# Sentinel PCI-DSS Solution Pack Quick Start

Released February 1, 2008

The Payment Card Industry Data Security Standard (PCI-DSS) Solution Pack provides an integrated set of Novell™ Sentinel content to address the following 21 requirements:

- 1.1.1: Firewall Configuration Changes
- 1.1.4: Detect Unauthorized Firewall Administration
- 1.4.2: Restrict Access from PCI Systems to the DMZ
- 3.5: Protect Cardholder Data Encryption Keys
- 7.1: Restrict Access to Cardholder Data
- 8.5.1: Control Creation, Deletion, and Modification of User Accounts
- 8.5.3: Change Passwords after First Use
- 8.5.4: Immediately Revoke Access for Terminated Users
- 8.5.5: Remove Inactive User Accounts
- 8.5.8: Prevent Shared Account Usage
- 8.5.9: Enforce Periodic Password Changes
- 8.5.13: Lock Accounts on Repeated Failed Logins
- 10.2.1: Audit User Access to Cardholder Data
- 10.2.2: Audit Administrative Actions
- 10.2.3: Audit Access to Audit Trails
- 10.2.4: Audit Invalid Logical Access Attempts
- 10.2.5: Audit User Authentication
- 10.2.6: Audit Initialization of Audit System
- 10.5.1: Limit Audit Trail Access by Business Need
- 10.5.2: Protect Audit Trail from Unauthorized Changes
- 10.5.5: Alert on Audit Trail Changes

The Solution Pack leverages the guided implementation and testing features of the Solution Manager to provide demonstrable adherence to event-driven and policy-driven requirements.
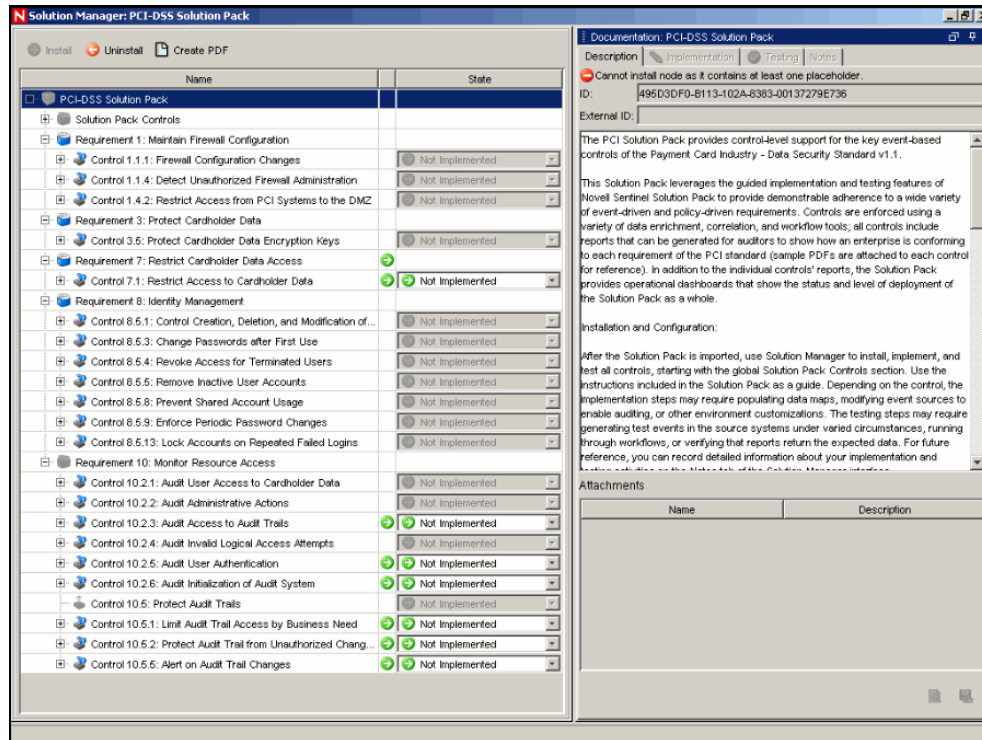
Controls are enforced using a variety of data enrichment, correlation, and workflow tools; all controls include reports that can be generated for auditors to show how an enterprise is conforming to each requirement of the PCI standard. In addition to the individual controls' reports, the Solution Pack provides operational dashboards that show the status and level of deployment of the Solution Pack as a whole, for example:
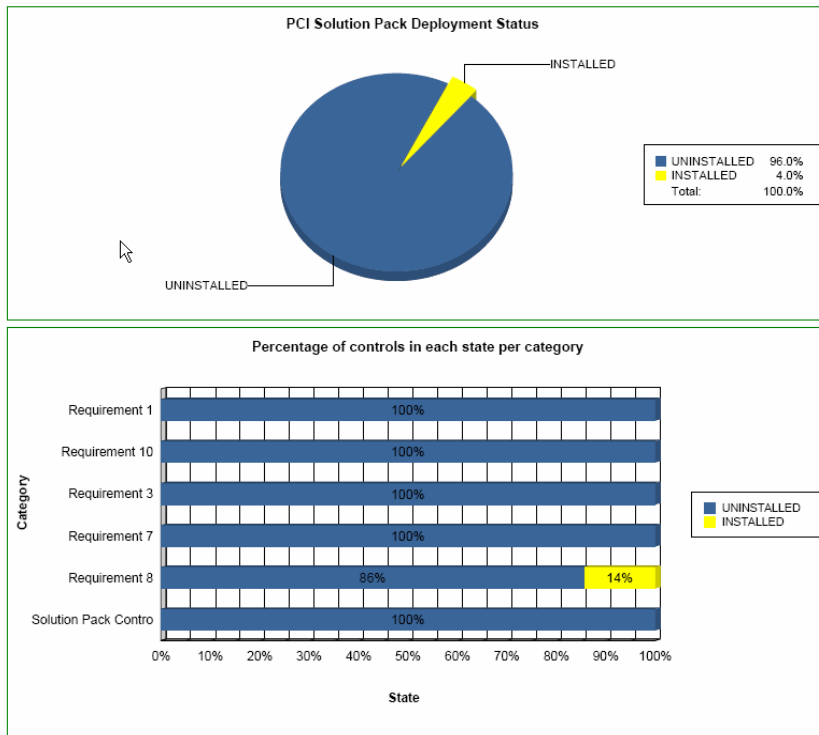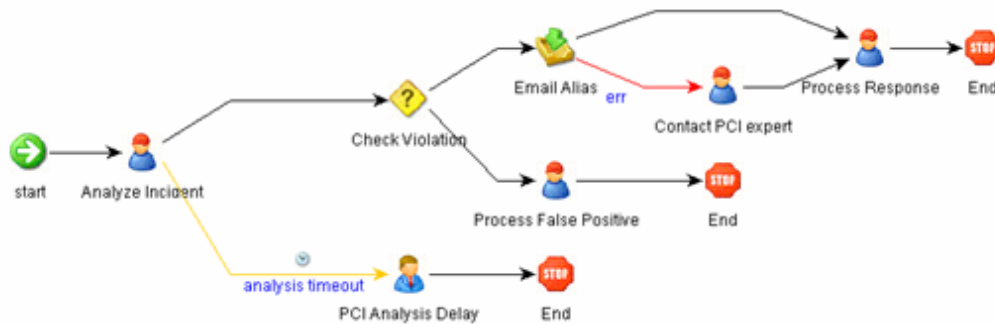

Workflows like the one below define the best-practice response to detected policy violations:

Getting Started

Detailed information about Solution Packs and the PCI-DSS Solution Pack in particular can be found in the Sentinel User's Guide and the documentation packaged with the Solution Pack. Here are some high-level instructions:

1. Apply the Sentinel 6.0 Service Pack 2 and Hotfix 1 to all machines in the Sentinel system.
2. Download and import the Solution Pack into the Sentinel Control Center using the Solution Manager.

   > **NOTE**: You may encounter one of two permissions problems. If you get an access error when you attempt to download the Solution Pack, it is probably because the Novell eLogin you are authenticating with is not associated with the PCI-DSS Solution Pack license. If you cannot see the Solution Manager in the Sentinel Control Center, you may need to request Solution Pack or Solution Manager permissions from your Sentinel Administrator.

3. Review the PCI-DSS Solution Pack documentation. You can download it from the Sentinel Content website or generate it yourself in Solution Manager.
4. Implement the "Global Setup" control under "Solution Pack Controls," which includes a set of preliminary tasks, including setting up collectors and connectors that monitor your PCI systems.
5. Implement and test each control according to the instructions in the Solution Pack, taking notes in the Solution Manager and attesting to the success of the implementation and testing procedures as you go. The implementation procedures may include configurations such as
   - Enabling auditing
   - Registering information related to PCI such as specific user roles, locations for cardholder/encryption key information, or systems in the DMZ
   - Configuring email addresses for notifications
6. Use the reports under "Solution Pack Controls" at any time to get a dashboard view of your enterprise's implementation status.

Additional Information

For the latest version of the PCI-DSS Solution Pack and information about Collector data assumptions, see the Solution Pack tab on the Sentinel Content pages:
http://support.novell.com/products/sentinel/sentinel6.html

For the latest Sentinel platform documentation, including general Solution Pack and ESM information, see the Sentinel documentation website:
http://www.novell.com/documentation/sentinel6

For technical support, contact Novell Technical Support through the Novell Customer Center:
http://www.novell.com/center/?sourceid=suplnav_customercenter

For the Sentinel customer forum, go to http://support.novell.com/forums/