




ThycoticCentrify

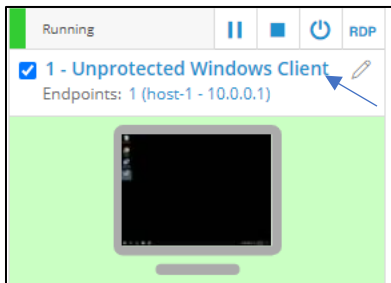


Privilege Manager

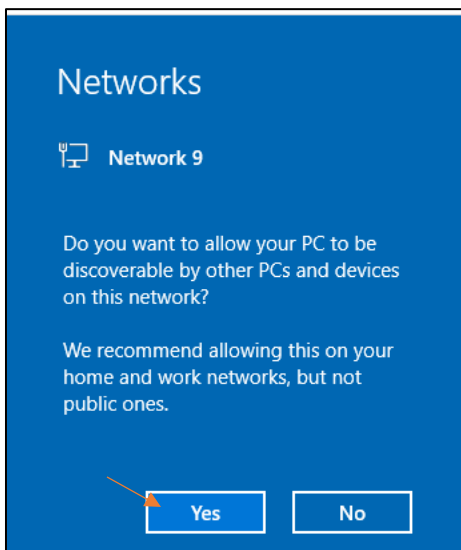
Become more Resilient against Ransomware with Proven PAM Strategies

Section 0: Access Hands- On Lab Environment

1. The link to your lab environment can be found by navigating to  and . Select the link that says . (This information will be populated after the Thursdays Dry Run. Skip to next step)
2. Open the **1 - Unprotected Windows Client** Virtual Machine by selecting the name



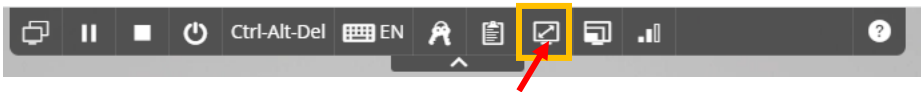
3. Select **Yes**, if prompted with Network Settings



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

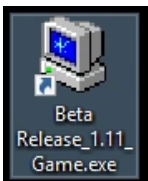


5. Select the **Fit to Window** button. This will allow you the maximum amount of workspace to complete this hands-on lab.



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!



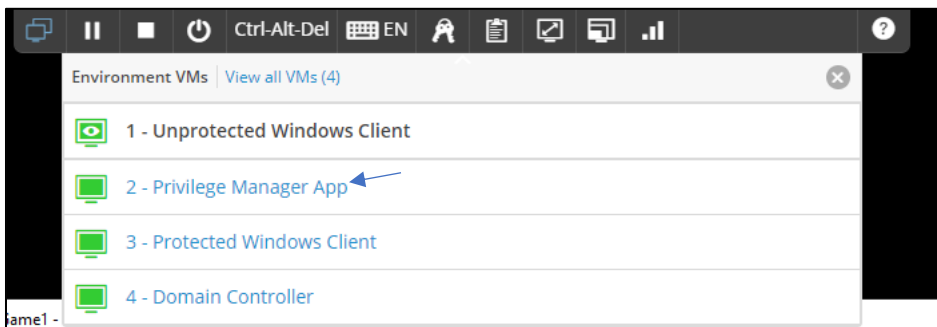
8. Yes, it is just graphics in WordPad, but if we can start WordPad we could start something malicious. Let's walk-through how this type of Ransomware attack can be prevented by restricting all local administrative privileges and implementing controls on the endpoint.

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

9. Expand the **Skytap Toolbar** at the top of your virtual machine and select the **Stacked Monitors**



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



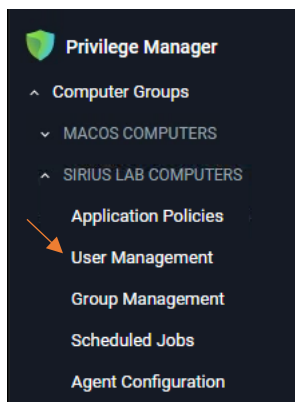
11. The Privilege Manager User Interface should be open. However, If you are prompted with a login screen enter:

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		
<div> 8 Items Built-In: All Managed: All </div> <div>Create User</div>		
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.

Account Details
Account Password
Groups
Statistics

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.

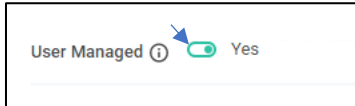
User Managed
Not Configured

User Name
Elias.Ruiz-adm

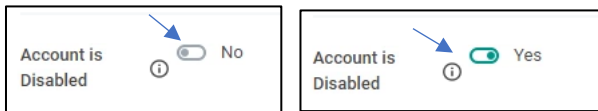
Full Name
Elias.Ruiz-adm

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.



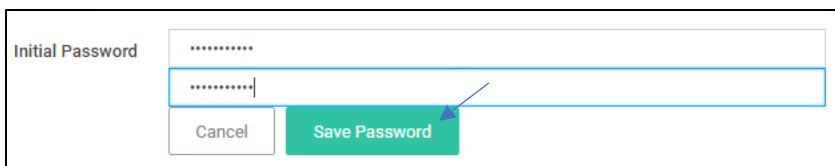
16. Since you do NOT want this account to be used any longer, toggle **Account is Disabled** from **No** to **Yes**



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



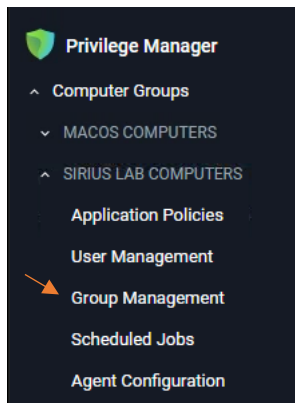
18. **Enter** and **re-enter** the password **Thycotic21!** and select **Save Password**



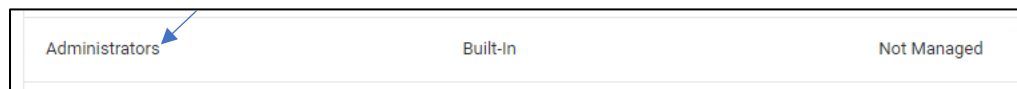
19. Select the **Save Changes** button at the top of the page and you have taken ownership of this account. (For extra credit, you could select the **Account Password** Tab to setup a password rotation and randomization schedule for the local account, but we won't cover that in this lab)



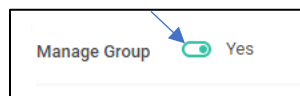
20. Select the **Group Management** option under **Sirius Lab Computers**



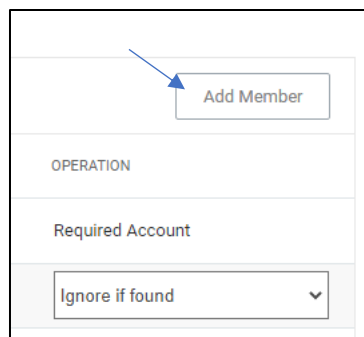
21. Here you can take ownership of **local groups with** Privilege Manager. This means that Privilege Manager will control the membership of these groups, and only users with the appropriate permissions in the application can make changes. **Select** the **Administrators** group



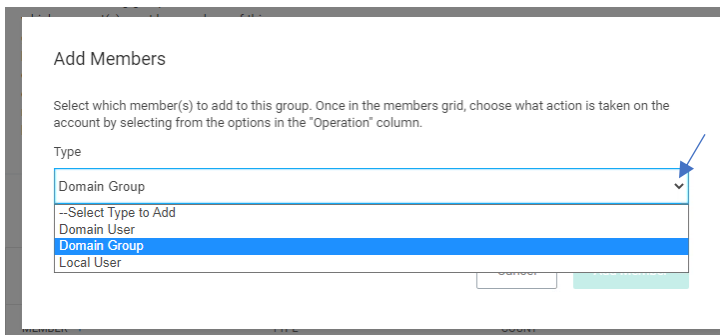
22. On this page, you can review the accounts that currently are members of the Administrator Group. Let's update the Administrators group to include the Help Desk team members so they can do their duties. Toggle **Manage Group** from Not Configured to **Yes**



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



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



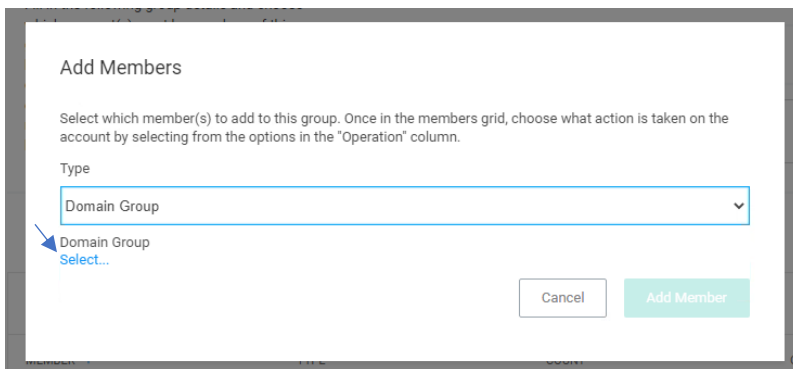
Add Members

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.

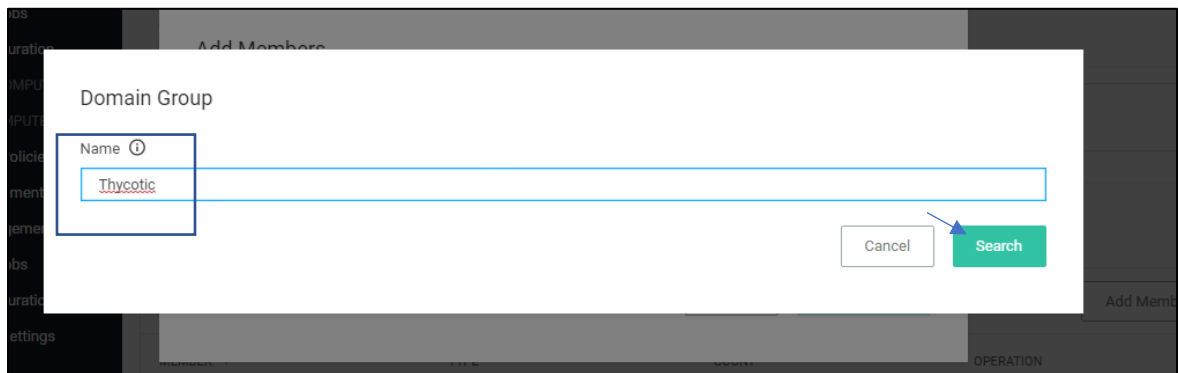
Type

Domain Group

Domain Group
[Select...](#)

Cancel Add Member

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



Domain Group

Name

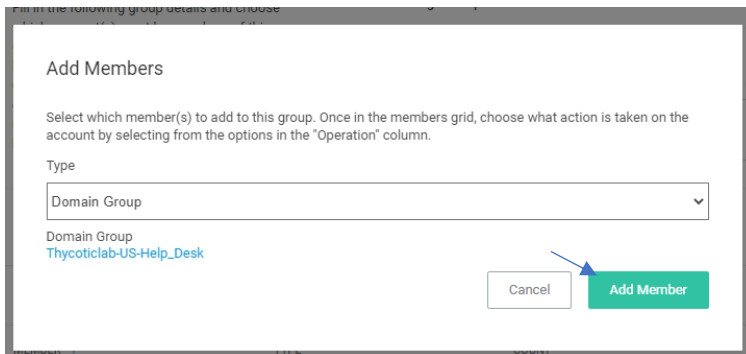
Thycotic

Cancel Search

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

Thycoticlab-US-Help_Desk	THYCOTICLAB
--------------------------	-------------

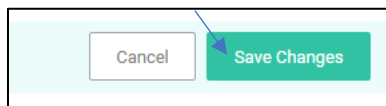
28. Select the **Add Member** button



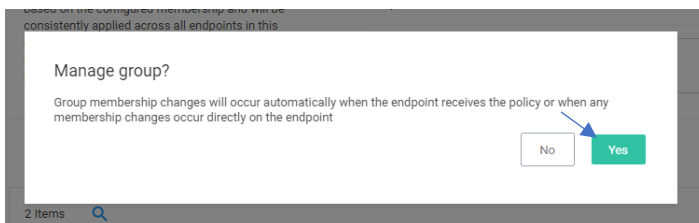
29. Confirm the **Thycoticlab-US-Help_Desk** group's **Operation** is set to **Add if missing**. This means if a new machine is added to the Sirius Lab Computer group in Privilege Manager and **Thycoticlab-US-Help_Desk** isn't a member of the Administrators group on that machine, the Agent will add it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



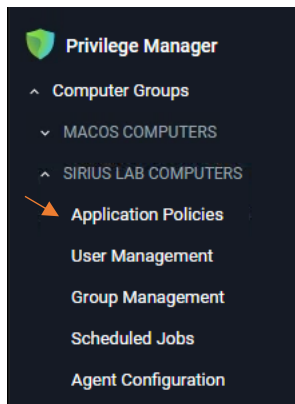
30. Select **Save Changes**. We will test these controls when we log into the protected machine later in this lab.



31. Select **Yes** when prompted



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**

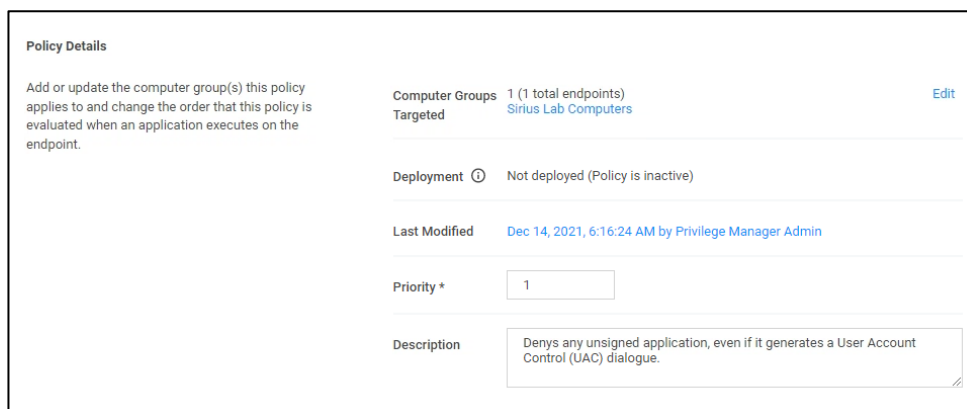


33. Notice the Ransomware protection policy has already been configured for you, but it has not been activated for use. Select the **Global – Ransomware Protection – Unsigned Applications Policy**



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



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**



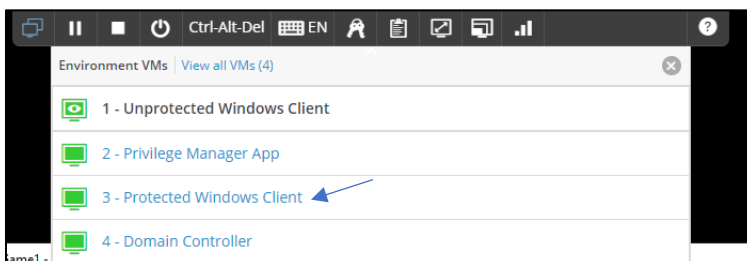
37. Now that the **Policy is Active**, continue to the next steps to walk through applying and testing the newly implemented endpoint controls

Section 3: Active Controls Protecting an Endpoint from Ransomware

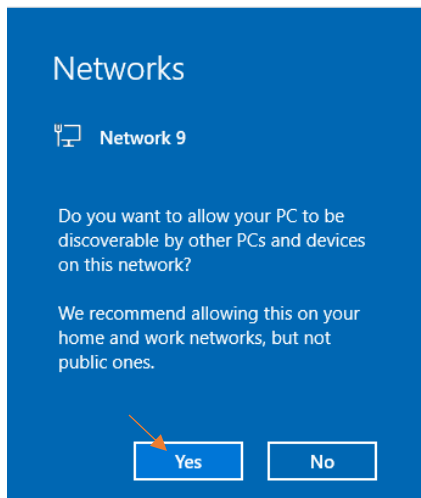
38. Expand the **Skytap Toolbar** at the top of your virtual machine and select the **Stacked Monitors**



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



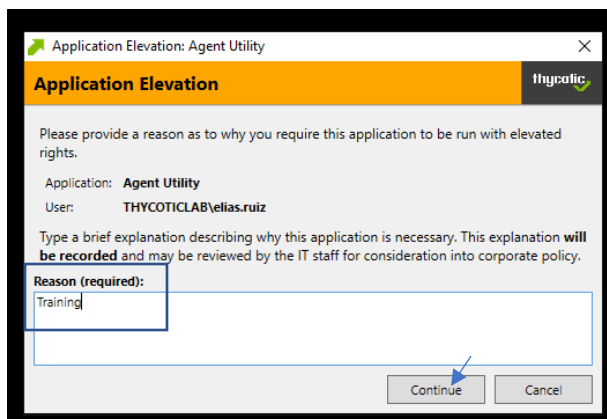
40. Select **Yes**, if prompted with Network Settings



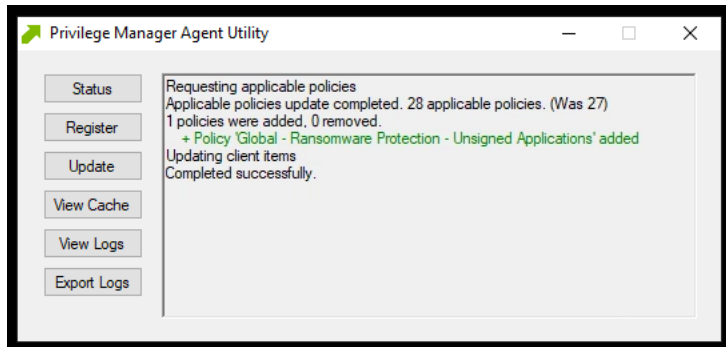
41. Select the **Agent Utility – shortcut** on the Desktop



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**



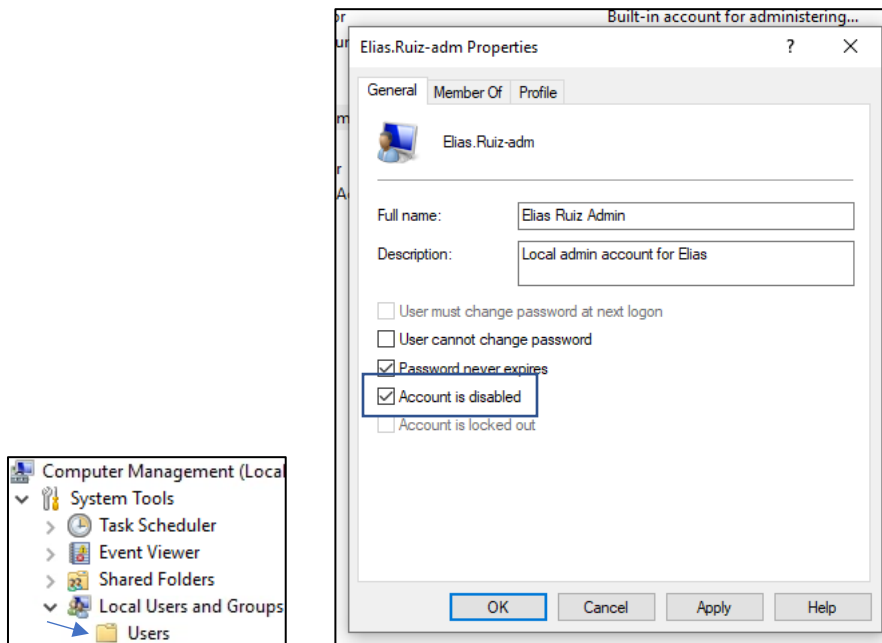
43. This will open the **Privilege Manager Agent Utility**. This tool is installed as a part of the Agent installation and allows users with the appropriate permissions to administer the Agent from the endpoint. This is often used to troubleshoot or quickly test a Policy. Select the **Update** button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



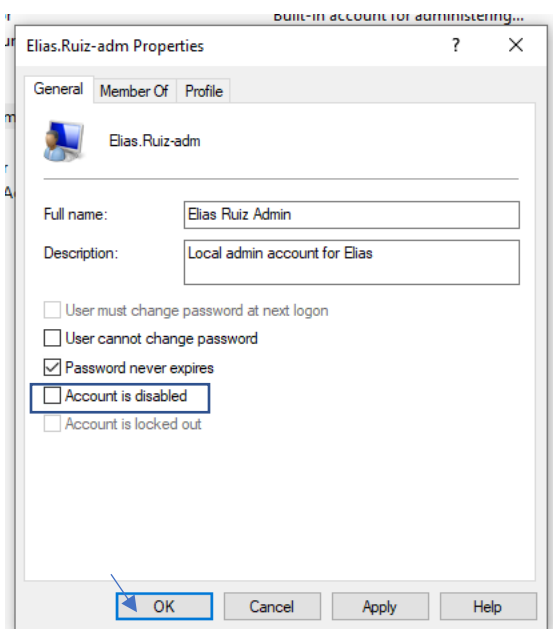
44. **Minimize** the **Privilege Manager Agent Utility**, once you see the Policy shown as added. It will be showing in green (As seen above). If you don't see the policy update in green – Wait a few moments and select the **Update** button again. You can also, click **View Logs** and search for “ransom”. 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**.



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

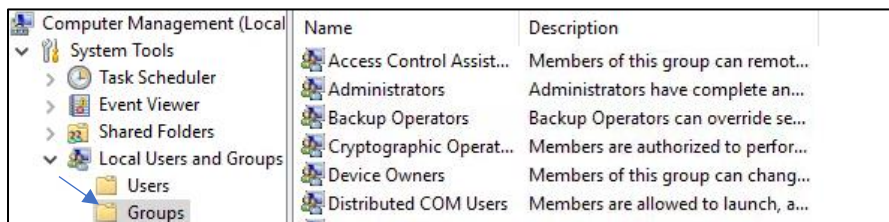


48. You should get an **Access Denied** Error. Notice that even though it seemed you were able to disable this account the **Privilege Manager agent didn't allow the change to save**. The local account settings on the endpoint will always match what is in Privilege Manager after

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.

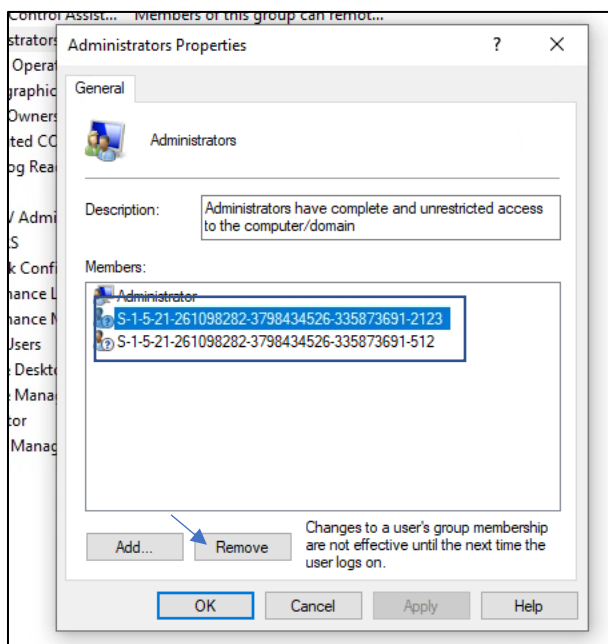
49. **Close/Cancel** the error message and the Elias.Ruiz-adm **properties** page

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

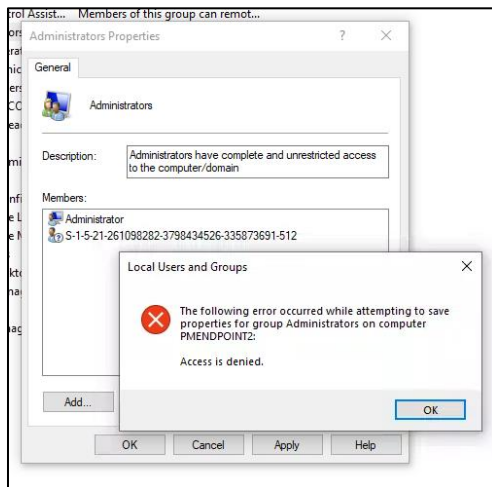


51. **Double-Click** the **Administrator** group to open the **properties** page. You may not see the **Thycotic-US-Help_Desk** group here until after the machine reboots, but you should see the Administrator account and some obfuscated accounts listed. Privilege Manager will also clean the obfuscated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

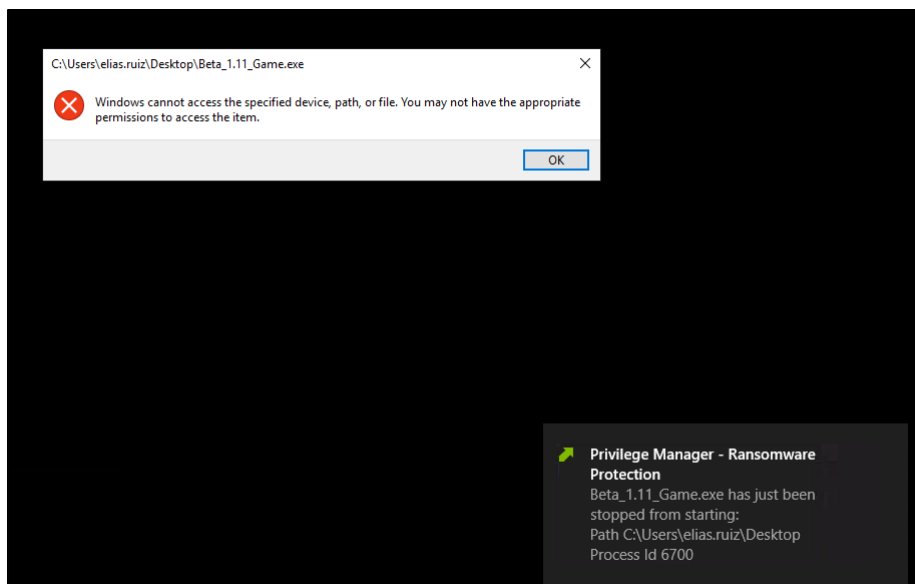
52. **Click** one of the **obfuscated accounts** and select **Remove**



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.



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.



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!