



## **Privilege Manager Ransomware**

---

Becoming More Resilient against Ransomware with  
Proven PAM Strategies



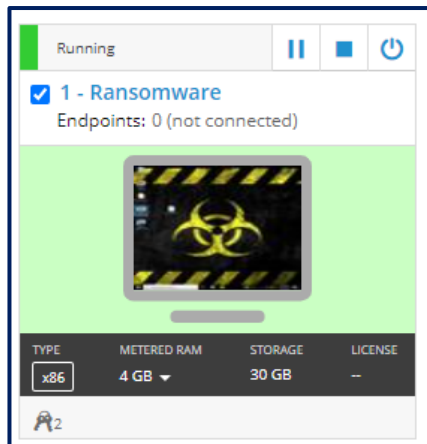
# Table of Contents

- 1. Access Hands-On Lab Environment.....
- 2. Malicious Application Running on an Unprotected Endpoint.....
- 3. Implement Active Controls to Prevent Ransomware Attacks using Privilege Manager.....
- 4. Active Controls Protecting an Endpoint from Ransomware.....
- 5. About Delinea .....

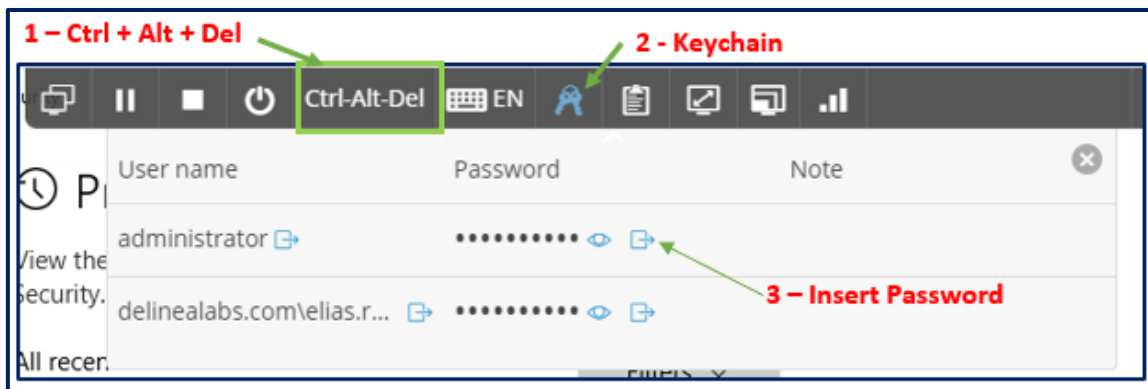
## Section 1: Access Hands-On Lab Environment

The leader of this session will specify how to get your lab environment.

1. Open the **1- Ransomware** virtual machine by selecting the name

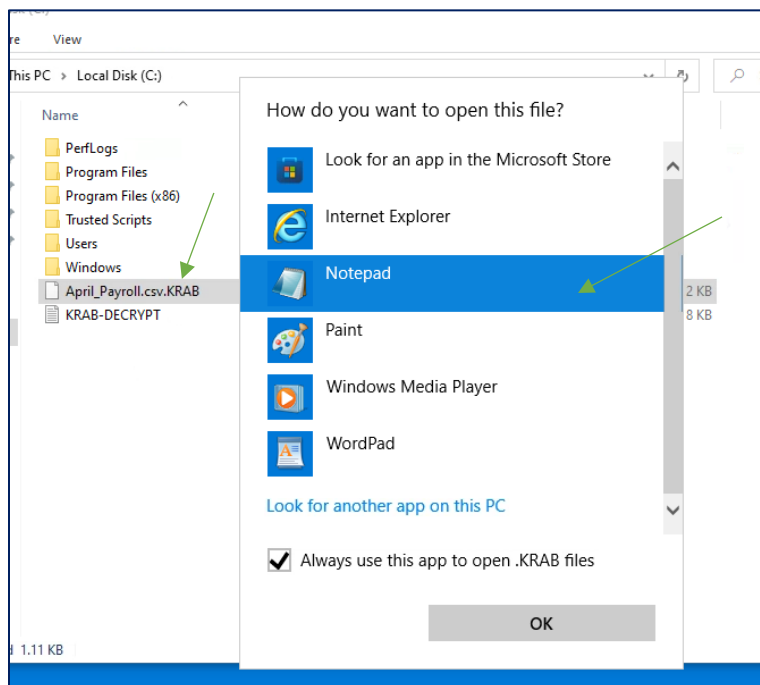


2. Select **Ctrl+Alt+Del** in the **Skytap toolbar** then *Login* with the **Elias Ruiz** account, also stored in the skytap toolbar

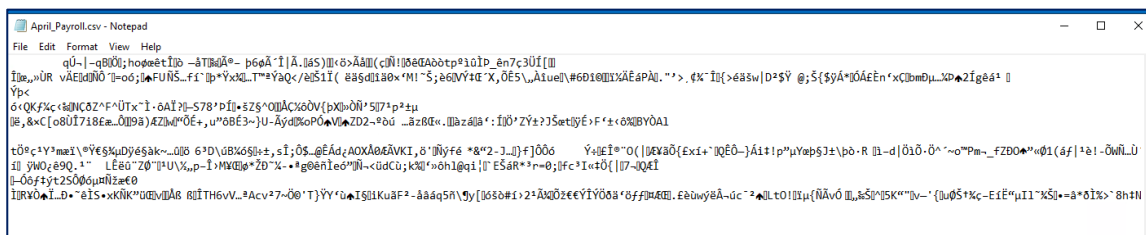


## Section 2: Malicious Application Running on an Unprotected Endpoint

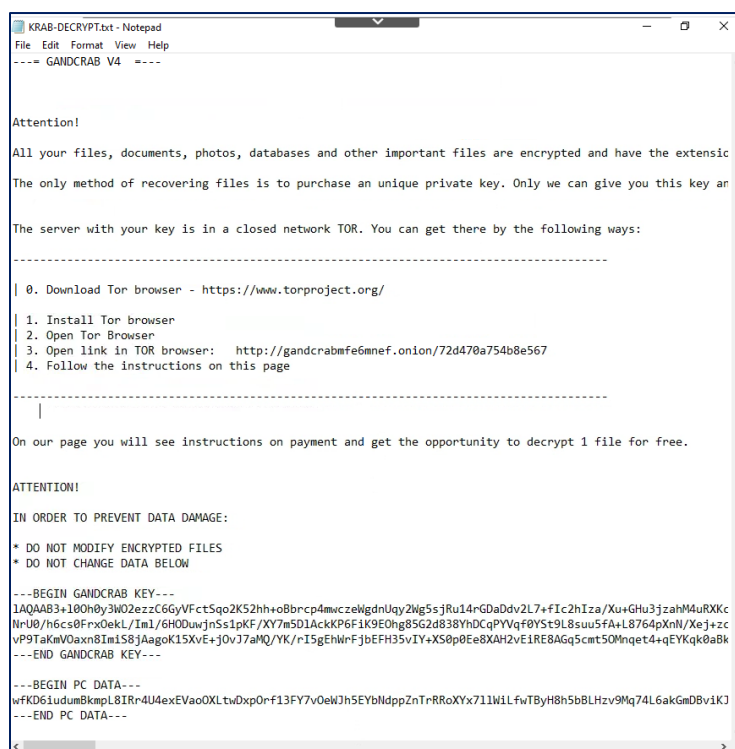
3. In this scenario, you are the Chief Financial Officer for a software company. You've downloaded the Firefox installer on your computer because your new laptop only came with Edge and Chrome installed. *Double-Click* the **Firefoxinstaller.exe** on the **Desktop** to run the installer.
4. *Select* **Yes** to bypass the UAC prompt
5. In this case, the **Firefox Installer** does not open as expected. You instantly think something may be wrong!
6. *Navigate* to the **C Drive** and try to view your company's payroll information by *Opening* the **April\_Payroll.csv** file with **Notepad**.



7. Notice this file has already been encrypted! **Close** the **April\_Payroll** file and any program compatibility prompts that may show.



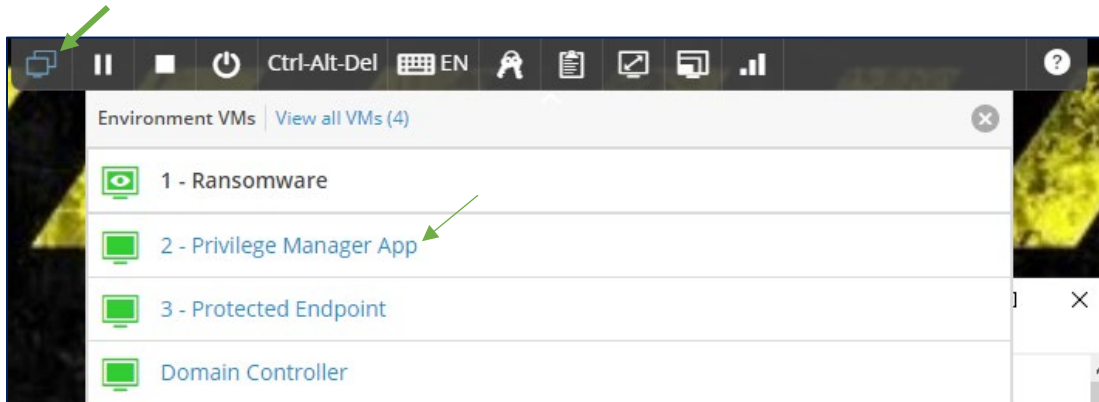
8. You've completely lost access to all payroll information. *Open* the **KRAB-DECRYPT.txt** file that should show under the C drive. Notice that it gives you directions on how to regain access to your data. You've experienced a **Ransomware Attack**!



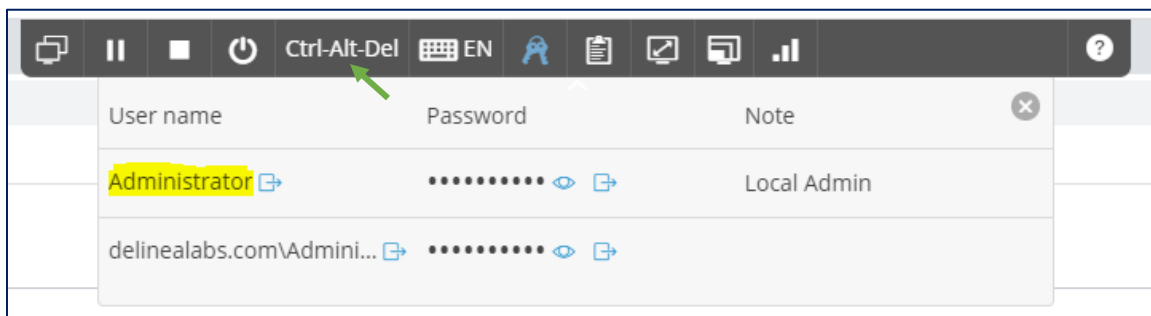
## Section 3: Implementing Active Controls to Prevent Ransomware Attacks using Privilege Manager

### Section 3.0 Accessing Privilege Manager

9. Use the Skytap toolbar to *Switch* from the **1-Ransomware** to the **2- Privilege Manage App** endpoint.



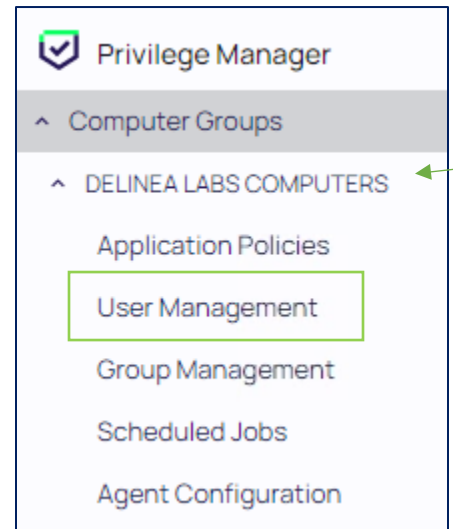
10. If needed, *Select* **Ctrl+Alt+Del** in the **Skytap toolbar** and *Login* with the **Administrator** account.



11. *Open* **Chrome**. The Privilege Manager URL should automatically open, but if it does not *Select* the **Privilege Manager bookmark** to open the Privilege Manager Application.
12. You should be *automatically logged* into **Privilege Manager**; however, if you need to *Login* use the **Administrator** account stored in the Skytap toolbar

### Section 3.1 Controlling Local Users with Privilege Manager

13. *Expand the Delinea Labs Computers Computer Group and Select User Management.*
14. 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. The information showing under User Management shows that **Jordan** has a local admin account that he should NOT have on this machine – “**Jordan Goode**”
15. Let's act on this information. *Select the Jordan Goode account.* Under the **Account Details** page 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 Management	
7 Items	Built-In: All ▼ Managed: All ▼ 🔍
USER NAME ↑	
Administrator	
DefaultAccount	
Elearning	
Guest	
Jordan Goode	

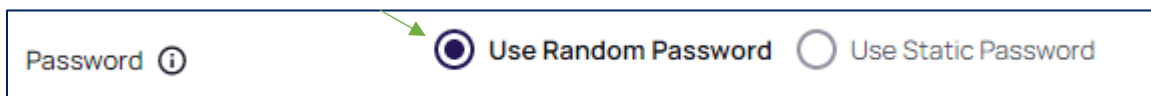
16. Toggle **User Managed** from Not Configured (**No**) to **Yes**. Notice you can change attributes associated with the local account such as the Full Name and Description. These changes will update the accounts attributes in Privilege Manager and on the endpoint.



17. Toggle **Account is Disabled** from **No** to **Yes** since you do NOT want this account to be used any longer.



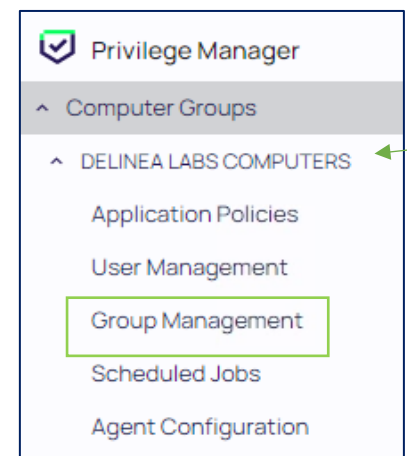
18. You also need to Set a **new password** for this account, so anyone using it previously can no longer access it when/if the account is re-enabled. Select the **Use Random Password** option for the **Password** setting.



19. Select **Save Changes**.

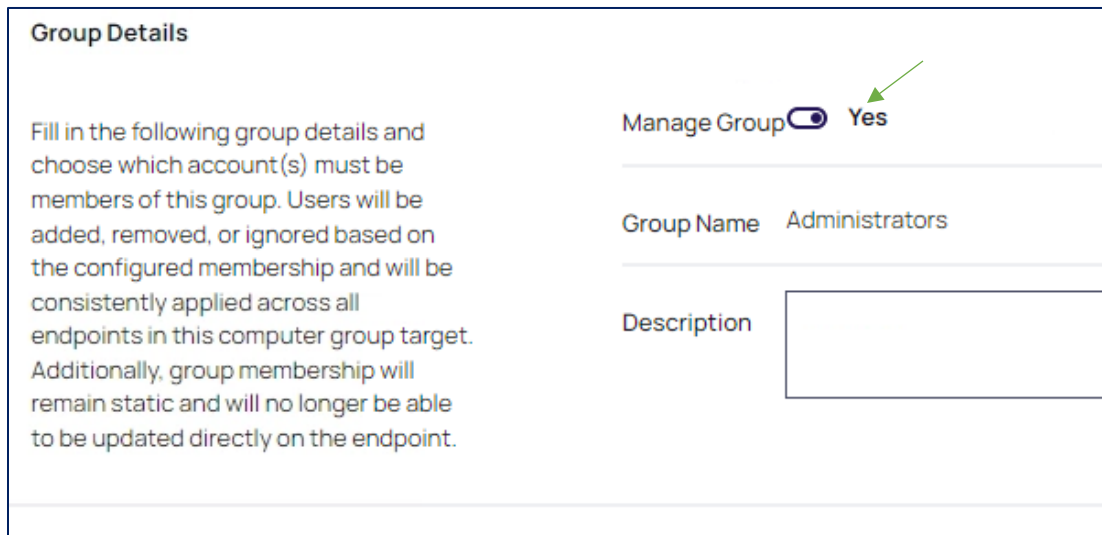
### Section 3.2 Controlling Local Groups with Privilege Manager

20. Select the **Group Management** option under **Delinea Lab Computers**. Here you can take ownership of local groups with Privilege Manager. This means that Privilege Manager will control the membership of the groups, and only users with the appropriate permissions in the application can make changes.
21. Select the **Administrators** group. 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 Windows Operation team members so they can do their duties.





22. Toggle **Manage Group** from **Not Configured** to **Yes**.



**Group Details**

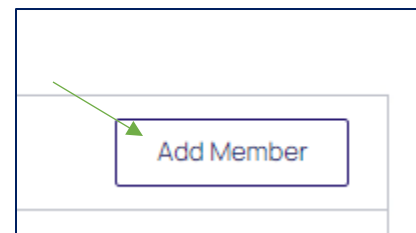
Fill in the following group details and choose which account(s) must be members of this group. Users will be added, removed, or ignored based on the configured membership and will be consistently applied across all endpoints in this computer group target. Additionally, group membership will remain static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

Manage Group ☒ **Yes**

Group Name Administrators

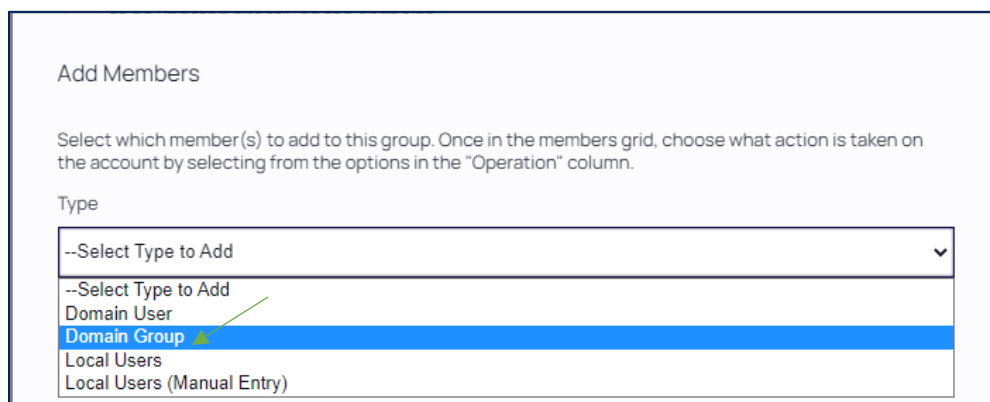
Description

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



Add Member

24. Select **Domain Group** under the **Type** dropdown



**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

--Select Type to Add

--Select Type to Add

Domain User

**Domain Group**

Local Users

Local Users (Manual Entry)

25. Click **Add** to select the additional group(s) you will give access to this Administrators local 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

Nothing selected

Add

Cancel

Add Member

26. Type **Delinealabs** in the *Name* search field and *Select Search*

Domain Group

Name ⓘ

Delinealabs

Search

Cancel

27. Select the **Delinealabs-US-Windows\_Ops** group found on Page 2

Domain Group

Domain Group	Domain Name
Delinealabs-US-VMware_Ops	DELINEALABS
Delinealabs-US-Windows_Ops	DELINEALABS

10 items per page

11 - 12 of 12 items

Cancel

Change Search

28. 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

Delinealabs-US-Windows\_Ops

Cancel

Add Member

29. Notice that **All Other Users and Groups Operation** is set to **Ignore If Found**. Let's implement more restrictive settings for this Administrator group. *Change the **Operation** to **Remove if Found**.*

Members			
4 Items		Add Member	
MEMBER	TYPE	COUNT	OPERATION
Administrator	Local User	1	Required Account
Delinealabs-US-Windows_Ops	Domain Group	0	Add if missing Remove
Domain Admins (DELINEALABS)	Domain Group	1	Add if missing ⓘ
svc_del_disc (DELINEALABS)	Domain User	1	Add if missing ⓘ
All Other Users and Groups ⓘ			Remove if found

30. Notice this change *automatically Sets* the **Operation** for the listed Members to **Add if Missing**. This means all machines currently in or added to the Delinea Labs Computer will have the following members:

- a. **Administrator** Local Windows User
- b. **Delinealabs-US-Windows\_Ops** Active Directory Group
- c. **Domain Admins** Active Directory Group
- d. **svc\_del\_disc** Active Directory service account

Any other accounts/groups attempted to be added to this group will be automatically removed by the Privilege Manager Agent.

Members			
4 Items		<button>Add Member</button>	
MEMBER	TYPE	COUNT	OPERATION
Administrator	Local User	1	Required Account
Delinealabs-US-Windows_Ops	Domain Group	0	<div> <div>Add if missing </div> <div>Remove</div> </div>
Domain Admins (DELINEALABS)	Domain Group	1	<div> <div>Add if missing </div> <div></div> </div>
svc_del_disc (DELINEALABS)	Domain User	1	<div> <div>Add if missing </div> <div></div> </div>
All Other Users and Groups			<div> <div>Remove if found </div> </div>

31. **Select Save Changes.** You will test these controls when you log into the **Protected Virtual Machine** later in this lab.

Administrators

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

Cancel
Save Changes

Group Details

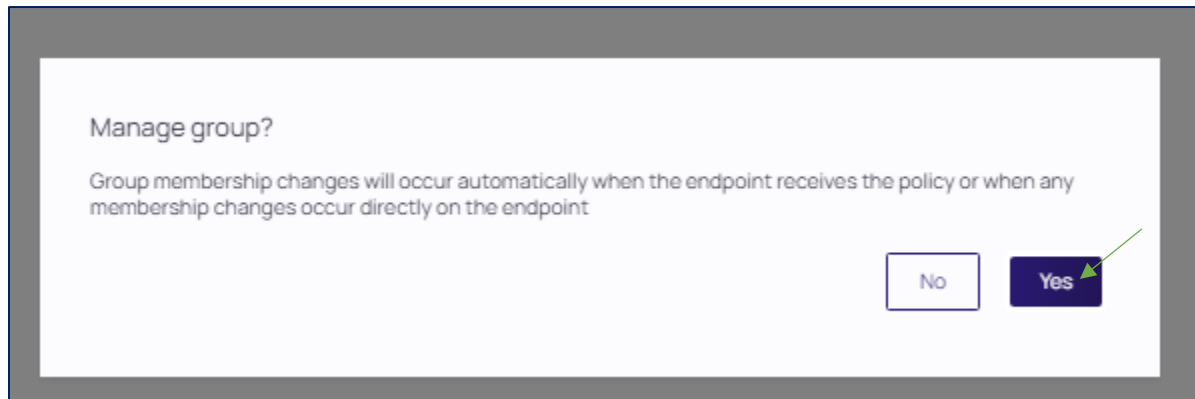
Fill in the following group details and choose which account(s) must be members of this group. Users will be added, removed, or ignored based on the configured membership and will be consistently applied across all endpoints in this computer group target. Additionally, group membership will remain static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

Manage Group
☒ Yes

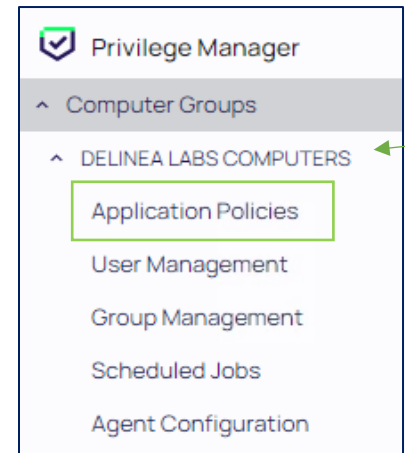
Group Name
Administrators

Description

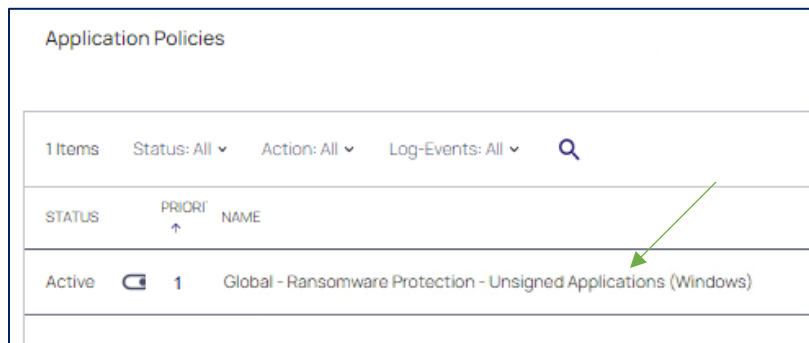
32. Click the **Yes** button to confirm the Manage Group settings



33. Now you've confirmed the Local Admin Rights on the machines within the Delinea Labs Computer Group have been locked down sufficiently. Let's review the Application Control Policies that will stop users from running malicious applications. **Select Application Policies under Delinea Lab Computers**



34. Notice the **Global - Ransomware Protection – Unsigned Applications (Windows)** Policy has already been configured for you, and it has already been activated for use. **Select the Ransomware Protection Policy**



35. Notice that the Policy shows information in **three** Sections:

a) **Policy Details:**

Policy Details allow you to control and view which Computer groups this Policy applies to, and the Priority (Order) of the Policy.

- **Computer Groups Targeted** - Which group(s) of endpoints have this Policy applied
- **Deployment** - How many of the targeted endpoints 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

b) **Conditions:**

Conditions control what needs to happen on the endpoint to trigger a Policy.

- **Application Targeted** – Which applications apply to this Policy
- **Inclusions** – Additional Filters that must be met for this Policy to apply
- **Exclusions** – Additional Filters that, if met, stop this Policy from applying

c) **Actions:**

Actions are what happens when the Policy is triggered.

- **Actions** – Filter that controls what will happen when Policy is triggered.

Global - Ransomware Protection - Unsigned Applications (Windows)

General Policy Events Change History

**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)

Deployment (1)

Last Modified

Priority \* (1)

Description

**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 (2)

Applications Targeted (1)

Inclusions (1)

Exclusions (1)

**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. Log Policy Events reports all application executions back to Privilege Manager's server for this policy

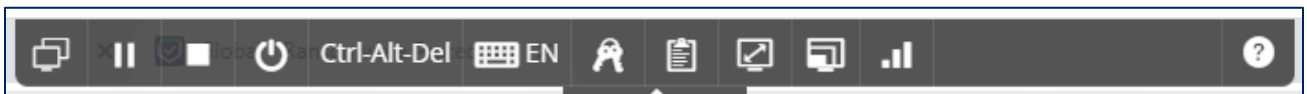
Actions (2)

Child Actions (1)

Log Policy Events

- **Child Actions** – Filter the controls what will happen if any Child Actions are opened
- **Log Policy Events** – If enabled, this will send information back to Privilege Manager

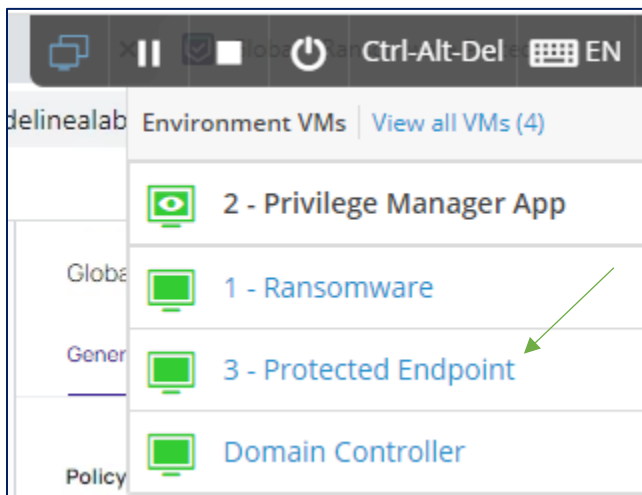
36. Since this Policy is already activated, there are no other steps that need to be taken in Privilege Manager. *Switch* to the **Protected Endpoint** by *Expanding* the **Skytap toolbar**



37. Select the **Computer Monitor** symbol



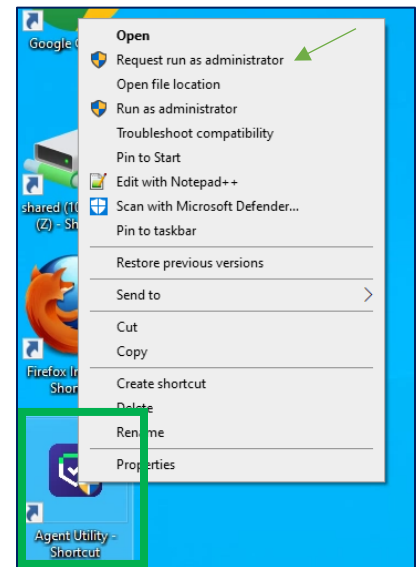
38. Select the **3- Protected Endpoint** link.



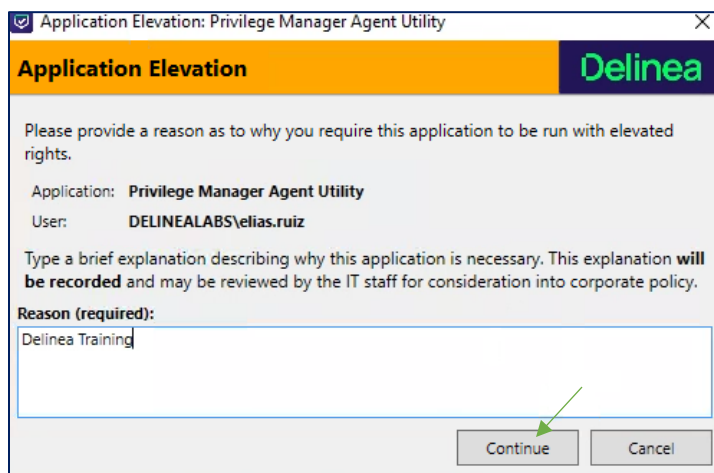
39. Use the **Skytap toolbar** to *Enter* **Ctrl+Alt+Delete** and *Login* with the **Delinealabs\Elias.Ruiz** account

## Section 4: Active Controls Protecting an Endpoint from Ransomware

40. Right-Click the **Agent Utility** from the **Desktop** and **Select Request Run as Administrator**.

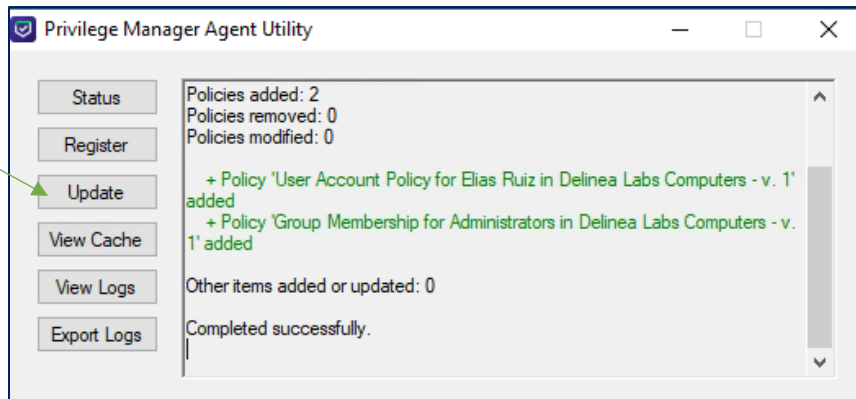


41. You will be prompted with a Privilege Manager **Justification Message** before the Agent is elevated. *Enter the Reason **Delinea Training** and Select **Continue***





42. Select **Update** to update the endpoint with the changes you made in Privilege Manager.



43. Open **Computer Management** from the **Desktop**. As a CFO, Jordan may need to perform certain tasks in Computer Management, but actions like changing memberships of local groups and/or changing attributes of certain local users should be restricted.

44. Expand **Local Users and Groups** and Select **Users**. Double-click the **Jordan Goode** account and notice it is **Disabled**.

45. Un-check **Account is disabled** to Enable the Jordan Goode account.

46. Select **OK**. Notice that even though it seemed you were able to enable this account, the Privilege Manager Agent didn't allow the change to save and gave an Access Denied error.

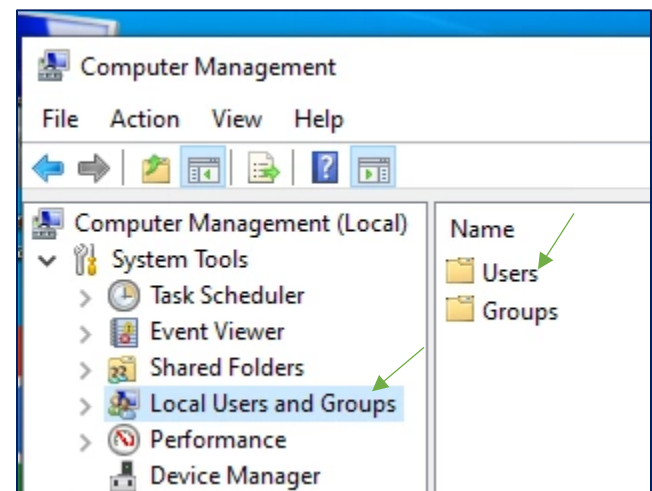
47. Select **OK** to close the error message

48. Select **Cancel** to Close the Jordan Goode Properties page

49. Select the **Groups** folder under **Local Users and Groups** in Computer Management

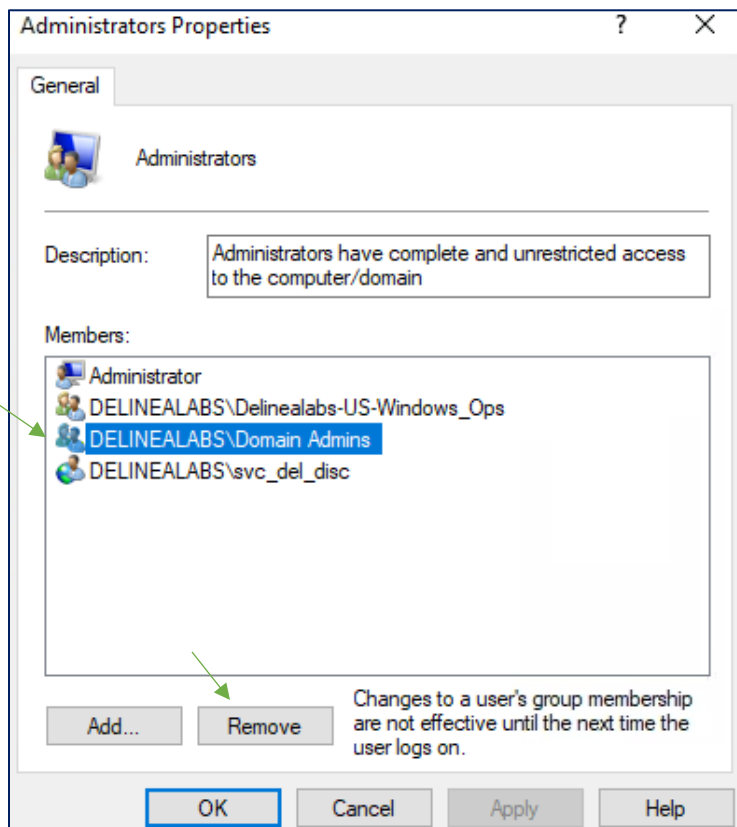
50. Double-Click the **Administrators** group to open the properties page. You will see the:

a. **Administrator** account



- b. **Delinealabs\Domain Admins** groups
- c. **Delinealabs-US-Windows\_ops** group
- d. **Delinealabs\svc\_del\_disc** account

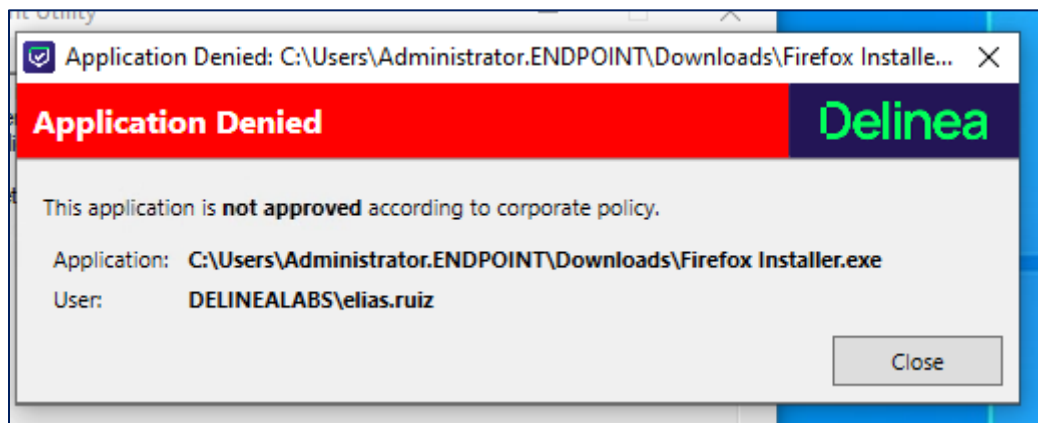
51. Click the **Delinealabs\Domain Admins** group and *Select Remove*. Click **OK**



52. *Select OK*. Again, it seems you can remove the group but you get an access denied error. *Close* the error message and *Select Cancel* on the **Administrators Properties** page.

53. *Reopen* the **administrators** group and you see the Domain Admins groups is still there. 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. Click **Cancel** to close the Administrator Group properties page.
55. Close **Computer Management**
56. Attempt to *Open* the **Firefox Installer-shortcut** from the **Desktop** and *Select Yes* to any prompts.
57. You will receive an **access denied error**. This application is no longer able to run on this endpoint which helps to protect this endpoint from a possible cause a Ransomware attack.



58. Close the **Application Denied** Message. 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 Delinea Ransomware Protection hands-on lab. Please let your instructor know if you have any additional questions!

You have successfully completed this hands-on lab! You should now have a better understanding of how to:

- Manage and deploy a Privilege Manager Policy to protect unknown applications from running on an endpoint
- Manage local users and groups to enforce least privilege controls that will help to protect against a Ransomware attack

## 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.