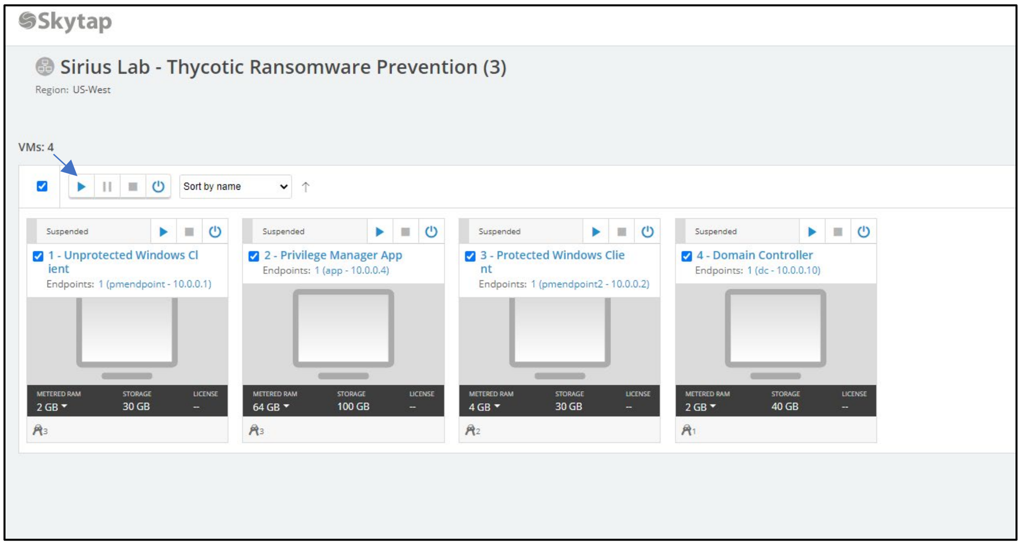
Privilege Manager

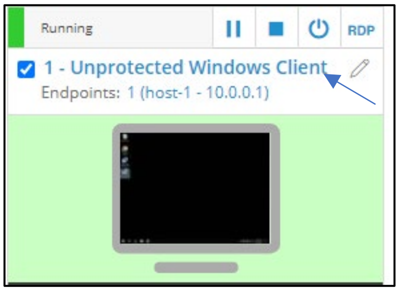
Become more Resilient against Ransomware with Proven PAM Strategies

Section 0: Access Hands-On Lab Environment

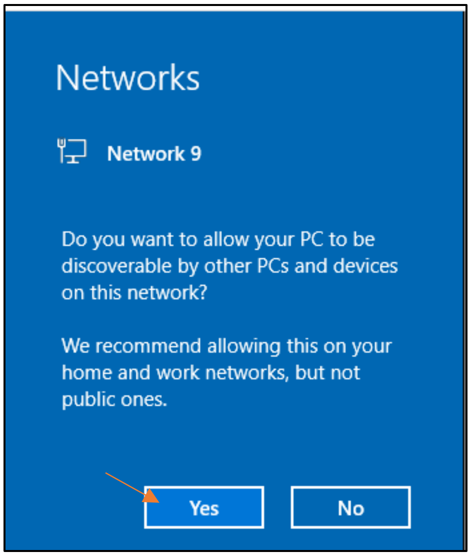
1. Select the Play button shown in the image below, if your virtual machines aren't showing as **Running**


Skytap
Sirius Lab - Thycotic Ransomware Prevention (3)
Region: US-West
VMs: 4
Sort by name
Suspended
1 - Unprotected Windows Cl ient
Endpoints: 1 (pmendpoint - 10.0.0.1)
METERED RAM 2 GB
STORAGE 30 GB
LICENSE --
Suspended
2 - Privilege Manager App
Endpoints: 1 (app - 10.0.0.4)
METERED RAM 64 GB
STORAGE 100 GB
LICENSE --
Suspended
3 - Protected Windows Clie nt
Endpoints: 1 (pmendpoint2 - 10.0.0.2)
METERED RAM 4 GB
STORAGE 30 GB
LICENSE --
Suspended
4 - Domain Controller
Endpoints: 1 (dc - 10.0.0.10)
METERED RAM 2 GB
STORAGE 40 GB
LICENSE --

2. Once all machines are running (Running machine shown in the image below), open the **1 - Unprotected Windows Client** Virtual Machine by selecting the name


Running
RDP
1 - Unprotected Windows Client
Endpoints: 1 (host-1 - 10.0.0.1)

3. Select **Yes**, if prompted with Network Settings



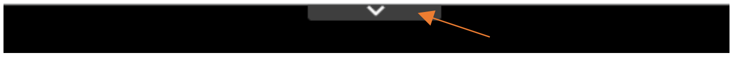
Networks

Network 9

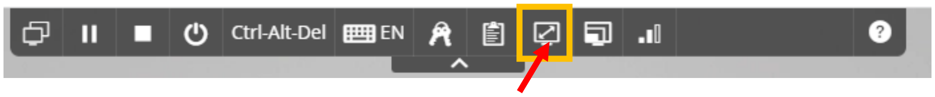
Do you want to allow your PC to be discoverable by other PCs and devices on this network?

We recommend allowing this on your home and work networks, but not public ones.

4. Locate the **Skytap toolbar** at the top of your Virtual Machine and expand it, if necessary, by selecting the **arrow**

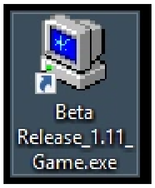


5. Select the **Fit to Window** button. This will allow you the maximum amount of workspace to complete this hands-on lab.

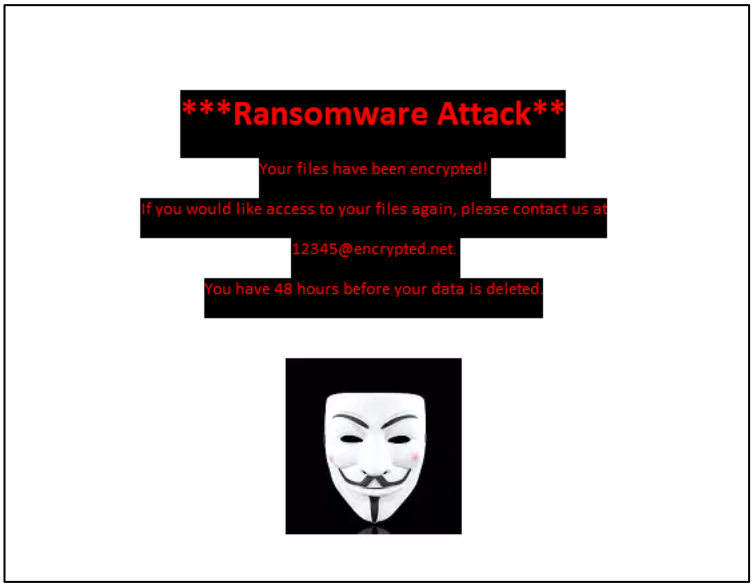


Section 1: Malicious Application Running on an Unprotected Endpoint

6. In this scenario, you are the new **Vice President of Product Management** for a gaming company. You've downloaded a competitor's beta release from an untrusted website, so you can test it and provide competitive advantages to your Sales team. **Open** the downloaded file from your **Desktop**. It is called **Beta Release_1.11_ Game.exe**



7. The Beta Release of the game does NOT open, instead you receive a pop-up informing you that your machine has been hit with a Ransomware attack!



***Ransomware Attack**

Your files have been encrypted!

If you would like access to your files again, please contact us at

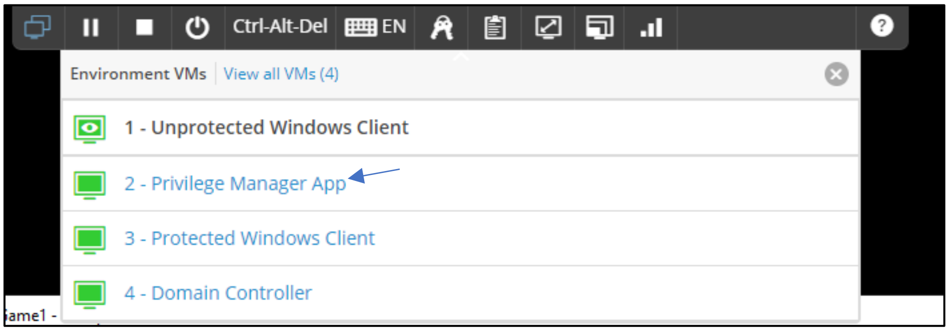
12345@encrypted.net.

You have 48 hours before your data is deleted.

8. Yes, it is just graphics in WordPad, but if we can start WordPad we could start something malicious. Let's walk-through how this type of Ransomware attack can be prevented by restricting all local administrative privileges and implementing controls on the endpoint.

Section 2: Implement Active Controls to Prevent Ransomware Attacks using Privilege Manager

10. Select the **2 - Privilege Manager App** Virtual Machine by selecting the name



1 - Unprotected Windows Client

2 - Privilege Manager App

3 - Protected Windows Client

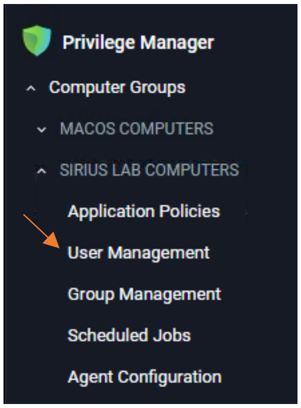
4 - Domain Controller

11. The Privilege Manager User Interface should be open. However, If you are prompted with a login screen enter:

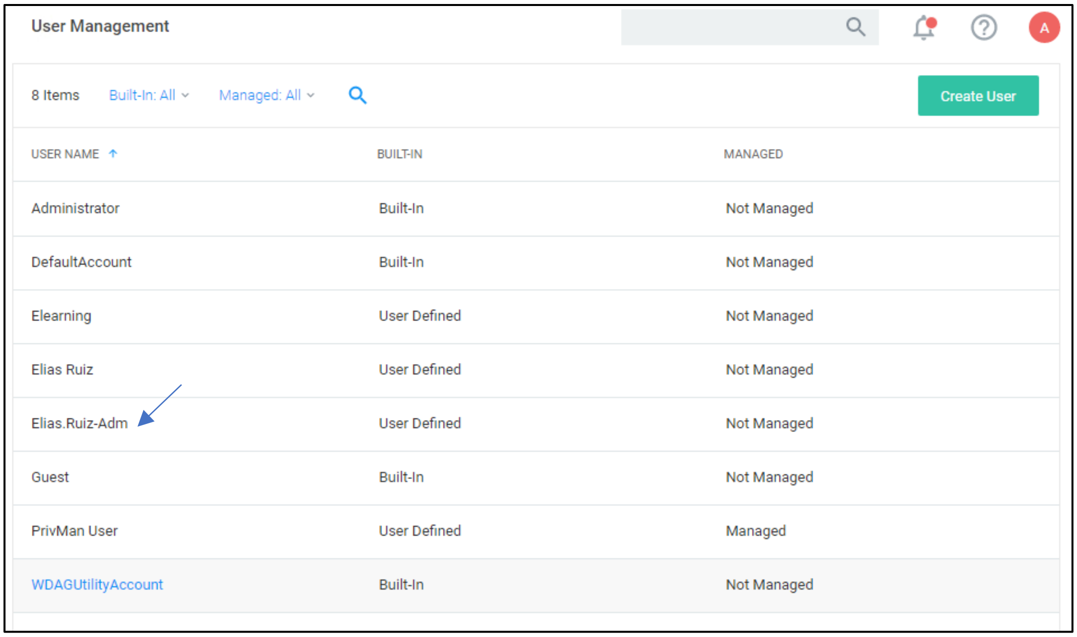
Username – **Admin**
Password – **ThycoticDemo!1**

and select the **Login** button.

12. Select **User Management** under the **Sirius Lab Computers** option, in the left-hand menu



13. On this page you can see the **local accounts** on the endpoints within the **Sirius Lab Computer Group**. It is very common that users have local administrative rights on their machine or access to a local admin account. This is usually for convenience purposes and is not a security best practice. Here you notice that Elias has a local admin account that he should NOT have on this machine – **Elias.Ruiz-Adm.**

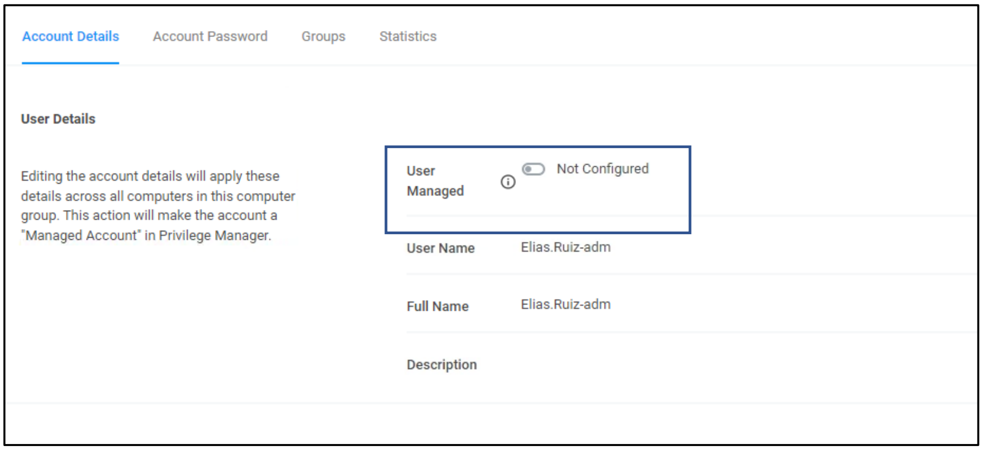


User Management

8 Items Built-In: All Managed: All

USER NAME	BUILT-IN	MANAGED
Administrator	Built-In	Not Managed
DefaultAccount	Built-In	Not Managed
Elearning	User Defined	Not Managed
Elias Ruiz	User Defined	Not Managed
Elias.Ruiz-Adm	User Defined	Not Managed
Guest	Built-In	Not Managed
PrivMan User	User Defined	Managed
WDAGUtilityAccount	Built-In	Not Managed

14. Let’s act on this information. **Select** the **Elias.Ruiz-Adm** account. Here you can take ownership of the credential with Privilege Manager. This means that Privilege Manager will act as a vault for this credential, and only users with the appropriate permissions in the application can access it.

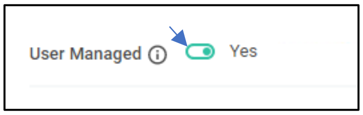


User Details

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 Manager.

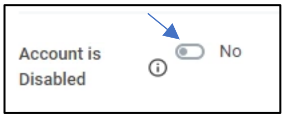
User Managed	Not Configured
User Name	Elias.Ruiz-adm
Full Name	Elias.Ruiz-adm
Description	

15. Toggle **User Managed** from **Not Configured** to **Yes.** Notice you can change attributes associated with the local account such as the **Full Name** and **Description.** These changes will update the accounts attributes in Privilege Manager and on the endpoint.

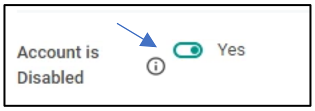


User Managed Yes

16. Since you do NOT want this account to be used any longer, toggle **Account is Disabled** from **No** to **Yes**

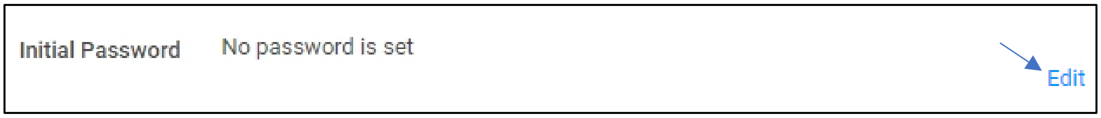


Account is Disabled No



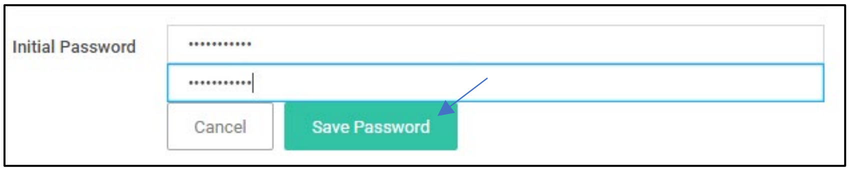
Account is Disabled Yes

17. We also need to **set a new password** for this account, so anyone using it previously can no longer access it when/if the account is re-enabled. Select the **Edit** link to the right of Initial Password



Initial Password No password is set Edit

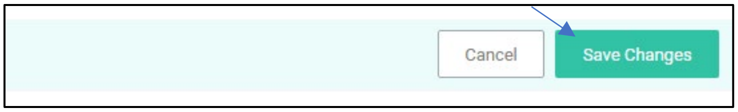
18. **Enter** and **re-enter** the password **Thycotic21!** and select **Save Password**



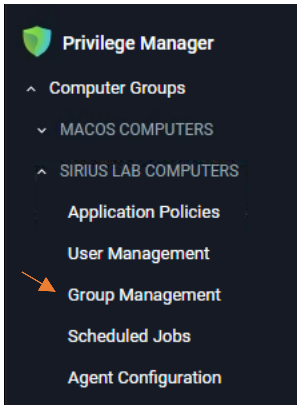
Initial Password •••••••••••

•••••••••••

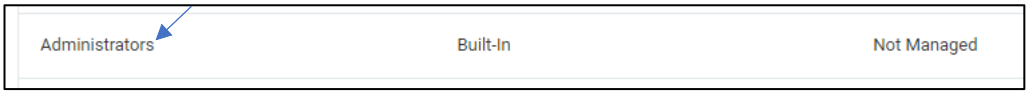
19. Select the **Save Changes** button at the top of the page and you have taken ownership of this account. (For extra credit, you could select the **Account Password** Tab to setup a password rotation and randomization schedule for the local account, but we won't cover that in this lab)



20. Select the **Group Management** option under **Sirius Lab Computers**

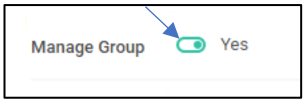


21. Here you can take ownership of **local groups with** Privilege Manager. This means that Privilege Manager will control the membership of these groups, and only users with the appropriate permissions in the application can make changes. **Select** the **Administrators** group



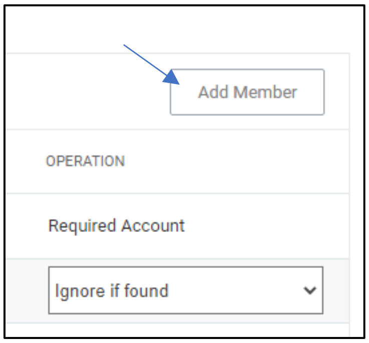
Administrators	Built-In	Not Managed

22. On this page, you can review the accounts that currently are members of the Administrator Group. Let's update the Administrators group to include the Help Desk team members so they can do their duties. Toggle **Manage Group** from Not Configured to **Yes**



Manage Group Yes

23. Scroll down and select the **Add Member** button. This will allow you to add new members to this group.

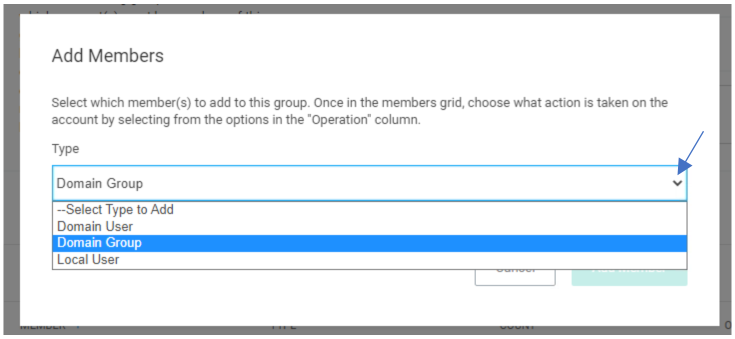


OPERATION

Required Account

Ignore if found

24. Select the **Type** dropdown and select **Domain Group**



Add Members

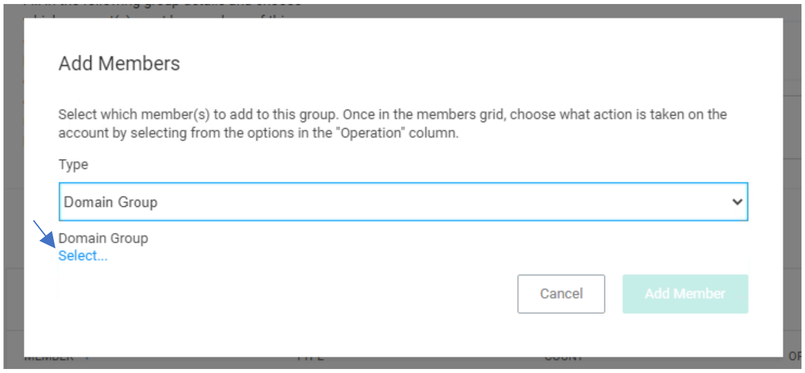
Select which member(s) to add to this group. Once in the members grid, choose what action is taken on the account by selecting from the options in the "Operation" column.

Type

Domain Group

--Select Type to Add
Domain User
Domain Group
Local User

25. Click the **Select** link below **Domain Group**



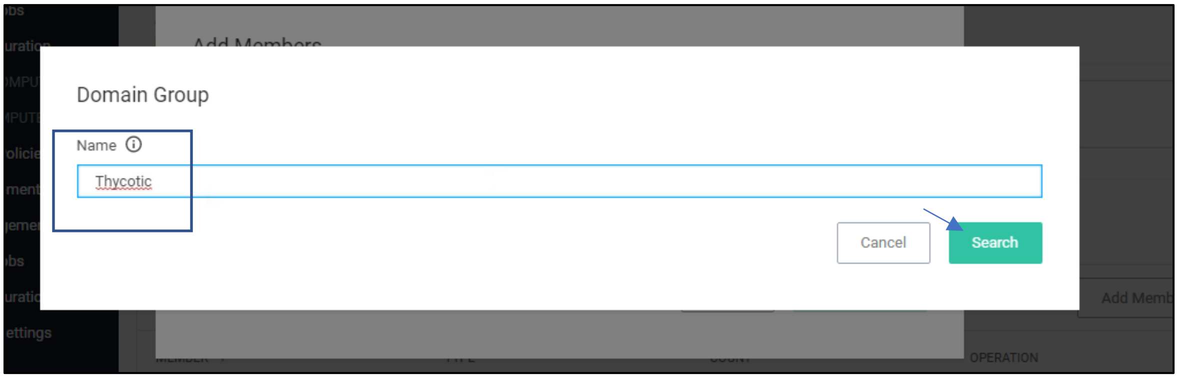
Add Members

Select which member(s) to add to this group. Once in the members grid, choose what action is taken on the account by selecting from the options in the "Operation" column.

Type: Domain Group

Domain Group
Select...

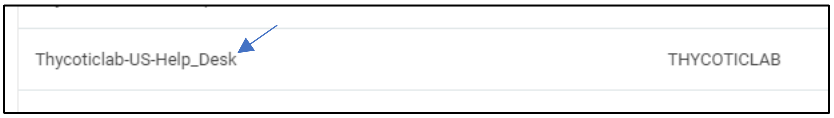
26. Type **Thycotic** in the search field and select **Search**



Domain Group

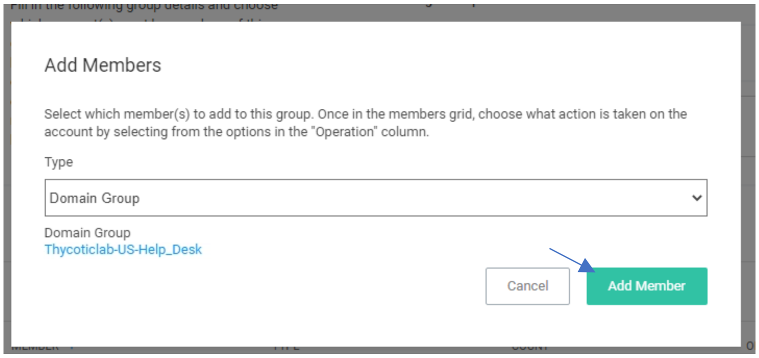
Name: Thycotic

27. Select the **Thycoticlab-US-Help_Desk** group



Thycoticlab-US-Help_Desk THYCOTICLAB

28. Select the **Add Member** button



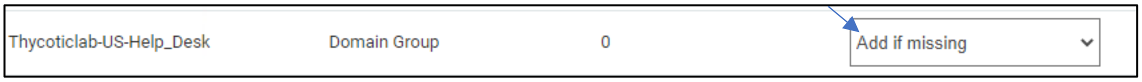
Add Members

Select which member(s) to add to this group. Once in the members grid, choose what action is taken on the account by selecting from the options in the "Operation" column.

Type: Domain Group

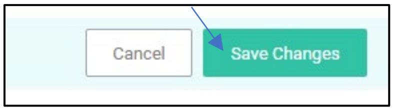
Domain Group
Thycoticlab-US-Help_Desk

29. Confirm the **Thycoticlab-Us-Help_Desk** group's **Operation** is set to **Add if missing**. This means if a new machine is added to the Sirius Lab Computer group in Privilege Manager and **Thycoticlab-US-Help_Desk** isn't a member of the Administrators group on that machine, the Agent will add it automatically.

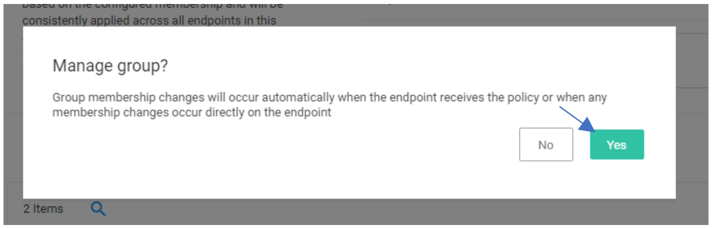


Thycoticlab-US-Help_Desk Domain Group 0 Add if missing

30. Select **Save Changes.** We will test these controls when we log into the protected machine later in this lab.



31. Select **Yes** when prompted

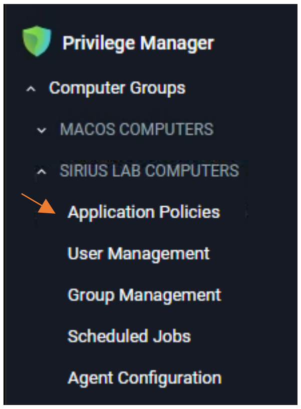


based on the configured membership and will be consistently applied across all endpoints in this

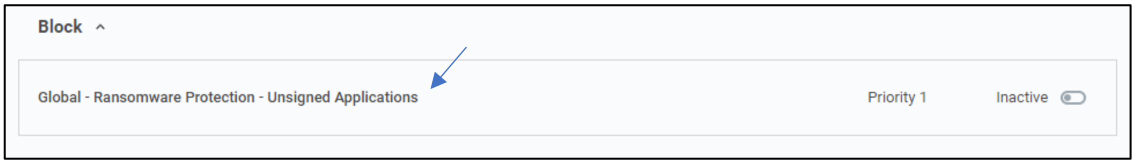
Manage group?

Group membership changes will occur automatically when the endpoint receives the policy or when any membership changes occur directly on the endpoint

32. Now we've confirmed the local admin rights on the machine have been locked down sufficiently. Let's review the **Application Control Policies** that will stop the user from being able to run malicious applications. Select **Application Policies** under **Sirius Lab Computers**



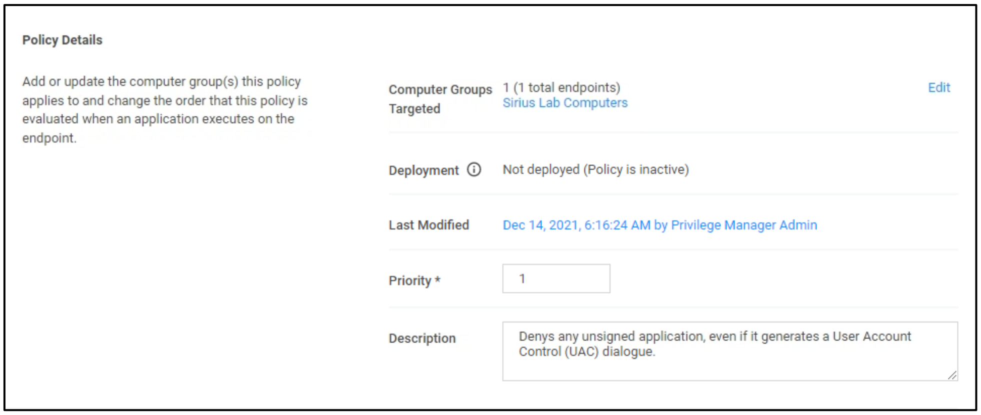
33. Notice the Ransomware protection policy has already been configured for you, but it has not been activated for use. Select the **Global – Ransomware Protection – Unsigned Applications** Policy



Block

Global - Ransomware Protection - Unsigned Applications | Priority 1 | Inactive

34. Notice that the Policy shows:
    - **Computer Groups Targeted** – Which group(s) of endpoints have this Policy applied
    - **Deployment** – How many of the endpoints targeted have the most up-to-date Policy
    - **Last Modified** – When the Policy was last changed and by which user
    - **Priority** – The order Policies will apply on the endpoint(s)
    - **Description** – A clear explanation of how this policy is intended to work on the endpoint

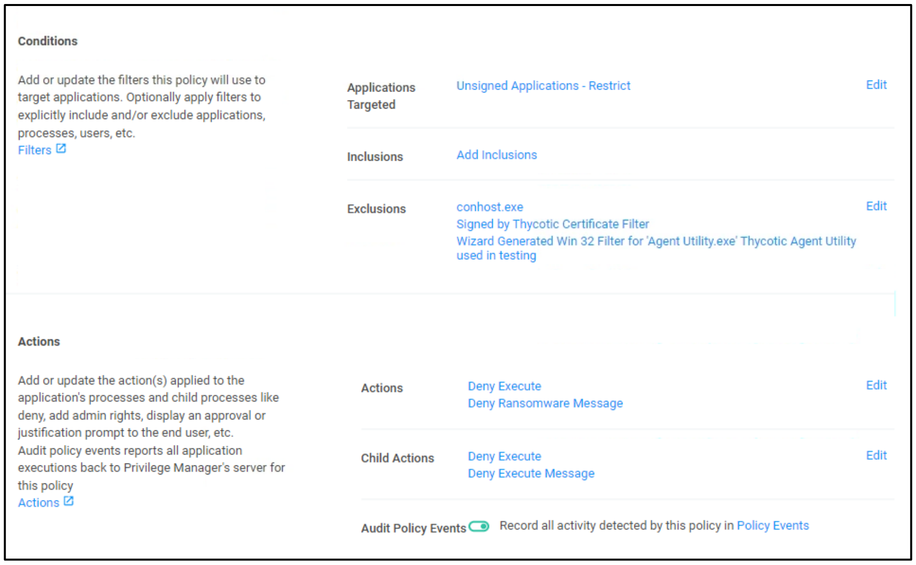


Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted	1 (1 total endpoints) Sirius Lab Computers	Edit
Deployment	Not deployed (Policy is inactive)	
Last Modified	Dec 14, 2021, 6:16:24 AM by Privilege Manager Admin	
Priority *	1	
Description	Denys any unsigned application, even if it generates a User Account Control (UAC) dialogue.	

35. If you scroll down, you will also see the Conditions and Actions Section of the Policy. **Conditions** control what needs to happen on the endpoint to trigger this Policy and **Actions** are what happens when the Policy is triggered.



Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc.
Filters

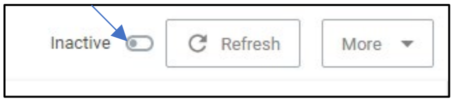
Applications Targeted	Unsigned Applications - Restrict	Edit
Inclusions	Add Inclusions	
Exclusions	conhost.exe Signed by Thycotic Certificate Filter Wizard Generated Win 32 Filter for 'Agent Utility.exe' Thycotic Agent Utility used in testing	Edit

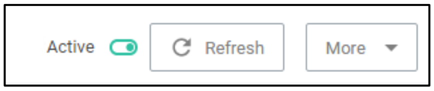
Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc.
Audit policy events reports all application executions back to Privilege Manager's server for this policy
Actions

Actions	Deny Execute Deny Ransomware Message	Edit
Child Actions	Deny Execute Deny Execute Message	Edit
Audit Policy Events	Record all activity detected by this policy in Policy Events	

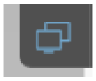
36. Scroll back to the top of the page and **toggle** the **Inactive** button to **Active**



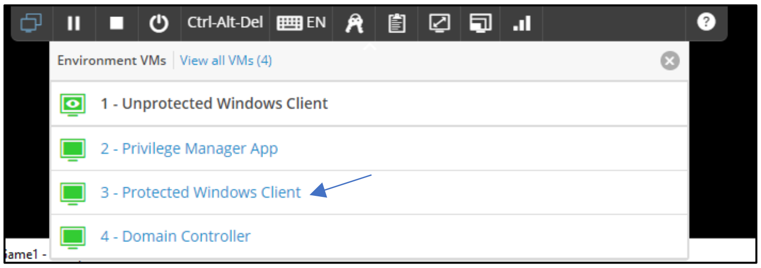


37. Now that the **Policy is Active**, continue to the next steps to walk through applying and testing the newly implemented endpoint controls

Section 3: Active Controls Protecting an Endpoint from Ransomware



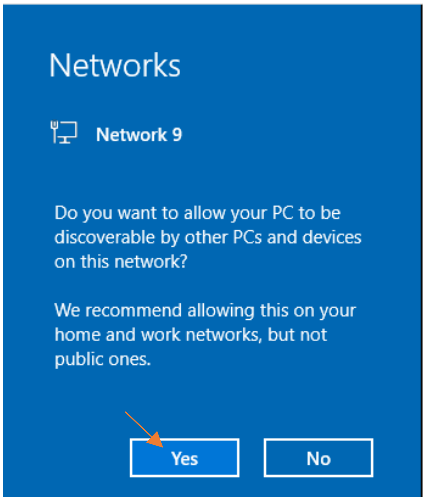
39. Select the **3 – Protected Windows Client** Virtual Machine by selecting the name



Environment VMs | View all VMs (4)

1 - Unprotected Windows Client
2 - Privilege Manager App
3 - Protected Windows Client
4 - Domain Controller

40. Select **Yes**, if prompted with Network Settings



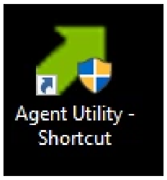
Networks

Network 9

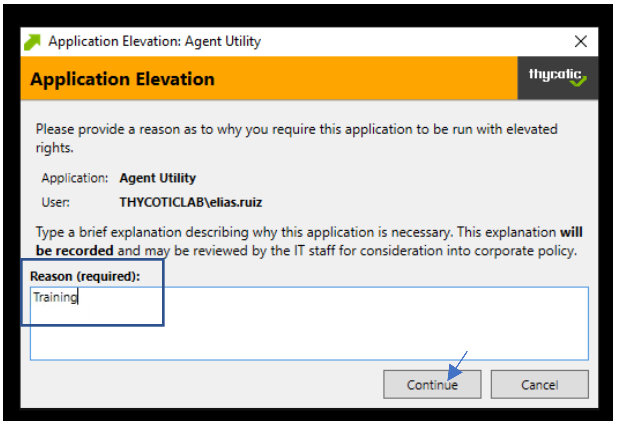
Do you want to allow your PC to be discoverable by other PCs and devices on this network?

We recommend allowing this on your home and work networks, but not public ones.

41. Select the **Agent Utility – shortcut** on the Desktop



42. You will be presented with a **Privilege Manager Elevation prompt** that requires you to provide a justification for using an application that requires elevated rights. This elevation feature takes away the need for users to have admin rights which assist organizations in reaching least privilege. Type **Training** and select **Continue**



Application Elevation: Agent Utility

Application Elevation

Please provide a reason as to why you require this application to be run with elevated rights.

Application: **Agent Utility**

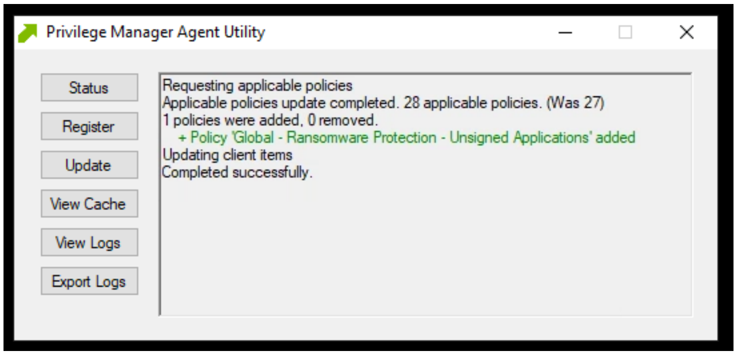
User: **THYCOTICLAB\elias.ruiz**

Type a brief explanation describing why this application is necessary. This explanation **will be recorded** and may be reviewed by the IT staff for consideration into corporate policy.

Reason (required):

Training

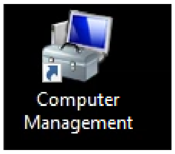
43. This will open the **Privilege Manager Agent Utility**. This tool is installed as a part of the Agent installation and allows users with the appropriate permissions to administer the Agent from the endpoint. This is often used to troubleshoot or quickly test a Policy. Select the **Update** button to update the endpoint with Policy you just activated.



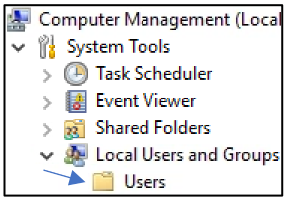
```
Requesting applicable policies
Applicable policies update completed. 28 applicable policies. (Was 27)
1 policies were added, 0 removed.
   + Policy 'Global - Ransomware Protection - Unsigned Applications' added
Updating client items
Completed successfully.
```

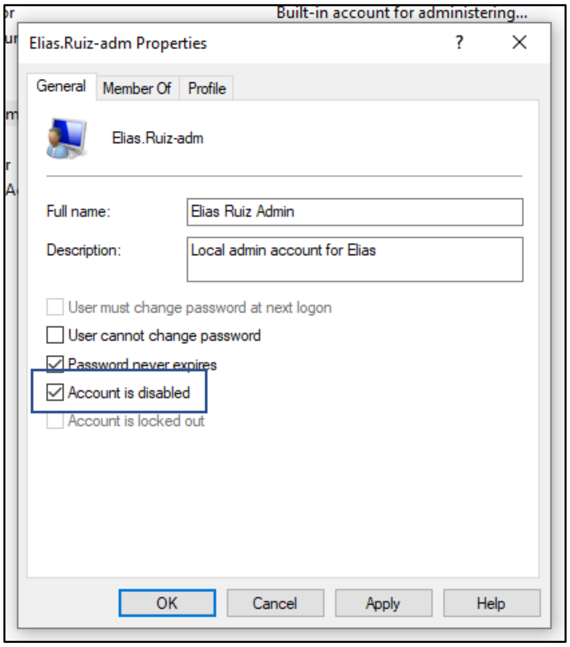
44. **Minimize** the **Privilege Manager Agent Utility**, once you see the Policy shown as added. It will be showing in green (As seen above). <u>If you don't see the policy update in green</u> – Wait a few moments and select the **Update** button again. You can also, click **View Logs** and search for "**ransom**". If you find the policy, it downloaded to the endpoint before you had a chance to manually update.

45. Now open **Computer Management** from the Desktop. As a VP of Product Management, Elias may need to perform certain tasks in Computer Management, but actions like changing memberships of local groups or changing attributes of certain local users should be restricted.



46. Expand **Local Users and Groups** and select **Users**. **Double-click** the **Elias.Ruiz-adm** account and notice it is **Disabled**.




Built-in account for administering...
Elias.Ruiz-adm Properties
?
General
Member Of
Profile
OK
Cancel
Apply
Help

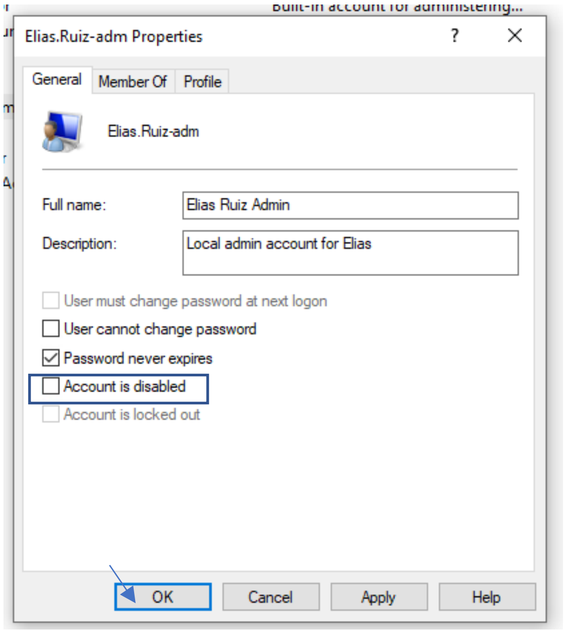
Elias.Ruiz-adm

Full name: Elias Ruiz Admin

Description: Local admin account for Elias

□ User must change password at next logon
□ User cannot change password
☑ Password never expires
☑ Account is disabled
□ Account is locked out

47. De-select **Account is disabled** and select **OK.**.


Built-in account for administering...
Elias.Ruiz-adm Properties
?
General
Member Of
Profile
OK
Cancel
Apply
Help

Elias.Ruiz-adm

Full name: Elias Ruiz Admin

Description: Local admin account for Elias

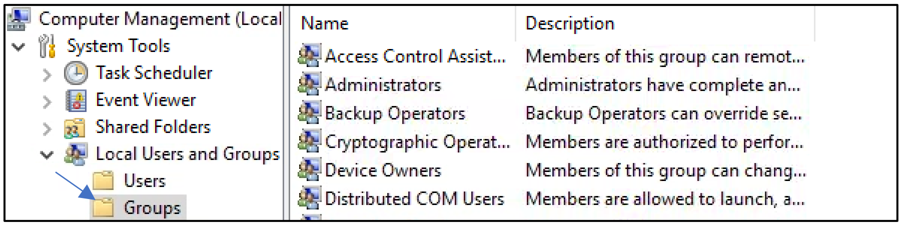
□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Account is disabled
□ Account is locked out

48. You should get an **Access Denied** Error. Notice that even though it seemed you were able disable this account the **Privilege Manager agent didn't allow the change to save.** The local account settings on the endpoint will always match what is in Privilege Manager after

ownership has been taken. Most Privilege Manager administrators would take the restrictions a step further by blocking access to the Management plugins the user shouldn't be using.

49. **Close/Cancel** the error message and the Elias.Ruiz-adm **properties page**

50. Select the **Groups** folder under **Local Users and Groups**

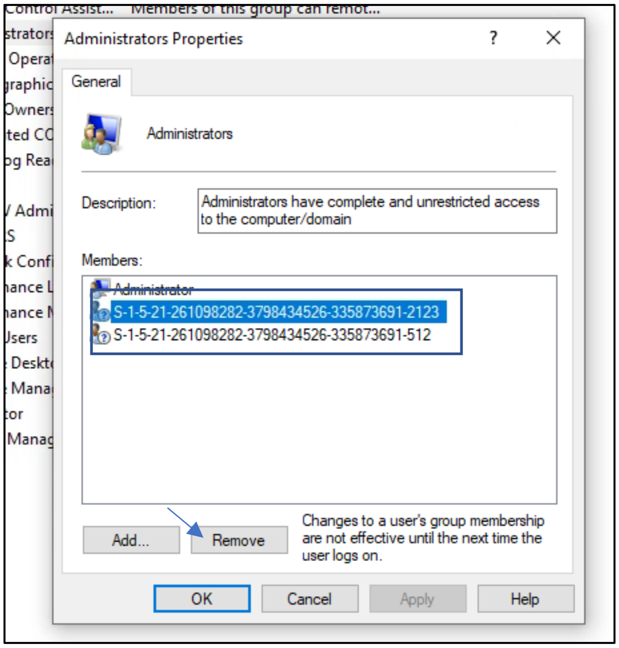


Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups

Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...

51. **Double-Click** the **Administrator** group to open the **properties** page. You may not see the **Thycotic-US-Help_Desk** group here until after the machine reboots, but you should see the Administrator account and some obfuscated accounts listed. Privilege Manager will also clean the obfuscated accounts after reboot as well.

52. **Click** one of the **obfuscated accounts** and select **Remove**



Administrators Properties

General

Administrators

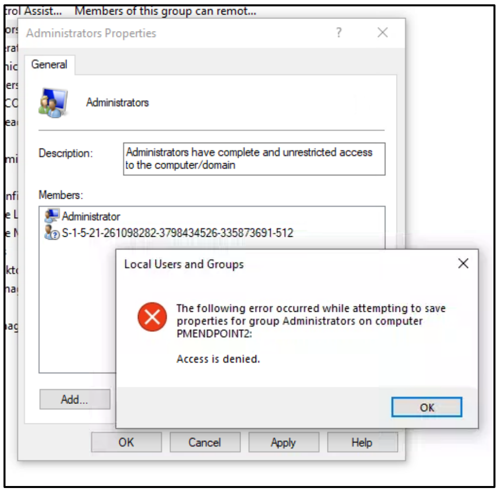
Description: Administrators have complete and unrestricted access to the computer/domain

Members:

Administrator
S-1-5-21-261098282-3798434526-335873691-2123
S-1-5-21-261098282-3798434526-335873691-512

Changes to a user's group membership are not effective until the next time the user logs on.

53. Select **OK**. You should get an access denied message because you are restricted from making any membership changes to this group. The Privilege Manager Agent is working as expected restricting activity on the endpoint. This protects the user and their organization from ransomware and other malicious attacks.


rol Assist... Members of this group can remot...
Administrators Properties
?
General
Add...
OK
Cancel
Apply
Help
OK

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:
Administrator
S-1-5-21-261098282-3798434526-335873691-512

Local Users and Groups

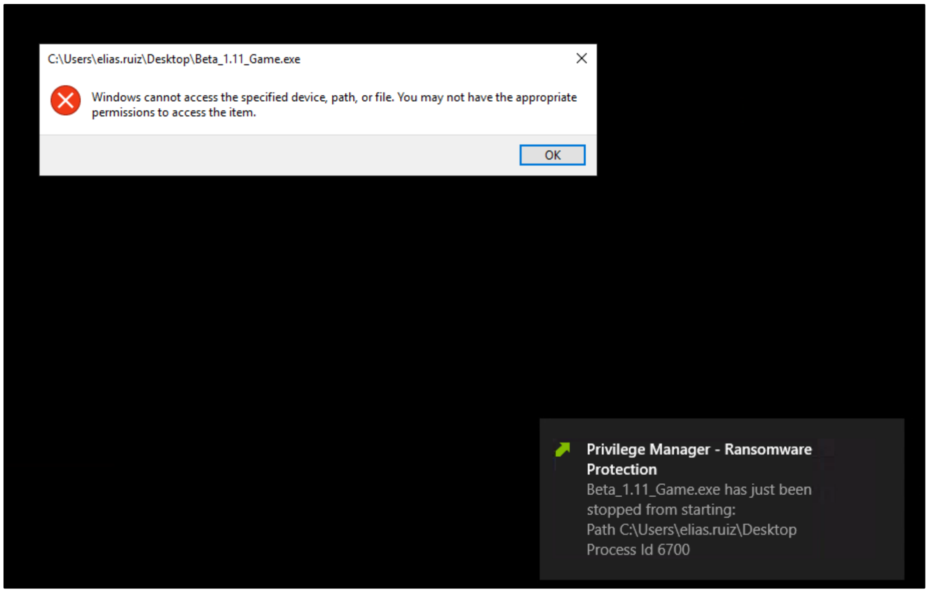
The following error occurred while attempting to save properties for group Administrators on computer PMENDPOINT2:

Access is denied.

54. Select **OK** to close the **Access Denied** message

55. Select **Cancel** to close the **Administrator group Properties** page. Minimize **Computer Management**

56. Now confirm you can no longer open the unsigned and unknown **Beta_1.11_Game** application by **selecting the application** from the **Desktop**. You will receive an **access denied** error and a customized message from Privilege Manager. This application is no longer able to run on this endpoint and possibly cause a Ransomware attack.



C:\Users\elias.ruiz\Desktop\Beta_1.11_Game.exe

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

Privilege Manager - Ransomware Protection
Beta_1.11_Game.exe has just been stopped from starting:
Path C:\Users\elias.ruiz\Desktop
Process Id 6700

57. The customized message is configured to disappear after 10 seconds. Select **OK** to close the access denied program message

58. Policies are meant to target known-bad application types or events, but still allow users to complete their job duties. For example, open **Google Chrome** from the **Desktop.** Notice the Agent is configured to allow this application to run because it’s trusted and needed by this user.

59. Close **Google Chrome**

60. You have completed the **Thycotic Ransomware Protection** hands-on lab. Please let your instructor know if you have any additional questions!