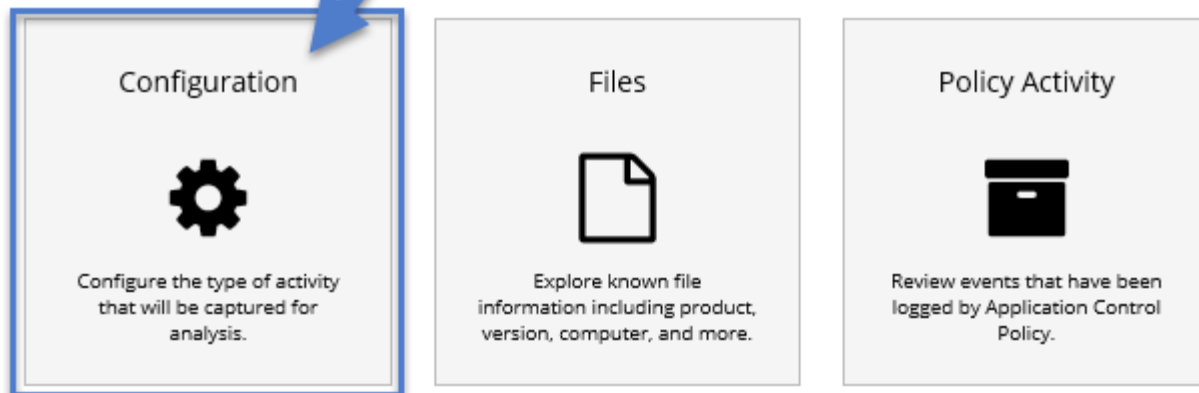
[Back](#)    [Edit](#)    [Enable](#)    [Create a Copy](#)    [See Events](#)

## 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.

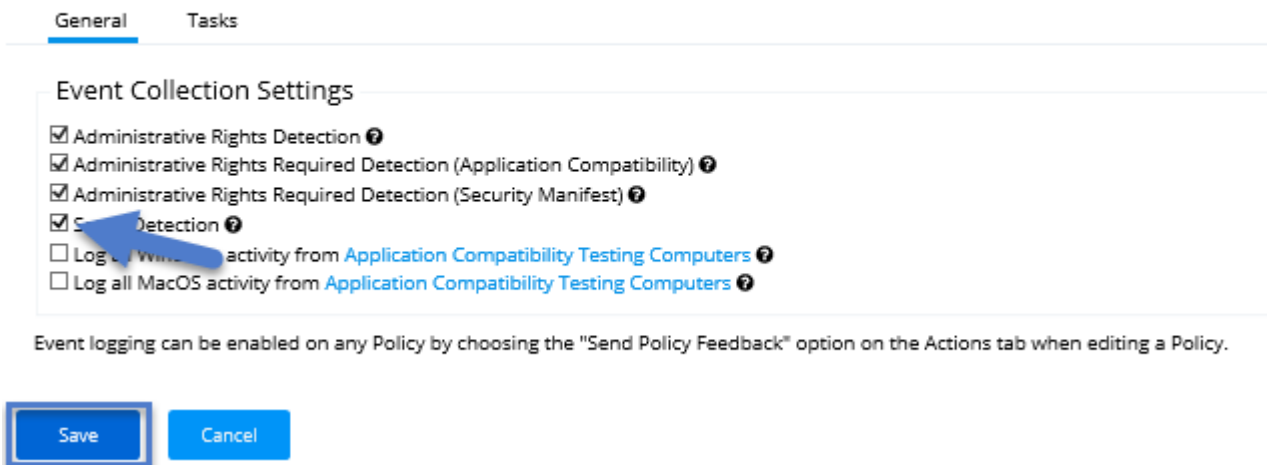
1. From Application Control's Dashboard, navigate to **Event Discovery**. Next, click **Configuration**.

## Event Discovery



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

### Event Discovery Configuration



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**

### Event Discovery Configuration

General Tasks

Event Collection Settings

- Administrative Rights Detection ?
- Administrative Rights Required Detection (Application Compatibility) ?
- Administrative Rights Required Detection (Security Manifest) ?
- Security Detection ?
- Log all Windows activity from **Application Compatibility Testing Computers** ?
- Log all MacOS activity from **Application Compatibility Testing Computers** ?

Event logging can be enabled on any Policy by choosing the "Send Policy Feedback" option on the Actions tab when editing a Policy.

Save Cancel

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.

Resource Filter > Application Compatibility Testing Computers

General Filter Definition Membership

Define the conditions below in order that will determine membership for this Resource Filter. ?

1) INCLUDE SPECIFIC RESOURCES (EXPLICITLY SPECIFY COMPUTERS TO INCLUDE) ?

JANE

EDIT RESOURCES TO INCLUDE

View Parameters

NAME	RESOURCE TYPE	SYSTEMTYPE	DOMAIN	MANUFACTURER	MODEL	IPADDRESS	CREATEDDATE
<input checked="" type="checkbox"/> JANE	Computer	X86-based PC	testlab.com	Microsoft Corporation	Virtual Machine	10.12.30.4	1/10/2018 6:27:40 AM

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.

The screenshot displays the 'Policy Activity' view. On the right, a list of events is shown, each with a filename, timestamp, description, and counts for pending and total results. Action links like 'Assign to Policy', 'Create Filter', 'View Policy', and 'Acknowledge Pending' are provided for each event. A blue arrow points to the 'Assign to Policy' link for the first event, 'InstallAgentUserBroker.exe'. On the left, a filter sidebar is visible with sections for 'Type', 'Number of Results', 'Last Change Date', 'Acknowledged', 'Event Type', 'Policy', and 'File Name'. The 'Type' section is expanded to show 'Policy Activity'. At the top right, there are pagination controls showing '1 to 10 of 20' and navigation arrows.

Type	Number of Results	Last Change Date	Acknowledged	Event Type (1)	Policy (2)	File Name (16)
Policy Activity	2000	Last 30 Days	Only Include Unacknowledged	Application Action (20)	Event Discovery Testing Computers Audit Policy (Windows) (16)	taskhostw.exe (2) cleanmgr.exe (2) DismHost.exe (2) wermgr.exe (2) InstallAgentUserBroker.exe (1) Show More (all)
				<b>InstallAgentUserBroker.exe</b> (Jan 24, 2018, 6:57:40 AM) Application Action from Event Discovery Testing Computers Audit Policy (Windows) Pending Count: 1   Total Count: 21 <a href="#">Assign to Policy</a>   <a href="#">Create Filter</a>   <a href="#">View Policy</a>   <a href="#">Acknowledge Pending</a>	<b>wuapihost.exe</b> (Jan 24, 2018, 6:57:40 AM) Application Action from Event Discovery Testing Computers Audit Policy (Windows) Pending Count: 21   Total Count: 21 <a href="#">Assign to Policy</a>   <a href="#">Create Filter</a>   <a href="#">View Policy</a>   <a href="#">Acknowledge Pending</a>	<b>taskhostw.exe</b> (Jan 24, 2018, 6:57:40 AM) Application Action from Event Discovery Testing Computers Audit Policy (Windows) Pending Count: 41   Total Count: 41 <a href="#">Assign to Policy</a>   <a href="#">Create Filter</a>   <a href="#">View Policy</a>   <a href="#">Acknowledge Pending</a>
				<b>InstallAgent.exe</b> (Jan 24, 2018, 6:57:40 AM) Application Action from Event Discovery Testing Computers Audit Policy (Windows) Pending Count: 21   Total Count: 21 <a href="#">Assign to Policy</a>   <a href="#">Create Filter</a>   <a href="#">View Policy</a>   <a href="#">Acknowledge Pending</a>	<b>AppHostRegistrationVerifier.exe</b> (Jan 16, 2018, 5:53:05 AM) Application Action from Event Discovery Testing Computers Audit Policy (Windows) Pending Count: 6   Total Count: 6 <a href="#">Assign to Policy</a>   <a href="#">Create Filter</a>   <a href="#">View Policy</a>   <a href="#">Acknowledge Pending</a>	<b>conhost.exe</b> (Jan 16, 2018, 5:53:05 AM) Application Action from Event Discovery Testing Computers Audit Policy (Windows) Pending Count: 8   Total Count: 8

## 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.

**Type**Files ✕**Number of Results**2000 ✎**Discovery Date**Last 30 Days ✎**Computer (2)**

This Server (177)

**ArelliaDisplayXamlAction.exe**

on JANE

[Assign to Policy](#) | [Create Filter](#)**Thycotic.Agent.User.exe**

on JANE

[Assign to Policy](#) | [Create Filter](#)

## New Loaded Resource

**FileName (156)**[New Loaded Resource](#)  
1/10/2018 6:59:44 AM (15)[New Loaded Resource](#)  
1/10/2018 6:59:38 AM (14)

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.

Resource Explorer &gt; New Loaded Resource 1/10/2018 6:59:44 AM

Summary
Known Data <span>▼</span>
Events
Associations

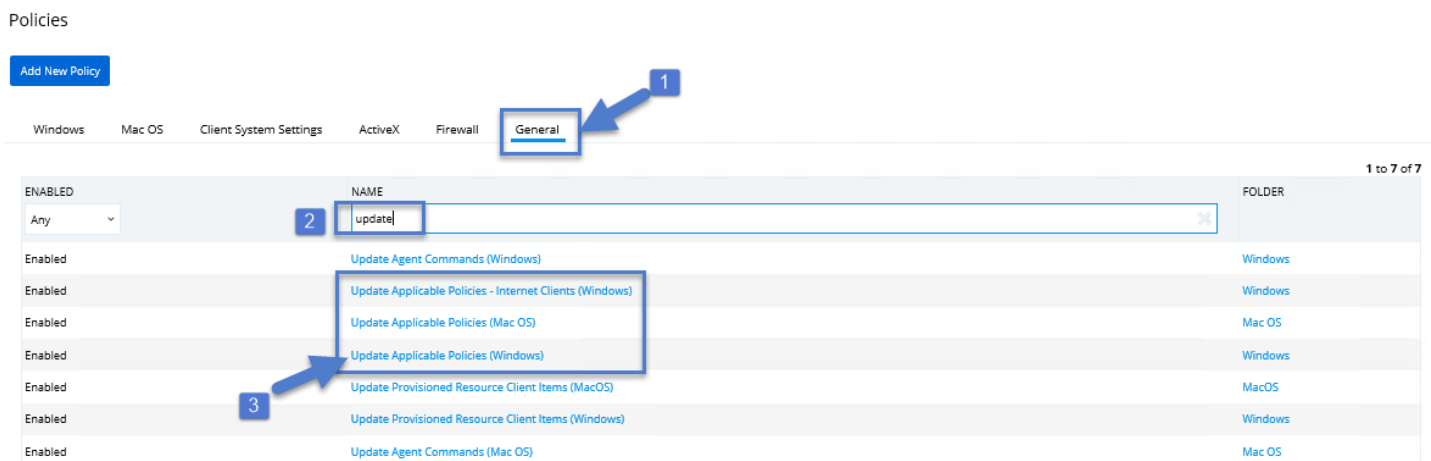
<b>File Name</b>	New Loaded Resource 1/10/2018 6:59:44 AM
<b>File Hashes</b>	sha1: 39fabd70efd9b7c11b768012a3a472b254dd778c <a href="#">View more details at VirusTotal.com</a>
<b>Discovery Status</b>	Pending assignment <span>🔔</span>

[Back](#)[Delete](#)[Discover Now](#)

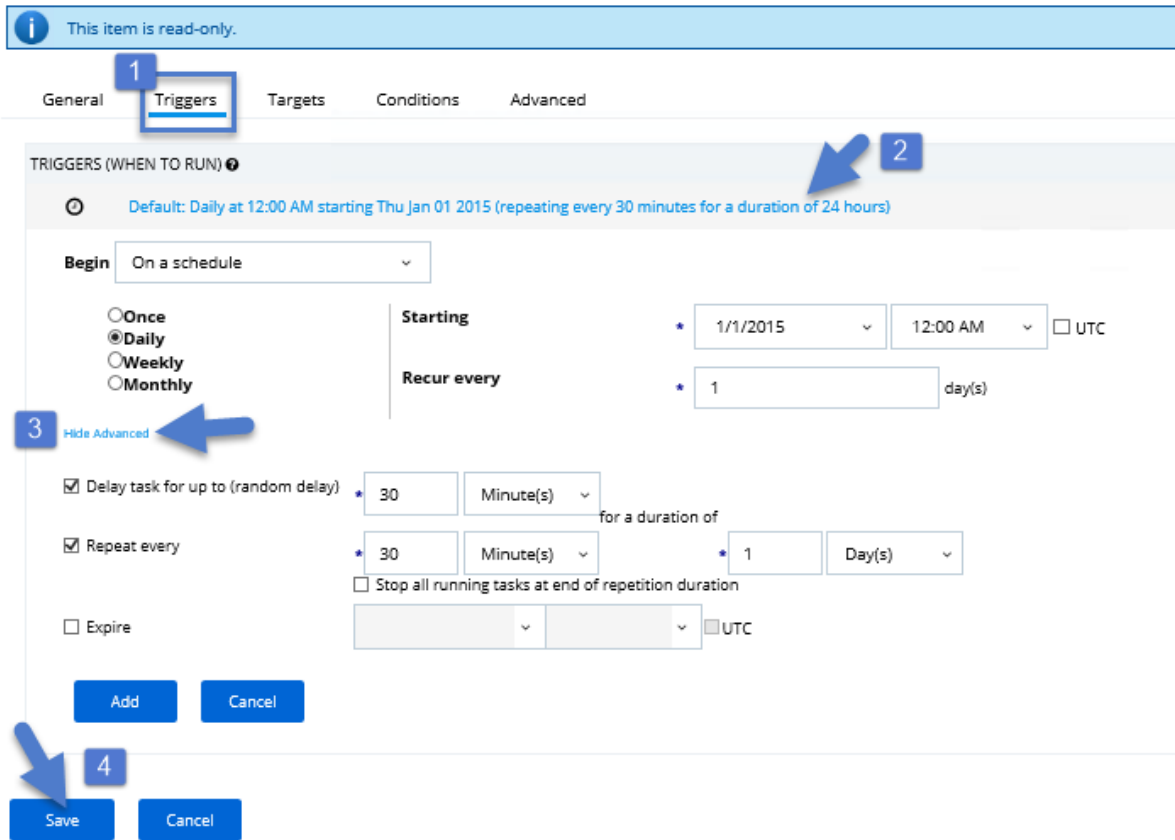
# Sending Policies to Endpoints

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:

General   Conditions   Actions   Policy Enforcement   **Deployment**

**Policy Deployment**  
Policies are automatically deployed to targeted managed computers on a schedule. Use the Policy Deployment tab to understand the status of a particular Policy in relation to the end points.

Refresh

Policy Cached on Server	True
Policy Modified	Jan 10, 2018, 12:46:54 PM
Policy Last Cached	Jan 10, 2018, 12:47:01 PM
<b>Total Resources Targeted</b>	<b>1</b>
<b>Resources with Policy</b>	<b>1</b>
<b>Resources with Latest Version</b>	<b>1</b>

Back   Edit   Disable   Create a Copy   See Events

## 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**.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd "C:\Program Files\Thycotic\Powershell\Arellia.Agent"
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> .\UpdateClientItems.ps1
```

Your results look something like this:

```
=====  
Client Items  
=====  
Refreshing Agent Commands: 8/18 client items  
Refreshing Agent Gauges: 0 client items  
Refreshing Agent Policies: 23/68 client items  
Refreshing Application Actions: 9/42 client items including 2 new item(s)  
  
* Added: Quarantine Message  
* Added: File Quarantine  
  
Refreshing File Filters: 23/210 client items  
Refreshing Provisioned Resources: 0 client items  
Refreshing Scap Entities: 0 client items  
Refreshing Windows Group Policies: 0/1 client items  
Refreshing Windows Group Policy Settings: 0 client items  
  
=====  
Policies  
=====  
  
(+) Added : Blacklist + Quarantine  
  
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> _
```

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.

Thycotic Powershell Log Viewer

Logs Settings

Modules: [All] Filter:

Error  Warning  Information  Trace

TimeGenerated	Message	Source	Module
10/08/2017 14:15:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:16:51 PM	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:15:51	Performing ACS ProcessEvents	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:14:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:15:51 PM	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:14:51	Performing ACS ProcessEvents	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:56	Received SSL Policy error for CN=DemoMain : RemoteCertificateChainErrors	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:56	The Thycotic Agent configured certificate B48F7B048559A38B3E808124EAB3001500BEE6D5 is invalid. The certfic...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:52	The Thycotic Agent configured certificate B48F7B048559A38B3E808124EAB3001500BEE6D5 is invalid. The certfic...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:52	Completed Taskinstance f19311c0-00af-4401-804e-f3c21c91db7e - Client Command 'Resource Discovery Command' ...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:52	Resource discoverer 0120439e-2ffb-422e-bbdb-f3e668534788 did not return any discoveryXml	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:52	Unable to locate a file with hash f1szTn2LViBO6pk3oGwBWmIAOb4= for Resource {7F5B334E-7D8B-5620-8EEA-99...	CFileResourceDisc...	ArelliaFileInvAgent.dl...
10/08/2017 14:13:52	Received SSL Policy error for CN=DemoMain : RemoteCertificateChainErrors	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:14:51 PM	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:51	Performing ACS ProcessEvents	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:51	Initiating taskinstance f19311c0-00af-4401-804e-f3c21c91db7e with clientCommandId 'Resource Discovery Command...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:47	Queued Task f19311c0-00af-4401-804e-f3c21c91db7e - Command 'Resource Discovery Command' (77582ef2-bd52-...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:12:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:13:51 PM	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:12:51	Performing ACS ProcessEvents	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:11:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:12:51 PM	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:11:51	The Thycotic Agent configured certificate B48F7B048559A38B3E808124EAB3001500BEE6D5 is invalid. The certfic...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:11:51	Performing ACS ProcessEvents	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:11:47	Policy 'Event Discovery Testing Computers Audit Policy (Windows)' (398d5118-13ad-4425-9877-b513bc4903db) (prios...	CASMonitor	ArelliaACSvc.exe

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**.

New Policy

Platform	* Windows
Policy Type	* Show All Templates
Template Type	* Other: Empty Policy
Name	* Whitelist Microsoft Security Catalog
Description	* This policy will allow applications from the Microsoft Security Catalog to run



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**.



**Warning:** This policy is not enabled. Managed computers won't receive this policy until it is enabled.

General | **Conditions** | Actions | Policy Enforcement | Deployment

Select the applications to control along with any optional criteria.

**Warning:** When no filters are chosen, the policy applies to **ALL** applications.

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

Add Application Target

INCLUSION FILTERS (OPTIONAL, ONLY APPLIES WHEN ALL MATCH)

ADD INCLUSION FILTER

Select an Inclusion Filter from the tree or use the [Filter](#) page to define more Filters.

View by:

<input type="checkbox"/>	NAME	TYPE	FOLDER
<input type="checkbox"/>	Executables in Windows Directories not present in Security Cat...	File Specification Filter	File Specifications (Windows)
<input type="checkbox"/>	Executables in Windows Directories not present in Security Cat...	File Specification Filter	File Specifications (Windows)
<input type="checkbox"/>	Manifest Present Filter	Manifest Filter	Manifest
<input type="checkbox"/>	Outlook Express	Win32 Exe Filter	Mail Clients
<input checked="" type="checkbox"/>	Present In Signed Security Catalog	Security Catalog Filter	Security Catalogs

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

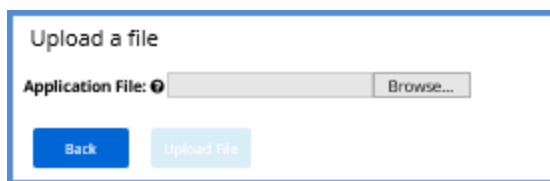
No action is required to add under the **Actions** tab, meaning that these items will be *Whitelisted* – i.e. they will be allowed to run with default permissions.

### 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**.


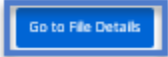


Click **Browse**, and select a file to upload. Click **Upload File**.

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

Upload a file






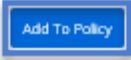
 

3. Click **Add to Policy**.

Resource Explorer > ChromeSetup.exe

Summary	
Known Data	
Events	
Associations	

<b>File Name</b>	ChromeSetup.exe
<b>Original File Name</b>	GoogleUpdateSetup.exe
<b>Product Name</b>	Google Update
<b>Version</b>	1.3.33.3
<b>Internal Name</b>	Google Update Setup
<b>Company Name</b>	Google Inc.
<b>Copyright</b>	Copyright 2007-2010 Google Inc.
<b>File Hashes</b>	Authenticode 2: 545fb11225400a97c91994481683e38c62257e75858bef99ce399c959825e96e md5: 1d7632b1c0a212b2e594104bcf25970a sha256: c1ccabfde7d9e739e78c4012bb5a4270dd66bcb359661b5bca8d1006f0dc2386a sha1: 22b20271ac7e04c182966067123eeefcd53b7a3d <a href="#">View more details at VirusTotal.com</a> Authenticode: 2ddec6e1d8af7d41baf4de749abbbfb3f5973

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**.

## Add New Policy

Create a new Policy targeted by the options selected below. A new Filter will be created that can also be used in conditions for other Policies. After the Policy is created it will need to be targeted at Managed Computers in order to be applied.

**Policy Options**

Add New Filter To:

Policy Type:

Name:

Description:

**Filter Options**

File Name:

Path:

Internal Name:

Original File Name:

File Version:

Product Name:

Product Version:

Company Name:

File must be signed by:

- 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.

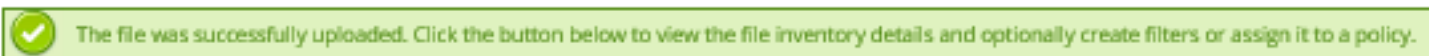
### Example: Blacklist iTunes with File Upload

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**.

#### Upload a file





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**.

New Policy

Platform Windows

Policy Type Blacklist / Deny Application Execution

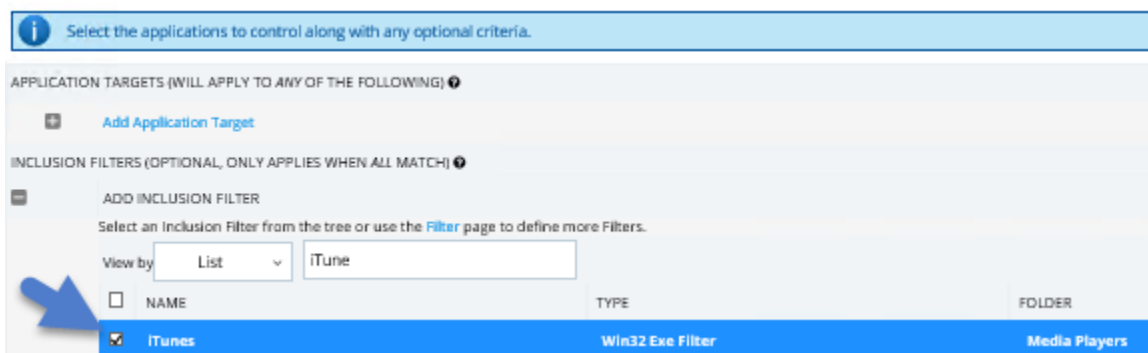
Template Type Blacklist: Deny Specific Applications

Name Block iTunes

Description This policy prevents iTunes from running.

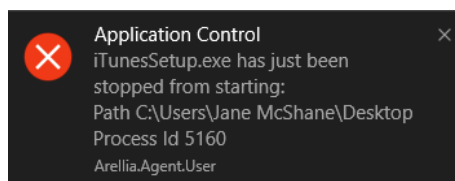
Back Create

- In the **Advanced Policy View** under the **Conditions** tab, select **Edit**, then **Add Inclusion Filter**.
- Select your iTunes filter/s, click **Add**, then **Save**.



- 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**.

## Filter > Malware Example

Details    Related Items

---

**Details**

<b>Name</b>	Malware Example
<b>Description</b>	This filter targets an example malware application
<b>Platform</b>	Windows

---

**File Specifications**


Enter criterion for this filter. This filter can be based on file names, location and/or file detail properties.

<b>File Name</b>	malware.exe
<b>File Path</b>	<input type="checkbox"/> Include subdirectories
<b>First Discovered</b>	<input checked="" type="radio"/> Anytime <input type="radio"/> In the last 0 minute(s)


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.


## Policy > Quarantine Malware Example


 This policy is not enabled. Managed computers won't receive this policy until it is enabled.

General **Conditions** Actions Policy Enforcement Deployment

 Select the applications to control along with any optional criteria.

 When no filters are chosen, the policy applies to **ALL** applications.

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING) 

 ADD APPLICATION TARGET


Select an Application Target from the folders below. Use the [Application Target](#) page to define more.



View by


<input type="checkbox"/>	NAME	TYPE	FOLDER
<input checked="" type="checkbox"/>	Malware Example	Win32 Exe Filter	Windows Filters



- 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:

C:\Users\Jane McShane\Desktop\malware.exe

 Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

 Calculator

 Application Control   
**malware.exe** has been quarantined.  
Arellia.Agent.User

# 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**

New Filter

Filter Details

Platform: Windows

Filter Type: File Specification Filter

Name: Fileshare

Description: Elevates files from team Fileshare

Buttons: Back, Create

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

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names: Fileshare

Path: \\Server\FileshareLocationPath

Drive Types:

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Second, create a New Policy:

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



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

New Policy

Platform: Windows

Policy Type: Show All Templates

Template Type: Other: Empty Policy

Name: Elevate Fileshare

Description: This policy will elevate all applications in Fileshare to have administrator rights

Back Create

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

General Conditions Actions Policy Enforcement Deployment

Select the applications to control along with any optional criteria.

When no filters are chosen, the policy applies to **ALL** applications.

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

Add Application Target

INCLUSION FILTERS (OPTIONAL, ONLY APPLIES WHEN ALL MATCH)

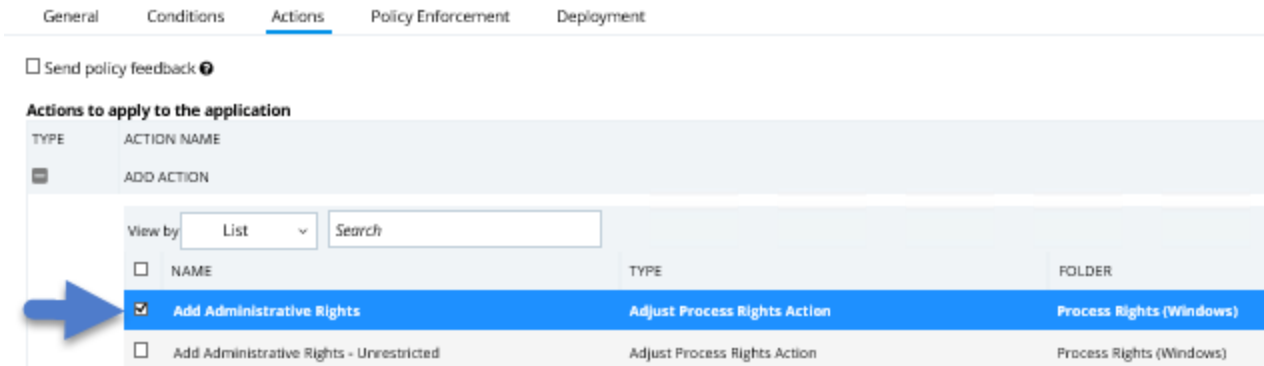
ADD INCLUSION FILTER

Select an Inclusion Filter from the tree or use the [Filter](#) page to define more Filters.

View by: List Fileshare

<input type="checkbox"/>	NAME	TYPE	FOLDER
<input checked="" type="checkbox"/>	Fileshare	File Specification Filter	Windows Filters

- 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**.

**New Filter**

---

Filter Details

<b>Platform</b>	* Windows
<b>Filter Type</b>	* Blank Win32 Executable Filter
<b>Name</b>	* Calculator
<b>Description</b>	This filter targets the Calculator <i>calc.exe</i> application

← Back
📄 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**.

**New Policy**

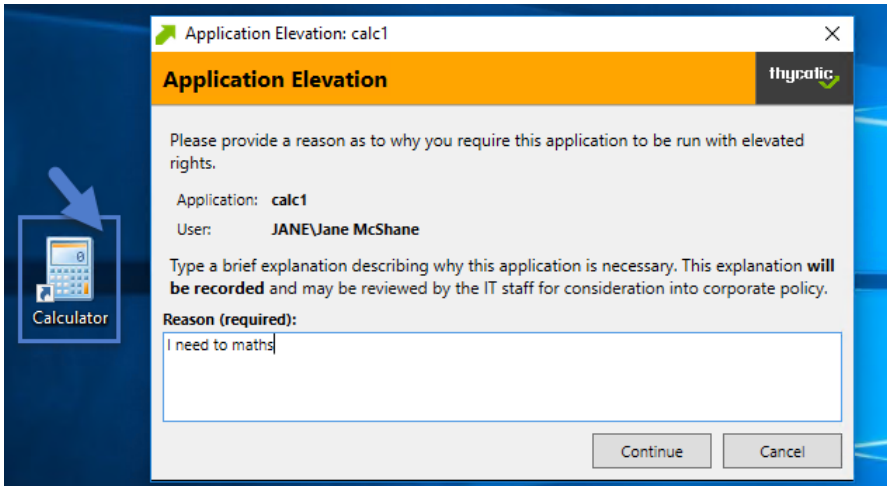
Platform	* Windows ▾
Policy Type	* Show All Templates ▾
Template Type	* Elevate: Add Administrator Rights to Specific Applications with Justification ▾
Name	* Y-U-Calculating?
Description	* This policy elevates the security rights for the calculator application after the user provides a reason for doing math

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**.

**File Specifications**

Enter criterion for this filter. This filter can be based on file names, location and/or file detail properties.

**File Name**

**File Path**

**First Discovered**

Include subdirectories

Anytime

In the last

minute(s)

---

**File Details**

To only match files with specific properties in the file details, enter those values in the fields below. A wildcard character (\*) is allowed only at the end. All values specified must match the file detail for the file to be included in the set.

**Internal name**

**Original filename**

**File version**

**Product name**

**Product version**

**Company name**

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**.

**New Policy**

**Platform** \*

**Policy Type** \*

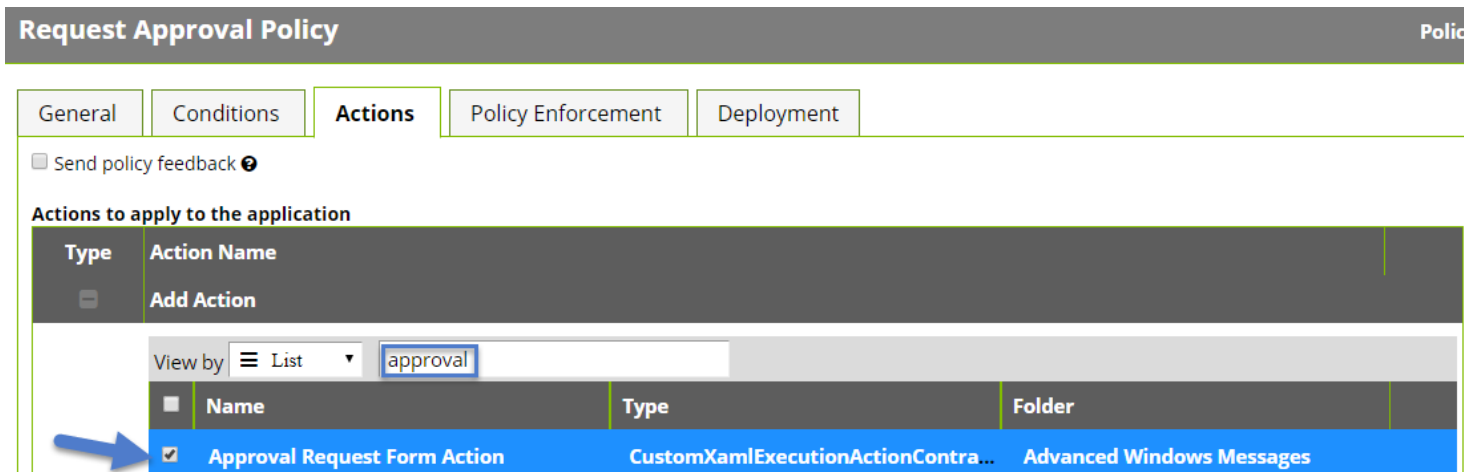
**Template Type** \*

**Name** \*

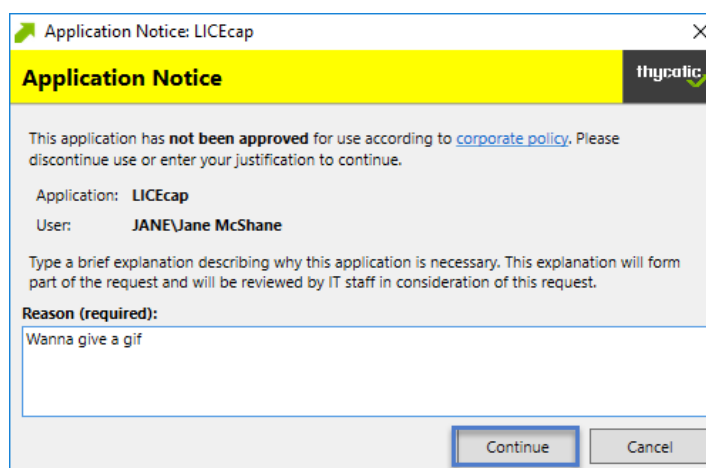
**Description** \*

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**.



- 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:

- 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**.

Thycotic Privilege Manager Search Items Search HOME TOOLS ADMIN REPORTS

### Manage Approval Requests

Review actions that are awaiting approval.

Refresh Approve Deny

Showing 1 to 1 of 1

Policy	User	User Reason	Requested
Request Approval Policy	JANE\Jane McShane	Wanna give a gif	August 10, 2017, 7:09 PM

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.

Application Notice: LICCap

### Application Notice

This application has **not been approved** for use according to [corporate policy](#). Please discontinue use or enter your justification to continue.

Application: LICCap  
User: JANE\Jane McShane

A previous request for this application has been submitted for review.

Approval status: **Approved**

Refresh Continue Cancel

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.

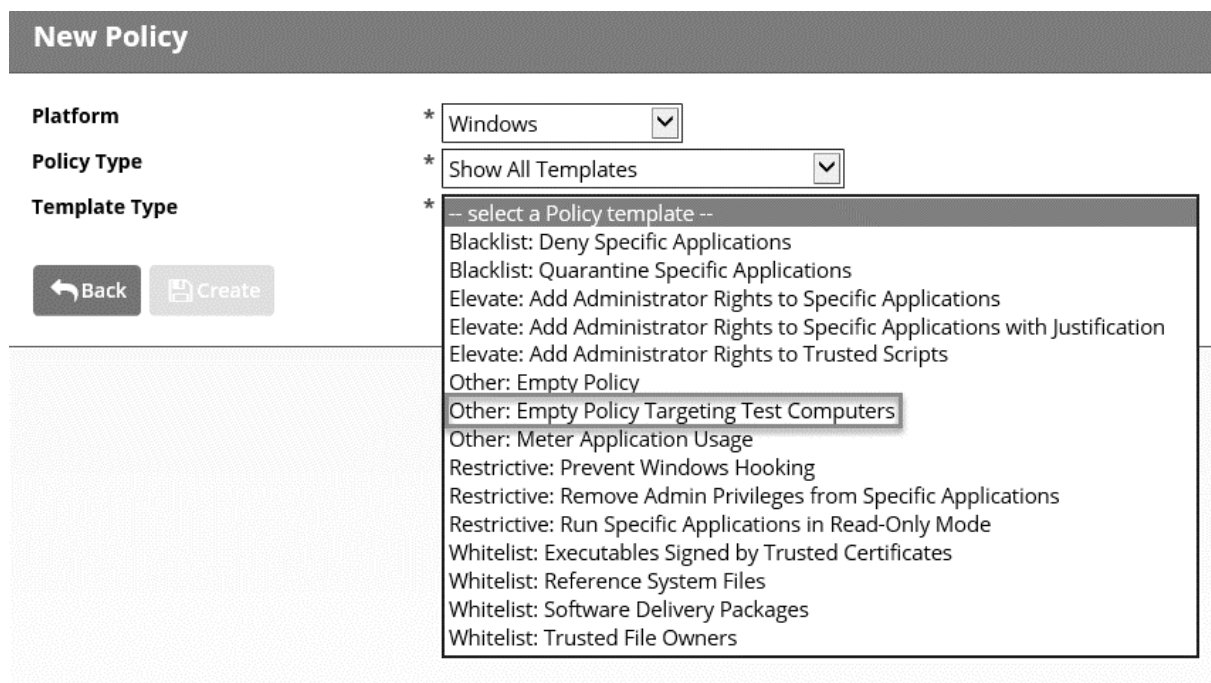
# Greylisting Policies

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:

**Catch-All Application Execution Policy**

General | **Conditions** | Actions | Policy Enforcement | Deployment

**Application Targets** (Will apply to *any* of the following) ⓘ

- Interactive Users

**Exclusion Filters** (Optional, does not apply when *any* match) ⓘ

- LocalSystem and Service applications
- Present in Signed Security Catalog

**Resource Targets** (Applied to these Managed Computers) ⓘ

- All Windows Computers with Application Control Agent Installed (Target)

← Back | Edit | Create a Copy | Delete | See Events

### Actions:

**Catch-All Application Execution Policy**

General | Conditions | **Actions** | Policy Enforcement | Deployment

Send policy feedback ⓘ

**Actions to apply to the application**  
No actions are currently being applied.

**Actions to apply to the child applications**  
 Use the same actions as the parent

← Back | Edit | Create a Copy | Delete | See Events

### Policy Enforcement:

## Catch-All Application Execution Policy

General	Conditions	Actions	<b>Policy Enforcement</b>	Deployment
---------	------------	---------	---------------------------	------------

Determine how this Policy is enforced.

- Continue enforcing policies after enforcing this policy ⓘ
- Continue enforcing policies for child processes after enforcing this policy ⓘ
- Stage 2 processing ⓘ
- Applies to all processes ⓘ

[← Back](#) [✎ Edit](#) [📄 Create a Copy](#) [🗑 Delete](#) [📅 See Events](#)

## 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](#) section of this User Guide. That section walks you how to do the following:

section of this User Guide. That section

- 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**.

### New Policy

Platform \* Windows

Policy Type \* Show All Templates

Template Type \* Other: Empty Policy

Name \* Deny Applications - VirusTotal Rating

Description \* Prevents applications flagged by VirusTotal as bad

[← Back](#) [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**.

Application Targets (Will apply to *any* of the following)

**Add Application Target**

Select an Application Target from the folders below. Use the [Application Target](#) page to define more.

View by  List  vir

Name	Type	Folder
<input type="checkbox"/> Manual Application Compatibility Setting	Environment Filter	Environment Variables
<input type="checkbox"/> User Access Control Consent Dialog Detected	Environment Filter	Environment Variables
<input type="checkbox"/> User Requested Run As Administrator	Environment Filter	Environment Variables
<input checked="" type="checkbox"/> <b>VirusTotal</b>	<b>Security Rating Filter</b>	<b>Windows Filters</b>

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**.

## Search

### Number of Results

5000

### Role Type Name (3)

File Specification Filter (1)

Win32 Exe Filter (1)

Secondary File Filter (1)

Showing 1 to 3 of 3

#### User's Temp Directory File Specification Filter

8/7/2017 - File Specification Filter

Used to target any file in the user's temp directory

#### User's Temp Directory Win32 Executable Filter

8/7/2017 - Win32 Exe Filter

Used to target any executable (.exe) in a user's temp directory

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** field to the following: (c:\\users\\[^\\]+\\downloads). **Save** your changes.

## User's Downloads Temp Directory File Specification Filter

### Details

### Related Items

#### Details

##### Name

\* User's Downloads Directory File Specification Filter

##### Description

Used to target any file in the user's temp directory

#### Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

##### File Names

##### Path

(c:\\users\\[^\\]+\\downloads)

##### Drive Types

- Unknown type
- No Root Directory
- Removable Drive (Floppy/USB)

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.

**Deny Applications – VirusTotal Rating**

General | **Conditions** | Actions | Policy Enforcement | Deployment

Select the applications to control along with any optional criteria.

**Application Targets** (Will apply to *any* of the following) ⓘ

VirusTotal

+ Add Application Target

**Inclusion Filters** (Optional, only applies when *all* match) ⓘ

+ Add Inclusion Filter

Select an Inclusion Filter from the tree or use the Filter page to define more Filters.




View by ☰ List user's






Name	Type	Folder
<input type="checkbox"/> Target MSI and Scripts executed from the User's Temp Direct...	Secondary File Filter	Secondary File
<input checked="" type="checkbox"/> <b>User's Directory Collection File Specification Filter</b>	<b>File Specification Filter</b>	<b>Common Windows Directories</b>
<input type="checkbox"/> User's Downloads Directory File Specification Filter	File Specification Filter	Common Windows Directories
<input type="checkbox"/> User's Temp Directory File Specification Filter	File Specification Filter	Common Windows Directories
<input type="checkbox"/> User's Temp Directory Win32 Executable Filter	Win32 Exe Filter	My Filters

Add Cancel

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.

## Deny Applications – VirusTotal Rating

General	<b>Conditions</b>	Actions	Policy Enforcement	Deployment
<b>Application Targets</b> (Will apply to <i>any</i> of the following) ⓘ				
 <a href="#">VirusTotal</a>				
<b>Inclusion Filters</b> (Optional, only applies when <i>all</i> match) ⓘ				
 <a href="#">User's Directory Collection File Specification Filter</a>				
<b>Resource Targets</b> (Applied to these Managed Computers) ⓘ				
 <a href="#">All Windows Computers with Application Control Agent Installed (Target)</a>				

 Back  Edit  Create a Copy  Delete  See Events

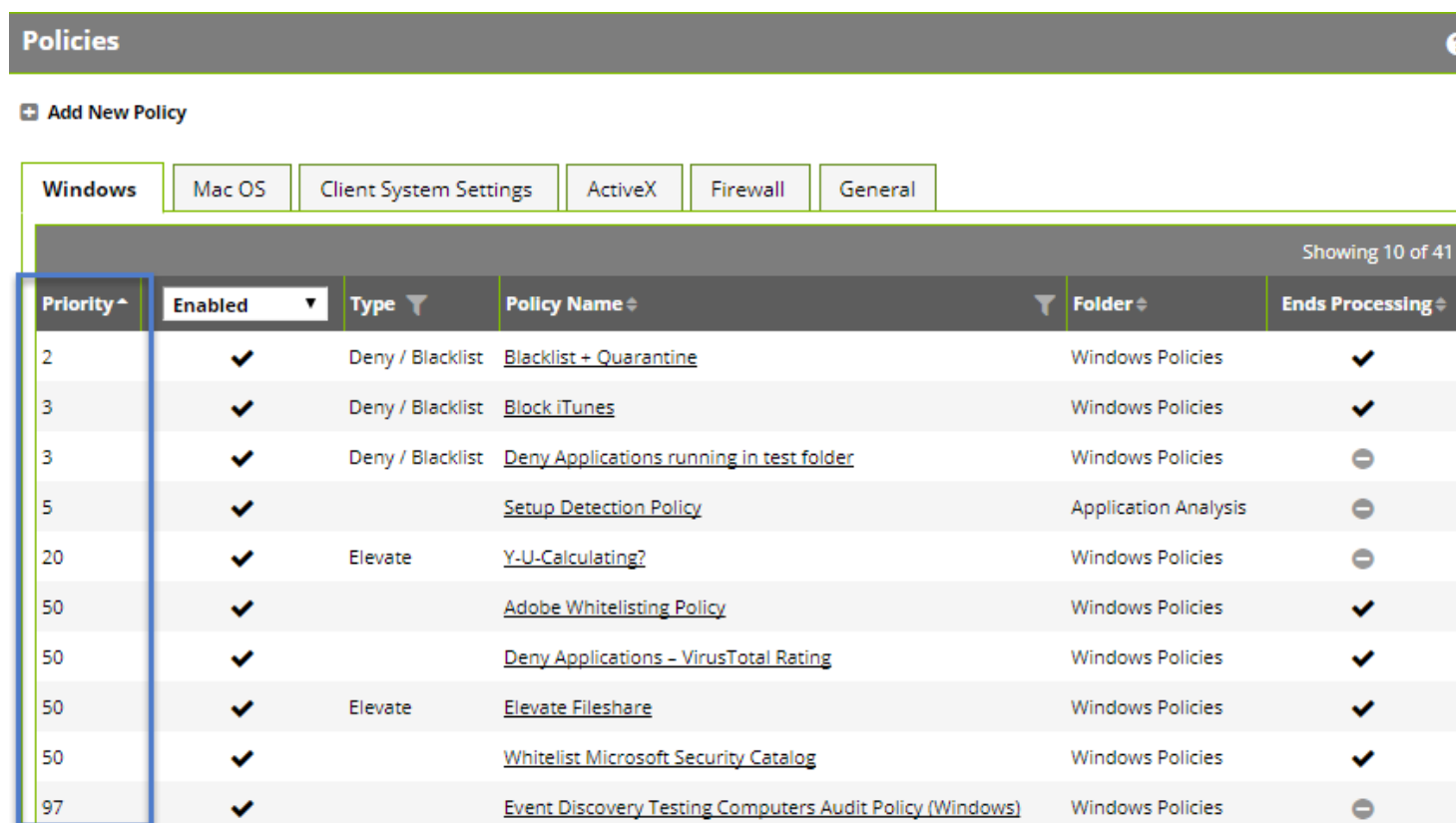
NOTE: This policy sends any application that is run from the user's Downloads or Temp directory to VirusTotal for a reputation check-in real time. If the application is graded with [Bad](#) from VirusTotal, the application will be denied.

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.



The screenshot shows the 'Policies' screen in Privilege Manager. At the top, there is a header 'Policies' and a button '+ Add New Policy'. Below the header, there are tabs for 'Windows', 'Mac OS', 'Client System Settings', 'ActiveX', 'Firewall', and 'General'. The 'Windows' tab is selected. The main area displays a table of policies. The table has columns for 'Priority', 'Enabled', 'Type', 'Policy Name', 'Folder', and 'Ends Processing'. The 'Priority' column is highlighted with a blue box. The table shows 10 policies, with the first three having a priority of 2, 3, and 3, and the rest having higher priorities (5, 20, 50, 50, 50, 97). The 'Ends Processing' column shows checkmarks for some policies and minus signs for others.

Priority ^	Enabled	Type	Policy Name	Folder	Ends Processing
2	✓	Deny / Blacklist	<a href="#">Blacklist + Quarantine</a>	Windows Policies	✓
3	✓	Deny / Blacklist	<a href="#">Block iTunes</a>	Windows Policies	✓
3	✓	Deny / Blacklist	<a href="#">Deny Applications running in test folder</a>	Windows Policies	⊖
5	✓		<a href="#">Setup Detection Policy</a>	Application Analysis	⊖
20	✓	Elevate	<a href="#">Y-U-Calculating?</a>	Windows Policies	⊖
50	✓		<a href="#">Adobe Whitelisting Policy</a>	Windows Policies	✓
50	✓		<a href="#">Deny Applications - VirusTotal Rating</a>	Windows Policies	✓
50	✓	Elevate	<a href="#">Elevate Fileshare</a>	Windows Policies	✓
50	✓		<a href="#">Whitelist Microsoft Security Catalog</a>	Windows Policies	✓
97	✓		<a href="#">Event Discovery Testing Computers Audit Policy (Windows)</a>	Windows Policies	⊖

## Example: Why Policy Priority Matters

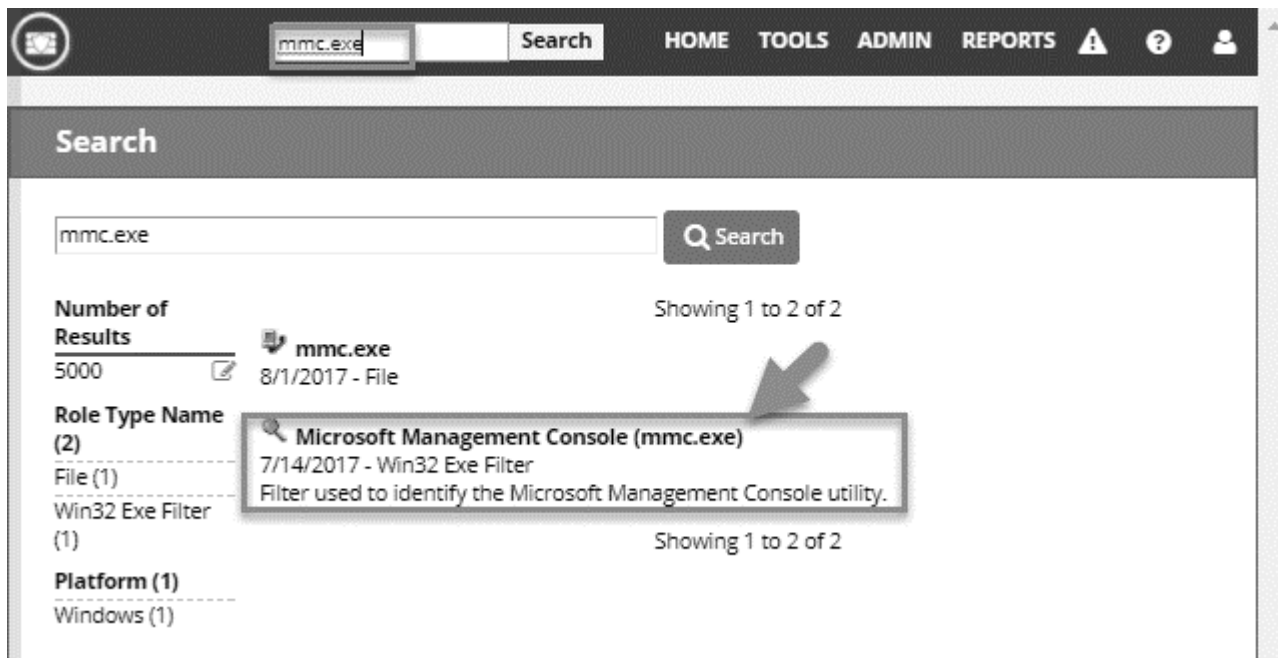
To illustrate the way policies are applied in order, this use case defines two policies to **1) block MMC.EXE**, but **2) allow a specific MMC Snap-in**.

### 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.)




## Deny Launching MMC Console Application Control Policy


**General** | Conditions | Actions | Policy Enforcement | Deployment


**Policy Name** \* Deny Launching MMC Console Application Control Policy

**Description** \* This policy will deny mmc.exe files

**Platform Type** Windows

**Folder**  Windows Policies

**Enabled**  


**Policy Priority** \* 50 


3. Click the **Conditions** tab.


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


## Deny Launching MMC Console Application Control Policy

**General** | **Conditions** | Actions | Policy Enforcement | Deployment


 Select the applications to control along with any optional criteria.


 When no filters are chosen, the policy applies to **ALL** applications.

**Application Targets** (Will apply to *any* of the following) 

 **Add Application Target**

Select an Application Target from the folders below. Use the [Application Target](#) page to define more.

View by  List

	Name	Type	Folder
<input checked="" type="checkbox"/>	Microsoft Management Console (mmc.exe)	Win32 Exe Filter	System Utilities

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

## Deny Launching MMC Console Application Control Policy

Policy

General | **Conditions** | Actions | Policy Enforcement | Deployment

Select the applications to control along with any optional criteria.

**Application Targets** (Will apply to *any* of the following)

- Microsoft Management Console (mmc.exe)
- Add Application Target

**Inclusion Filters** (Optional, only applies when *all* match)

- Add Inclusion Filter

**Exclusion Filters** (Optional, does not apply when *any* match)

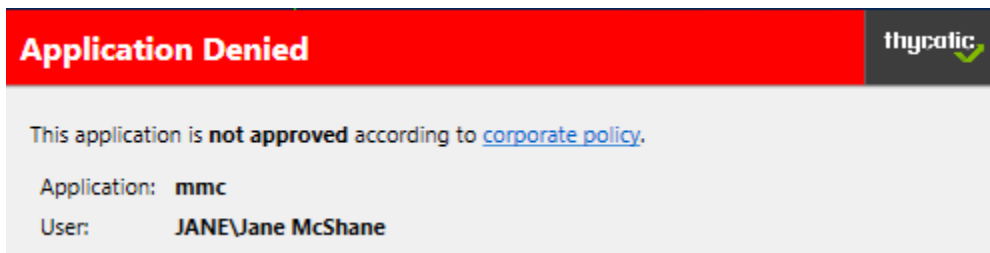
- Administrators (Include Disabled)
- Add Exclusion Filter

**Resource Targets** (Applied to these Managed Computers)

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

- 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.)

**Allow Print Management Plug-in Application Control Policy**

**General** | Conditions | Actions | Policy Enforcement | Deployment

**Policy Name** \* Allow Print Management Plug-in Application Control Policy

**Description** \* This policy will allow the print management Plug-in

**Platform** Windows

**Type**

**Folder** Windows Policies

**Enabled**

**Policy Priority** \* 49

Save Cancel

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.

**Application Targets** (Will apply to *any* of the following) ⓘ

[Microsoft Management Console \(mmc.exe\)](#)

[Add Application Target](#)

---

**Inclusion Filters** (Optional, only applies when *all* match) ⓘ

**Add Inclusion Filter**

Select an Inclusion Filter from the tree or use the [Filter](#) page to define more Filters.

View by List

<input type="checkbox"/>	Name	Type	Folder
<input type="checkbox"/>	Add Printer Commandline Arguments	Commandline Filter	System Utility Arguments
<input type="checkbox"/>	Printer Control Utility (printui.exe)	Win32 Exe Filter	System Utilities
<input checked="" type="checkbox"/>	printmanagement.msc Commandline Fil...	Commandline Filter	MMC Snap-Ins

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:

Priority ^	Enabled ▾	Type ▾	Policy Name ⇅	Folder ⇅	Ends Processing
2	✓	Deny / Blacklist	<a href="#">Blacklist + Quarantine</a>	Windows Policies	✓
3	✓	Deny / Blacklist	<a href="#">Deny Applications running in test folder</a>	Windows Policies	⊖
3	✓	Deny / Blacklist	<a href="#">Block iTunes</a>	Windows Policies	✓
5	✓		<a href="#">Setup Detection Policy</a>	Application Analysis	⊖
20	✓	Elevate	<a href="#">Y-U-Calculating?</a>	Windows Policies	⊖
49	✓	Elevate	<a href="#">Allow Print Management Plug-in Application Control Policy</a>	Windows Policies	✓
50	✓		<a href="#">Deny Launching MMC Console Application Control Policy</a>	Windows Policies	✓
50	✓	Elevate	<a href="#">Elevate Fileshare</a>	Windows Policies	✓
50	✓		<a href="#">Deny Applications - VirusTotal Rating</a>	Windows Policies	✓
50	✓		<a href="#">Adobe Whitelisting Policy</a>	Windows Policies	✓
97	✓		<a href="#">Event Discovery Testing Computers Audit Policy (Windows)</a>	Windows Policies	⊖

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.

### Windows Privilege Personas

 Personas are a defined set of privileges for a specific role. Users are assigned a persona on a specific resource target or computer that will elevate their identity to perform specific tasks.

[Add New Persona](#)

ENABLED	NAME	DESCRIPTION
Any	Filter	
NO	SQL Administrators Persona	This persona automatically elevates applications that are commonly needed to manage SQL servers.

## 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.

Persona > Network Administrators Persona

**Settings**

**Name** Network Administrators Persona

**Description** This persona automatically elevates applications that are commonly needed to manage network configuration settings.

**Enabled**

**Behaviors**

NAME	PARAMETERS
Elevate NLB Configuration	No additional parameters
Elevate Specific MMC Snap-ins Privilege	Allow DHCP (dhcplmgmt.msc) Allow DNS Configuration (dnsmgmt.msc)

**Add Behavior**

**Select privilege type**

- select a privilege template –
- Elevate Adding Inbound TCP Firewall Rule Privilege
- Elevate App Pool Recycling via AppCmd Recycle
- Elevate Disk Defrag
- Elevate IIS Manager (inetmgr.exe) Privilege
- Elevate IISReset Privilege
- Elevate ISCSI Connection Configuration
- Elevate NLB Configuration
- Elevate ODBC Configuration
- Elevate Specific MMC Snap-ins Privilege

**Targets**

COMPUTER COLLECTIONS

DOMAIN USER GROUPS

This Persona does not have any targets. To

**Add Target**

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.

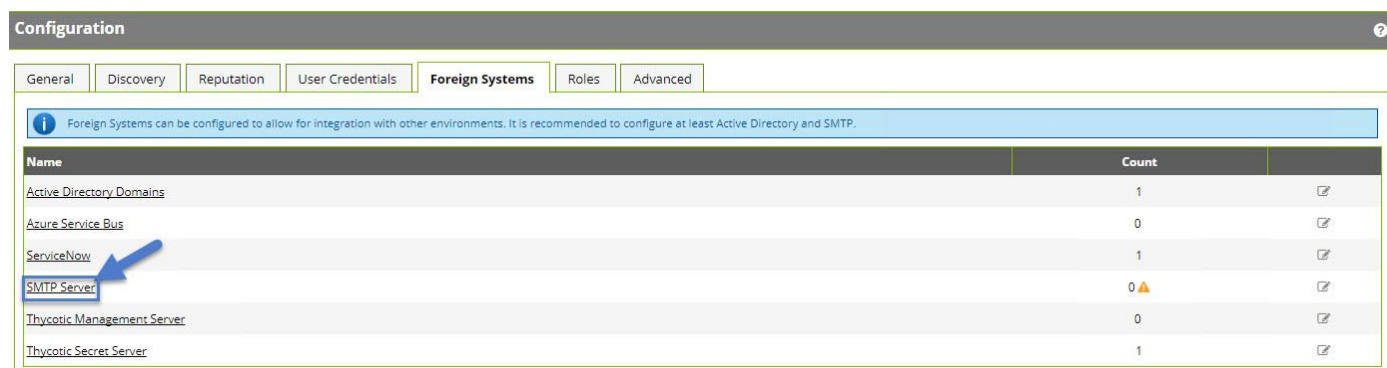
# Integrations

## 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**.

### Manual Approval Process with E-mail Alerts

Details

Name \* Manual Approval Process with E-mail Alerts

Description

---

Settings

Approval role allowed ⓘ TMS Administrators

Start activity ⓘ Send E-mail for New Approval Task

Activity parameters

Report To Run \* Most Recent Pending Application Approval Request

From Address \* approvalrequests@companyname.com

To Address \* username@companyname.com; username2@companyname.com; username3@companyname.com

SMTP Server

[View Parameters](#)

- \* Test Email
- \*  SSL Enabled

## 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, sign up at [virustotal.com](https://www.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/>, 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/>. On the Currently Installed Products screen, choose **Install/Upgrade Products**.

### Currently Installed Products

Product Name	Installed	Available	Published	
<a href="#">Thycotic Application Control Solution</a>	10.3.1015	10.3.1015	7/12/2017 7:31 AM	Repair
<a href="#">Thycotic Directory Services Connector</a>	10.3.1003	10.3.1003	7/12/2017 7:31 AM	Repair
<a href="#">Thycotic File Inventory Solution</a>	10.3.1010	10.3.1012 New	8/1/2017 9:53 AM	Upgrade
<a href="#">Thycotic Management Server Core Solution</a>	10.3.1092	10.3.1092	7/12/2017 7:31 AM	Repair
<a href="#">Thycotic Privilege Manager</a>	10.3.1043	10.3.1043	7/12/2017 7:31 AM	Repair
<a href="#">Thycotic RDP Monitor Solution</a>	10.3.1001	10.3.1001	7/12/2017 7:31 AM	Repair

Install/Upgrade Products Refresh

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

### Select Products to Install

Thycotic File Inventory Solution 10.3.1012 Required i Show installed products

Thycotic Local Security Solution 10.3.1004 i

Thycotic Management Server Silverlight Console 10.3.1033 i

Thycotic Mobile Console Solution 10.3.1003 i

Thycotic Security Analysis Solution 10.3.1002 i

Thycotic Symantec Management Platform Connector 10.3.1001 i

Thycotic SysLog Connector 10.3.1002 i

Thycotic System Center Configuration Manager Connector 10.3.1001 i

Thycotic VirusTotal Reputation Connector 10.3.1012 i

Install Refresh

### Installation Progress

✓ Thycotic VirusTotal Reputation Connector

---

**Complete** 1 minute 10 seconds

Setup completed successfully. You can go back to the Home page and launch the console.

Home

[Show Install Log](#)

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

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

**Configuration**

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

**User Credentials**

+ User Credential

Name	Description	Last Modified By
<a href="#">Default Proxy Server User Credential</a>	Proxy Server User Credential	Principal Self Well Known Group
<a href="#">Default User Credential</a>	Default User Credential	Principal Self Well Known Group
<a href="#">VirusTotal API Key</a>	Credential for the VirusTotal API Key	admin

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

**Details**

Details

Name \* VirusTotal API Key

Description Credential for the VirusTotal API Key

Settings

Account Name VirusTotal API Key

Password .....

Confirm Password .....

Save Cancel

Next, create a Security Rating Filter for VirusTotal:

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

**New Filter**

Filter Details

Platform \* Windows

Filter Type \* Security Rating Filter

Name \* VirusTotal

Description This filter will target VirusTotal for Reputation Checking

Security rating system  
[View Parameters](#)  
 \* VirusTotal Rating System

[Back](#) [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**.

**Select Products to Install**

Thycotic Application Control Solution 10.3.2021 New ⓘ

Thycotic Local Security Solution 10.3.1004 ⓘ

Thycotic Management Server Core Solution 10.3.2102 Required ⓘ

Thycotic Management Server Silverlight Console 10.3.2055 Required ⓘ

Thycotic Mobile Console Solution 10.3.1003 ⓘ

Thycotic Privilege Manager 10.3.2055 New ⓘ

Thycotic ServiceNow Connector 10.3.1010 ⓘ

Thycotic SysLog Connector 10.3.1002 ⓘ

Thycotic System Center Configuration Manager Connector 10.3.1001 ⓘ

Thycotic VirusTotal Reputation Connector 10.3.2021 New ⓘ


[Install](#) [Refresh](#) [Show installed products](#)

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

**Configuration**

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

User Credentials


+ User Credential 

Name	Description	Last Modified By
<a href="#">Default Proxy Server User Credential</a>	Proxy Server User Credential	Principal Self Well Known Group
<a href="#">Default User Credential</a>	Default User Credential	Principal Self Well Known Group
<a href="#">js.lab.domain</a>	sync admin	SSadmin
<a href="#">ServiceNow</a>	ServiceNow Sync Creds	SSadmin

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**.

**Configuration**


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

 Foreign Systems can be configured to allow for integration with other environments. It is recommended to configure at least Active Directory and SMTP.

**Name**

[Active Directory Domains](#)

[Azure Service Bus](#)

[ServiceNow](#) 

[SMTP Server](#)

[Thycotic Management Server](#)

[Thycotic Secret Server](#)

Thycotic 10.3 Privilege Manager

Search Items  Search

HOME TOOLS ADMIN REPORTS

### ServiceNow Server

Details

Name ServiceNow Server  
Description ServiceNow Server

Settings

Credential ServiceNow  
Uri https://[redacted].service-now.com/

Back Edit Create a Copy Delete View as XML

- 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](#).

Thycotic 10.3 Privilege Manager

Search Items  Search

HOME TOOLS ADMIN REPORTS

### Search

create servicenow  Search

Number of Results 5000 Showing 1 to 1 of 1

Role Type Name (1) Registered Activity Task (1)

**Create ServiceNow Items for TMS Approvals**  
7/11/2017 - Registered Activity Task  
Creates basic ServiceNow items required by TMS approval.  
[Item Viewer](#) | [View XML](#)

Showing 1 to 1 of 1

### Create ServiceNow Items for TMS Approvals

Settings

Task Name \* Interactive run on Tue Aug 08 2017

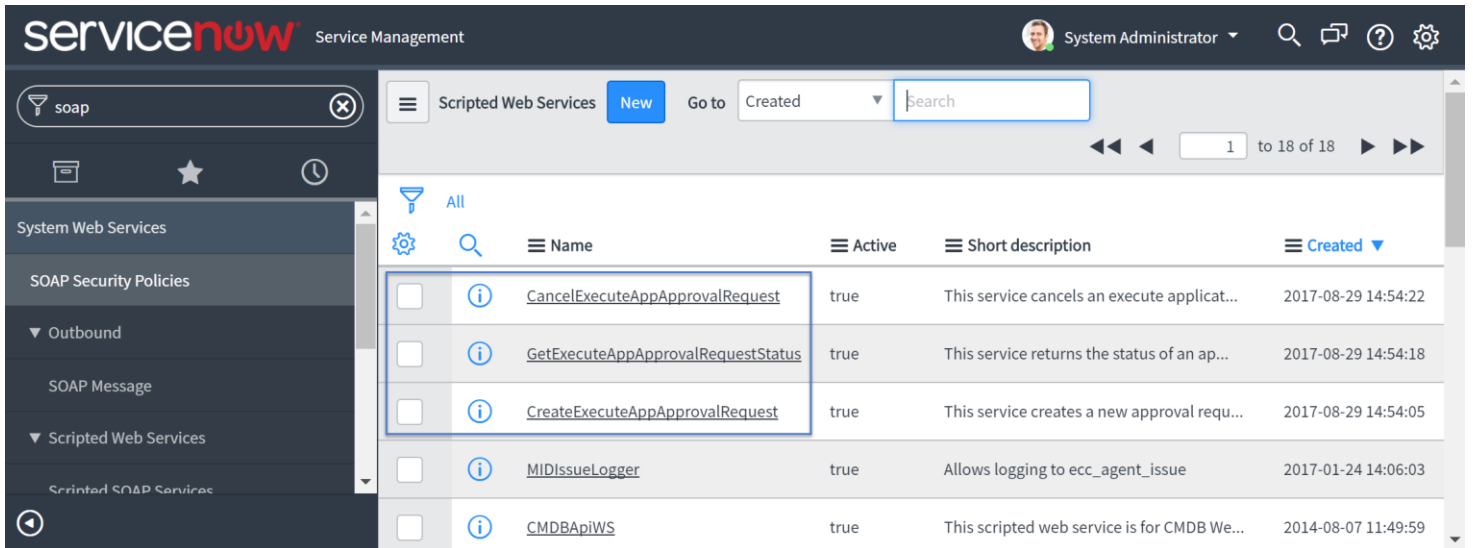
ServiceNow ID

View Parameters

\* Select resource...

	Name	Resource Type	Description
+	ServiceNow Server	ServiceNow Management Server	ServiceNow Server

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.

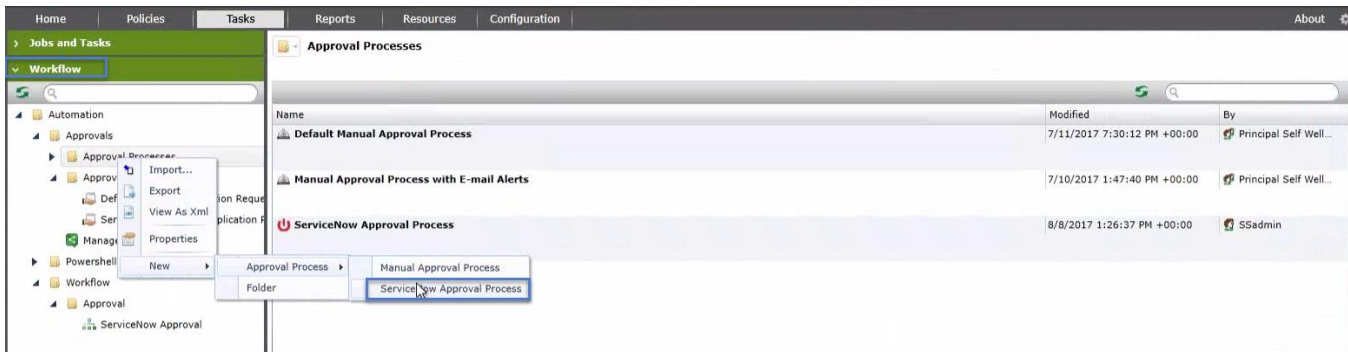
Next, navigate to the **Management Server Silverlight Console** (installed in step 3):

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**.

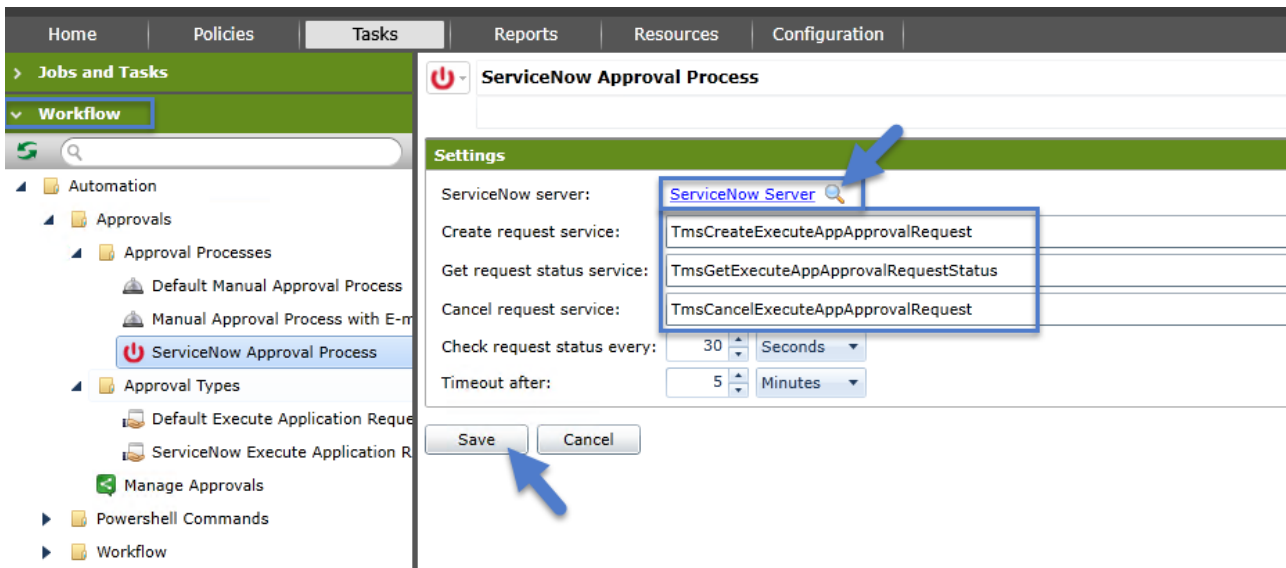
10. Click the **Tasks** tab, scroll to find Workflow in the left window, and expand the window. Navigate to **Automation > Approvals**, right click **Approval Processes**, then **New > Approval Process > ServiceNow Approval Process**.

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**.

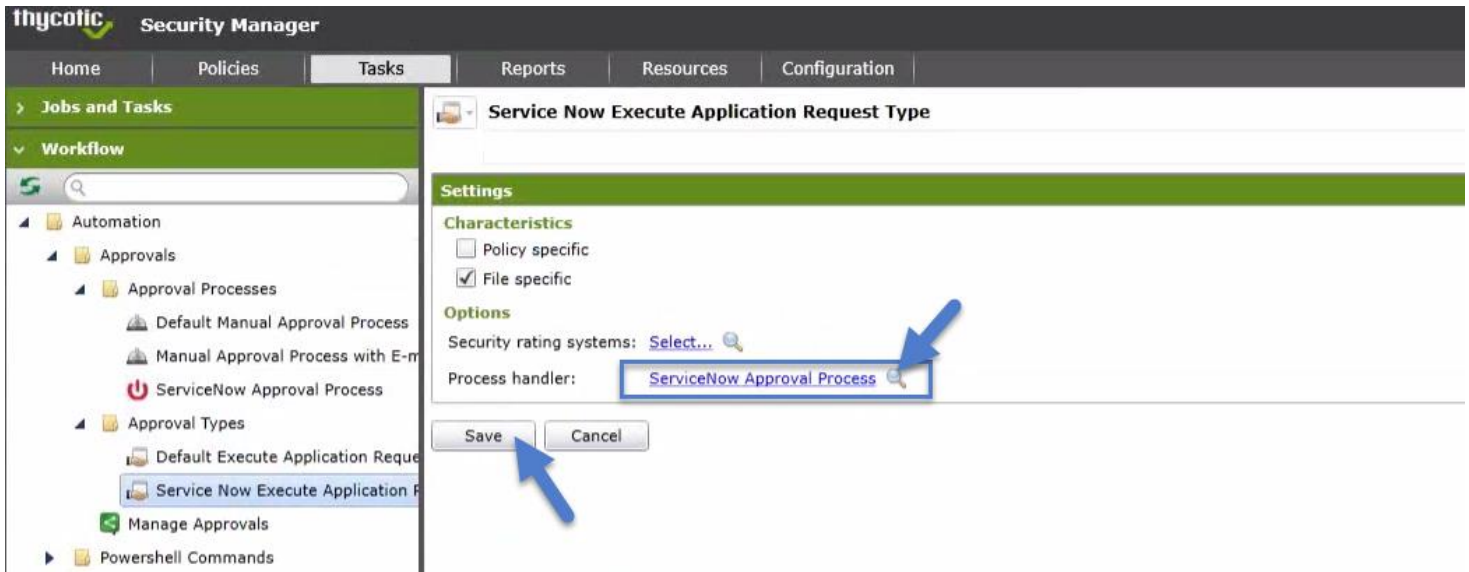
Now, still under **Workflow** in your Silverlight **Tasks** tab,

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

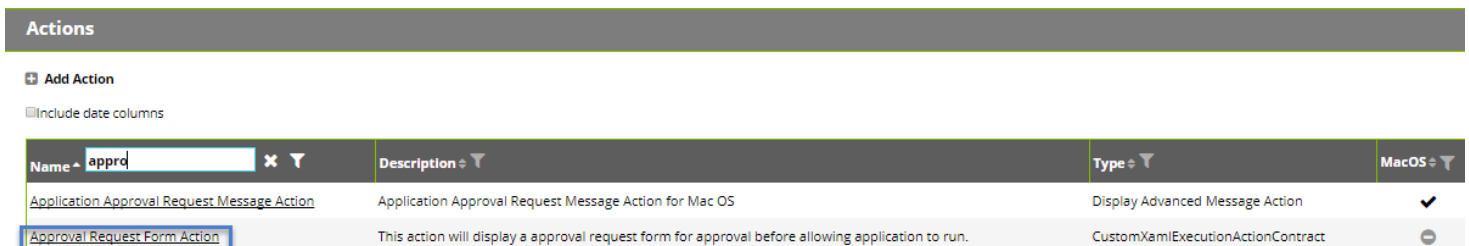


16. Click **Service Now Execute Application Process** under **Approval Types**.

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**.

## ServiceNow Approval Request Form Action

Details	Related Items
<b>Details</b>	
Name	* ServiceNow Approval Request Form Action
Description	This action will display a approval request form for approval before allowing application to run.
<b>Settings</b>	
<input type="checkbox"/> Require authentication: <input type="radio"/> By the interactive end-user <input checked="" type="radio"/> By a member of the group:	
Approval type	* ServiceNow Execute Application Request Type
<b>Window Design</b>	
Message prompt logo	
Application label	Choose File   No file chosen
Approval status label	Application:
Approval status section	Approval status: A previous request for this application has been submitted for review.
Cancel button text	Cancel
Continue button text	Continue
Information section	This application has not been approved for use according to corporate policy. Please discontinue use or enter your justification to continue through ServiceNow.
Instruction section	Type a brief explanation describing why this application is necessary. This explanation will form part of the request and will be reviewed by IT staff in consideration of this request.

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

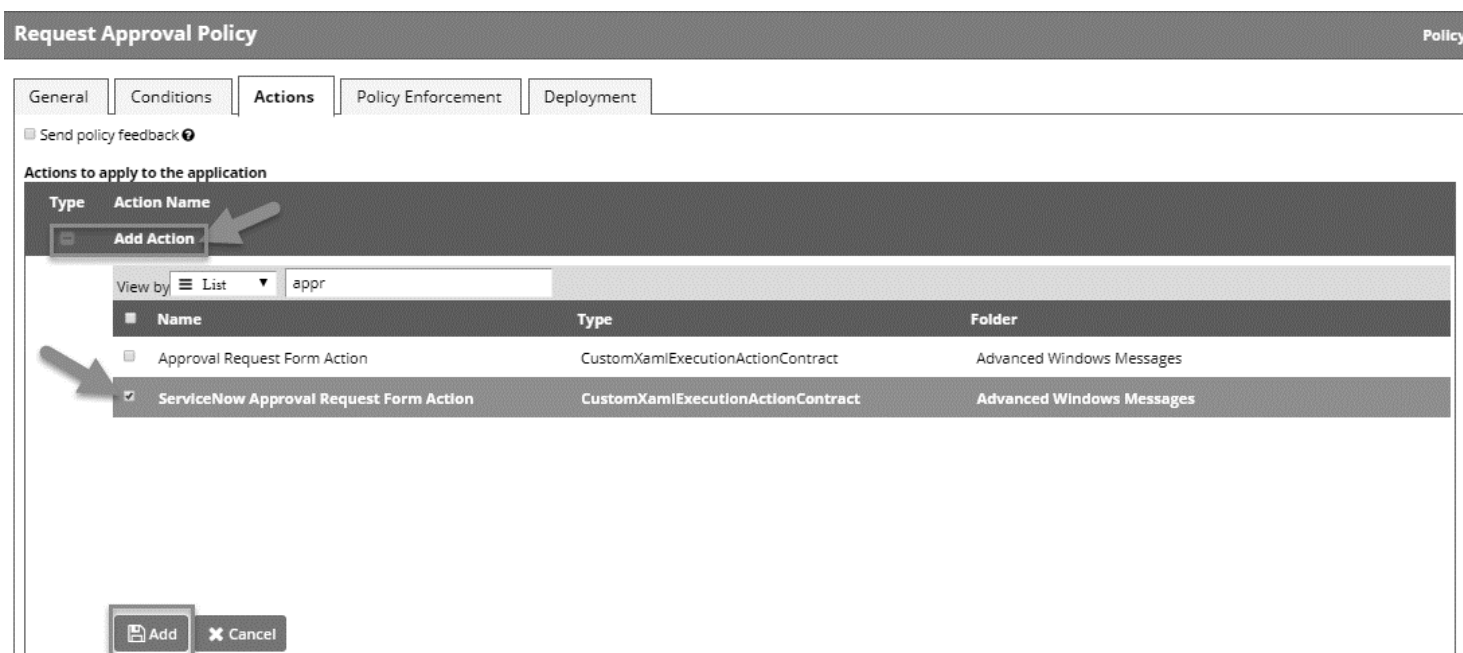
20. Click **Edit**. Next to Approval Type, search for **ServiceNow Execute Application Request Type**.

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**.

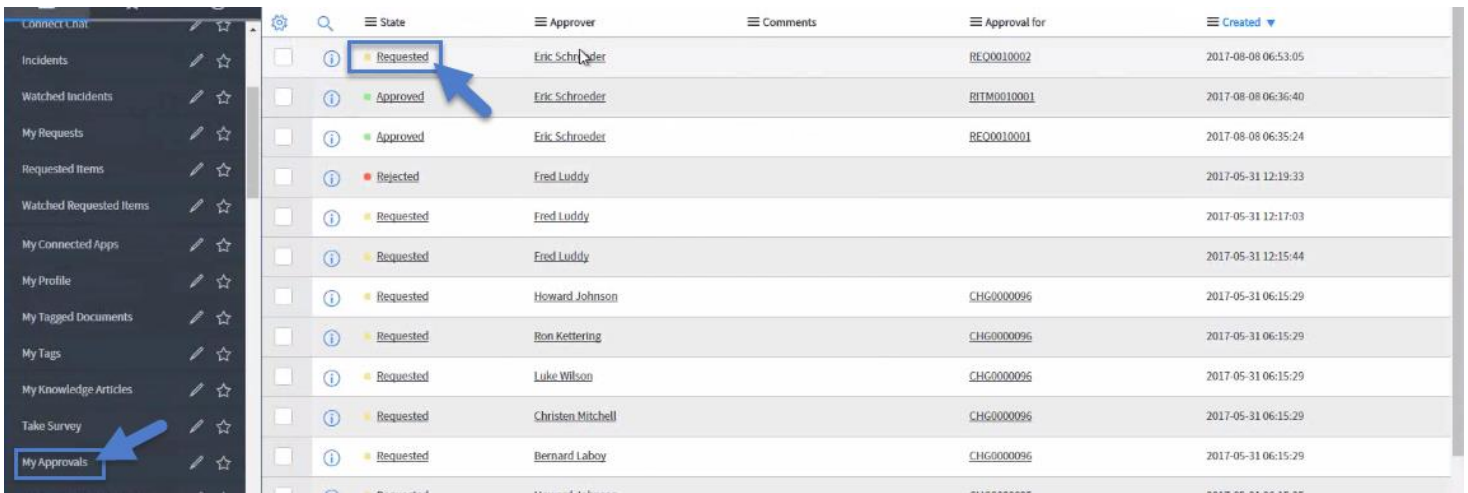


23. **Update your endpoints** by sending this new policy to target agents. Policies automatically update according to a schedule. For steps on how to do this immediately, see page 12 of the [Privilege Manager User Guide](#).

### Integration Workflow:

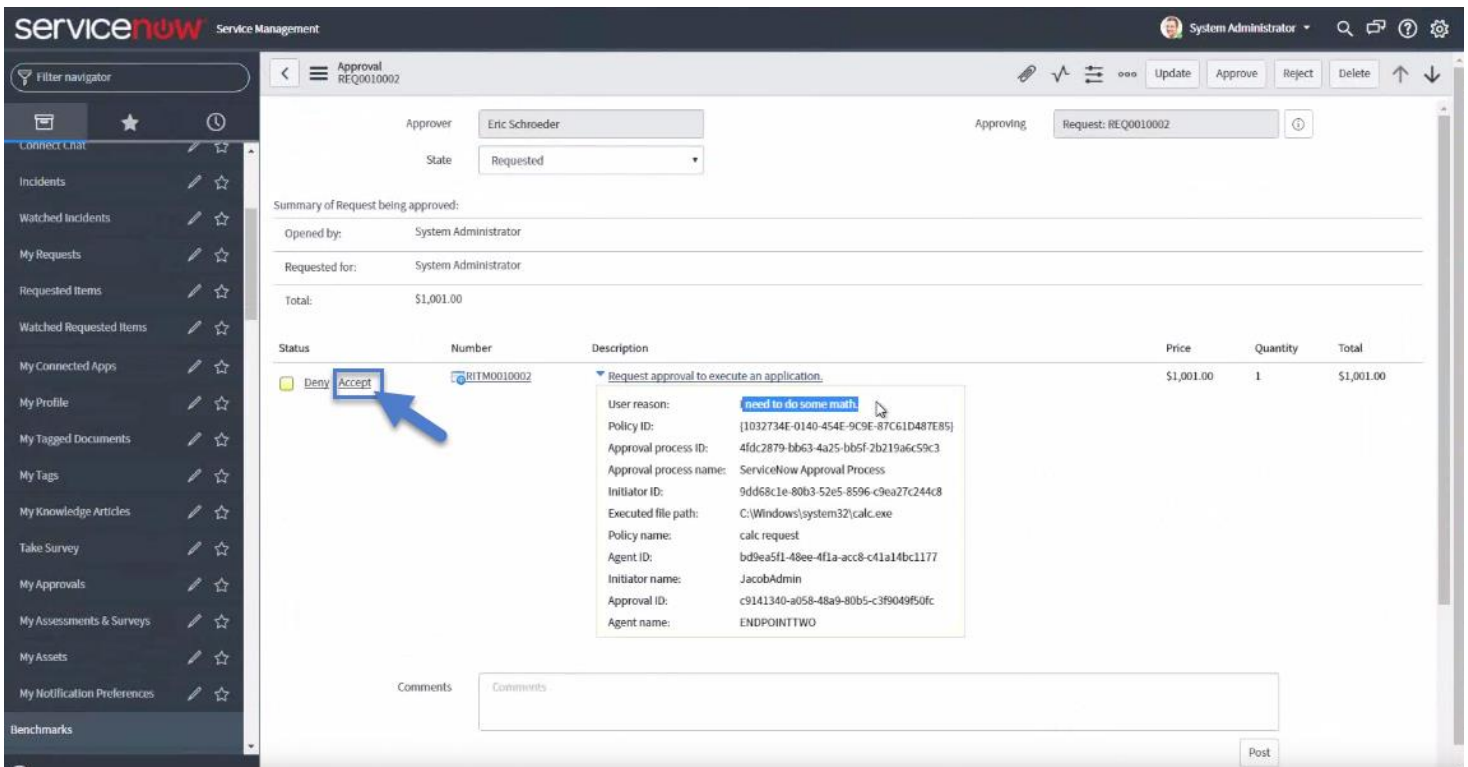
Now that you have a policy that is attached to your ServiceNow integrated Action, the requests from your policy is sent through ServiceNow for approval.

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.

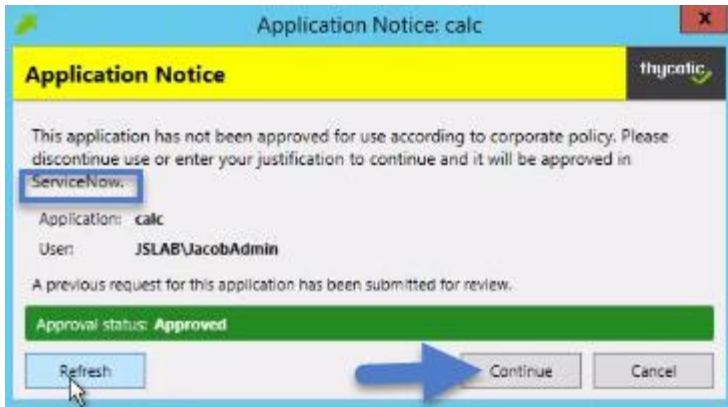


25. Go to **MyApprovals** in ServiceNow and you see your new requests. Click **Requested** for details.

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.



# 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 Privilege Vault. It is found in Privilege Manager 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.

**Privilege Vault** – Privilege Vault is a product that many IT teams use to securely manage privileged accounts and passwords in an organization. Privilege Manager and Privilege Vault 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 Privilege Vault license page houses Privilege Manager licenses, and Privilege Vault 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.