

Detailed Analysis – Achieving PCI Compliance with SkyView Partners’ Products for AIX

The Payment Card Industry has a published set of Data Security Standards to which organization’s accepting and storing credit card information must comply. Since these Data Security Standards are written in generic terms, one must do some interpretation to determine how the requirements apply to IBM AIX servers.

Using the requirements directly from the Payment Card Industry’s Data Security Standards, the requirements are translated into AIX terminology and a description of how SkyView products assist is provided.

SkyView product description:

[SkyView Policy Minder for AIX](#) is an IBM AIX security compliance tool that compares your systems' current settings against your organization’s security policy requirements. Your policy implementation is documented and non-compliant items are identified. Using the FixIt function, non-compliant items can be set back to match policy settings. Policy Minder automates the process of keeping your AIX servers’ security configuration in compliance with your security policy.

PCI Requirements – Section 2.2.1 and 2.2.3, 2.3, 4.1 and 8.4

- Implement only one primary function per server to prevent functions that require different security levels (2.2.1)
- Configure system security parameters to prevent misuse. (2.2.3)
- Encrypt all non-console administrative access (2.3)
- Use strong cryptography and protocols (4.1)
- Render all password unreadable during transmission

Solution: Use the Daemons category of **Policy Minder** to ensure only those daemons are active that support the intended purpose (role) of the server. You can also use this category to ensure non-encrypted services (such as non-SSL-enabled telnet) are not active and that SSH is in use. This will ensure passwords are encrypted during transmission and admin access is over an encrypted session. Use the Configuration policy category to ensure configuration settings remain configured appropriately. If a daemon is activated or a configuration setting is changed, a compliance check will identify it as non-compliant. Run FixIt to start or stop the daemon to match the policy requirements.

PCI Requirements – Section 2.1 and 6.3.6:

- Always change vendor-supplied defaults before installing a system on the network (2.1)
- Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers. (6.3.6)

Solution: Use **Policy Minder** to check user account configuration settings. Policy Minder can also be used to ensure the configuration settings aren’t changed from your policy requirements during the installation of a vendor package.

PCI Requirements – Section 3.5.2:

- Store encryption keys in the fewest locations possible. (3.5.2)

Solution: Use the Files category of **Policy Minder** to search for files of specific names or file extensions. If a legitimate source for storing encryption keys, use the Files category to ensure the permissions on the file remain set correctly.

PCI Requirements – Section 6.1:

- Ensure patches are up-to-date (6.1)

Solution: Use the Script category of **Policy Minder** to run a script against all servers to ensure they are at the patch level required by your policy.

PCI Requirements – Section 7.1, 7.1.1 and 7.1.2:

- Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: (7.1)
 - Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities (7.1.1)
 - Assignment of privileges is based on individual personnel’s job classification and function (7.1.2)

Solution: **Policy Minder** provides an automated method for the discovery of new user accounts with admin rights or members of groups with admin rights. In addition, the User account category in Policy Minder allows you to define the appropriate attributes for each type of user account – admin, operator, developer, etc. Compliance checks identify the account and its attributes that are out of compliance with the definition. Policy Minder’s FixIt function allows administrators to change the user account attributes to be in compliance with the definition and provides a report of the change.

PCI Requirements – Section 7.2, 7.2.1, 7.2.2 and 7.2.3:

- Establish an access control system for systems components with multiple users that restrict access based on a user’s need to know, and is set to “deny all” unless specifically allowed. This access control system must include the following: (7.2)
 - Coverage of all system components (7.2.1)
 - Assignment of privileges to individuals based on job classification and function (7.2.2)
 - Default “deny-all” setting (7.2.3)

Solution: Use the File category in **Policy Minder** to maintain compliance for the permissions settings on files and directories. Compliance checks will identify the each item out of compliance (that is, with the incorrect permission settings) along with the details of what’s causing the non-

compliance status. Policy Minder's FixIt function can be used by administrators to change the settings to match the requirements and provides a documented record of the change. Use the Configuration policy category to ensure the default umask value is set to 'deny all' or no access.

PCI Requirement – Section 8.5.1:

- Control addition, deletion and modification of user IDs, credentials and other identifier objects.

Solution: Use the Configuration policy category of **Policy Minder** to maintain the default configuration settings for the creation of new user accounts. Use the User account category to ensure user account settings are not overridden from global settings. Finally use the User account category to ensure appropriate configuration of all user accounts on the server. Compliance checks identify changes to accounts and attributes which do not match policy requirements. In addition, FixIt can be used to fix the non-compliant user account attributes or configuration policy settings.

PCI Requirement – Section 8.5.4:

- Immediately revoke access for any terminated users.

Solution: **Policy Minder's** User account category can be used in conjunction with the FixIt function revoke user account access. FixIt produces a report which can be used as proof to your auditor that terminated users' accounts are set so that they cannot be used.

PCI Requirement – Section 8.5.5:

- Remove/disable inactive user accounts at least every 90 days.

Solution: **Policy Minder** can simplify the discovery and automate the removal of inactive accounts. You can use Policy Minder to find and take action on inactive accounts, such as configuring the account so that it can't log in. To simplify the processing of these profiles, you can omit profiles that are an exception – that is, should never have action take on them. This way, the list of profiles only contains those on which action should be taken. When printing this policy, profiles omitted are documented.)

PCI Requirement – Section 8.5.6:

- Enable accounts used by vendors for remote maintenance only during the time period needed.

Solution: The user account category of **Policy Minder** can be configured to examine the status of specific vendor accounts. The FixIt function can be scheduled (using the integrated cron function) to run nightly to set any user account (including vendors) so that it cannot be used for sign on.

PCI Requirements – Section 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, and 8.5.15:

- Change user passwords at least every 90 days (8.5.9)
- Require a minimum password length of at least seven characters (8.5.10)
- Use passwords containing both numeric and alphabetic characters (8.5.11)
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used. (8.5.12)
- Limit repeated access attempts by locking out the user ID after not more than six attempts. (8.5.13)
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal. (8.5.15)

Solution: Use the Configuration policy category of **Policy Minder** to check the password and session time-out system values to ensure they meet these requirements. In addition, use the User account category to examine user account settings to ensure these values have not been overridden in the user account configuration file.

PCI Requirement – Section 11.5

- Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. (11.5)

Solutions: Use the monitoring feature of the File category in Policy Minder to establish a checksum over critical files. Run regular compliance checks to determine whether the files have been changed.

PCI Requirements – Section 12.1, 12.1.1, 12.1.2, 12.1.3:

- Establish, publish, maintain, and disseminate a security policy that accomplishes the following: (12.1)
 - Addresses all PCI DSS requirements. (12.1.1)

Solutions: Use **Policy Minder** to document the AIX implementation of your security policy requirements. Risk acceptance statements can be added to the policy definitions as well as cross-references to specific sections of your organization's security policy. All of these can be printed in PDF format and given to your auditor as documentation of your policy implementation.

PCI Requirement – Section 12.2:

- Develop daily operational security procedures that are consistent with requirements in this specification (12.2)

Solution: Use the integrated cron function of **Policy Minder** to schedule regular compliance checks on a frequency that means your policy and compliance requirements.

These are just some of the ways SkyView Partners' products can reduce the cost and complexities of maintaining your AIX compliance requirements. For more information, please visit the SkyView Partners website at www.skyviewpartners.com.

Who is SkyView Partners? SkyView Partners Inc. is a firm specializing in policy-based security compliance management and assessment software as well as security services for IBM i (AS/400 and iSeries) and AIX customers.