



Cyber-Ark/McAfee ePO Integration Guide

August 2010

All rights reserved. This document contains information and ideas, which are proprietary to Cyber-Ark Software. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, without the prior written permission of Cyber-Ark Software.

EPOIG-0810

Copyright © 2000-2010 by Cyber-Ark® Software Ltd. All rights reserved.

Table of Contents

Overview	4
Technical Details.....	4
Prerequisites	5
Adding ePO Integration to a Partner Software	5
Configuring the PVWA	5
Customizing the Look of the Privileged Account Request Window	8
Limiting the Number of Requests per Minute	9
Preparing the ePO Server.....	10
Installing the Cyber-Ark Integration Module	10
Event Reporting	10
Uninstalling ePO Integration	10

Overview

This document is a guide to setting up the integration of Cyber-Ark and McAfee ePolicy Orchestrator (ePO).

Cyber-Ark provides an integration plug-in that will send PIM security related events (privileged credentials retrieved/used) to the ePO server. Customers will be able to define whether security events will be generated and redirected to the ePO server (according to the managed devices sensitivity) for each PIM Policy.

This integration enriches the security related information that is accessible through the ePO console with information about privileged account usage. Customers will be able to query, report and present this information through standard ePO console tools.

Technical Details

- o The ePO agent will be installed on the Cyber-Ark IIS server that hosts the Password Vault Web Access (PVWA) web application.
- o According to Cyber-Ark configuration, the Cyber-Ark PVWA will generate an event and send it to the ePO agent using a customized plug-in that Cyber-Ark provides to its customers.
- o The ePO agent will redirect the events to the ePO Server.
- o Events can be reviewed and queried from the ePO console.

Prerequisites

This section details the pre-requisites required for partner product installation.

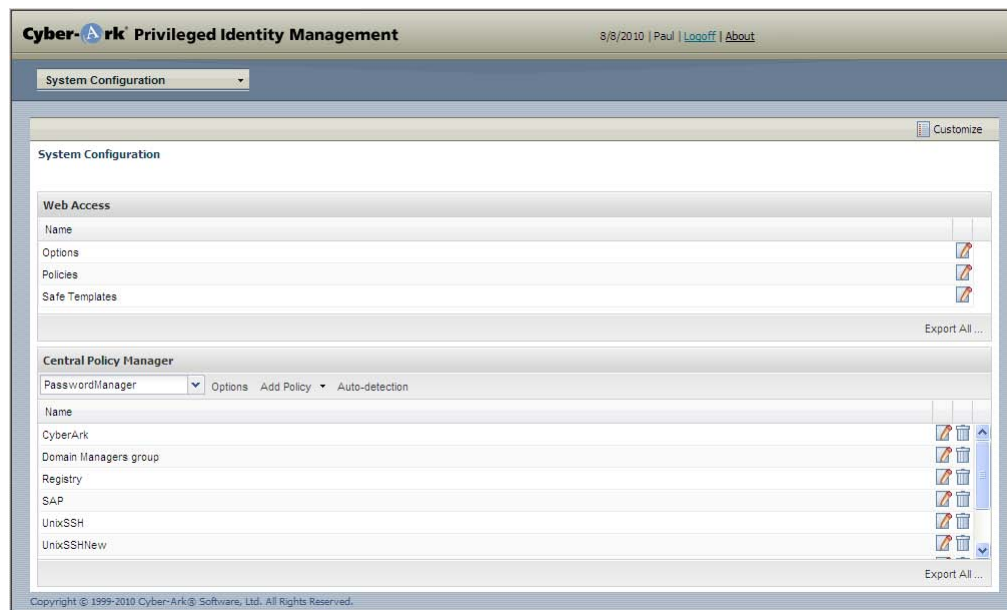
- o PIM Suite v5.5 or above
- o McAfee ePO Agent must be installed on the PVWA machine

Adding ePO Integration to a Partner Software

1. Copy the **CyberArk.Plugins.McAfeeEPO.dll** to the \bin folder under the PasswordVault website (for example, c:\inetpub\wwwroot\PasswordVault\bin).
2. Copy the McAfee agent events **COM interop dll** (Interop.GENEVTINFLib.dll) to the \bin directory.

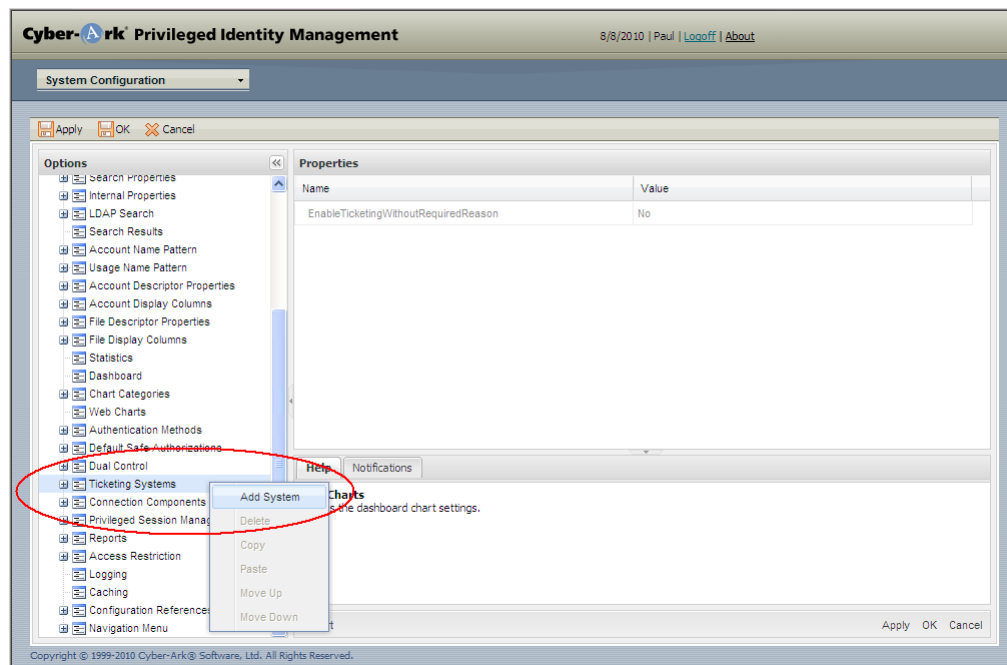
Configuring the PVWA

1. With a system administrator user, log on to the PVWA and display the **System Configuration** page.



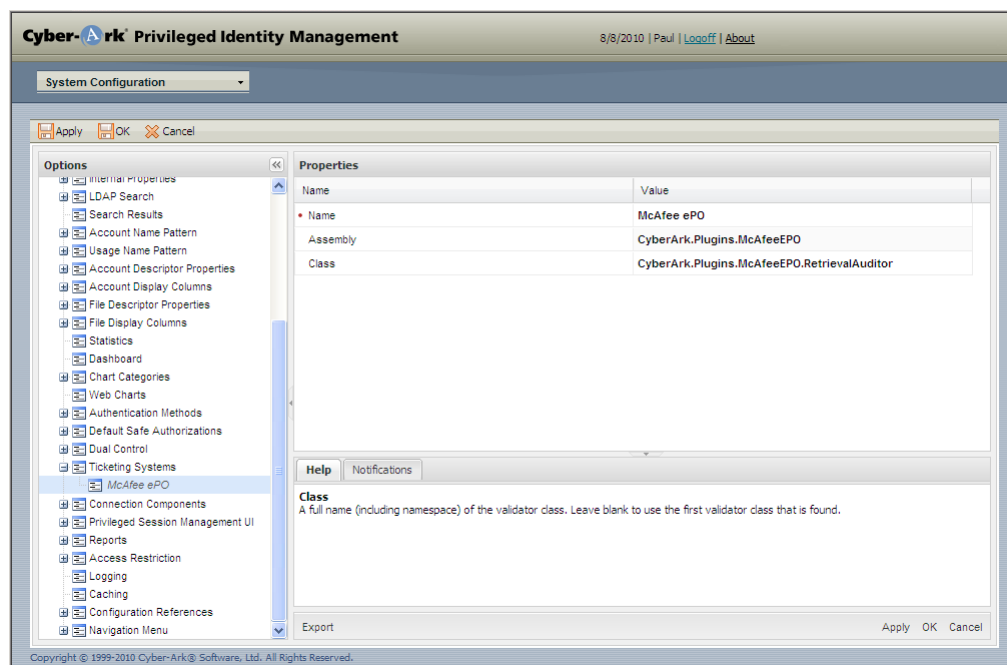
2. In the Web Access section, select **Options** to access the application configuration.

3. In the **Ticketing Systems** section, add a new **System** node.

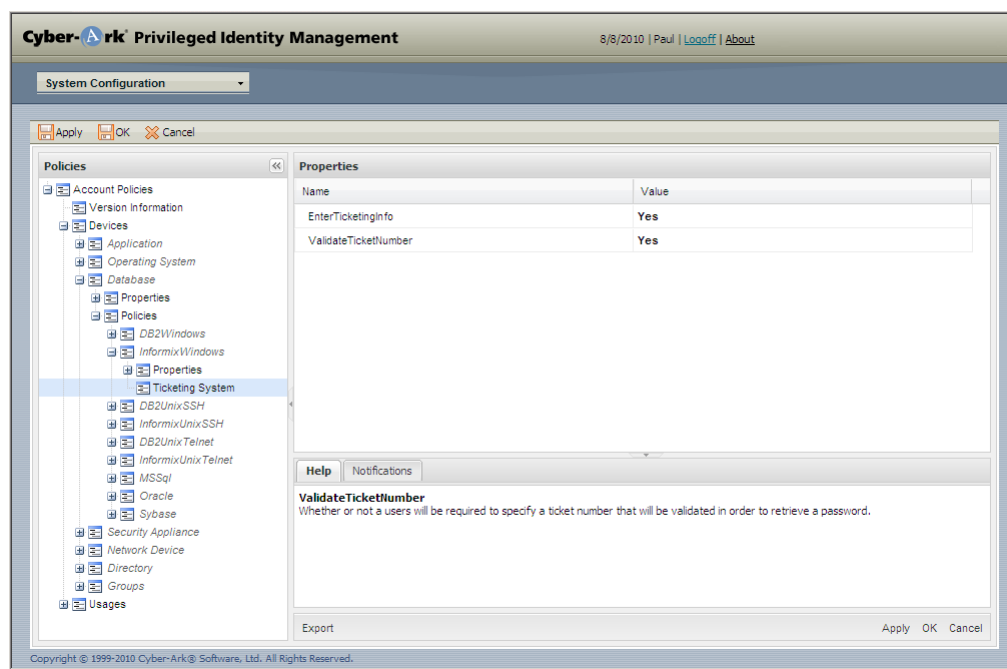


A new System section is added under Ticketing System.

4. Specify the following parameters to configure the new Ticketing System:
- Name – Specify any name for the system, for example, **McAfee ePO**
 - Assembly – Specify **CyberArk.Plugins.McAfeeEPO**
 - Class – Specify **CyberArk.Plugins.McAfeeEPO.RetrievalAuditor**

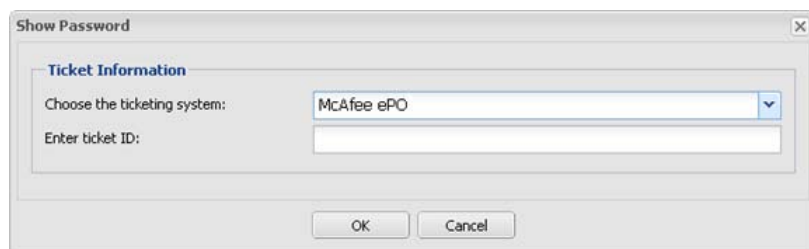


5. Click **OK** to save the new configurations and return to the System Configuration page.
6. In the Web Access section, select **Policies**.
7. Expand the **Devices** folder, then expand the device type to configure.
8. Display the contents of the **Policies** folder, then expand the policy to configure.
9. Select Ticketing System; the ticketing system configuration parameters are displayed.
10. Specify the following values:
 - EnterTicketingInfo – Specify **Yes**
 - ValidateTicketNumber – Specify **Yes**



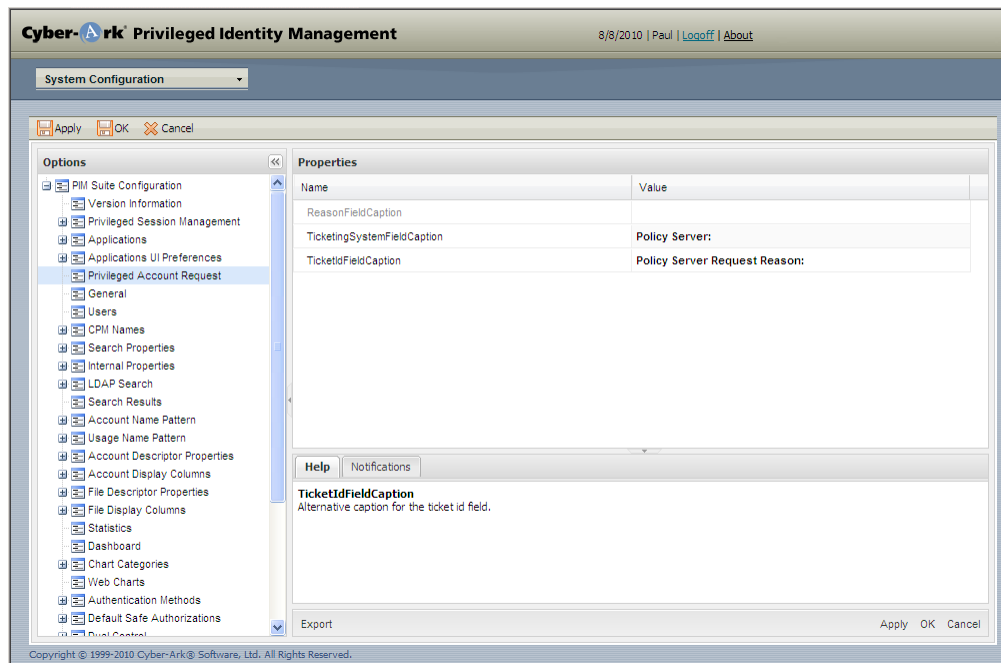
All accounts associated with this policy will invoke the McAfee agent integration plugin when the password is retrieved, regardless of whether it is displayed, copied or used to connect to the remote device).

For example, if the EnterTicketingInfo and ValidateTicketNumber parameters are set to Yes in the WinDomain policy, the following dialogue window will be displayed before the password of an account associated with the WinDomain policy is displayed:

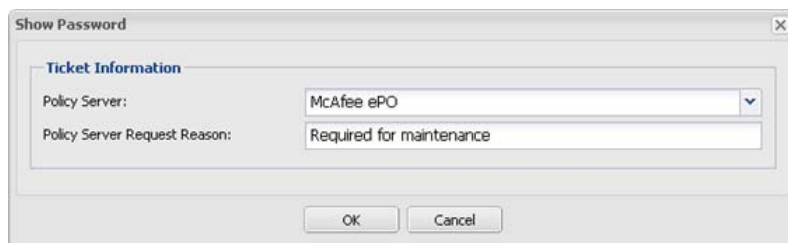


Customizing the Look of the Privileged Account Request Window

You can customize certain display names in the Password Retrieval Request window by editing the properties in the Privileged Account Request parameters in the Web Access Options in the System Configuration page.



As a result of these changes, the custom display names will be shown in the Privileged Account Request window, as shown below:

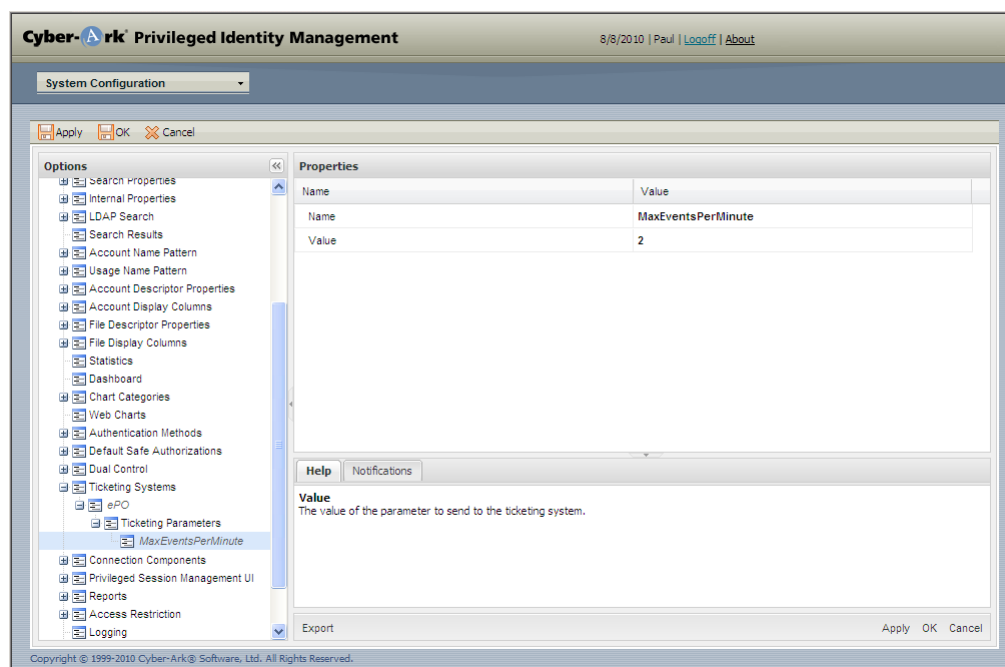


Limiting the Number of Requests per Minute

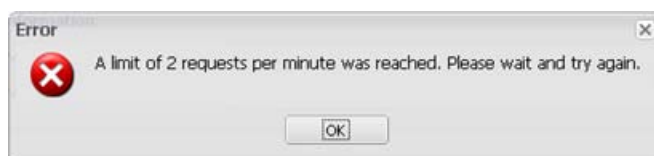
The number of requests that can be sent each minute can be tracked and limited over a timeframe of one minute. When the specified limit is reached, no more requests will be sent until the end of the minute interval. This timeframe is reset every minute, regardless of the number of requests that are sent.

The limit of requests that can be sent each minute is configured in the Web Access Options, in the Ticketing Systems section.

1. In the System Configurations page, display the **Web Access Options**.
2. In the Ticketing System section, right-click **McAfee ePO**, then select **Add Ticketing Parameters**; a new section for Ticketing Parameters is created under McAfee ePO.
3. Right-click Ticketing Parameters and select **Add Parameter**; a new parameter is added under Ticketing Parameters.
4. Specify the following properties:
 - Name – Specify **MaxEventsPerMinute**
 - Value – Specify **2**



After the requests limit is reached, additional password requests will be denied and the following message will be displayed each time a password request is created:



Preparing the ePO Server

Installing the Cyber-Ark Integration Module

Follow the McAfee ePO documentation and install the Cyber-Ark extension package from the supplied **Cyber-Ark_PVWA.zip** file.

Event Reporting

The integration plugin sends the following event:

- o 201350 – Password fetch event

This event is sent for accounts that are integrated with ePO, according to their system policy, when the password of that account is retrieved (shown, copied to the clipboard, or used transparently to connect to a remote machine). The event includes information about the action performed, specified in the following fields:

- o SafeName
- o FolderName
- o ObjectName
- o MachineAddress
- o TransparentMachineAddress
- o UserName
- o PolicyId
- o RequestingUser
- o RequestingUserFirstName
- o RequestingUserSurname
- o RequestingUserEmail
- o ProvidedReason
- o AdditionalProperties (as a concatenated list)

Uninstalling ePO Integration

Follow the McAfee ePo documentation and uninstall the **Cyber-Ark_PVWA** package.

To remove DB entities manually, remove the Cyber-Ark_PVWA_PasswordFetchEvents table from the dbo schema and remove the CyberArk_PVWA_PasswordFetchEvents_Insert stored procedure.