



Creating/Configuring Amazon WorkSpaces Bundles with CyberArk Endpoint Privilege Manager

CONFIGURATION & STEPS

To create a WorkSpaces bundle, please follow the instructions outlined on the documentation provided in the link below:

https://docs.aws.amazon.com/workspaces/latest/adminguide/create-custom-bundle.html#custom_image_best_practices

Before the step that asks to run the Image Checker, on the documentation referenced above, you will need to perform the following steps based on the documentation for CyberArk Endpoint Privilege Manager.

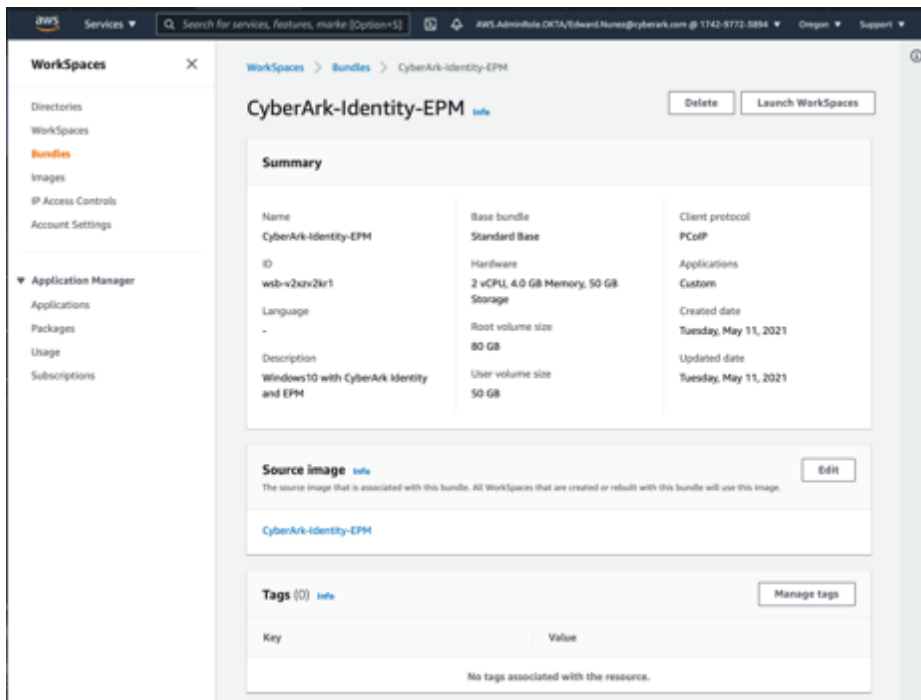
<https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM/Latest/en/Content/Installation/Windows-InstallAgents.htm>

1. Follow the instructions outline here: <https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM/Latest/en/Content/Installation/Windows-InstallAgents.htm>
Once you download the installation package, enter an installation key that will be used later on this guide. Place the installation package in a location in C: Drive that will be available when performing step 3 below.
2. We will configure a silent install for Manual installation on Windows Immediate Enforcement Agents as detailed here: <https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM/Latest/en/Content/Installation/Windows-InstallAgents.htm#ManualinstallationonWindowsImmediateEnforcementAgents>
3. On the WorkSpace that you're using to create your custom image, open C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml in Notepad or another text editor, and define the command to perform the silent install for the CyberArk EPM Agent. This can be defined in the oobeSystem pass with a command to be executed on first logon (within the component named "Microsoft-Windows-Shell-Setup") to the WorkSpace, and it should look like this:

```
<settings pass="oobeSystem">
  <component name="Microsoft-Windows-Shell-Setup" ...>
    ...
    <FirstLogonCommands>
      <SynchronousCommand wcm:action="add">
        <Order>1</Order>
        <Description>Install CyberArk EPM Agent</Description>
        <CommandLine>msiexec /i "**FULLPATH-TO-EPM-INSTALLATION-PACKAGE**" INSTALLATIONKEY=**INSTALLATION-KEY**
      /qn</CommandLine>
      </SynchronousCommand>
    </FirstLogonCommands>
  </component>
  ...
</settings>
```

Replace the corresponding values for ****FULLPATH-TO-EPM-INSTALLATION-PACKAGE**** and ****INSTALLATION-KEY**** from step 1 above. Save the file.

4. Once previous steps are done, you can proceed with the AWS Image Checker and subsequent steps as defined in the document (listed at the beginning of this guide) to finish up the WorkSpace image and bundle creation.
5. Once the bundle is created, you can use it to launch new WorkSpaces which will be automatically enrolled with CyberArk EndPoint Privilege Manager.



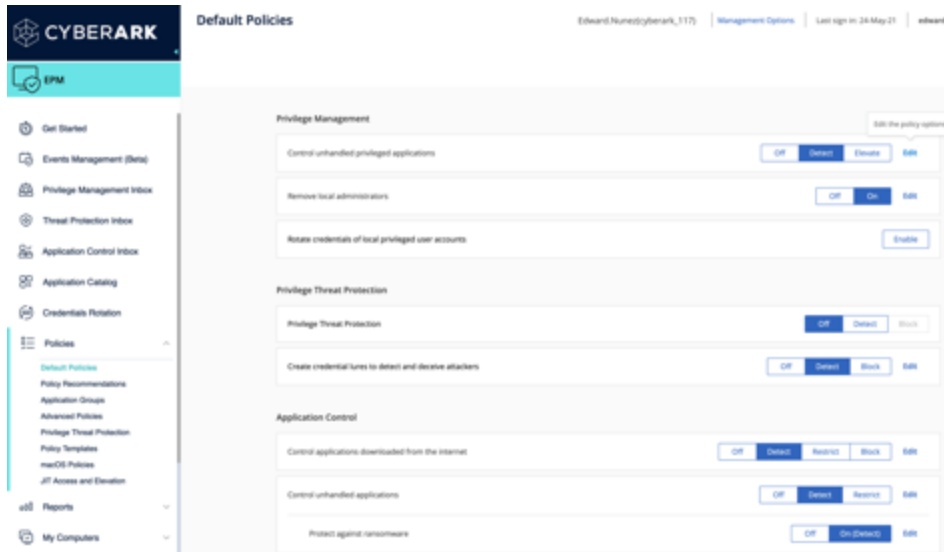
6. On first logon, the installation for the CyberArk EPM Agent should be triggered, and the new WorkSpace should be listed as a computer in the CyberArk EndPoint Privilege Manager.

The screenshot displays the CyberArk 'My Computers' interface. The left sidebar contains navigation links for EPM, Application Catalog, Credentials Rotation, Policies, Reports, My Computers (selected), and Threat Intelligence. The main content area shows a list of computers under the heading 'Computers - Total 2'. Two computers are listed: 'YOSHIKAZU.MITLABS' and 'YOSHIKAZU.RBPT.GRHE'. The table columns are: Computer, Logged in, Agent Connectivity Status, Agent Operational Alert, Application Catalog, and Threat Protection.

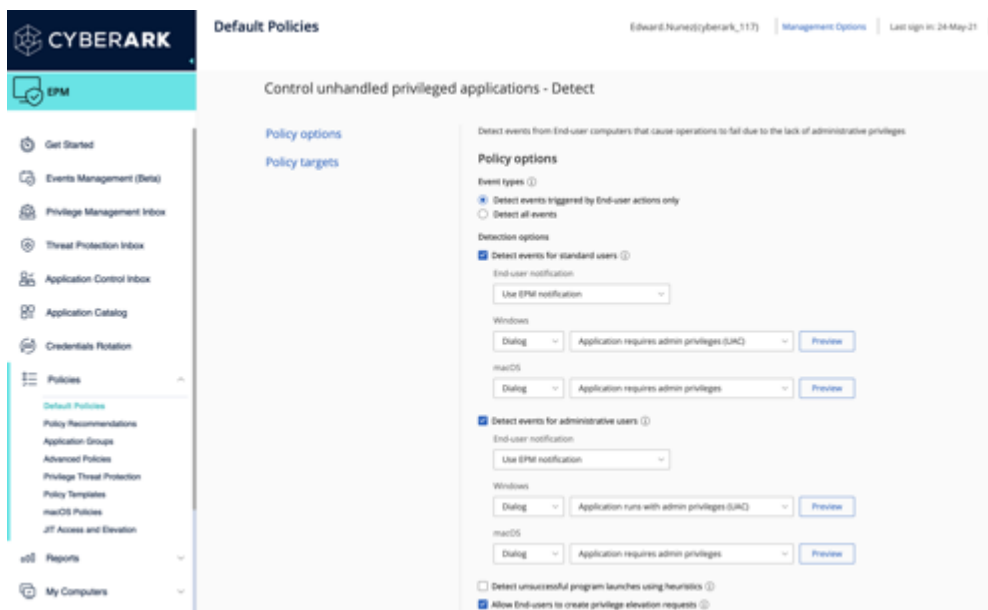
Computer	Logged in	Agent Connectivity Status	Agent Operational Alert	Application Catalog	Threat Protection
YOSHIKAZU.MITLABS		Disconnected (Last seen)			N/A
YOSHIKAZU.RBPT.GRHE	CASCI@helgebric	Disconnected (Last seen)			N/A

CYBERARK EPM – USE CASES & BEST PRACTICES

As best practice, CyberArk recommends removing local administrators from endpoint computers. For this, set to “On” the value for “Remove local administrators”, you can configure exceptions in the policy options. The idea is to have least-privileged users. They can escalate requests when they need to perform tasks with administrative permissions.



You can also configure the dialog to be shown when escalations are to be requested and detected by CyberArk EPM.



Once policy is configured, on next logon/restart the local administrator users will be removed.

Figure 1 Before Removal

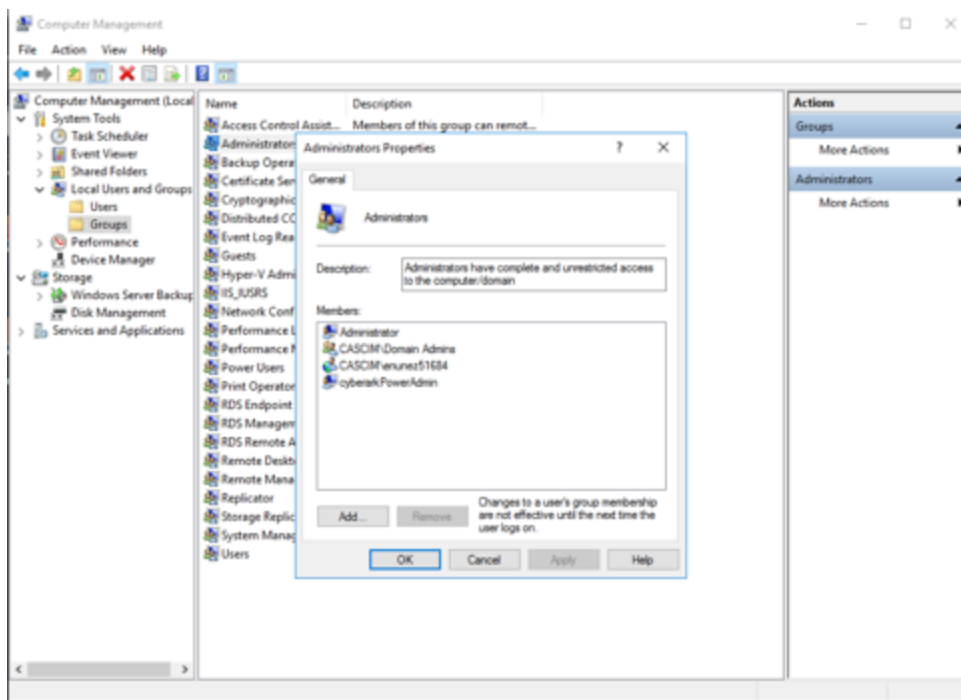
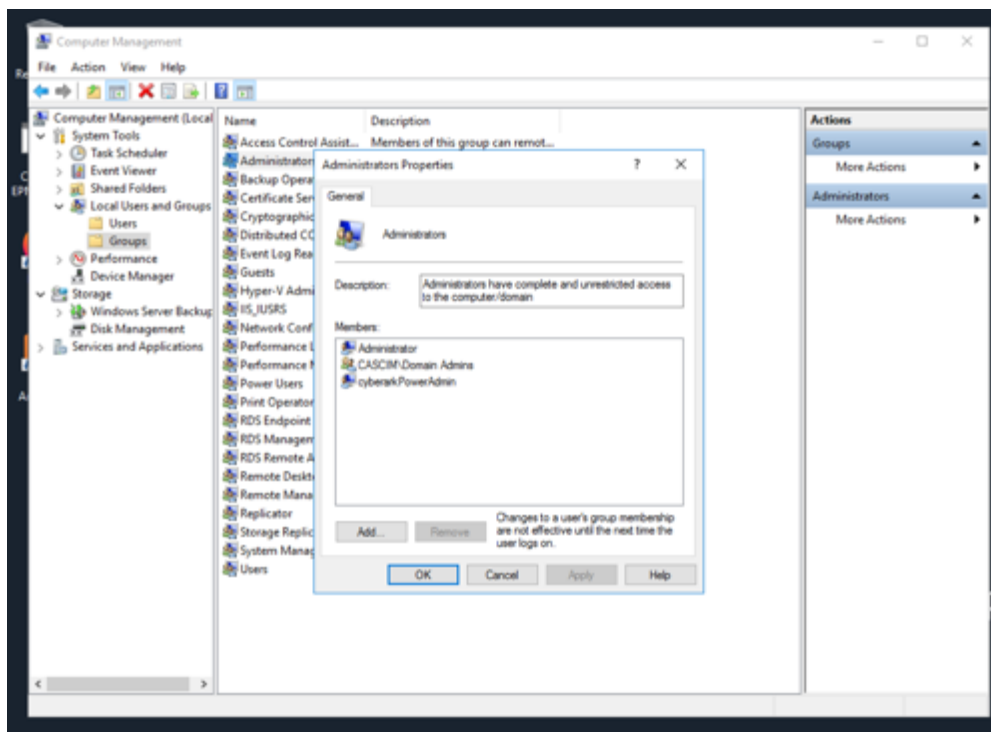
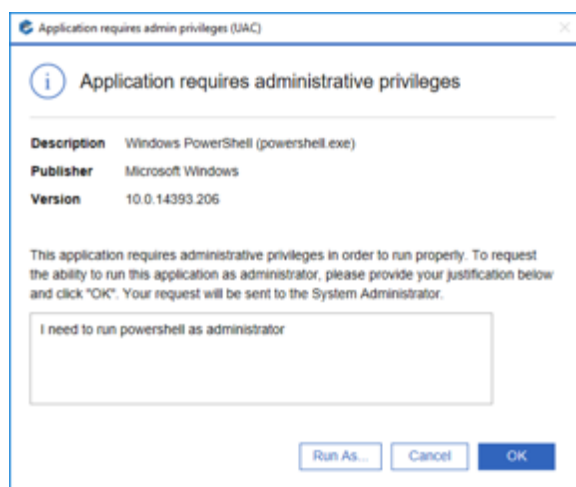
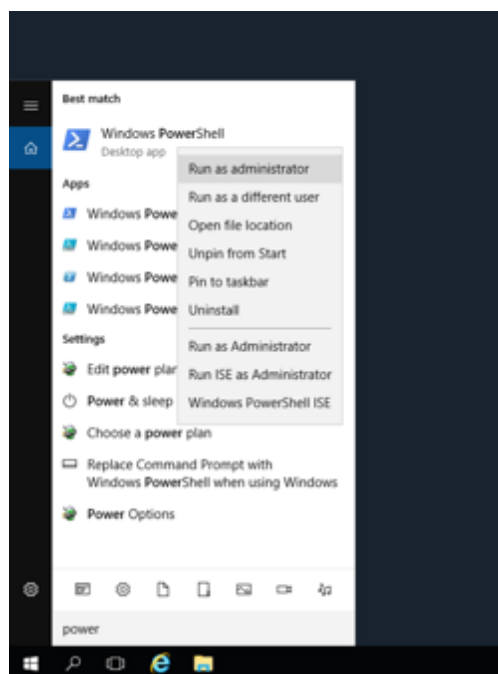


Figure 2 After Removal



Escalation request via CyberArk EPM



CYBERARK

EPM

Timeline

Computers

Application Events

Policy Audit Events

Threat Detection Events

Application Events

Edward.Nunez@cyberark_117 > Windows PowerShell (powershell.exe) | Last sign in: 24-May-21 | edward.nunez@cyberark.com <

Updated at: 8:41 AM

Filters

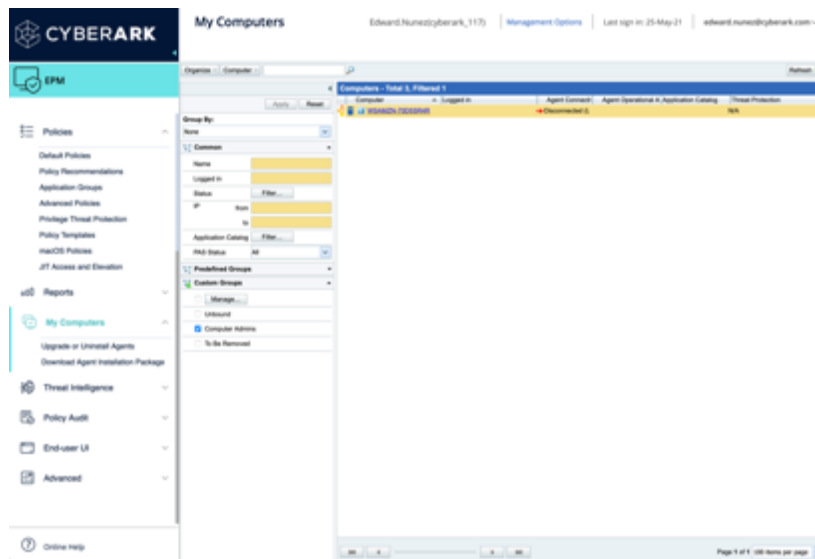
Computer: [] User: [] User Role: All Justification: All Last Time: Last year [Apply]

Additional Filters

2 results

Computer	User	Event	Time	Additional Info	Count
WSAAM2N-7D055H48	casimhenunez@1684	Elevation request	08:14:40	I need to run powershell as adm...	1
WSAAM2N-M7U6QP0	casimhenunez@cyberark	Elevation request	13-May-21 09:03:11	[09:03 13-May-2021] I need to r...	2

You can define policies to be applied to a group of computers and users. This allows to have certain group of computers/users with the ability to execute privileged commands, as well as simplifying the administration. In the image below we have assigned the computer to a custom group named “Computer Admins” for such purpose.



Then in the policy, you can allow elevation by the computers members of the group “Computer Admins”

