

IBM PowerSC

Express Edition

Version 1.1.3

*PowerSC Express Edition*

**IBM**



IBM PowerSC

Express Edition

Version 1.1.3

*PowerSC Express Edition*

**IBM**

**Note**

Before using this information and the product it supports, read the information in "Notices" on page 111.

This edition applies to IBM PowerSC Express Edition Version 1.1.3 and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2012, 2014.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>About this document . . . . .</b>	<b>v</b>	Monitoring systems for continued compliance with AIX Profile Manager . . . . .	101
<b>What's new in PowerSC Express Edition 1.1.3 . . . . .</b>	<b>1</b>	Configuring PowerSC Security and Compliance Automation . . . . .	101
<b>PowerSC Express Edition Release Notes Version 1.1.3. . . . .</b>	<b>3</b>	Configuring PowerSC compliance options settings . . . . .	102
<b>PowerSC Express Edition 1.1.3 concepts</b>	<b>5</b>	Configuring PowerSC compliance from the command line . . . . .	102
<b>Installing PowerSC Express Edition Version 1.1.3. . . . .</b>	<b>7</b>	Configuring PowerSC compliance with AIX Profile Manager . . . . .	103
<b>Security and Compliance Automation ..</b>	<b>9</b>	<b>PowerSC Real Time Compliance . ..</b>	<b>105</b>
Security and Compliance Automation concepts . . . . .	9	Installing PowerSC Real Time Compliance. . . . .	105
Department of Defense STIG compliance . . . . .	9	Configuring PowerSC Real Time Compliance. . . . .	105
Payment Card Industry - Data Security Standard compliance . . . . .	80	Identifying files monitored by the PowerSC Real Time Compliance feature . . . . .	106
Sarbanes-Oxley Act and COBIT compliance. . . . .	93	Setting alerts for PowerSC Real Time Compliance . . . . .	106
Health Insurance Portability and Accountability Act (HIPAA) . . . . .	94	<b>PowerSC Express Edition commands</b>	<b>107</b>
Managing Security and Compliance Automation ..	99	psccxpert Command . . . . .	107
Investigating a failed rule . . . . .	100	<b>Notices . . . . .</b>	<b>111</b>
Updating the failed rule. . . . .	100	Privacy policy considerations . . . . .	113
Creating custom security configuration profile	100	Trademarks . . . . .	113
Testing the applications with AIX Profile Manager . . . . .	101	<b>Index . . . . .</b>	<b>115</b>



---

## About this document

This document provides system administrators with complete information about file, system, and network security.

### Highlighting

The following highlighting conventions are used in this document:

<b>Bold</b>	Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects.
<i>Italics</i>	Identifies parameters whose actual names or values are to be supplied by the user.
Monospace	Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information you should actually type.

### Case-sensitivity in AIX®

Everything in the AIX operating system is case-sensitive, which means that it distinguishes between uppercase and lowercase letters. For example, you can use the **ls** command to list files. If you type **LS**, the system responds that the command is not found. Likewise, **FILEA**, **FiLea**, and **filea** are three distinct file names, even if they reside in the same directory. To avoid causing undesirable actions to be performed, always ensure that you use the correct case.

### ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.





---

## What's new in PowerSC Express Edition 1.1.3

Read about new or significantly changed information for the What's new in the PowerSC™ Express Edition 1.1.3 topic collection.

### How to see what's new or changed

In this PDF file, you might see revision bars (|) in the left margin that identifies new and changed information.

### December 2014

The following information provides a summary of the new and updated content for PowerSC Express Edition 1.1.3.2:

- Updated the compliance actions for various profile items in “Department of Defense STIG compliance” on page 9.
- Updated the Network File System protocol information in “Payment Card Industry - Data Security Standard compliance” on page 80.
- Updated the compliance actions for various profile items in “Payment Card Industry - Data Security Standard compliance” on page 80.
- Updated the “pscxpert Command” on page 107.
- Replaced references to the **aixpert** command with the **pscxpert** command in various topics.
- Removed and updated obsolete information in various topics.

### April 2014

The following information provides a summary of the new and updated content for PowerSC Express Edition 1.1.3.1:

- Updated the information about the support for the United States Department of Defense STIG in “Department of Defense STIG compliance” on page 9.
- Updated the flags for the “pscxpert Command” on page 107.
- Removed and updated obsolete information in various topics.

### December 2013

The following information provides a summary of the new and updated content for PowerSC Express Edition 1.1.3:

- Added information about the README.ICEexpress file in “Installing PowerSC Express Edition Version 1.1.3” on page 7.
- Updated the information about the support for the Payment Card Industry - Data Security Standard compliance for version 2.0 of the standard in “Payment Card Industry - Data Security Standard compliance” on page 80.
- Updated the path for the **RbacEnablement** command in “Health Insurance Portability and Accountability Act (HIPAA)” on page 94.
- Added the “pscxpert Command” on page 107.
- Updated an example in “pscxpert Command” on page 107.

## **May 2013**

Added a table that describes how the AIX Security Expert feature ensures compliance with the Payment Card Industry - Data Security Standard to “Payment Card Industry - Data Security Standard compliance” on page 80.

## **November 2012**

The following information provides a summary of the new and updated content for PowerSC Express Edition 1.1.2:

- Added documentation that describes the Real Time Compliance feature in “PowerSC Real Time Compliance” on page 105.
- Added documentation for the support of the standards as defined by the “Health Insurance Portability and Accountability Act (HIPAA)” on page 94.

---

## PowerSC Express Edition Release Notes Version 1.1.3

The release notes contain information about changes to PowerSC Express Edition Versions 1.1.3 that were identified after the documentation was completed.

### What's new

Read about new or changed information in the IBM® PowerSC Express Edition release notes topic collection.

#### May 2014

The following information describes new or changed items that were identified after finalizing the IBM PowerSC Express Edition content:

When you migrate partitions with the DataBase, Department of Defense, Department of Defense Version 2, or Payment Card Industry profiles enabled on your Virtual I/O Server (VIOS), secure tunnels are automatically requested for the migration. An update to the secure tunnel migration process will be provided in VIOS Service Pack 2.2.3.3.

#### December 2013

The location of the IBM PowerSC content in the information center was restructured.

### Read this before installation

To view the most current version of the Release Notes, go to the online Release Notes in the Knowledge Center ([http://www.ibm.com/support/knowledgecenter/SSNRQU\\_1.1.3/com.ibm.powersc113.ee/powersc\\_ee\\_rn.htm](http://www.ibm.com/support/knowledgecenter/SSNRQU_1.1.3/com.ibm.powersc113.ee/powersc_ee_rn.htm)).

PowerSC Express Edition is a licensed program and is not included with the AIX operating system.

**Note:** This software might contain errors that could result in a critical business impact. Install the latest available fixes prior to using this software.

### Installation, migration, upgrade, and configuration information

For information about installing PowerSC, see “Installing PowerSC Express Edition Version 1.1.3” on page 7.

#### | Fix for Live Partition Mobility (LPM) using IP Security (IPSec) tunnels

- | A fix for secure tunnel migration support will be available in VIOS service pack 2.2.3.3. This service pack will address APAR IV59934 and should be installed on the VIOS servers.



## PowerSC Express Edition 1.1.3 concepts

This overview of PowerSC explains the features, components, and the hardware support related to the PowerSC Express Edition feature.

PowerSC Express Edition 1.1.3 provides security and control of the systems operating within a cloud or in virtualized data centers, and provides an enterprise view and management capabilities. PowerSC Express Edition is a suite of features that includes Security and Compliance Automation and Real Time Compliance. The security technology that is placed within the virtualization layer provides additional security to stand-alone systems.

The following table provides details about the editions, the features included in the editions, the components, and the processor-based hardware on which each component is available.

*Table 1. PowerSC Express Edition components, description, operating system supported, and hardware supported*

Components	Description	Operating system supported	Hardware supported
Security and Compliance Automation	Automates the setting, monitoring, and auditing of security and compliance configuration for the following standards: <ul style="list-style-type: none"> <li>• Payment Card Industry Data Security Standard (PCI DSS)</li> <li>• Sarbanes-Oxley Act and COBIT compliance (SOX/COBIT)</li> <li>• U.S. Department of Defense (DoD) STIG</li> <li>• Health Insurance Portability and Accountability Act (HIPAA)</li> </ul>	<ul style="list-style-type: none"> <li>• AIX 5.3</li> <li>• AIX 6.1</li> <li>• AIX 7.1</li> </ul>	<ul style="list-style-type: none"> <li>• POWER5</li> <li>• POWER6®</li> <li>• POWER7®</li> </ul>
Real Time Compliance	Monitors an enabled AIX system to maintain security and provides alerts when a change to the system violates a rule that is identified in the configuration policy.	<ul style="list-style-type: none"> <li>• IBM AIX 6 with Technology Level 7, or later, with AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 6.1.7.0), or later</li> <li>• IBM AIX 7 with Technology Level 1, or later, with AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 7.1.1.0), or later</li> </ul>	There is no specific hardware requirement.



---

## Installing PowerSC Express Edition Version 1.1.3

PowerSC Express Edition includes the `powerscExp.ice` package. The `powerscExp.ice` package supports AIX 5.3, AIX 6.1 and AIX Version 7.1.

The `powerscExp.ice` package must be installed on all AIX systems that require the security and compliance feature of the PowerSC Express Edition.

Install PowerSC Express Edition by using one of the following interfaces:

- The **installp** command from the command-line interface (CLI)
- The SMIT interface

To install the PowerSC Express Edition by using the SMIT interface, complete the following steps:

1. Run the following command:  

```
% smitty installp
```
2. Select the **Install Software** option.
3. Select the input device or directory for the software to specify the location and the installation file of the IBM Compliance Expert installation image. For example, if the installation image has the directory path and file name `/usr/sys/inst.images/powerscExp.ice`, you must specify the file path in the **INPUT** field.
4. View and accept the license agreement. Accept the license agreement by using the down arrow to select **ACCEPT new license agreements**, and press the tab key to change the value to **Yes**.
5. Press **Enter** to start the installation.
6. Verify that the command status is **OK** after the installation is complete.

A readme file named `README.ICEexpress` is installed in the `/etc/security/aixpert` directory. This file contains the implementation details for the compliance profiles that are included with PowerSC Express Edition.

### Viewing the software license

The software license can be viewed in the CLI by using the following command:

```
% installp -lE -d path/filename
```

Where *path/filename* specifies the PowerSC Standard Edition installation image.

For example, you can enter the following command using the CLI to specify the license information related to the PowerSC Express Edition:

```
% installp -lE -d /usr/sys/inst.images/powerscExp.ice
```





---

## Security and Compliance Automation

AIX Profile Manager manages predefined profiles for security and compliance. The PowerSC Real Time Compliance continuously monitors enabled AIX systems to ensure that they are configured consistently and securely.

The XML profiles automate the recommended AIX system configuration of IBM to be consistent with the Payment Card Data Security Standard, the Sarbanes-Oxley Act, or the U.S. Department of Defense UNIX Security Technical Implementation Guide and Health Insurance Portability and Accountability Act (HIPAA). The organizations that comply with the security standards must use the predefined system security settings.

The AIX Profile Manager operates as an IBM Systems Director plug-in that simplifies applying security settings, monitoring security settings, and auditing security settings for both the AIX operating system and Virtual I/O Server (VIOS) systems. To use the security compliance feature, the PowerSC application must be installed on the AIX managed systems that conform to the compliance standards. The Security and Compliance Automation feature is included in the PowerSC Express Edition, and the PowerSC Standard Edition.

The PowerSC Express Edition installation package, 5765-G82, must be installed on AIX managed systems. The installation package installs the `powerscExp.ice` fileset that can be implemented on the system by using the AIX Profile Manager or the `pscexpert` command. PowerSC with IBM Compliance Expert Express (ICEE) compliance is enabled to manage and improve the XML profiles. The XML profiles are managed by the AIX Profile Manager.

- | **Note:** Install all applications on the system before you apply a security profile.

---

## Security and Compliance Automation concepts

The PowerSC security and compliance feature is an automated method to configure and audit AIX systems in accordance with the U.S. Department of Defense (DoD) Security Technical Implementation Guide (STIG).

PowerSC helps to automate the configuration and monitoring of systems that must be compliant with the Payment Card Industry (PCI) data security standard (DSS) version 1.2. Therefore, PowerSC security and compliance feature is an accurate and complete method of security configuration automation that is used to meet the IT compliance requirements of the DoD UNIX STIG, the PCI DSS, the Sarbanes-Oxley act, COBIT compliance (SOX/COBIT), and the Health Insurance Portability and Accountability Act (HIPAA).

**Note:** PowerSC security and compliance updates the existing xml profiles that are used by IBM Compliance Expert express (ICEE) edition. The PowerSC Express Edition xml profiles can be used with the `pscexpert` command, similar to ICEE.

The preconfigured compliance profiles delivered with the PowerSC Express Edition reduce the administrative workload of interpreting compliance documentation and implementing the standards as specific system configuration parameters. This technology reduces the cost of compliance configuration and auditing by automating the processes. IBM PowerSC Express Edition is designed to help effectively manage the system requirement associated with external standard compliance that can potentially reduce costs and improve compliance.

## Department of Defense STIG compliance

The U.S. Department of Defense (DoD) requires highly secure computer systems. This level of security and quality defined by DoD meets with the quality and customer base of AIX on Power Systems™ server.

A secure operating system, such as AIX, must be configured accurately to attain the specified security goals. The DoD recognized the need for security configurations of all operating systems in Directive 8500.1. This directive established the policy and assigned the responsibility to the US defense information security agency (DISA) to provide security configuration guidance.

DISA developed the principles and guidelines in the UNIX Security Technical Implementation Guide (STIG) that provides an environment that meets or exceeds the security requirements of DoD systems that are operating at the mission assurance category (MAC) II sensitive level, which contains sensitive information. The US DoD has stringent IT security requirements and enumerated the details of the required configuration settings to ensure that the system operates in a secure manner. You can leverage the required expert guidance. PowerSC Express Edition helps to automate the process of configuring the settings as defined by DoD.

**Note:** All of the custom script files that are provided to maintain DoD compliance are in the `/etc/security/psceexpert/dodv2` directory.

Beginning with the 1.1.3.1 service pack of IBM PowerSC, PowerSC supports the requirements of the version 1 release 2 of the AIX DoD STIG. A summary of the requirements and how to ensure that compliance are provided in the tables that follow.

*Table 2. DoD general requirements*

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
AIX00020	2	AIX Trusted Computing Base software must be implemented.	<p><b>Location</b>  <code>/etc/security/psceexpert/dodv2/trust</code></p> <p><b>Compliance action</b>            Ensures that the system meets the specified requirements.</p>
AIX00040	2	The <code>securetcpip</code> command must be used.	<p><b>Location</b>  <code>/etc/security/psceexpert/dodv2/dodsecuretcpip</code></p> <p><b>Compliance action</b>            Ensures that the system meets the specified requirements.</p>
AIX00060	2	The system must be checked weekly for unauthorized <code>setuid</code> files, and unauthorized modification to authorized <code>setuid</code> files.	<p><b>Location</b>  <code>/etc/security/psceexpert/dodv2/trust</code></p> <p><b>Compliance action</b>            Checks weekly to identify changes to the specified files.</p>
AIX00080	1	The <code>SYSTEM</code> attribute must not be set to <i>none</i> for any account.	<p><b>Location</b>  <code>/etc/security/psceexpert/dodv2/SYSattr</code></p> <p><b>Compliance action</b>            Ensures that the specified attribute is set to a value other than <i>none</i>.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the <code>DoDv2_to_AIXDefault.xml</code> file. You must manually change this setting.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
AIX00200	2	The system must not allow directed broadcasts to move through the gateway.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the direct_broadcast network option to 0.</p>
AIX00210	2	The system must provide protection from Internet Control Message Protocol (ICMP) attacks on TCP connections.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the tcp_icmpsecure network option to 1.</p>
AIX00220	2	The system must provide protection for the TCP stack against connection resets, synchronize (SYN), and data injection attacks.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Ensures that the value for the tcp_tcpsecure network option is set to 7.</p>
AIX00230	2	The system must provide protection against IP fragmentation attacks.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the ip_nfrag network option to 200.</p>
AIX00300	1,2,3	The system must not have the bootp service active.	<p><b>Location</b> /etc/security/pscxpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the specified service.</p>
AIX00310	2	The /etc/ftpaccess.ct1 files must exist.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2loginherald</p> <p><b>Compliance action</b> Ensures that the file exists.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN000020	2	The system must require authentication when starting in single-user mode.	<p><b>Location</b> /etc/security/pscxpert/dodv2/rootpasswd_home</p> <p><b>Compliance action</b> Ensures that the root account for any bootable partitions has a password in the /etc/security/passwd file. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN000100	1	The operating system must be a supported release.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2cat1</p> <p><b>Compliance action</b> Displays the results of the specified rule tests.</p>
GEN000120	2	The most current system security patches and updates must be installed.	<p><b>Location</b> /usr/sbin/instfix -i  /etc/security/pscxpert/dodv2/dodv2cat1</p> <p><b>Compliance action</b> Configure this using the Trusted Network Connect feature.</p>
GEN000140	2	The system must be checked weekly for unauthorized setuid files, and unauthorized modification to authorized setuid files.	<p><b>Location</b> /etc/security/pscxpert/dodv2/trust</p> <p><b>Compliance action</b> Checks weekly to identify changes to the specified files.</p>
GEN000220	2	The system must be checked weekly for unauthorized setuid files, and unauthorized modification to authorized setuid files.	<p><b>Location</b> /etc/security/pscxpert/dodv2/trust</p> <p><b>Compliance action</b> Checks weekly to identify changes to the specified files.</p>
GEN000240	2	The system clock must be synchronized to an authoritative Department of Defense (DoD) time source.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2cmntrows</p> <p><b>Compliance action</b> Ensures that the system clock is compliant.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN000241	2	The system clock must be synchronized continuously, or at least daily.	<p><b>Location</b> /etc/security/psceexpert/dodv2/dodv2cmntrows</p> <p><b>Compliance action</b> Ensures that the system clock is compliant.</p>
GEN000242	2	The system must use at least two time sources for clock synchronization.	<p><b>Location</b> /etc/security/psceexpert/dodv2/dodv2netrules</p> <p><b>Compliance action</b> Ensures that more than one time source is used for synchronizing the clock.</p>
GEN000280	2	Direct logins to the following types of accounts must not be allowed: <ul style="list-style-type: none"> <li>• application</li> <li>• default</li> <li>• shared</li> <li>• utility</li> </ul>	<p><b>Location</b> /etc/security/psceexpert/dodv2/lockacc_rlogin</p> <p><b>Compliance action</b> Prevents direct logins to the specified accounts.</p>
GEN000290	2	The system must not have unnecessary accounts.	<p><b>Location</b> /etc/security/psceexpert/dodv2/lockacc_rlogin</p> <p><b>Compliance action</b> Ensures that there are no unused accounts.</p>
GEN000300 (related to GEN000320, GEN000380, GEN000880)	2	All accounts on the system must have unique user or account names, and unique user or account passwords.	<p><b>Location</b> /etc/security/psceexpert/dodv2/grpusrpass_chk</p> <p><b>Compliance action</b> Ensures that all accounts meet the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN000320 (related to GEN000300, GEN000380, GEN000880)	2	All accounts on the system must have unique user or account names, and unique user or account passwords.	<p><b>Location</b> /etc/security/psceexpert/dodv2/grpusrpass_chk</p> <p><b>Compliance action</b> Ensures that all accounts meet the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN000340	2	User IDs (UIDs) and Group IDs (GIDs) that are reserved for system accounts must not be assigned to non-system accounts or non-system groups.	<p><b>Location</b> /etc/security/pscxpert/dodv2/account</p> <p><b>Compliance action</b> This setting is automatically enabled to enforce this rule.</p>
GEN000360	2	UIDs and GIDs that are reserved for system accounts must not be assigned to non-system accounts or non-system groups.	<p><b>Location</b> /etc/security/pscxpert/dodv2/account</p> <p><b>Compliance action</b> This setting is automatically enabled to enforce this rule.</p>
GEN000380 (related to GEN000300, GEN000320, GEN000880)	2	All accounts on the system must have unique user or account names, and unique user or account passwords.	<p><b>Location</b> /etc/security/pscxpert/dodv2/grpusrpass_chk</p> <p><b>Compliance action</b> Ensures that all accounts meet the specified requirements.</p>
GEN000400	2	The Department of Defense (DoD) login banner must be displayed immediately before, or as part of, console login prompts.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2loginherald</p> <p><b>Compliance action</b> Displays the required banner.</p>
GEN000402	2	The DoD login banner must be displayed immediately before, or as part of, graphical desktop environment login prompts.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2loginherald</p> <p><b>Compliance action</b> The login banner is set to the Department of Defense banner.</p>
GEN000410	2	The File Transfer Protocol over SSL (FTPS) or File Transfer Protocol (FTP) service on the system must be configured with the DoD login banner.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2loginherald</p> <p><b>Compliance action</b> Displays the banner when you use FTP.</p>
GEN000440	2	Successful and unsuccessful attempts to log in and log out must be recorded.	<p><b>Location</b> /etc/security/pscxpert/dodv2/loginout</p> <p><b>Compliance action</b> Enables the required logging.</p>
GEN000452	2	The system must display the date and time of the last successful account login at the time of each log in.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Displays the required information.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN000460	2	This rule disables an account after 3 consecutive failed logon attempts.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chusrattrdod</p> <p><b>Compliance action</b> Sets the login attempt limit to the specified value.</p>
GEN000480	2	This rule sets the login delay time to 4 seconds.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chdefstanzadod</p> <p><b>Compliance action</b> Sets the login delay time to the required value.</p>
GEN000540	2	This rule ensures the system global password configuration files are configured according to password requirements.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chusrattrdod</p> <p><b>Compliance action</b> Sets the required password settings.</p>
GEN000560	1	All accounts on the system must have valid passwords.	<p><b>Location</b> /etc/security/pscxpert/dodv2/grpusrpass_chk</p> <p><b>Compliance action</b> Ensures that accounts have passwords.</p>
GEN000580	2	This rule ensures that all passwords contain a minimum of 14 characters.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chusrattrdod</p> <p><b>Compliance action</b> Sets the minimum password length to 14 characters.</p>
GEN000585	2	The system must use a Federal Information Processing Standards (FIPS) 140-2 approved cryptographic hashing algorithm for generating account password hashes.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fipspasswd</p> <p><b>Compliance action</b> Ensures that the password hashes use an approved hashing algorithm.</p>
GEN000590	2	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fipspasswd</p> <p><b>Compliance action</b> Ensures that the password hashes use an approved hashing algorithm.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN000595	2	Use a FIPS 140-2 approved cryptographic hashing algorithm when generating the password hashes that are stored on the system.	<p><b>Location</b> /etc/security/pwscexpert/dodv2/fipspasswd</p> <p><b>Compliance action</b> Ensures that the password hashes use an approved hashing algorithm.</p>
GEN000640	2	This rule requires a minimum of one non-alphabetic character in a password	<p><b>Location</b> /etc/security/pwscexpert/dodv2/chusrattrdod</p> <p><b>Compliance action</b> Sets the minimum number of non-alphabetic characters in a password to 1.</p>
GEN000680	2	This rule ensures that passwords contain no more than three consecutive repeating characters	<p><b>Location</b> /etc/security/pwscexpert/dodv2/chusrattrdod</p> <p><b>Compliance action</b> Sets the maximum number of repeating characters in a password to 3.</p>
GEN000700	2	This rule ensures the system global password configuration files are configured according to password requirements.	<p><b>Location</b> /etc/security/pwscexpert/dodv2/chusrattrdod</p> <p><b>Compliance action</b> Ensures that the password configuration files meet the requirements.</p>
GEN000740	2	All non-interactive and automated processing account passwords must be locked (GEN000280). Direct logins must not be allowed to shared or default or application or utility accounts. (GEN002640) Default system accounts must be disabled or removed.	<p><b>Location</b> /etc/security/pwscexpert/dodv2/loginout  /etc/security/pwscexpert/dodv2/lockacc_rlogin</p> <p><b>Compliance action</b> This setting is automatically enabled.</p>
GEN000740	2	All non-interactive and automated processing account passwords must be changed at least once per year or be locked.	<p><b>Location</b> /etc/security/pwscexpert/dodv2/lockacc_rlogin</p> <p><b>Compliance action</b> Ensures that the specified passwords are changed annually or locked.</p>



Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN000750	2	This rule requires new passwords to contain a minimum of 4 characters that were not in the old password.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chusratrdod</p> <p><b>Compliance action</b> Sets the minimum number of new characters that are required in a new password to 4.</p>
GEN000760	2	Accounts must be locked after 35 days of inactivity.	<p><b>Location</b> /etc/security/pscxpert/dodv2/disableacctdod</p> <p><b>Compliance action</b> Locks accounts after 35 days of inactivity.</p>
GEN000790	2	The system must prevent the use of dictionary words for passwords.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chuserstanzadod</p> <p><b>Compliance action</b> Ensures that the default password that is being set is not weak.</p>
GEN000800	2	This rule ensures that the last five passwords are not reused.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chusratrdod</p> <p><b>Compliance action</b> Ensures that the new password is not the same as any of the last 5 passwords.</p>
GEN000880 (related to GEN000300, GEN000320, GEN000380)	2	All accounts on the system must have unique user or account names, and unique user or account passwords.	<p><b>Location</b> /etc/security/pscxpert/dodv2/grpusrpass_chk</p> <p><b>Compliance action</b> Ensures that all accounts meet the specified requirements.</p>
GEN000900	3	The root user's home directory must not be the root directory (/).	<p><b>Location</b> /etc/security/pscxpert/dodv2/rootpasswd_home</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirement. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN000940	2	The root account's executable search path must be the vendor default, and must contain only absolute paths.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN000945	2	The root account's library search path must be the system default, and must contain only absolute paths.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN000950	2	The root account's list of preloaded libraries must be empty.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN000960 (related to GEN003000, GEN003020, GEN003160, GEN003360, GEN003380)	2	The root account must not have world-writable directories in its executable search path.	<p><b>Location</b> /etc/security/pscxpert/dodv2/rmwpaths</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN000980	2	The system must prevent the root account from directly logging in, except from the system console.	<p><b>Location</b> /etc/security/pscxpert/ dodv2/chuserstanzadod</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN001000	2	Remote consoles must be disabled or protected from unauthorized access.	<p><b>Location</b> /etc/security/pscxpert/ dodv2/remotconsole</p> <p><b>Compliance action</b> Ensures that the specified consoles are disabled.</p>
GEN001020	2	The root account must not be used for direct login.	<p><b>Location</b> /etc/security/pscxpert/ dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Disables the root account from logging in directly.</p>
GEN001060	2	The system must log successful and unsuccessful attempts to access the root account.	<p><b>Location</b> /etc/security/pscxpert/ dodv2/loginout</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN001100	1	Root passwords must never be passed over a network in text form.	<p><b>Location</b> /etc/security/pscxpert/ dodv2/chuserstanzadod</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN001120	2	The system must not allow root login by using the SSH protocol.	<p><b>Location</b> /etc/security/pscxpert/ dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Disables root login for SSH.</p>
GEN001440	3	All interactive users must be assigned a home directory in the /etc/passwd file.	<p><b>Location</b> /etc/security/pscxpert/ dodv2/grpusrpass_chk</p> <p><b>Compliance action</b> Ensures that all interactive users have the specified directory.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001475	2	The /etc/group file must not contain any group password hashes.	<p><b>Location</b> /etc/security/pscxpert/dodv2/passwdhash</p> <p><b>Compliance action</b> Ensures that there are no group password hashes in the specified file. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001600	2	Run control scripts' executable search paths must contain only absolute paths.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001605	2	Run control scripts' library search paths must contain only absolute paths.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001610	2	Run control scripts' lists of preloaded libraries must contain only absolute paths.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001840	2	All global initialization files' executable search paths must contain only absolute paths.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001845	2	All global initialization files' library search paths must contain only absolute paths.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001850	2	All global initialization files' lists of preloaded libraries must contain only absolute paths.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001900	2	All local initialization files' executable search paths must contain only absolute paths.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001901	2	All local initialization files' library search paths must contain only absolute paths.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001902	2	All local initialization files' lists of preloaded libraries must contain only absolute paths.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fixpathvars</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001940	2	User initialization files must not run world-writable programs.	<p><b>Location</b> /etc/security/psceexpert/dodv2/rmwwpaths</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN001980	2	The .rhosts, .shosts, hosts.equiv, shosts.equiv, /etc/passwd, /etc/shadow, or the /etc/group files must not contain a plus sign (+) without defining the entries for NIS+ netgroups.	<p><b>Location</b> /etc/security/psceexpert/dodv2/dodv2netrules</p> <p><b>Compliance action</b> Ensures that the specified files meet the specified requirements.</p>
GEN002000	2	There must be no .netrc files on the system.	<p><b>Location</b> /etc/security/psceexpert/dodv2/dodv2netrules</p> <p><b>Compliance action</b> Ensures that there are none of specified files on the system. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN002020	2	All .rhosts, .shosts, or hosts.equiv files must contain only trusted host-user pairs.	<p><b>Location</b> /etc/security/psccexpert/dodv2/dodv2netrules</p> <p><b>Compliance action</b> Ensures that the specified files conform to this requirement.</p>
GEN002040	1	This rule disables .rhosts, .shosts, and hosts.equiv files or shosts.equiv files.	<p><b>Location</b> /etc/security/psccexpert/dodv2/mvhostsfilesdod</p> <p><b>Compliance action</b> Disables the specified files.</p>
GEN002120	1,2	This rule checks and configures user shells.	<p><b>Location</b> /etc/security/psccexpert/dodv2/usershells</p> <p><b>Compliance action</b> Creates the required shells. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN002140	1,2	All shells that are referenced in the /etc/passwd list must be listed in the /etc/shells file, except any shells that are specified to prevent logins.	<p><b>Location</b> /etc/security/psccexpert/dodv2/usershells</p> <p><b>Compliance action</b> Ensures that the shells are listed in the correct files. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN002280	2	Device files and directories must be writable only by users with a system account, or as the system is configured by the vendor.	<p><b>Location</b> /etc/security/psccexpert/dodv2/wdevfiles</p> <p><b>Compliance action</b> Displays world-writable device files, directories, and any other files on the system that are in non-public directories.</p>
GEN002300	2	Device files that are used for backup must be readable, writable, or both, only by the root user or the backup user.	<p><b>Location</b> /etc/security/psccexpert/dodv2/wdevfiles</p> <p><b>Compliance action</b> Displays world-writable device files, directories, and any other files on the system that are in non-public directories.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN002400	2	The system must be checked weekly for unauthorized <code>setuid</code> files, and unauthorized modification to authorized <code>setuid</code> files.	<p><b>Location</b></p> <p><code>/etc/security/psccexpert/dodv2/trust</code></p> <p><b>Compliance action</b></p> <p>Checks weekly to identify changes to the specified files.  <b>Note:</b> Compare the two newest weekly logs that are created in the <code>/var/security/psccexpert</code> directory to verify that there was no unauthorized activity.</p>
GEN002420	2	Removable media, remote file systems, and any file system that does not contain approved <code>setuid</code> files must be mounted by using the <code>nosuid</code> option.	<p><b>Location</b></p> <p><code>/etc/security/psccexpert/dodv2/fsmntoptions</code></p> <p><b>Compliance action</b></p> <p>Ensures that the remotely mounted file systems have the specified options.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the <code>DoDv2_to_AIXDefault.xml</code> file. You must manually change this setting.</p>
GEN002430	2	Removable media, remote file systems, and any file system that does not contain approved device files must be mounted by using the <code>nODEV</code> option.	<p><b>Location</b></p> <p><code>/etc/security/psccexpert/dodv2/fsmntoptions</code></p> <p><b>Compliance action</b></p> <p>Ensures that the remotely mounted file systems have the specified options.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the <code>DoDv2_to_AIXDefault.xml</code> file. You must manually change this setting.</p>
GEN002480	2	Public directories must be the only world-writable directories, and world-writable files must be located only in public directories.	<p><b>Location</b></p> <p><code>/etc/security/psccexpert/dodv2/wdevfiles</code></p> <p><code>/etc/security/psccexpert/dodv2/fpmdodfiles</code></p> <p><b>Compliance action</b></p> <p>Reports when world-writable files are not in public directories.</p>



Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN002640	2	Default system accounts must be disabled or removed.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/lockacc_rlogin</p> <p>/etc/security/pscxpert/dodv2/loginout</p> <p><b>Compliance action</b></p> <p>Disables default system accounts.</p>
GEN002660	2	Auditing must be enabled.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/dodaudit</p> <p><b>Compliance action</b></p> <p>Enables the dodaudit command, which enables auditing.</p>
GEN002720	2	The audit system must be configured to audit failed attempts to access files and programs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/dodaudit</p> <p><b>Compliance action</b></p> <p>Automatically enables the specified auditing.</p>
GEN002740	2	The audit system must be configured to audit file deletions.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/dodaudit</p> <p><b>Compliance action</b></p> <p>Automatically enables the specified auditing.</p>
GEN002750	3	The audit system must be configured to audit account creation.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/dodaudit</p> <p><b>Compliance action</b></p> <p>Automatically enables the specified auditing.</p>
GEN002751	3	The audit system must be configured to audit account modification.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/dodaudit</p> <p><b>Compliance action</b></p> <p>Automatically enables the specified auditing.</p>
GEN002752	3	The audit system must be configured to audit accounts that are disabled.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/dodaudit</p> <p><b>Compliance action</b></p> <p>Automatically enables the specified auditing.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN002753	3	The audit system must be configured to audit account termination.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodaudit</p> <p><b>Compliance action</b> Automatically enables the specified auditing.</p>
GEN002760	2	The audit system must be configured to audit all administrative, privileged, and security actions.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodaudit</p> <p><b>Compliance action</b> Automatically enables the specified auditing.</p>
GEN002800	2	The audit system must be configured to audit login, logout, and session initiation.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodaudit</p> <p><b>Compliance action</b> Automatically enables the specified auditing.</p>
GEN002820	2	The audit system must be configured to audit all discretionary access control permission modifications.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodaudit</p> <p><b>Compliance action</b> Automatically enables the specified auditing.</p>
GEN002825	2	The audit system must be configured to audit the loading and unloading of dynamic kernel modules.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodaudit</p> <p><b>Compliance action</b> Automatically enables the specified auditing.</p>
GEN002860	2	Audit logs must be rotated daily.	<p><b>Location</b> /etc/security/pscxpert/dodv2/rotateauditdod</p> <p><b>Compliance action</b> Ensures that audit logs are rotated.</p>
GEN002960	2	Access to the cron utility must be controlled by using the cron.allow file or cron.deny file, or both.	<p><b>Location</b> /etc/security/pscxpert/dodv2/limitsysacc</p> <p><b>Compliance action</b> Ensures that the compliant limits are enabled.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003000 (related to GEN000960, GEN003020, GEN003160, GEN003360, GEN003380)	2	Cron must not run group-writable or world-writable programs.	<b>Location</b> /etc/security/psceexpert/ dodv2/rmwpaths  <b>Compliance action</b> Ensures that the compliant limits are enabled. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.
GEN003020 (related to GEN000960, GEN003000, GEN003160, GEN003360, GEN003380)	2	Cron must not run programs in, or subordinate to, world-writable directories.	<b>Location</b> /etc/security/psceexpert/ dodv2/rmwpaths  <b>Compliance action</b> Removes the world-writable permission from the cron program directories. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.
GEN003060	2	Default system accounts (except for root) must not be listed in the cron.allow file, or must be included in the cron.deny file if the cron.allow file does not exist.	<b>Location</b> cron.allow or cron.deny  <b>Compliance action</b> Ensures that the system meets the specified requirements.
GEN003160 (related to GEN000960, GEN003000, GEN003020, GEN003360, GEN003380)	2	Cron logging must be running.	<b>Location</b> /etc/security/psceexpert/ dodv2/rmwpaths  <b>Compliance action</b> Ensures that the system meets the specified requirements.
GEN003280	2	Access to the at utility must be controlled by using the at.allow and the at.deny files.	<b>Location</b> /etc/security/psceexpert/ dodv2/chcronfilesdod  <b>Compliance action</b> Ensures that the system meets the specified requirements.
GEN003300	2	The at.deny file must not be empty, if it exists.	<b>Location</b> /etc/security/psceexpert/ dodv2/chcronfilesdod  <b>Compliance action</b> Ensures that the system meets the specified requirements.

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003320	2	Default system accounts that are not root must not be listed in the <code>at.allow</code> file, or must be included in the <code>at.deny</code> file if the <code>at.allow</code> file does not exist.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/chcronfilesdod</code></p> <p><b>Compliance action</b>            Ensures that the system meets the specified requirements.</p>
GEN003360 (related to GEN000960, GEN003000, GEN003020, GEN003160, GEN003380)	2	The <code>at</code> daemon must not run group-writable or world-writable programs.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/rmwvpaths</code></p> <p><b>Compliance action</b>            Ensures that the system meets the specified requirements.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the <code>DoDv2_to_AIXDefault.xml</code> file. You must manually change this setting.</p>
GEN003380 (related to GEN000960, GEN003000, GEN003020, GEN003160, GEN003360)	2	The <code>at</code> daemon must not run programs in, or subordinate to, world-writable directories.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/rmwvpaths</code></p> <p><b>Compliance action</b>            Ensures that the system meets the specified requirements.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the <code>DoDv2_to_AIXDefault.xml</code> file. You must manually change this setting.</p>
GEN003510	2	Kernel core dumps must be disabled unless they are needed.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/coredumpdev</code></p> <p><b>Compliance action</b>            Disables kernel core dumps.</p>
GEN003540	2	The system must use non-executable program stacks.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/sedconfigdod</code></p> <p><b>Compliance action</b>            Enforces the use of non-executable program stacks.</p>
GEN003600	2	The system must not forward IPv4 source-routed packets.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/ntwkoptsdod</code></p> <p><b>Compliance action</b>            Sets the value of the <code>ipsrcforward</code> network option to <code>0</code>.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003601	2	TCP backlog queue sizes must be set appropriately.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the clean_partial_conns network option to 1.</p>
GEN003603	2	The system must not respond to Internet Control Message Protocol version 4 (ICMPv4) echoes that are sent to a broadcast address.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the bcastping network option to 0.</p>
GEN003604	2	The system must not respond to ICMP time stamp requests that are sent to a broadcast address.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the bcastping network option to 0.</p>
GEN003605	2	The system must not apply reversed source routing to TCP responses.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the nonlocsrcroute network option to 0.</p>
GEN003606	2	The system must prevent local applications from generating source-routed packets.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the ipsrcroutesend network option to 0.</p>
GEN003607	2	The system must not accept source-routed IPv4 packets.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Disables the ability to accept source-routes IPv4 packets.</p>
GEN003609	2	The system must ignore IPv4 ICMP redirect messages.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the ipignoreredirects network option to 1.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003610	2	The system must not send IPv4 ICMP redirect messages.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the ipsendredirects network option to 0.</p>
GEN003612	2	The system must be configured to use TCP syncookies when a TCP SYN flood occurs.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the clean_partial_conns network option to 1.</p>
GEN003640	2	The root file system must use journaling, or another method of ensuring file system consistency.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chkjournal</p> <p><b>Compliance action</b> Enables journaling on the root file system.</p>
GEN003660	2	The system must log authentication informational data.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chsyslogdod</p> <p><b>Compliance action</b> Enables the logging of auth and info data.</p>
GEN003700	2	The inetd and xinetd must be disabled or removed if no network services are using them.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2services</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN003810	2	This portmap or rpcbindservices must not be running unless they are needed.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2services</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN003815	2	The portmap or rpcbindservices must not be installed unless they are being used.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2services</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003820-3860	1,2,3	The rsh, rexexec, and telnet daemons, and the rlogind service must not be running.	<p><b>Location</b> /etc/security/pscxpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN003865	2	Network analysis tools must not be installed.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2services</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN003900	2	The hosts.lpd file (or equivalent) must not contain an addition sign (+).	<p><b>Location</b> /etc/security/pscxpert/dodv2/printers</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN004220	1	Administrative accounts must not run a web browser, except as needed for local service administration.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2cat1</p> <p><b>Compliance action</b> Displays the results of the specified rule tests.</p>
GEN004460	2	This rule logs auth and info data.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chsyslogdod</p> <p><b>Compliance action</b> Enables the logging of auth and info data.</p>
GEN004540	2	This rule disables the sendmail help command.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sendmailhelp  /etc/security/pscxpert/dodv2/dodv2cmntrows</p> <p><b>Compliance action</b> Disables the specified command.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN004580	2	The system must not use .forward files.	<p><b>Location</b> /etc/security/psceexpert/dodv2/forward</p> <p><b>Compliance action</b> Disables the specified files. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN004600	1	The SMTP service must be the most current version.	<p><b>Location</b> /etc/security/psceexpert/dodv2/SMTP_ver</p> <p><b>Compliance action</b> Ensures that the latest version of the specified service is running. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN004620	2	The sendmail server must have the debugging feature disabled.	<p><b>Location</b> /etc/security/psceexpert/dodv2/SMTP_ver</p> <p><b>Compliance action</b> Disables the sendmail debugging feature.</p>
GEN004640	1	The SMTP service must not have an active uuencode alias.	<p><b>Location</b> /etc/security/psceexpert/dodv2/SMTPuuencode</p> <p><b>Compliance action</b> Disables the uuencode alias.</p>
GEN004710	2	Mail relaying must be restricted.	<p><b>Location</b> /etc/security/psceexpert/dodv2/sendmaildod</p> <p><b>Compliance action</b> Restricts mail relay.</p>
GEN004800	1,2,3	Unencrypted FTP must not be used on the system.	<p><b>Location</b> /etc/security/psceexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>



Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN004820	2	Anonymous FTP must not be active on the system unless it is authorized.	<p><b>Location</b> /etc/security/pscxpert/dodv2/anonuser</p> <p><b>Compliance action</b> Disables anonymous FTP on the system. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN004840	2	If the system is an anonymous FTP server, it must be isolated to the Demilitarized Zone (DMZ) network.	<p><b>Location</b> /etc/security/pscxpert/dodv2/anonuser</p> <p><b>Compliance action</b> Ensures that an anonymous FTP on the system is on the DMZ network.</p>
GEN004880	2	The ftpusers file must exist.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chdodftpusers</p> <p><b>Compliance action</b> Ensures that the specified file is on the system.</p>
GEN004900	2	The ftpusers file must contain the account names that are not allowed to use the FTP protocol.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chdodftpusers</p> <p><b>Compliance action</b> Ensures that the file contains the required account names.</p>
GEN005000	1	Anonymous FTP accounts must not have a functional shell.	<p><b>Location</b> /etc/security/pscxpert/dodv2/usershells</p> <p><b>Compliance action</b> Removes shells from anonymous FTP accounts. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN005080	1	The TFTP daemon must operate in secure-mode, which provides access only to a single directory on the host file system.	<p><b>Location</b> /etc/security/pscxpert/dodv2/tftpdod</p> <p><b>Compliance action</b> Ensures that the daemon meets the specified requirements.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN005120	2	The TFTP daemon must be configured to vendor specifications, including a dedicated TFTP user account, a non-login shell, such as <code>/bin/false</code> , and a home directory that is owned by the TFTP user.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/tftpdod</code></p> <p><b>Compliance action</b>            Ensures that the system meets the specified requirements.</p>
GEN005140	1,2,3	Any active TFTP daemon must be authorized and approved in the system accreditation package.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/inetdservices</code></p> <p><b>Compliance action</b>            Ensures that the daemon is authorized.</p>
GEN005160	1,2	Any X Window System host must write <code>.Xauthority</code> files.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/dodv2disableX</code></p> <p><b>Compliance action</b>            Ensures that the host wrote the specified files.</p>
GEN005200	1,2	Any X Window System displays cannot be exported publicly.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/dodv2disableX</code></p> <p><b>Compliance action</b>            Disables the dissemination of the specified programs.</p>
GEN005220	1,2	The <code>.Xauthority</code> or <code>X*.hosts</code> (or equivalent) files must be used to restrict access to the X Window System server.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/dodv2disableX</code></p> <p><b>Compliance action</b>            Ensures that the specified files are available to restrict access to the server.</p>
GEN005240	1,2	The <code>.Xauthority</code> utility must allow access only to authorized hosts.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/dodv2disableX</code></p> <p><b>Compliance action</b>            Ensures that the access is limited to authorized hosts.</p>
GEN005260	2	This rule disables X Window System connections and XServer login manager.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/dodv2cmntrows</code></p> <p><b>Compliance action</b>            Disables the required connections and login manager.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN005280	1,2,3	The system must not have the UUCP service active.	<p><b>Location</b></p> <p>/etc/security/psceexpert/dodv2/inetdservices</p> <p><b>Compliance action</b></p> <p>Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN005300	2	SNMP communities must be changed from the default settings.	<p><b>Location</b></p> <p>/etc/security/psceexpert/dodv2/chsnmp</p> <p><b>Compliance action</b></p> <p>Ensures that the system meets the specified requirements.</p>
GEN005305	2	SNMP service must use only SNMPv3 or a later version.	<p><b>Location</b></p> <p>/etc/security/psceexpert/dodv2/chsnmp</p> <p><b>Compliance action</b></p> <p>Ensures that the system meets the specified requirements.</p>
GEN005306	2	SNMP service must require the use of a FIPS 140-2.	<p><b>Location</b></p> <p>/etc/security/psceexpert/dodv2/chsnmp</p> <p><b>Compliance action</b></p> <p>Ensures that the system meets the specified requirements.</p>
GEN005440	2	The system must use a remote syslog server (log host).	<p><b>Location</b></p> <p>/etc/security/psceexpert/dodv2/EnableTrustedLogging</p> <p><b>Compliance action</b></p> <p>Ensures that the system is using a remote syslog server.</p>
GEN005450	2	The system must use a remote syslog server (log host).	<p><b>Location</b></p> <p>/etc/security/psceexpert/dodv2/EnableTrustedLogging</p> <p><b>Compliance action</b></p> <p>Ensures that the system is using a remote syslog server.</p>
GEN005460	2	The system must use a remote syslog server (log host).	<p><b>Location</b></p> <p>/etc/security/psceexpert/dodv2/EnableTrustedLogging</p> <p><b>Compliance action</b></p> <p>Ensures that the system is using a remote syslog server.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN005480	2	The system must use a remote syslog server (log host).	<p><b>Location</b> /etc/security/pscxpert/dodv2/EnableTrustedLogging</p> <p><b>Compliance action</b> Ensures that the system is using a remote syslog server.</p>
GEN005500	2	The SSH daemon must be configured to use only the Secure Shell version 2 (SSHv2) protocol.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005501	2	The SSH client must be configured to use only the SSHv2 protocol.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005504	2	The SSH daemon must only listen on management network addresses, unless it is authorized for uses other than management.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005505	2	The SSH daemon must be configured to use only ciphers that conform to Federal Information Processing Standards (FIPS) 140-2 standards.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005506	2	The SSH daemon must be configured to use only ciphers that conform to FIPS 140-2 standards.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005507	2	The SSH daemon must be configured to use only Message Authentication Codes (MACs) with cryptographic hash algorithms that conform to FIPS 140-2 standards.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005510	2	The SSH client must be configured to use only MACs with ciphers that conform to FIPS 140-2 standards.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN005511	2	The SSH client must be configured to use only MACs with ciphers that conform to FIPS 140-2 standards.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005512	2	The SSH daemon must be configured to use only MACs with cryptographic hash algorithms that conform to FIPS 140-2 standards.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005521	2	The SSH daemon must restrict login to specific users, groups, or both.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005536	2	The SSH daemon must perform strict mode checking of the home directory configuration files.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005537	2	The SSH daemon must use privilege separation.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005538	2	The SSH daemon must not allow rhosts to authenticate by using the Rivest-Shamir-Adleman (RSA) cryptosystem.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005539	2	The SSH daemon must not allow compression or must allow compression only after a successful authentication.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005550	2	The SSH daemon must be configured with the DoD logon banner.	<p><b>Location</b> /etc/security/pscxpert/dodv2/sshDoDconfig</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN005560	2	Determine whether there is a default gateway that is configured for IPv4.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chkgtway</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting. <b>Note:</b> If your system is running the IPv6 protocol, ensure that the <i>ipv6_enabled</i> setting in the /etc/security/pscxpert/ipv6.conf file is set to the value of yes. If system is not using IPv6, then ensure that the <i>ipv6_enabled</i> value is set to no.</p>
GEN005570	2	Determine whether there is a default gateway that is configured for IPv6.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chkgtway</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting. <b>Note:</b> If your system is running the IPv6 protocol, ensure that the <i>ipv6_enabled</i> setting in the /etc/security/pscxpert/ipv6.conf file is set to the value of yes. If system is not using IPv6, then ensure that the <i>ipv6_enabled</i> value is set to no.</p>
GEN005590	2	The system must not be running any routing protocol daemons, unless the system is a router.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2cmntrows</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN005590	2	The system must not be running any routing protocol daemons, unless the system is a router.	<p><b>Location</b> /etc/security/psceexpert/dodv2/dodv2cmntrows</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN005600	2	IP forwarding for IPv4 must not be enabled unless the system is a router.	<p><b>Location</b> /etc/security/psceexpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the ipforwarding network option to 0.</p>
GEN005610	2	The system must not have IP forwarding for IPv6 enabled unless the system is an IPv6 router.	<p><b>Location</b> /etc/security/psceexpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the ip6forwarding network option to 1.</p>
GEN005820	2	The NFS anonymous UID and GID must be configured to values without permissions.	<p><b>Location</b> /etc/security/psceexpert/dodv2/nfsoptions</p> <p><b>Compliance action</b> Ensures that the specified IDs do not have permissions.</p>
GEN005840	2	The NFS server must be configured to restrict file system access to local hosts.	<p><b>Location</b> /etc/security/psceexpert/dodv2/nfsoptions</p> <p><b>Compliance action</b> Configures NFS server to restrict access to local hosts.</p>
GEN005880	2	The NFS server must not allow remote root access.	<p><b>Location</b> /etc/security/psceexpert/dodv2/nfsoptions</p> <p><b>Compliance action</b> Disables remote root access on the NFS server.</p>
GEN005900	2	The <i>nosuid</i> option must be enabled on all NFS client mounts.	<p><b>Location</b> /etc/security/psceexpert/dodv2/nosuid</p> <p><b>Compliance action</b> Enables the <i>nosuid</i> option on all NFS client mounts.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN006060	2	The system must not run Samba unless it is needed.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2services</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN006380	1	The system must not use UDP for NIS or NIS+.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2cat1</p> <p><b>Compliance action</b> Displays the results of the specified rule tests.</p>
GEN006400	2	The Network Information System (NIS) protocol must not be used.	<p><b>Location</b> /etc/security/pscxpert/dodv2/nisplus</p> <p><b>Compliance action</b> Disables the specified protocol. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN006420	2	NIS maps must be protected by using hard-to-guess domain names.	<p><b>Location</b> /etc/security/pscxpert/dodv2/nisplus</p> <p><b>Compliance action</b> Ensures that domain names are not easy to determine.</p>
GEN006460	2	Any NIS+ server must be operating at security level 2.	<p><b>Location</b> /etc/security/pscxpert/dodv2/nisplus</p> <p><b>Compliance action</b> Ensures that the server is at the specified minimum security level. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN006480	2	The system must be checked weekly for unauthorized setuid files, and unauthorized modification to authorized setuid files.	<p><b>Location</b> /etc/security/pscxpert/dodv2/trust</p> <p><b>Compliance action</b> Checks weekly to identify changes to the specified files.</p>



Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN006560	2	The system must be checked weekly for unauthorized <code>setuid</code> files, and unauthorized modification to authorized <code>setuid</code> files.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/trust</code></p> <p><b>Compliance action</b>  Checks weekly to identify changes to the specified files.</p>
GEN006580	2	The system must use an access control program.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/checktcpd</code></p> <p><b>Compliance action</b>  Ensures that the system meets the specified requirements.</p>
GEN006600	2	The system's access control program must log each system access attempt.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/chsyslogdod</code></p> <p><b>Compliance action</b>  Ensures that access attempts are logged.</p>
GEN006620	2	The system's access control program must be configured to grant or deny system access to specific hosts.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/chetchostsdod</code></p> <p><b>Compliance action</b>  Configures the <code>hosts.deny</code> and <code>hosts.allow</code> files to the required settings.</p>
GEN007020	2	The Stream Control Transmission Protocol (SCTP) must be disabled.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/dodv2netrules</code></p> <p><b>Compliance action</b>  Disables the specified protocol.</p>
GEN007700	2	The IPv6 protocol handler must not be bound to the network stack unless it is needed.	<p><b>Location</b>  <code>/etc/security/pscxpert/dodv2/rminet6</code></p> <p><b>Compliance action</b>  Disables the IPv6 protocol handler from the network stack, unless the handler is specified in the <code>/etc/ipv6.conf</code> file.  <b>Note:</b> If your system is running the IPv6 protocol, ensure that the <code>ipv6_enabled</code> setting in the <code>/etc/security/pscxpert/ipv6.conf</code> file is set to the value of <code>yes</code>. If system is not using IPv6, then ensure that the <code>ipv6_enabled</code> value is set to <code>no</code>.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN007780	2	The system must not have 6to4 tunnels enabled.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/rmiface</p> <p><b>Compliance action</b></p> <p>Disables the specified tunnels.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN007820	2	The system must not have IP tunnels configured.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/rmtunnel</p> <p><b>Compliance action</b></p> <p>Disables IP tunnels.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN007840	2	The DHCP client must be disabled if it is not used.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/dodv2services</p> <p><b>Compliance action</b></p> <p>Ensures that the system meets the specified requirements.</p>
GEN007850	2	The DHCP client must not send dynamic DNS updates.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/dodv2services</p> <p><b>Compliance action</b></p> <p>Ensures that the system meets the specified requirements.</p>
GEN007860	2	The system must ignore IPv6 ICMP redirect messages.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b></p> <p>Sets the value of the ipignoreredirects network option to 1.</p>
GEN007880	2	The system must not send IPv6 ICMP redirects.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b></p> <p>Sets the value of the ipsendredirects network option to 0.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN007900	2	The system must use an appropriate reverse-path filter for IPv6 network traffic, if the system uses IPv6.	<p><b>Location</b> /etc/security/psceexpert/dodv2/chuserstanzadod</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN007920	2	The system must not forward IPv6 source-routed packets.	<p><b>Location</b> /etc/security/psceexpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the ip6srcrouteforward network option to 0.</p>
GEN007940: GEN003607	2	The system must not accept source-routed IPv4 or IPv6 packets.	<p><b>Location</b> /etc/security/psceexpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the ipsrcrouterecv network option to 0.</p>
GEN007950	2	The system must not respond to ICMPv6 echo requests that are sent to a broadcast address.	<p><b>Location</b> /etc/security/psceexpert/dodv2/ntwkoptsdod</p> <p><b>Compliance action</b> Sets the value of the bcastping network option to 0.</p>
GEN008000	2	If the system is using Lightweight Directory Access Protocol (LDAP) for authentication or account information, certificates that are used to authenticate to the LDAP server must be provided from DoD PKI or a DoD-approved method.	<p><b>Location</b> /etc/security/psceexpert/dodv2/ldap_config</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN008020	2	If the system is using LDAP for authentication or account information, the LDAP Transport Layer Security (TLS) connection must require the server to provide a certificate with a valid trust path.	<p><b>Location</b> /etc/security/psceexpert/dodv2/ldap_config</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN008050	2	If the system is using LDAP for authentication or account information, the /etc/ldap.conf file (or equivalent) must not contain passwords.	<p><b>Location</b> /etc/security/psceexpert/dodv2/ldap_config</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN008380	2	The system must be checked weekly for unauthorized setuid files, and unauthorized modification to authorized setuid files.	<p><b>Location</b> /etc/security/pscxpert/dodv2/trust</p> <p><b>Compliance action</b> Checks weekly to identify changes to the specified files.</p>
GEN008520	2	The system must employ a local firewall that guards the host against port scans. The firewall must shun vulnerable ports for 5 minutes to guard the host against port scans.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ipsecshunports</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements.</p>
GEN008540	2	The system's local firewall must implement a <i>deny-all, allow-by-exception</i> policy.	<p><b>Location</b> /etc/security/pscxpert/dodv2/ipsecshunhost1s</p> <p><b>Compliance action</b> Ensures that the system meets the specified requirements. <b>Note:</b> You can enter additional filter rules in the /etc/security/aixpert/bin/filter.txt file. These rules are integrated by the ipsecshunhost1s.sh script when you apply the profile. The entries should be in the following format: <i>port_number:ip_address:action</i>  where the possible values for <i>action</i> are Allow or Deny.</p>
GEN008600	1	The system must be configured to start only from the system boot configuration.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2cat1</p> <p><b>Compliance action</b> Ensures that the starting the system only uses the system boot configuration.</p>
GEN008640	1	The system must not use removable media as the boot loader.	<p><b>Location</b> /etc/security/pscxpert/dodv2/dodv2cat1</p> <p><b>Compliance action</b> Ensures that the system does not boot from a removable drive.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN009140	1,2,3	The system must not have the chargen service active.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009160	1,2,3	The system must not have the Calendar Management Service Daemon (CMSD) service active.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009180	1,2,3	The system must not have the tool-talk database server (ttdbserver) service active.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009190	1,2,3	The system must not have the comsat service active.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009200-9330	1,2,3	The system cannot have other services and daemons active.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009210	2	The system must not have the discard service active.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN009220	2	The system must not have the dtspc service active.	<p><b>Location</b> /etc/security/pscxpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009230	2	The system must not have the echo service active.	<p><b>Location</b> /etc/security/pscxpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009240	2	The system must not have Internet Message Access Protocol (IMAP) service active.	<p><b>Location</b> /etc/security/pscxpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009250	2	The system must not have the PostOffice Protocol (POP3) service active.	<p><b>Location</b> /etc/security/pscxpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009260	2	The system must not have the talk or ntalk services active.	<p><b>Location</b> /etc/security/pscxpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009270	2	The system must not have the netstat service active on the InetD process.	<p><b>Location</b> /etc/security/pscxpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN009280	2	The system must not have the PCNFS service active.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009290	2	The system must not have the systat service active.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009300	2	The inetd time service must not be active on the system on the inetd daemon.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009310	2	The system must not have the rusersd service active.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009320	2	The system must not have the sprayd service active.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>
GEN009330	2	The system must not have the rstatd service active.	<p><b>Location</b> /etc/security/psccexpert/dodv2/inetdservices</p> <p><b>Compliance action</b> Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.</p>

Table 2. DoD general requirements (continued)

Department of Defense STIG checkpoint ID	Category of the STIG rule	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN009340	2	X server login managers must not be running unless they are needed for X11 session management.	<p><b>Location</b> /etc/security/psceexpert/dodv2/dodv2cmtrows</p> <p><b>Compliance action</b> This rule disables X Window System connections and XServer login manager.</p>

Table 3. DoD ownership requirements

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
AIX00085	The /etc/netshvc.conf file must be owned by root.	<p><b>Location</b> /etc/security/psceexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root.</p>
AIX00090	The /etc/netshvc.conf file must be group-owned by bin, sys, or system.	<p><b>Location</b> /etc/security/psceexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by bin, sys, or system.</p>
AIX00320	The /etc/ftpaccess.c1 file must be owned by root.	<p><b>Location</b> /etc/security/psceexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root.</p>
AIX00330	The /etc/ftpaccess.c1 file must be group-owned by bin, sys, or system.	<p><b>Location</b> /etc/security/psceexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by bin, sys, or system.</p>
GEN000250	The time synchronization configuration file (such as /etc/ntp.conf) must be owned by root.	<p><b>Location</b> /etc/security/psceexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root.</p>
GEN000251	The time synchronization configuration file (such as /etc/ntp.conf) must be group-owned by bin, sys, or system.	<p><b>Location</b> /etc/security/psceexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by bin, sys, or system.</p>



Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001160	All files and directories must have a valid owner.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that all files and directories have a valid owner.</p>
GEN001170	All files and directories must have a valid group owner.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that all files and directories have a valid owner.</p>
GEN001220	All system files, programs, and directories must be owned by a system account.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the system files, programs, and directories are owned by a system account.</p>
GEN001240	System files, programs, and directories must be group-owned by a system group.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>All system files, programs, and directories are group-owned by a system group.</p>
GEN001320	Network Information Systems (NIS)/NIS+/yp files must be owned by root, sys, or bin.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are owned by root, sys, or bin.</p>
GEN001340	NIS/NIS+/yp files must be group-owned by sys, bin, other, or system.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are owned by sys, bin, other, or system.</p>
GEN001362	The /etc/resolv.conf file must be owned by root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root.</p>
GEN001363	The /etc/resolv.conf file must be group-owned by bin, sys, or system.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by bin, sys, or system.</p>

Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001366	The /etc/hosts file must be owned by root.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root.</p>
GEN001367	The /etc/hosts file must be group-owned by bin, sys, or system.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by bin, sys, or system.</p>
GEN001371	The /etc/nsswitch.conf file must be owned by root.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root.</p>
GEN001372	The /etc/nsswitch.conf file must be group-owned by root, bin, sys, or system.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by root, bin, sys, or system.</p>
GEN001378	The /etc/passwd file must be owned by root.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root.</p>
GEN001379	The /etc/passwd file must be group-owned by bin, security, sys, or system.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by bin, security, sys, or system.</p>
GEN001391	The /etc/group file must be owned by root	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root.</p>
GEN001392	The /etc/group file must be group-owned by bin, security, sys, or system.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by bin, security, sys, or system.</p>

Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001400	The /etc/security/passwd file must be owned by root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root.</p>
GEN001410	The /etc/security/passwd file must be group-owned by bin, security, sys, or system.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by bin, security, sys, or system.</p>
GEN001500	All interactive users' home directories must be owned by their respective users.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that all of the interactive users' home directories must be owned by their respective users.</p>
GEN001520	All interactive users' home directories must be group-owned by the home directory owner's primary group.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that all interactive users' home directories are group-owned by the home directory owner's primary group.</p>
GEN001540	All files and directories that are contained in the interactive user's home directories must be owned by the home directory's owner.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that all files and directories that are contained in the interactive user's home directories are owned by the home directory's owner.</p>
GEN001550	All files and directories that are contained in the user's home directories must be group-owned by a group in which the home directory's owner is a member.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that all files and directories that are contained in the user's home directories must be group-owned by a group in which the home directory's owner is a member.</p>
GEN001660	All system start files must be owned by root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are owned by root.</p>

Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001680	All system start files must be group-owned by sys, bin, other, or system.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are group-owned by sys, bin, other, or system.</p>
GEN001740	All global initialization files must be owned by root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are owned by root.</p>
GEN001760	All global initialization files must be group-owned by sys, bin, system, or security.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are group-owned by sys, bin, system, or security.</p>
GEN001820	All skeleton files and directories (typically in /etc/skel) must be owned by root or bin.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files and directories are owned by root or bin.</p>
GEN001830	All skeleton files (typically in /etc/skel) must be group-owned by security.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are group-owned by security.</p>
GEN001860	All local initialization files must be owned by the user or root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are owned by the user or root.</p>
GEN001870	Local initialization files must be group-owned by the user's primary group or root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the local initialization files must be group-owned by the user's primary group or root.</p>

Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN002060	All .rhosts, .shosts, .netrc, or hosts.equiv files must be accessible by only root or the owner.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p>/etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that only the root or the owner can access the specified files.</p>
GEN002100	The .rhosts file must not be supported by the Pluggable Authentication Module (PAM).	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is not available by using PAM.</p>
GEN002200	All shell files must be owned by root or bin.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are owned by root or bin.</p>
GEN002210	All shell files must be group-owned by root, bin, sys, or system.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are group-owned by root, bin, sys, or system.</p>
GEN002340	Audio devices must be owned by root.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that all audio devices are owned by root.</p>
GEN002360	Audio devices must be group-owned by root, sys, bin, or system.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that all audio devices are group-owned by root, sys, bin, or system.</p>
GEN002520	All public directories must be owned by root or an application account.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that all public directories are owned by root or an application account.</p>

Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN002540	All public directories must be group-owned by system or an application group.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that all public directories are group-owned by system or an application group.</p>
GEN002680	System audit logs must be owned by root.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are owned by root.</p>
GEN002690	System audit logs must be group-owned by bin, sys, or system.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are group-owned by bin, sys, or system.</p>
GEN003020	Cron must not run programs in, or subordinate to, world-writable directories.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Prevents cron from running programs in, or subordinate to, world-writable directories.</p>
GEN003040	Crontabs must be owned by root or the crontab creator.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that crontabs are owned by root or by the crontab creator.</p>
GEN003050	Crontab files must be group-owned by system, cron, or the crontab creator's primary group.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the crontab files are group-owned by system, cron, or the crontab creator's primary group.</p>
GEN003110	Cron and crontab directories must not have extended access control lists.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified directories do not have extended access control lists.</p>

Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003120	Cron and crontab directories must be owned by root or bin.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that cron and crontab directories are owned by root or bin.</p>
GEN003140	Cron and crontab directories must be group-owned by system, sys, bin, or cron.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified directories are group-owned by system, sys, bin, or cron.</p>
GEN003160	Cron logging must be implemented.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that cron logging is implemented.</p>
GEN003240	The cron.allow file must be owned by root, bin, or sys.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root, bin, or sys.</p>
GEN003250	The cron.allow file must be group-owned by system, bin, sys, or cron.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by system, bin, sys, or cron.</p>
GEN003260	The cron.deny file must be owned by root, bin, or sys.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root, bin, or sys.</p>
GEN003270	The cron.deny file must be group-owned by system, bin, sys, or cron.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by system, bin, sys, or cron.</p>
GEN003420	The at directory must be owned by root, bin, sys, daemon, or cron.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified directory is owned by root, sys, daemon, or cron.</p>

Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003430	The at directory must be group-owned by system, bin, sys, or cron.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified directory is group-owned by system, bin, sys, or cron.</p>
GEN003460	The at.allow file must be owned by root, bin, or sys.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root, bin, or sys.</p>
GEN003470	The at.allow file must be group-owned by system, bin, sys, or cron.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by system, bin, sys, or cron.</p>
GEN003480	The at.deny file must be owned by root, bin, or sys.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root, bin, or sys.</p>
GEN003490	The at.deny file must be group-owned by system, bin, sys, or cron.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by system, bin, sys, or cron.</p>
GEN003720	The inetd.conf file, xinetd.conf file, and the xinetd.d directory must be owned by root or bin.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files and directory are owned by root or bin.</p>
GEN003730	The inetd.conf file, xinetd.conf file, and the xinetd.d directory must be group-owned by bin, sys, or system.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files and directory are group-owned by bin, sys, or system.</p>
GEN003760	The services file must be owned by root or bin.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root or bin.</p>



Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003770	The services file must be group-owned by bin, sys, or system.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by bin, sys, or system.</p>
GEN003920	The hosts.lpd (or equivalent) file must be owned by root, bin, sys, or lp.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root, bin, sys, or lp.</p>
GEN003930	The hosts.lpd (or equivalent) file must be group-owned by bin, sys, or system.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by bin, sys, or system.</p>
GEN003960	The <b>traceroute</b> command owner must be root.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the owner of the command is root.</p>
GEN003980	The <b>traceroute</b> command must be group-owned by sys, bin, or system.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the command is group-owned by sys, bin, or system.</p>
GEN004360	The alias file must be owned by root.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root.</p>
GEN004370	The aliases file must be group-owned by sys, bin, or system.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by sys, bin, or system.</p>

Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN004400	Files that are run through a mail aliases file must be owned by root and must be located within a directory that is owned and writable only by root.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that files that are run through a mail aliases file are owned by root and are located within a directory that is owned and writable only by root.</p>
GEN004410	Files that are run through a mail aliases file must be group-owned by root, bin, sys, or other. They must also be located within a directory that is group-owned by root, bin, sys, or other.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that files that are run through a mail aliases file are group-owned by root, bin, sys, or other. and are located within a directory that is group-owned by root, bin, sys, or other.</p>
GEN004480	The SMTP service log file must be owned by root.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root.</p>
GEN004920	The ftpusers file must be owned by root.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root.</p>
GEN004930	The ftpusers file must be group-owned by bin, sys, or system.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by bin, sys, or system.</p>
GEN005360	The snmpd.conf file must be owned by root.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is owned by root.</p>
GEN005365	The snmpd.conf file must be group-owned by bin, sys, or system.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by bin, sys, or system.</p>

Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN005400	The /etc/syslog.conf file must be owned by root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root.</p>
GEN005420	The /etc/syslog.conf file must be group-owned by bin, sys, or system.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by bin, sys, or system.</p>
GEN005610	The system must not have IP forwarding for IPv6 enabled, unless the system is an IPv6 router.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that IP forwarding for IPv6 is not enabled unless the system is being used as an IPv6 router.</p>
GEN005740	The NFS export configuration file must be owned by root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root.</p>
GEN005750	The NFS export configuration file must be group-owned by root, bin, sys, or system.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by root, bin, sys, or system.</p>
GEN005800	All NFS-exported system files and system directories must be owned by root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root.</p>
GEN005810	All NFS-exported system files and system directories must be group-owned by root, bin, sys, or system.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files and directories are group-owned by root, bin, sys, or system.</p>
GEN006100	The /usr/lib/smb.conf file must be owned by root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root.</p>

Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN006120	The /usr/lib/smb.conf file must be group-owned by bin, sys, or system.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by bin, sys, or system.</p>
GEN006160	The /var/private/smbpasswd file must be owned by root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root.</p>
GEN006180	The /var/private/smbpasswd file must be group-owned by sys or system.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by sys or system.</p>
GEN006340	Files in the /etc/news directory must be owned by root or news.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified directory is owned by root or news.</p>
GEN006360	The files in /etc/news must be group-owned by system or news.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files are group-owned by system or news.</p>
GEN008080	If the system is using LDAP for authentication or account information, the /etc/ldap.conf (or equivalent) file must be owned by root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root.</p>
GEN008100	If the system is using LDAP for authentication or account information, the /etc/ldap.conf (or equivalent) file must be group-owned by security, bin, sys, or system.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is group-owned by bin, sys, or system.</p>
GEN008140	If the system is using LDAP for authentication or account information, the TLS certificate authority file or directory must be owned by root.	<p><b>Location</b></p> <p>/etc/security/psccexpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file is owned by root.</p>

Table 3. DoD ownership requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN008160	If the system is using LDAP for authentication or account information, the TLS certificate authority file or directory must be group-owned by root, bin, sys, or system.	<p><b>Location</b> /etc/security/pscxpert/dodv2/chowndodfiles</p> <p><b>Compliance action</b> Ensures that the specified file is group-owned by bin, sys, or system.</p>

Table 4. DoD standards for file permissions

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
AIX00100	The /etc/netsvc.conf file must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
AIX00340	The /etc/ftpaccess.ct1 file must have mode 0640 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN000252	The time synchronization configuration file (such as /etc/ntp.conf) must have mode 0640 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN000920	The root account's home directory (other than /) must have mode 0700.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the directory is set to the specified permission mode, or to one that is less permissive.</p>
GEN001140	System files and directories must not have uneven access permissions.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the access permissions are consistent.</p>

Table 4. DoD standards for file permissions (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001180	All network services daemon files must have mode 0755 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN001200	All system command files must have mode 0755 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN001260	System log files must have mode 0640 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN001280	Manual page files must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN001300	Library files must have mode 0755 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN001360	The NIS/NIS+/yp files must have mode 0755 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN001364	The /etc/resolv.conf file must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>

Table 4. DoD standards for file permissions (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001368	The /etc/hosts file must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN001373	The /etc/nsswitch.conf file must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN001380	The /etc/passwd file must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN001393	The /etc/group file must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN001420	The /etc/security/passwd file must have mode 0400.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN001480	All of a user's home directories must have a mode of 0750 or less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN001560	All files and directories that are contained in a user's home directories must have mode 0750 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>

Table 4. DoD standards for file permissions (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001580	All run control scripts must have mode 0755 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN001640	Run control scripts must not run world-writable programs or scripts.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Checks programs, such as cron, for world-writable programs or scripts.</p>
GEN001720	All global initialization files must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN001800	All skeleton files (for example, files in /etc/skel) must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN001880	All local initialization files must have mode 0740 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN002220	All shell files must have mode 0755 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN002320	Audio devices must have mode 0660 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the audio devices are set to the specified permission mode, or one that is less permissive,</p>



Table 4. DoD standards for file permissions (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN002560	The system and user default <b>umask</b> must be 077.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the specified settings are 077.</p>
GEN002700	System audit logs must have mode 0640 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN002717	System audit tool executable files must have mode 0750 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN002980	The cron.allow file must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN003080	Crontab files must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN003090	Crontab files must not have extended access control lists (ACLs).	<p><b>Location</b> /etc/security/psceexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the specified files do not have extended ACLs.</p>
GEN003100	Cron and crontab directories must have mode 0755 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psceexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the specified directories are set to the specified permissions mode, or to one that is less permissive.</p>

Table 4. DoD standards for file permissions (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003180	The cronlog file must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN003200	The cron.deny file must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN003252	The at.deny file must have mode 0640 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN003340	The at.allow file must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN003400	The at directory must have mode 0755 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the directory is set to the specified permission mode, or to one that is less permissive.</p>
GEN003440	At jobs must not set the <b>umask</b> parameter to a value less restrictive than 077.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the parameter is set to the specified permission mode, or to one that is less permissive.</p>
GEN003740	The inetd.conf and xinetd.conf files must have mode 0440 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>

Table 4. DoD standards for file permissions (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003780	The services file must have mode 0444 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN003940	The hosts.lpd file (or equivalent) must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN004000	The traceroute file must have mode 0700 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN004380	The alias file must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN004420	Files that are run through a mail aliases file must have mode 0755 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN004500	The SMTP service log file must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN004940	The ftpusers file must have mode 0640 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>

Table 4. DoD standards for file permissions (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN005040	All FTP users must have a default <b>umask</b> setting of 077.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the setting is correct.</p>
GEN005100	The TFTP daemon must have mode 0755 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the daemon is set to the specified mode, or to one that is less permissive.</p>
GEN005180	All .Xauthority files must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN005320	The snmpd.conf file must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN005340	Management Information Base (MIB) files must have mode 0640 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN005390	The /etc/syslog.conf file must have mode 0640 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN005522	The SSH public host key files must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>

Table 4. DoD standards for file permissions (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN005523	The SSH private host key files must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the files are set to the specified permission mode, or to one that is less permissive.</p>
GEN006140	The /usr/lib/smb.conf file must have mode 0644 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN006200	The /var/private/smbpasswd file must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN006260	The /etc/news/hosts.nntp file (or equivalent) must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN006280	The /etc/news/hosts.nntp.nolimit file (or equivalent) must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN006300	The /etc/news/nntp.access file (or equivalent) must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN006320	The /etc/news/passwd.nntp file (or equivalent) must have mode 0600 or a mode that is less permissive.	<p><b>Location</b> /etc/security/psccexpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b> Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>

Table 4. DoD standards for file permissions (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN008060	If the system is using LDAP for authentication or account information, the /etc/ldap.conf (or equivalent) file must have mode 0644 or less permissive.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the file is set to the specified permission mode, or to one that is less permissive.</p>
GEN008180	If the system is using LDAP for authentication or account information, the TLS certificate authority file, directory, or both must have mode 0644 (0755 for directories) or less permissive.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/fpmdodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified file, directories, or both, are set to the specified permission mode, or to one that is less permissive.</p>

Table 5. DoD access control list (ACL) requirements

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
AIX00110	The /etc/netsvc.conf file must not have an extended access control list (ACL).	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
AIX00350	The /etc/ftppaccess.ctl file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN000253	The time synchronization configuration file (such as /etc/ntp.conf) must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 5. DoD access control list (ACL) requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN000930	The root account's home directory must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001190	All network services daemon files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001210	All system command files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001270	System log files must not have extended ACLs, except as needed to support authorized software.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001310	All library files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 5. DoD access control list (ACL) requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001361	NIS/NIS+/yp command files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001365	The /etc/resolv.conf file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001369	The /etc/hosts file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001374	The /etc/nsswitch.conf file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001390	The /etc/passwd file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>



Table 5. DoD access control list (ACL) requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001394	The /etc/group file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001430	The /etc/security/passwd file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001570	All files and directories that are contained in user home directories must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001590	All run control scripts must have no extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001730	All global initialization files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 5. DoD access control list (ACL) requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN001810	Skeleton files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN001890	Local initialization files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN002230	All shell files must not have extended ACLs	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN002330	Audio devices must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN002710	All system audit files must not have extended ACLs	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 5. DoD access control list (ACL) requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN002990	Extended ACLs should be disabled for the cron.allow and cron.deny files.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN003090	Crontab files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN003110	Cron and crontab directories must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN003190	The cron log files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN003210	The cron.deny file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 5. DoD access control list (ACL) requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003245	The at.allow file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN003255	The at.deny file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN003410	The at directory must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN003745	The inetd.conf and xinetd.conf files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN003790	The services file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 5. DoD access control list (ACL) requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN003950	The hosts.lpd file (or equivalent) must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN004010	The traceroute file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN004390	The alias file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN004430	Files that are run through a mail aliases file must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN004510	The SMTP service log file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL. <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 5. DoD access control list (ACL) requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN004950	The ftpusers file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN005190	The .xauthority files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN005350	Management Information Base (MIB) files must not have extended ACLs.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN005375	The snmpd.conf file must not have an extended ACL	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN005395	The /etc/syslog.conf file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 5. DoD access control list (ACL) requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN006150	The /usr/lib/smb.conf file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN006210	The /var/private/smbpasswd file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN006270	The /etc/news/hosts.nntp file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN006290	The /etc/news/hosts.nntp.nolimit file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN006310	The /etc/news/nnrp.access file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

Table 5. DoD access control list (ACL) requirements (continued)

Department of Defense STIG checkpoint ID	Description	Location of the script where the action is defined and the results of the action that enables compliance
GEN006330	The /etc/news/passwd.nntp file must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Disables the specified extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN008120	If the system is using LDAP for authentication or account information, the /etc/ldap.conf (or equivalent) file must not have an extended access control list (ACL).	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified files do not have an extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>
GEN008200	If the system is using LDAP for authentication or account information, the LDAP TLS certificate authority file or directory (as appropriate) must not have an extended ACL.	<p><b>Location</b></p> <p>/etc/security/pscxpert/dodv2/ acldodfiles</p> <p><b>Compliance action</b></p> <p>Ensures that the specified directory or file does not have an extended ACL.  <b>Note:</b> This setting is not automatically changed when the policy is reset to the AIX default policy by using the DoDv2_to_AIXDefault.xml file. You must manually change this setting.</p>

**Related information:**

 Department of Defense STIG compliance

## Payment Card Industry - Data Security Standard compliance

The Payment Card Industry - Data Security Standard (PCI - DSS) categorizes IT security into 12 sections that are called the 12 requirements and security assessment procedures.

The 12 requirements and security assessment procedures of IT security that are defined by PCI - DSS include the following items:

**Requirement 1: Install and maintain a firewall configuration to protect the data of the cardholder.**

Section 1.1.5 and Section 2.2.2: Documented list of services and ports necessary for business. This requirement is implemented by disabling unnecessary and insecure services.

Section 1.3.6: Securing and synchronizing router configuration files. This requirement is implemented by setting the Network option *clean\_partial\_conns* value to 1.



**Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.**

Section 2.1: Always change vendor-supplied defaults before you install a system on the network. This requirement is implemented by disabling the Simple Network Management Protocol (SNMP) daemon.

**Requirement 3: Protect the stored data of the cardholder.**

This requirement is implemented by enabling the Encrypted File System (EFS) feature that is provided with the AIX operating system.

**Requirement 4: Encrypt the data of the cardholder when you transmit the data across open public networks.**

This requirement is implemented by enabling the IP Security (IPSEC) feature that is provided with the AIX operating system.

**Requirement 5: Use and regularly update anti-virus software programs.**

This requirement is implemented by using the Trusted Execution policy program. Trusted Execution is the recommended anti-virus software, and it is native to the AIX operating system. PCI requires that you capture the logs from the Trusted Execution program by enabling security information and event management (SIEM) to monitor the alerts. By running the Trusted Execution program in log-only mode, it does not stop the checks when an error is caused by a hash mismatch.

**Requirement 6: Develop and maintain secure systems and applications.**

To implement this requirement, you must install the required patches to your system manually. If you purchased PowerSC Standard Edition, you can use the Trusted Network Connect (TNC) feature.

**Requirement 7: Restrict access to the cardholder data, by business need to know.**

You can implement strong access control measures by using the RBAC feature to enable rules and roles. RBAC cannot be automated because it requires the input of an administrator to be enabled.

The RbacEnablement checks the system to determine whether the isso, so, and sa properties for the roles exist on the system. If these properties do not exist, the script creates them. This script is also run as part of the AIXPert checks that it completes when it is running commands, such as the pscxpert -c command.

**Requirement 8: Assign a unique ID to each person who has access to the computer.**

You can implement this requirement by enabling PCI profiles. The following rules apply to PCI profile:

- Section 8.5.9: Change user passwords at least every 90 days.
- Section 8.5.10: Require a minimum password length of 7 characters.
- Section 8.5.11: Use a password that contains both numerals and alphabetic characters.
- Section 8.5.12: Do not allow an individual to submit a new password that is the same as the previous four passwords that were used.
- Section 8.5.13: Limit repeated access attempts by locking out the user ID after six unsuccessful attempts.
- Section 8.5.14: Set the lockout duration to 30 minutes, or until an administrator re-enables the user ID.
- Section 8.5.15: Require a user to reenter a password to reactivate a terminal after it is idle for 15 minutes or longer.

**Requirement 9: Restrict physical access to the data of the cardholder.**

Store repositories that contain sensitive cardholder data in an access-restricted room.

**Requirement 10: Track and monitor all access to network resources and to the cardholder data.**

Section 10.2: This requirement is implemented by logging access to the system components by enabling the automatic logs on the system components.

**Requirement 11: Regularly test the security systems and processes.**

This requirement is implemented by using the Real-Time Compliance feature.

**Requirement 12: Maintain a security policy that includes information security for employees and contractors.**

Section 12.3.9: Activation of modems for vendors only when needed by vendors with immediate deactivation after use. This requirement is implemented by disabling remote root login, activating on a needed basis by a system administrator, and then deactivating when it is no longer needed.

PowerSC Express Edition reduces the configuration management that is required to meet the guidelines that are defined by PCI DSS. However, the entire process cannot be automated.

For example, restricting access to the data of the cardholder based on the business requirement cannot be automated. The AIX operating system provides strong security technologies, such as Role Based Access Control (RBAC); however, PowerSC Express Edition cannot automate this configuration because it cannot determine the individuals who require access and the individuals who do not. IBM Compliance Expert can automate the configuration of other security settings that are consistent with the PCI requirements.

| When the PCI profile is applied to a database environment, several TCP and UDP ports that are used by  
| the software stack are disabled by restrictions. You must enable these ports and disable the Trusted  
| Execution function to run the application and workload. Run the following commands to remove the  
| restrictions on the ports and disable the Trusted Execution function:

```
| trustchk -p TE=OFF  
| tcptr -delete 9091 65535  
| tcptr -delete 9090 9090  
| tcptr -delete 112 9089  
| tcptr -add 9091 65535 1024 1
```

**Note:** All of the custom script files that are provided to maintain PCI - DSS compliance are in the /etc/security/psceexpert/bin directory.

The following table shows how PowerSC Express Edition addresses the requirements of the PCI DSS standard by using the functions of the AIX Security Expert utility:

*Table 6. Settings related to the PCI DSS compliance 2.0 standard*

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
2.1	Always change vendor-supplied defaults before installing a system on the network. For example, include passwords, simple network management protocol community strings, and eliminate unnecessary accounts.	Sets the minimum number of weeks that must pass before you can change a password to 0 weeks.	<b>Location</b> /etc/security/psceexpert/bin/ chusrattr  <b>Compliant value</b> minage=0
8.5.9	Change user passwords at least every 90 days.	Sets the maximum number of weeks that a password is valid to 13 weeks.	<b>Location</b> /etc/security/psceexpert/bin/ chusrattr  <b>Compliant value</b> maxage=13

Table 6. Settings related to the PCI DSS compliance 2.0 standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
2.1	Always change vendor-supplied defaults before installing a system on the network. For example, include passwords, simple network management protocol community strings, and eliminate unnecessary accounts.	Sets the number of weeks that an account with an expired password remains in the system to 8 weeks.	<b>Location</b> /etc/security/psceexpert/bin/chusrattr  <b>Compliant value</b> maxexpired=8
8.5.10	Require a minimum password length of at least 7 characters.	Sets the minimum password length to 7 characters.	<b>Location</b> /etc/security/psceexpert/bin/chusrattr  <b>Compliant value</b> minlen=7
8.5.11	Use passwords that contain both numeric and alphabetic characters.	Sets the minimum number of alphabetic characters that are required in a password to 1. This setting ensures that the password contains alphabetic characters.	<b>Location</b> /etc/security/psceexpert/bin/chusrattr  <b>Compliant value</b> minalpha=1
8.5.11	Use passwords that contain both numeric and alphabetic characters.	Sets the minimum number of non-alphabetic characters that are required in a password to 1. This setting ensures that the password contains nonalphabetic characters.	<b>Location</b> /etc/security/psceexpert/bin/chusrattr  <b>Compliant value</b> minother=1
2.1	Always change vendor-supplied defaults before installing a system on the network. For example, include passwords, simple network management protocol community strings, and eliminate unnecessary accounts.	Sets the maximum number of times that a character can be repeated in a password to 8. This setting indicates that a character in a password can be repeated an unlimited number of times as long as it conforms to the other password limitations.	<b>Location</b> /etc/security/psceexpert/bin/chusrattr  <b>Compliant value</b> maxrepeats=8
8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	Sets the number of weeks before a password can be reused to 52.	<b>Location</b> /etc/security/psceexpert/bin/chusrattr  <b>Compliant value</b> histexpire=52
8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	Sets the number of previous passwords that you cannot reuse to 4.	<b>Location</b> /etc/security/psceexpert/bin/chusrattr  <b>Compliant value</b> histsize=4
8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Sets the number of consecutive unsuccessful login attempts that disables an account to 6 attempts for each non-root account.	<b>Location</b> /etc/security/psceexpert/bin/chusrattr  <b>Compliant value</b> loginretries=6

Table 6. Settings related to the PCI DSS compliance 2.0 standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Sets the number of consecutive unsuccessful login attempts that disables a port to 6 attempts.	<b>Location</b> /etc/security/pscxpert/bin/chdefstanza /etc/security/login.cfg <b>Compliant value</b> logindisable=6
8.5.14	Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	Sets the duration of time that a port is locked after it is disabled by the <i>logindisable</i> attribute to 30 minutes.	<b>Location</b> /etc/security/pscxpert/bin/chdefstanza /etc/security/login.cfg <b>Compliant value</b> loginreenable=30
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	Disables the remote root login function by setting its value to false. The system administrator can activate the remote login function as needed, and then deactivate it when the task is complete.	<b>Location</b> /etc/security/pscxpert/bin/chuserstanza /etc/security/user <b>Compliant value</b> rlogin=false root
8.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	Enables the function that ensures that all users have a unique user name before they can access system components or card holder data by setting that function to a value of true.	<b>Location</b> /etc/security/pscxpert/bin/chuserstanza /etc/security/user <b>Compliant value</b> login=true root
10.2	Enable auditing on the system.	Enables auditing of the binary files on the system.	<b>Location</b> /etc/security/pscxpert/bin/pciaudit <b>Compliant value</b> h
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the lpd daemon.	Stops the lpd daemon and comments out the corresponding entry in the /etc/inittab file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/comntrows <b>Compliant value</b> lpd: /etc/inittab : d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the Common Desktop Environment (CDE).	Disables the CDE function when the layer four traceroute (LFT) is not configured.	<b>Location</b> /etc/security/pscxpert/bin/comntrows <b>Compliant value</b> "dt" "/etc/inittab" ":" d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the timed daemon.	Stops the timed daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/rctcpip <b>Compliant value</b> timed d

Table 6. Settings related to the PCI DSS compliance 2.0 standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the NTP daemon.	Stops the NTP daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	<b>Location</b> /etc/security/psceexpert/bin/rctcpip <b>Compliant value</b> xntpd d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the rwhod daemon.	Stops the rwhod daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	<b>Location</b> /etc/security/psceexpert/bin/rctcpip <b>Compliant value</b> rwhod d
2.1	Change the vendor-supplied defaults before installing a system on the network, which includes disabling the SNMP daemon.	Stops the SNMP daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	<b>Location</b> /etc/security/psceexpert/bin/rctcpip <b>Compliant value</b> snmpd d
2.1	Change vendor-supplied defaults before installing a system on the network, which includes disabling the SNMPMIBD daemon.	Disables the SNMPMIBD daemon.	<b>Location</b> /etc/security/psceexpert/bin/rctcpip <b>Compliant value</b> snmpmibd d
2.1	Change vendor-supplied defaults before installing a system on the network, which includes disabling the AIXMIBD daemon.	Disables the AIXMIBD daemon.	<b>Location</b> /etc/security/psceexpert/bin/rctcpip <b>Compliant value</b> aixmibd d
2.1	Change vendor-supplied defaults before installing a system on the network, which includes disabling the HOSTMIBD daemon.	Disables the HOSTMIBD daemon.	<b>Location</b> /etc/security/psceexpert/bin/rctcpip <b>Compliant value</b> hostmibd d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the DPID2 daemon.	Stops the DPID2 daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	<b>Location</b> /etc/security/psceexpert/bin/rctcpip <b>Compliant value</b> dpid2 d
2.1	Change vendor-supplied defaults before installing a system on the network, which includes stopping the DHCP server.	Disables the DHCP server.	<b>Location</b> /etc/security/psceexpert/bin/rctcpip <b>Compliant value</b> dhcpsd d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the DHCP agent.	Stops and disables the DHCP relay agent and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the agent.	<b>Location</b> /etc/security/psceexpert/bin/rctcpip <b>Compliant value</b> dhcprd d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the rshd daemon.	Stops and disables all instances of the rshd daemon and the rshdpci_shell service, and comments out the corresponding entries in the /etc/inetd.conf file that automatically start the instances.	<b>Location</b> /etc/security/psceexpert/bin/ cominetdconf <b>Compliant value</b> shell tcp d

Table 6. Settings related to the PCI DSS compliance 2.0 standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the rlogind daemon.	Stops and disables all instances of the rlogind daemon and rlogindpci.rlogin service. The AIX Security Expert utility also comments out the corresponding entries in the /etc/inetd.conf file that automatically start the instances.	<b>Location</b> /etc/security/pscxpert/bin/ cominetdconf  <b>Compliant value</b> login tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the rexecd daemon.	Stops and disables all instances of the rexecd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/ cominetdconf  <b>Compliant value</b> exec tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the comsat daemon.	Stops and disables all instances of the comsat daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/ cominetdconf  <b>Compliant value</b> comsat udp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the fingerd daemon.	Stops and disables all instances of the fingerd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/ cominetdconf  <b>Compliant value</b> finger tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the systat daemon.	Stops and disables all instances of the systat daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/ cominetdconf  <b>Compliant value</b> systat tcp d
2.1	Change vendor-supplied defaults before installing a system on the network, which includes disabling the netstat command.	Disables the netstat command.	<b>Location</b> /etc/security/pscxpert/bin/ cominetdconf  <b>Compliant value</b> netstat tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the tftpd daemon.	Stops and disables all instances of the tftpd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/ cominetdconf  <b>Compliant value</b> tftpd udp d

Table 6. Settings related to the PCI DSS compliance 2.0 standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the talkd daemon.	Stops and disables all instances of the talkd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf <b>Compliant value</b> talk udp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the rquotad daemon.	Stops and disables all instances of the rquotad daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf <b>Compliant value</b> rquotad udp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the rstatd daemon.	Stops and disables all instances of the rstatd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf <b>Compliant value</b> rstatd udp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the rusersd daemon.	Stops and disables all instances of the rusersd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf <b>Compliant value</b> rusersd udp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the rwalld daemon.	Stops and disables all instances of the rwalld daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf <b>Compliant value</b> rwalld udp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the sprayd daemon.	Stops and disables all instances of the sprayd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf <b>Compliant value</b> sprayd udp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the pcnfsd daemon.	Stops and disables all instances of the pcnfsd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf <b>Compliant value</b> pcnfsd udp d

Table 6. Settings related to the PCI DSS compliance 2.0 standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the TCP echo service.	Stops and disables all instances of the echo(tcp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> echo tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the TCP discard service.	Stops and disables all instances of the discard(tcp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> discard tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the TCP chargen service.	Stops and disables all instances of the chargen(tcp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> chargen tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the TCP daytime service.	Stops and disables all instances of the daytime(tcp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> daytime tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the TCP time service.	Stops and disables all instances of the timed(tcp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> time tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the UDP echo service.	Stops and disables all instances of the echo(udp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> echo udp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the UDP discard service.	Stops and disables all instances of the discard(udp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> discard udp d



Table 6. Settings related to the PCI DSS compliance 2.0 standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the UDP chargen service.	Stops and disables all instances of the chargen(udp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> chargen udp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the UDP daytime service.	Stops and disables all instances of the daytime(udp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> daytime udp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the UDP time service.	Stops and disables all instances of the timed(udp) service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> time udp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the FTP service.	Stops and disables all instances of the ftpd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> ftp tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the telnet service.	Stops and disables all instances of the telnetd daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> telnet tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes dtspc.	Stops and disables all instances of the dtspc daemon. The AIX Security Expert also comments out the corresponding entry in the /etc/inittab file that automatically starts the daemon when the LFT is not configured and the CDE is disabled in the /etc/inittab file.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> dtspc tcp d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the ttldbserver service.	Stops and disables all instances of the ttldbserver service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf  <b>Compliant value</b> ttldbserver tcp d

Table 6. Settings related to the PCI DSS compliance 2.0 standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the cmsd service.	Stops and disables all instances of the cmsd service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	<b>Location</b> /etc/security/pscxpert/bin/cominetdconf <b>Compliant value</b> cmsd udp d
2.2.3	Configure system security parameters to prevent misuse.	Removes the Set User ID (SUID) commands.	<b>Location</b> /etc/security/pscxpert/bin/rmsuidfrmrcmds <b>Compliant value</b> r
2.2.3	Configure system security parameters to prevent misuse.	Enables the lowest security level for the File Permissions Manager.	<b>Location</b> /etc/security/pscxpert/bin/filepermgr <b>Compliant value</b> l
2.2.3	Configure system security parameters to prevent misuse.	Modifies the Network File System protocol with restricted settings that conform to the PCI security requirements. These restricted settings include disabling remote root access and anonymous UID and GID access.	<b>Location</b> /etc/security/pscxpert/bin/nfsconfig <b>Compliant value</b> e
2.2.2	Enable only necessary and secure services, protocols, daemons, and so on, as required for the correct function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	Disables the rlogind, rshd, and tftpd daemons, which are not secure.	<b>Location</b> /etc/security/pscxpert/bin/dismrtdmns <b>Compliant value</b> d
2.2.2	Enable only necessary and secure services, protocols, daemons, and so on, as required for the correct function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	Disables the rlogind, rshd, and tftpd daemons, which are not secure.	<b>Location</b> /etc/security/pscxpert/bin/rmrhostsnetrc <b>Compliant value</b> h
2.2.2	Enable only necessary and secure services, protocols, daemons, and so on, as required for the correct function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	Disables the logind, rshd, and tftpdpci_rmetchostsequiv daemons, which are not secure.	<b>Location</b> /etc/security/pscxpert/bin/rmetchostsequiv <b>Compliant value</b> No compliant value is required.

Table 6. Settings related to the PCI DSS compliance 2.0 standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
1.3.6	Implement stateful inspection, or packet filtering, in which only established connections are allowed on the network.	Enables the network <b>clean_partial_conns</b> option by setting its value to 1.	<p><b>Location</b> /etc/security/psccexpert/bin/ntwkopts</p> <p><b>Compliant value</b> clean_partial_conns=1 s</p>
1.3.6	Implement stateful inspection, or packet filtering, in which only established connections are allowed on the network.	Enables TCP security by setting the network <b>tcp_tcpsecure</b> option to a value of 7. This setting provides protection against data, reset (RST), and TCP connection request (SYN) attacks.	<p><b>Location</b> /etc/security/psccexpert/bin/ntwkopts</p> <p><b>Compliant value</b> tcp_tcpsecure=7 s</p>
	Protect unauthorized access to unused ports.	Sets up the system to shun the hosts for 5 minutes to prevent other systems from accessing unused ports.	<p><b>Location</b> /etc/security/psccexpert/bin/ipsecshunhosthls</p> <p><b>Compliant value</b> No compliant value is required. <b>Note:</b> You can enter additional filter rules in the /etc/security/aixpert/bin/filter.txt file. These rules are integrated by the ipsecshunhosthls.sh script when you apply the profile. The entries should be in the following format: <i>port_number:ip_address:action</i>  where the possible values for <i>action</i> are Allow or Deny.</p>
	Protect the host from port scans.	Sets up the system to shun vulnerable ports for 5 minutes, which prevents port scans.	<p><b>Location</b> /etc/security/psccexpert/bin/ipsecshunports</p> <p><b>Compliant value</b> No compliant value is required. <b>Note:</b> You can enter additional filter rules in the /etc/security/aixpert/bin/filter.txt file. These rules are integrated by the ipsecshunhosthls.sh script when you apply the profile. The entries should be in the following format: <i>port_number:ip_address:action</i>  where the possible values for <i>action</i> are Allow or Deny.</p>
	Limit object creation permissions.	Sets default object creation permissions to 22.	<p><b>Location</b> /etc/security/psccexpert/bin/chusrattr</p> <p><b>Compliant value</b> umask=22</p>


Table 6. Settings related to the PCI DSS compliance 2.0 standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
	Limit system access.	Makes the root ID the only one that is listed in the cron.allow file and removes the cron.deny file from the system.	<b>Location</b> /etc/security/pscxpert/bin/limitsysacc <b>Compliant value</b> h
	Remove dot from the path root.	Removes the dots from the PATH environment variable in the following files that are located in the root home directory: <ul style="list-style-type: none"> <li>.cshrc</li> <li>.kshrc</li> <li>.login</li> <li>.profile</li> </ul>	<b>Location</b> /etc/security/pscxpert/bin/rmdotfrmpathroot <b>Compliant value</b> No compliant value is required.
	Remove dot from the non-root path:	Removes the dots from PATH environment variable in the following files that are in the user home directory: <ul style="list-style-type: none"> <li>.cshrc</li> <li>.kshrc</li> <li>.login</li> <li>.profile</li> </ul>	<b>Location</b> /etc/security/pscxpert/bin/rmdotfrmpathnroot <b>Compliant value</b> No compliant value is required.
	Limit system access.	Adds the root user capability and user name in the /etc/ftpusers file.	<b>Location</b> /etc/security/pscxpert/bin/chetcftpusers <b>Compliant value</b> a
	Remove the guest account.	Removes the guest account and its files.	<b>Location</b> /etc/security/pscxpert/bin/execcmds <b>Compliant value</b> "rmuser guest; rm -rf /home/guest; ODMDIR=/etc/objrepos odmdelete -qloc0=/home/guest -o inventory"
	Prevent launching programs in content space.	Enables the stack execution disable (SED) feature.	<b>Location</b> /etc/security/pscxpert/bin/sedconfig <b>Compliant value</b> No compliant value is required.
	Ensure that the password for root is not weak.	Starts a root password integrity check against the root password, thereby ensuring a strong root password.	<b>Location</b> /etc/security/pscxpert/bin/chuserstanza <b>Compliant value</b> /etc/security/user dictionlist=/etc/security/aixpert/dictionary/English rootpci_rootpwdintchk

Table 6. Settings related to the PCI DSS compliance 2.0 standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
8.5.15	Limit access to the system by setting the session idle time.	Sets the idle time limit to 15 minutes. If the session is idle for longer than 15 minutes, you must reenter the password.	<b>Location</b> /etc/security/pscxpert/bin/autologoff <b>Compliant value</b> 900
	Limit traffic access to cardholder information.	Sets the TCP traffic regulation to its high setting, which enforces denial-of-service mitigation on ports.	<b>Location</b> /etc/security/pscxpert/bin/tcptr_aixpert <b>Compliant value</b> pci
	Maintain a secure connection when migrating data.	Enables automated IP Security (IPSec) tunnel creation between Virtual I/O Servers during live partition migration.	<b>Location</b> /etc/security/pscxpert/bin/cfgsecmig <b>Compliant value</b> on
1.3.5	Limit packets from unknown sources.	Allows the packets from the Hardware Management Console.	<b>Location</b> /etc/security/pscxpert/bin/ipsecpermihostorport <b>Compliant value</b> No compliant value is required.
5.1.1	Maintain antivirus software.	Maintains the system integrity by detecting, removing, and protecting against known types of malicious software.	<b>Location</b> /etc/security/pscxpert/bin/manageITsecurity <b>Compliant value</b> No compliant value is required.
	Maintain access on an as needed basis.	Enable role-based access control (RBAC) by creating system operator, system administrator, and information system security officer user roles with the required permissions.	<b>Location</b> /etc/security/pscxpert/bin/EnableRbac <b>Compliant value</b> No compliant value is required.

**Related information:**

 [Payment card industry DSS compliance](#)

## Sarbanes-Oxley Act and COBIT compliance

The Sarbanes-Oxley (SOX) Act of 2002 that is based on the 107th congress of the United States of America oversees the audit of public companies that are subject to the securities laws, and related matters, in order to protect the interests of investors.

SOX Section 404 mandates the management assessment over internal controls. For most organizations, internal controls span their information technology systems, which process and report the financial data of the company. The SOX Act provides specific details on IT and IT security. Many SOX auditors rely on standards, such as COBIT as a method to gauge and audit proper IT governance and control. The PowerSC Express Edition SOX/COBIT XML configuration option provides the security configuration of AIX and Virtual I/O Server (VIOS systems that is required to meet the COBIT compliance guidelines.


The IBM Compliance Expert Express Edition runs on AIX 7.1, AIX 6.1, and AIX 5.3.


Compliance with external standards is a responsibility of an AIX system administrator's workload. The IBM Compliance Expert Express Edition is designed to simplify managing the operating system settings and the reports that are required for standards compliance.

The preconfigured compliance profiles delivered with the IBM Compliance Expert Express Edition reduce the administrative workload of interpreting compliance documentation and implementing those standards as specific system configuration parameters.

The capabilities of the IBM Compliance Expert Express Edition are designed to help clients to effectively manage the system requirements, which are associated with external standard compliance that can potentially reduce costs while improving compliance. All external security standards include aspects other than the system configuration settings. The use of IBM Compliance Expert Express Edition cannot ensure standards compliance. The Compliance Expert is designed to simplify the management of systems configuration setting that helps administrators to focus on other aspects of standards compliance.

#### **Related information:**

 [COBIT compliance](#)

 [Sarbanes-Oxley \(SOX\) compliance](#)

## **Health Insurance Portability and Accountability Act (HIPAA)**

The Health Insurance Portability and Accountability Act (HIPAA) is a security profile that focuses on the protection of Electronically Protected Health Information (EPHI).

The HIPAA Security Rule specifically focuses on the protection of EPHI, and only a subset of agencies are subject to the HIPAA Security Rule based on their functions and use of EPHI.

All HIPAA covered entities, similar to some of the federal agencies, must comply with the HIPAA Security Rule.

The HIPAA Security Rule focuses on protecting the confidentiality, integrity, and availability of EPHI, as defined in the Security Rule.

The EPHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and disclosures.

The requirements, standards, and implementation specifications of the HIPAA Security Rule apply to the following covered entities:

- Healthcare providers
- Health plans
- Healthcare clearinghouses
- Medicare prescriptions and drug card sponsors

The following table details about the several sections of the HIPAA Security Rule and each section includes several standards and implementation specifications.

**Note:** All of the custom script files that are provided to maintain HIPAA compliance are in the `/etc/security/psccexpert/bin` directory.

Table 7. HIPAA rules and implementation details

Sections of HIPAA Security Rule	Implementation specification	The aixpert implementation	Commands and return values
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	Implements the procedures to regularly review the records of the information system activity, such as audit logs, access reports, and security incident reports.	Determines whether auditing is enabled in the system.	<b>Command:</b>  <b>#audit query.</b>  <b>Return value:</b> If successful, this command exits with a value of 0. If unsuccessful, the command exits with a value of 1.
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	Implements the procedures to regularly review the records of the information system activity, such as audit logs, access reports, and security incident reports.	Enables auditing in the system. Also, configures the events to be captured.	<b>Command:</b>  <b># audit start &gt;/dev/null 2&gt;&amp;1.</b>  <b>Return value:</b> If successful, this command exits with a value of 0. If unsuccessful, the command exits with a value of 1.  The following events are audited:  <b>FILE_Mknod, FILE_Open, FS_Mkdir, PROC_Execute, DEV_Create, FILE_Acl, FILE_Chpriv, FILE_Fchpriv, FILE_Mode, INIT_Start, PASSWORD_Change, PASSWORD_Check, PROC_Adjtime, PROC_Kill, PROC_Privilege, PROC_Setpgid, USER_SU, USER_Change, USER_Create, USER_Login, USER_Logout, USER_Reboot, USER_Remove, USER_SetEnv, USER_SU, FILE_Acl,FILE_Fchmod,FILE_Fchown</b>
164.312 (a) (2) (iv)	Encryption and Decryption (A):Implements a mechanism to encrypt and decrypt the EPHI.	Determines whether the encrypted file system (EFS) is enabled on the system.	<b>Command:</b>  <b># efskeymgr -V &gt;/dev/null 2&gt;&amp;1.</b>  <b>Return value:</b> If EFS is already enabled, this command exits with a value of 0. If EFS is not enabled, this command exits with a value of 1.
164.312 (a) (2) (iii)	Automatic Logoff (A): Implements the electronic procedures to end an electronic session after a predefined interval of inactivity.	Configures the system to log out from interactive processes after 15 minutes of inactivity.	<b>Command:</b>  <b>grep TMOUT= /etc/security /.profile &gt;/dev/null 2&gt;&amp;1</b>  <b>echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT.</b>  <b>Return value:</b> If the command fails to find the value <b>TMOUT=15</b> , the script exits with a value of 1. Otherwise, the command exits with a value of 0.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Ensures that all passwords contain a minimum of 14 characters.	<b>Command:</b>  <b>chsec -f /etc/security/user -s user -a minlen=8.</b>  <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the script exits with an error code of 1.

Table 7. HIPAA rules and implementation details (continued)

Sections of HIPAA Security Rule	Implementation specification	The aixpert implementation	Commands and return values
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Ensures that all passwords include at least two alphabetic characters, one of which must be capitalized.	<b>Command:</b> <code>chsec -f /etc/security/user -s user -a minalpha=4.</code> <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Specifies the minimum number of nonalphabetic characters in a password to 2.	<b>Command:</b> <code>#chsec -f /etc/security/user -s user -a minother=2.</code> <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Ensure that all passwords contain no repetitive characters.	<b>Command:</b> <code>#chsec -f /etc/security/user -s user -a maxrepeats=1.</code> <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Ensure that a password is not reused within the last five changes.	<b>Command:</b> <code>#chsec -f /etc/security/user -s user -a histsize=5.</code> <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Specifies the maximum number of weeks to 13 weeks, for the password to remain valid.	<b>Command:</b> <code>#chsec -f /etc/security/user -s user -a maxage=8.</code> <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Removes any minimum number of week requirements before a password can be changed.	<b>Command:</b> <code>#chsec -f /etc/security/user -s user -a minage=2.</code> <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Specifies the maximum number of weeks to 4 weeks, to change an expired password, after the value of the <code>maxage</code> parameter set by the user expires.	<b>Command:</b> <code>#chsec -f /etc/security/user -s user -a maxexpired=4.</code> <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.



Table 7. HIPAA rules and implementation details (continued)

Sections of HIPAA Security Rule	Implementation specification	The aixpert implementation	Commands and return values
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Specifies the minimum number of characters that cannot be repeated from the old password is 4 characters.	<b>Command:</b>  <code>#chsec -f /etc/security/user -s user -a mindiff=4.</code>  <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Specifies that the number of days is 5 to wait before the system issues a warning that a password change is required.	<b>Command:</b>  <code>#chsec -f /etc/security/user -s user -a pwdwarntime = 5.</code>  <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Verifies the correctness of user definitions and fixes the errors.	<b>Command:</b>  <code>/usr/bin/usrck -y ALL</code>  <code>/usr/bin/usrck -n ALL.</code>  <b>Return value:</b> The command does not return a value. The command checks and fixes the errors, if any.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Locks the account after three consecutive failed login attempts.	<b>Command:</b>  <code>#chsec -f /etc/security/user -s user -a loginretries=3.</code>  <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Specifies the delay between one unsuccessful login to the other as 5 seconds.	<b>Command:</b>  <code>chsec -f /etc/security/login.cfg -s default -a logindelay=5.</code>  <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Specifies the number of unsuccessful login attempts on a port, before the port is locked as 10.	<b>Command:</b>  <code>chsec -f /etc/security/lastlog -s username -a \ unsuccessful_login_count=10.</code>  <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Specifies the time interval in a port for the unsuccessful login attempts before the port is disabled as 60 seconds.	<b>Command:</b>  <code>#chsec -f /etc/security/lastlog -s user -a time_last_unsuccessful_login=60.</code>  <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.

Table 7. HIPAA rules and implementation details (continued)

Sections of HIPAA Security Rule	Implementation specification	The aixpert implementation	Commands and return values
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Specifies the time interval after which a port is unlocked and after being disabled, as 30 minutes.	<b>Command:</b>  <code>#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30.</code>  <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Specifies the time interval to type a password as 30 seconds.	<b>Command:</b>  <code>chsec -f /etc/security/login.cfg -s usw -a logintimeout=30.</code>  <b>Return value:</b> If successful, this script exits with a value of 0. If unsuccessful, the command exits with an error code of 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Password Management (A):Implements the procedures for creating, changing, and protecting passwords.	Ensure that accounts are locked after 35 days of inactivity.	<b>Command:</b>  <code>grep TMOUT= /etc/security /.profile &gt; /dev/null 2&gt;&amp;1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}.</code>  <b>Return value:</b> If the command fails to set the value of <code>account_locked</code> to <code>true</code> , the script exits with a value of 1. Otherwise, the command exits with a value of 0.
164.312 (c) (1)	Implements the policies and procedures to protect the EPHI from incorrect alteration or destruction.	Set the trusted execution (TE) policies to ON.	<b>Command:</b>  Turns on <code>CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON</code> For example, <code>trustchk -p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON.</code>  <b>Return value:</b> On failure, the script exits with a value of 1.
164.312 (e) (1)	Implements the technical security measures to prevent unauthorized access to the EPHI that is being transmitted over an electronic communication network.	Determines whether the <code>ssh</code> filesets are installed. If not, displays an error message.	<b>Command:</b>  <code># lsipp -l   grep openssh &gt; /dev/null 2&gt;&amp;1.</code>  <b>Return value:</b> If return code for this command is 0, the script exits with a value of 0. If <code>ssh</code> filesets are not installed, the script exits with a value of 1 and displays the error message <code>Install ssh filesets for secure transmission.</code>

The following table details about the several functions of the HIPAA Security Rule and each function includes several standards and implementation specifications.

Table 8. HIPAA Functions and implementation details

HIPAA functions	Implementation specification	The aixpert implementation	Commands and return values
Error logging	Consolidates errors from different logs and sends emails the administrator.	Determines whether any hardware errors exist.  Determines whether there are any unrecoverable errors from the <b>trcfile</b> file in the location, <code>/var/adm/ras/trcfile</code> .  Sends the errors to <b>root@&lt;hostname&gt;</b> .	<b>Command:</b>  <b>errpt -d H.</b>  <b>Return value:</b> If successful, this command exits with a value of 0. If unsuccessful, the command exits with a value of 1.
FPM enablement	Changes file permissions.	Changes the permission of files from a list of permissions and files by using the <b>fpm</b> command.	<b>Command:</b>  <b># fpm -1 &lt;level&gt; -f &lt;commands file&gt;</b> .  <b>Return value:</b> If successful, this command exits with a value of 0. If unsuccessful, the command exits with a value of 1.
RBAC enablement	Creates <b>isso</b> , <b>so</b> , and <b>sa</b> users and assigns appropriate roles to the users.	Suggests that you create <b>isso</b> , <b>so</b> , and <b>sa</b> users.  Assigns appropriate roles to the users.	<b>Command:</b>  <b>/etc/security/pscxpert/bin/RbacEnablement.</b>

## Managing Security and Compliance Automation

Learn about the process of planning and deploying PowerSC Security and Compliance Automation profiles on a group of systems in accordance with the accepted IT governance and compliance procedures.

As part of compliance and IT governance, systems running similar workload and security classes of data must be managed and configured consistently. To plan and deploy compliance on systems, complete the following tasks:

### Identifying the work groups of the system

The compliance and IT governance guidelines state that the systems running on similar workload and security classes of data must be managed and configured consistently. Therefore, you must identify all systems in a similar workgroup.

### Using a nonproduction test system for the initial setup

Apply the appropriate PowerSC compliance profile to the test system.

Consider the following examples for applying compliance profiles to the AIX operating system.

Example 1: Applying DoD.xml

```
% aixpert -f /etc/security/aixpert/custom/DoD.xml
Processedrules=38      Passedrules=38  Failedrules=0   Level=AllRules
```

```
Input file=/etc/security/aixpert/custom/DoD.xml
```

In this example, there are no failed rules, that is, `Failedrules=0`. This means that all rules are successfully applied, and the test phase can be started. If there are failures, detailed output is generated.

Example 2: Applying PCI.xml with a failure

```
# aixpert -f /etc/security/aixpert/custom/PCI.xml
do_action(): rule(pci_grpck) : failed.
Processedrules=85      Passedrules=84  Failedrules=1   Level=AllRules
```

Input file=/etc/security/aixpert/custom/PCI.xml

The failure of the pci\_grpck rule must be resolved. The possible causes for failure include the following reasons:

- The rule does not apply to the environment and must be removed.
- There is an issue on the system that must be fixed.

## Investigating a failed rule

In most cases, there is no failure when applying a PowerSC security and compliance profile. However, the system can have prerequisites related to installation that are missing or other issues that require attention from the administrator.

The cause of the failure can be investigated by using the following example:

View the /etc/security/aixpert/custom/PCI.xml file and locate the failing rule. In this example the rule is pci\_grpck. Run the **fgrep** command, search the pci\_grpck failing rule, and see the associated XML rule.

```
fgrep -p pci_grpck /etc/security/aixpert/custom/PCI.xml
<AIXPertEntry name="pci_grpck" function="grpck"
<AIXPertRuleType type="DLS"/
<AIXPertDescription>Implements portions of PCI Section 8.2,
Check group definitions: Verifies the correctness of group definitions and fixes the errors
</AIXPertDescription
<AIXPertPrereqList>bos.rte.security,bos.rte.date,bos.rte.ILS</AIXPertPrereqList
<AIXPertCommand
/etc/security/aixpert/bin/execcmds</AIXPertCommand
<AIXPertArgs
"/usr/sbin/grpck -y ALL; /usr/sbin/grpck -n ALL"</AIXPertArgs
<AIXPertGroup
User Group System and Password Definitions</AIXPertGroup
</AIXPertEntry
```

From the pci\_grpck rule, the /usr/sbin/grpck command can be seen.

## Updating the failed rule

When applying a PowerSC security and compliance profile, you can detect errors.

The system can have missing installation prerequisites or other issues that require attention from the administrator. After determining the underlying command of the failed rule, examine the system to understand the configuration command that is failing. The system might have a security issue. It might also be the case that a particular rule is not applicable to the environment of the system. Then, a custom security profile must be created.

## Creating custom security configuration profile

If a rule is not applicable to the specific environment of the system, most compliance organizations permit documented exceptions.

To remove a rule and to create a custom security policy and configuration file, complete the following steps:

1. Copy the contents of the following files into a single file named /etc/security/aixpert/custom/<my\_security\_policy>.xml:  
/etc/security/aixpert/custom/[PCI.xml|DoD.xml|SOX-COBIT.xml]

2. Edit the `<my_security_policy>.xml` file by removing the rule that is not applicable from the opening XML tag `<AIXPertEntry name...` to the ending XML tag `</AIXPertEntry`.

You can insert additional configuration rules for security. Insert the additional rules to the XML `AIXPertSecurityHardening` schema. You cannot change the PowerSC profiles directly, but you can customize the profiles.

For most environments, you must create a custom XML policy. To distribute a customer profile to other systems, you must securely copy the customized XML policy to the system that requires the same configuration. A secure protocol, such as secure file transfer protocol (SFTP), is used to distribute a custom XML policy to other systems, and the profile is stored in a secure location `/etc/security/aixpert/custom/<my_security_policy.xml>/etc/security/aixpert/custom/`

Log on to the system where a custom profile must be created, and run the following command:

```
pscxpert -f : /etc/security/aixpert/custom/<my_security_policy>.xml
```

## Testing the applications with AIX Profile Manager

The security configurations can affect applications and the way the system is accessed and managed. It is important to test the applications and the expected management methods of the system before deploying the system into a production environment.

The regulatory compliance standards impose a security configuration that is more stringent than an out-of-the-box configuration. To test the system, complete the following steps:

1. Select **View and Manage profiles** from the right pane of the AIX Profile Manager welcome page.
2. Select the profile that is used by the template for deploying to the systems to be monitored.
3. Click **Compare**.
4. Select the managed group, or select individual systems within the group and click **Add**, to add them to the selected box.
5. Click **OK**.

The compare operation starts.

## Monitoring systems for continued compliance with AIX Profile Manager

The security configurations can affect applications and the way the system is accessed and managed. It is important to monitor the applications and the expected management methods of the system when deploying the system into a production environment.

To use AIX Profile Manager to monitor an AIX system, complete the following steps:

1. Select **View and Manage profiles** from the right pane of the AIX Profile Manager welcome page.
2. Select the profile that is used by the template for deploying to the systems to be monitored.
3. Click **Compare**.
4. Select the managed group, or select individual systems within the group and add them to the selected box.
5. Click **OK**.

The compare operation starts.

---

## Configuring PowerSC Security and Compliance Automation

Learn the procedure to configure PowerSC for Security and Compliance Automation from the command-line and by using AIX Profile Manager.

## Configuring PowerSC compliance options settings

Learn the basics of PowerSC security and compliance automation feature, test the configuration on nonproduction test systems, and plan and deploy the settings. When you apply a compliance configuration, the settings change numerous configuration settings on the operating system.

**Note:** Some compliance standards and profiles disable Telnet, because Telnet uses clear text passwords. Therefore, you must have Open SSH installed, configured, and working. You can use any other secure means of communication with the system being configured. These compliance standards require the root login to be disabled. Configure one or more non-root users before you continue applying the configuration changes. This configuration does not disable root, and you can log in as a non-root user and run the **su** command to root. Test if you can establish the SSH connection to the system, log in as the non-root user, and run command to root.

To access the DoD, PCI, SOX, or COBIT configuration profiles, use the following directory:

- The profiles in the AIX operating system are placed in the `/etc/security/aixpert/custom` directory.
- The profiles in Virtual I/O Server (VIOS) are placed in the `/etc/security/aixpert/core` directory.

## Configuring PowerSC compliance from the command line

Implement or check the compliance profile by using the **pscxpert** command on the AIX system, and the **viosecure** command on the Virtual I/O Server (VIOS).

To apply the PowerSC compliance profiles on an AIX system, enter one of the following commands, which depends on the level of security compliance you want to apply.

Table 9. PowerSC commands for AIX

Command	Compliance standard
<code>% pscxpert -f /etc/security/aixpert/custom/DoD.xml</code>	<i>US Department of Defense UNIX security technical implementation guide</i>
<code>% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml</code>	<i>Health Insurance Portability and Accountability Act</i>
<code>% pscxpert -f /etc/security/aixpert/custom/PCI.xml</code>	<i>Payment card industry-Data security standard</i>
<code>% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml</code>	<i>Sarbanes-Oxley Act of 2002 – COBIT IT Governance</i>

To apply the PowerSC compliance profiles on a VIOS system, enter one of the following commands for the level of security compliance you want to apply.

Table 10. PowerSC commands for the Virtual I/O Server

Command	Compliance Standard
<code>% viosecure -file /etc/security/aixpert/custom/DoD.xml</code>	<i>US Department of Defense UNIX security technical implementation guide</i>
<code>% viosecure -file /etc/security/aixpert/custom/Hipaa.xml</code>	<i>Health Insurance Portability and Accountability Act</i>
<code>% viosecure -file /etc/security/aixpert/custom/PCI.xml</code>	<i>Payment card industry-Data security standard</i>
<code>% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml</code>	<i>Sarbanes-Oxley Act of 2002 – COBIT IT Governance</i>

The **pscxpert** command on the AIX system and the **viosecure** command in VIOS can take time to run because they are checking or setting the entire system, and making security-related configuration changes. The output is similar to the following example:

```
Processedrules=38      Passedrules=38  Failedrules=0   Level=AllRules
```

However, some rules fail depending on the AIX environment, installation set, and the previous configuration.

For example, a prerequisite rule can fail because the system does not have the required installation files. It is necessary to understand each failure and resolve it before deploying the compliance profiles throughout the data center.

**Related concepts:**

“Managing Security and Compliance Automation” on page 99

Learn about the process of planning and deploying PowerSC Security and Compliance Automation profiles on a group of systems in accordance with the accepted IT governance and compliance procedures.

## Configuring PowerSC compliance with AIX Profile Manager

Learn the procedure to configure PowerSC security and compliance profiles and to deploy the configuration onto an AIX managed system by using the AIX Profile Manager.

To configure PowerSC security and compliance profiles by using AIX Profile Manager, complete the following steps:

1. Log in to IBM Systems Director and select AIX Profile Manager.
2. Create a template that is based on one of the PowerSC security and compliance profiles by completing the following steps:
  - a. Click **View and manage templates** from the right pane of the AIX Profile Manager welcome page.
  - b. Click **Create**.
  - c. Click **Operating System** from the **Template type** list.
  - d. Provide a name for the template in the **Configuration template name** field.
  - e. Click **Continue > Save**.
3. Select the profile to use with the template by selecting **Browse** under the **Select which profile to use for this template** option. The profiles display the following items:
  - `ice_DLS.xml` is the default security level of the AIX operating system.
  - `ice_DoD.xml` is the Department of Defense Security and Implementation Guide for UNIX settings.
  - `ice_HLS.xml` is a generic high-level security for AIX settings.
  - `ice_LLS.xml` is the low-level security for AIX settings.
  - `ice_MLS.xml` is the medium level security for AIX settings.
  - `ice_PCI.xml` is the Payment Card Industry setting for the AIX operating system.
  - `ice_SOX.xml` is the SOX or COBIT settings for the AIX operating system.
4. Remove any profile from the selected box.
5. Select **Add** to move the required profile into the selected box.
6. Click **Save**.

To deploy the configuration onto an AIX managed system, complete the following steps:

1. Select **View and Manage Templates** from the right pane of the AIX Profile Manager welcome page.
2. Select the required template to deploy.
3. Click **Deploy**.
4. Select the systems to deploy the profile, and click **Add** to move the required profile into the selected box.
5. Click **OK** to deploy the configuration template. The system is configured according to the selected template of the profile.

For the deployment to be successful for DoD, PCI, or SOX, PowerSC Express Edition or PowerSC Standard Edition must be installed at the end point of the AIX system. If the system that is being

deployed does not have PowerSC installed, the deployment fails. The IBM Systems Director deploys the configuration template to the selected AIX system end points and configures them according to the compliance requirements.

**Related information:**

AIX Profile Manager

IBM Systems Director



---

## PowerSC Real Time Compliance

The PowerSC Real Time Compliance feature continuously monitors enabled AIX systems to ensure that they are configured consistently and securely.

The PowerSC Real Time Compliance feature works with the PowerSC Compliance Automation and AIX Security Expert policies to provide notification when compliance violations occur or when a monitored file is changed. When the security configuration policy of a system is violated, the PowerSC Real Time Compliance feature sends an email or a text message to alert the system administrator.

The PowerSC Real Time Compliance feature is a passive security feature that supports predefined or changed compliance profiles that include the Department of Defense Security Technical Implementation Guide, the Payment Card Industry Data Security Standard, the Sarbanes-Oxley Act, and COBIT compliance. It provides a default list of files to monitor for changes, but you can add files to the list.

---

## Installing PowerSC Real Time Compliance

The PowerSC Real Time Compliance feature is installed with the PowerSC Express Edition, and it is not part of the base AIX operating system.

To install the PowerSC Express Edition, which includes the PowerSC Real Time Compliance, complete the following steps:

1. Ensure that you are running one of the following AIX operating systems on the system where you are installing the PowerSC Real Time Compliance feature:
  - IBM AIX 6 with Technology Level 7, or later, with AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 6.1.7.0), or later
  - IBM AIX 7 with Technology Level 1, or later, with AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 7.1.1.0), or later
2. If you have already installed PowerSC Express Edition version 1.1.2.0, or later, you can add the required files for the PowerSC Real Time Compliance feature by reinstalling the PowerSC Express Edition or by updating the installed version of the PowerSC Real Time Compliance feature to the latest version.
3. To update the PowerSC Real Time Compliance feature fileset, install the powerscExp.rtc fileset from the installation package for PowerSC Express Edition version 1.1.2.0, or later.
4. For a new installation of PowerSC Express Edition version 1.1.2.0, or earlier, follow the instructions in Installing PowerSC Express Edition Version 1.1.2, or earlier.

---

## Configuring PowerSC Real Time Compliance

You can configure PowerSC Real Time Compliance to send alerts when violations of a compliance profile or changes to a monitored file occur. Some examples of the profiles include, the Department of Defense Security Technical Implementation Guide, the Payment Card Industry Data Security Standard, the Sarbanes-Oxley Act, and COBIT.

You can configure PowerSC Real Time Compliance by using one of the following methods:

- Enter the **mkrtc** command.
- Run the SMIT tool by entering the following command:  
smit RTC

## Identifying files monitored by the PowerSC Real Time Compliance feature

The PowerSC Real Time Compliance feature monitors a default list of files from the high-level security settings for changes, which can be customized by adding or removing files from the list of files in the `/etc/security/rtc/rtcd_policy.conf` file.

There are two methods of identifying the compliance template that is applied on a system. One method is to use the `pscxpert` command, and the other is to use the AIX Profile Manager with IBM Systems Director.

When the compliance profile is identified, you can add additional files to the list of files to monitor by including the additional files in the `/etc/security/rtc/rtcd_policy.conf` file. After the file is saved, the new list is immediately used as a baseline and monitored for changes without restarting the system.

## Setting alerts for PowerSC Real Time Compliance

You must configure the notification of the PowerSC Real Time Compliance feature by indicating the type of alerts and the recipients of the alerts.

The `rtcd` daemon, which is the main component of the PowerSC Real Time Compliance feature, obtains its information about the types of alerts and recipients from the `/etc/security/rtc/rtcd.conf` configuration file. You can edit this file to update the information by using a text editor.

For more information about the options and how to modify this file, see the information about the `rtcd.conf` file.

### Related information:

[/etc/security/rtc/rtcd.conf file format for real-time compliance](#)

---

## PowerSC Express Edition commands

The commands that are available with PowerSC Express Edition provide the method of changing the compliance settings by using the command line.

---

### pscxpert Command

#### Purpose

Aids the system administrator in setting the security configuration.

#### Syntax

**pscxpert**

**pscxpert -l h | high | m | medium | l | low | d | default [ -p ] [-n -o *filename*] [ -a -o *filename* ]**

**pscxpert -c [ -P *filename*] [-r] [-R] [-l h | high | m | medium | l | low | d | default ] [ -p ]**

**pscxpert -u [ -p ]**

**pscxpert -d**

**pscxpert [-f *profile\_name* ]**

**pscxpert [-f *profile\_name* ] [ -a -o *filename* ] [ -p ]**

**pscxpert -t**

#### Description

The **pscxpert** command sets a variety of system configuration settings to enable the desired security level.

Running the **pscxpert** command with only the **-l** flag set implements the security settings promptly without allowing the user to configure the settings. For example, running the **pscxpert -l high** command applies all of the high-level security settings to the system automatically. However, running the **pscxpert -l** command with the **-n** and **-o *filename*** options saves the security settings to a file specified by the *filename* parameter. The **-f** flag then applies the new configurations.

After the initial selection, a menu is displayed itemizing all security configuration options associated with the selected security level. These options can be accepted in whole or individually toggled off or on. After any secondary changes, the **pscxpert** command continues to apply the security settings to the computer system.

- | Run the **pscxpert** command as the root user of the target Virtual I/O Server. When you are not logged in
- | as the root user of the target Virtual I/O Server, run the **oem\_setup\_env** command before you run the
- | **pscxpert** command.

**Note:** Rerun the **pscxpert** command after any major systems changes, such as the installation or updates of software. If a particular security configuration item is not selected when the **pscxpert** command is rerun, that configuration item is skipped.

#### Flags

Item	Description
-a	The settings with the associated security level options are written to the file specified by the <b>-o</b> flag, in abbreviated format. You must specify the <b>-o</b> option when you specify the <b>-a</b> option.
-c	Checks the security settings against the previously applied set of rules. If the check against a rule fails, the previous versions of the rule are also checked. This process continues until the check passes, or until all of the instances of the failed rule in the <b>/etc/security/aixpert/core/appliedaixpert.xml</b> file are checked.
-d	Displays the document type definition (DTD).
-f	Applies the security settings that are provided in the specified <i>profile_name</i> file. The profiles are located in the <b>/etc/security/aixpert/custom</b> directory. The available profiles include the following standard profiles:

**DataBase.xml**

This file contains the requirements for the default database settings.

**DoD.xml**

This file contains the requirements for the Department of Defense Security Technical Implementation Guide (STIG) settings.

**DoD\_to\_AIXDefault.xml**

This changes the settings to the default AIX settings.

**DoDv2.xml**

This file contains the requirements for version 2 of the Department of Defense Security Technical Implementation Guide (STIG) settings.

**DoDv2\_to\_AIXDefault.xml**

This changes the settings to the default AIX settings.

**Hipaa.xml**

This file contains the requirements for the Health Insurance Portability and Accountability Act (HIPAA) settings.

**PCI.xml** This file contains the requirements for the Payment card industry Data Security Standard settings.

**PCIv3.xml**

This file contains the requirements for the Payment card industry Data Security Standard Version 3 settings.

**PCI\_to\_AIXDefault.xml**

This file changes the settings to the default AIX settings

**PCIv3\_to\_AIXDefault.xml**

This file changes the settings to the default AIX settings

**SOX-COBIT.xml**

This file contains the requirements for the Sarbanes-Oxley Act and COBIT settings.

You can also create custom profiles in the same directory and apply them to your settings by renaming and modifying the existing XML files.

For example, the following command applies the HIPAA profile to your system:

```
pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
```

When you specify the **-f** option, security settings are consistently applied from system to system by securely transferring and applying an **appliedaixpert.xml** file from system to system.

All of the successfully applied rules are written to the **/etc/security/aixpert/core/appliedaixpert.xml** file and the corresponding undo action rules are written to the **/etc/security/aixpert/core/undo.xml** file.

Item	Description
-l	<p>Sets the system security settings to the specified level. This flag has the following options:</p> <p><b>h   high</b> Specifies high-level security options.</p> <p><b>m   medium</b> Specifies medium-level security options.</p> <p><b>l   low</b> Specifies low-level security options.</p> <p><b>d   default</b> Specifies AIX standards-level security options.</p> <p>If you specify both the <b>-l</b> and <b>-n</b> flags, the security settings are not implemented on the system; however, they are only written to the file that you specified in the <b>-o</b> flag.</p> <p>All the successfully applied rules are written to the <code>/etc/security/aixpert/core/appliedaixpert.xml</code> file and the corresponding undo action rules are written to the <code>/etc/security/aixpert/core/undo.xml</code> file.</p> <p><b>Attention:</b> When you use the <b>d   default</b> option, the option can overwrite the configured security settings that you had previously set by using the <b>pscxpert</b> command or independently, and restores the system to its traditional open configuration.</p>
-n	Writes the settings with the associated security level options to the file specified by the <b>-o</b> flag. You must specify the <b>-o</b> option when you use the <b>-n</b> option.
-o	Stores security output to the file that is specified by the <i>filename</i> variable. The read and write permissions of the output file are set to root as a security precaution. This file must be protected against unwanted access.
-p	Specifies that the output of the security rules is displayed by using verbose output. The <b>-p</b> option logs the rules processed into the audit subsystem if the <b>auditing</b> option is turned on. This option can be used with any of the <b>-l</b> , <b>-u</b> , <b>-c</b> , and <b>-f</b> options.
-P	Accepts the profile name as input. This option is used along with the <b>-c</b> option. The <b>-c</b> option along with the <b>-P</b> option is used to check the compatibility of the system with the profile passed.
-r	Writes the existing settings of the system to the <code>/etc/security/aixpert/check_report.txt</code> file. You can use the output in security or compliance audit reports. The report describes each setting, how it might relate to a regulatory compliance requirement, and whether the check passed or failed.
-R	Produces the same output as the <b>-r</b> flag, but this flag also appends a description about each script or program used to implement the configuration setting.
-t	Displays the type of the profile applied on the system.
-u	Undoes the security settings that are applied.
	<b>Note:</b> You cannot use the <b>-u</b> flag to reverse the application of the Department of Defense Version 2 profile or the Payment Card Industry Version 3 profile. To remove these profiles after they are added, apply the profile that is included with the <code>DoDv2_to_AIXDefault.xml</code> file or the <code>PCIv3_to_AIXDefault.xml</code> file, respectively.

## Parameters

Item	Description
<i>filename</i>	The output file that stores the security settings. Root permission is required to access this file.
<i>profile_name</i>	The file name of the profile that provides compliance rules for the system. Root permission is required to access this file.

## Security

The **pscxpert** command can be run only by root.

## Examples

- To write all of the high-level security options to an output file, enter the following command:  

```
pscxpert -l high -n -o /etc/security/pscxpert/plugin/myPreferredSettings.xml
```

After completing this command, the output file can be edited, and specific security roles can be commented out by enclosing them in the standard XML comment string (<!-- begins the comment and -\> closes the comment).

2. To apply the security settings from the Department of Defense STIG configuration file, enter the following command:

```
pscxpert -f /etc/security/aixpert/custom/DoD.xml
```

3. To apply the security settings from the HIPAA configuration file, enter the following command:

```
pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
```

4. To check the security settings of the system, and to log the rules that failed into the audit subsystem, enter the following command:

```
pscxpert -c -p
```

5. To generate reports and write them to the /etc/security/aixpert/check\_report.txt file, enter the following command:

```
pscxpert -c -r
```

## Location

Item	Description
<code>/usr/sbin/pscxpert</code>	Contains the <code>pscxpert</code> command.

## Files

Item	Description
<code>/etc/security/aixpert/log/aixpert.log</code>	Contains a trace log of applied security settings. This does not use the syslog standard. The <code>pscxpert</code> command writes directly to the file, has read-write permissions, and requires root security.
<code>/etc/security/aixpert/log/firstboot.log</code>	Contains a trace log of the security settings that were applied during the first boot of a Secure by Default (SbD) installation.
<code>/etc/security/aixpert/core/undo.xml</code>	Contains an XML listing of security settings, which can be undone.

---

## Notices

This information was developed for products and services that are offered in the USA.

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

IBM 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:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
United States of America*

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

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION 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 states 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. IBM 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-IBM 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 IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply 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:

*IBM Corporation  
Dept. LRAS/Bldg. 903  
11501 Burnet Road  
Austin, TX 78758-3400  
USA*

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 IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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 the names and addresses used by an actual business enterprise 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 IBM, 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. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM 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:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. \_enter the year or years\_. All rights reserved.

---

## Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as the customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at <http://www.ibm.com/privacy> and IBM’s Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at <http://www.ibm.com/software/info/product-privacy>.

---

## Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

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



---

# Index

## C

Configuring PowerSC Security and Compliance Automation 102

## D

Department of Defence STIG compliance 10

## F

feature  
PowerSC Real Time Compliance 105

## H

hardware and software requirements 5

## I

Investigating a failed rule 100

## M

Managing Security and Compliance Automation 99, 100, 101  
Monitoring systems for continued compliance 101

## O

overview 5

## P

Payment Card Industry - DSS compliance 80  
PowerSC 10, 80, 93, 99, 102  
Real-Time Compliance 105  
PowerSC Express Edition 5  
pscxpert command 107

## R

Real-Time Compliance 105

## S

security  
PowerSC  
Real-Time Compliance 105  
SOX and COBIT 93

## T

Testing the applications 101

## U

Updating the failed rule 100







Printed in USA