Oracle® Enterprise Manager

Application Configuration Console PCI Compliance

Release 5.3.2

E14654-02

September 2009

Oracle Enterprise Manager Application Configuration Console PCI Compliance Release 5.3.2

E14654-02

Primary Author: James Garrison

Contents

List of Tables

Preface

This document describes how you can use Application Configuration Console to check and monitor your environment for compliance with the Payment Card Industry Data Security Standard.

Audience

This document is intended for administrators and other parties who are responsible for ensuring that their operating system environment complies with the standards set forth by the Security Standards Council to protect credit card data.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at `http://www.fcc.gov/cgb/consumerfacts/trs.html`, and a list of phone numbers is available at `http://www.fcc.gov/cgb/dro/trsphonebk.html`.

Related Documents

For more information, see the following documents in the Application Configuration Console documentation set:

- *Release Notes*
- *Getting Started*
- *Installation Guide*
- *Command Line Interface Reference*
- *Performance and Tuning Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Overview

This chapter defines PCI compliance and Application Configuration Console's role in supporting it.

1.1 What Is PCI Compliance?

Payment Card Industry Data Security Standard or PCI DSS is the result of a mandate by major credit card brands such as VISA, MasterCard, and American Express to improve security of credit card data. The standard stipulates compliance with a set of account protection mechanisms by taking actions such as the following:

- Maintain an information security policy.
- Use and update anti-virus software.
- Encrypt transmission of cardholder data.
- Maintain firewall configuration.
- Take physical access control measures.
- Prevent insecure configuration management.
- Track system configurations.
- Monitor file and directory permissions to ensure that only authorized personnel ve access.
- Monitor access changes to system services, ensuring that all unnecessary and insecure services and protocols are disabled.
- Monitor user account policies such as password aging, and password complexity.

1.2 What If I Don't Handle Credit Card Transactions?

While aimed at merchants, processors, point-of-sale vendors, financial institutions, and payment companies, the spirit of the standard is geared to securing sensitive data, something every business and private citizen can identify with. In this case, the result of the action taken holds significance, even if the codified rule that requires it doesn't. In other words, the fact that you take steps to ensure proper user authentication and password management is what's important, not that you satisfy PCI requirement 8.5.

1.3 How Does Application Configuration Console Support Compliance?

Application Configuration Console is in the business of automating configuration, change, and release management processes. Monitoring changes to operating system security settings is a natural extension of this core competence.

The Application Configuration Console PCI Compliance Automation Module extends Application Configuration Console by providing the tools for creating assets that capture operating system security settings. The tools then provide for these assets to be audited for compliance with recommended standards. Once you have a baseline for your environment, Application Configuration Console's tracking capabilities take over to monitor for any changes and to ensure remediation of detected differences.

1.4 Is Application Configuration Console's PCI Compliance Across the Board?

The Security Standards Council does not avow a single-sourced solution to its mandate. PCI compliance covers a broad spectrum of initiatives, some of which exist outside the reach of Application Configuration Console software influence.

Table 1–1 revisits the previously referenced list of account protection mechanisms identified by the Security Standards Council, this time noting which are supported by the Application Configuration Console PCI Compliance Automation Module.

Table 1–1 PCI Requirements Supported by Application Configuration Console

PCI Requirement	Supported
Maintain an information security policy	No
Use and update anti-virus software	No
Encrypt transmission of cardholder data	No
Maintain firewall configuration	No
Take physical access control measures	No
Prevent insecure configuration management	Yes
Track system configurations	Yes
Monitor file and directory permissions to ensure that only authorized personnel have access	Yes
Monitor access changes to system services, ensuring that all unnecessary and insecure services and protocols are disabled	Yes
Monitor user account policies such as password aging, and password complexity	Yes

1.5 More Information

This book describes use of the PCI Compliance Automation Module to achieve compliance with recommended operating system security settings. Its focus is on Application Configuration Console functionality in that limited context. For detailed information on system features and how to use them, consult the *Application Configuration Console Online Help*.

2

PCI Compliance Automation Module

This chapter instructs how to install Application Configuration Console's PCI Compliance Automation Module and describes the installed components.

2.1 Prerequisites

PCI compliance in a Windows environment requires that you have the Windows Resource Extensions (WRE) installed. WRE is an Application Configuration Console product add-in that enables you to extract Windows configuration data from Windows servers to create assets in Application Configuration Console. To do this, the Server connects to proxy service, which in turn, runs Visual Basic scripts on target machines to extract the data and pass it back through the Application Configuration Console Server to the Clients.

PCI compliance for Windows functions in the same way, using the proxy service to run scripts against target machines to create PCI assets.

For information on installation and setup of WRE, see the Application Configuration Console Installation Guide. See the Windows Resource Extensions Online Help for a detailed description of WRE and how to use it.

Important

Regardless of whether you have an earlier version of WRE installed, or you are installing the 5.3.2 version to satisfy this prerequisite, you must then unzip a set of PCI scripts to the proxy service host, as follows:

1. Navigate to the following root folder on the distribution media:

   ```
   \extensions
   ```

2. Open the `WindowsRE.zip` file to expose the contents.
3. Extract `windows_pci_scripts.zip` to the following location on the proxy service host:

   proxyroot`\OpenSSH\mValentScripts`

You must do this for the PCI auditing function to work in your Windows environment. Now proceed with the PCI Compliance Automation Module installation.

2.2 Installing the PCI Compliance Automation Module

To install automation modules, you must start the Application Configuration Console Server, then start the Client and log in as a member of the Administrators group.

1. Copy the JAR file for the PCI Compliance Automation Module to the Server host system.
2. In the Client, select **Admin > Install Extension** in the menu bar.

   The Install Extension dialog opens.
3. Select "automation" as the extension type.
4. Click **Browse** to locate the JAR file in the file system.
5. Click **OK** to install the automation module.

The automation module features are available immediately after installation. You do not need to restart the Application Configuration Console Server or Clients.

The installation includes Windows, Linux, and Solaris solutions; that is, there are sets of resource specifications and complementary auditing dictionaries for each platform. All PCI resource specifications and dictionaries appear in their respective folders in the Navigator view:

- **System > Resource Specifications > PCI_AUDIT_AUTOMATION_MODULE**
- **System > Property Dictionaries**

2.3 About Resource Specifications

Resource specifications identify resources on external systems from which Application Configuration Console assets will be created. The PCI Compliance Automation Module uses command resource specifications that define commands and scripts to be executed on remote hosts to extract security-related configuration data. Organizations then audit the assets created from the extracted data to see if their settings match the settings recommended for PCI compliance.

2.4 About Auditing Dictionaries

Auditing dictionaries are lists of name value pairs derived from the various PCI standards defined by the Security Standards Council. Where appropriate, a command resource definition includes metadata that names the auditing dictionary against which to validate the configuration settings. When you audit an asset for compliance, configuration settings are compared to the appropriate dictionary, with the following potential outcome:

- The named dictionary, as designated by the command resource definition, does not exist; no auditing of the configuration occurs
- A property in the dictionary is missing in the configuration
- A property value in the configuration differs from the expected value in the dictionary

Not all PCI asset configurations are intended to validate against an auditing dictionary. In these cases, the information will predictably change, but there is no set value that represents compliance. It is sufficient that the supplied resource specifications result in assets that can be automatically monitored as part of the overall security audit.

2.5 Windows Resource Specifications and Dictionaries

The command resource specifications for Windows extract various operating system settings related to security. There are seven resource specifications in this category:

- Six that consist of a single command resource definition
- One that combines three of the seven command resource definitions from above; these three have complementary dictionaries

These command resource definitions use XML mapping when creating assets. The installation program sets the remote script path in the command resource definition to the machine that hosts the proxy service. Command line arguments are predefined. You should not edit these values unless instructed to do so by Oracle Technical Support or Professional Services personnel.

Table 2–1 identifies the Windows PCI command resource specifications. For Windows, the command resource definition and, where applicable, the auditing dictionary have the same name as the resource specification.

Table 2–1 Windows PCI Resource Specifications and Supported Requirements

Resource Specification	PCI Rule	Description
`PCI_Win32_OS`	2.2.2-3	Enumerates various Windows Server 2003 operating system settings: Computer system summary Operating system summary Logical disk environment Variables startup commands Services
`PCI_Win32_FilePermissions`	2.2.3 11.5	Enumerates NTFS permissions on a predefined list of files recommended by the *Windows Server 2003 Hardening Guide*.
`PCI_Win32_RSOP_SecurityInfo`	2.2.3 8.5.9-14 10.2.3 10.5.1 10.7	Enumerates security settings applied by a Group Policy Object.
`PCI_Win32_RegistryKeys_ GPOSecurityOptions`	2.2.3	Enumerates security-specific Registry keys and their values set by a Group Policy Object (Security Options section) and applied to a Windows Server 2003.
`PCI_Win32_SecurityUpdates`	6.1	Enumerates all installed Hotfixes that are security-related.
`PCI_Win32_UsersAndGroups`	8.1	Enumerates the existing local user and group accounts on a Windows Server 2003.
`PCI_Win32_ComplianceCombo`	2.2.3 8.5.9-14 10.2-3 10.5.1 10.7 11.5	Combines three of the above resource specifications.

The PCI_Win32_ComplianceCombo resource specification is just that, a combination of these three resource specifications:

- PCI_Win32_FilePermissions
- PCI_Win32_RSOP_SecurityInfo
- PCI_Win32_RegistryKeys_GPOSecurityOptions

Together they create an asset consisting of three configurations, each of which has a complementary auditing dictionary of the same name against which to validate. In other words, from a compliance standpoint, you have the option of creating three assets each consisting of a single configuration, or a single asset consisting of three configurations. It's simply a matter of preference.

The Windows auditing dictionaries are based on the following standards documents:

- *Payment Card Industry Data Security Standard* version 1.1
- *Windows Server 2003 Hardening Guide*
- The Center for Internet Security’s *Windows Server 2003 Operating System Legacy, Enterprise, and Specialized Security Benchmark Consensus Security Settings for Domain Member Servers* version 2.0

2.6 Linux Resource Specifications and Dictionaries

The command resource specifications for Linux extract various operating system settings related to security. There are four resource specifications in this category:

- One all-purpose Linux OS specification that consists of eight command resource definitions, each of which has a complementary dictionary
- Three specialized specifications, each of which has a single command resource definition and no complementary dictionary

These command resource definitions use Java Properties mapping when creating assets. The remote script path and command line arguments are predefined. You should not edit these values unless instructed to do so by Oracle Technical Support or Professional Services personnel.

The Linux auditing dictionaries are based on the *Payment Card Industry Data Security Standard* version 1.1.

Table 2–2 identifies the PCI_Linux resource specification, which has eight command resource definitions and complementary auditing dictionaries.

Table 2–2 ***`PCI_Linux` Command Resource Definitions and Supported Requirements***

Resource Definition/ Auditing Dictionary	PCI Rule	Description

`System Log File Permissions`
`PCI_Linux_SysLogFilePermissions`
	10.5.5	Extracts permissions, and owner and group status on logs such as:
		`var/log/boot.log`
		`var/log/btmp`
		`var/log/cron`

`At_Cron File Permissions`
`PCI_Linux_CronPermissions`
	7.1	Extracts permissions, and owner and group status on files that restrict access to submit at and `cron` jobs, such as:
		`etc/at.allow`
		`etc/cron.allow`
		`etc/cron/deny`

`User Environment File Permissions`
`PCI_Linux_UserEnvFilePermissions`
	8.5	Extracts permissions, and owner and group status on files that contain information on user accounts, such as:
		`etc/group`
		`etc/gshadow`
		`etc/passwd`
		`etc/shadow`

`Login Configuration File`
`PCI_Linux_LoginConfiguration`
	8.5.9-10	Extracts password-related information, such as:
		Maximum days use of a password
		Days warning before password expiration
		Minimum days between password changes

`Empty Password Verification`
`PCI_Linux_EmptyPassword`
	8.5.10	Reports on empty passwords on existing accounts

`Warning Banner File Permissions`
`PCI_Linux_WarningBannerPermissions`
	7.1	Extracts permissions, owner and group status, and size of the file that contains system display information, such as message of the day

`System Services`
`PCI_Linux_SystemServices`
	2.2.2	Reports on run-level information for system services such as Telnet, ftp, and so forth

`TCP Wrapper Support Services`
`PCI_Linux_`
`TCPWrapperSupportServices`
	1.3	Reports on services that are compiled with TCP wrapper support

2.7 Solaris Resource Specifications and Dictionaries

The command resource specifications for Solaris extract various operating system settings related to security. There are four resource specifications in this category:

- One all-purpose Solaris OS specification that consists of 12 command resource definitions, each of which has a complementary dictionary
- Three specialized specifications, each of which has a single command resource definition and no complementary dictionary

These command resource definitions use Java Properties mapping when creating assets. The remote script path and command line arguments are predefined. You should not edit these values unless instructed to do so by Oracle Technical Support or Professional Services personnel.

The Solaris auditing dictionaries are based on the *Payment Card Industry Data Data Security Standard* version 1.1

Table 2–3 identifies the `PCI_Solaris` resource specification, which has 12 command resource definitions and complementary auditing dictionaries.

Table 2–3 `PCI_Solaris` Command Resource Definitions and Supported Requirements

Resource Definition/ Auditing Dictionary	PCI Rule	Description

`At-Cron File Permissions`
`PCI_Solaris_CronPermissions`
	7.1	Extracts permissions, and owner and group status on files that restrict access to submit at and `cron` jobs, such as:
		`etc/at.allow`
		`etc/cron.allow`
		`etc/cron/deny`

`User Environment File Permissions`
`PCI_Solaris_UserEnvFilePermissions`
	8.5	Extracts permissions, and owner and group status on files that contain information on user accounts, such as:
		`etc/group`
		`etc/gshadow`
		`etc/passwd`
		`etc/shadow`

`Empty Password Verification`
`PCI_Solaris_EmptyPassword`
	8.5.10	Reports on empty passwords on existing accounts

`Warning Banner File Permissions`
`PCI_Solaris_WarningBannerPermissions`
	7.1	Extracts permissions, owner and group status, and size of the file that contains system display information, such as message of the day

`System Log File Permissions`
`PCI_Solaris_SysLogFilePermissions`
	10.5.5	Extracts permissions, and owner and group status on logs such as:
		`var/adm/boot.log`
		`var/adm/last.log`
		`var/adm/secure`

`System Log File Permissions 2`
`PCI_Solaris_SysLogFilePermissions`
	10.5.5	Extracts permissions, and owner and group status on logs such as:
		`var/cron`
		`var/samba`

Table 2–3 (Cont.) `PCI_Solaris` Command Resource Definitions and Supported

Resource Definition/ Auditing Dictionary	PCI Rule	Description

`System Log File Permissions 3`
`PCI_Solaris_SysLogFilePermissions`
	10.5.5	Extracts permissions, and owner and group status on logs such as:
		`var/log/syslog`
		`var/log/rpmpkgs`

`System Log File Permissions 4`
`PCI_Solaris_SysLogFilePermissions`
	10.5.5	Extracts permissions, and owner and group status on `var/lib/pgsql`

`System Log File Permissions 5`
`PCI_Solaris_SysLogFilePermissions`
	10.5.5	Extracts permissions, and owner and group status on `usr/bin/dmesg`

`System Log File Permissions 6`
`PCI_Solaris_SysLogFilePermissions`
	10.5.5	Extracts permissions, and owner and group status on `dev/ksyms`

`Login Configuration`
`PCI_Solaris_LoginConfiguration`
	8.5.9	Extracts password-related information, such as:
		Whether a password is required
		Number of login retries allowed
		`UMASK` value used

`Login Configuration 2`
`PCI_Solaris_LoginConfiguration`
	8.5.9-10	Extracts password-related information, such as:
		Minimum password length
		Minimum time before a password change
		Maximum time a password can be valid

Table 2–4 identifies the three specialized resource specifications and their command resource definitions. There are no complementary dictionaries for these definitions.

Table 2–4 Other Solaris Resource Specifications and Supported Requirements

Resource Specification/ Resource Definition	PCI Rule	Description

`PCI_Solaris_Default_Logins`
`Default Logins`
	2.1	Reports on default logins that should be restricted such as anonymous, guest, and so forth

`PCI_Solaris_UnauthorizedSUIDBinaries`
`Unauthorized SUID Binaries`
	7.1	Reports on programs that are set as `SUID/GUID` root programs

`PCI_Solaris_WorldWritableStickyBitDirs`
`World Writable Sticky Bit Directories`
	7.1	Reports on world-writable directories that do not have the sticky bit set

Chapter 3 shows how to use the supplied resource specifications to create PCI assets.

3

Loading PCI Assets

After installing the PCI Compliance Automation Module, you are ready to load your PCI assets.

3.1 PCI Assets for Windows

Before adding Windows PCI assets, you should create a container tree in the Navigator view that represents the systems you want to validate for compliance.

To add PCI assets for a Windows platform:

1. Right-click the container you set up in the Navigator view and select **Add > Asset** in the popup menu.
2. Type a name for the asset you are adding. (If you don't enter a name, it defaults to the resource specification you select, which may be an appropriate naming convention to use).
3. Click the **Use Resource Specification** radio button if necessary, then select the PCI Windows specification that applies.
4. Select a **Host/Endpoint** and **Authentication Pack** from the respective drop-down lists. These are the values you have defined for the machine that hosts the proxy service.
5. In the **Windows Resource Adapter Settings** tab, identify the **Target Machine**, that is, the host from which to extract the security settings.

   Ignore the rest of the selections in this dialog.
6. Click **OK**.

   A progress indicator appears, after which you should see a confirmation message of success. Close the message and look for the asset under the selected container in the Navigator view.

Repeat the process for each type of PCI asset you want to add.

3.2 PCI Assets for Linux

Before adding Linux PCI assets, you should create a container tree in the Navigator view that represents the systems you want to validate for compliance.

To add PCI assets for a Linux platform:

1. Right-click the container you set up in the Navigator view and select **Add > Asset** in the popup menu.
2. Type a name for the asset you are adding. (If you don’t enter a name, it defaults to the resource specification you select, which may be a suitable naming convention to use).
3. Click the **Use Resource Specification** radio button if necessary, then select the PCI Linux resource specification that applies.
4. Select the **Host/Endpoint** from which you want to extract the security settings.
5. Select the **Authentication Pack** that has the appropriate credentials to access the selected host.

   Ignore the rest of the selections in this dialog.
6. Click **OK**.

   A progress indicator appears, after which you should see a confirmation message of success. Close the message and look for the asset under the selected container in the Navigator view.

Repeat the process for each type of PCI asset you want to add.

3.3 PCI Assets for Solaris

Before adding Solaris PCI assets, you should create a container tree in the Navigator view that represents the systems you want to validate for compliance.

To add PCI assets for a Solaris platform:

1. Right-click the container you set up in the Navigator view and select **Add > Asset** in the popup menu.
2. Type a name for the asset you are adding. (If you don’t enter a name, it defaults to the resource specification you select, which may be a suitable naming convention to use).
3. Click the **Use Resource Specification** radio button if necessary, then select the PCI Solaris resource specification.
4. Select the **Host/Endpoint** from which you want to extract the security settings.
5. Select the **Authentication Pack** that has the appropriate credentials to access the selected host.

   Ignore the rest of the selections in this dialog.
6. Click **OK**.

   A progress indicator appears, after which you should see a confirmation message of success. Close the message and look for the asset under the selected container in the Navigator view.

Repeat the process for each type of PCI asset you want to add.

4

Auditing and PCI Compliance

This chapter describes how to perform and reconcile compliance audits, and how to set up tracking to ensure continued compliance.

4.1 The Audit Process

To check for PCI compliance, you run audits on the assets that were created based on the supplied resource specifications. The purpose of an audit is to determine the degree of compliance of your computing systems vis-a-vis the standards set forth by the Security Standards Council. There are two ways to run audits:

- In the Navigator view, on a single asset
- In Web Reports, on a collection of assets

The first is a method of expedience. It's a convenient way to take a pulse on a particular asset; that is, to get a sense of how close to compliance the configuration is.

Web Reports is the preferred method for a variety of reasons. You can report on multiple assets. It presents the information in a visually pleasing format. You can schedule the audit to run automatically on a recurring basis. You can distribute the output in a variety of formats.

4.1.1 Running Audits In the Navigator View

To run an audit on a PCI asset in the Navigator view:

1. Right-click the asset you want to audit and select **PCI Auditing > Audit Asset**. The PCI icon denotes assets that are auditable.
2. In the confirmation dialog that opens, click **OK** to run the job. Click **Advanced Settings** if you want to enter a comment or schedule job execution for a later time.

   The audit job appears in the Jobs view (lower right portion of the Client window). You may have to click the **Jobs** tab to display the view.
3. When **Completion Status** says audit complete, right-click anywhere in the line and select **Show Details**.

   The Output log denotes success or failure of the audit, and describes the findings as to missing properties and unmatched property values. This record of the audit is available in the Scripting Jobs view until purged as part of regular housekeeping, or deleted by the owner.

4.1.2 Running Audits in Web Reports

Web Reports is Application Configuration Console’s browser-based reporting tool. (A URL to access Web Reports is installed on a Windows host as part of Client installation.) You can access Web Reports from a shortcut on the Client Start menu.

To run an audit on PCI assets in Web Reports:

1. Start up Web Reports. You can use the Client Start menu shortcut or point your browser at the following URL:

   ```
   https://mVserverHost:9943/mvwebreports/index.jsp
   ```

2. On the **Audit** menu, select **PCI Compliance**.
3. Select a **Source** in the report criteria column on the left. The source can be any combination of projects or other containers, or of selected assets. Only assets denoted by the PCI icon are auditable.
4. Click **Generate Report**.

   After a moment, the results of the audit appear in the reporting page.

Notice the legend at the bottom of the last page of a report. The implications are as follows:

- **Passed**–an asset and its configurations are in compliance with the properties and values in the auditing dictionary.
- **Failed**–some or all of an asset's configurations are not in compliance, either because properties in the dictionary are missing from the configuration or there are discrepancies in configuration and dictionary property values.
- **Skipped**–an asset's configuration was not audited because there is no referenced auditing dictionary; an asset that has a mix of passed and skipped configurations is considered to be in compliance.

The report lists configurations within assets that are arranged alphabetically. The last update refers to when external data was last written to Application Configuration Console. This can reflect the initial asset load, a manual update performed within Application Configuration Console, or the result of a tracking event with auto-update. Actual value is the property value in the asset configuration; expected value derives from the auditing dictionary. Path identifies the origin of the property in the external resource. This is useful for resolving like-named properties.

4.2 Reconciling an Audit

You should have no reasonable expectation that your environment is in compliance when you first audit your PCI assets. The task faced by your security experts is to evaluate the results and draw up a plan of redress. When is it prudent to follow the council’s recommendations and when is there an acceptable risk to deviate from those recommendations. Obviously this will be an evolving process, but the clearly defined objective is to eventually establish a baseline at which your operating system security settings reflect your desired level of compliance.

If your security team decides to follow the recommendations to the letter, then the process is straightforward: change your configurations at their source to match the properties and values in the dictionaries.

More likely, though, your team will choose to override or ignore any number of property values in various configurations. Oracle feels that best practice in this case is to preserve the installed environment by making modifications to copies of product dictionaries. In brief, these are the steps you would take:

1. In Application Configuration Console, export the auditing dictionary whose settings you want to customize.
2. Edit the XML file by changing the dictionary name and the definition URI of each property. Rename the file when you save it.
3. Import into Application Configuration Console the renamed version of the auditing dictionary.
4. Open the imported dictionary in the Application Configuration Console Editor area. Delete the properties you want to ignore, and otherwise change property values to the settings you want to validate against.
5. In the associated resource specification, edit the command resource definition metadata to reference the imported auditing dictionary.
6. Add a new asset, based on the revised resource specification and dictionary.
7. Perform an audit on the asset to ensure compliance under the revised standards.

Step 1: Export the Auditing Dictionary

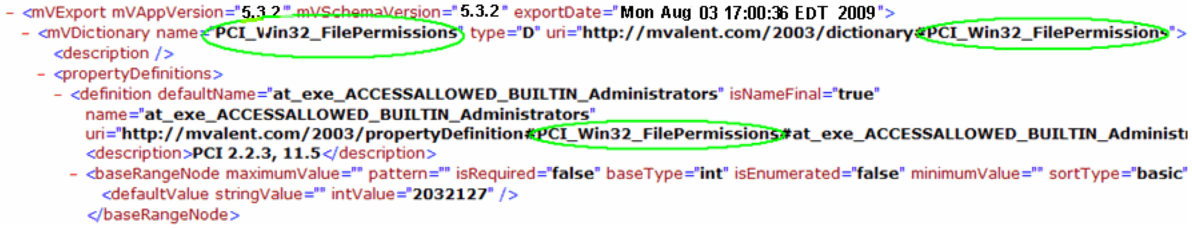
1. In the **Property Dictionaries** folder in the Navigator view, right-click the dictionary you want to customize and select **Export**.
2. Select a **Host/Endpoint** and **Authentication Pack** where you can write the XML file.
3. Click **Browse** to indicate the directory location where you want to write the file.
4. Click **OK** to complete the export operation.

Step 2: Change the Dictionary Name

Edit the exported XML file to change the dictionary name and URI dictionary references:

1. In an XML or a text editor, open the exported dictionary XML file.
2. Change the dictionary name to your custom name in the `mvDictionary name` tag and in the URI value immediately following.
3. Change the dictionary name as specified in the URI value in *each* `definition` tag that appears in the file. Effectively, there is a tag for each property name value pair.
4. Save the file in XML format as the same name of your custom dictionary.

The graphic below illustrates which values (circled in green) to edit:



```
- <mVExport mVAppVersion="5.3.2" mVSchemaVersion="5.3.2" exportDate="Mon Aug 03 17:00:36 EDT 2009">
  - <mVDictionary name="PCI_Win32_FilePermissions" type="D" uri="http://mvalent.com/2003/dictionary#PCI_Win32_FilePermissions">
      <description />
    - <propertyDefinitions>
      - <definition defaultName="at_exe_ACCESSALLOWED_BUILTIN_Administrators" isNameFinal="true"
          name="at_exe_ACCESSALLOWED_BUILTIN_Administrators"
          uri="http://mvalent.com/2003/propertyDefinition#PCI_Win32_FilePermissions#at_exe_ACCESSALLOWED_BUILTIN_Administi
          <description>PCI 2.2.3, 11.5</description>
        - <baseRangeNode maximumValue="" pattern="" isRequired="false" baseType="int" isEnumerated="false" minimumValue="" sortType="basic"
            <defaultValue stringValue="" intValue="2032127" />
          </baseRangeNode>
```

Step 3: Import the Edited Auditing Dictionary

1. Right-click the **Property Dictionaries** folder in the Navigator view and select **Import**.
2. Select the same **Host/Endpoint** and **Authentication Pack** where you exported the auditing dictionary.
3. Click **Browse** to indicate the directory location where you wrote the XML file.
4. Click **OK** to complete the import operation.

Step 4: Edit the Properties in the Custom Dictionary

Customize the contents of your dictionary:

1. In the **Property Dictionaries** folder in the Navigator view, right-click the custom dictionary you imported and select **Open**.
2. In the Editor area, click the **Edit** button.
3. In the **Name** column, select those properties you want to remove. Use Ctrl-Click and Shift-Click to select multiple properties.
4. Click **Delete** to remove the selected properties.
5. Edit individual property values by selecting the property in the **Name** column and changing the **Default Value** for the property on the right.
6. Click **Save** to complete customization of your dictionary.

Note that if you want add new properties to your custom dictionary, as opposed to deleting or changing them, you can do this as well in the Editor area.

Step 5: Edit the Resource Specification Command Definition Metadata

Change the command resource specification to reference the correct dictionary:

1. In the Navigator view under the **Resource Specifications** folder, open the **PCI_AUDIT_AUTOMATION_MODULE** folder.
2. Right-click the appropriate resource specification and select **Open**.
3. In the Editor area, click the **Edit** button.
4. Select the row in the **Command Definitions** section and double-click the value in the **Metadata** column.
5. In the Edit Metadata dialog, click in the dictionary name row. This populates the name and value edit boxes.
6. Change the Value to the custom dictionary name.
7. Click **Apply** to confirm the change; click **OK** to close the dialog.
8. Click **Save** to complete the operation.

Step 6: Add New Assets

Add new assets based on the revised resource specification and dictionary. See Chapter 3 for information on loading assets.

Step 7: Audit New Assets

Audit the new assets you loaded. See Section 4.1, "The Audit Process," at the beginning of this chapter.

4.3 Working with Dictionaries

The property name value pairs in an auditing dictionary drive the auditing process. Metadata on the configuration controls which dictionary to use to perform auditing. The configuration dictionary metadata derives from the value of the `AUDIT_PROPERTY_DICTIONARY_NAME` metadata set in the resource specification command definition. Table 4–1 breaks down the various options with respect to working with dictionaries.

Table 4–1 Product Dictionary Options

Option	Action
Use a custom dictionary to create PCI assets	Change the dictionary metadata in the resource specification command definition to the name of the custom dictionary
Use a custom dictionary to perform an audit of the asset	Change the dictionary metadata in the asset configuration to the name of the custom dictionary
Create PCI assets that ignore certain configurations	Remove or rename the dictionary metadata in the resource specification command definition
Perform an audit of an asset that ignores certain configurations	Remove or rename the dictionary metadata in the asset configuration

Step 5 under "Reconciling an Audit" describes where and how to edit dictionary metadata in a resource specification command definition. The other option referenced in Table 4–1 is to edit dictionary metadata in the asset configuration. Here's how:

1. In the Navigator view, expand the PCI container to expose the appropriate asset view (Resource View, by default).
2. Open the asset configuration whose auditing dictionary you want to edit.
3. In the Editor area, click the **Metadata** tab, then click the **Edit** button.
4. Under User defined, look for `AUDIT_PROPERTY_DICTIONARY_NAME`. Edit the value as appropriate.
5. Click **Save** to complete the operation.

Note: When you rename a dictionary, due diligence dictates that you investigate any configuration flagged as skipped in the audit report, to ensure dictionary names are correct. For example, a typo in the metadata name would cause the configuration to be skipped.

4.4 Compliance Baseline

The winnowing process should eventually yield a set of assets that the security team deems compliant. This is the baseline against which to track for changes that might indicate a security risk or breach.

A likely scenario takes the following approach:

- All PCI assets are organized as part of a single project
- Tracking on PCI assets occurs daily; alerts are e-mailed to the security team
- The PCI audit report runs weekly; the generated report is e-mailed to the security team

- Security team meets as necessary to reconcile detected differences

4.4.1 Tracking PCI Assets

You schedule tracking on asset views. The default is the Resource View.

1. Expand the PCI project in the Navigator view to expose the PCI asset views.
2. Right-click an asset view and select **Open**.
3. In the Editor area, click the **Tracking Schedule** tab at the bottom.
4. Click the **Edit** button and enable tracking for assets.
5. Select all configurations in the asset view.
6. Select all configurations in the asset view.
7. Enter the e-mail address of the security team.
8. For the **Update** option, select **Replace**.
9. Click **Save** to complete the scheduling operation.

> **Note:** The **Replace** update option causes the Application Configuration Console data to be overwritten with the external configuration data whenever tracking detects a difference. In other words, the operating system files are assumed to be correct unless the security team overrules this assumption.

4.4.2 Scheduling PCI Audits

The security team can decide the frequency of PCI auditing. Running the PCI Audit report once a week might be a reasonable starting point. Remember that it can be scheduled to run automatically during off-peak hours.

To schedule the PCI Audit report:

1. Start Web Reports in your browser.
2. On the **Audit** menu, select **PCI Compliance**.
3. In the report criteria column, select the project containing the PCI assets to audit as the **Source**.
4. Click the **Schedule Report** button.
5. Fill in the dialog with appropriate scheduling information.

   For example, you might schedule auditing to be performed on all PCI assets within the selected project at midnight every Sunday, with the resulting report to be e-mailed in PDF format to all members of the security team for their review.
6. Click **OK** to schedule the report.