



CYBERARK & RAPID7 INSIGHTVM INTEGRATION

Name of Company: Rapid7

Website: www.rapid7.com

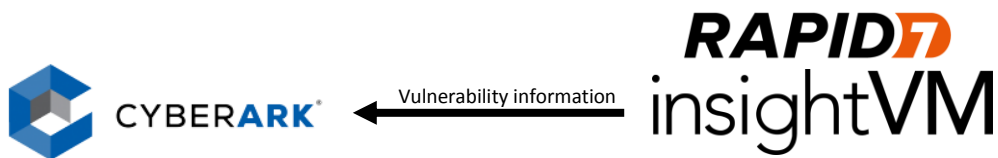
Name of Product: InsightVM

Date: June 2019

KEY BENEFITS

The CyberArk & Rapid7 InsightVM integration can prevent users from accessing compromised systems and, in turn, helps to make your organization's environment more secure. You can block access to a specific system that shows high-risk vulnerability scores until the vulnerability is eliminated, while still allowing authorized technicians access in order to remediate that particular machine. Leverage this integration to ensure your credential management and privileged access evolves with your ever-changing environment.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



The integration between Rapid7 InsightVM and CyberArk was developed around the CyberArk's PVWA Ticketing Integration framework (which provides a powerful user-exit capability) used in this particular case, to validate whether access (Show, Copy, or Connect) to a server's privileged account should be granted or not, due to vulnerabilities exposed by the information queried against Rapid7 InsightVM.

The distribution zip contains two DLL files (**CyberArk.Rapid7ConditionalAccess.dll** & **RestSharp.dll**). The interaction with Rapid7 InsightVM is governed by a specific set of Ticketing Parameters described in the Configuration section of this document.

The integration implements a hierarchy: *Vulnerability Manager -> Vulnerability Subset -> Conditions*

These are defined as Ticketing System parameters defined in the PVWA Administration page. You can specify as many parameters as required. The parameters can be specified in different hierarchies and levels and are transferred to the integration module in an xml object when a user clicks on Show, Copy, or Connect. Based on the logic defined by these parameters, the integration module determines if the user will be denied access to a server with vulnerabilities. See Appendix 1 for an example of the XML object.

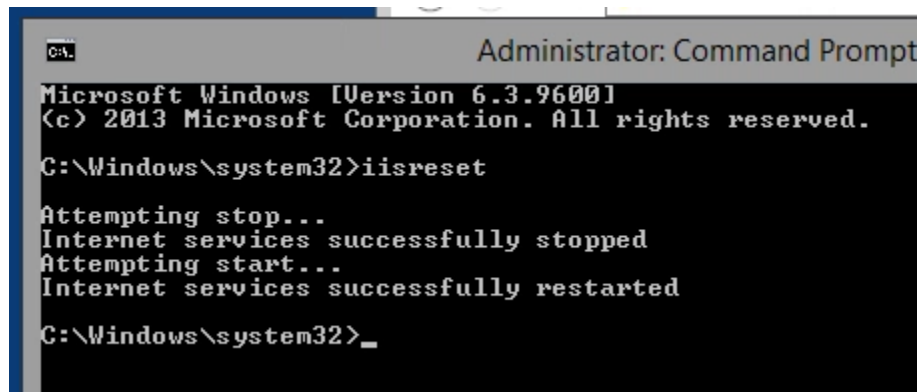
INSTALLATION

Extract the Rapid7ConditionalAccess distribution into a clean folder. It contains the following files:

- CyberArk.Rapid7ConditionalAccess.dll
- RestSharp.dll

INSTALL THE CODE

Copy the two DLL's on the distribution to %inetpub%\wwwroot\PasswordVault\Bin or %inetpub%\wwwroot\PasswordVault\Bin (in v10+) on the PVWA server, then restart IIS:



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

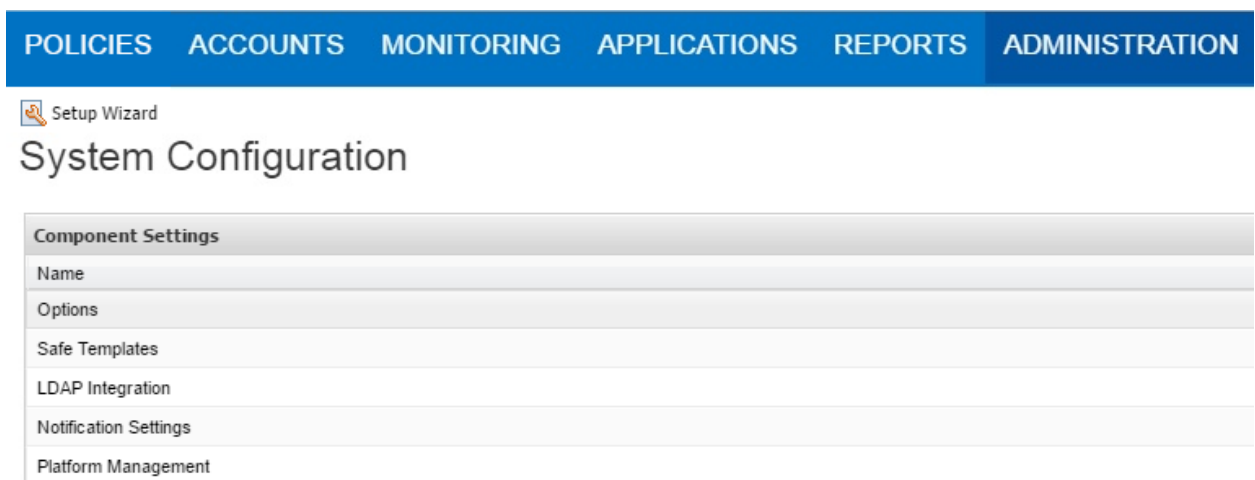
C:\Windows\system32>iisreset

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted

C:\Windows\system32>_
```

CONFIGURATION

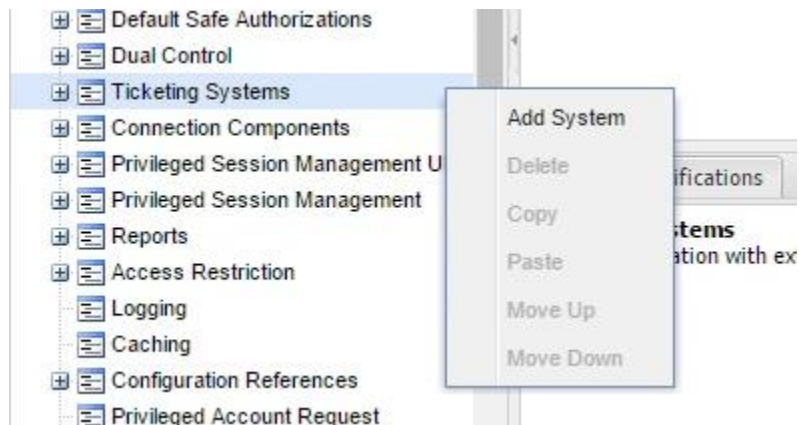
Log-in to the PVWA as a vault administrator user, then go to **ADMINISTRATION** and click on **Options**:



The screenshot shows the PVWA web interface. At the top is a navigation bar with the following tabs: POLICIES, ACCOUNTS, MONITORING, APPLICATIONS, REPORTS, and ADMINISTRATION. Below the navigation bar is a section titled "Setup Wizard" with a sub-header "System Configuration". Under this header is a table with the following rows:

Component Settings	
Name	
Options	
Safe Templates	
LDAP Integration	
Notification Settings	
Platform Management	

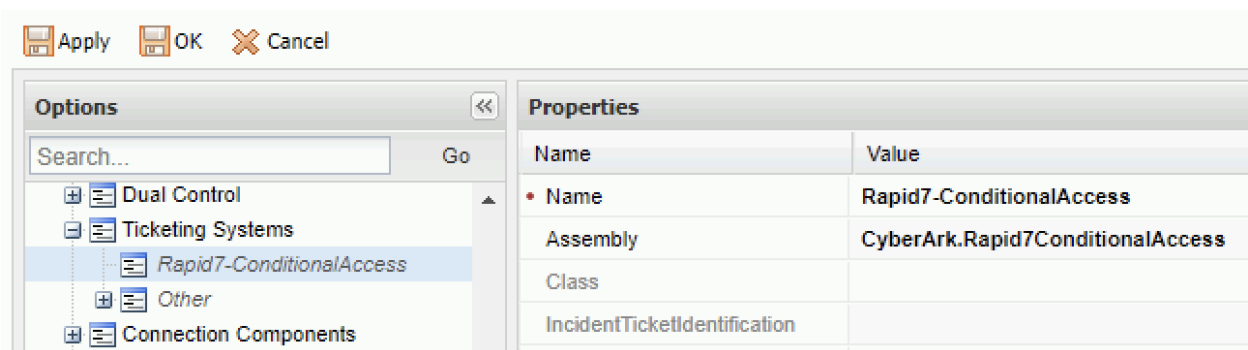
Right click on **Ticketing Systems** and select **Add System**:



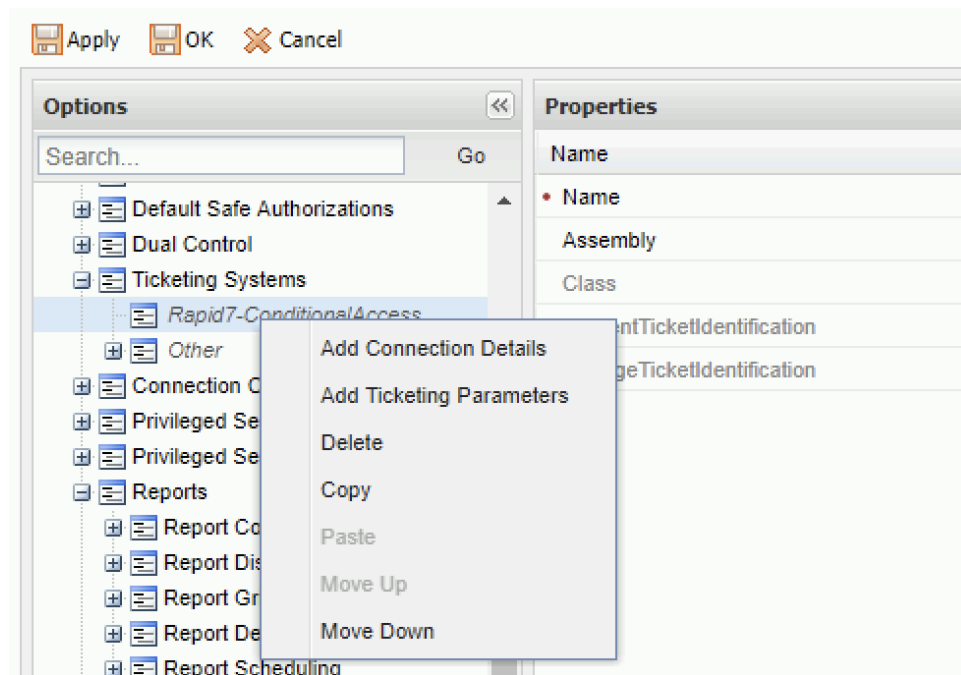
On the **Properties** section enter the following information:

Name: You can enter any value. (We will use “Rapid7-ConditionalAccess” as reference)

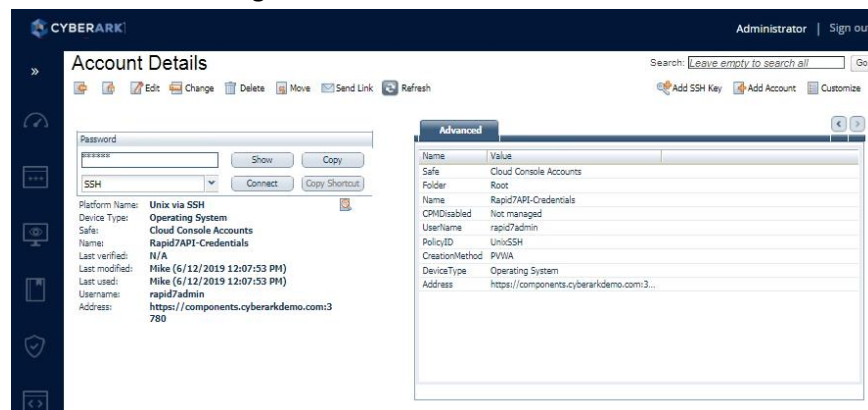
Assembly: Corresponds to the name of the dll file provided in the package. You *must* enter **CyberArk.Rapid7ConditionalAccess** as shown here:



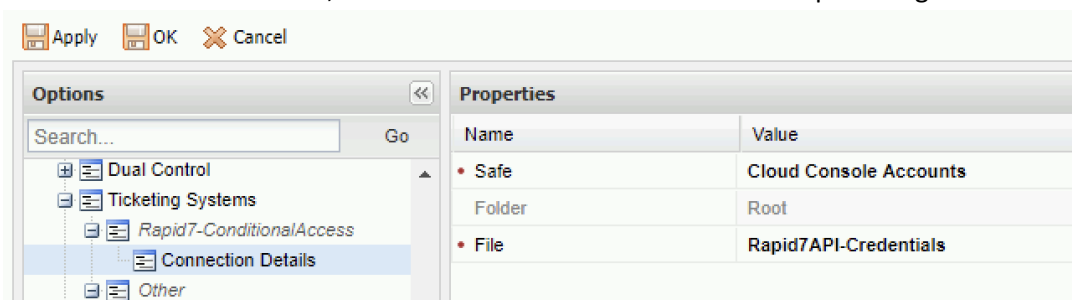
After clicking **Apply**, “Rapid7-ConditionalAccess” will appear under **Ticketing Systems**. Right click on it and select **Add Connection Details**:



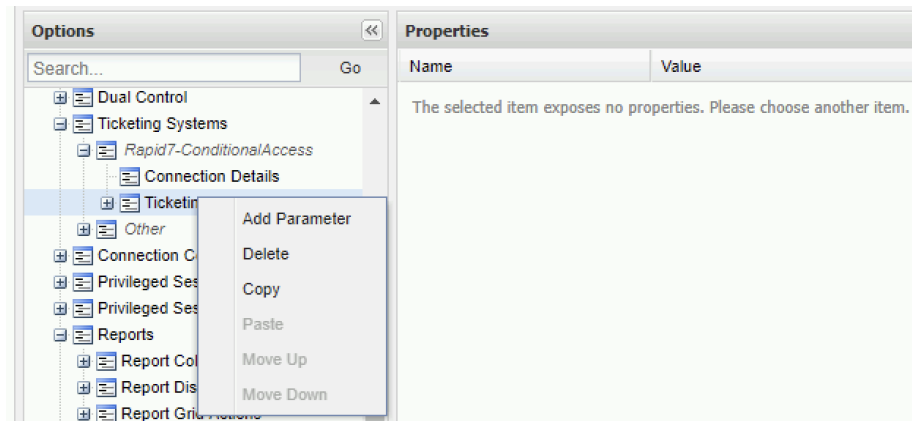
If the CyberArk CPM plugin for Rapid7 is not available use any unmanaged account to store the credential needed to connect to InsightVM:



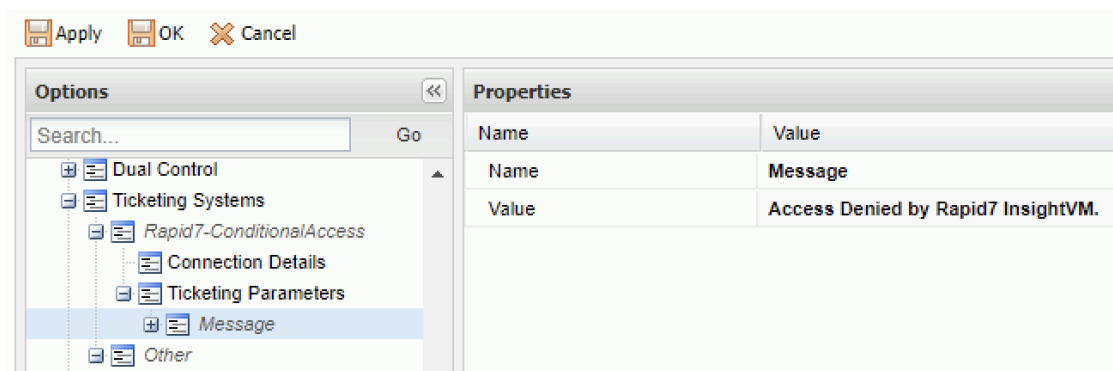
You will need to provide the safe, folder (root), and object name from the account already stored in CyberArk that holds the username, address and credential to connect to Rapid7 InsightVM API:



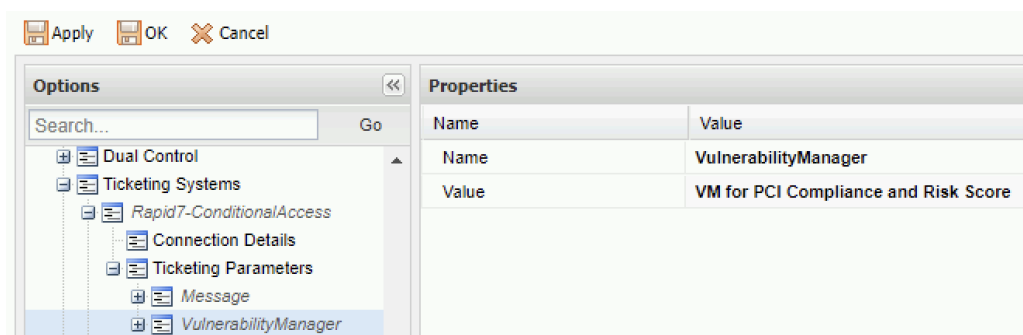
Click OK, then Right Click on Rapid7-ConditionalAccess and select **Add Ticketing Parameters**. A new **Ticketing Parameters** section will appear under Rapid7-ConditionalAccess, below Connection Details. Right click on it and select **Add Parameter**:



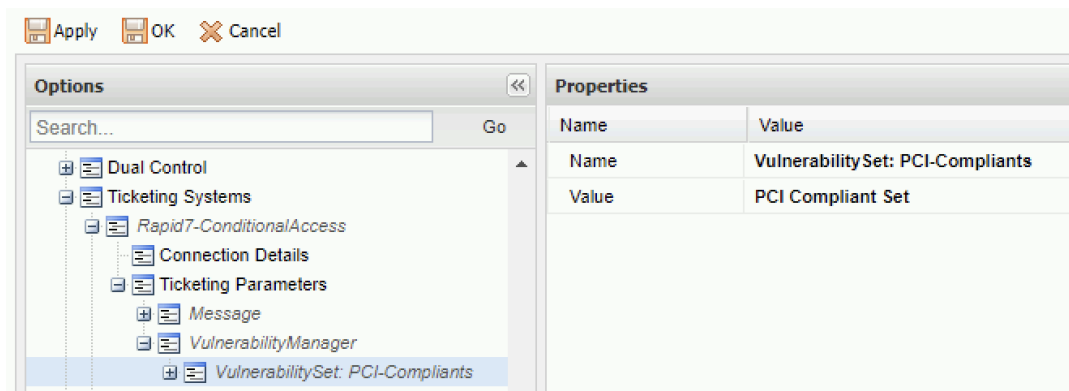
Name this Parameter **Message** and enter a generic message you want the PVWA to display when denying access to a vulnerable server. This message will apply to ALL Vulnerability Managers.



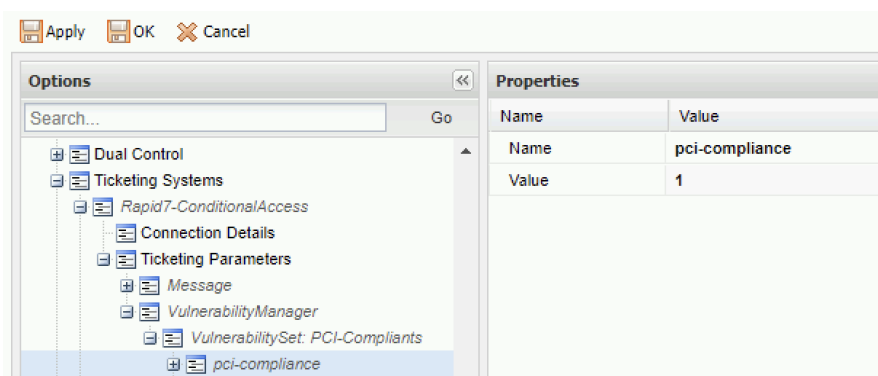
You will be able to define additional messages, which will follow the generic message, providing specific details, in the following subsections. Repeat the process to add a new parameter called **VulnerabilityManager**. The value of this parameter is not validated but you can use the value for reference purposes:



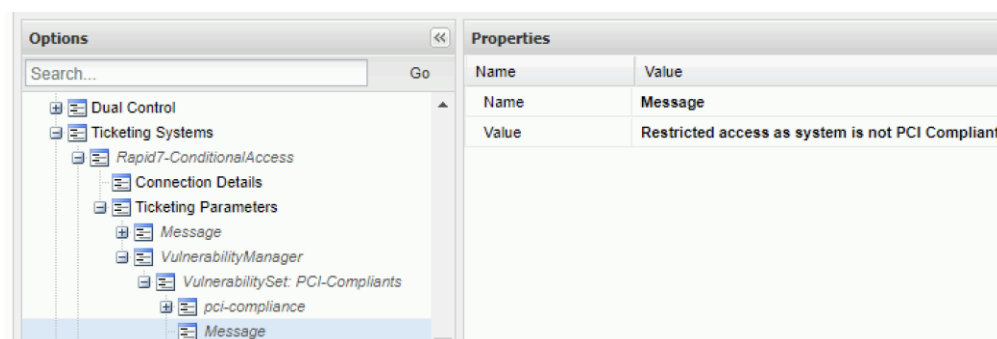
Next step is to add a **Vulnerability Set**. Right click on **VulnerabilityManager** and select **Add Parameter**. On Name enter **VulnerabilitySet** or use “**VulnerabilitySet:**” as prefix. Use Value for documentation purposes:



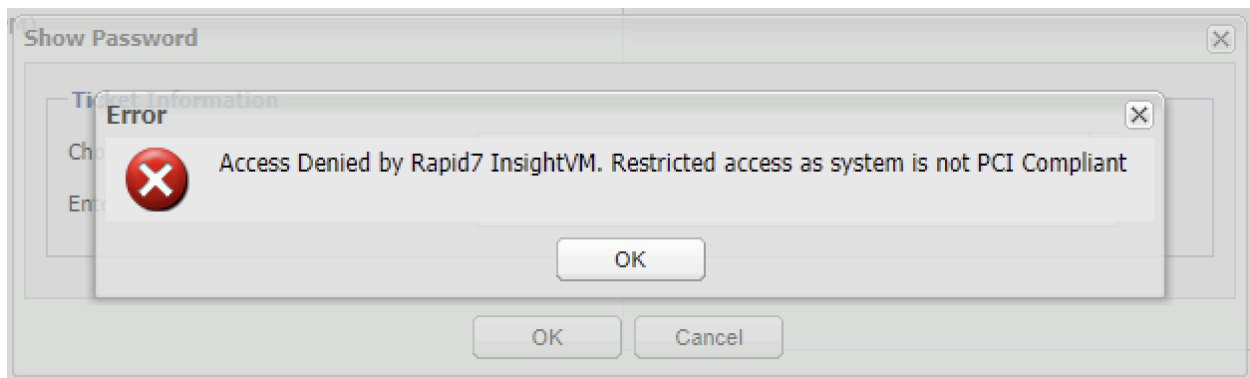
This integration is able to validate multiple properties from both InsightVM and CyberArk. See Appendix 2 for the complete list. To allow access to servers identified by InsightVM as PCI Compliant, right click on **VulnerabilitySet** and select **Add Parameter**. Name it **pci-compliance** and enter a Value of **1**.



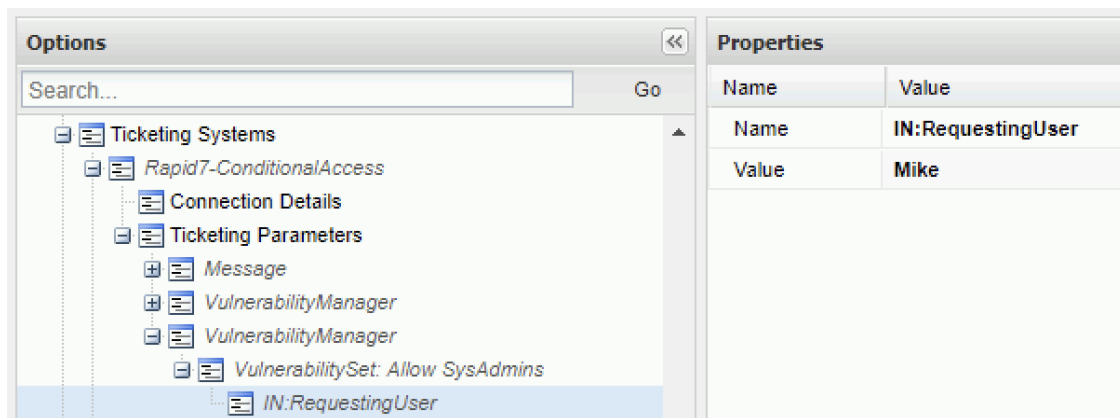
It's highly recommended that you also add a specific message, that will be appended to the generic message defined earlier, explaining the reason users are being denied access. Right click on **VulnerabilitySet** -> **Add Parameter** and named it **Message**. Enter **Restricted access as system is not PCI Compliant** and save it:



When you try to access (show/copy/connect) to any account residing on a server that is identified by InsightVM as not PCI Compliant you will get an error message:

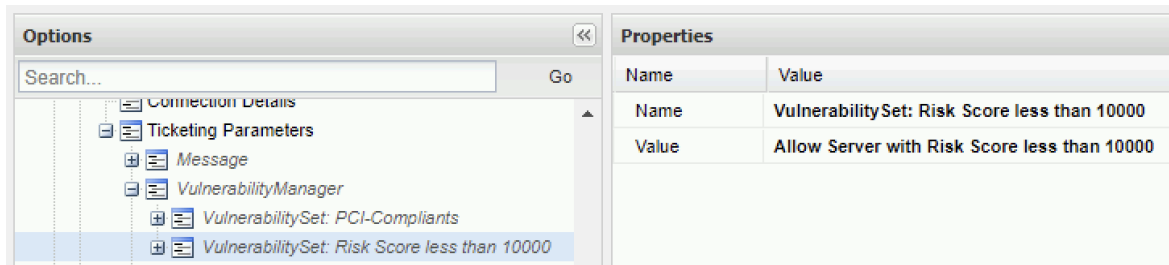


This completely locks all users from access to all servers identified as non PCI Compliant by InsightVM. However this is not very useful because somebody will need to connect to fix the vulnerabilities. Let's add a vulnerability manager to allow a senior Sysadmin to connect and repair the vulnerabilities. Follow the previous instructions to add a VulnerabilityManager, and add to it a Vulnerability Set with another parameter to the Vulnerability Set called **IN:RequestingUser** and assign a value of **Mike** and save it:

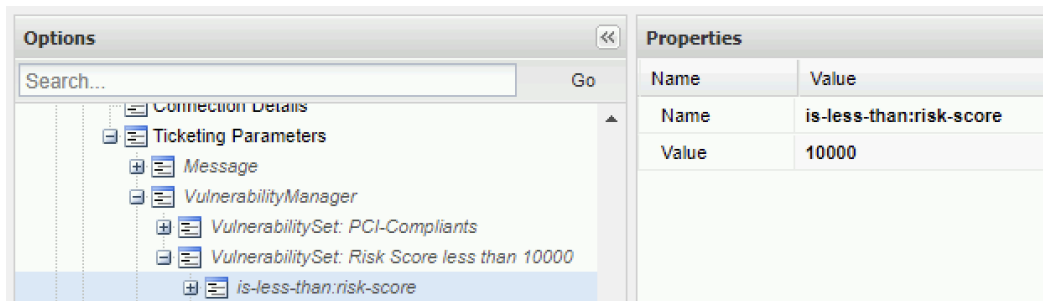


This will allow only user Mike to connect to these servers, so the vulnerabilities can be addressed. The IN operator allows you to specify a list, in this case of users.

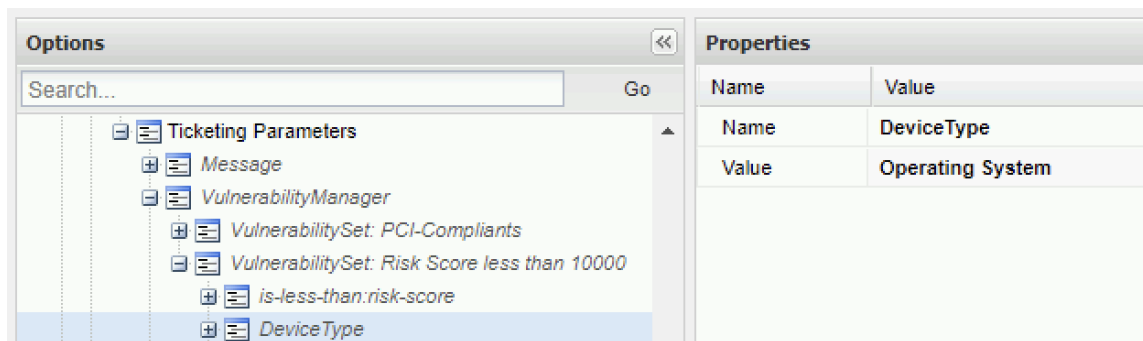
Let's allow access to all OS accounts residing on servers classified by InsightVM with a risk score less than 10000, start by creating a new Vulnerability Set by right clicking on **Ticketing Parameters** and selecting **Add Parameter**. Under **Name** enter **VulnerabilitySet** and under **Value** a good label for documentation purposes:



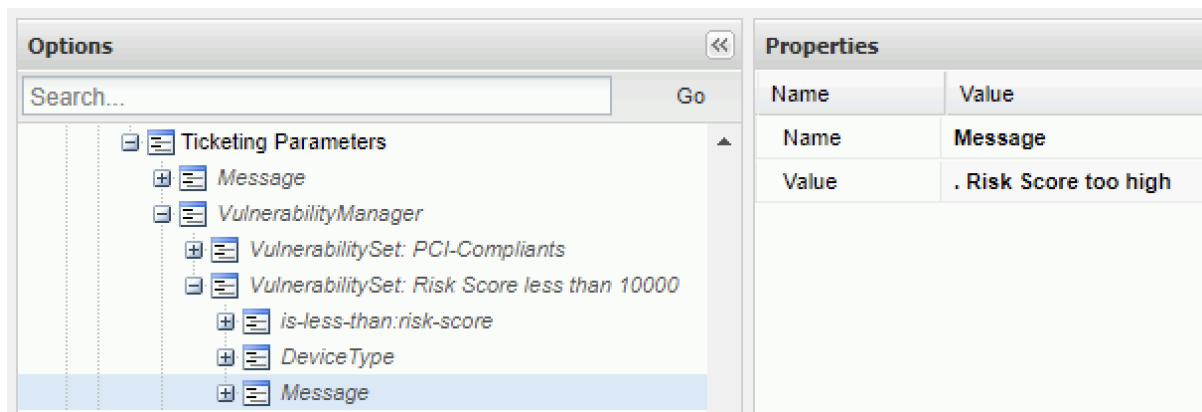
Add a parameter to your newly created Vulnerability Set. Name it **is-less-than:risk-score**, enter 10000 in **Value** and save it.



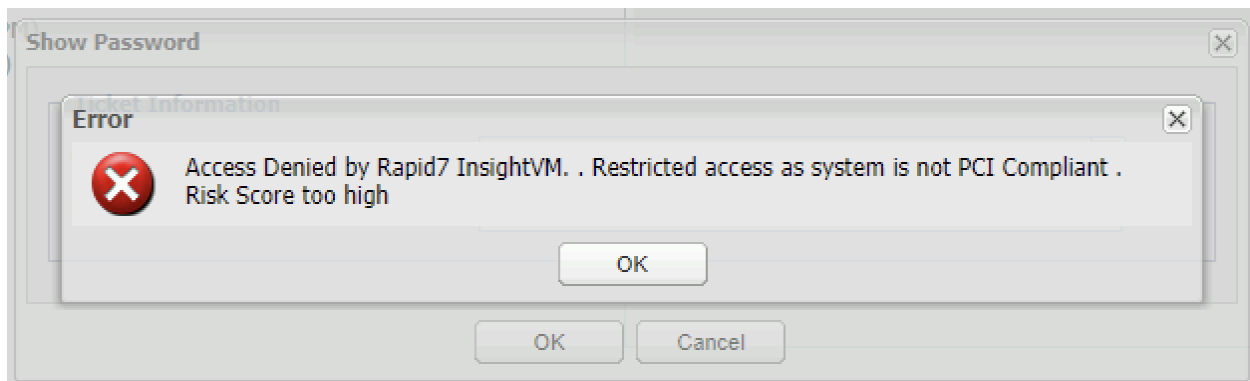
Now add a new parameter called **DeviceType** and enter **Operating System** as its value



Finally let's add a customized error message that will provide users with a meaningful message in case this condition is not matched:



When a user, other than Mike (as we still are allowing Mike to be able to operate based on VulnerabilityManager defined previously), attempts to connect to a server on which InsightVM has identified a Risk Score above 10000. The message will also contain the different messages for the different VulnerabilitySets not matching, and that are applicable to the account being targeted.



Also notice that this will only apply to Operating Systems type of accounts, all other account types will be allowed access.

Finally keep in mind that Vulnerability Managers and Vulnerability Sets are evaluated as an OR, meaning when the first one is found to be true we stop evaluating the rest. The parameters and conditions inside a Vulnerability Set are evaluated as an AND, meaning that all of them must be true for the Vulnerability Set to deny access. Use this rule to properly segment conditions across Vulnerability Sets to manage access.

Options

- [-] Ticketing Systems
 - [-] Rapid7-ConditionalAccess
 - [-] Connection Details
 - [-] Ticketing Parameters
 - [-] Message
 - [-] VulnerabilityManager
 - [-] VulnerabilitySet: PCI-Compliants
 - [-] Message
 - [-] pci-compliance
 - [-] DeviceType
 - [-] VulnerabilitySet: Risk Score less than 10000
 - [-] Message
 - [-] is-less-than:risk-score
 - [-] DeviceType
 - [-] VulnerabilitySet: Approved for ORACLE
 - [-] Message
 - [-] custom-tag
 - [-] DeviceType
 - [-] VulnerabilitySet: Approved for Admins
 - [-] Message
 - [-] custom-tag
 - [-] DeviceType
 - [-] VulnerabilityManager
 - [-] VulnerabilitySet: Allow SysAdmins
 - [-] IN:RequestingUser
 - [-] AllowTransparentConnection

Properties

Name	Value
Name	custom-tag
Value	OK-ADMINS

ENABLING THE INTEGRATION FOR THE RELEVANT PLATFORMS

Enable the integration (Ticketing System) for platforms where you want to deny access to servers with specific vulnerabilities identified by Rapid7 InsightVM. Log-in to the PVWA as a vault administrator user, go to **ADMINISTRATION** and click on **Platform Management**. Select your platform and click on **Edit**:

Name	Device Type	Status
Twitter via https	Website	Active
Unix via SSH	Operating System	Active
Unix via SSH Keys	Operating System	Active
Unix via SSH Keys for AWS	Operating System	Active
Unix via SSH with ADBridge	Operating System	Active
VMWare ESX Account	Operating System	Active
VMWare vCenter Personal	Application	Active
VMWare vCenter Shared Accounts	Application	Active
Windows Desktop Local Accounts	Operating System	Active
Windows Domain - Multi Level Approval	Operating System	Active
Windows Domain Account	Operating System	Active
Windows Server Local Accounts	Operating System	Active
Z-Series	Windows Domain Account Operating System	Active
[Sample Password Group Platform]	Misc	Inactive

Unix via SSH

DESCRIPTION
None

STATUS ?
Active

Duplicate Edit

If you do not already have an active Ticketing System, then expand **UI & Workflows**, click on **Ticketing System**, and set both **EnterTicketingInfo** and **ValidateTicketNumber** to **Yes**. Then click **OK**:

Apply OK Cancel

Unix via SSH

Search... Go

- Target Account Platform
 - UI & Workflows
 - Properties
 - Linked Accounts
 - Ticketing System**
 - Privileged Session Management

Properties	
Name	Value
EnterTicketingInfo	Yes
ValidateTicketNumber	Yes
DisableDualControlForIncidentTickets	No
DisableDualControlForChangeTickets	No
TicketValidationTimingWithDualControl	WhenAccessingAccountAfterConfirmation

Note: If you have multiple ticketing systems you can enable only some of them for a specific platform, please refer to section “*Integrating with Ticketing Systems*” of the “*Privileged Account Security Implementation Guide*” documentation.

APPENDIX 1: XML EXAMPLE

```
<TicketingSystems EnableTicketingWithoutRequiredReason="Yes">
  <System Name="Rapid7-ConditionalAccess" Assembly="CyberArk.Rapid7ConditionalAccess">
    <ConnectionDetails Safe="Cloud Console Accounts" File="Rapid7API-Credentials" />
    <TicketingParameters>
      <Parameter Name="Message" Value="Access Denied by Rapid7 InsightVM. " />
      <Parameter Name="VulnerabilityManager" Value="VM for PCI Compliance and Risk Score">
        <Parameter Name="VulnerabilitySet: PCI-Compliant" Value="PCI Compliant">
          <Parameter Name="Message" Value=". Restricted access as system is not PCI Compliant" />
          <Parameter Name="pci-compliance" Value="1" />
          <Parameter Name="DeviceType" Value="Operating System" />
        </Parameter>
        <Parameter Name="VulnerabilitySet: Risk Score less than 10000" Value="Risk Score less than 10000">
          <Parameter Name="Message" Value=". Risk Score too high" />
          <Parameter Name="is-less-than:risk-score" Value="10000" />
          <Parameter Name="DeviceType" Value="Operating System" />
        </Parameter>
        <Parameter Name="VulnerabilitySet: Approved for ORACLE" Value="Assets tagged with OK-ORACLE">
          <Parameter Name="Message" Value=". Access not allowed, ask Security Admin to tag asset with OK-ORACLE." />
          <Parameter Name="custom-tag" Value="OK-ORACLE" />
          <Parameter Name="DeviceType" Value="Database" />
        </Parameter>
        <Parameter Name="VulnerabilitySet: Approved for Admins" Value="Assets tagged with OK-ADMINS">
          <Parameter Name="Message" Value=". Access not allowed, ask Security Admin to tag asset with OK-ADMINS." />
          <Parameter Name="custom-tag" Value="OK-ADMINS" />
          <Parameter Name="DeviceType" Value="Operating System" />
        </Parameter>
      </Parameter>
      <Parameter Name="VulnerabilityManager" Value="Allow SysAdmins">
        <Parameter Name="VulnerabilitySet: Allow SysAdmins" Value="Allow Sys Admins">
          <Parameter Name="IN:RequestingUser" Value="Mike" />
          <Parameter Name="AllowTransparentConnection" Value="true" />
        </Parameter>
      </Parameter>
    </TicketingParameters>
  </System>
</TicketingSystems>
```

APPENDIX 2: SUPPORTED PROPERTIES AND CONDITIONS

You can add the following Rapid7 InsightVM and CyberArk parameters to further refine what a CyberArk user will be allowed to do on a server with Vulnerabilities:

CyberArk Property	Description
SafeName	The Safe where the requested account is stored.
MachineAddress	The address of the machine specified on the account, if it exists.
TransparentMachine Address	The address of the machine used in a transparent connection, if it exists.
UserName	The name of the user specified on the requested account.
PolicyId	The name of the platform specified on the requested account.
RequestingUser	The name of the user requesting the account.
DeviceType	The DeviceType that's been accessed. It allows to restrict access to OS accounts while allowing access to Database accounts on a server with OS vulnerabilities.
AllowTransparentConnection	When True, this property grants login access to a vulnerable server while denying Show/Copy

In addition to the properties listed above, all target account properties are available, such as: DeviceType, Port, Database, LogonDomain, etc.

Supporting exact match comparisons or regular expressions you can add logic like:

- Do not allow if the DeviceType is "Operating System"
- Do not allow if SafeName or PolicyID has PCI in their name

Properties can be prefixed by operators when being defined in the ticketing system. See example in previous section to allow Mike access.

RAPID7 INSIGHTVM OPERATORS

Operator	Value	Lower	Upper
are	string		
contains	string		
does-not-contain	string		
ends with	string		
in	Array[string]		
in-range		numeric	numeric
includes	Array[string]		
is	string		
is-applied			

is-between		numeric	numeric
is-earlier-than	numeric		
is-empty			
is-greater-than	numeric		
is-on-or-after	string (yyyy-MM-dd)		
is-on-or-before	string (yyyy-MM-dd)		
is-not	string		
is-not-applied			
is-not-empty			
is-within-the-last	string		
less-than	string		
like	string		
not-contains	string		
not-in	Array[string]		
not-in-range		numeric	numeric
not-like	string		
starts-with	string		

RAPID7 INSIGHTVM PROPERTIES & OPERATORS

Fields & Operators

Field	Operators
alternate-address-type	in
container-image	is is-not starts-with ends-with contains does-not-contain is-like not-like
container-status	is is-not
containers	are
criticality-tag	is is-not is-greater-than is-less-than is-applied is-not-applied
custom-tag	is is-not starts-with ends-with contains does-not-contain is-applied is-not-applied
cve	is is-not contains does-not-contain
cvss-access-complexity	is is-not
cvss-authentication-required	is is-not
cvss-access-vector	is is-not

cvss-availability-impact	is is-not
cvss-confidentiality-impact	is is-not
cvss-integrity-impact	is is-not
cvss-v3-confidentiality-impact	is is-not
cvss-v3-integrity-impact	is is-not
cvss-v3-availability-impact	is is-not
cvss-v3-attack-vector	is is-not
cvss-v3-attack-complexity	is is-not
cvss-v3-user-interaction	is is-not
cvss-v3-privileges-required	is is-not
host-name	is is-not starts-with ends-with contains does-not-contain is-empty is-not-empty is-like not-like
host-type	in not-in
ip-address	is is-not in-range not-in-range is-like not-like
ip-address-type	in not-in
last-scan-date	is-on-or-before is-on-or-after is-between is-earlier-than is-within-the-last
location-tag	is is-not starts-with ends-with contains does-not-contain is-applied is-not-applied
mobile-device-last-sync-time	is-within-the-last is-earlier-than
open-ports	is is-not in-range
operating-system	contains does-not-contain is-empty is-not-empty
owner-tag	is is-not starts-with ends-with contains does-not-contain is-applied is-not-applied
pci-compliance	is
risk-score	is is-not in-range greater-than less-than
service-name	contains does-not-contain
site-id	in not-in
software	contains does-not-contain
vAsset-cluster	is is-not contains does-not-contain starts-with
vAsset-datacenter	is is-not
vAsset-host-name	is is-not contains does-not-contain starts-with
vAsset-power-state	in not-in
vAsset-resource-pool-path	contains does-not-contain

vulnerability-assessed	is-on-or-before is-on-or-after is-between is-earlier-than is-within-the-last
vulnerability-category	is is-not starts-with ends-with contains does-not-contain
vulnerability-cvss-v3-score	is is-not
vulnerability-cvss-score	is is-not in-range is-greater-than is-less-than
vulnerability-exposures	includes does-not-include
vulnerability-title	contains does-not-contain is is-not starts-with ends-with
vulnerability-validated-status	are

Field & Enumerated/Acceptable Values:

Field	Acceptable Values
<code>alternate-address-type</code>	0=IPv4, 1=IPv6
<code>containers</code>	0=present, 1=not present
<code>container-status</code>	created running paused restarting exited dead unknown
<code>cvss-access-complexity</code>	• <code>L</code> = Low • <code>M</code> = Medium • <code>H</code> = High
<code>cvss-integrity-impact</code>	• <code>N</code> = None • <code>P</code> = Partial • <code>C</code> = Complete
<code>cvss-confidentiality-impact</code>	• <code>N</code> = None • <code>P</code> = Partial • <code>C</code> = Complete
<code>cvss-availability-impact</code>	• <code>N</code> = None • <code>P</code> = Partial • <code>C</code> = Complete
<code>cvss-access-vector</code>	• <code>L</code> = Local • <code>A</code> = Adjacent • <code>N</code> = Network
<code>cvss-authentication-required</code>	• <code>N</code> = None • <code>S</code> = Single • <code>M</code> = Multiple
<code>cvss-v3-confidentiality-impact</code>	• <code>L</code> = Local • <code>L</code> = Low • <code>N</code> = None • <code>H</code> = High
<code>cvss-v3-integrity-impact</code>	• <code>L</code> = Local • <code>L</code> = Low • <code>N</code> = None • <code>H</code> = High
<code>cvss-v3-availability-impact</code>	• <code>N</code> = None • <code>L</code> = Low • <code>H</code> = High

cvss-v3-attack-vector	• N = Network • A = Adjacent • L = Local • P = Physical
cvss-v3-attack-complexity	• L = Low • H = High
cvss-v3-user-interaction	• N = None • R = Required
cvss-v3-privileges-required	• N = None • L = Low • H = High
host-type	0=Unknown, 1=Guest, 2=Hypervisor, 3=Physical, 4=Mobile
ip-address-type	0=IPv4, 1=IPv6
pci-compliance	0=fail, 1=pass
vulnerability-validated-status	0=present, 1=not present