

**BigFix Compliance
PCI Add-on User's Guide**



Special notice

Before using this information and the product it supports, read the information in [Notices \(on page 72\)](#).

Edition notice

This edition applies to version 2.0.1 of BigFix Compliance Analytics and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

- Chapter 1. Overview..... 1**
 - What's new in PCI DSS content update release..... 1
 - PCI DSS overview..... 4
 - PCI DSS checklists..... 5
 - PCI DSS policies..... 8
 - Key users..... 10

- Chapter 2. Setup..... 12**
 - Subscribing to the SCM reporting site..... 12
 - Accessing the PCI DSS Fixlet sites..... 12
 - Configuring endpoints..... 14
 - Filesystem scan configuration..... 19
 - Setting up the PCI DSS Policy Reports for BigFix Compliance Analytics V1.9 and later..... 19
 - Disabling the PCI DSS Policy Reports..... 21
 - Setting up custom reporting for BigFix Compliance Analytics V1.8 and earlier..... 22
 - Installing the Requirements and Milestones reports manually..... 22
 - Updating the Requirements and Milestones reports manually..... 24
 - Installing the Requirements and Milestones reports with the import_milestones.sh script..... 25
 - Updating the Requirements and Milestones reports with the import_milestones.sh script..... 26

- Chapter 3. Using checks and checklists..... 28**
 - Viewing check Fixlets from the HCL BigFix console..... 28
 - Viewing checks from BigFix Compliance Analytics..... 29

Creating custom checklists.....	29
Modifying check parameters.....	31
Remediating configuration settings.....	32
Chapter 4. Understanding the results in BigFix Compliance Analytics.....	34
Starting BigFix Compliance Analytics.....	34
Importing data to BigFix Compliance Analytics.....	35
Viewing reports from BigFix Compliance Analytics.....	37
Viewing PCI DSS compliance results.....	38
Viewing reports on BigFix Compliance Analytics V1.9 and later.....	39
Viewing custom reporting on BigFix Compliance Analytics V1.8 and earlier.....	52
Creating exceptions.....	69
Chapter 5. Resources.....	71
Notices.....	72

Chapter 1. Overview

HCL BigFix Compliance PCI Add-on is a new chargeable component that provides security configuration checklists that are based on the Payment Card Industry Data Security Standard (PCI DSS). These compliance checks are designed to help ensure continuous compliance at every endpoint in your organization.

This PCI component uses the Security Configuration Management (SCM), which is a module under BigFix Compliance. SCM provides a comprehensive library of technical controls to detect and enforce security configurations for endpoints and servers in your organization. By using BigFix Compliance, you have instant visibility into the configurations of systems within a globally distributed infrastructure.

SCM includes a web interface, BigFix Compliance Analytics (formerly known as Security and Compliance Analytics, or SCA), which summarizes and analyzes large data streams and shows the health of your IT assets. BigFix Compliance Analytics provides report views and tools for managing the vulnerability that is found by the BigFix Compliance checks. These compliance reporting tools and views help you to identify configuration issues, which consequently enforce constant policy compliance.

These technical controls and reporting tools are based on industry best practices and standards for endpoints and server security configuration.

What's new in PCI DSS content update release


HCL BigFix Compliance PCI Add-on provides additional support and enhancement in the recent update.


For a detailed list of releases, see the [PCI DSS Release Notes](#).

PCI DSS Policy Reporting

The new PCI DSS Policy reporting, which is available in BigFix Compliance Analytics V1.9, identifies the level of compliance for each system within an entire organization based on a specific PCI DSS requirement or PCI DSS milestone. It also provides a report which shows

an aggregated view of compliance data across all PCI DSS checklists. To view the available policy reporting, see [PCI DSS policies \(on page 8\)](#).

 **Note:** BigFix Compliance PCI Add-on provides the **PCI DSS Reporting** site to allow you to use the Policy feature in BigFix Compliance Analytics V1.9. This site contains the metadata file required for creating the PCI DSS Requirements and Milestones based reports.

 **Important:** You must complete a few other prerequisites before you can use the PCI DSS Policy reporting. For more information, see [Setting up the PCI DSS Policy Reports for BigFix Compliance Analytics V1.9 and later \(on page 19\)](#).

The PCI DSS Policy reporting enables the following users to prepare and manage compliance for PCI DSS:

- Compliance Managers can generate reports from a requirements perspective to prepare for the audit report in accordance with the guidelines provided by the PCI Security Standards Council.
- Compliance Managers and organizations can use the milestone report views during early PCI DSS adoption to understand compliance posture and prioritize actions.
- IT Managers can map the compliance data to specific computers and assign corresponding personnel to remediate non-compliant checks.

Additional operating system support

BigFix Compliance PCI Add-on continues to expand its support coverage. The following operating systems have been recently supported:

Windows Server 2016

The PCI DSS Checklist for Windows 2016 is based on the guidance provided by the Payment Card Industry Data Security Standard (PCI DSS) v3.2 and contains security configuration checks that evaluate the security settings of your Windows Server 2016 endpoints according to PCI DSS.

Some of the checks allow you to use the parameterized setting to enable customization for compliance evaluation.

Some of the checks also support remediation that allows BigFix operators to efficiently remediate a non-compliance issue with a single action.

Solaris 10 and Solaris 11

The PCI DSS Checklist for Solaris 10 and PCI DSS Checklist for Solaris 11 are based on the guidance provided by the Payment Card Industry Data Security Standard (PCI DSS) v3.2 and contains security configuration checks that evaluate the security settings of your Solaris endpoints according to PCI DSS.

Some of the checks allow you to use the parameterized setting to enable customization for compliance evaluation. Note that parameterization requires the creation of a custom site.

Some of the checks also support remediation that allows BigFix operators to efficiently remediate a non-compliance issue with a single action.

CentOS 6 and CentOS 7

Checks for CentOS 6 are now supported in the PCI DSS Checklist for RHEL 6, while checks for CentOS 7 are now supported in the PCI DSS Checklist for RHEL 7. The checks are based on the existing RHEL 6 and RHEL 7 checks.

If you have not enabled the PCI DSS Checklist for RHEL 6 site or the PCI DSS Checklist for RHEL 7 site before, you can find them listed in the **License Overview** dashboard as PCI DSS Checklist for RHEL 6, CentOS 6 and PCI DSS Checklist for RHEL 7, CentOS 7. If the sites are already enabled, they are referred to as PCI DSS Checklist for RHEL 6 and PCI DSS Checklist for RHEL 7. Despite the name, the sites support checks for both RHEL and CentOS.

AIX 6.1

The PCI DSS Checklist for AIX 6 is based on the guidance provided by the Payment Card Industry Data Security Standard (PCI DSS) v3.2 and contains security configuration checks that evaluate the security settings of your AIX 6.1 endpoints according to PCI DSS.

Some of the AIX 6 checks allow you to use the parameterized setting to enable customization for compliance evaluation. Note that parameterization requires the creation of a custom site.

The AIX 6 checks do not provide actions that you can take to automatically remediate non-compliant settings on endpoints. However, manual remediation steps are made available in the Fixlet description.

AIX 7.2

The PCI DSS Checklist for AIX 7 is based on the guidance provided by the Payment Card Industry Data Security Standard (PCI DSS) v3.2 and contains security configuration checks that evaluate the security settings of your AIX 7.2 endpoints according to PCI DSS.

Some of the AIX 7 checks allow you to use the parameterized setting to enable customization for compliance evaluation. Note that parameterization requires the creation of a custom site.

The AIX 7 checks do not provide actions that you can take to automatically remediate non-compliant settings on endpoints. However, manual remediation steps are made available in the Fixlet description.

Remediation support for Windows 10, Windows 7, Windows 2012, Windows 2008, and AIX 7

The sites for these operating systems are updated to include more checks with remediation support, allowing BigFix operators to efficiently remediate a non-compliance issue with a single action.

PCI DSS overview

HCL BigFix Compliance PCI Add-on provides checklists for PCI compliance. The Payment Card Industry Data Security Standard (PCI DSS) is a baseline of technical and organizational requirements that are related to the Payment Card Industry.

The PCI DSS states that you must establish a secure payments environment throughout your organization to achieve compliance. BigFix Compliance enforces security configurations for endpoints and servers in your organization. It can help your organization protect endpoints and assure assessors or regulators that you are meeting security compliance for PCI DSS.

By complying with the PCI DSS standards you ensure that cardholder data and sensitive authentication data are secure and well-protected from malicious users and attacks.

The PCI DSS applies to all entities involved in payment card processing and requires continuous compliance with the security standards and best practices set by the PCI Security Standards Council. For more information about PCI DSS, see the [PCI Security Standards Council](#) website.


When endpoints are protected, all entities that are involved in payment card processing are secure.

PCI DSS checklists


SCM is organized through checklists that assess and manage the endpoint and server configurations. Each compliance checklist is distributed by BigFix as an external Fixlet site.

SCM provides a large number of checklists to report compliance and remediate endpoint security configurations based on industry best practices, such as Center of Internet Security (CIS) and Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG). HCL BigFix Compliance also provides security configuration checklists for Payment Card Industry Data Security Standard (PCI DSS) compliance.

Each PCI DSS checklist contains technical checks that are based on the PCI standard. For details on PCI standard, see [PCI DSS Requirements and Security Assessment Procedures](#).

 **Note:** The checks that are specific to PCI DSS Requirements and Security Assessment Procedures v3.2 are considered as best practices until they become mandatory in 2018. You can exclude those checks from the compliance report using the standard exception mechanism available in BigFix Compliance Analytics (formerly known as SCA). For more information, see [Creating exceptions \(on page 69\)](#).



These technical checks assess security policies and configurations on each endpoint, provide remediation steps to fix vulnerabilities, and provide reporting capabilities. Compliance data can be explored from the reports that provide the requirements perspective or the prioritized approach. For BigFix Compliance Analytics V1.9 or later, see [Viewing the Policy View List report \(on page 41\)](#). For BigFix Compliance Analytics V1.8 or earlier, see [Viewing custom reports \(on page 52\)](#).

 **Note:** PCI DSS requirements 9, 11, and 12, which are process-oriented in nature, are not covered in SCM.


Each PCI DSS checklist targets a specific type of operating system or middleware, and is composed of a collection of checks that get evaluated on the endpoints.

The following PCI DSS checklists are available:

Table 1. Available PCI DSS Checklists

Checklist Name	Supported Operating Systems and Servers
PCI DSS Checklist for AIX 6	AIX 6.1
PCI DSS Checklist for AIX 7	AIX V7.1, V7.2
PCI DSS Checklist for MS IIS 7	Microsoft IIS 7
PCI DSS Checklist for MS SQL 2008	Microsoft SQL Server 2008
PCI DSS Checklist for MS SQL 2012	Microsoft SQL Server 2012
PCI DSS Checklist for RHEL 5	Red Hat Enterprise Linux 5
PCI DSS Checklist for RHEL 6, CentOS 6	Red Hat Enterprise Linux 6
 Note: If this site is not enabled, it is displayed in the License Overview dashboard as PCI DSS Checklist for RHEL 6, CentOS 6. Otherwise, it is listed as PCI DSS Checklist for RHEL 6, but supports both RHEL 6 and CentOS 6.	CentOS 6
PCI DSS Checklist for RHEL 7, CentOS 7	Red Hat Enterprise Linux 7
 Note: If this site is not enabled, it is displayed in the License Overview	CentOS 7

Checklist Name	Supported Operating Systems and Servers
dashboard as PCI DSS Checklist for RHEL 7, CentOS 7. Otherwise, it is listed as PCI DSS Checklist for RHEL 7, but supports both RHEL 7 and CentOS 7.	
PCI DSS Checklist for Solaris 10	Solaris 10
PCI DSS Checklist for Solaris 11	Solaris 11
PCI DSS Checklist for Windows 7	Microsoft Windows 7
PCI DSS Checklist for Windows 10	Microsoft Windows 10 Enterprise (V10.0.10586 and V10.0.14393)
PCI DSS Checklist for Windows 2008	Microsoft Windows Server2008 Microsoft Windows Server 2008 R2
PCI DSS Checklist for Windows 2012	Microsoft Windows Server2012 Microsoft Windows Server 2012 R2
PCI DSS Checklist for Windows 2016	Microsoft Windows Server 2016
PCI DSS Checklist for Windows Embedded Standard 7	Microsoft Windows Embedded Standard 7
PCI DSS Checklist for Windows Embedded POSReady 7	Microsoft Windows Embedded POSReady 7
PCI DSS Checklist for Windows Embedded POSReady 2009	Microsoft Windows Embedded POSReady 2009

 **Note:** The Linux support is exclusively for Red Hat Enterprise Linux and CentOS Linux operating systems. It does not include add-ons or middleware such as JBoss and Apache.

PCI DSS checklist content

You can access a checklist by subscribing to the external Fixlet sites that are provided by SCM. A single site can contain checks for multiple requirements.

Each site contains a set of Fixlets and Analyses, where Fixlets or checks correspond to a specific configuration setting in accordance with the PCI DSS requirements. A Fixlet evaluates a system setting against a specific policy value and displays the compliance state of an endpoint. An analysis is associated to each Fixlet that retrieves the actual state of each configuration item on an endpoint.

Most of the Fixlets have a parameterized setting to enable customization for compliance evaluation.

Each Fixlet contains instructions on how to manually remediate a non-compliant endpoint. These steps can be found in the **Description** tab. Some of these Fixlets provide actions that you can take to automatically remediate non-compliant settings on endpoints. For more information about remediation support, see the [PCI DSS Release Notes](#).

The compliance status of each PCI DSS check and checklist is calculated by Security and Compliance Analytics (SCA), which is now known as BigFix Compliance Analytics, during a periodic Extract Transform and Load (ETL) process. Some checklists require you to run the **Environment Setup Task**. For more information, see [Configuring endpoints \(on page 14\)](#).

PCI DSS policies

BigFix Compliance Analytics V1.9 releases a new policy reporting capability, which provides an aggregated view of compliance from a PCI DSS Requirement or PCI DSS Milestone report perspective.


To view the policies, click **Reports > Policies**.

Table 2. Available PCI DSS policies

Policy Report Name	Description
PCI DSS Milestones View	<p>The PCI DSS Milestones View contains checklists that are based on the PCI DSS Milestone. It retrieves compliance data results from the endpoints that are subscribed to the custom copy of the PCI DSS external sites and displays the aggregated data in a single view.</p> <p>This reporting view can help identify the level of compliance for each system within an entire organization based on the PCI DSS milestones.</p> <p>This view is based on the Prioritized Approach for PCI DSS document and can be useful for early PCI DSS adoption or prioritization of remediation actions. Compliance Managers</p>

Policy Report Name	Description
PCI DSS Requirements View	<p>and organizations can run an early assessment, such as the beginning of the PCI DSS implementation, on the remediation actions that they would need to take on noncompliance high risk systems.</p> <p>This view also allows IT Managers to map compliance data to specific computers and assign corresponding personnel to run remediation actions on a system with non-compliant checks. They also use this reporting view to help them decide on the work prioritization for IT operators.</p> <p>You must enable the PCI DSS Reporting site from the License Overview dashboard in the BigFix console to use this policy view.</p>
PCI DSS Checklists	<p>The PCI DSS Requirements View contains checklists that are based on each PCI DSS Requirement. It retrieves compliance data results from the endpoints that are subscribed to the custom copy of the PCI DSS external sites and displays the aggregated data in a single view.</p> <p>This reporting view can help identify the level of compliance for each system within an entire organization based on the PCI DSS requirement. This view is based on the Requirements and Security Assessment Procedures document and can be useful for Compliance Managers in preparing for an audit.</p> <p>You must enable the PCI DSS Reporting site from the License Overview dashboard in the BigFix console to use this policy view.</p> <p>The PCI DSS Checklists view contains custom PCI DSS checklists only. It retrieves compliance data results from the endpoints that are subscribed to the custom copy of the PCI DSS external sites and displays the aggregated data in a single view.</p>

Policy Report Name	Description
SCM Checklists	<p>This reporting view can help Compliance Managers identify the level of compliance for each system within an entire organization based on the overall PCI DSS checklist. It can help also IT Managers to map compliance data to specific computers and assign corresponding personnel to run remediation actions on a system with non-compliant checks.</p> <p>You must enable the PCI DSS Reporting site from the License Overview dashboard in the BigFix console to use this policy view.</p> <p>The SCM Checklists view contains all SCM checklists, including the out-of-the-box checklists for PCI DSS. This reporting view shows the compliance results of the endpoints that are subscribed to the PCI DSS external sites and non-PCI DSS related external and custom sites.</p> <p>This reporting view is available to allow users, who do not have license to the BigFix Compliance PCI Add-on offering, to use the Policy feature in BigFix Compliance version 1.9. Therefore, it is not dependent on the PCI DSS Reporting site.</p>

 **Note:** The source documents for the PCI DSS Requirement and Milestone Policy Views are made available by the PCI Security Standards Council and can be accessed from the *PCI Security Standard Council Document Library* at https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss.


Sample reports can be found in [Viewing reports on BigFix Compliance Analytics V1.9 and later \(on page 39\)](#).

Key users

Learn how users use the PCI DSS checklists for their role.


IT Managers, who commonly take the role of a BigFix Console Operator, focus on the detailed day-to-day configuration management of all systems to use detailed information for each endpoint. They are expected to run remediation actions on endpoints. They use the PCI DSS checklists to enforce security policies and document the current state of compliance against corporate policies. They also use the PCI DSS Milestones Reporting view to help them decide on the work prioritization for IT operators.

Compliance Managers use the PCI DSS reporting when preparing for audit reports. The reports can be generated based on a PCI DSS template that covers requirements or milestones, and can help in assessing the actions needed to resolve a non-compliance check.

 **Note:** If concerns regarding separation of duties arise, use BigFix version 9.2 or later where access control for actions is allowed.

Chapter 2. Setup

Complete configuration steps to access the PCI DSS checklists and checks and ensure accurate relevance evaluation on the endpoints.

 **Note:** BigFix for Security and Compliance Analytics (SCA) is now called BigFix Compliance Analytics. The listed resources have yet to be rebranded.

This guide assumes that you have installed and configured Security Management Configuration (SCM) successfully. You can access the PCI DSS checklists only after that step is completed and if you have a license for BigFix Compliance PCI Add-on.

This guide does not describe the installation and configuration steps for BigFix nor for BigFix Compliance Analytics. For a list of documentation on SCM and BigFix Compliance Analytics, see [Resources \(on page 71\)](#).

Subscribing to the SCM reporting site

To fully use the reporting functions in the BigFix Compliance Analytics, you must subscribe to the SCM reporting site.

1. From the BigFix console, go to the **BigFix Management** and click **License Overview**.
The dashboard opens.
2. Scroll down to the **Security and Compliance** section and enable the **SCM Reporting** site.
3. Click **SCM Reporting** from the navigation tree.
4. From the **Computer Subscriptions** tab, change the value from **No computers** to **All computers** then select **Save Changes**.

Accessing the PCI DSS Fixlet sites

Before you can access the security configuration checklists that are related to PCI DSS, you must acquire the sites and accept the license agreement. After you acquire the site,

you must gather the contents of the site to your console. You must also subscribe your computers to the site so that they can access the PCI DSS content.

If you have enabled any of the PCI DSS beta sites in your environment, you must first remove them to avoid any conflicting issues with the production sites. If you fail to do so, the content in the production sites will fail.

You can access the PCI DSS sites only if you have a valid license for the HCL BigFix Compliance PCI Add-on component. For details about getting a license, contact [HCL Software Support](#).

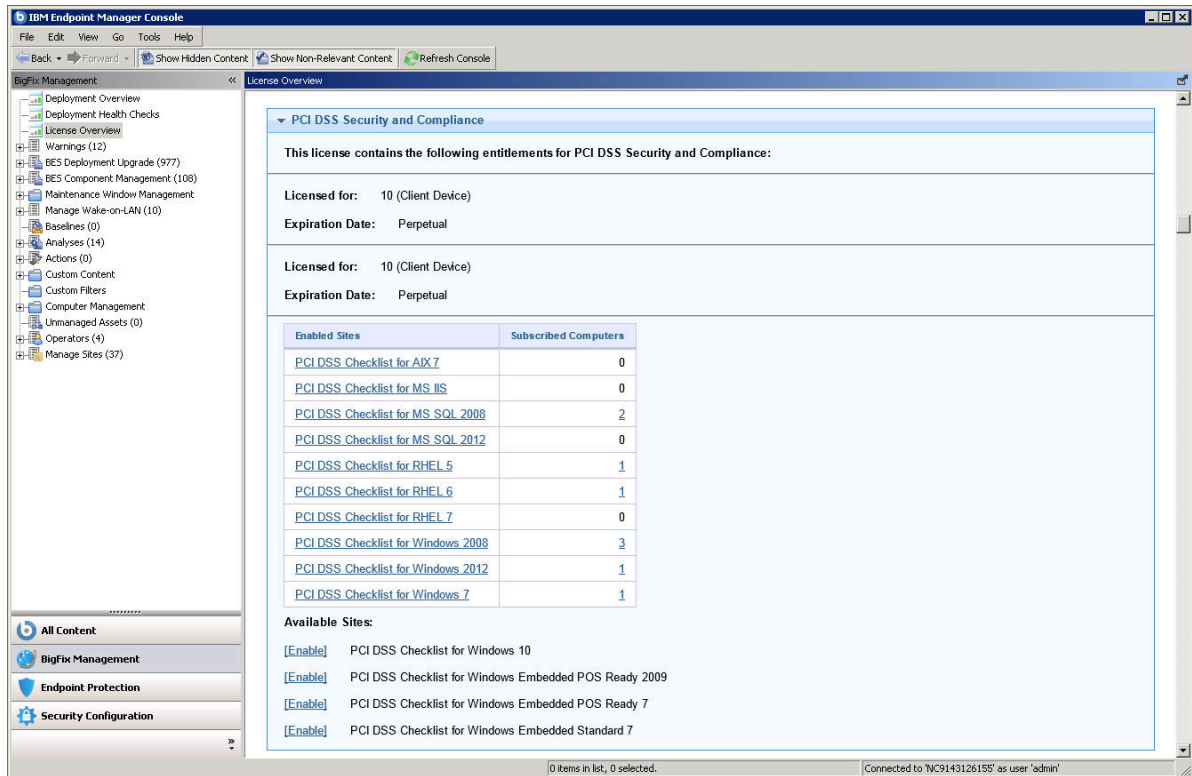
The procedure for acquiring the PCI DSS sites and gathering the contents of the site is similar to the procedure for other BigFix applications and sites. You can subscribe to a PCI DSS site by using the License Overview Dashboard from the BigFix Management domain only if you have purchased the license.

1. From the BigFix console, go to the **BigFix Management** domain and click **License Overview**.
2. Scroll down to the **PCI DSS Security and Compliance** section of the **License Overview** dashboard.


 **Note:** The **PCI DSS Security and Compliance** section will only be visible if you have purchased the license.

3. Click **Enable** beside the PCI DSS sites that you want to your computers to subscribe to. The site is added as an external site in the HCL BigFix Console. It typically takes a few minutes for the contents to become available on your system.

Figure 1. License Overview dashboard




4. Go to the **Security Configuration** domain.
5. Click **All Security Configuration > Sites > External Sites**, and then click the added site.
6. Click the **Computer Subscriptions** tab to subscribe the computers to a site.

 **Note:** Limit the access to the site to only the computers that you want to be able to use the PCI DSS checklists.

Configuring endpoints

Some checklists require you to run the **Environment Setup Task** to populate the necessary properties on the endpoints to enable relevance evaluation. Run this task when it shows as relevant and refresh the results on the endpoint.

 **Note:** You only need to complete this additional prerequisite task if you are using the PCI DSS Checklist for AIX 7 or the PCI DSS Checklist for AIX 6 site.

If Trusted Execution (TE) is implemented in AIX systems, the **Environment Setup Task** is not able to run the scripts from the Fixlets as designed, which would then cause relevance issues. To avoid such issues, provide the following paths in the Trusted Execution Path list during TEP enablement:

```
/var/opt/BESClient/___BESData/<siteName>/SCM/AIX/71
/var/opt/BESClient/___BESData/<siteName>/SCM/AIX/util
/var/opt/BESClient/___BESData/<siteName>/SCM
```


where *<siteName>* is the name of the site that is used in your environment.

For external sites, the name used in the path is identical to the site name. For example, `/var/opt/BESClient/___BESData/PCI DSS Checklist for AIX 7/SCM/AIX/71`.


For custom sites, the spaces in the name are replaced with underscores and the `CustomSite_` prefix is added. For example, `/var/opt/BESClient/___BESData/CustomSite_Checklist_for_AIX_7/SCM/AIX/71`.

You must run the **Environment Setup Task** if you are using any of the following sites or checklists:

- PCI DSS Checklist for AIX 6
- PCI DSS Checklist for AIX 7
- PCI DSS Checklist for MS IIS 7
- PCI DSS Checklist for MS SQL 2008
- PCI DSS Checklist for MS SQL 2012
- PCI DSS Checklist for RHEL 5
- PCI DSS Checklist for RHEL 6

 **Note:** This site supports CentOS 6. If this site is not enabled, it is displayed in the **License Overview** dashboard as PCI DSS Checklist for RHEL, CentOS 6. If the site is enabled, it is listed as PCI DSS Checklist for RHEL 6, but supports both RHEL 6 and CentOS 6.

- PCI DSS Checklist for RHEL 7

 **Note:** If this site is not enabled, it is displayed in the License Overview dashboard as PCI DSS Checklist for RHEL 7, CentOS 7. Otherwise, it is listed as PCI DSS Checklist for RHEL 7, but supports both RHEL 7 and CentOS 7.

- PCI DSS Checklist for Solaris 10
- PCI DSS Checklist for Solaris 11

 **Note:** You do not need to complete this task if you are not using any of these checklists.

The check Fixlets from these sites will only show the current results when the **Environment Setup Task** completes.

Schedule periodic execution of the **Environment Setup Task** if you are using any of the mixed content sites.

1. From the **Security Configuration** domain, click **All Security Configuration > Sites > External Sites**.
2. Select a checklist, and click **Fixlets and Tasks**.
3. In the List panel, locate and click **Environment Setup Task**.

Figure 2. Environment Setup Task in the PCI DSS Checklist for MS IIS 7 site

The screenshot shows the BigFix console interface. At the top, there is a table titled 'Fixlets and Tasks' with columns for ID, Source ID, Site, and Name. The table lists several PCI DSS Checklist for RHEL 7 items and an 'Environment Setup Task'. The 'Environment Setup Task' is selected, and its details are shown in a pane below. The details pane has tabs for 'Description', 'Details', 'Applicable Computers (0)', and 'Action History (0)'. The 'Description' tab is active, showing the task's purpose, category, and a note. Below the description is an 'Actions' section with a link to deploy the task.

ID	Source ID	Site	Name
72		PCI DSS Checklist for RHEL 7	Applicability Fixlet - PCI-DSS - RHEL7
131054279		PCI DSS Checklist for RHEL 7	Environment Setup Task
181146472	pcidss-1.4.b_1.6	PCI DSS Checklist for RHEL 7	Verify that Source Routed Packet Acceptance is disabled - RedHat 7
181147472	pcidss-1.4.b_2.6	PCI DSS Checklist for RHEL 7	Verify that ICMP Redirect Acceptance is disabled - RedHat 7
181148472	pcidss-1.4.b_3.6	PCI DSS Checklist for RHEL 7	Verify that Secure ICMP Redirect Acceptance is disabled - RedHat 7
181149472	pcidss-1.4.b_4.6	PCI DSS Checklist for RHEL 7	Verify that "firewall" is set to Enable - RedHat 7
1001064	pcidss-10.1_6	PCI DSS Checklist for RHEL 7	Verify to Keep All Auditing Information - RedHat 7

Task: Environment Setup Task

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (0) | Action History (0)

Description

Environment Setup Task

Category:
Environment Setup Task

Description:
This task populates the necessary properties on the endpoints to enable relevance evaluation. It runs the detect scripts from the Fixlets, if any, and generates the result files, which are then used in evaluating the relevance for both a Fixlet and Analysis.

You must run this task periodically to gather the latest content.

Note: This task is responsible for updating the reports in Security and Compliance Analytics with the latest information. To ensure that you get the latest content, run this task on the endpoint before running an import.

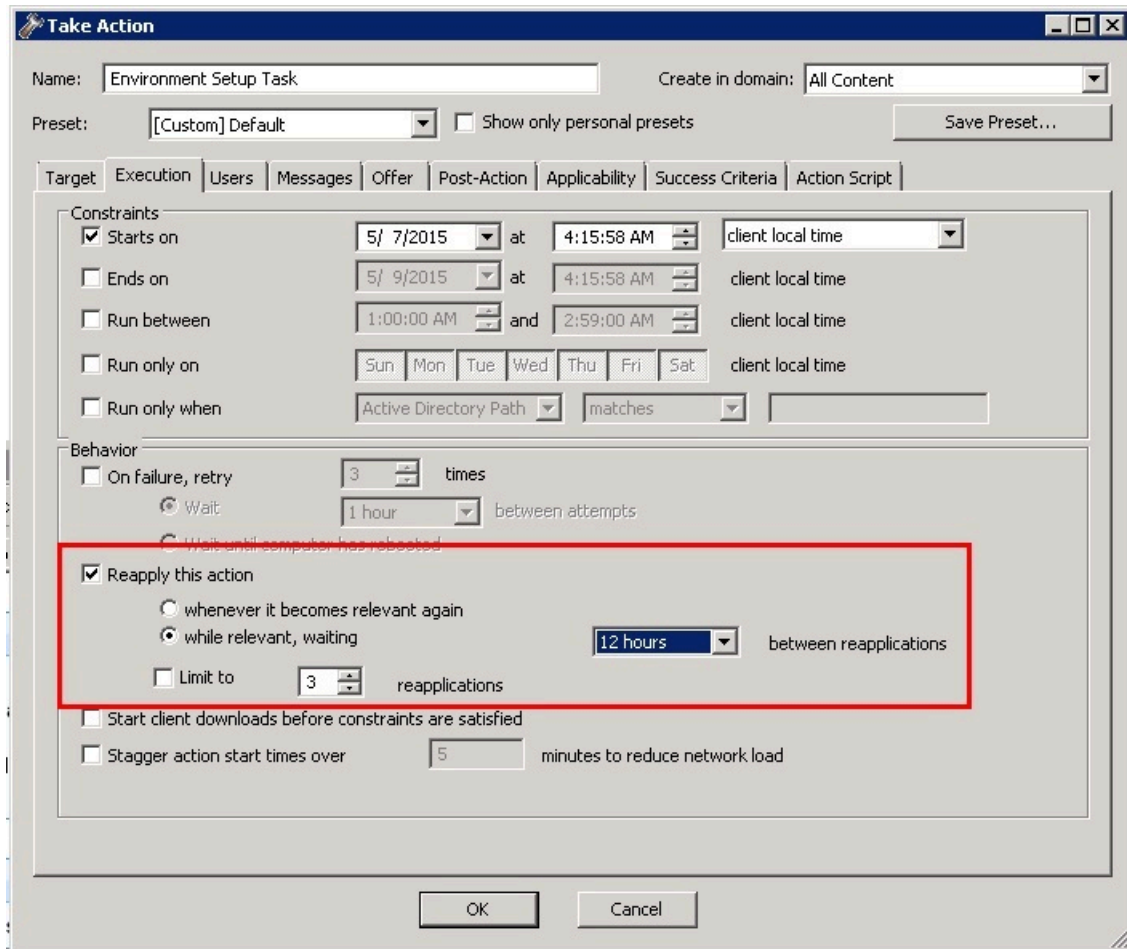
Build ID: SCM-PCI-DSS-Rhel7-1.1.0.0-20151014-014102

Actions

- Click [here](#) to deploy this action.

4. Click **Take Action** to deploy the task. You can also click the appropriate link in the Actions box.
5. Select the appropriate endpoints in your environment.
6. Click the **Execution** tab.

Figure 3. Take Action - Execution tab



7. Set the environment task to run daily and click **OK**.

8. When the task completes, refresh the endpoints.

The **Environment Setup Task** also updates the reports in the Security and Compliance Analytics console (now known as BigFix Compliance Analytics) with the latest results. To ensure that you get the latest content, run this task on the endpoint before running an import. For automatic, daily import to BigFix Compliance Analytics, there is no need to schedule more than one run of the **Environment Setup Task** action.


Filesystem scan configuration

If you are using the PCI DSS checklist for AIX 7 or AIX 6, you can further configure the range of filesystems and directories to be included in the property file used for relevance evaluation.

Some of the AIX Fixlets verify attributes and ownership of various subsets of files on local drives, including the property file that is created by the **Environment Setup Task**. This property file denotes the list of files that are used by the Fixlets in the checklist for AIX. It contains a list of all local and regular files with the exclusion of remote filesystems and special filesystems such as `/tmp` or `/dev`.

BigFix provides the `globalfind` feature to help prevent multiple scanning of local filesystems, which in turn provides better performance results.

You can set the parameters for the `globalfind` feature from **Configure Filesystem Scan Options** to indicate the mount points, directories, or filesystems that are not to be included in the property file. For example, you can specify to skip the data partitions that have too many files.

 **Note:** The parameter changes will only take effect after the next Environment Setup Task run.

Setting up the PCI DSS Policy Reports for BigFix Compliance Analytics V1.9 and later


BigFix Compliance Analytics version 1.9 provides PCI DSS Policy reports that contain aggregated data across checklists, which identifies the level of compliance for a specific PCI DSS requirement or milestone. To generate the policy reports, complete the required setup.

You must configure both the BigFix console and BigFix Compliance Analytics to view the following PCI DSS Policy Reports:

- PCI DSS Milestones View

- PCI DSS Requirements View
- PCI DSS Checklists

These reports retrieve compliance data results from custom sites, not from the external sites. To ensure a complete report of your deployment in the listed reports, configure custom sites for each PCI DSS external site containing the checks. This rule does not apply to the PCI DSS Reporting site.

 **Note:** Endpoints that are subscribed to the PCI DSS external sites are shown in the SCM Checklists policy report. The configuration steps discussed in this section do not apply to the SCM Checklists policy report.


If there are several custom copies of a PCI DSS external site, an endpoint must be subscribed to only a single instance of the custom site. For example, if PCI DSS Checklist for RHEL 5 has two custom sites named RHEL 6-Custom1 and RHEL 6-Custom2, you must subscribe the endpoints to either RHEL 6-Custom1 or RHEL 6-Custom2 at a single time. If the endpoints are subscribed to both custom sites, ETL will fail during import. A sample message for the failure is as follows:

```
Duplicate Check Result(s) detected, you have fixlets with the same scm-id
that
belong to two different sites (external and custom site), you need to
unsubscribe
from external site and re-run Import.
```

In such cases, consider using BigFix Compliance Analytics V1.8 and removing the PCI DSS Policies Reports as described in [Disabling the PCI DSS Policy Reports \(on page 21\)](#).

1. From the BigFix console, create a custom site for each external PCI DSS checklist and subscribe endpoints to it.

You can use the **Create Custom Checklist** dashboard from the SCM Reporting site to create custom copies of the checklists. For more information, see [Creating custom checklists \(on page 29\)](#).

 **Important:** You can only use one custom copy of the PCI DSS external site. Do not subscribe the endpoints to the external sites because the results are not covered in the reporting.

2. From the BigFix console, enable the **PCI DSS Reporting** site.
 - a. Go to the **BigFix Management** and click **License Overview** . The dashboard opens.
 - b. Scroll down the dashboard and find the **Security and Compliance** section, and enable the **PCI DSS Reporting** site.
 - c. Click **PCI DSS Reporting** from the navigation tree.

The **PCI DSS Reporting** site contains the metadata file that is needed to create policies in BigFix Compliance Analytics version 1.9. You do not need to set the computer subscriptions for this site.

3. Configure the API connection from BigFix Compliance Analytics.

For more information about creating a data source, see [Adding a data source](#).

Disabling the PCI DSS Policy Reports

If for any reason you decide not to use the PCI DSS Policy reporting after completing the configuration, you can still disable the reporting with a few steps.

To disable the generation of PCI DSS Policy Reports in BigFix Compliance Analytics V1.9, complete the following steps.

1. Disable the **PCI DSS Reporting** site from the BigFix console.

Do the following steps:

- a. Go to the **Security Configuration** domain.
- b. Click **All Security Configuration > Sites > External Sites**, and then click the **PCI DSS Reporting** site to open it.

 **Note:** You can also open the **PCI DSS Reporting** site from the **License Overview** dashboard.

c. From the Work Area Tool bar, click **Remove**.

2. Run a data import from the BigFix Compliance Analytics console.

For more information, see [Importing data to BigFix Compliance Analytics \(on page 35\)](#).

Setting up custom reporting for BigFix Compliance Analytics V1.8 and earlier

BigFix Compliance PCI Add-on provides reports that show the cumulative state aggregated on the level of specific PCI DSS requirements or milestones. To view such reports on BigFix Compliance Analytics V1.8 and earlier console, you must complete a few configuration steps.

The steps in this section is for BigFix Compliance Analytics V1.8 and earlier. You do not need to complete these steps to view the reports on BigFix Compliance Analytics V1.9 and later.

For BigFix Compliance Analytics V1.9 and later, see [Setting up the PCI DSS Policy Reports for BigFix Compliance Analytics V1.9 and later \(on page 19\)](#).

Installing the Requirements and Milestones reports manually

You must complete configuration steps to install the Requirements and Milestones reports in your BigFix environment. This information applies only to BigFix Compliance Analytics V1.8 or earlier.

To access the PCI DSS Requirements and Milestones Reporting from SCA, complete the following steps:

1. Subscribe to either the **PCI DSS Checklist for Windows 2012** site or the **PCI DSS Checklist for RHEL 6** site.


2. Deploy the **Environment Setup Task - Download Requirements and Milestones Reporting Installer** task to download the reports installer (`import_milestones.zip` package).
3. Extract the BES directory with `.bes` files to your local disk.

To install the reports manually, you must import each of the `.bes` file to a separate custom site using the BigFix console.

1. Create a custom site for each `.bes` file.
 - a. From the BigFix console, click **Tools > Create Custom Site**.
 - b. Enter a name for the custom site and click **OK**. For example, `PCIDSS_Milestone_1`.
2. Import a Fixlet to the custom site.
 - a. On your local disk, browse for the Fixlet that you want to add in the custom site and double-click it.

The dialog window on the BigFix console opens.
 - b. On the right-upper corner of the console, select the custom site that you created for this Fixlet in step 1 and click **OK**.


All the Fixlets are available in the BigFix console.
 - c. Complete steps 1 and 2 for each `.bes` file.
 - d. When all the custom sites for the Requirement and Milestones Reports are created and new Fixlets and analyses are imported in the BigFix Console, set the computer subscription for each site.

 **Note:** To enhance this process, you can use Computer Groups. You can create the groups manually, assign computers to them, and then assign the computer groups to the reporting custom sites.

 - e. Run the Environment Setup Tasks.

There are two separate environment setup tasks. One task is designed for the PCIDSS Milestone site and the other for all other Requirement and Milestones Reporting sites. Both of them are located under **PCIDSS_Milestones** site.

- f. Import data to BigFix Compliance Analytics by running an import on the BigFix Compliance Analytics console.

 **Note:** In case of updates to the Requirements and Milestones Reporting, you must delete the outdated content from the BigFix console. For more information, see [Updating the reports manually \(on page 24\)](#).

Updating the Requirements and Milestones reports manually

You must complete configuration steps to update the Requirements and Milestones reports. This information is applicable only to BigFix Compliance Analytics V1.8 or earlier.

1. Remove all the Fixlets and analyses in every custom site that you have created for the reporting. You might also need to delete the custom site. This step ensures that no duplicates are created.
2. Import the new version of the Fixlets and analyses by importing the definitions from the `.bes` files.
 - a. On your local disk, browse for the Fixlet that you want to add in the custom site and double-click on it. The dialog window on the BigFix console opens.
 - b. On the right-upper corner of the console, select the custom site that you created for this Fixlet in step 1 and click **OK**.
3. After the sites are updated, you need to run both environmental setup tasks.

There are two separate environment setup tasks. One task is designed for the PCIDSS Milestone site and the other for all other Requirement and Milestones Reporting sites. Both of them are located under **PCIDSS_Milestones** site.

 **Note:** Ensure that computers are subscribed to the site.

Installing the Requirements and Milestones reports with the `import_milestones.sh` script

The provided installation script creates and configures the necessary files to collect data from the endpoints and display them in the reports in BigFix Compliance Analytics version 1.8 or earlier.

- Ensure that you have the 'curl' package installed as it is required to use the script.
- To access the PCI DSS Requirements and Milestones Reporting from BigFix Compliance Analytics version 1.8 or earlier, complete the following steps:
 1. Subscribe to either the **PCI DSS Checklist for Windows 2012** site or the **PCI DSS Checklist for RHEL 6** site.
 2. Deploy the **Environment Setup Task - Download Requirements and Milestones Reporting Installer** task to download the reports installer (`import_milestones.zip` package).
 3. Extract the files to your local disk. The package contains:
 - `import_milestones.sh` script
 - BES directory with `.bes` files
 - META-INF directory with the manifest


The `import_milestones.sh` script can be used on Windows or Linux OS and with Cygwin and curl package. Running the script creates the following resources in your local disk:

- Three computer groups: `PCIDSS_Requirement_Group`, `PCIDSS_Milestones_Group`, `PCIDSS_Milestone_Group`
- 16 custom sites and uploads them in the BigFix console with the corresponding Fixlets.

1. Update the script with the URL to BigFix console and credentials as follows:

```
host="https://<host>:<port>"
userpass="Admin:XXXXXXXXX"
```


For the port number, see the masthead file located in `<InstallationPath>\BigFix Enterprise\BES Installers\Server\masthead.afxm`. The default port is 52311.

 **Note:** When modifying the file on a Windows OS, you need to keep the UNIX formatting (end of line character).

2. Execute the script in the current directory:

```
./import_milestones.sh
```

3. When all the custom sites for the Requirement and Milestones Reports are created in the BigFix console along with the Fixlets, you must subscribe all computers to each site.

 **Note:** To enhance this process, you can use the Computer Groups that were created and assigned to the reporting custom sites. You must assign computers to the groups.

4. Run the Environment Setup Tasks.

There are two separate environment setup tasks: one is designed for the PCIDSS Milestone site and the other for all other Requirement and Milestones Reporting sites. Both of them are located under **PCIDSS_Milestones** site.

5. Import data to BigFix Compliance Analytics by running an import on the BigFix Compliance Analytics console.

Updating the Requirements and Milestones reports with the `import_milestones.sh` script

Use the `import_milestones.sh` script to update the Requirements and Milestones Reporting.

To update the reports, you can use the script the same way as you would during the installation. For details about the steps, see [Installing the Requirements and Milestones reports with the `import_milestones.sh` script \(on page 25\)](#).

The `import_milestones.sh` script removes the Fixlets and analyses from the relevant reporting custom sites and imports the new versions of the files. During the removal, the percentage of action progress will be presented. The whole process might take approximately one hour to complete.

When the update process is completed, all the sites contain the new Fixlets and analyses.

The computer assignments using the computer groups will not be affected.

Chapter 3. Using checks and checklists

The check Fixlets in Configuration Management checklists assess an endpoint against a configuration standard. Many check Fixlets have a corresponding analysis, sometimes referred to as measured values, that report the value of the element that the check Fixlet evaluates.

Viewing check Fixlets from the HCL BigFix console

A check Fixlet becomes relevant when a client computer is out of compliance with a configuration standard. By viewing the Configuration Management Fixlets, Console Operators can identify non-compliant computers and the corresponding standards.

Subscribe to the PCI DSS Fixlet sites to gain access to the check Fixlets.


Complete the following steps to view the check Fixlets in the HCL BigFix Console after subscribing and gathering the site content.

1. From the **Security Configuration** domain, click **All Security Configuration > Sites > External Sites**.
2. Expand a checklist.
3. Click **Fixlets and Tasks**. The **Fixlets and Tasks** section opens.
4. Click one of the Fixlets displayed in the list.
The Fixlet opens with the following tabs: **Description**, **Details**, **Applicable Computers**, and **Action History**.
5. Click the **Description** tab to view the text that describes the Fixlet.


The Fixlet is applicable to a subset of endpoints on your network. The size of that subset is shown in the **Applicable Computers** tab.

A Fixlet typically has a description of the check appended with the rationale and guidelines of the actions for remediation. If the Fixlet is relevant, you must take

an action listed in the Remediation section of the description to remediate the noncompliance. You can also access the associated analysis from the description.

 **Note:** The Check ID refers to the Source ID of the Fixlet.

6. If you are using any of the checklists for AIX 7, MS SQL 2008, MS SQL 2012, MS IIS 7, RHEL 5, RHEL 6, RHEL 7, Solaris 10, or Solaris 11, run the **Environment Setup Task**.

 **Note:** Run the **Environment Setup Task** periodically to gather the latest results. For more information about this task, see [Configuring endpoints \(on page 14\)](#).

Viewing checks from BigFix Compliance Analytics

The compliance status of each PCI DSS check and checklist is calculated by BigFix Compliance Analytics during a periodic Extract Transform and Load (ETL) process.

BigFix Compliance Analytics provides report views and tools for managing the vulnerability of PCI DSS checks.

The PCI DSS checks that are activated in the HCL BigFix console are evaluated on each computer in your deployment and returns a status of pass, fail, or not applicable to BigFix Compliance Analytics.

Each computer also reports computer properties and analysis values, such as check measured values that are active in your deployment. Check results are aggregated by the BigFix Compliance Analytics server and augmented by computer properties and analysis values to provide compliance overviews and detailed lists of results.

For more information about how the checks are presented in different compliance reports, see [Understanding the results in BigFix Compliance Analytics \(on page 34\)](#).

Creating custom checklists

Create custom copies of the PCI DSS content if you want to modify the checks based on a specific corporate policy. You can manually create a custom site to host the PCI DSS

checklists or use the Create Custom Checklist wizard to create copies of the PCI DSS checklists and save them in a custom site.

You must subscribe to the SCM Reporting external site.

You can use custom checklists to fine-tune your ability to customize Configuration Management parameters, which gives you control over your security status. Custom checklists target specific sets of computers with tailored content using the subscription mechanism. This allows statistics to be gathered with finer granularity. For more information, see [Modifying check parameters \(on page 31\)](#).

- Creating custom checklists manually
 1. From the Security Configuration Domain, go to **Configuration Management > Checklist Tools > Create Custom Checklist**.
 2. Enter the name of the new checklist.
 3. Select the target platform.
 4. Click the drop-down menu to select which external checklist you copy the checks from. As you select the checks, they are shown in the staged list at the lower part of the window.
 5. Click the **Activate Measured Value analyses after copying** check box to activate all analyses that were copied.
 6. Click **Create Checklist**.


The console begins copying the checks in the selected lists into your new custom checklist. The process might take several minutes, depending on the number and size of the checklists selected.

- Creating custom checklist by using the Create Custom Checklist wizard
 1. Select **Tools > Create Custom Site**.
 2. You are prompted for a name for your custom site. Enter a name and click **OK**.
 3. From the Domain panel, find your site under **Sites > Custom** and click it to describe your site.

From the **Details** tab, enter a description of your site. From the **Domain** pull-down menu, select a Domain to house your site.

4. From the **Computer Subscriptions** tab, indicate which subset of your BigFix client computers you want to subscribe to this site.
5. From the **Operator Permissions** tab, you can grant specific access permissions to specific operators.
6. Click the **Save Changes** button above the work area to complete the description of your site. You must enter your password to propagate your new custom site.

Subscribe computers to the custom checklist.

 **Note:** Custom checklists do not support site relevance, so take extra precaution when you subscribe computers to custom checklists.

Modifying check parameters

In addition to monitoring compliance status and remediating settings that are out of compliance, you can also modify the values for the defined configuration settings according to company policies.

To modify the desired value of the check parameter in the Fixlet check description, you must first create a custom site. For more information about custom sites, see [Creating custom checklists \(on page 29\)](#).

Parameters are stored as site settings, so you can parameterize the same check differently for each site containing a copy of the check.

 **Note:** Not all checks in custom sites can be parameterized.

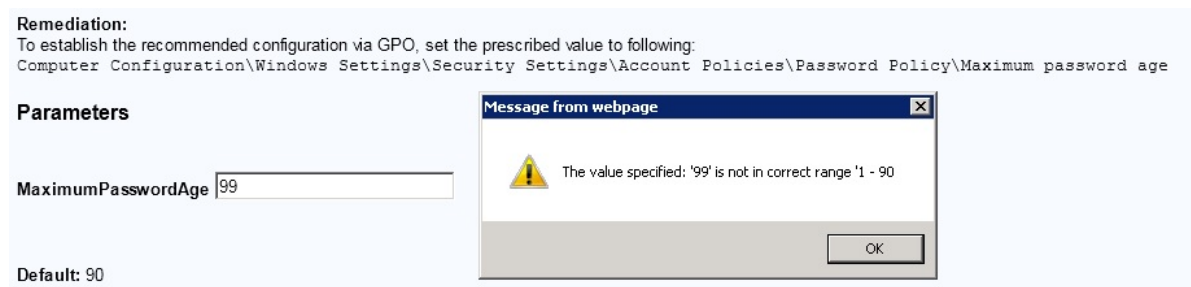
Some of the Fixlet checks allow you to set a more restrictive value than the one specified by the PCI DSS, giving you greater flexibility to customize security policies to meet a specific situation.

⚠ Important: Custom parameterization may take a few minutes to process. Allow enough time between updating a check parameter and executing the Environment Setup Task for optimum results.

📄 Note: Pparameter changes will only take effect after you run the **Environment Setup Task**. For information about this task, see [Configuring endpoints \(on page 14\)](#).

1. Open the Fixlet check and click the **Description** tab.
2. Scroll down to the **Parameters** section and enter the value.

Figure 4. Parameterization





3. Click **Save**.
4. Deploy the Fixlet.

Remediating configuration settings

The PCI DSS checklists for AIX 6, AIX 7, Red Hat Enterprise Linux (RHEL) 5, RHEL 6, RHEL 7, Solaris 10, Solaris 11, Windows 2008, Windows 2012, Windows 7, Windows 10, Windows Embedded POSReady 7, and Windows Embedded Standard 7 support remediation. Console operators can resolve a vulnerability issue with a single action. A remediation action can only be taken on an endpoint where the Fixlet is relevant.

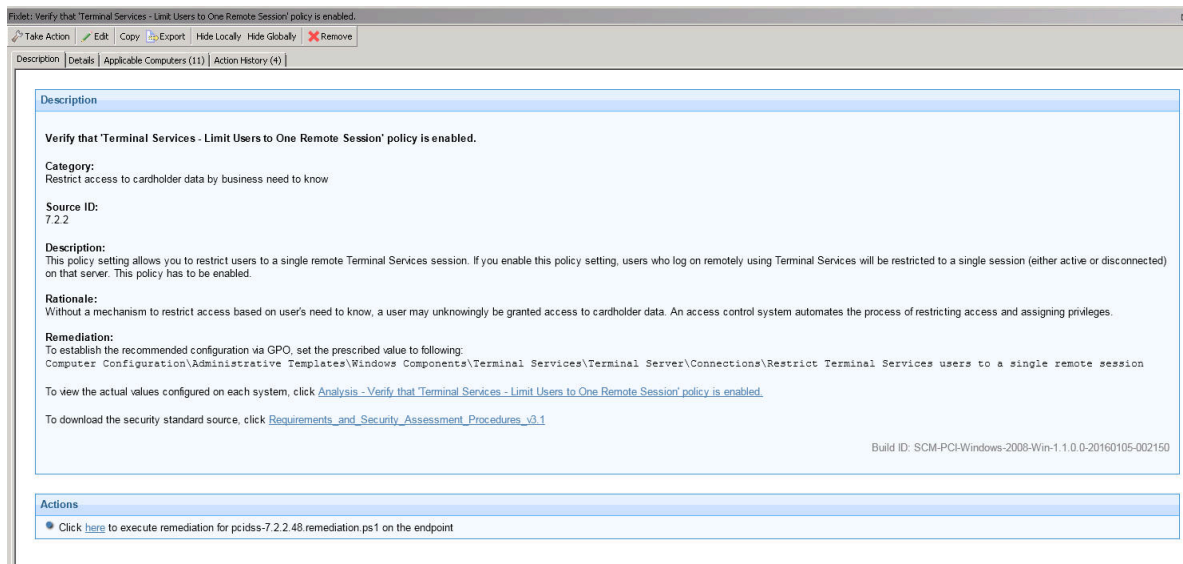
You can audit, assess, and remediate configuration settings using Security and Compliance Analytics (SCA), which is now known as BigFix Compliance Analytics. For Fixlet checks that can be automatically remediated, an action is displayed in the relevant Fixlet. You can take a remediation action only on the relevant and selected endpoints.

 **Note:** Not all Fixlets have a remediation action.

 **Note:** When the external global policy is enabled, any changes to the local endpoint is overwritten. In such case, the remediation action must be run using the external global policy solution.

1. From the Security Configuration Domain, go to **All Security Configuration > Fixlets and Tasks**.
2. Expand the sub-folders to search for the Fixlet you want to enable.
3. In the **Fixlet** window, click the **Description** tab and scroll down to the Actions box.
4. Click in the Actions box link to remediate the specified policy issue.

Figure 5. Check containing an action for remediation



The screenshot shows a window titled "Fixlet: Verify that 'Terminal Services - Limit Users to One Remote Session' policy is enabled." The window has a menu bar with "Take Action", "Edit", "Copy", "Export", "Hide Locally", "Hide Globally", and "Remove". Below the menu bar are tabs for "Description", "Details", "Applicable Computers (11)", and "Action History (4)". The "Description" tab is active, showing the following content:

Description

Verify that 'Terminal Services - Limit Users to One Remote Session' policy is enabled.

Category:
Restrict access to cardholder data by business need to know

Source ID:
7.2.2

Description:
This policy setting allows you to restrict users to a single remote Terminal Services session. If you enable this policy setting, users who log on remotely using Terminal Services will be restricted to a single session (either active or disconnected) on that server. This policy has to be enabled.

Rationale:
Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. An access control system automates the process of restricting access and assigning privileges.

Remediation:
To establish the recommended configuration via GPO, set the prescribed value to following:
Computer: Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Connections\Restrict Terminal Services users to a single remote session

To view the actual values configured on each system, click [Analysis - Verify that 'Terminal Services - Limit Users to One Remote Session' policy is enabled](#).

To download the security standard source, click [Requirements and Security Assessment Procedures_v3.1](#)

Build ID: SCM-PCI-Windows-2008-Win-1.1.0.0-20160105-002150

Actions

- Click [here](#) to execute remediation for pcidss-7.2.2.48.remediation.ps1 on the endpoint

5. Set your parameters in the Take Action dialog and click **OK**.

Chapter 4. Understanding the results in BigFix Compliance Analytics

Use BigFix Compliance Analytics (formerly known as Security and Compliance Analytics or SCA) to navigate and explore security configuration check results.

BigFix Compliance Analytics is a web-based application designed to help you manage security, vulnerability, and risk assessment. The application tabulates security and vulnerability compliance check results to identify configuration issues and report levels of compliance toward security configuration goals. Compliance data is collected with each nightly import and is presented with historical context for trend analysis.

These reports can be filtered, sorted, grouped, customized, or exported according to your preferences and requirements.

For more information about using BigFix Compliance Analytics, see the [BigFix Compliance Analytics User's Guide](#).

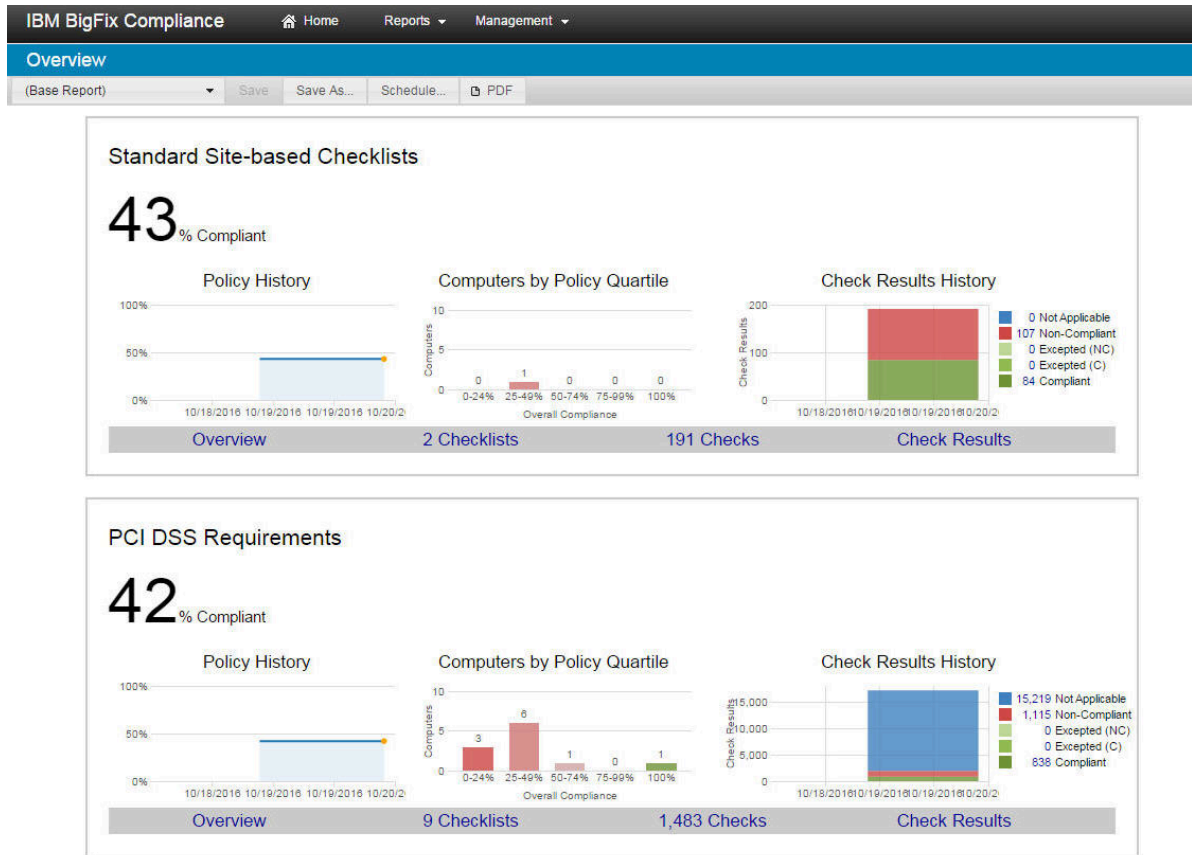
Starting BigFix Compliance Analytics

Use any of the supported web browsers to open the web-based application.

Before you can use Security and Compliance Analytics (SCA), which is now known as BigFix Compliance Analytics, you must complete the necessary installation and configuration steps. For more information, see the [BigFix Compliance Analytics Setup Guide](#).

1. Open Mozilla Firefox or Internet Explorer.
2. In the **URL** field, enter `http://localhost:<port>/scm`, where *port* is the server HTTP port that was specified during the BigFix Compliance Analytics installation.

Figure 6. BigFix Compliance Analytics 1.9 - Overview page

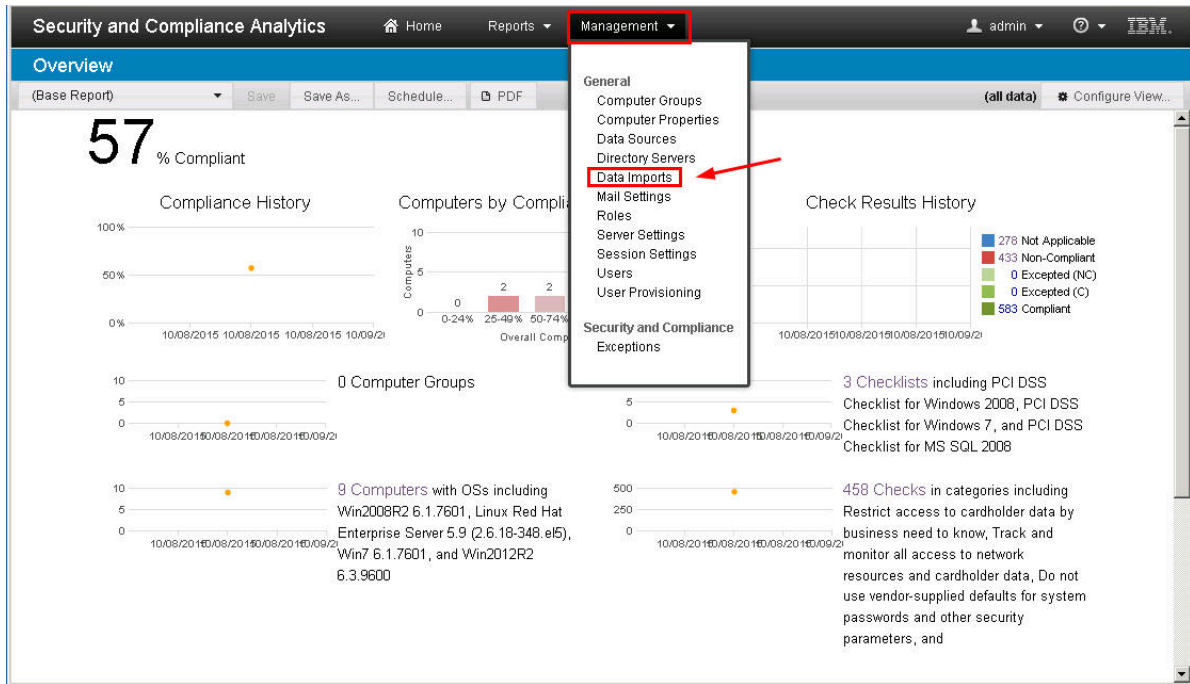


Importing data to BigFix Compliance Analytics

Depending on your configuration, the Extract Transform and Load (ETL) process that computes the compliance status of each check and checklist could take a long time. To ensure that you are viewing the latest reports, verify that the imports are configured to run automatically and that a recent import has completed successfully.

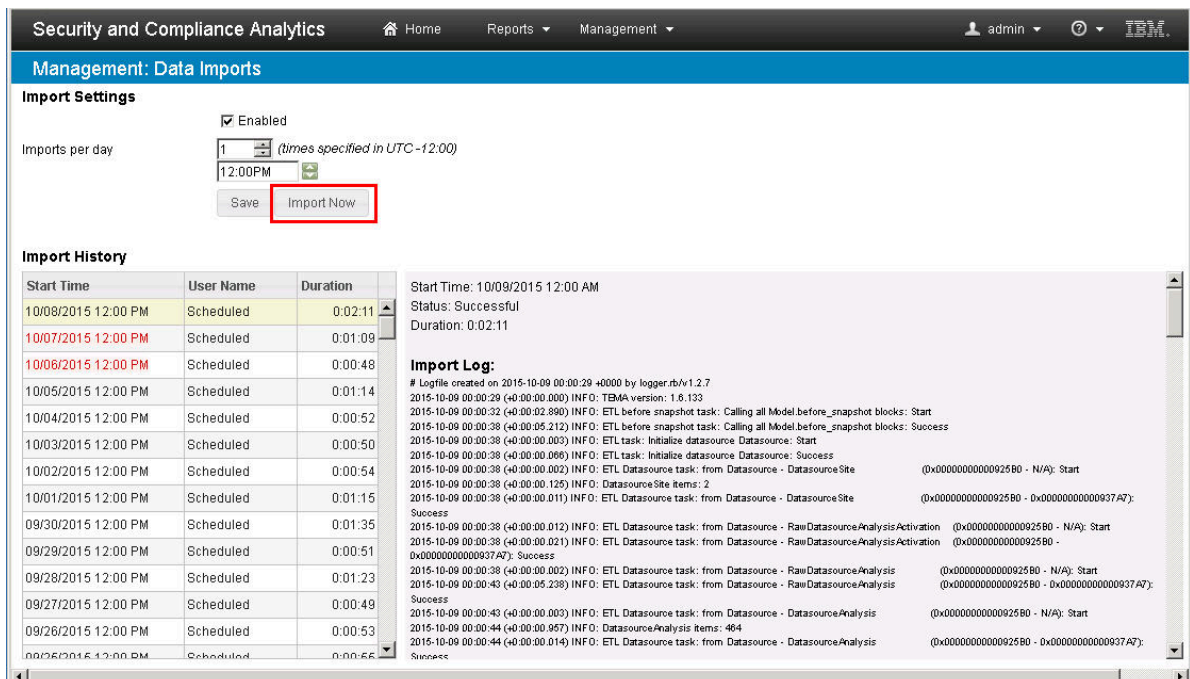
1. From the BigFix Compliance Analytics console, click **Management > Imports**.

Figure 7. Management menu



2. Click Import Now.

Figure 8. Import Now button



Viewing reports from BigFix Compliance Analytics

BigFix Compliance Analytics displays reports that contain the compliance status of your deployment. Each PCI DSS checklist and its checks are exported periodically into Compliance Analytics.

You can view the compliance status of your deployment from any of the four report types:

Overview Reports

In BigFix Compliance Analytics version 1.8 and earlier, the home page defaults to the Overview report that provides a graphical representation of all the SCM checks. The report includes graphs that illustrate the Compliance History, Computers by Compliance Quartile, Deployment Information, and Checks Results History.

In BigFix Compliance Analytics version 1.9 and later, the home page defaults to the Overview report that provides a graphical representation of the Policy History, Computers by Policy Quartile, and Check Results History for all PCI DSS Policies if the steps discussed at [Setting up the PCI DSS Policy Reports for BigFix Compliance Analytics V1.9 and later \(on page 19\)](#) are completed. If the aforementioned steps are not completed, the Overview report defaults to the view that is similar to the report in BigFix Compliance Analytics version 1.8.

List Reports

The List report shows a list of checklists, checks, computers, computers groups, or vulnerabilities in the deployment. It provides the attributes of each type and the overall, historical aggregate compliance results of all types on all visible computers.

Each row entry in the report represents a list type, such as checklists, checks, computers, computers groups, or vulnerabilities.

Check Results Reports

The Check Results report shows the list of all checks and computers, attributes of each computer and check, and the historical compliance result for each check on each computer.

Each row entry in the report represents a single check on a single computer.

Exceptions Reports


The Exception report shows the list and status of exceptions in the given scope applied to each computer visible to the logged-in user, together with attributes of each check, each computer, and each exception.

Each row entry in the report represents a single check on a single computer as specified by an exception.

Each of these reports contain graphical and tabular views of different aspects of your deployment compliance status. For more information about the available report types, see [Viewing deployment compliance status reports](#).

Viewing PCI DSS compliance results


This section shows how you can view the results of PCI DSS compliance at a checklist, checks, and check results levels.

 **Note:** Data is updated in BigFix Compliance Analytics once a day. To ensure that your reports contain the latest data, run the import feature after running the Environment Setup tasks in the applicable sites.

Before you start accessing the available reports, complete the following tasks:

- Import data to ensure that the reports contain the latest data. For more information, see [Importing data to BigFix Compliance Analytics \(on page 35\)](#).
- If you were involved in the Early Access Program, unsubscribe from any of the PCI DSS beta sites to avoid any issues during import.

Viewing reports on BigFix Compliance Analytics V1.9 and later

 **Note:** The PCI DSS Policy Reports are available only when you complete the steps described in [Setting up the PCI DSS Policy Reports for BigFix Compliance Analytics V1.9 and later \(on page 19\)](#).

The concept of checklists in BigFix Compliance Analytics version 1.9 differs from previous versions. Previously, a checklist is equivalent to a BigFix site. However, with policy reporting being introduced in this version, a checklist can now be associated with a policy view.

A policy view is based on an approach to gain compliance for PCI DSS, such as PCI DSS requirement or PCI DSS milestone. For more information about policy views, see [PCI DSS policies \(on page 8\)](#).

For simplicity, these checklists that are associated to policies will be referenced as Policy Checklists in this document.

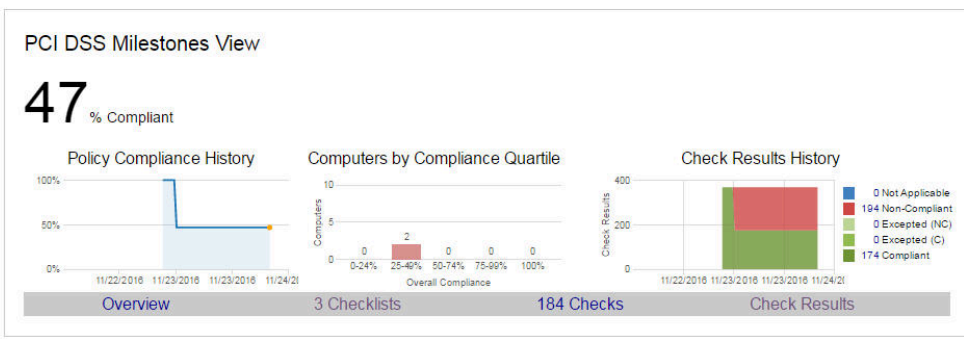
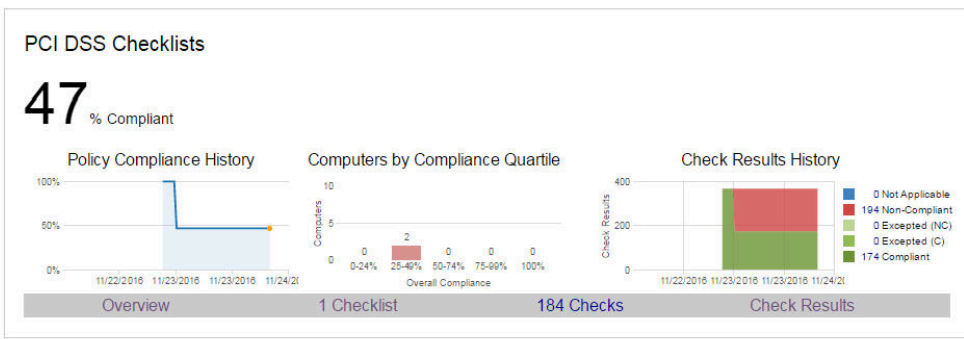
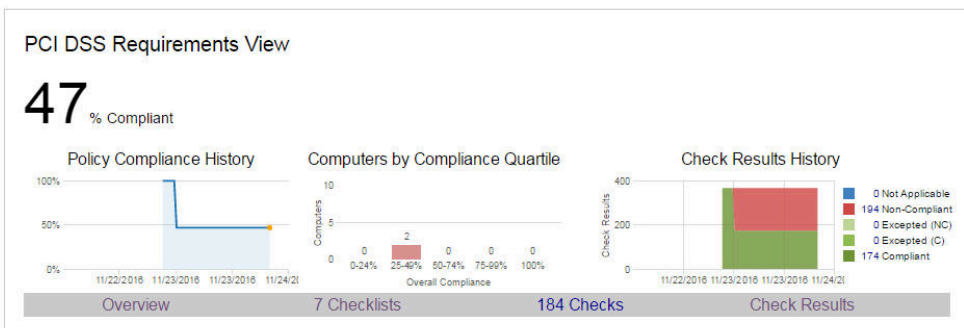
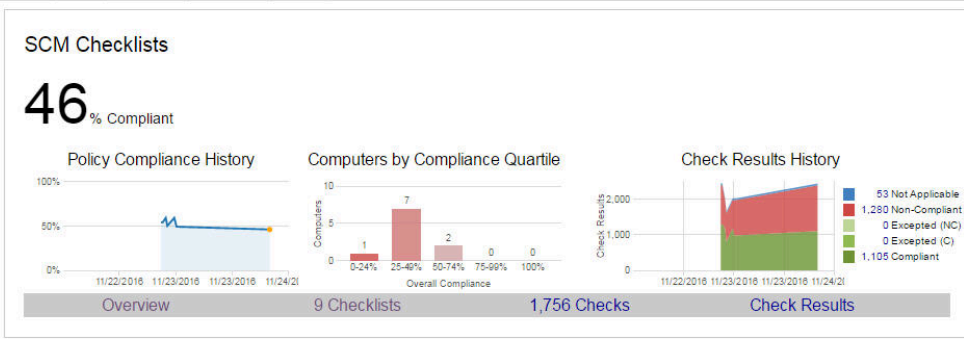
Policy Checklists contain a collection of checks that run across multiple PCI DSS sites. These checklists provide a new way of reporting, which can help you better assess and identify the level of compliance in your organization.

Viewing the Overview report

Starting from BigFix Compliance Analytics V1.9, the home page defaults to the Overview report that provides a graphical representation of the Policy History, Computers by Policy Quartile, and Check Results History for all PCI DSS Policies.

You can quickly drill down to the checklists, checks, or check results views for each PCI DSS Policy Overview report by using the quick links.

Figure 9. Overview page displaying the PCI DSS policies compliance overview summary

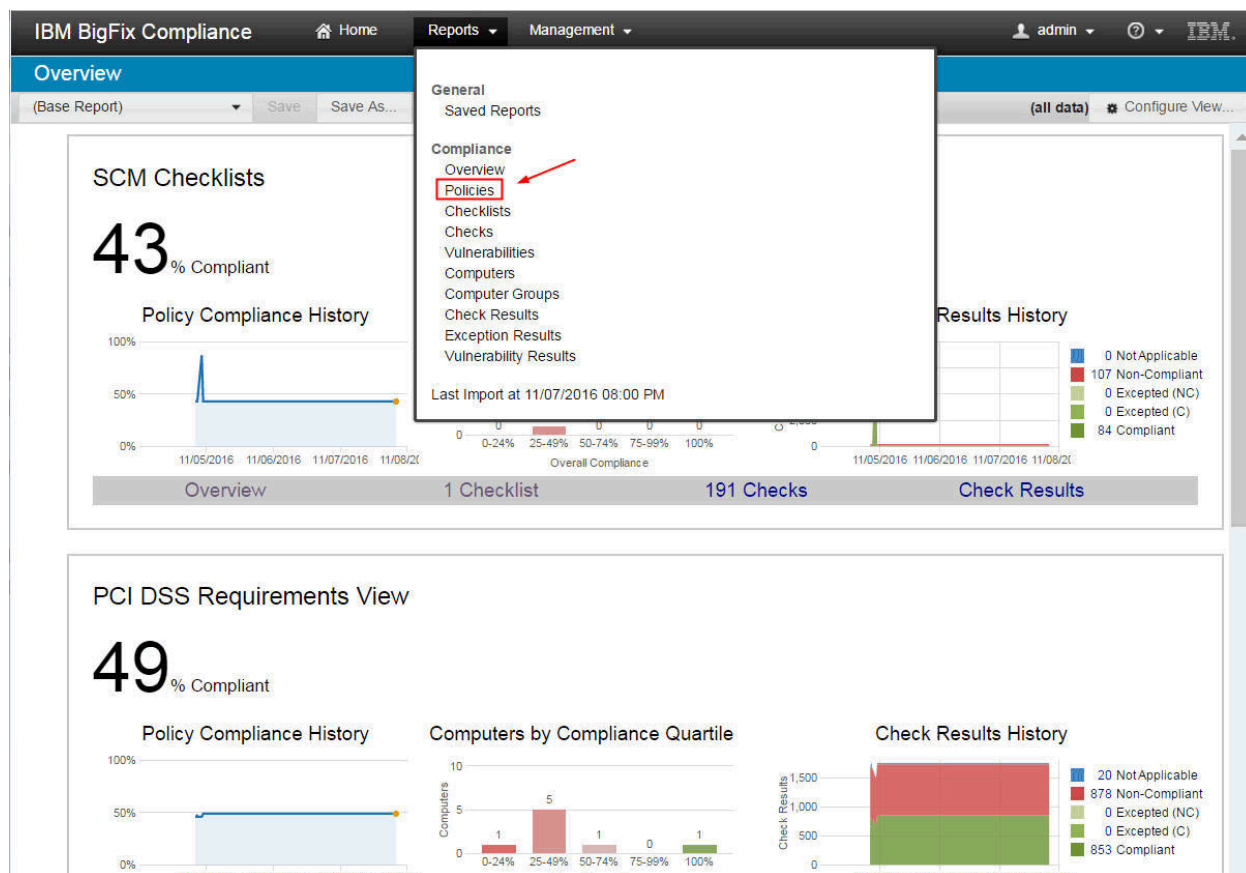


Viewing the Policy View List report

The Policy View List report shows a list of policies that provide the cumulative state aggregated on the level of a specific PCI DSS requirement or milestone. Results from the Requirements and Milestones reports include summary views at the home page or on the computer level.

To view the policies, click **Reports > Policies**. You can also access them from the Overview page.

Figure 10. Policies menu



The Policy View List report provides high-level compliance information at a policy level or across checklists.

Figure 11. List of available policies

Policies		
Name	Publisher	Compliance
PCI DSS Checklists	IBM	47% 174 194 1 Checklist 184 Checks 2 Computers
PCI DSS Milestones View	PCI Security Standards Council	47% 174 194 3 Checklists 184 Checks 2 Computers
PCI DSS Requirements View	PCI Security Standards Council	47% 174 194 7 Checklists 184 Checks 2 Computers
SCM Checklists	Various publishers	46% 1,105 1,280 9 Checklists 1,756 Checks 10 Computers

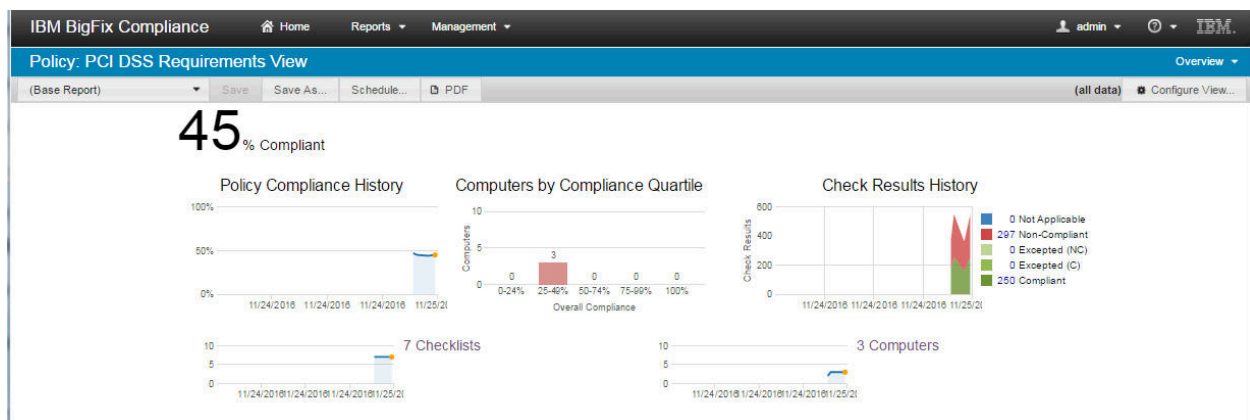
Viewing the Policy View Overview report

The Policy Overview report shows information about a single policy and overall, historical compliance for the policy as applied to all computers visible to logged in users.

The Overview report provides a graphical representation of the Policy History, Computers by Policy Quartile, and Check Results History for each of the PCI DSS Policy. The BigFix Compliance Analytics V1.9 home page lists the Overview reports for all policies.

You can click each policy from the home page to display the standard Overview report. The PCI DSS Requirement View is shown as an example.

Figure 12. PCI DSS Requirement policy overview



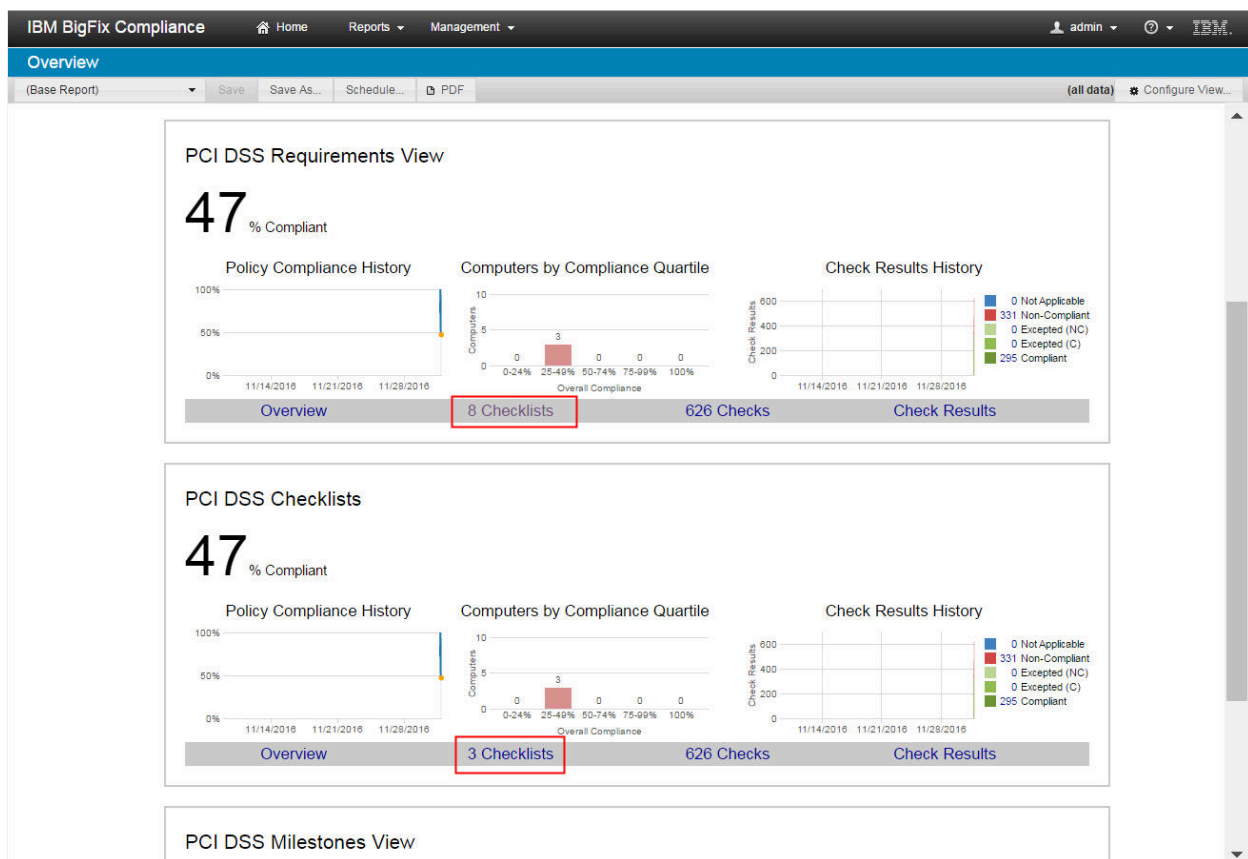
You can also access the standard Overview report from the Policy List report by clicking a policy view name.

Viewing the Policy Checklist List report

A policy checklist is based on the policy views or compliance approaches that are made available in BigFix Compliance Analytics V1.9. It contains a collection of checks that may belong to multiple PCI DSS checklists or sites.

You can view all the checklists under a policy from the Overview report, either from the home page or the Policy View Overview report. The quick links in each of the policy view in the home page is clickable.

Figure 13. Overview report from the home page



The Policy Checklist List report view provides high-level compliance information at a checklist level based on a Policy View. It displays the list of checklists in the deployment together with the attributes of each checklist and the overall, historical aggregate compliance results of all checks on all visible computers for each checklist.

Figure 14. Policy List Report

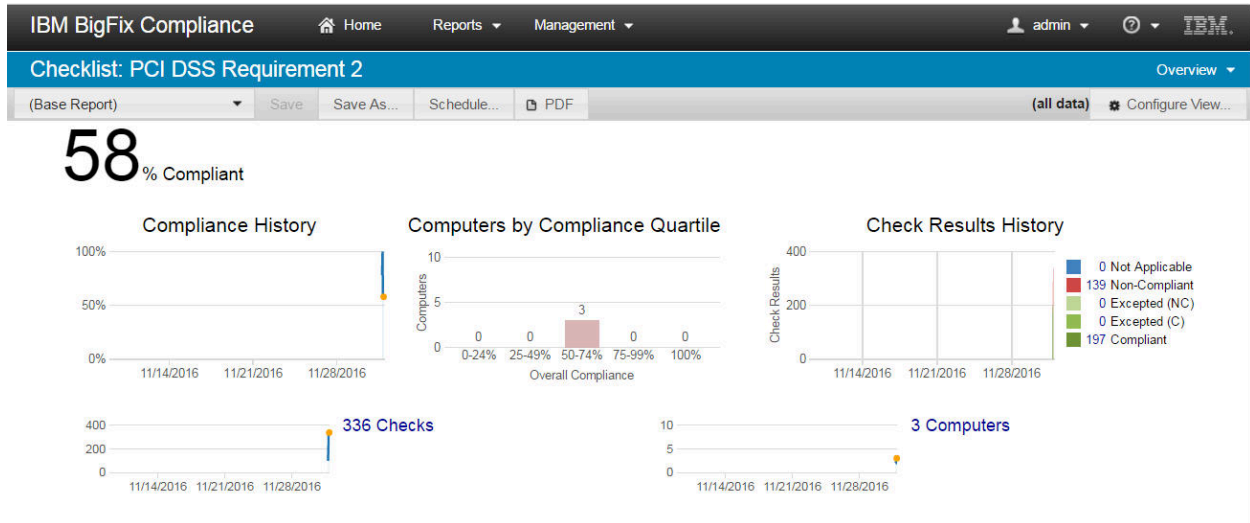
IBM BigFix Compliance		Home	Reports	Management	admin	IBM
Policy: PCI DSS Requirements View						Checklists
(Base Report)		Save	Save As...	Schedule...	CSV	PDF
8 rows (all data)						Configure View...
Name	Compliance					
	11/09/2016 - 12/02/2016	0%	25%	50%	75%	100%
PCI DSS Requirement 1	33% 9 Checks 2 Computers					
PCI DSS Requirement 10	22% 74 Checks 3 Computers					
PCI DSS Requirement 2	58% 336 Checks 3 Computers					
PCI DSS Requirement 4	33% 12 Checks 3 Computers					
PCI DSS Requirement 5	0% 2 Checks 1 Computer					
PCI DSS Requirement 6	12% 8 Checks 3 Computers					
PCI DSS Requirement 7	48% 124 Checks 3 Computers					
PCI DSS Requirement 8	21% 61 Checks 3 Computers					

Viewing the Policy Checklist Overview report

The Policy Checklist Overview report shows information about a single policy checklist, which may contain checks from multiple PCI DSS checklists or sites. It includes information such as the quantity of checks in the policy checklist, and the overall, historical aggregate compliance for the policy checklist as applied to all computers visible to logged in users.

To view the overview information of a policy checklist, click the checklist name from the Checklist List report. The PCI DSS Requirement 5 policy checklist is shown as an example. The Checklist Overview Report displays.

Figure 15. Checklist overview



The Overview shows a graphic representation of compliance history, computers by compliance quartile, and check results history with an overall compliance percentage shown in the top-left corner of the console.

Viewing the Checks List report

The Checks List report shows the list of checks available in a policy checklist.

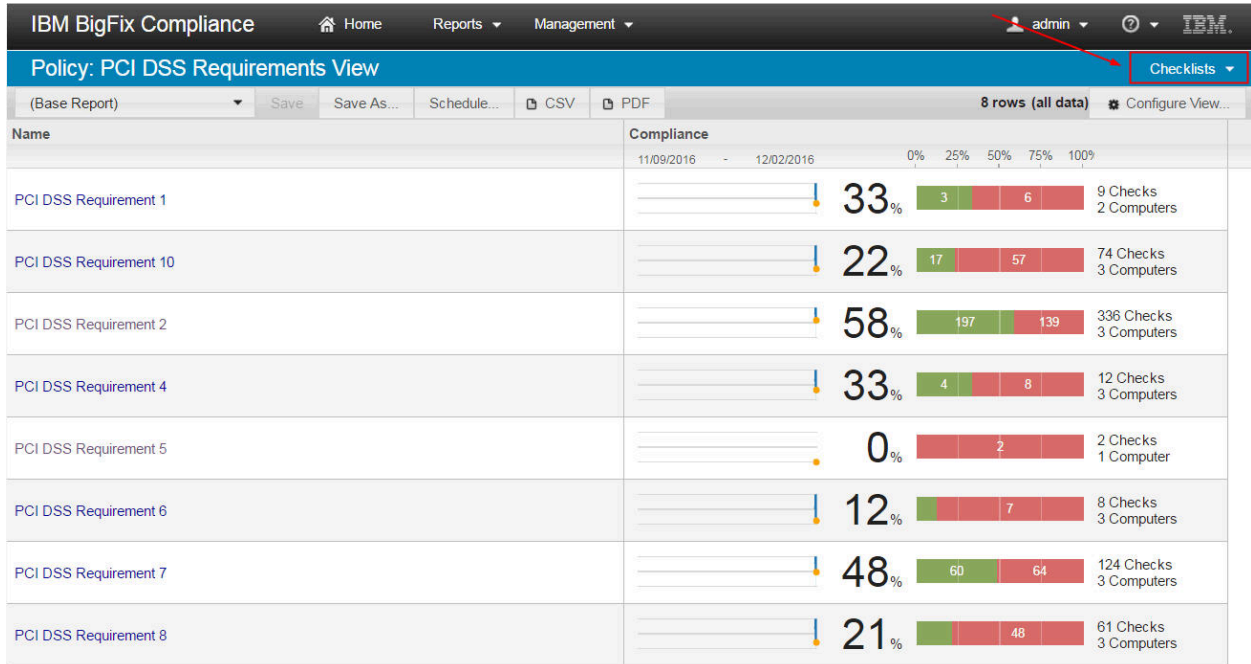
In the following figure, the Policy Checklist Overview report shows that there are 336 checks available in the PCI DSS Requirement 2 checklist. To view these checks in detail, drill down to the checks by clicking on the link.

Figure 16. Number of available checks in a checklist



You can also access the Check List report from the Policy List report by the Report View drop-down list, which is highlighted in the following figure. This method allows you to view all the checks for a policy view, as well as to drill down to a particular checklist and then view its checks.

Figure 17. Policy List Report



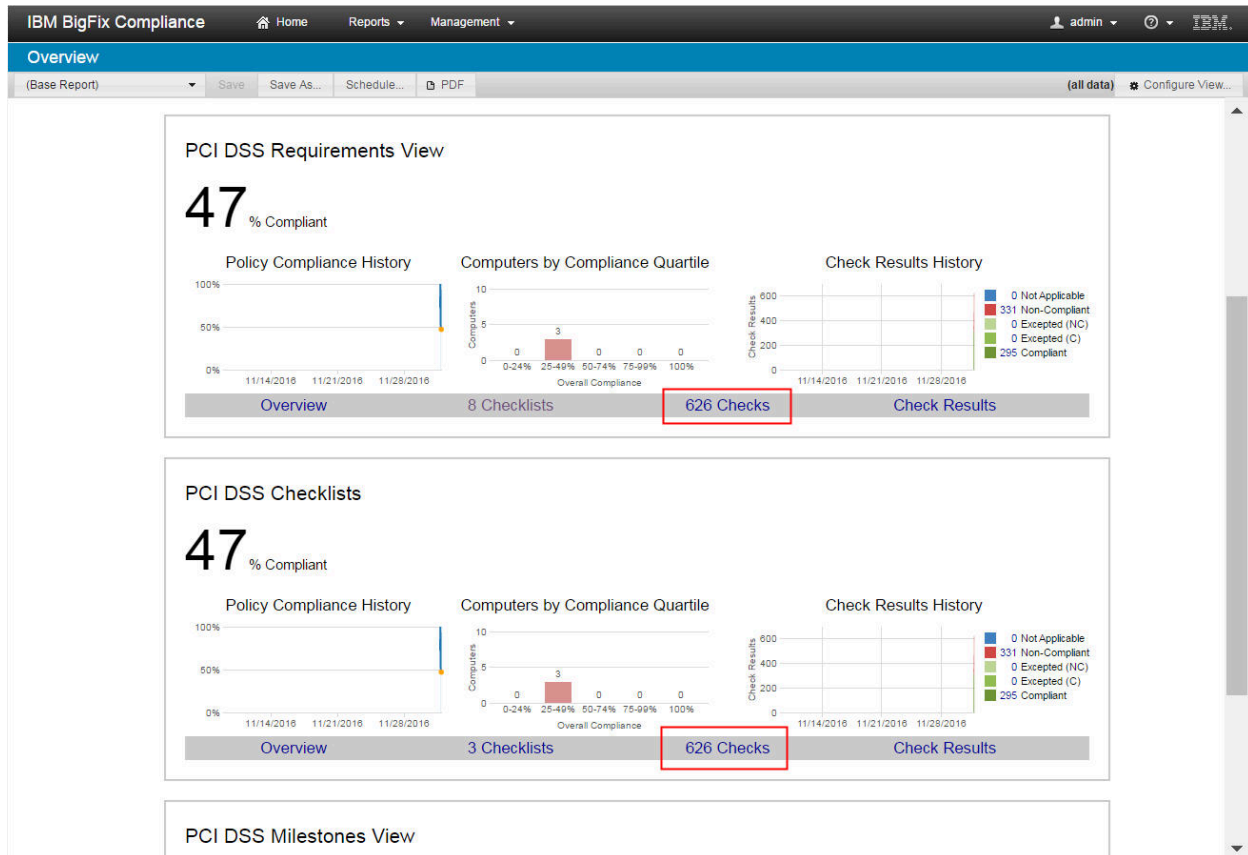
The Checks report shows the list of checks in the given scope together with the attributes of each check and the overall, historical aggregate compliance results (the aggregate of all visible computer's pass and fail score) of each check. To see the direct reference to a standard, you can configure the report view to display the Source ID.

Figure 18. List of checks

Name	Source ID	Desired Values	Compliance
Verify that "cronie-anacron" package is removed	pcidss-2.2.2.a.21.6	cronieAnacron: Not installed	0% 1 Computer
Verify that "daytime-dgram" service is disabled	pcidss-2.2.2.a.3.6	daytimeDgram: Disabled	100% 1 Computer
Verify that "daytime-dgram" service is disabled	pcidss-2.2.2.a_3.8	daytimeDgram: Off	100% 1 Computer
Verify that "daytime-stream" service is disabled	pcidss-2.2.2.a.4.6	daytimeStream: Disabled	100% 1 Computer
Verify that "daytime-stream" service is disabled	pcidss-2.2.2.a_4.8	daytimeStream: Off	100% 1 Computer
Verify that "DHCP" server is removed	pcidss-2.2.2.a.16.6	dhcp: Not installed	100% 1 Computer
Verify that "echo-dgram" service is disabled	pcidss-2.2.2.a_5.8	echoDgram: Off	100% 1 Computer
Verify that "echo-dgram" service is disabled	pcidss-2.2.2.a.5.6	echoDgram: Disabled	100% 1 Computer
Verify that "echo-stream" service is disabled	pcidss-2.2.2.a_6.8	echoStream: Off	100% 1 Computer
Verify that "echo-stream" service is disabled	pcidss-2.2.2.a.6.6	echoStream: Disabled	100% 1 Computer

Alternatively, you can access the overall Checks List report from the Overview report in the home page. You can then filter the checks according to your preference.

Figure 19. Overview report with the highlighted Checks link



Viewing the Checks Overview report

The Checks Overview report shows detailed information about a check, such as the source information, description, and remediation steps. It also contains overall, historical aggregate compliance of the check as evaluated by all computers visible to logged in users.

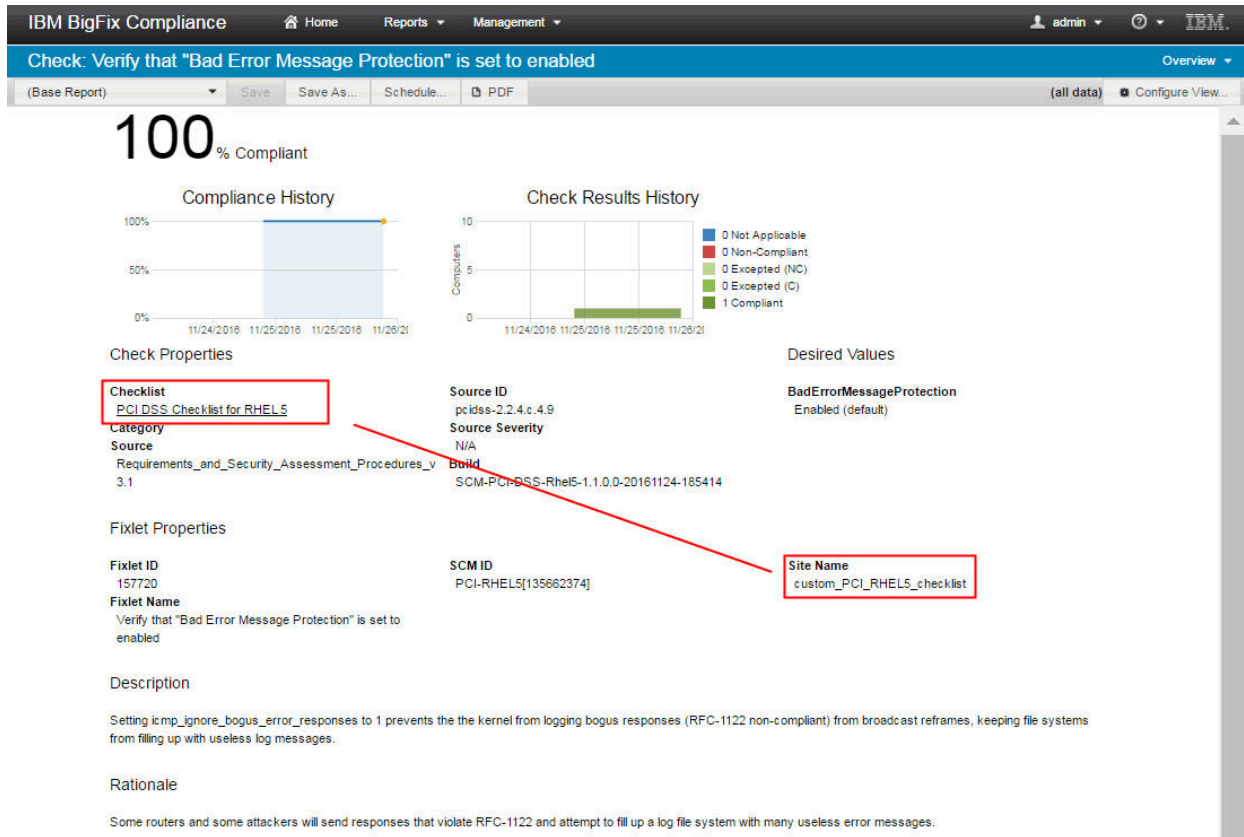
You can drill down to each check from the Checks List report to view more details.

The Checks Overview report shows a graphic representation of Compliance and Check Results history with an overall compliance percentage.

Note: The PCI DSS Checklists policy view does not cover the external sites for the PCI DSS checklists in BigFix Compliance Analytics version 1.9.

The checks under the PCI DSS Checklists policy view are evaluated using the custom copy of the checklist as indicated in the sample Check Overview report in the following figure:

Figure 20. Overview details of a check from the PCI DSS Checklists policy view



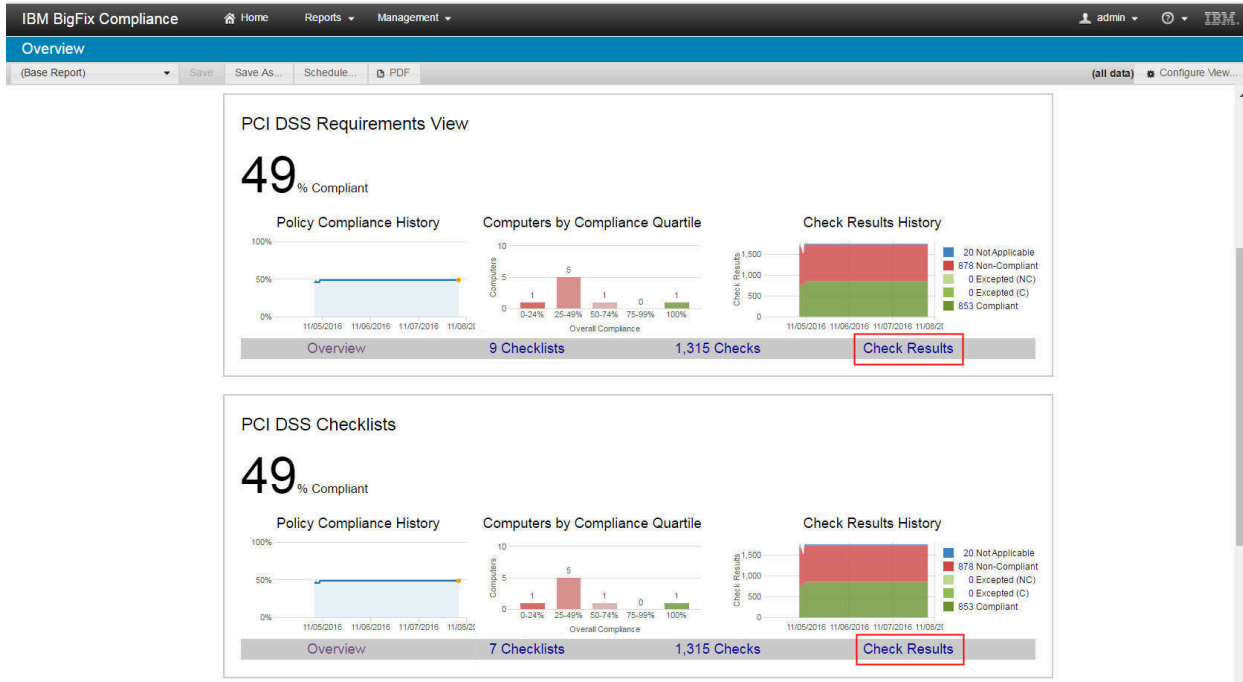
To ensure accurate reporting, complete the steps described in [Setting up the PCI DSS Policy Reports for BigFix Compliance Analytics V1.9 and later \(on page 19\)](#).

Viewing the Check Results List report

The Check Results List report shows the checklist, check name, computer name, the date when the results were last seen, and the level of compliance. It provides the attributes of each computer and check, and the historical compliance result for each check on each computer.

You can access the Check Results report for a particular policy view from the home page as shown in the following figure.

Figure 21. Check Results List Report link in the home page



Alternatively, you can access the Checks Results List report for a particular policy view from the Policy List report by using the drop-down list as shown in the following figure.

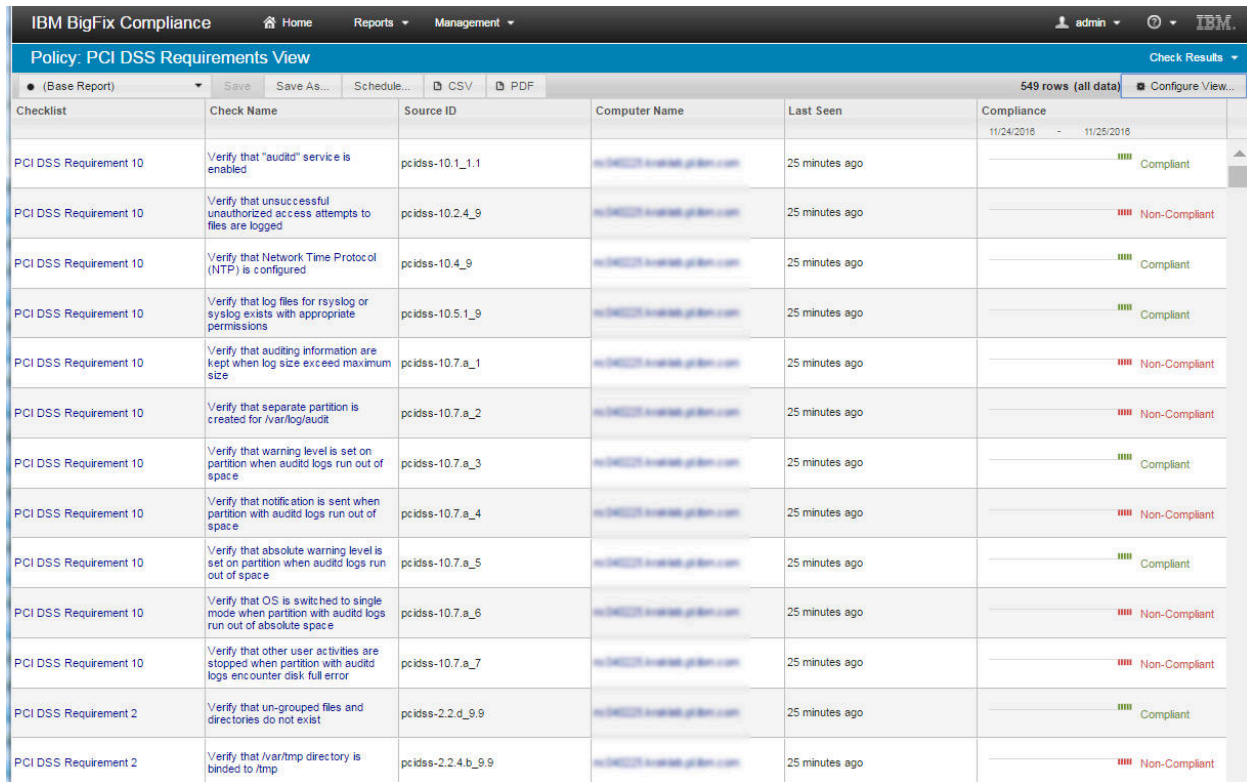
Figure 22. Policy List Report

The screenshot shows the 'Policy: PCI DSS Requirements View' in the IBM BigFix Compliance interface. A red arrow points to the 'Checklists' dropdown menu in the top right corner. Below the navigation bar, there is a table with 8 rows of data. Each row represents a PCI DSS requirement and includes a compliance percentage, a bar chart showing the distribution of checks, and the total number of checks and computers associated with that requirement.

Name	Compliance	Checks	Computers
PCI DSS Requirement 1	33%	9 Checks	2 Computers
PCI DSS Requirement 10	22%	74 Checks	3 Computers
PCI DSS Requirement 2	58%	336 Checks	3 Computers
PCI DSS Requirement 4	33%	12 Checks	3 Computers
PCI DSS Requirement 5	0%	2 Checks	1 Computer
PCI DSS Requirement 6	12%	8 Checks	3 Computers
PCI DSS Requirement 7	48%	124 Checks	3 Computers
PCI DSS Requirement 8	21%	61 Checks	3 Computers

You can then configure the view to show only the PCI DSS checks that you need by using the source ID as the filtering condition.

Figure 23. Checks Results List Report



Checklist	Check Name	Source ID	Computer Name	Last Seen	Compliance
PCI DSS Requirement 10	Verify that "auditd" service is enabled	pcidss-10.1_1	pcidss-10.1_1	25 minutes ago	Compliant
PCI DSS Requirement 10	Verify that unsuccessful unauthorized access attempts to files are logged	pcidss-10.2.4_9	pcidss-10.2.4_9	25 minutes ago	Non-Compliant
PCI DSS Requirement 10	Verify that Network Time Protocol (NTP) is configured	pcidss-10.4_9	pcidss-10.4_9	25 minutes ago	Compliant
PCI DSS Requirement 10	Verify that log files for rsyslog or syslog exists with appropriate permissions	pcidss-10.5.1_9	pcidss-10.5.1_9	25 minutes ago	Compliant
PCI DSS Requirement 10	Verify that auditing information are kept when log size exceed maximum size	pcidss-10.7.a_1	pcidss-10.7.a_1	25 minutes ago	Non-Compliant
PCI DSS Requirement 10	Verify that separate partition is created for /var/log/audit	pcidss-10.7.a_2	pcidss-10.7.a_2	25 minutes ago	Non-Compliant
PCI DSS Requirement 10	Verify that warning level is set on partition when auditd logs run out of space	pcidss-10.7.a_3	pcidss-10.7.a_3	25 minutes ago	Compliant
PCI DSS Requirement 10	Verify that notification is sent when partition with auditd logs run out of space	pcidss-10.7.a_4	pcidss-10.7.a_4	25 minutes ago	Non-Compliant
PCI DSS Requirement 10	Verify that absolute warning level is set on partition when auditd logs run out of space	pcidss-10.7.a_5	pcidss-10.7.a_5	25 minutes ago	Compliant
PCI DSS Requirement 10	Verify that OS is switched to single mode when partition with auditd logs run out of absolute space	pcidss-10.7.a_6	pcidss-10.7.a_6	25 minutes ago	Non-Compliant
PCI DSS Requirement 10	Verify that other user activities are stopped when partition with auditd logs encounter disk full error	pcidss-10.7.a_7	pcidss-10.7.a_7	25 minutes ago	Non-Compliant
PCI DSS Requirement 2	Verify that un-grouped files and directories do not exist	pcidss-2.2.d_9.9	pcidss-2.2.d_9.9	25 minutes ago	Compliant
PCI DSS Requirement 2	Verify that /var/tmp directory is binded to /tmp	pcidss-2.2.4.b_9.9	pcidss-2.2.4.b_9.9	25 minutes ago	Non-Compliant

Viewing custom reporting on BigFix Compliance Analytics V1.8 and earlier

PCI DSS Requirements Reporting

BigFix Compliance PCI Add-on provides additional reports to show a cumulative compliance state of your endpoints based on the PCI DSS Requirements.

To view the PCI DSS Requirements reports, complete the steps in [Setting up custom reporting for BigFix Compliance Analytics V1.8 and earlier \(on page 22\)](#).

The PCI DSS Requirements reports are generated based on the *Requirements and Security Assessment Procedures* document. Each requirement has a corresponding checklist.

Note: PCI DSS requirements 9, 11, and 12, which are process-oriented in nature, are not covered in BigFix Compliance.

These reports contain checklists that are mapped from the PCI DSS requirements and sub-requirements as seen in the following figure. The mapping was used in creating the checklists for the requirements perspective.

Figure 24. PCI DSS Requirement mapping

Checks List for PCI DSS Requirement 10 and mapping to PCI DSS standard

The screenshot displays the 'Checklist: PCIDSS Requirement 10' in the IBM BigFix Compliance interface. It features a table of cumulative states for various requirement sub-items (e.g., pcidss-10.1, pcidss-10.2, etc.), each with a 'Component checks' link. A red box highlights a detailed table mapping PCI DSS requirements to testing procedures. A red arrow points from the 'Component checks' column to this mapping table.

PCI DSS Requirements	Testing Procedures
10.1 Implement audit trails to link all access to system components to each individual user.	10.1 Verify, through observation and interviewing the system administrator, that: <ul style="list-style-type: none"> Audit trails are enabled and active for system components. Access to system components is linked to individual users.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	10.2 Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following:
10.2.1 All individual user accesses to cardholder data	10.2.1 Verify all individual access to cardholder data is logged.
10.2.2 All actions taken by any individual with root or administrative privileges	10.2.2 Verify all actions taken by any individual with root or administrative privileges are logged.

Each requirement has a corresponding checklist. To view the list of checklists, which represent the PCI DSS requirements, click **Reports > Checklists**. You can view more information about a checklist by clicking the checklist name from the Checklist view.

Figure 25. PCI DSS Requirement Checklist List

The screenshot shows the 'Checklists' view in the IBM BigFix Compliance interface. It displays a table with 9 rows of filtered data, showing compliance percentages and the number of checks and computers for each requirement.

Name	Compliance
PCIDSS_Requirement_1	100% (138 checks, 3 Computers)
PCIDSS_Requirement_2	90% (103 checks, 3 Computers)
PCIDSS_Requirement_3	100% (166 checks, 3 Computers)
PCIDSS_Requirement_4	88% (32 checks, 3 Computers)
PCIDSS_Requirement_5	100% (36 checks, 3 Computers)
PCIDSS_Requirement_6	98% (151 checks, 3 Computers)
PCIDSS_Requirement_7	90% (27 checks, 3 Computers)
PCIDSS_Requirement_8	92% (141 checks, 3 Computers)
PCIDSS_Requirement_10	90% (109 checks, 3 Computers)

Checklist Overview

To view an overview of a specific requirement checklist, click **Reports > Checklists**. Then, select a requirement checklist: `PCIDSS_Requirement_<number>`.

The Overview presents a graphic representation of compliance history, computers by compliance quartile, and check results history with an overall compliance percentage shown in the top left corner of the console.

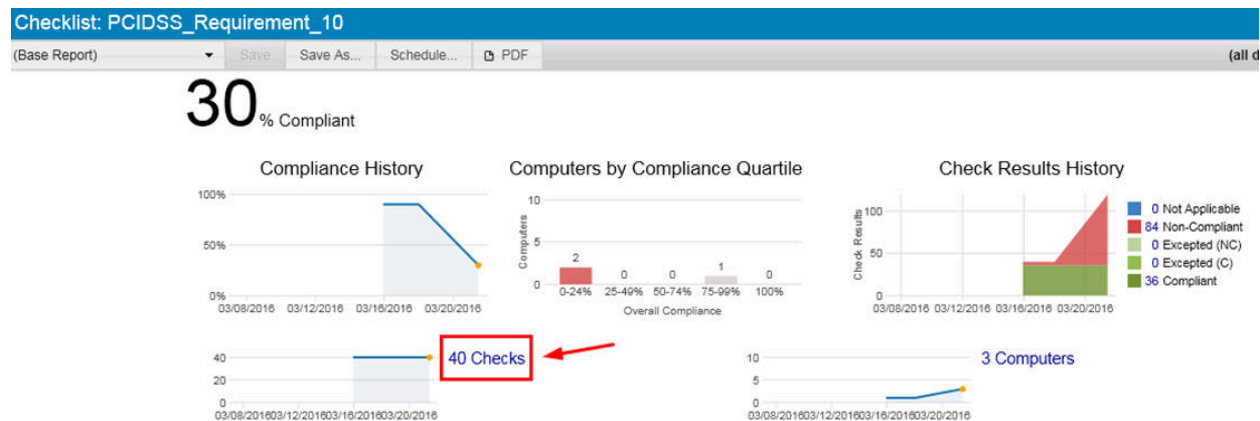
From this view, you can:

- View the list of checks by clicking on the number of checks available.
- View the list of computers by clicking on the number of computers available.
- View the list of checks and computers based on their compliance status.

Checks List

You can view the available checks in a checklist in detail by drilling down to the checks. You can do this by clicking the number of checks displayed on the Checklist Overview page.

Figure 26. PCI DSS Requirement Checklist Overview - Checks Link



This view shows a list of all checks, each in its cumulative state, for a requirement checklist. In the following figure, the cumulative state for each check for requirement 10 is displayed.

Figure 27. PCI DSS Requirement Check List

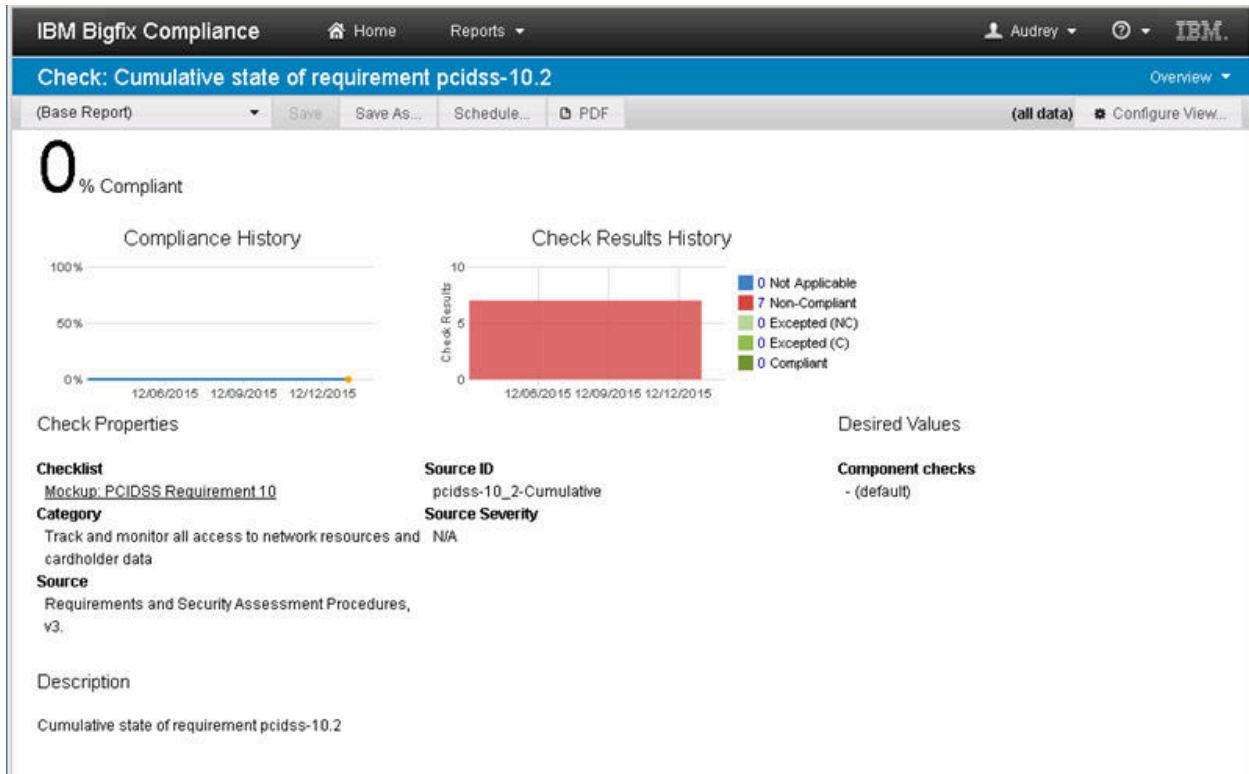
Name	Desired Values	Compliance				
		03/07/2016 - 03/22/2016	0%	25%	50%	75%
Cumulative state of requirement pcidss-10.1	Component checks: -	0%	0	3	3	Computers
Cumulative state of requirement pcidss-10.2	Component checks: -	0%	0	3	3	Computers
Cumulative state of requirement pcidss-10.2.1	Component checks: -	33%	1	2	3	Computers
Cumulative state of requirement pcidss-10.2.2	Component checks: -	33%	1	2	3	Computers
Cumulative state of requirement pcidss-10.2.3	Component checks: -	33%	1	2	3	Computers
Cumulative state of requirement pcidss-10.2.4	Component checks: -	0%	0	3	3	Computers
Cumulative state of requirement pcidss-10.2.6	Component checks: -	33%	1	2	3	Computers

Check Overview

You can drill down to a specific check to view an overview of the cumulative check result. To do this, you can either click on a check name from the check list (as shown in the previous screenshot) or click **Reports > Checks** and select the cumulative check or click any check in the list.

This view shows a graphic representation of compliance history and check results history for a particular check, in this case, requirement 10.2.

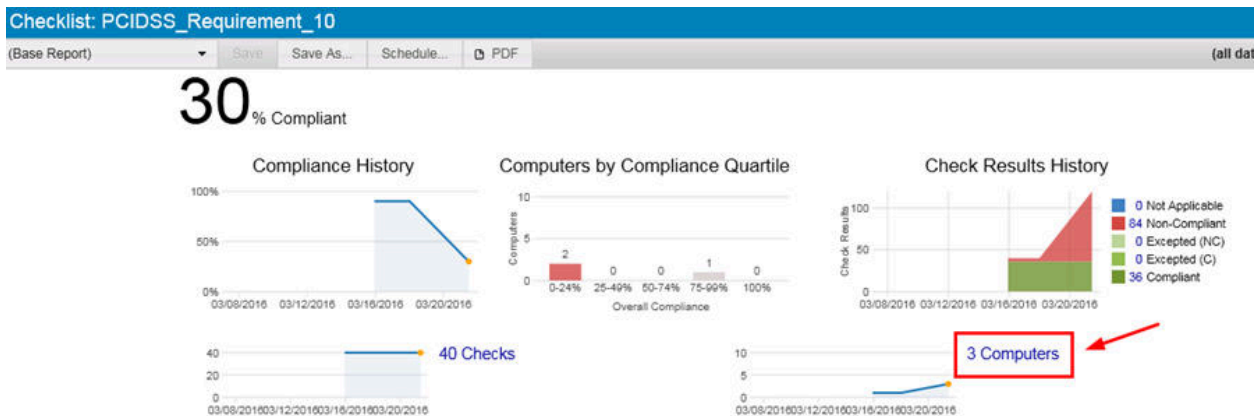
Figure 28. PCI DSS Requirement Check Overview



List of Computers

You can view the list of computers that are relevant to a specific requirement. To view this report, click the number of computers displayed on the Checklist Overview page.

Figure 29. PCI DSS Requirement Check Overview - Computers Link



This view shows a list of all computers with additional information, such as operating system. It also shows the corresponding compliance status for each computer.

Figure 30. PCI DSS Requirement Check Overview - Computers Link

Computer Name	Last Seen	Compliance
NC9143127061	about an hour ago	90% (36/40 Checks)
NC041142	about an hour ago	0% (0/40 Checks)
NC043020	about an hour ago	0% (0/40 Checks)

List of compliant checks and computers

You can configure the view according to the information that you want to display by using the Configure View option.

Figure 31. Configure View Option

Name	Desired Values	Compliance
Cumulative state of requirement pcidss-10.1	Component checks: -	0% (3/3 Computers)
Cumulative state of requirement pcidss-10.2	Component checks: -	0% (3/3 Computers)
Cumulative state of requirement pcidss-10.2.1	Component checks: -	33% (1/2/3 Computers)
Cumulative state of requirement pcidss-10.2.2	Component checks: -	33% (1/2/3 Computers)
Cumulative state of requirement pcidss-10.2.3	Component checks: -	33% (1/2/3 Computers)
Cumulative state of requirement pcidss-10.2.4	Component checks: -	0% (3/3 Computers)
Cumulative state of requirement pcidss-10.2.6	Component checks: -	33% (1/2/3 Computers)

In this example, use Filters to specify that you want to view only the checks and computers that compliant to PCI DSS requirement 10.

Figure 32. Configure View Dialog

Configure View

Options
 Autosize Columns

Columns

Check

<input checked="" type="checkbox"/> Check Name	<input type="checkbox"/> Source ID
<input type="checkbox"/> Category	<input type="checkbox"/> Source Release Date
<input type="checkbox"/> Source	<input type="checkbox"/> Source Severity

Computer

<input checked="" type="checkbox"/> Computer Name	<input type="checkbox"/> DNS Name
<input type="checkbox"/> Data Source Name	<input type="checkbox"/> IP Address
<input checked="" type="checkbox"/> Last Seen	<input type="checkbox"/> Computer ID
<input type="checkbox"/> Operating System	

Check Result

<input type="checkbox"/> Desired Values	<input checked="" type="checkbox"/> Compliance
<input type="checkbox"/> Overridden	<input type="checkbox"/> Measured Values
<input type="checkbox"/> State	

Time Range

All

Last 3 days

03/07/2016 to 03/22/2016

Filters

Specify the report filter which matches **all** of the following conditions:

State	in set	Compliant	<input type="button" value="−"/>	<input type="button" value="+"/>
-------	--------	-----------	----------------------------------	----------------------------------

This view shows which computers and checks are in compliance with a particular requirement checklist, in this case, requirement 10.

Figure 33. Report configured to show compliance to a specific requirement

Check Name	Computer Name	Last Seen	Compliance
Cumulative state of requirement pcidss-10.2.1	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.2.2	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.2.3	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.2.6	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.3.1	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.3.2	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.3.3	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.3.4	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.3.5	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.3.6	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.4	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.4.1	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-10.4.1.a	NC9143127061	about an hour ago	Compliant

You can also configure the view to show computers and checks that are not in compliance with a particular requirement checklist.

PCI DSS Milestones Reporting

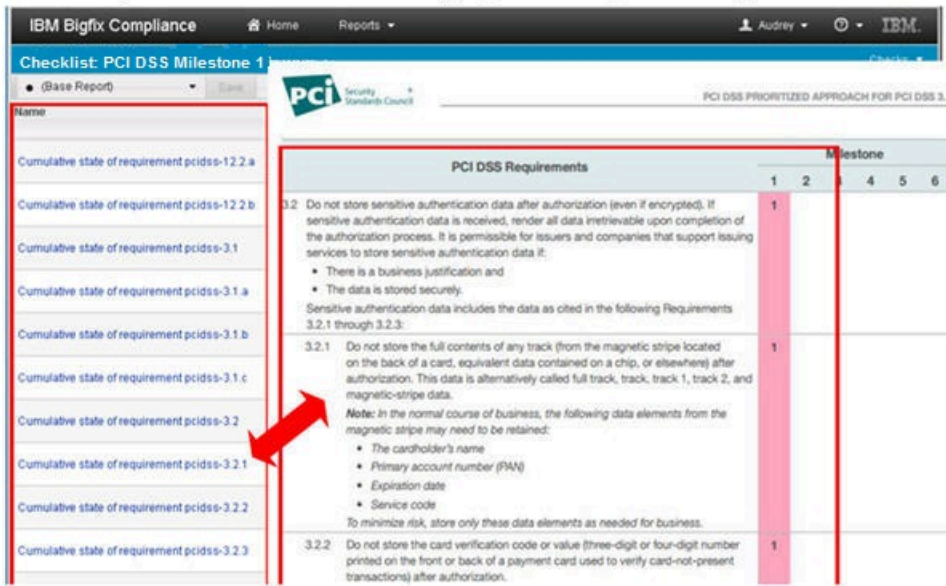
BigFix Compliance PCI Add-on provides additional reports to show a cumulative compliance state of your endpoints based on the PCI DSS Milestones.

To view the PCI DSS Requirements reports, complete the steps in [Setting up custom reporting for BigFix Compliance Analytics V1.8 and earlier \(on page 22\)](#).

The PCI DSS Milestones reports are generated based on the *Prioritized Approach for PCI DSS* document. The mapping was used in creating the checklists for the prioritized approach.

Figure 34. PCI DSS Milestone mapping

Checks List for PCI DSS Milestone 1 and mapping to PCI DSS prioritized approach

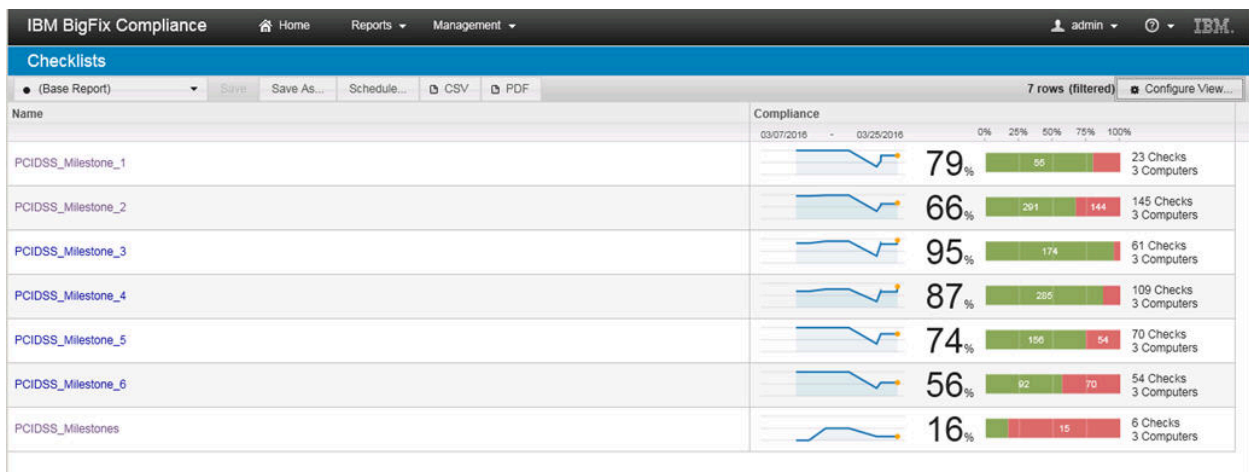


Each milestone has a corresponding checklist and is intended to provide a roadmap to address risks in a prioritized order. Milestones enable merchants to demonstrate progress on compliance process.

To view the list of checklists, click **Reports > Checklists**. There are 7 milestone checklists in total, including the milestone summary checklist.

You can view more information about a checklist by clicking the checklist name from the Checklist view.

Figure 35. PCI DSS Milestone Checklist List



Milestones Summary Checklist Overview

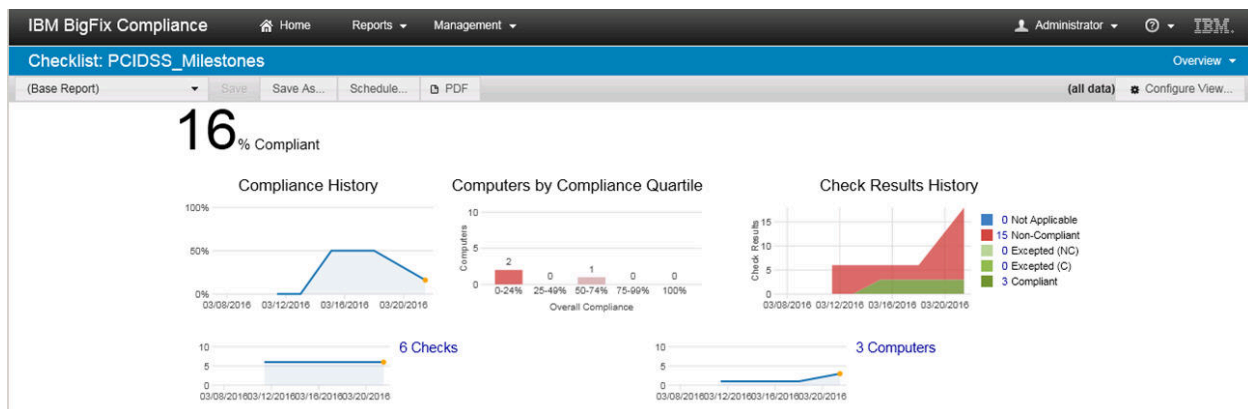
To view the Milestones Summary checklist, click **Reports > Checklists**. Then, select **PCIDSS_Milestones**.

This view shows a summary of all six milestones in a graphic representation of compliance history, computers by compliance quartile, and check results history with an overall compliance percentage shown in the top left corner of the console.

From this view, you can:

- View the list of checks by clicking on the number of checks available.
- View the list of computers by clicking on the number of computers available.
- View the list of checks and computers based on their compliance status.

Figure 36. PCI DSS Milestone Summary Checklist Overview



Checklist Overview

To view an overview of a specific milestone checklist, click **Reports > Checklists**. Then, select a milestone: **PCIDSS_Milestone_<number>**.

The Overview presents a graphic representation of compliance history, computers by compliance quartile, and check results history with an overall compliance percentage shown in the top left corner of the console.

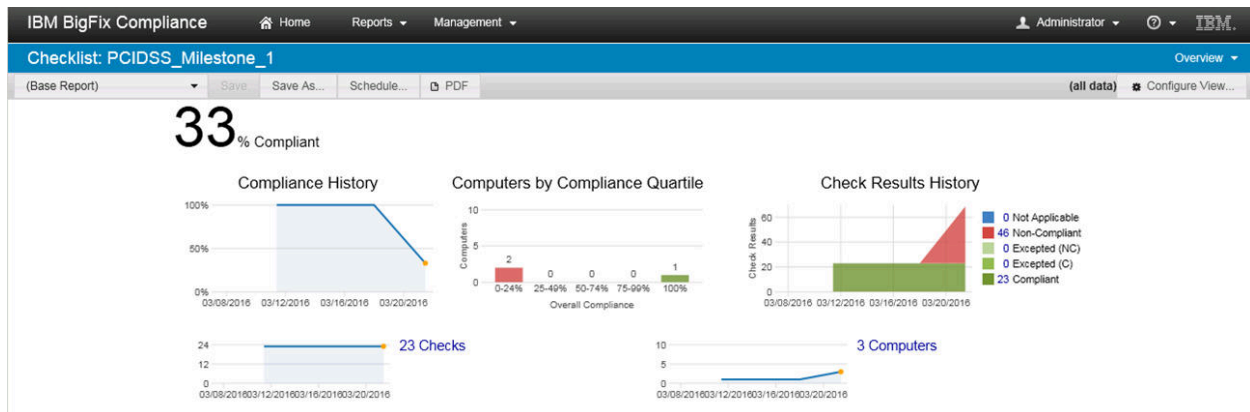
From this view, you can:

- View the list of checks by clicking on the number of checks available.

- View the list of computers by clicking on the number of computers available.
- View the list of checks and computers based on their compliance status.

In this example, you can see the overview of the PCIDSS_Milestone_1 checklist.

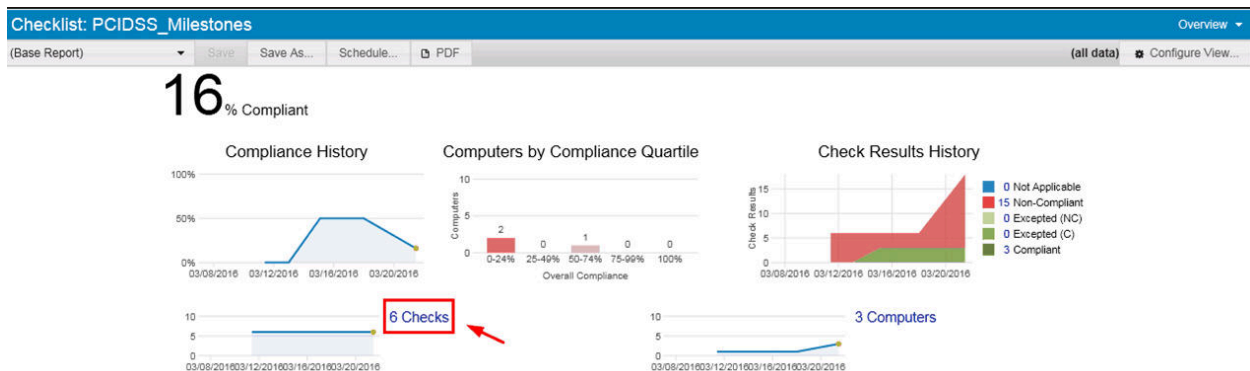
Figure 37. PCI DSS Milestone Checklist Overview



Checks List

You can view the available checks in a checklist in detail by drilling down to the checks. You can do this by clicking the number of checks displayed on the Checklist Overview page.

Figure 38. PCI DSS Milestone Checklist Overview - Checks Link



The Checks List report shows the list of checks in the given scope together with attributes of each check and the overall, historical aggregate compliance results (the aggregate of all visible computer's pass and fail score) of each check.

Figure 39. PCI DSS Milestone Check List

Name	Desired Values	Compliance
Cumulative state of requirement pcidss-1.1.2	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-1.1.2.a	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-1.1.2.b	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-1.1.3	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-12.2	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-12.2.a	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-12.2.b	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-3.1	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-3.1.a	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-3.1.b	Component checks: -	33% 1 2 3 Computers

List of Computers

You can view the list of computers that are relevant to a specific milestone. To view this report, click the number of computers displayed on the Checklist Overview page.

Figure 40. PCI DSS Milestone Check Overview - Computers Link



This view lists all the computers that are applicable to a particular milestone checklist, in this case, milestone 1.

Figure 41. PCI DSS Milestone Check Overview - Computers Link

Computer Name	Last Seen	Compliance
NC9143127061	about an hour ago	100% 23 23 Checks
NC041142	about an hour ago	0% 23 23 Checks
NC043020	about an hour ago	0% 23 23 Checks

List of compliant checks and computers

You can configure the view according to what information you want to display by using the Configure View option.

Figure 42. Configure View Option

Name	Desired Values	Compliance
Cumulative state of requirement pcidss-1.1.2	Component checks: -	03/07/2016 - 03/22/2016 33% 1 2 3 Computers
Cumulative state of requirement pcidss-1.1.2.a	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-1.1.2.b	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-1.1.3	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-12.2	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-12.2.a	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-12.2.b	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-3.1	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-3.1.a	Component checks: -	33% 1 2 3 Computers
Cumulative state of requirement pcidss-3.1.b	Component checks: -	33% 1 2 3 Computers

In this example, use Filters to specify that you want to view only the checks and computers that compliant to PCI DSS milestone 1.

Figure 43. Configure View Dialog

Configure View

Options
 Autosize Columns

Columns

Check

Check Name Source ID
 Category Source Release Date
 Source Source Severity

Computer

Computer Name DNS Name
 Data Source Name IP Address
 Last Seen Computer ID
 Operating System

Check Result

Desired Values Compliance
 Overridden Measured Values
 State

Time Range

All
 Last 3 days
 03/07/2016 to 03/22/2016

Filters

Specify the report filter which matches **all** of the following conditions:

State in set Compliant

Submit Cancel

This view shows which computers and checks are in compliance with a particular milestone checklist, in this case, milestone 1.

Figure 44. Report configured to show compliance to a specific requirement

IBM BigFix Compliance			
Checklist: PCIDSS_Milestone_1			
Check Name	Computer Name	Last Seen	Compliance
Cumulative state of requirement pcidss-1.1.2	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-1.1.2.a	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-1.1.2.b	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-1.1.3	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-12.2	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-12.2.a	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-12.2.b	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-3.1	NC9143127061	about an hour ago	Compliant
Cumulative state of requirement pcidss-3.1.a	NC9143127061	about an hour ago	Compliant

You can also configure the view to show computers and checks that are not in compliance with a particular milestone checklist.

Saving customized reports

Use the Saved Reports feature to retain a specific format for the report without creating the same settings for future use. The displayed columns and filters you used to customize the view are also saved.

1. Navigate to the report that you want to save.
2. Use the Configure View option to set the information that you want to show in the report.
3. Add a filter to specify a specific condition for the report view and click **Submit**.

Figure 45. Add filters

Configure View

Options

Autosize Columns

Columns

Checklist

ID Data Source Name

Name Compliance

Scoped Compliance

Check Count Total Excepted (NC)

Computer Count Total Non-Compliant

Total Compliant Total Not Applicable

Total Excepted (C) Compliance Percentage

Time Range

All

Last 3 days

03/07/2016 to 03/25/2016

03/08/2016 03/10/2016 03/12/2016 03/14/2016 03/16/2016 03/18/2016 03/20/2016 03/22/2016 03/24/2016

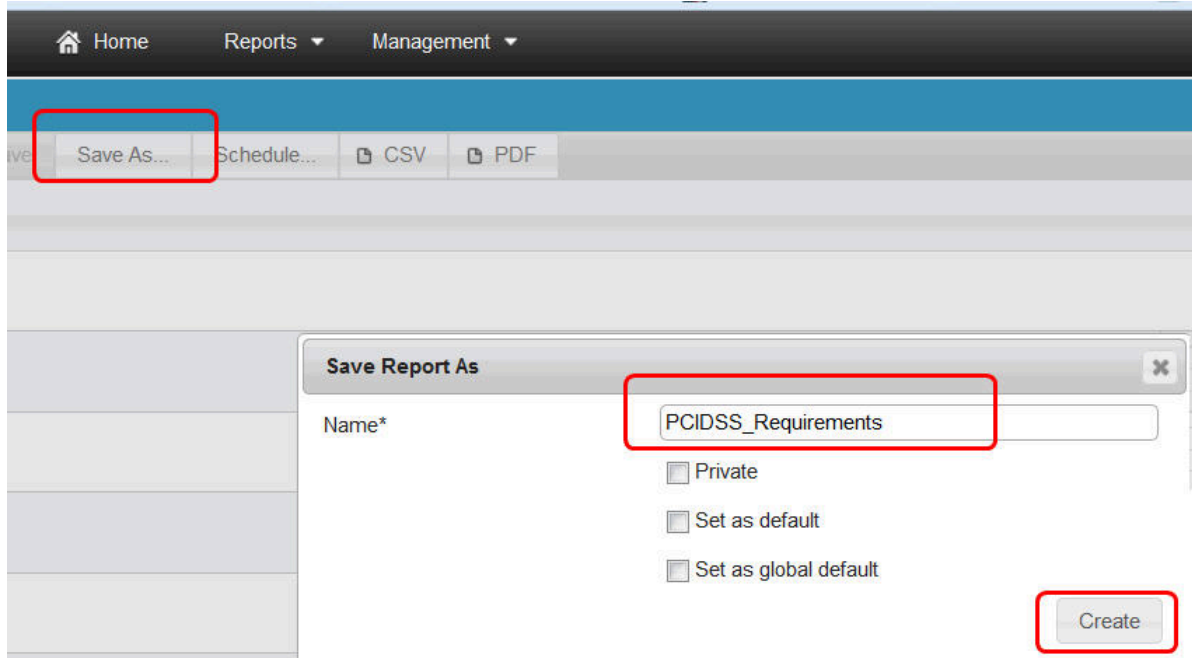
Filters

Specify the report filter which matches of the following conditions:

4. To save the report, click **Save As**.

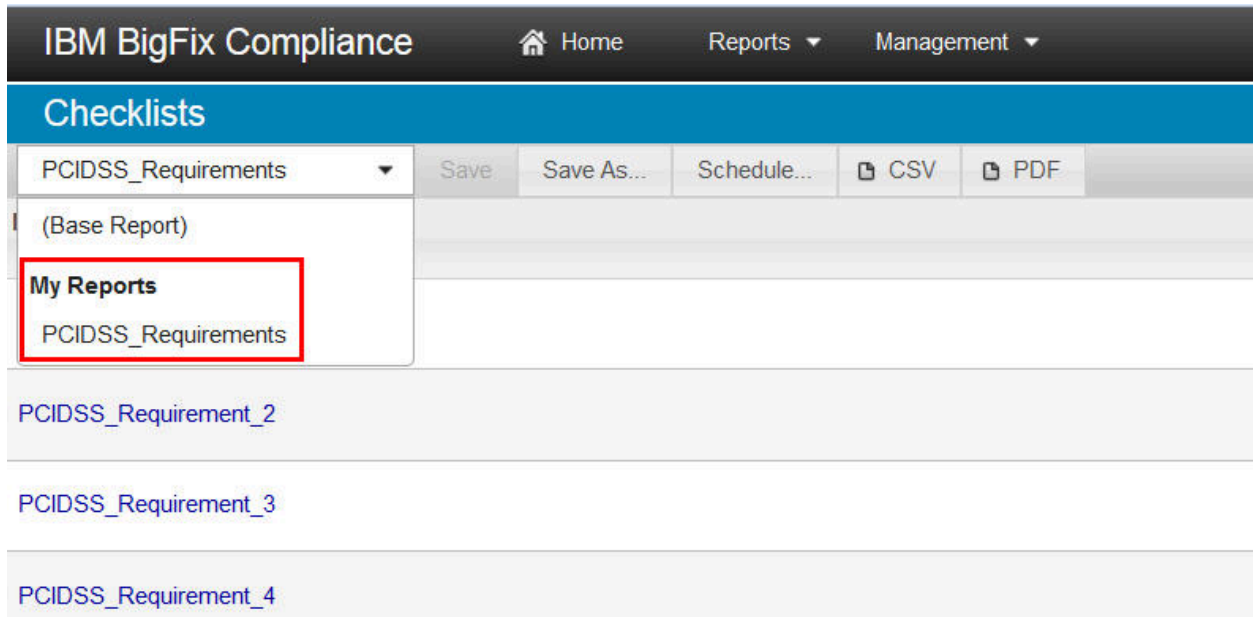
5. Enter a name to identify the report to be saved and click **Create**.

Figure 46. Save as report



The saved report becomes available in the Saved Reports list report and visible in the drop-down box on the left side of the sub-navigation area when viewing that report type.

Figure 47. My Reports

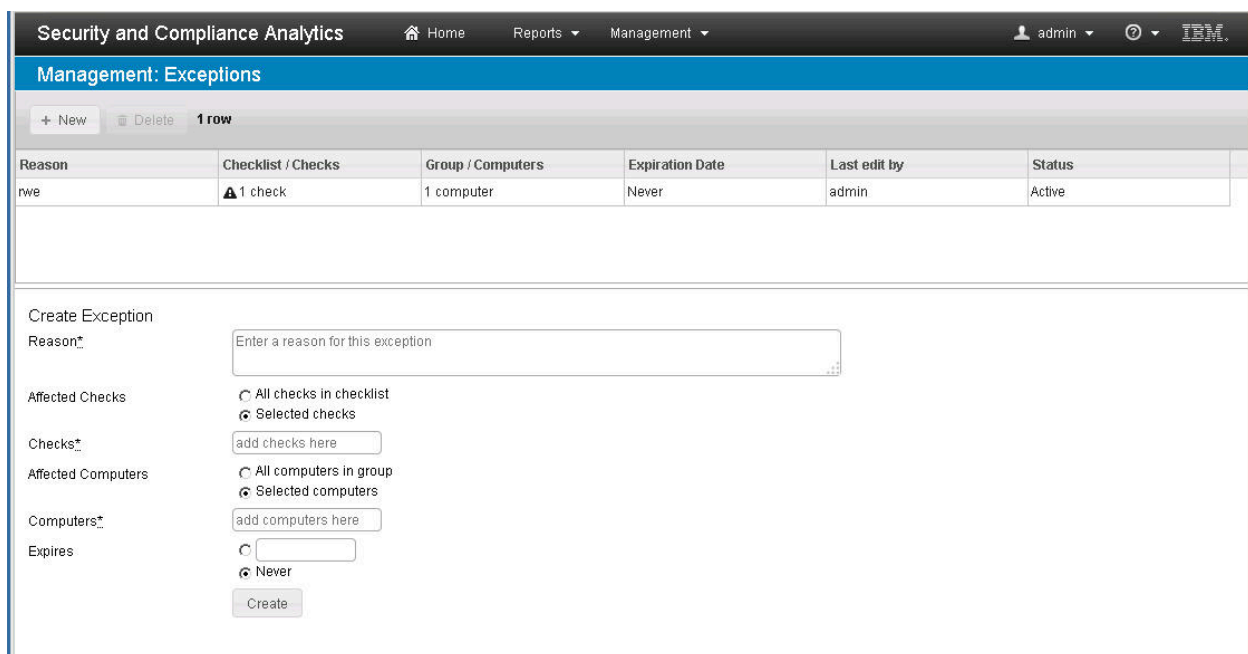


Creating exceptions

You can file for the endpoint to be excluded from the PCI DSS checks if some endpoints require compliance to older policies or standards.

Security and Compliance Analytics (SCA), which is now known as BigFix Compliance Analytics, provides a separate interface for Exception Management where you can set exceptions to exclude data from your compliance reports.

Figure 48. Exceptions page



The screenshot displays the 'Management: Exceptions' interface. At the top, there is a navigation bar with 'Home', 'Reports', and 'Management' menus, and a user profile for 'admin'. Below the navigation bar, the page title is 'Management: Exceptions'. There are '+ New' and 'Delete' buttons, and a '1 row' indicator. A table lists the exception details:

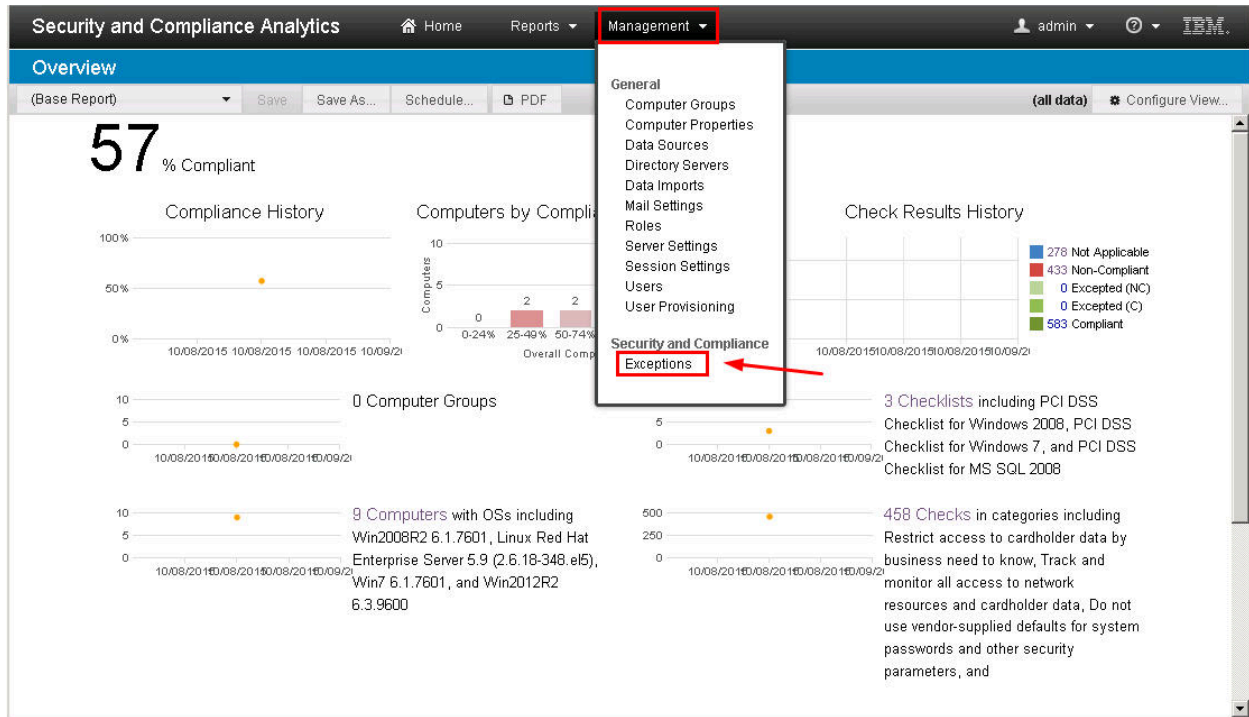
Reason	Checklist / Checks	Group / Computers	Expiration Date	Last edit by	Status
nwe	▲ 1 check	1 computer	Never	admin	Active

Below the table is a 'Create Exception' form with the following fields and options:

- Reason***: A text input field with the placeholder 'Enter a reason for this exception'.
- Affected Checks**: Radio buttons for 'All checks in checklist' and 'Selected checks' (selected).
- Checks***: A text input field with the placeholder 'add checks here'.
- Affected Computers**: Radio buttons for 'All computers in group' and 'Selected computers' (selected).
- Computers***: A text input field with the placeholder 'add computers here'.
- Expires**: Radio buttons for a date input field and 'Never' (selected).
- Create**: A button to submit the form.

To access the Exceptions interface, click **Management > Exceptions**.

Figure 49. Management menu



You can create and edit exceptions for checks, computers, computer groups, and checklists with or without an expiration date.

Chapter 5. Resources

You can find more information about Security Configuration Management and PCI DSS in the following resources.

Each document opens in a new window.

- [PCI DSS Requirements and Security Assessment Procedures](#)
- [PCI DSS Release Notes](#)
- [Security Configuration Management User's Guide](#)
- [Security and Compliance Analytics Setup Guide](#)
- [Security and Compliance developerWorks wiki](#)

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or

any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).

Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.