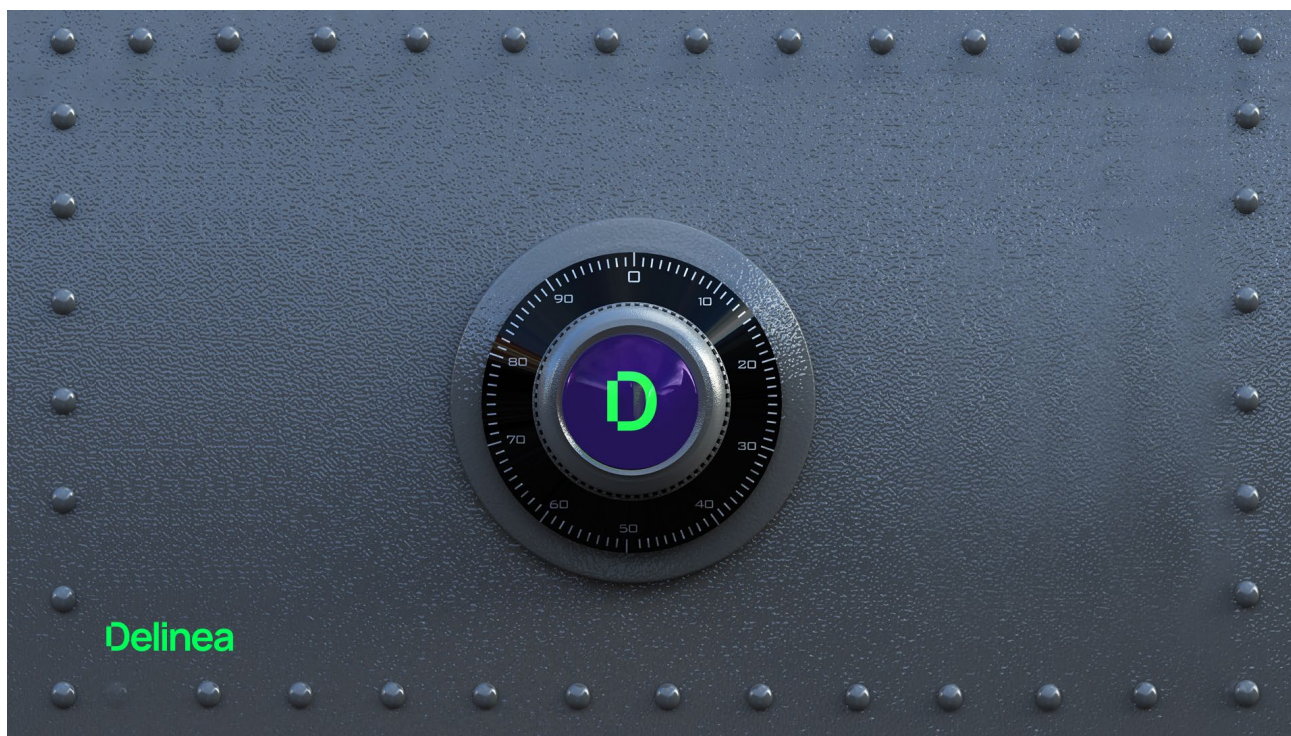


Delinea Privilege Manager



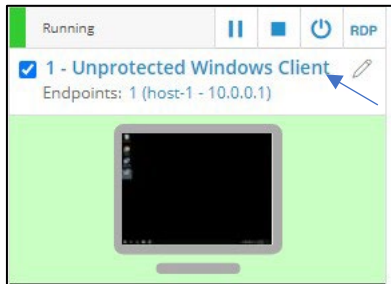
Becoming more Resilient against Ransomware with Proven PAM Strategies

Contents

Section 0: Access Hands-On Lab Environment.....	3
Section 1: Malicious Application Running on an Unprotected Endpoint	5
Section 2: Implement Active Controls to Prevent Ransomware Attacks using Privilege Manager.....	6
Section 3: Implement Active Controls to Prevent Ransomware Attacks using Privilege Manager.....	17
About Delinea	26

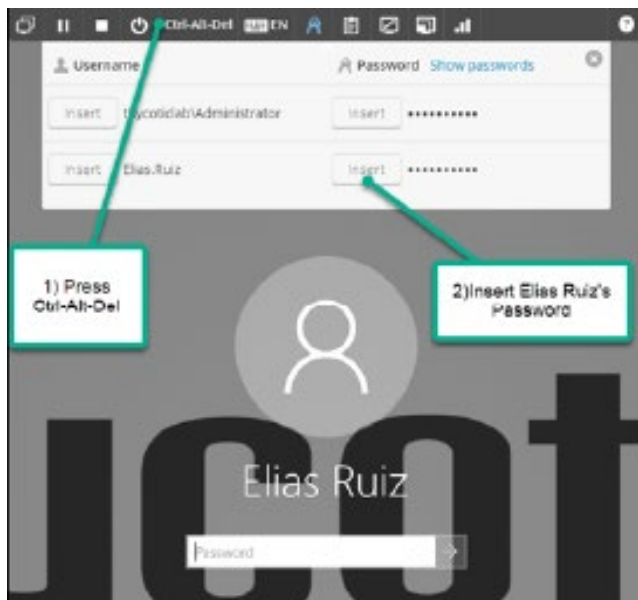
Section 0: Access Hands-On Lab Environment

- 1 The leader of this session will specify how to get to your lab environment.
- 2 Open the **1 - Unprotected Windows Client** Virtual Machine by selecting the name

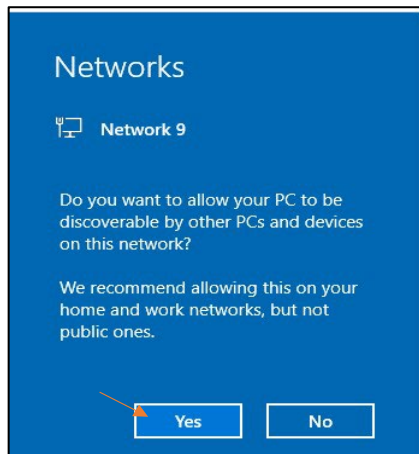


- 3 Login to the client using the following credentials:
 - Username: Elias Ruiz
 - Password: ThycoticDemo!

Note: You can also use the keys icon on the Skytap bar



- 4 Select **Yes**, if prompted with Network Settings



- 5 Locate the Skytap toolbar at the top of your Virtual Machine and expand it, if necessary, by selecting the arrow

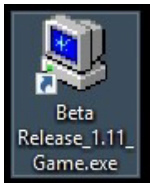


- 6 Select the Fit to Window button. This will allow you the maximum amount of workspace to complete this hands-on lab.



Section 1: Malicious Application Running on an Unprotected Endpoint

- 1 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



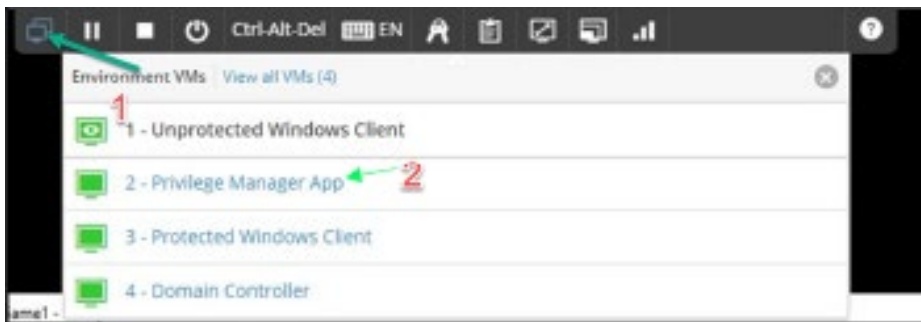
- 2 The Beta Release of the game does NOT open, instead you receive a pop-up informing you that your machine has been hit with a Ransomware attack!



- 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

1. Expand the **Skytap Toolbar** at the top of your virtual machine and select the **Stacked Monitors**
2. Open the "2 - Privilege Manager App" Virtual Machine by selecting the name.

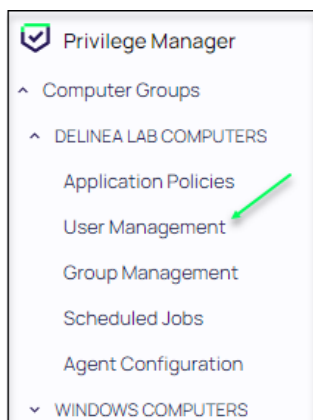


3. Login using **THYCOTICLAB\Administrator** and password **ThycoticDemo!**
4. Open **Chrome**
5. Click the **Privilege Manager** shortcut in the top left corner to open the UI.

Note: In some cases the UI of Privilege Manager does not start. In those cases, close the tab of Privilege Manager and add a new tab and click the Privilege Manager shortcut in the top left corner to open the UI.

6. The Privilege Manager User Interface should be open. However, if you are prompted with a login screen enter the following then select the **Login** button.
 - Username – **Admin**
 - Password – **ThycoticDemo!1**

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



8. On this page you can see the **local accounts** on the endpoints within the **Delinea 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

Create User

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

9. 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.

10.

The screenshot shows the 'Account Details' tab for the 'Elias.Ruiz-Adm' account. The 'User Managed' toggle is highlighted with a green box and is currently set to 'Not Configured'. Below this, the 'User Name' and 'Full Name' are listed as 'Elias.Ruiz-adm'. The 'Description' field is empty. A note on the left states: '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.'

11. 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.

A close-up of the 'User Managed' toggle switch, which is now set to 'Yes'. A green arrow points to the toggle switch.

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

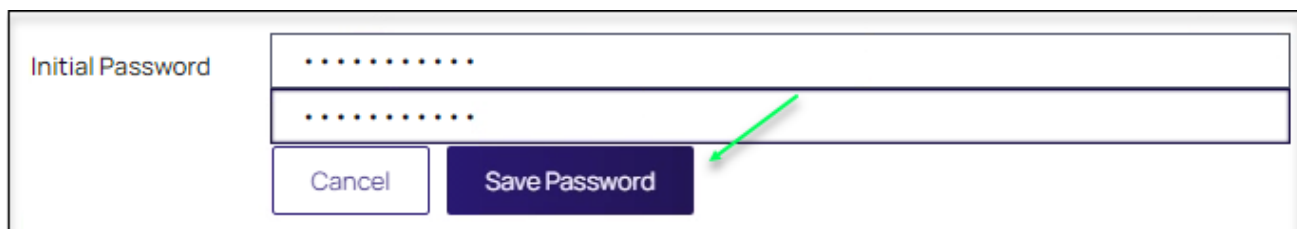
Two side-by-side close-ups of the 'Account is Disabled' toggle switch. The left one is set to 'No' and the right one is set to 'Yes', both with green arrows pointing to the toggle.

13. 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](#)

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



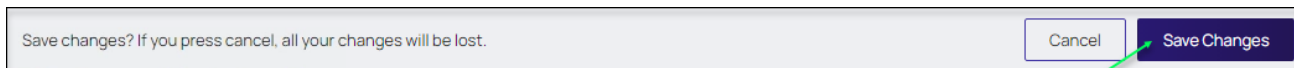
Initial Password

.....

.....

[Cancel](#) [Save Password](#)

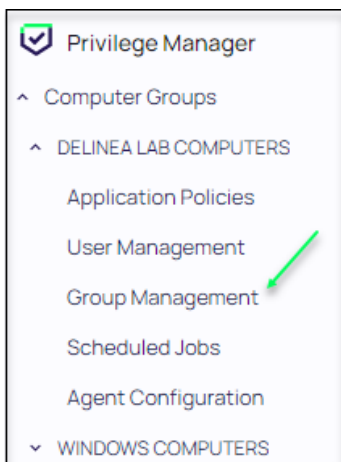
15. Select the **Save Changes** button at the top of the page and you have taken ownership of this account. (For extra credit, you could select the **Account Password** Tab to setup a password rotation and randomization schedule for the local account, but we won't cover that in this lab.)



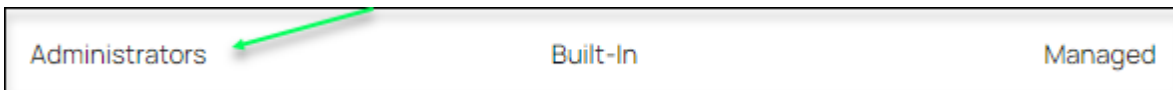
Save changes? If you press cancel, all your changes will be lost.

[Cancel](#) [Save Changes](#)

16. Select the **Group Management** option under **Delinea Lab Computers**




17. 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**



18. On this page, you can review the accounts that are currently 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**



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

			Add Member
COUNT	OPERATION		
2	Required Account		
1	Ignore if found	▼	ⓘ
0	Add if missing	▼	Remove

20. In the **“Type”** dropdown, 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 Users

Local Users (Manual Entry)

21. 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

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

Domain Group

Name ⓘ

Thycotic

Cancel

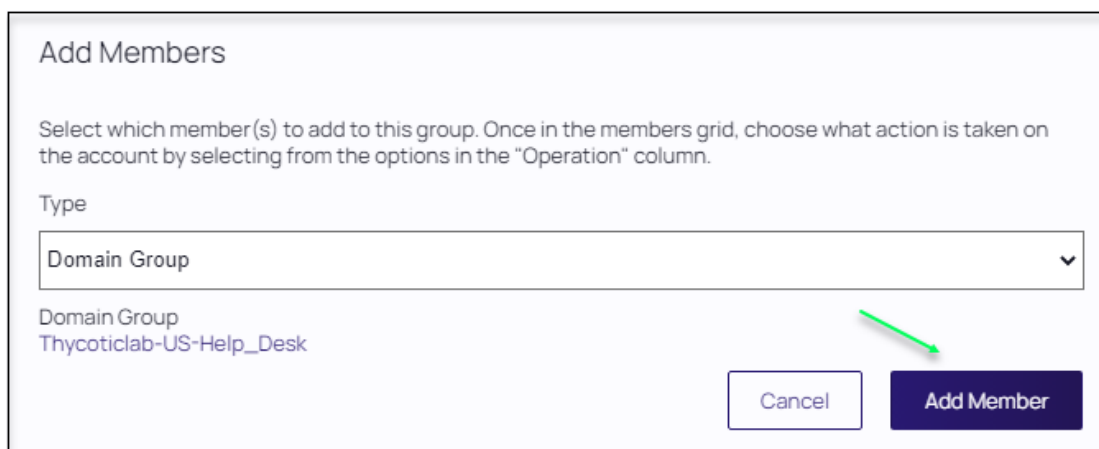
Search

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

Thycoticlab-US-Help_Desk

THYCOTICLAB

24. Click **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

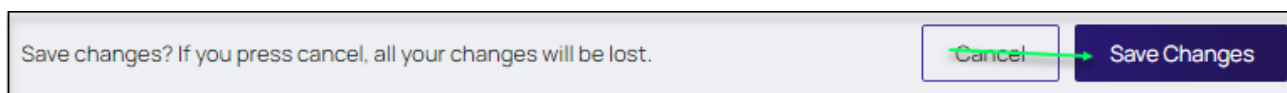
Cancel Add Member

25. 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 Delinea 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.



Domain Admins (THYCOTICLAB)	Domain Group	1	Add if missing
-----------------------------	--------------	---	----------------

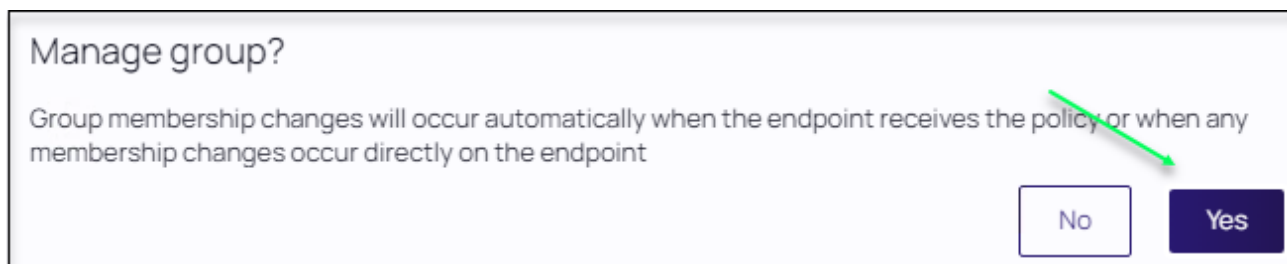
26. Select **Save Changes**. We will test these controls when we log into the protected machine later in this lab.



Save changes? If you press cancel, all your changes will be lost.

Cancel Save Changes

27. Click **Yes** to confirm the **Manage Group** setting

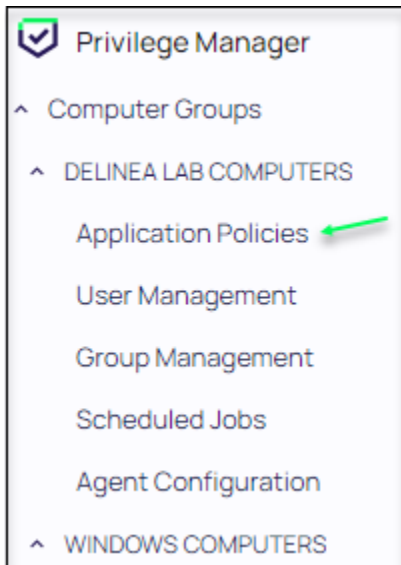


Manage group?

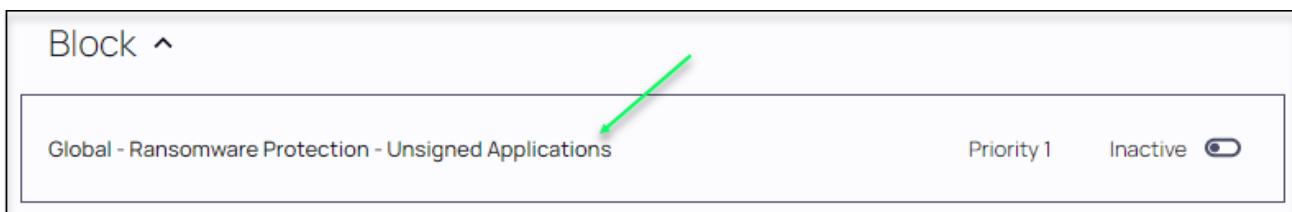
Group membership changes will occur automatically when the endpoint receives the policy or when any membership changes occur directly on the endpoint

No Yes

28. 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 **Delinea Lab Computers**



29. 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



30. Notice that the Policy shows:

1. **Computer Groups Targeted** – Which group(s) of endpoints have this Policy applied
2. **Deployment** – How many of the endpoints targeted have the most up-to-date Policy
3. **Last Modified** – When the Policy was last changed and by which user
4. **Priority** – The order Policies will apply on the endpoint(s)
5. **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.

1	Computer Groups Targeted	1 (4 total endpoints) Delinea Lab Computers	Edit
2	Deployment ⓘ	Not deployed (Policy is inactive)	
3	Last Modified	Aug 23, 2022, 10:21:06 AM by Privilege Manager Admin	
4	Priority *	<input type="text" value="1"/>	
5	Description	Denys any unsigned application, even if it generates a User Account Control (UAC) dialogue.	

31. 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	Application Denied Message Action Deny Ransomware Message	Edit
Child Actions	Deny Ransomware Message	Edit
Audit Policy Events	<input checked="" type="checkbox"/> Record all activity detected by this policy in Policy Events	

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



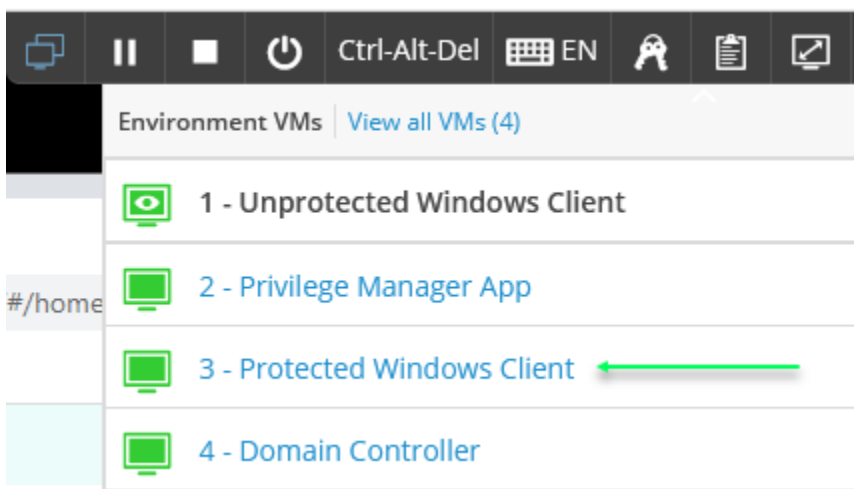
33. Now that the **Policy is Active**, continue to the next steps to walk through applying and testing the newly implemented endpoint controls

Section 3: Implement Active Controls to Prevent Ransomware Attacks using Privilege Manager

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



2. Select the “**3 – Protected Windows Client**” Virtual Machine by selecting the name

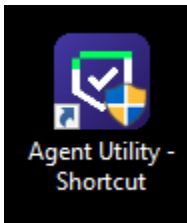


3. Login to the Protected Windows client using the following credentials:
 - Username: Elias Ruiz
 - Password: ThycoticDemo!
4. Select **Yes**, if prompted with Network Settings

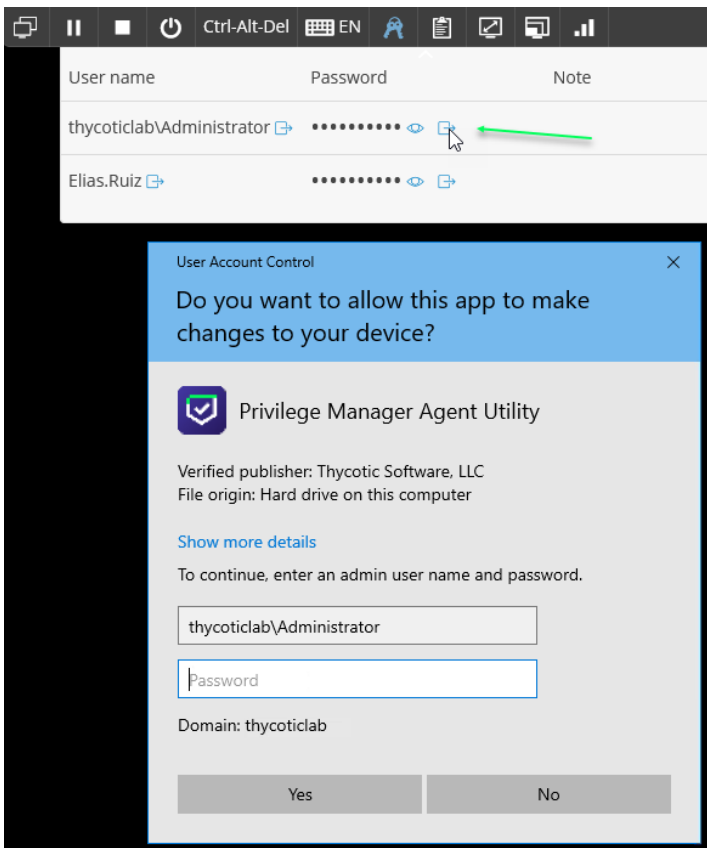
Note:

The Privilege Manager agent has already been installed and registered to the Privilege Manager server. To read more on the process steps, please look at <https://docs.delinea.com/pmgr/current/agents> for the details.

5. On the desktop click the **“Agent Utility - Shortcut”**

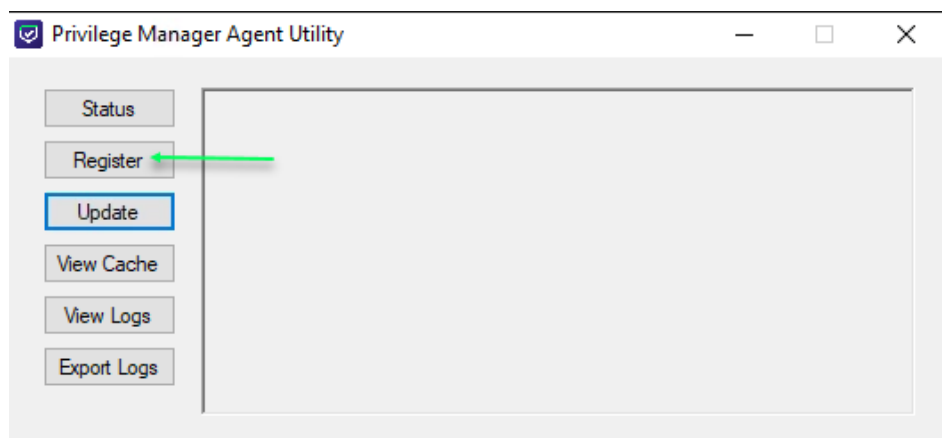


6. You will be prompted for the administrator credentials. Enter them from the keys icon in the toolbar again.



7. 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.

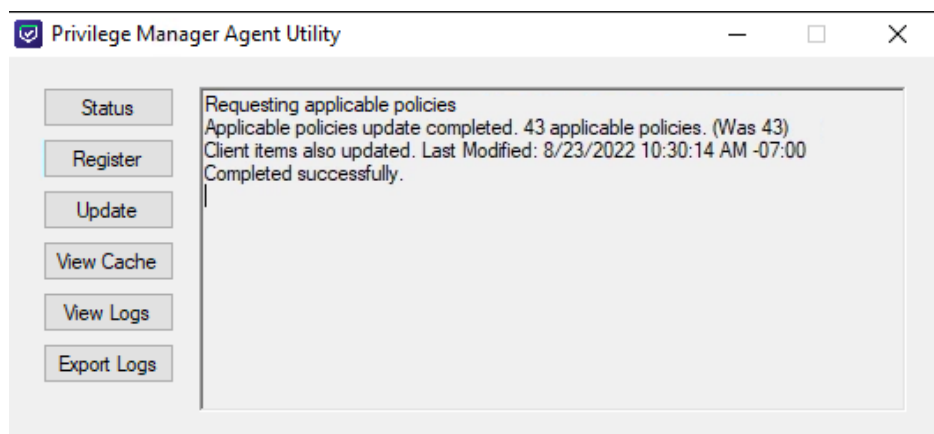
8. Select the **Register** button to connect the agent to the app.



9. Select the **Update** button in the **Privilege Manager Agent Utility**, once you see the Policy shown as added. It will be showing in green. 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.

Note:

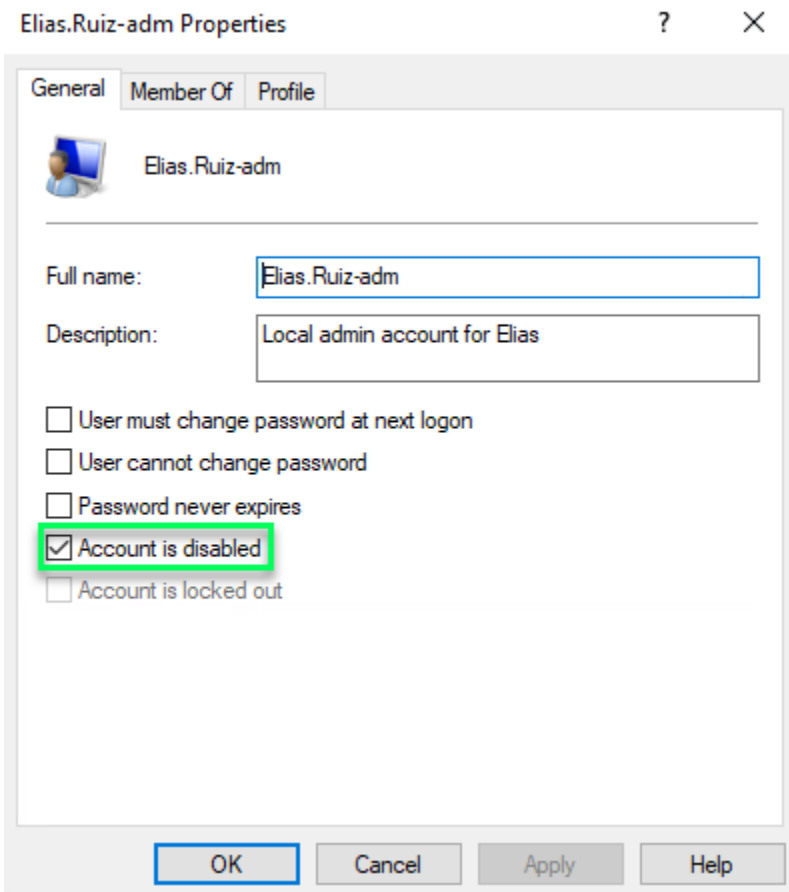
If you waited too long, the agent will have pulled the new policy and you will not see the green line mentioning the policy got pulled from the server. The agent is configured to pull policies every 5 minutes.



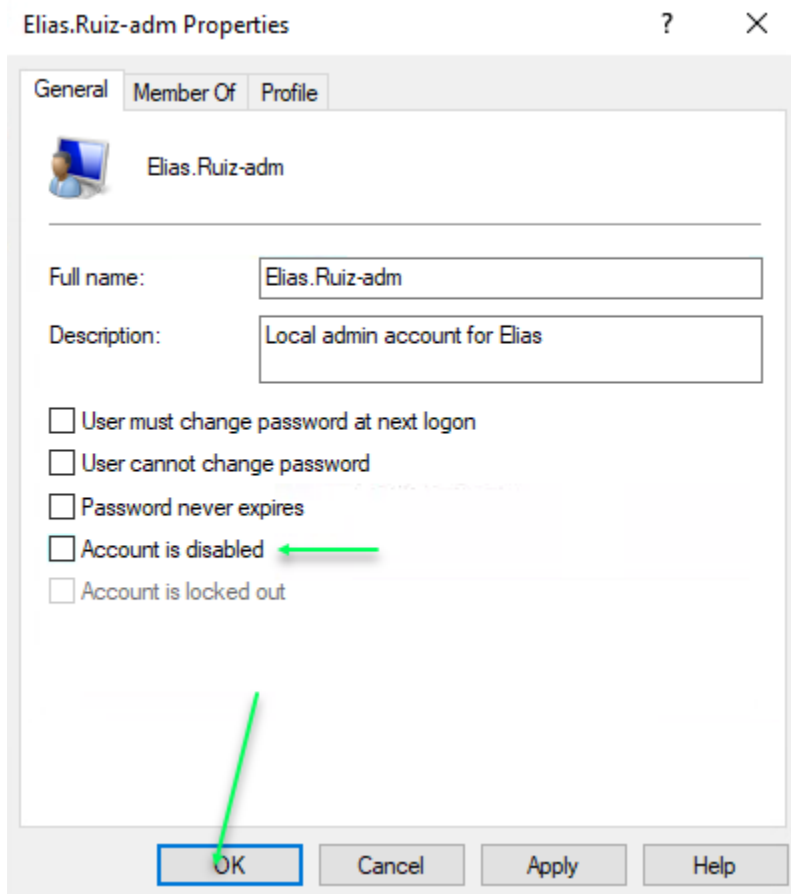
10. Now open **Computer Management** from the Desktop. As a VP of Product Management, Elias may need to perform certain tasks in Computer Management, but actions like changing memberships of local groups or changing attributes of certain local users should be restricted.



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



12. De-select **Account is Disabled** and select **OK**



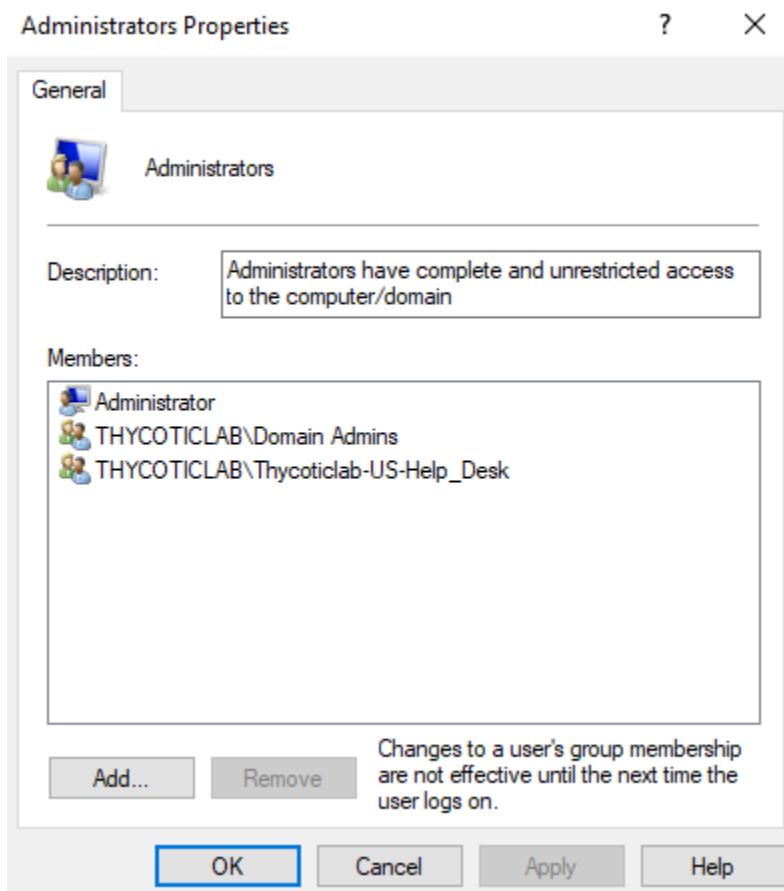
13. You should get an **Access Denied** Error. Notice that even though it seemed you were able to disable this account the **Privilege Manager agent didn't allow the change to save**. The local account settings on the endpoint will always match what is in Privilege Manager after ownership has been taken. Most Privilege Manager administrators would take the restrictions a step further by blocking access to the Management plugins the user shouldn't be using.

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

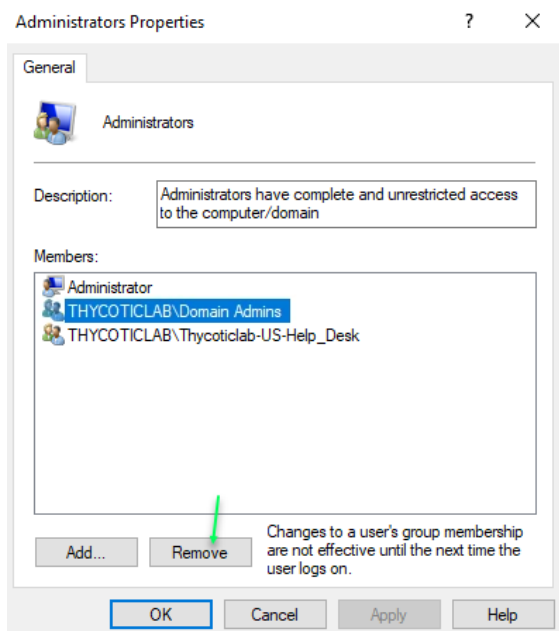
15. Select the **Groups** folder under **Local Users and Groups**



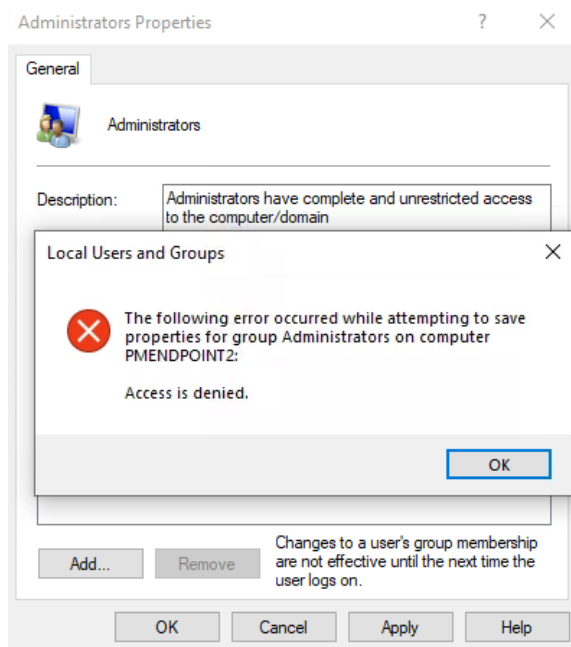
16. **Double-Click** the **Administrators** group to open the **Properties** page. You will see the **Thycotic-US-Help_Desk** group here.



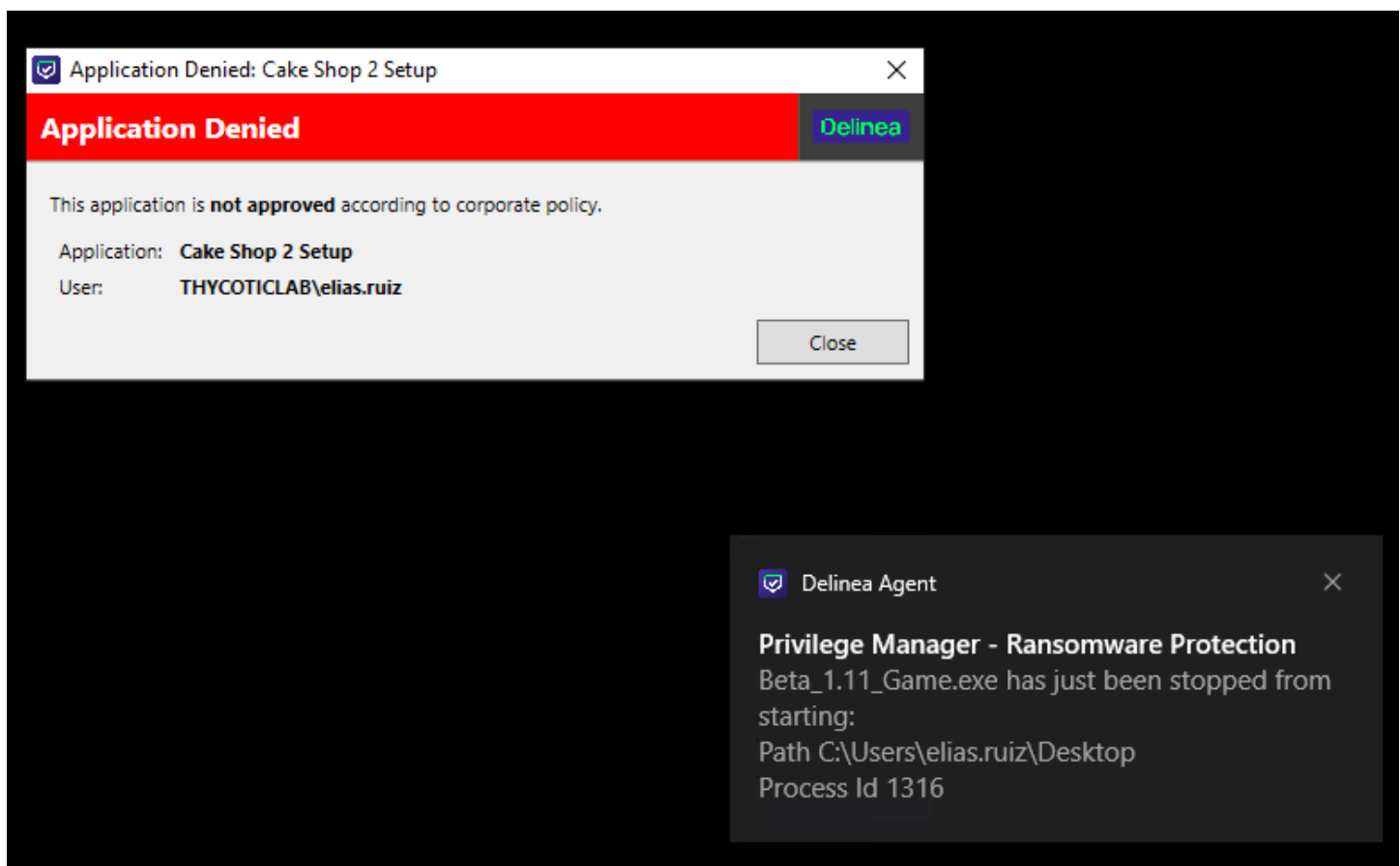
17. Click on the **THYCOTICLAB\Domain Admins** account and select **Remove**



18. 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.

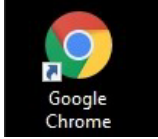


19. Select **OK** to close the **Access Denied** message
20. Select **Cancel** to close the **Administrator group Properties** page. Minimize **Computer Management**
21. Now confirm you can no longer open the unsigned and unknown **Beta_1.11_Game** application by **selecting the application** from the **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.



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

23. 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.



24. Close **Google Chrome**

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

About Delinea

Delinea is a leading provider of privileged access management (PAM) solutions for the modern, hybrid enterprise. We make privileged access more accessible by eliminating complexity and defining the boundaries of access to reduce risk, ensure compliance, and simplify security. Delinea empowers thousands of customers worldwide, including over half the Fortune 100. Our customers include the world's largest financial institutions, intelligence agencies, and critical infrastructure companies.

delinea.com