

vmware

VMware vCenter™ Protect Essentials Plus
Configuration Management



Quick Start Guide

VMware vCenter™ Protect Essentials Plus

Configuration Management

Copyright

Copyright © 2011 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

No part of this document may be reproduced or retransmitted in any form or by any means electronic, mechanical, or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use without written permission of VMware, Inc.

Trademarks

vCenter, VMware, and the VMware logo are either registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Document Information and Print History

This document provides quick start information for the most commonly performed tasks in vCenter Protect Essentials Plus – Configuration Management.

Document number: N/A

Date	Version	Description
May 2011	Original version	Original release of the NetChk Configure Quick Start Guide.
November 2011	4.3	Rebrand and update content for vCenter Protect Essentials Plus – Configuration Management 4.3.

Table of Contents

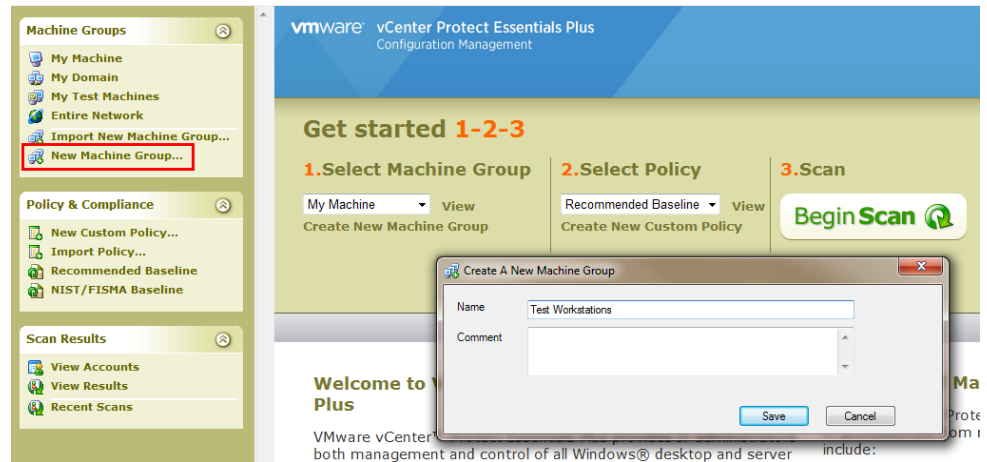
CREATE A MACHINE GROUP	1
IMPORT AN EXISTING MACHINE GROUP	3
SCAN AND ENFORCE USING AN EXISTING POLICY	5
CREATE A NEW CUSTOM POLICY BY MANUALLY SELECTING POLICY CHECKS	7
CREATE A NEW CUSTOM POLICY USING THE “CREATE FROM SELECTED OS” OPTION	9
CREATE A NEW CUSTOM POLICY FROM AN EXISTING MACHINE	11
IMPORT POLICIES	15
MERGE POLICIES	17
ADD CUSTOM CHECKS TO A POLICY AND ENFORCE.....	20
REPORTING	23

This page intentionally left blank.

The document is designed for duplex printing.

CREATE A MACHINE GROUP

1. In the **Machine Groups** list click **New Machine Group**.



2. Name the machine group and then click **Save**.

The machine group dialog is displayed.



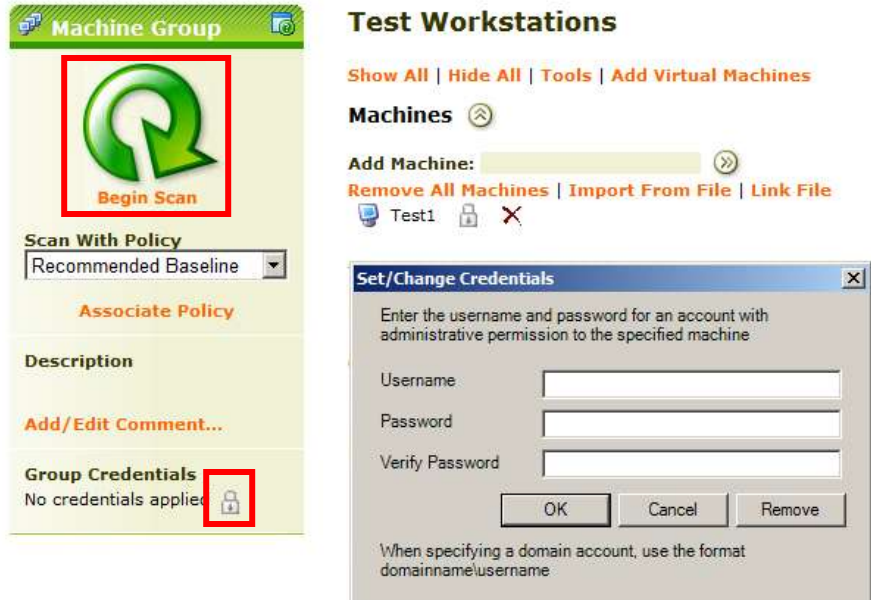
3. In the **Add Machine** box type the machine name and then click the right arrow to add the machine.

To add a machine by another method (domain, OU, IP address, etc.) click on the down arrow to expand the method and enter the required information.

- Specify credentials for the group by clicking the padlock icon.

Note: You can also specify credentials on a machine basis by clicking the padlock icon located next to each machine.

In the popup, enter the credentials for the machines.

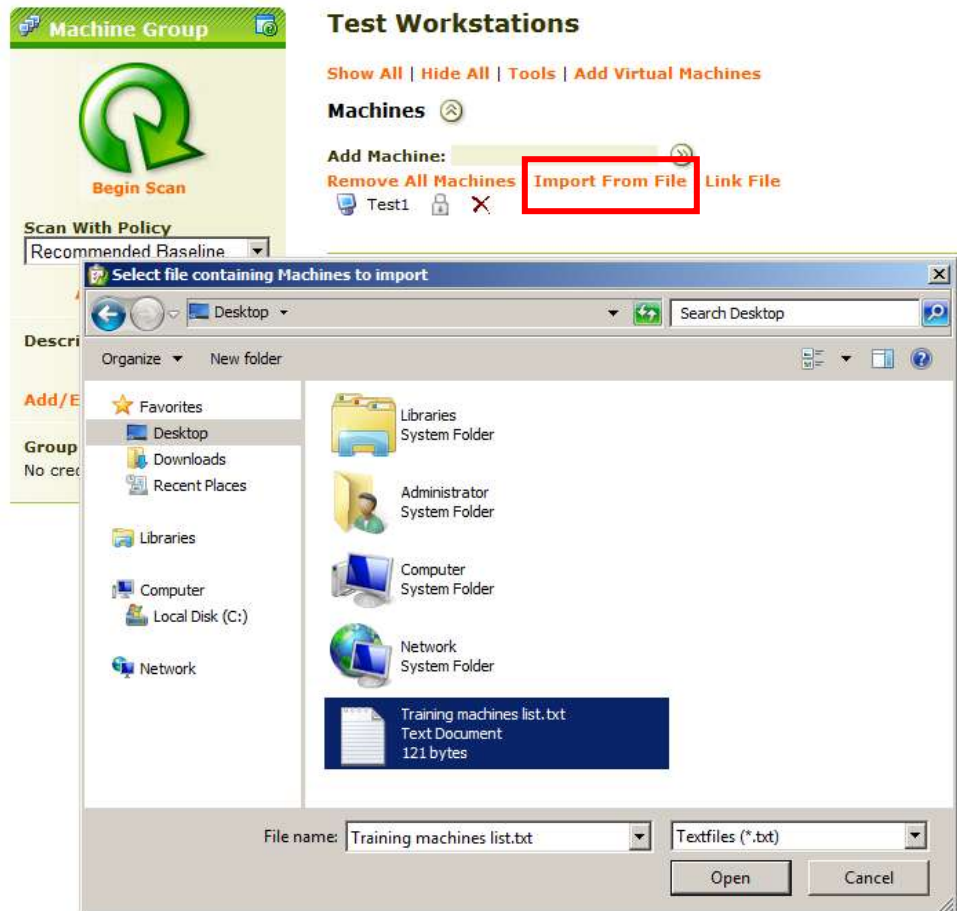


- Click **Begin Scan** to confirm that credentials are correct.

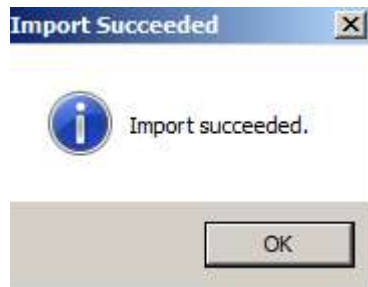
IMPORT AN EXISTING MACHINE GROUP

You can easily import a machine group that has been exported from NetChk Protect or NetChk Configure.

1. Choose an existing machine group or create a new group.
2. Click **Import From File**.
3. Browse to the location of your .txt file and click **Open**.



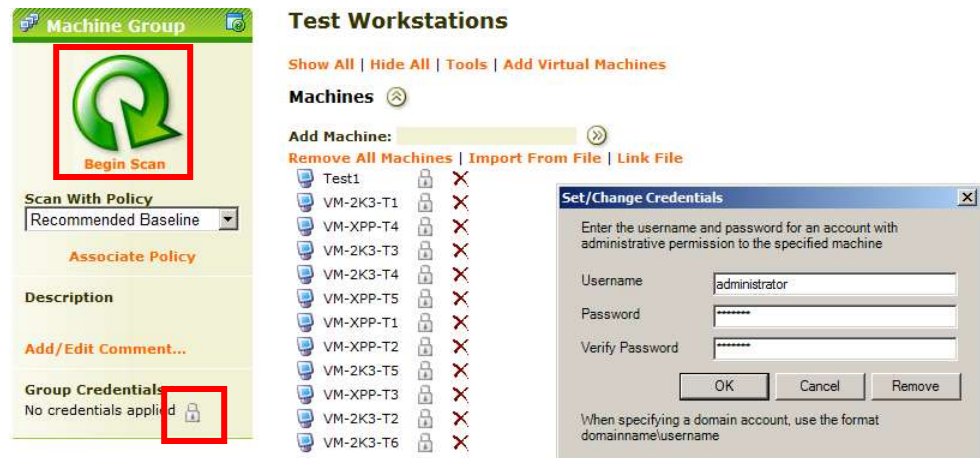
The **Import Succeeded** dialog is displayed.



4. Click **OK**.
5. Specify credentials for the group by clicking the padlock icon.

Note: You can also specify credentials on a machine basis by clicking the padlock icon located next to each machine.

In the popup, enter the credentials for the machines.

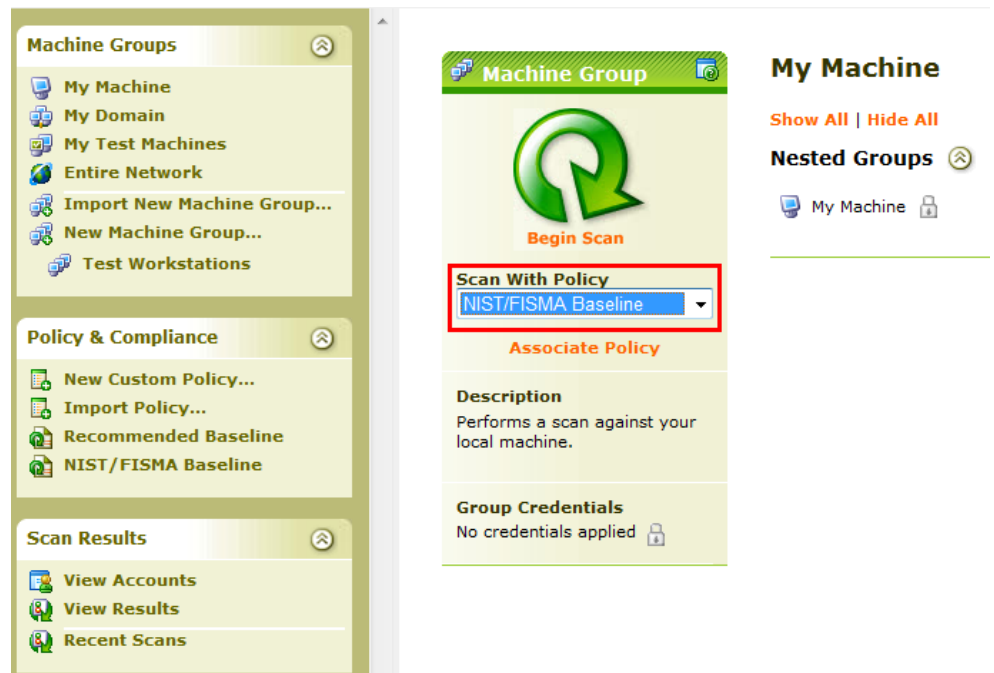


6. Click **Begin Scan** to confirm that credentials are correct.

SCAN AND ENFORCE USING AN EXISTING POLICY

CAUTION! The values specified for the policy checks in the pre-defined policies provided within vCenter Protect Essentials Plus – Configuration Management may not be suitable for every environment. It is strongly recommended that you test enforcement of the policy checks on a small sample of machines in a non-production environment before you enforce the checks on a large scale. This is particularly important when enforcing checks defined within custom policy groups.

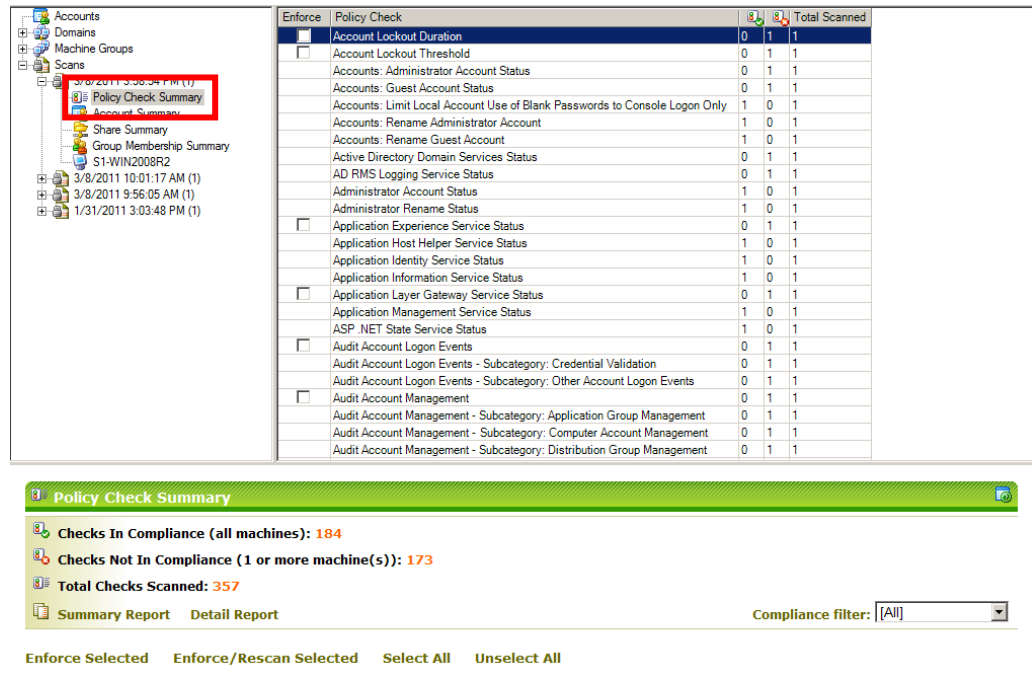
1. From the home page select the machine group you want to scan.
2. In the **Scan With Policy** box select the policy you want to use when scanning the machine.
3. Click **Begin Scan**.



4. The software will analyze your machines and compare them to the policy that you selected.

Note: Most policy checks in vCenter Protect Essentials Plus – Configuration Management are able to be enforced remotely. You can also view manual implementation information on checks for cases where you may not have remote enforcement as an option. To view this information click on a check and in the information window below you can scroll down and see the rationale and manual implementation for the check.

5. When the scan is complete click on **Policy Check Summary**.



6. In the bottom pane, click **Select All** to select all checks.

7. Read the following cautionary statement.

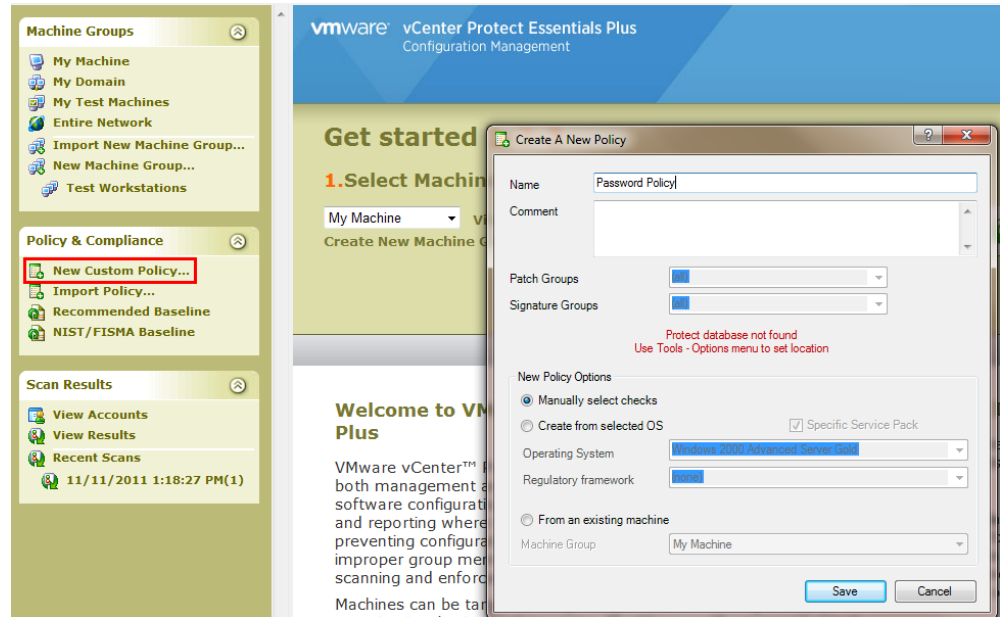
CAUTION! The values specified for the policy checks in the pre-defined policies provided within vCenter Protect Essentials Plus – Configuration Management may not be suitable for every environment. It is strongly recommended that you test enforcement of the policy checks on a small sample of machines in a non-production environment before you enforce the checks on a large scale. This is particularly important when enforcing checks defined within custom policy groups.

8. In the bottom pane click **Enforce/Rescan Selected**.

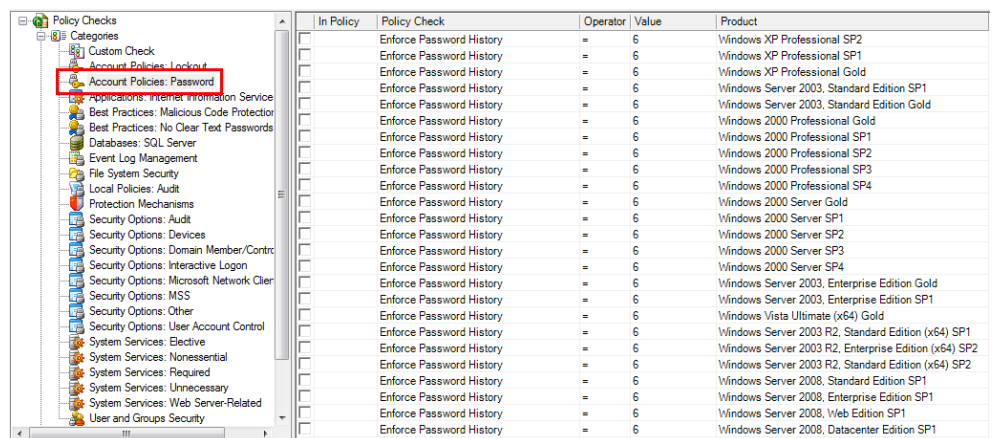
This will update all the selected policy checks and will then perform another scan, using the same parameters of the original scan. Performing a scan immediately after performing an enforcement enables you to verify that the policy checks were updated correctly.

CREATE A NEW CUSTOM POLICY BY MANUALLY SELECTING POLICY CHECKS

1. In the **Policy & Compliance** list click **New Custom Policy**.
2. Name the policy and click **Save**.



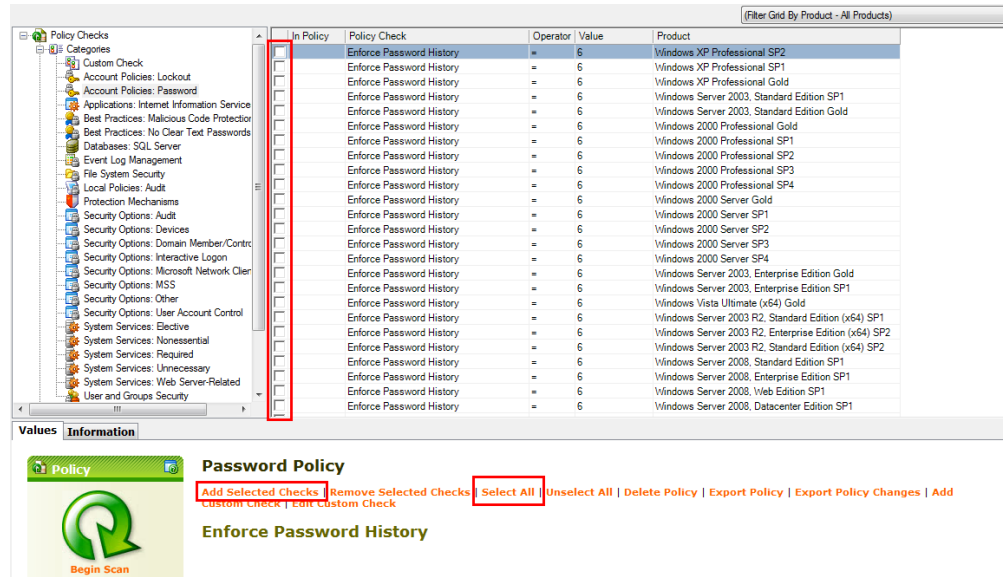
3. In the top left navigation window, expand the **Categories** list and then select one of the categories. For example:



4. In the right-hand pane, enable the check boxes of the policy checks you wish to choose.

Tip: If you want to select all items, click on **Select All** in the bottom pane.

Create a New Custom Policy by Manually Selecting Policy Checks



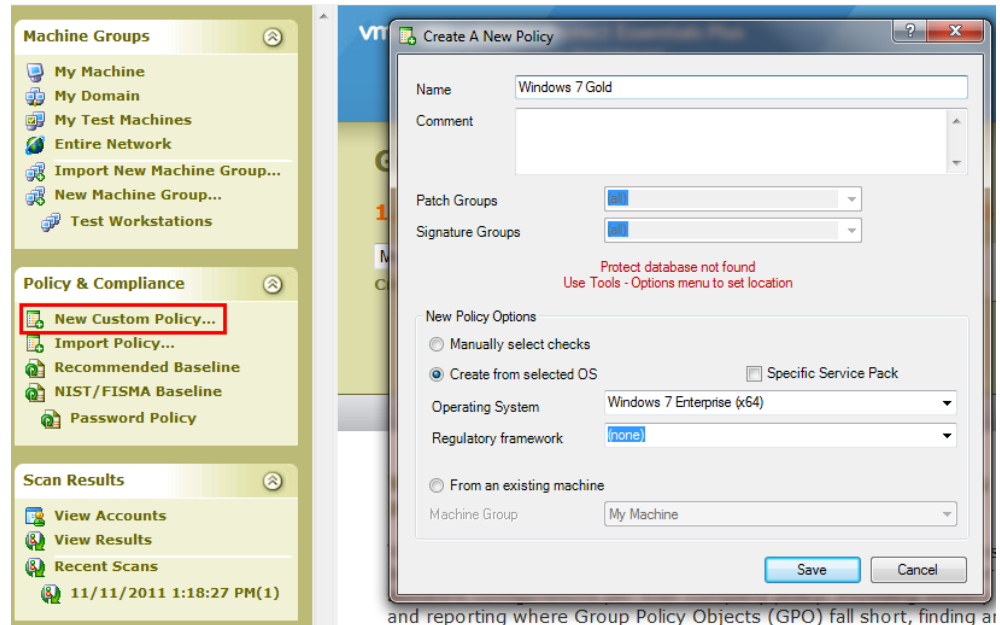
- To add the selected checks to the new policy, in the bottom pane click **Add Selected Checks**.

Notice in the policy window that all selected checks will now display a green check icon in the **In Policy** column.

- Click the **Save** toolbar icon.
- If the **Change Control** dialog is displayed, type a comment that explains the rationale for the change.

CREATE A NEW CUSTOM POLICY USING THE “CREATE FROM SELECTED OS” OPTION

1. In the **Policy & Compliance** list click **New Custom Policy**.
2. Type a name for the new policy.



3. Select **Create from Selected OS**.
4. Clear the **Specific Service Pack** check box.

This will make all service packs for the chosen operating system available in the policy.

5. In the **Operating System** box choose the desired operating system.
6. Click **Save**.

All policy checks for the specified operating system are loaded into the top right pane.

Create a New Custom Policy Using the “Create From Selected OS” Option

The screenshot shows the Policy Manager interface. On the left, there is a tree view of Policy Checks categorized by NIST 800-53, PCI DSS 1.1, PCI DSS 1.2, and PCI DSS 2.0. The main area displays a list of policy checks with columns for 'In Policy', 'Policy Check', 'Operator', 'Value', and 'Product'. The 'Accounts: Rename Administrator Account' check is selected and highlighted in blue.

In Policy	Policy Check	Operator	Value	Product
<input type="checkbox"/>	Account Lockout Duration	=	0	Windows 7 Enterprise (x64) Gold
<input type="checkbox"/>	Account Lockout Duration	=	0	Windows 7 Enterprise (x64) SP1
<input type="checkbox"/>	Account Lockout Threshold	=	5	Windows 7 Enterprise (x64) Gold
<input type="checkbox"/>	Account Lockout Threshold	=	5	Windows 7 Enterprise (x64) SP1
<input type="checkbox"/>	Accounts: Administrator Account Status	=	Enabled	Windows 7 Enterprise (x64) Gold
<input type="checkbox"/>	Accounts: Administrator Account Status	=	Enabled	Windows 7 Enterprise (x64) SP1
<input type="checkbox"/>	Accounts: Guest Account Status	=	Disabled	Windows 7 Enterprise (x64) Gold
<input type="checkbox"/>	Accounts: Guest Account Status	=	Disabled	Windows 7 Enterprise (x64) SP1
<input type="checkbox"/>	Accounts: Limit Local Account Use of Blank Passwords to Console Logon Only	=	Enabled	Windows 7 Enterprise (x64) Gold
<input type="checkbox"/>	Accounts: Limit Local Account Use of Blank Passwords to Console Logon Only	=	Enabled	Windows 7 Enterprise (x64) SP1
<input checked="" type="checkbox"/>	Accounts: Rename Administrator Account	=	(Not Defined By)	Windows 7 Enterprise (x64) Gold
<input type="checkbox"/>	Accounts: Rename Administrator Account	=	(Not Defined By)	Windows 7 Enterprise (x64) SP1
<input type="checkbox"/>	Accounts: Rename Guest Account	=	(Not Defined By)	Windows 7 Enterprise (x64) Gold
<input type="checkbox"/>	Accounts: Rename Guest Account	=	(Not Defined By)	Windows 7 Enterprise (x64) SP1
<input type="checkbox"/>	ActiveX Installer Service Status	=	Manual	Windows 7 Enterprise (x64) Gold
<input type="checkbox"/>	ActiveX Installer Service Status	=	Manual	Windows 7 Enterprise (x64) SP1
<input type="checkbox"/>	Adaptive Brightness Service Status	=	Manual	Windows 7 Enterprise (x64) Gold
<input type="checkbox"/>	Adaptive Brightness Service Status	=	Manual	Windows 7 Enterprise (x64) SP1
<input type="checkbox"/>	Administrator Account Status	=	Enabled	Windows 7 Enterprise (x64) Gold

Below the table, the 'Values' tab is active, showing the 'Information' for the selected policy. The policy is titled 'Windows 7 Gold' and 'Accounts: Rename Administrator Account'. It includes a 'Begin Scan' button, a 'Scan Machine Group' dropdown set to 'My Machine', and a 'Select Patch Group' dropdown set to '(all)'. The 'Make all check values the same' option is checked. The 'Operator' is set to '=' and the 'Value' is '(Not Defined By GPO)'.

7. Select the policy checks you want included in this custom policy and then click the Save icon.

You can create a custom policy for each of your operating systems you have on your network.

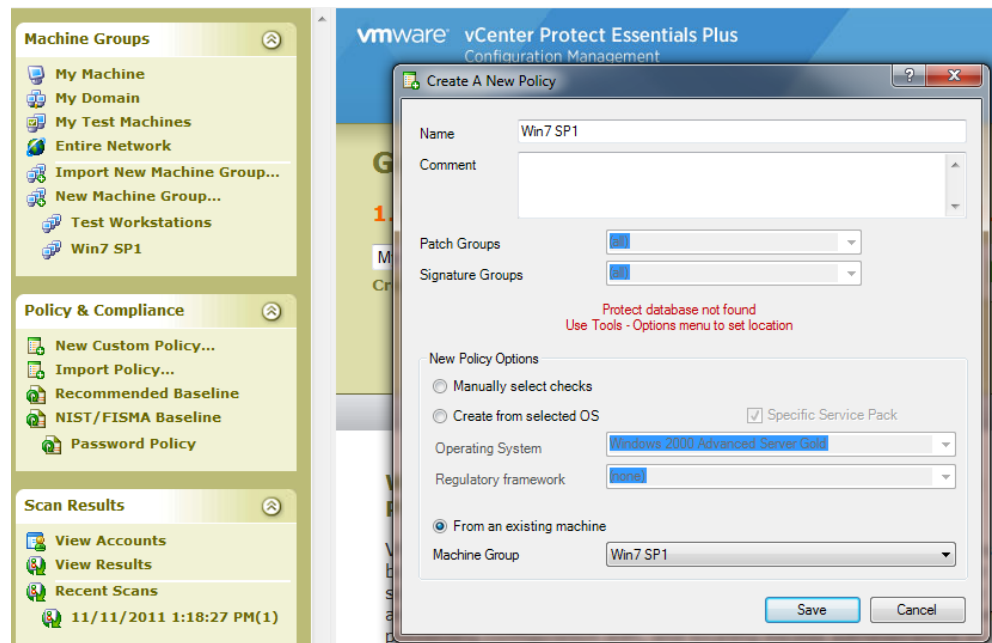
CREATE A NEW CUSTOM POLICY FROM AN EXISTING MACHINE

vCenter Protect Essentials Plus – Configuration Management enables you to create a new policy by cloning the configuration of an established machine. This is a quick and powerful way to create a policy that can immediately be used to scan similar machines in your organization for compliance. The idea is for you to configure one machine in your organization that represents your organization's "gold standard." You then clone a policy using the policy checks on that machine. This process can be very useful when working with vendors or government agencies that provide machines that are pre-configured according to a particular standard.

1. Create a machine group that contains just the one machine you want to use as your gold standard.

There can only be a single machine in the group for this to work.

2. In the **Policy & Compliance** list click **New Custom Policy**.
3. Type a name for the policy.

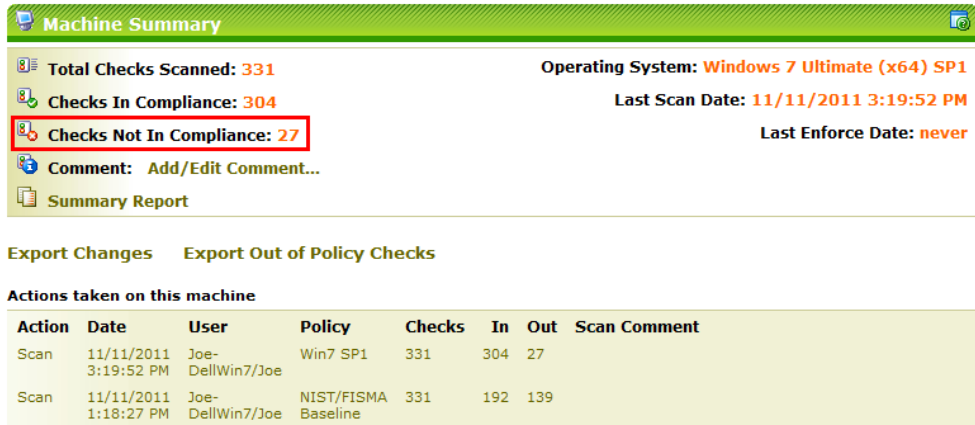


3. Enable the **From an existing machine** check box.
4. Choose the machine group you created in Step 1 and then click **Save**.

The machine is scanned. Every policy check and its associated value found on the machine is added to the new policy. When the process is complete the new policy is displayed.

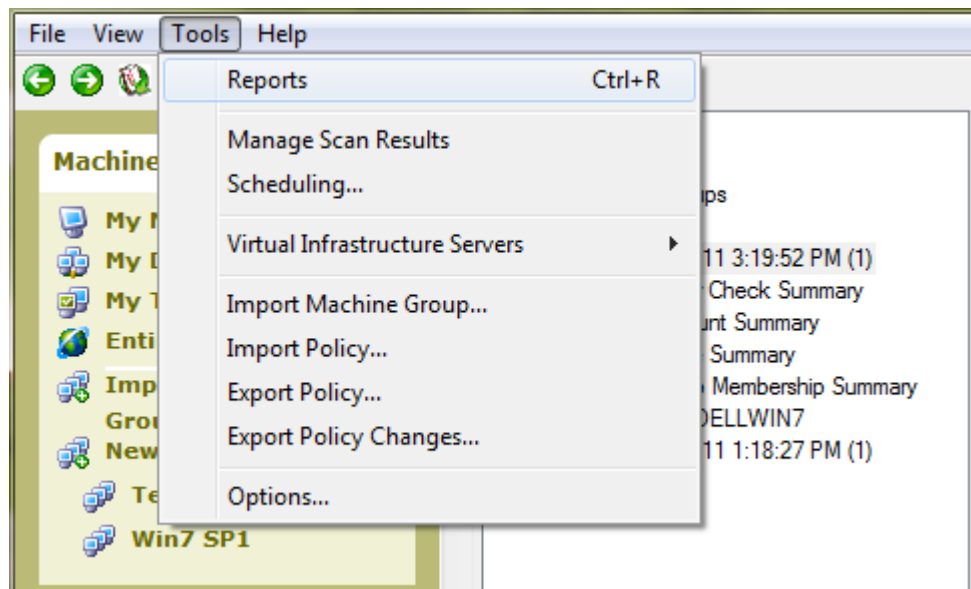
- After the policy is created, rescan the machine group you just copied using the new policy you created based on its configuration and you will find the machine is most likely out of compliance.

This is due to checks that we could not determine on the target machine. Rather than ignore them we add them in so you are aware and can triage their importance and delete if unnecessary.



You can view the policy checks that are out of compliance by sorting the **Compliance** column in the top right pane.

- Select **Tools > Reports**.



- In the **Select Report to View** box choose **Machine Scan History Details**.
- In the **Scan to report on** box and choose the first scan on the list.
This will be the scan we just ran.
- In the **In/Out of compliance** box choose **Out of Compliance**.
- Click **Generate Report**.

Report Gallery

Pick Report...
Please select a report to view. Then specify report criteria below and click the 'Generate Report'

Select Report to View: Machine Scan History Details

Description: Scan history details by scan by machine.

Pick Filter Options...
Please use the following options to set your desired report filter.

Scan to report on: Nov 11 2011 3:19PM: 1 Machines Scanned

Machine Group to report on: [All Machine Groups]

Policy to report on: [All Policies]

Machine to report on: [All Machines]

Policy Check to report on: [All Policy Checks]

Domain to report on: [All Domains]

In/Out of compliance: Out of Compliance

Show Frameworks: [Don't Show]

View Report...
To view report using the filter options set above, click 'Generate Report'.

Generate Report

11. Use the report to cross reference and select the non-compliant checks in the custom policy. For example:

Machine Scan History Details



Report Date: 11/11/2011 3:27 PM

Scan Machine: WORKGROUP\JOE-DELLWIN7			
Scan Date: 11/11/2011 3:19 PM	Policy: Win7 SP1		
Domain: WORKGROUP	IP Address: 192.168.65.19	Product: Windows 7 Ultimate (x64) SP1	
Checks Scanned: 27	Checks Compliant: 0	Checks Noncompliant: 27	
Policy Check	Finding	Operator Policy	Compliance
Audit: Force Audit Policy Subcategory Settings (Windows Vista or	Not Found	= Not Found	✘
Devices: Allowed to Format and Eject Removable Media	Not Found	= Not Found	✘
Devices: Restrict CD-ROM Access to Locally Logged-On User Only	Not Found	= Not Found	✘
Devices: Restrict Floppy Access to Locally Logged-On User Only	Not Found	= Not Found	✘
Interactive Logon: Do Not Require CTRL+ALT+DEL	Not Found	= Not Found	✘
Maximum Setup Log Size		=	✘

Create a New Custom Policy From an Existing Machine

In Policy	Policy Check	Operator	Value	Product
<input type="checkbox"/>	Audit System Events - Subcategory: IPsec Driver	=	No Auditing	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Audit System Events - Subcategory: Other System Events	=	Success and Fai	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Audit System Events - Subcategory: Security State Change	=	Success	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Audit System Events - Subcategory: Security System Extension	=	No Auditing	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Audit System Events - Subcategory: System Integrity	=	Success and Fai	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Audit: Audit the Access of Global System Objects	=	Disabled	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Audit: Audit the Use of Backup and Restore Privilege	=	Disabled	Windows 7 Ultimate (x64) SP1
<input checked="" type="checkbox"/>	Audit: Force Audit Policy Subcategory Settings (Windows Vista or Later) to Override Audit Policy Category Settings	=	Not Found	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Audit: Shut Down System Immediately if Unable to Log Security Audits	=	Disabled	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Automatic Logon	=	Disabled	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Automatic Updates Service Status	=	Automatic-Runni	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Background Intelligent Transfer Service Status	=	Manual	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Backup Operators Restricted Group	=	No Group Memb	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Base Filtering Engine Service Status	=	Automatic-Runni	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	BitLocker Drive Encryption Service Status	=	Manual	Windows 7 Ultimate (x64) SP1
<input type="checkbox"/>	Block Level Backup Engine Service Status	=	Manual	Windows 7 Ultimate (x64) SP1

Win7 SP1

[Add Selected Checks](#) | [Remove Selected Checks](#) | [Select All](#) | [Unselect All](#) | [Delete Policy](#) | [Export Policy](#) | [Export Policy Changes](#) | [Add Custom Check](#) | [Edit Custom Check](#)

Audit: Force Audit Policy Subcategory Settings (Windows Vista or Later) to Override Audit Policy Category Settings

Make all check values the same

Product: Windows 7 Ultimate (x64) SP1

Operator	Value
=	Disabled

Begin Scan

Scan Machine Group: My Machine

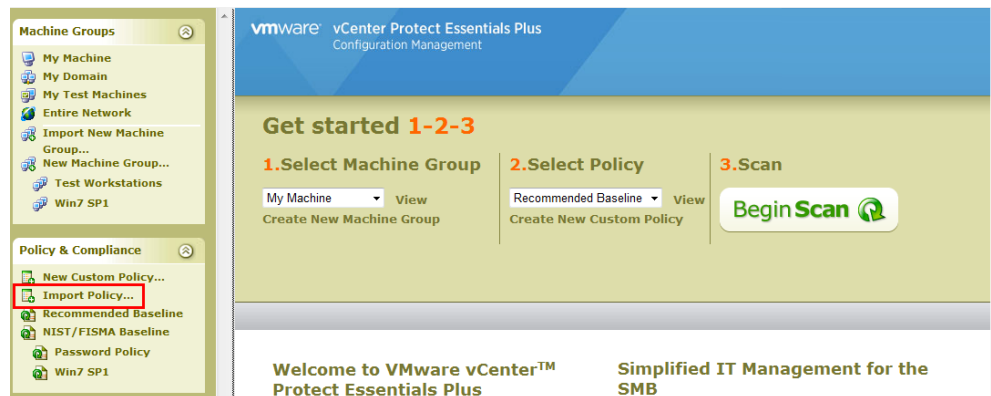
12. Within the custom policy, select each non-compliant check.
13. Click **Remove Selected Checks**.
14. Click the Save toolbar icon.
15. Rescan the machine group using the updated custom policy. The new result should now show a compliant scan.

IMPORT POLICIES

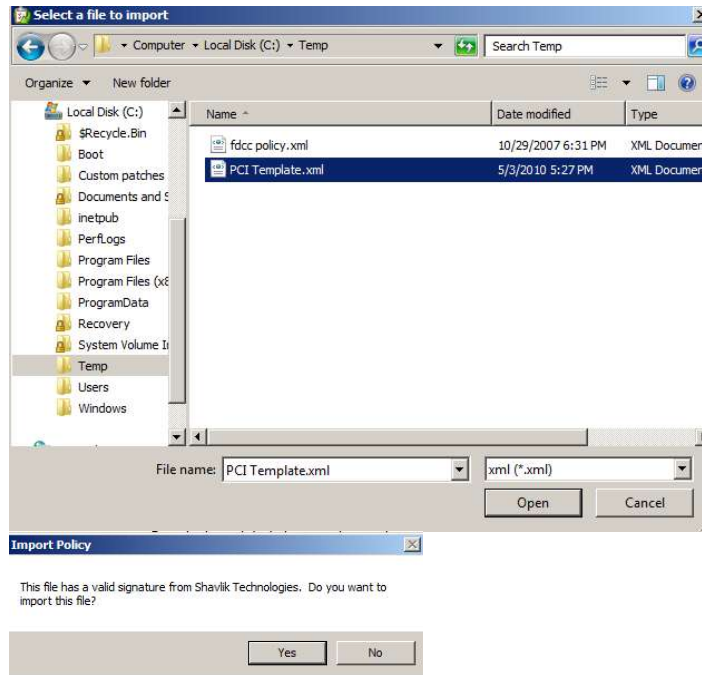
1. Use a Web browser to go to http://hfnetchk4.shavlik.com/downloads/pci_baseline.zip.
2. Download the **PCI Template** and save the PCI_Baseline.zip file to a folder.



3. Extract the **PCI_Baseline.xml** file from the zip file to a folder.
4. In vCenter Protect Essentials Plus – Configuration Management, in the **Policy & Compliance** list, click **Import Policy**.



5. Locate the **PCI_Baseline.xml** file and click **Open**.



6. On the **Import Policy** dialog click **Yes** (for security reasons this file contains a digital signature from VMware).

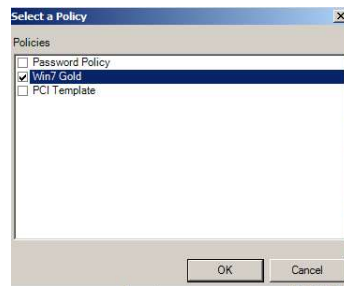
The policy will be imported. The PCI template is very large and may take several minutes to import.

Once the import is complete, refresh the screen and the PCI Template will be contained in the **Policy & Compliance** list.

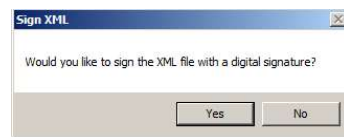
MERGE POLICIES

Merging two policies into one gives you the ability to create a single unified policy rather than supporting each OS\SP variation in your environment with a separate policy.

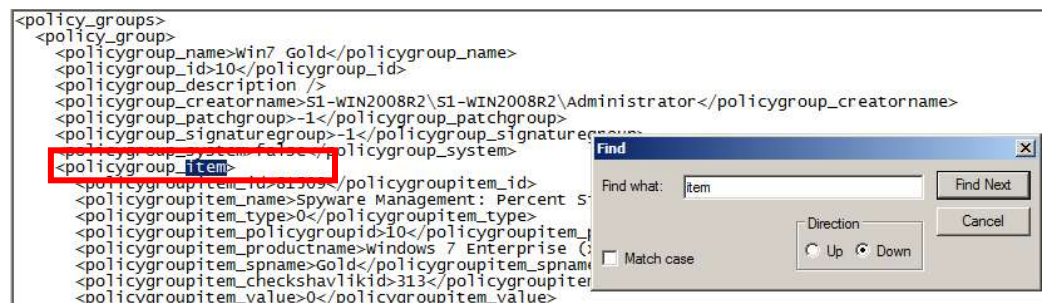
1. Select **Tools > Export Policy**.
2. In the **Select a Policy** dialog select the desired policy and then click **OK**.



3. Name the file and save it to your hard drive.



4. On the **Sign XML** dialog click **No**.
5. Export a different policy by repeating steps 1-4.
6. Within Windows Explorer, right-click on the first policy you exported and click **Edit**.
7. Find the first **policygroup_item** tag.



8. Copy all **policygroup_item** tags.

```

<policygroupitem_type>0</policygroupitem_type>
<policygroupitem_policygroupid>10</policygroupitem_policygroupid>
<policygroupitem_productname>windows 7 Enterprise (x64)</policygroupitem_productname>
<policygroupitem_sname>Gold</policygroupitem_sname>
<policygroupitem_checkshavlikid>173</policygroupitem_checkshavlikid>
<policygroupitem_value>true</policygroupitem_value>
<policygroupitem_operator>=</policygroupitem_operator>
<policygroupitem_displayvalue>sysadmin Only</policygroupitem_displayvalue>
</policygroup_item>
<policygroup_item>
<policygroupitem_id>81835</policygroupitem_id>
<policygroupitem_name>SQL Server: Account Weak Password Status</policygroupitem_name>
<policygroupitem_type>0</policygroupitem_type>
<policygroupitem_policygroupid>10</policygroupitem_policygroupid>
<policygroupitem_productname>windows 7 Enterprise (x64)</policygroupitem_productname>
<policygroupitem_sname>Gold</policygroupitem_sname>
<policygroupitem_checkshavlikid>175</policygroupitem_checkshavlikid>
<policygroupitem_value>false</policygroupitem_value>
<policygroupitem_operator>=</policygroupitem_operator>
<policygroupitem_displayvalue>Allow Weak Passwords</policygroupitem_displayvalue>
</policygroup_item>
<policygroup_item>
<policygroupitem_id>81836</policygroupitem_id>
<policygroupitem_name>SQL Server: Authentication Mode Status</policygroupitem_name>
<policygroupitem_type>0</policygroupitem_type>
<policygroupitem_policygroupid>10</policygroupitem_policygroupid>
<policygroupitem_productname>windows 7 Enterprise (x64)</policygroupitem_productname>
<policygroupitem_sname>Gold</policygroupitem_sname>
<policygroupitem_checkshavlikid>176</policygroupitem_checkshavlikid>
<policygroupitem_value>true</policygroupitem_value>
<policygroupitem_operator>=</policygroupitem_operator>
<policygroupitem_displayvalue>windows Authentication Mode</policygroupitem_displayvalue>
</policygroup_item>
</policy_group>
</policy_groups>

```

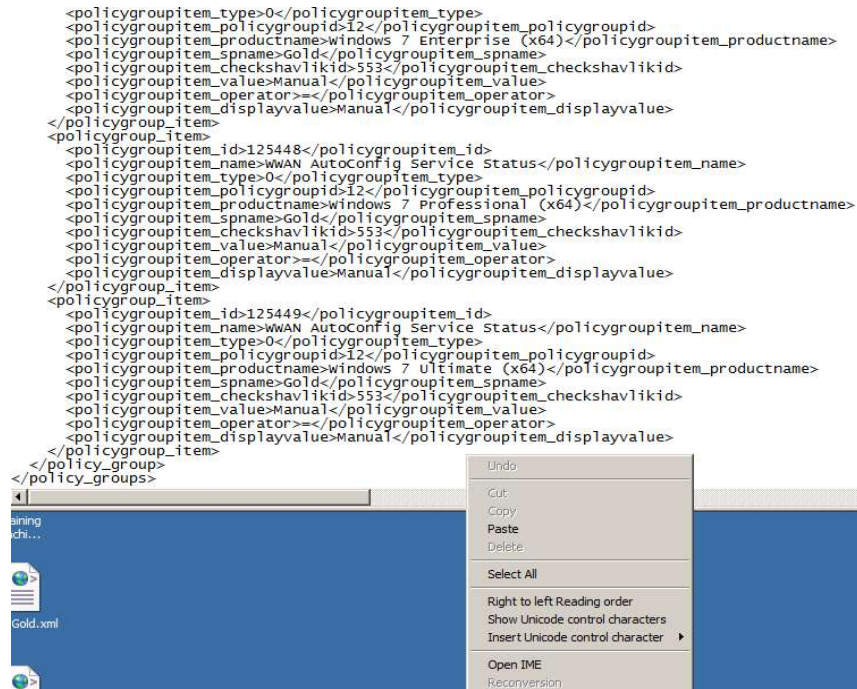
9. In Windows Explorer, right-click on the second policy you exported and click on **Edit**.10. Go to the **policygroup_name** tag and rename the policy.

```

<policy_groups>
  <policy_group>
    <policygroup_name>win7 Gold</policygroup_name>
    <policygroup_id>10</policygroup_id>
    <policygroup_description />
    <policygroup_creatorname>S1-WIN2008R2\S1-WIN2008R2\A
    <policygroup_patchgroup>-1</policygroup_patchgroup>
    <policygroup_signaturegroup>-1</policygroup_signaturegroup>
    <policygroup_system>false</policygroup_system>
  </policy_group>
</policy_groups>

```

11. Scroll to the very bottom of the second policy and paste the copied items after the last **</Policygroup_item>** tag.



12. Select **File > Save As**, name the file, and set the **Save as type** to **All files**.

13. Within vCenter Protect Essentials Plus – Configuration Management, click on **Import Policy**.

14. Locate the newly merged policy and click **Open**.



The merged policy is imported into vCenter Protect Essentials Plus – Configuration Management.

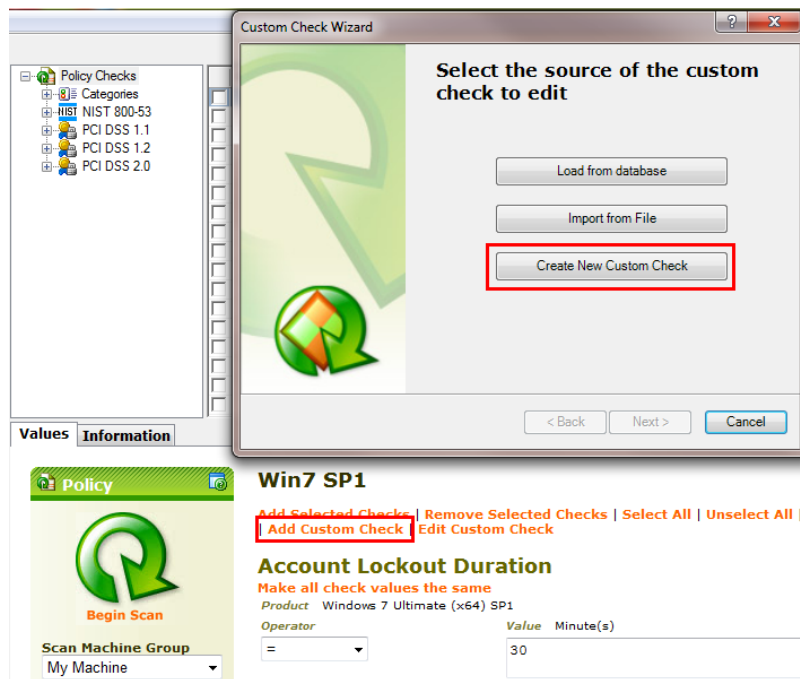
15. In the **Policy & Compliance** list select the new policy and select one of the checks to verify you see both OS variations available.

ADD CUSTOM CHECKS TO A POLICY AND ENFORCE

vCenter Protect Essentials Plus – Configuration Management enables you to create your own custom policy checks. This allows you to track items that are unique to your organization. The following example shows how you can check to make sure that Windows Firewall automatically loads at start up.

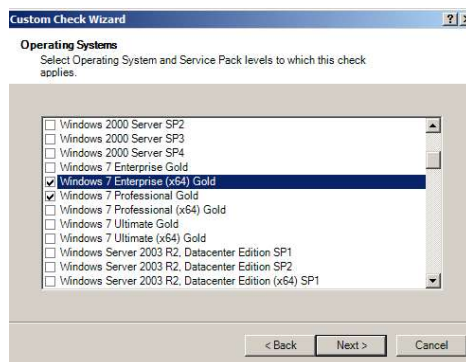
1. In the **Policy & Compliance** list click on any custom policy.
2. In the bottom pane click **Add Custom Check**.

Note: This link is not available from either of the two predefined policies because they cannot be modified.



3. On the **Custom Check Wizard** dialog click **Create New Custom Check**.

The **Operating Systems** dialog is displayed.



4. Select one or more operating systems and then click **Next**.

The **General Properties** dialog is displayed.

5. In the **Name** box type **Firewall Check**.
6. In the **Type** box choose **Service Status** and then click **Next**.

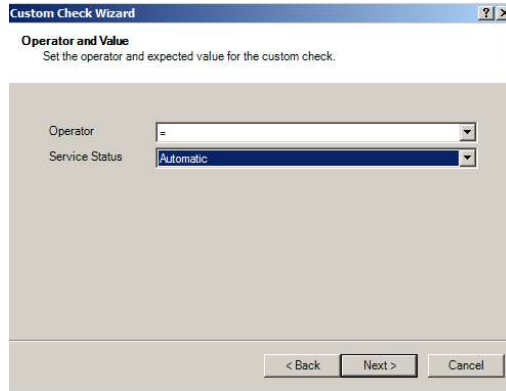
The **Type Specific Properties** dialog is displayed.

7. In the **Service** name box type **MpsSvc**.

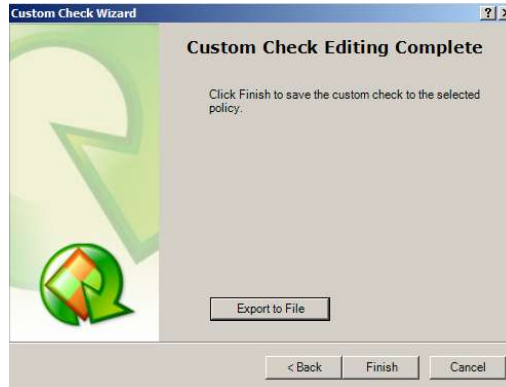
Hint: To find the service name, go to Administrative Tools > Services in Windows and right-click on the service you want to check. Click on Properties, the service name is listed at the top.

8. Click **Test Check**. If it checks out, click on **Next**.

The **Operator and Value** dialog is displayed.



9. In the **Operator** box choose =.
10. In the **Service Status** box choose **Automatic** and then click **Next**.
11. Click **Finish**.



We just demonstrated how to create one of the more common custom checks. The ability to add custom checks is a powerful feature in vCenter Protect Essentials Plus – Configuration Management. Every environment is different and there is no end to the possible combinations of settings that could be necessary for an administrator to configure and support for their environment. The ability to automate the assessment and enforcement of the configuration settings saves countless hours of time and effort to maintain consistent machine configurations.

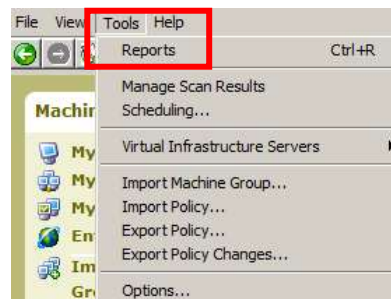
REPORTING

vCenter Protect Essentials Plus – Configuration Management enables you to generate many different types of audit ready reports.

Executive Summary

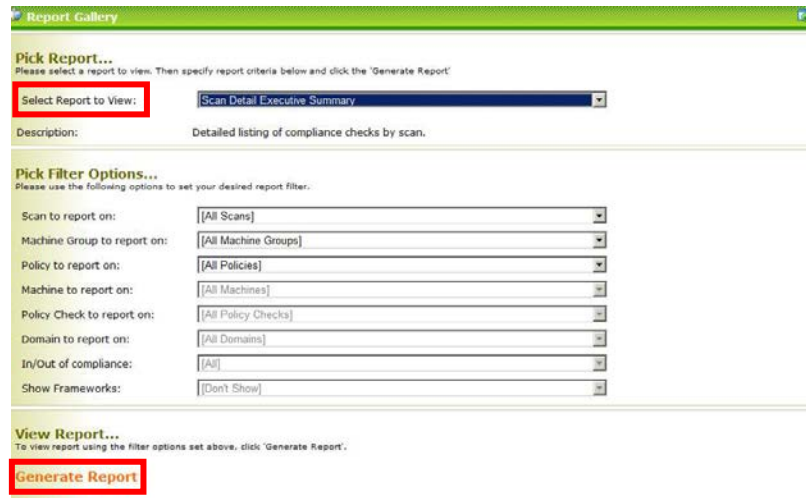
This report gives a brief high-level view of scans you have performed in your environment.

1. Select **Tools > Reports**.



2. In the **Select Report to View** box, choose **Scan Detail Executive Summary**.
3. Click **Generate Report**.

This generates a report of all scans conducted to date.



Local Account Summary

This report shows the local accounts detected for the machines in the scan result chosen.

1. Select **Tools > Reports**.
2. In the **Select Report to View** box choose **Local Account Summary**.

Pick Report...
Please select a report to view. Then specify report criteria below and click the 'Generate Report'.

Select Report to View: Local Account Summary

Description: Detailed listing of local account information by machine by scan.

Pick Filter Options...
Please use the following options to set your desired report filter.

Scan to report on: Mar 9 2011 2:48PM 1 Machines Scanned

Machine Group to report on: [All Machine Groups]

Policy to report on: [All Policies]

Machine to report on: [All Machines]

Policy Check to report on: [All Policy Checks]

Domain to report on: [All Domains]

In/Out of compliance: [All]

Show Frameworks: [Don't Show]

View Report...
To view report using the filter options set above, click 'Generate Report'.

Generate Report

3. In the **Scan to report on** box choose the first scan in the list.
4. Click **Generate Report**.

Scan Policy Compliance Summary by Item

This report shows a very extensive break down of what was detected as in or out of compliance. Using the frameworks it maps all checks to the framework of your choice to create an audit-ready report that will save large amounts of time and effort during an audit.

1. Select **Tools > Reports**.
2. In the **Select Report to View** box choose **Scan Policy Compliance Summary by Item**.

Pick Report...
Please select a report to view. Then specify report criteria below and click the 'Generate Report'.

Select Report to View: Scan Policy Compliance Summary by Item

Description: Summary of machine compliance by check by scan.

Pick Filter Options...
Please use the following options to set your desired report filter.

Scan to report on: Mar 9 2011 2:48PM: 1 Machines Scanned

Machine Group to report on: [All Machine Groups]

Policy to report on: [All Policies]

Machine to report on: [All Machines]

Policy Check to report on: [All Policy Checks]

Domain to report on: [All Domains]

In/Out of compliance: [All]

Show Frameworks: PCI DSS 1.1

View Report...
To view report using the filter options set above, click 'Generate Report'.

Generate Report

3. In the **Scan to report on** box choose the first scan in the list.
4. In the **Show Frameworks** box choose **PCI DSS 1.1**.
5. Click **Generate Report**.

VMware, Inc.
3401 Hillview Avenue
Palo Alto, California 94304