IBM PowerSC

Standard Edition

Version 1.1.5

PowerSC Standard Edition

IBM

IBM PowerSC

Standard Edition

Version 1.1.5

PowerSC Standard Edition

IBM

Contents

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:

Bold	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.
Italics	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 Standard Edition 1.1.5

Read about new or significantly changed information for the PowerSC™ Standard Edition Version 1.1.5 topic collection.

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

March 2017

Include AIX 7.2 as a supported operating system in the section that explains the PowerSC Standard Edition features, components, and hardware support.

- "PowerSC Standard Edition 1.1.5 concepts" on page 5

October 2016

- Added information about compliance profiles in the following topics:
  - "North American Electric Reliability Corporation compliance" on page 92
  - "Payment Card Industry - Data Security Standard compliance" on page 71
- Added a Graphical User Interface (GUI). For more information about the GUI, see the "PowerSC graphical user interface (GUI)" on page 137 topic.

PowerSC Standard Edition Release Notes

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

PowerSC Standard Edition Release Notes Version 1.1.5

The following release notes pertain to PowerSC Standard Edition Release Notes Version 1.1.5.

Setting the Resident Set Size (rss) on the PowerSC graphical user interface (GUI) server

The PowerSC GUI server must have the Resident Set Size (rss) value set to at least 131072 blocks (64 MB). To check or change this setting:

1. You must be a root user or a sudo root user to check or change this setting on the PowerSC GUI server

2. Edit the `/etc/security/limits` file.

3. Search for the occurrence of rss in the file. For example:

```
default: fsize = 2097151
          core = 2097151
           cpu = -1
          data = 262144
           rss = 65536
         stack = 65536
       nofiles = 2000
```

4. The rss value is frequently set to the default value of 65536 (32 MB). Change the rss to a value of 131072, which is 64 MB. For example:

```
default: fsize = 2097151
          core = 2097151
           cpu = -1
          data = 262144
           rss = 131072
         stack = 65536
       nofiles = 2000
```

5. Reboot the server. On the AIX operating system, you can use the command **shutdown -Fr**.

Backing up PowerSC GUI server directories

On the PowerSC GUI server, some site-specific customizations are stored under a site-specific subdirectory of the installation path. For example:

- Custom profiles and custom groups that are created by the user are stored under the directory `/opt/powersc/uiServer/knowledge/site/powerscui`

You should ensure that the `/opt/powersc/uiServer/knowledge/site/powerscui/` directory is backed up.

In the following example, the commands are run from the `/opt/powersc/uiServer/knowledge/site/powerscui/` directory.

To back up the directory, run the following command:

```
tar -cvf siteStuff.tar /opt/powersc/uiServer/knowledge/site/powerscui/
```

To restore a backup file, run the following command:

```
tar -xvf siteStuff.tar
```

Payment Card Industry (PCIv3) standard released with PowerSC 1.1.5

For the new version of the Payment Card Industry (PCIv3) standard that is released with PowerSC 1.1.5, you must install APAR IV73419 on the AIX operating system.

Trusted Network connect for OpenSource packages

A processing delay might occur while the TNC Server is receiving the OpenSource packages from the Patch Management Server.

Read this information before installing PowerSC

To view the most current version of the Release Notes, see the online Release Notes in IBM® Knowledge Center

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

Note: Before you use this software, you should go to the Fix Central website and install the latest available fixes that address security vulnerabilities and other critical issues.

Installation, migration, upgrade, and configuration information

For information about installing PowerSC Standard Edition, see Installing PowerSC Standard Edition Version 1.1.5.

For information about hardware and versions of the AIX operating system that are supported for PowerSC Standard Edition, see PowerSC Standard Edition 1.1.5 concepts.

Additional fileset requirement for running Trusted Network Connect

To run Trusted Network Connect, you must install the `powerscStd.tnc_commands` fileset that is available on your IBM PowerSC Standard Edition DVD. Install the fileset on your AIX system by using the **installp** command. This fileset provides the function of the **psconf** and **pmconf** commands.

Note: If you are using the IP Referrer function of Trusted Network Connect, you must also install the `powerscStd.tnc_commands` fileset on your VIOS system.

PowerSC Standard Edition 1.1.5 concepts

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

PowerSC Standard Edition 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 Standard Edition is a suite of features that includes Security and Compliance Automation, Trusted Boot, Trusted Firewall, Trusted Logging, and Trusted Network Connect and Patch management. 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 Standard Edition components, description, operating system support, and hardware support

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: • Payment Card Industry Data Security Standard (PCI DSS) • Sarbanes-Oxley Act and COBIT compliance (SOX/COBIT) • U.S. Department of Defense (DoD) STIG • Health Insurance Portability and Accountability Act (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6® • POWER7® • POWER8
Trusted Boot	Measures the boot image, operating system, and applications, and attests their trust by using the virtual trusted platform module (TPM) technology.	• AIX 6 with 6100-07, or later • AIX 7 with 7100-01, or later	POWER7 firmware eFW7.4, or later
Trusted Firewall	Saves time and resources by enabling direct routing across specified virtual LANs (VLANs) that are controlled by the same Virtual I/O Server.	• AIX 6.1 • AIX 7.1 • AIX 7.2 • VIOS Version 2.2.1.4, or later	• POWER6 • POWER7 • POWER8 • Virtual I/O Server Version 6.1S, or later
Trusted Logging	The logs of AIX are centrally located on the Virtual I/O Server (VIOS) in real time. This feature provides tamperproof logging and convenient log backup and management.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8

Table 1. PowerSC Standard Edition components, description, operating system support, and hardware support (continued)

Components	Description	Operating system supported	Hardware supported
Trusted Network Connect and patch management	Verifies that all AIX systems in the virtual environment are at the specified software and patch level and provides management tools to ensure that all AIX systems are at the specified software level. Provides alerts if a down-level virtual system is added to the network or if a security patch is issued that affects the systems.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Trusted Network Connect client	The Trusted Network Connect client requires one of the components listed with the operating system.	• AIX 6.1 with 6100-06, or later • AIX version 7.1 Service Update Management Assistant (SUMA) console system within the SUMA environment for patch management • AIX version 7.2.1 Service Update Management Assistant (SUMA) console system within the SUMA environment for patch management	

Installing PowerSC Standard Edition 1.1.5

You must install a fileset for each specific function of PowerSC Standard Edition.

The following filesets are available for PowerSC Standard Edition and PowerSC graphical user interface (GUI):

- `powerscStd.ice`: Installed on AIX systems that require the Security and Compliance Automation feature of PowerSC Standard Edition.
- `powerscStd.vtpm`: Installed on AIX systems that require the Trusted Boot feature of PowerSC Standard Edition.
- `powerscStd.vlog`: Installed on AIX systems that require the Trusted Logging feature of PowerSC Standard Edition.
- `powerscStd.tnc_pm`: Installed on the AIX Version 6.1 with the 6100-06 Technology Level, or later, or on AIX Version 7.1, or later, Service Update Management Assistant (SUMA) console system within the SUMA environment for patch management.
- `powerscStd.svm`: Installed on AIX systems that might benefit from the routing feature of PowerSC Standard Edition.
- `powerscStd.rtc`: Installed on AIX systems that require the Real Time Compliance feature of PowerSC Standard Edition.
- `powerscStd.uiAgent.rte`: Installed on AIX systems that will be managed using the PowerSC graphical user interface (GUI).
- `powerscStd.uiServer.rte`: Installed on the AIX system configured specifically for running the PowerSC graphical user interface (GUI) Server.

You can install PowerSC Standard Edition and PowerSC graphical user interface (GUI) by using one of the following interfaces:

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

To install PowerSC Standard 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/powerscStd.vtpm`, 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.

See "Installing PowerSC GUI" on page 138 for more information on installing the PowerSC graphical user interface (GUI)

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 Standard Edition:

```
% installp -lE -d  /usr/sys/inst.images/powerscStd.vtpm
```

Related concepts:

"PowerSC Standard Edition 1.1.5 concepts" on page 5
This overview of PowerSC Standard Edition explains the features, components, and the hardware support related to the PowerSC Standard Edition feature.

"Installing Trusted Boot" on page 109
There are some required hardware and software configurations that are required to install Trusted Boot.

"Installing Trusted Network Connect" on page 127
Installing the components of Trusted Network Connect (TNC) requires you to complete certain steps.

Related tasks:

"Installing Trusted Firewall" on page 115
Installing the PowerSC Trusted Firewall is similar to installing other PowerSC features.

"Installing Trusted Logging" on page 122
You can install the PowerSC Trusted Logging feature by using the command line interface or the SMIT tool.

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 Standard Edition.

The PowerSC Standard Edition installation package, 5765-PSE, must be installed on AIX managed systems. The installation package installs the `powerscStd.ice` fileset that can be implemented on the system by using the AIX Profile Manager or the **pscxpert** 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), the Payment Card Industry (PCI) data security standard (DSS), the Sarbanes-Oxley act, COBIT compliance (SOX/COBIT), and the Health Insurance Portability and Accountability Act (HIPAA).

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, 2.0, or 3.0. 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. You can use the PowerSC Standard Edition XML profiles with the **pscxpert** command, similar to ICEE.

The preconfigured compliance profiles delivered with PowerSC Standard 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. IBMPowerSC Standard 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 Standard 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/pscexpert/dodv2` directory.

PowerSC Standard Edition 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.	**Location**
			    `/etc/security/pscexpert/dodv2/trust`
			
			Compliance action
			    Ensures that the system meets the specified requirements.

AIX00040	2	The **securetcpip** command must be used.	**Location**
			    `/etc/security/pscexpert/dodv2/dodsecuretcpip`
			
			Compliance action
			    Ensures that the system meets the specified requirements.

AIX00060	2	The system must be checked weekly for unauthorized `setuid` files, and unauthorized modification to authorized `setuid` files.	**Location**
			    `/etc/security/pscexpert/dodv2/trust`
			
			Compliance action
			    Checks weekly to identify changes to the specified files.

AIX00080	1	The SYSTEM attribute must not be set to *none* for any account.	**Location**
			    `/etc/security/pscexpert/dodv2/SYSattr`
			
			Compliance action
			    Ensures that the specified attribute is set to a value other than *none*.
			    Note: 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.

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.	**Location**
			    /etc/security/pscexpert/dodv2/ntwkoptsdod
			Compliance action
			    Sets the value of the direct_broadcast network option to *0*.

AIX00210	2	The system must provide protection from Internet Control Message Protocol (ICMP) attacks on TCP connections.	**Location**
			    /etc/security/pscexpert/dodv2/ntwkoptsdod
			Compliance action
			    Sets the value of the tcp_icmpsecure network option to *1*.

AIX00220	2	The system must provide protection for the TCP stack against connection resets, synchronize (SYN), and data injection attacks.	**Location**
			    /etc/security/pscexpert/dodv2/ntwkoptsdod
			Compliance action
			    Ensures that the value for the tcp_tcpsecure network option is set to *7*.

AIX00230	2	The system must provide protection against IP fragmentation attacks.	**Location**
			    /etc/security/pscexpert/dodv2/ntwkoptsdod
			Compliance action
			    Sets the value of the ip_nfrag network option to *200*.

AIX00300	1,2,3	The system must not have the bootp service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			Compliance action
			    Disables the specified service.

AIX00310	2	The /etc/ftpaccess.ctl files must exist.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2loginherald
			Compliance action
			    Ensures that the file exists.

GEN000020	2	The system must require authentication when starting in single-user mode.	**Location**
			    /etc/security/pscexpert/dodv2/rootpasswd_home
			Compliance action
			    Ensures that the root account for any bootable partitions has a password in the /etc/security/passwd file.
			    Note: 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.

GEN000100	1	The operating system must be a supported release.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2cat1
			Compliance action
			    Displays the results of the specified rule tests.

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

GEN000120	2	The most current system security patches and updates must be installed.	**Location**
			    `/usr/sbin/instfix -i`
			    `/etc/security/pscexpert/dodv2/dodv2cat1`
			
			Compliance action
			    Configure this using the Trusted Network Connect feature.

GEN000140	2	The system must be checked weekly for unauthorized `setuid` files, and unauthorized modification to authorized `setuid` files.	**Location**
			    `/etc/security/pscexpert/dodv2/trust`
			
			Compliance action
			    Checks weekly to identify changes to the specified files.

GEN000220	2	The system must be checked weekly for unauthorized `setuid` files, and unauthorized modification to authorized `setuid` files.	**Location**
			    `/etc/security/pscexpert/dodv2/trust`
			
			Compliance action
			    Checks weekly to identify changes to the specified files.

GEN000240	2	The system clock must be synchronized to an authoritative Department of Defense (DoD) time source.	**Location**
			    `/etc/security/pscexpert/dodv2/dodv2cmntrows`
			
			Compliance action
			    Ensures that the system clock is compliant.

GEN000241	2	The system clock must be synchronized continuously, or at least daily.	**Location**
			    `/etc/security/pscexpert/dodv2/dodv2cmntrows`
			
			Compliance action
			    Ensures that the system clock is compliant.

GEN000242	2	The system must use at least two time sources for clock synchronization.	**Location**
			    `/etc/security/pscexpert/dodv2/dodv2netrules`
			
			Compliance action
			    Ensures that more than one time source is used for synchronizing the clock.

GEN000280	2	Direct logins to the following types of accounts must not be allowed:
		• application
		• default
		• shared
		• utility
			Location
			    `/etc/security/pscexpert/dodv2/lockacc_rlogin`
			
			Compliance action
			    Prevents direct logins to the specified accounts.

GEN000290	2	The system must not have unnecessary accounts.	**Location**
			    `/etc/security/pscexpert/dodv2/lockacc_rlogin`
			
			Compliance action
			    Ensures that there are no unused accounts.

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
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.	**Location** 　　/etc/security/pscexpert/dodv2/grpusrpass_chk **Compliance action** 　　Ensures that all accounts meet the specified requirements. 　　**Note:** 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.
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.	**Location** 　　/etc/security/pscexpert/dodv2/grpusrpass_chk **Compliance action** 　　Ensures that all accounts meet the specified requirements. 　　**Note:** 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.
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.	**Location** 　　/etc/security/pscexpert/dodv2/account **Compliance action** 　　This setting is automatically enabled to enforce this rule.
GEN000360	2	UIDs and GIDs that are reserved for system accounts must not be assigned to non-system accounts or non-system groups.	**Location** 　　/etc/security/pscexpert/dodv2/account **Compliance action** 　　This setting is automatically enabled to enforce this rule.
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.	**Location** 　　/etc/security/pscexpert/dodv2/grpusrpass_chk **Compliance action** 　　Ensures that all accounts meet the specified requirements.
GEN000400	2	The Department of Defense (DoD) login banner must be displayed immediately before, or as part of, console login prompts.	**Location** 　　/etc/security/pscexpert/dodv2/dodv2loginherald **Compliance action** 　　Displays the required banner.
GEN000402	2	The DoD login banner must be displayed immediately before, or as part of, graphical desktop environment login prompts.	**Location** 　　/etc/security/pscexpert/dodv2/dodv2loginherald **Compliance action** 　　The login banner is set to the Department of Defense banner.
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.	**Location** 　　/etc/security/pscexpert/dodv2/dodv2loginherald **Compliance action** 　　Displays the banner when you use FTP.

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

GEN000440	2	Successful and unsuccessful attempts to log in and log out must be recorded.	**Location**
			    /etc/security/pscexpert/dodv2/loginout
			
			Compliance action
			    Enables the required logging.

GEN000452	2	The system must display the date and time of the last successful account login at the time of each log in.	**Location**
			    /etc/security/pscexpert/dodv2/sshDoDconfig
			
			Compliance action
			    Displays the required information.

GEN000460	2	This rule disables an account after 3 consecutive failed logon attempts.	**Location**
			    /etc/security/pscexpert/dodv2/chusrattrdod
			
			Compliance action
			    Sets the login attempt limit to the specified value.

GEN000480	2	This rule sets the login delay time to 4 seconds.	**Location**
			    /etc/security/pscexpert/dodv2/chdefstanzadod
			
			Compliance action
			    Sets the login delay time to the required value.

GEN000540	2	This rule ensures the system global password configuration files are configured according to password requirements.	**Location**
			    /etc/security/pscexpert/dodv2/chusrattrdod
			
			Compliance action
			    Sets the required password settings.

GEN000560	1	All accounts on the system must have valid passwords.	**Location**
			    /etc/security/pscexpert/dodv2/grpusrpass_chk
			
			Compliance action
			    Ensures that accounts have passwords.

GEN000580	2	This rule ensures that all passwords contain a minimum of 14 characters.	**Location**
			    /etc/security/pscexpert/dodv2/chusrattrdod
			
			Compliance action
			    Sets the minimum password length to 14 characters.

GEN000585	2	The system must use a Federal Information Processing Standards (FIPS) 140-2 approved cryptographic hashing algorithm for generating account password hashes.	**Location**
			    /etc/security/pscexpert/dodv2/fipspasswd
			
			Compliance action
			    Ensures that the password hashes use an approved hashing algorithm.

GEN000590	2	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes.	**Location**
			    /etc/security/pscexpert/dodv2/fipspasswd
			
			Compliance action
			    Ensures that the password hashes use an approved hashing algorithm.

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.	**Location**
			    /etc/security/pscexpert/dodv2/fipspasswd
			
			Compliance action
			    Ensures that the password hashes use an approved hashing algorithm.

GEN000640	2	This rule requires a minimum of one non-alphabetic character in a password	**Location**
			    /etc/security/pscexpert/dodv2/chusrattrdod
			
			Compliance action
			    Sets the minimum number of non-alphabetic characters in a password to 1.

GEN000680	2	This rule ensures that passwords contain no more than three consecutive repeating characters	**Location**
			    /etc/security/pscexpert/dodv2/chusrattrdod
			
			Compliance action
			    Sets the maximum number of repeating characters in a password to 3.

GEN000700	2	This rule ensures the system global password configuration files are configured according to password requirements.	**Location**
			    /etc/security/pscexpert/dodv2/chusrattrdod
			
			Compliance action
			    Ensures that the password configuration files meet the requirements.

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.	**Location**
			    /etc/security/pscexpert/dodv2/loginout
			    /etc/security/pscexpert/dodv2/lockacc_rlogin
			
			Compliance action
			    This setting is automatically enabled.

GEN000740	2	All non-interactive and automated processing account passwords must be changed at least once per year or be locked.	**Location**
			    /etc/security/pscexpert/dodv2/lockacc_rlogin
			
			Compliance action
			    Ensures that the specified passwords are changed annually or locked.

GEN000750	2	This rule requires new passwords to contain a minimum of 4 characters that were not in the old password.	**Location**
			    /etc/security/pscexpert/dodv2/chusrattrdod
			
			Compliance action
			    Sets the minimum number of new characters that are required in a new password to 4.

GEN000760	2	Accounts must be locked after 35 days of inactivity.	**Location**
			    /etc/security/pscexpert/dodv2/disableacctdod
			
			Compliance action
			    Locks accounts after 35 days of inactivity.

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

GEN000790	2	The system must prevent the use of dictionary words for passwords.	**Location**
			    `/etc/security/pscexpert/dodv2/chuserstanzadod`
			Compliance action
			    Ensures that the default password that is being set is not weak.

GEN000800	2	This rule ensures that the last five passwords are not reused.	**Location**
			    `/etc/security/pscexpert/dodv2/chusrattrdod`
			Compliance action
			    Ensures that the new password is not the same as any of the last 5 passwords.

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.	**Location**
			    `/etc/security/pscexpert/dodv2/grpusrpass_chk`
			Compliance action
			    Ensures that all accounts meet the specified requirements.

GEN000900	3	The root user's home directory must not be the root directory (/).	**Location**
			    `/etc/security/pscexpert/dodv2/rootpasswd_home`
			Compliance action
			    Ensures that the system meets the specified requirement.
			Note: 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.

GEN000940	2	The root account's executable search path must be the vendor default, and must contain only absolute paths.	**Location**
			    `/etc/security/pscexpert/dodv2/fixpathvars`
			Compliance action
			    Ensures that the system meets the specified requirements.
			Note: 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.

GEN000945	2	The root account's library search path must be the system default, and must contain only absolute paths.	**Location**
			    `/etc/security/pscexpert/dodv2/fixpathvars`
			Compliance action
			    Ensures that the system meets the specified requirements.
			Note: 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.

GEN000950	2	The root account's list of preloaded libraries must be empty.	**Location**
			    `/etc/security/pscexpert/dodv2/fixpathvars`
			Compliance action
			    Ensures that the system meets the specified requirements.
			Note: 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.

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
GEN000960 (related to GEN003000, GEN003020, GEN003160, GEN003360, GEN003380)	2	The root account must not have world-writable directories in its executable search path.	**Location** /etc/security/pscexpert/dodv2/rmwwpaths **Compliance action** Ensures that the system meets the specified requirements. **Note:** 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.
GEN000980	2	The system must prevent the root account from directly logging in, except from the system console.	**Location** /etc/security/pscexpert/dodv2/chuserstanzadod **Compliance action** Ensures that the system meets the specified requirements.
GEN001000	2	Remote consoles must be disabled or protected from unauthorized access.	**Location** /etc/security/pscexpert/dodv2/remoteconsole **Compliance action** Ensures that the specified consoles are disabled.
GEN001020	2	The root account must not be used for direct login.	**Location** /etc/security/pscexpert/dodv2/sshDoDconfig **Compliance action** Disables the root account from logging in directly.
GEN001060	2	The system must log successful and unsuccessful attempts to access the root account.	**Location** /etc/security/pscexpert/dodv2/loginout **Compliance action** Ensures that the system meets the specified requirements.
GEN001100	1	Root passwords must never be passed over a network in text form.	**Location** /etc/security/pscexpert/dodv2/chuserstanzadod **Compliance action** Ensures that the system meets the specified requirements.
GEN001120	2	The system must not allow root login by using the SSH protocol.	**Location** /etc/security/pscexpert/dodv2/sshDoDconfig **Compliance action** Disables root login for SSH.
GEN001440	3	All interactive users must be assigned a home directory in the /etc/passwd file.	**Location** /etc/security/pscexpert/dodv2/grpusrpass_chk **Compliance action** Ensures that all interactive users have the specified directory.

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.	**Location**
			    /etc/security/pscexpert/dodv2/passwdhash
			
			Compliance action
			    Ensures that there are no group password hashes in the specified file.
			    Note: 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.

GEN001600	2	Run control scripts' executable search paths must contain only absolute paths.	**Location**
			    /etc/security/pscexpert/dodv2/fixpathvars
			
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.

GEN001605	2	Run control scripts' library search paths must contain only absolute paths.	**Location**
			    /etc/security/pscexpert/dodv2/fixpathvars
			
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.

GEN001610	2	Run control scripts' lists of preloaded libraries must contain only absolute paths.	**Location**
			    /etc/security/pscexpert/dodv2/fixpathvars
			
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.

GEN001840	2	All global initialization files' executable search paths must contain only absolute paths.	**Location**
			    /etc/security/pscexpert/dodv2/fixpathvars
			
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.

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

GEN001845	2	All global initialization files' library search paths must contain only absolute paths.	**Location**
			    /etc/security/pscexpert/dodv2/fixpathvars
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.

GEN001850	2	All global initialization files' lists of preloaded libraries must contain only absolute paths.	**Location**
			    /etc/security/pscexpert/dodv2/fixpathvars
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.

GEN001900	2	All local initialization files' executable search paths must contain only absolute paths.	**Location**
			    /etc/security/pscexpert/dodv2/fixpathvars
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.

GEN001901	2	All local initialization files' library search paths must contain only absolute paths.	**Location**
			    /etc/security/pscexpert/dodv2/fixpathvars
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.

GEN001902	2	All local initialization files' lists of preloaded libraries must contain only absolute paths.	**Location**
			    /etc/security/pscexpert/dodv2/fixpathvars
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.

GEN001940	2	User initialization files must not run world-writable programs.	**Location**
			    /etc/security/pscexpert/dodv2/rmwwpaths
			Compliance action
			    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

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.	**Location**
			    `/etc/security/pscexpert/dodv2/dodv2netrules`
			
			Compliance action
			    Ensures that the specified files meet the specified requirements.

GEN002000	2	There must be no `.netrc` files on the system.	**Location**
			    `/etc/security/pscexpert/dodv2/dodv2netrules`
			
			Compliance action
			    Ensures that there are none of specified files on the system.
			    Note: 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.

GEN002020	2	All `.rhosts`, `.shosts`, or `hosts.equiv` files must contain only trusted host-user pairs.	**Location**
			    `/etc/security/pscexpert/dodv2/dodv2netrules`
			
			Compliance action
			    Ensures that the specified files conform to this requirement.

GEN002040	1	This rule disables `.rhosts`, `.shosts`, and `hosts.equiv` files or `shosts.equiv` files.	**Location**
			    `/etc/security/pscexpert/dodv2/mvhostsfilesdod`
			
			Compliance action
			    Disables the specified files.

GEN002120	1,2	This rule checks and configures user shells.	**Location**
			    `/etc/security/pscexpert/dodv2/usershells`
			
			Compliance action
			    Creates the required shells.
			    Note: 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.

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.	**Location**
			    `/etc/security/pscexpert/dodv2/usershells`
			
			Compliance action
			    Ensures that the shells are listed in the correct files.
			    Note: 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.

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.	**Location**
			    `/etc/security/pscexpert/dodv2/wwdevfiles`
			
			Compliance action
			    Displays world-writable device files, directories, and any other files on the system that are in non-public directories.

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

GEN002300	2	Device files that are used for backup must be readable, writable, or both, only by the root user or the backup user.	**Location**
			    `/etc/security/pscexpert/dodv2/wwdevfiles`
			
			Compliance action
			    Displays world-writable device files, directories, and any other files on the system that are in non-public directories.

GEN002400	2	The system must be checked weekly for unauthorized `setuid` files, and unauthorized modification to authorized `setuid` files.	**Location**
			    `/etc/security/pscexpert/dodv2/trust`
			
			Compliance action
			    Checks weekly to identify changes to the specified files.
			    Note: Compare the two newest weekly logs that are created in the `/var/security/pscexpert` directory to verify that there was no unauthorized activity.

GEN002420	2	Removable media, remote file systems, and any file system that does not contain approved `setuid` files must be mounted by using the *nosuid* option.	**Location**
			    `/etc/security/pscexpert/dodv2/fsmntoptions`
			
			Compliance action
			    Ensures that the remotely mounted file systems have the specified options.
			    Note: 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.

GEN002430	2	Removable media, remote file systems, and any file system that does not contain approved device files must be mounted by using the *nodev* option.	**Location**
			    `/etc/security/pscexpert/dodv2/fsmntoptions`
			
			Compliance action
			    Ensures that the remotely mounted file systems have the specified options.
			    Note: 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.

GEN002480	2	Public directories must be the only world-writable directories, and world-writable files must be located only in public directories.	**Location**
			    `/etc/security/pscexpert/dodv2/wwdevfiles`
			
			    `/etc/security/pscexpert/dodv2/fpmdodfiles`
			
			Compliance action
			    Reports when world-writable files are not in public directories.

GEN002640	2	Default system accounts must be disabled or removed.	**Location**
			    `/etc/security/pscexpert/dodv2/lockacc_rlogin`
			
			    `/etc/security/pscexpert/dodv2/loginout`
			
			Compliance action
			    Disables default system accounts.

GEN002660	2	Auditing must be enabled.	**Location**
			    `/etc/security/pscexpert/dodv2/dodaudit`
			
			Compliance action
			    Enables the `dodaudit` command, which enables auditing.

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

GEN002720	2	The audit system must be configured to audit failed attempts to access files and programs.	**Location**
			    /etc/security/pscexpert/dodv2/dodaudit
			Compliance action
			    Automatically enables the specified auditing.

GEN002740	2	The audit system must be configured to audit file deletions.	**Location**
			    /etc/security/pscexpert/dodv2/dodaudit
			Compliance action
			    Automatically enables the specified auditing.

GEN002750	3	The audit system must be configured to audit account creation.	**Location**
			    /etc/security/pscexpert/dodv2/dodaudit
			Compliance action
			    Automatically enables the specified auditing.

GEN002751	3	The audit system must be configured to audit account modification.	**Location**
			    /etc/security/pscexpert/dodv2/dodaudit
			Compliance action
			    Automatically enables the specified auditing.

GEN002752	3	The audit system must be configured to audit accounts that are disabled.	**Location**
			    /etc/security/pscexpert/dodv2/dodaudit
			Compliance action
			    Automatically enables the specified auditing.

GEN002753	3	The audit system must be configured to audit account termination.	**Location**
			    /etc/security/pscexpert/dodv2/dodaudit
			Compliance action
			    Automatically enables the specified auditing.

GEN002760	2	The audit system must be configured to audit all administrative, privileged, and security actions.	**Location**
			    /etc/security/pscexpert/dodv2/dodaudit
			Compliance action
			    Automatically enables the specified auditing.

GEN002800	2	The audit system must be configured to audit login, logout, and session initiation.	**Location**
			    /etc/security/pscexpert/dodv2/dodaudit
			Compliance action
			    Automatically enables the specified auditing.

GEN002820	2	The audit system must be configured to audit all discretionary access control permission modifications.	**Location**
			    /etc/security/pscexpert/dodv2/dodaudit
			Compliance action
			    Automatically enables the specified auditing.

GEN002825	2	The audit system must be configured to audit the loading and unloading of dynamic kernel modules.	**Location**
			    /etc/security/pscexpert/dodv2/dodaudit
			Compliance action
			    Automatically enables the specified auditing.

GEN002860	2	Audit logs must be rotated daily.	**Location**
			    /etc/security/pscexpert/dodv2/rotateauditdod
			Compliance action
			    Ensures that audit logs are rotated.

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
GEN002960	2	Access to the `cron` utility must be controlled by using the `cron.allow` file or `cron.deny` file, or both.	**Location** /etc/security/pscexpert/dodv2/limitsysacc **Compliance action** Ensures that the compliant limits are enabled.
GEN003000 (related to GEN000960, GEN003020, GEN003160, GEN003360, GEN003380)	2	Cron must not run group-writable or world-writable programs.	**Location** /etc/security/pscexpert/dodv2/rmwwpaths **Compliance action** Ensures that the compliant limits are enabled. **Note:** 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.	**Location** /etc/security/pscexpert/dodv2/rmwwpaths **Compliance action** Removes the world-writable permission from the `cron` program directories. **Note:** 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.	**Location** `cron.allow` or `cron.deny` **Compliance action** Ensures that the system meets the specified requirements.
GEN003160 (related to GEN000960, GEN003000, GEN003020, GEN003360, GEN003380)	2	Cron logging must be running.	**Location** /etc/security/pscexpert/dodv2/rmwwpaths **Compliance action** 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.	**Location** /etc/security/pscexpert/dodv2/chcronfilesdod **Compliance action** Ensures that the system meets the specified requirements.
GEN003300	2	The `at.deny` file must not be empty, if it exists.	**Location** /etc/security/pscexpert/dodv2/chcronfilesdod **Compliance action** 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 `at.allow` file, or must be included in the `at.deny` file if the `at.allow` file does not exist.	**Location**
			    /etc/security/pscexpert/dodv2/chcronfilesdod
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN003360 (related to GEN000960, GEN003000, GEN003020, GEN003160, GEN003380)	2	The at daemon must not run group-writable or world-writable programs.	**Location**
			    /etc/security/pscexpert/dodv2/rmwwpaths
			
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.

GEN003380 (related to GEN000960, GEN003000, GEN003020, GEN003160, GEN003360)	2	The at daemon must not run programs in, or subordinate to, world-writable directories.	**Location**
			    /etc/security/pscexpert/dodv2/rmwwpaths
			
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.

GEN003510	2	Kernel core dumps must be disabled unless they are needed.	**Location**
			    /etc/security/pscexpert/dodv2/coredumpdev
			
			Compliance action
			    Disables kernel core dumps.

GEN003540	2	The system must use non-executable program stacks.	**Location**
			    /etc/security/pscexpert/dodv2/sedconfigdod
			
			Compliance action
			    Enforces the use of non-executable program stacks.

GEN003600	2	The system must not forward IPv4 source-routed packets.	**Location**
			    /etc/security/pscexpert/dodv2/ntwkoptsdod
			
			Compliance action
			    Sets the value of the `ipsrcforward` network option to *0.*

GEN003601	2	TCP backlog queue sizes must be set appropriately.	**Location**
			    /etc/security/pscexpert/dodv2/ntwkoptsdod
			
			Compliance action
			    Sets the value of the `clean_partial_ conns` network option to *1.*

GEN003603	2	The system must not respond to Internet Control Message Protocol version 4 (ICMPv4) echoes that are sent to a broadcast address.	**Location**
			    /etc/security/pscexpert/dodv2/ntwkoptsdod
			
			Compliance action
			    Sets the value of the `bcastping` network option to *0.*

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
GEN003604	2	The system must not respond to ICMP time stamp requests that are sent to a broadcast address.	**Location** 　　　　/etc/security/pscexpert/dodv2/ntwkoptsdod **Compliance action** 　　　　Sets the value of the bcastping network option to *0*.
GEN003605	2	The system must not apply reversed source routing to TCP responses.	**Location** 　　　　/etc/security/pscexpert/dodv2/ntwkoptsdod **Compliance action** 　　　　Sets the value of the nonlocsrcroute network option to *0*.
GEN003606	2	The system must prevent local applications from generating source-routed packets.	**Location** 　　　　/etc/security/pscexpert/dodv2/ntwkoptsdod **Compliance action** 　　　　Sets the value of the ipsrcroutesend network option to *0*.
GEN003607	2	The system must not accept source-routed IPv4 packets.	**Location** 　　　　/etc/security/pscexpert/dodv2/ntwkoptsdod **Compliance action** 　　　　Disables the ability to accept source-routes IPv4 packets.
GEN003609	2	The system must ignore IPv4 ICMP redirect messages.	**Location** 　　　　/etc/security/pscexpert/dodv2/ntwkoptsdod **Compliance action** 　　　　Sets the value of the ipignoreredirects network option to *1*.
GEN003610	2	The system must not send IPv4 ICMP redirect messages.	**Location** 　　　　/etc/security/pscexpert/dodv2/ntwkoptsdod **Compliance action** 　　　　Sets the value of the ipsendredirects network option to *0*.
GEN003612	2	The system must be configured to use TCP syncookies when a TCP SYN flood occurs.	**Location** 　　　　/etc/security/pscexpert/dodv2/ntwkoptsdod **Compliance action** 　　　　Sets the value of the clean_partial _conns network option to *1*.
GEN003640	2	The root file system must use journaling, or another method of ensuring file system consistency.	**Location** 　　　　/etc/security/pscexpert/dodv2/chkjournal **Compliance action** 　　　　Enables journaling on the root file system.
GEN003660	2	The system must log authentication informational data.	**Location** 　　　　/etc/security/pscexpert/dodv2/chsyslogdod **Compliance action** 　　　　Enables the logging of auth and info data.

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

GEN003700	2	The `inetd` and `xinetd` must be disabled or removed if no network services are using them.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2services
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN003810	2	This `portmap` or `rpcbindservices` must not be running unless they are needed.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2services
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN003815	2	The `portmap` or `rpcbindservices` must not be installed unless they are being used.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2services
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN003820-3860	1,2,3	The `rsh`, `rexec`, and `telnet` daemons, and the `rlogind` service must not be running.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			Compliance action
			    Disables the required daemons and services by commenting out entries in the `/etc/inetd.conf` file.

GEN003865	2	Network analysis tools must not be installed.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2services
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN003900	2	The `hosts.lpd` file (or equivalent) must not contain an addition sign (+).	**Location**
			    /etc/security/pscexpert/dodv2/printers
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN004220	1	Administrative accounts must not run a web browser, except as needed for local service administration.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2cat1
			Compliance action
			    Displays the results of the specified rule tests.

GEN004460	2	This rule logs `auth` and `info` data.	**Location**
			    /etc/security/pscexpert/dodv2/chsyslogdod
			Compliance action
			    Enables the logging of `auth` and `info` data.

GEN004540	2	This rule disables the `sendmail` help command.	**Location**
			    /etc/security/pscexpert/dodv2/sendmailhelp
			    /etc/security/pscexpert/dodv2/dodv2cmntrows
			Compliance action
			    Disables the specified command.

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.	**Location**
			  /etc/security/pscexpert/dodv2/forward
			
			Compliance action
			  Disables the specified files.
			  Note: 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.

GEN004600	1	The SMTP service must be the most current version.	**Location**
			  /etc/security/pscexpert/dodv2/SMTP_ver
			
			Compliance action
			  Ensures that the latest version of the specified service is running.
			  Note: 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.

GEN004620	2	The sendmail server must have the debugging feature disabled.	**Location**
			  /etc/security/pscexpert/dodv2/SMTP_ver
			
			Compliance action
			  Disables the sendmail debugging feature.

GEN004640	1	The SMTP service must not have an active uudecode alias.	**Location**
			  /etc/security/pscexpert/dodv2/SMTPuucode
			
			Compliance action
			  Disables the uudecode alias.

GEN004710	2	Mail relaying must be restricted.	**Location**
			  /etc/security/pscexpert/dodv2/sendmaildod
			
			Compliance action
			  Restricts mail relay.

GEN004800	1,2,3	Unencrypted FTP must not be used on the system.	**Location**
			  /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			  Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN004820	2	Anonymous FTP must not be active on the system unless it is authorized.	**Location**
			  /etc/security/pscexpert/dodv2/anonuser
			
			Compliance action
			  Disables anonymous FTP on the system.
			  Note: 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.

GEN004840	2	If the system is an anonymous FTP server, it must be isolated to the Demilitarized Zone (DMZ) network.	**Location**
			  /etc/security/pscexpert/dodv2/anonuser
			
			Compliance action
			  Ensures that an anonymous FTP on the system is on the DMZ network.

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

GEN004880	2	The `ftpusers` file must exist.	**Location**
			      /etc/security/pscexpert/dodv2/chdodftpusers
			
			Compliance action
			      Ensures that the specified file is on the system.

GEN004900	2	The `ftpusers` file must contain the account names that are not allowed to use the FTP protocol.	**Location**
			      /etc/security/pscexpert/dodv2/chdodftpusers
			
			Compliance action
			      Ensures that the file contains the required account names.

GEN005000	1	Anonymous FTP accounts must not have a functional shell.	**Location**
			      /etc/security/pscexpert/dodv2/usershells
			
			Compliance action
			      Removes shells from anonymous FTP accounts.
			      Note: 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.

GEN005080	1	The `TFTP` daemon must operate in secure-mode, which provides access only to a single directory on the host file system.	**Location**
			      /etc/security/pscexpert/dodv2/tftpdod
			
			Compliance action
			      Ensures that the daemon meets the specified requirements.

GEN005120	2	The TFTP daemon must be configured to vendor specifications, including a dedicated TFTP user account, a non-login shell, such as `/bin/false`, and a home directory that is owned by the TFTP user.	**Location**
			      /etc/security/pscexpert/dodv2/tftpdod
			
			Compliance action
			      Ensures that the system meets the specified requirements.

GEN005140	1,2,3	Any active TFTP daemon must be authorized and approved in the system accreditation package.	**Location**
			      /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			      Ensures that the daemon is authorized.

GEN005160	1,2	Any X Window System host must write `.Xauthority` files.	**Location**
			      /etc/security/pscexpert/dodv2/dodv2disableX
			
			Compliance action
			      Ensures that the host wrote the specified files.

GEN005200	1,2	Any X Window System displays cannot be exported publicly.	**Location**
			      /etc/security/pscexpert/dodv2/dodv2disableX
			
			Compliance action
			      Disables the dissemination of the specified programs.

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

GEN005220	1,2	The .Xauthority or X*.hosts (or equivalent) files must be used to restrict access to the X Window System server.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2disableX
			Compliance action
			    Ensures that the specified files are available to restrict access to the server.

GEN005240	1,2	The .Xauthority utility must allow access only to authorized hosts.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2disableX
			Compliance action
			    Ensures that the access is limited to authorized hosts.

GEN005260	2	This rule disables X Window System connections and XServer login manager.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2cmntrows
			Compliance action
			    Disables the required connections and login manager.

GEN005280	1,2,3	The system must not have the UUCP service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN005300	2	SNMP communities must be changed from the default settings.	**Location**
			    /etc/security/pscexpert/dodv2/chsnmp
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005305	2	SNMP service must use only SNMPv3 or a later version.	**Location**
			    /etc/security/pscexpert/dodv2/chsnmp
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005306	2	SNMP service must require the use of a FIPS 140-2.	**Location**
			    /etc/security/pscexpert/dodv2/chsnmp
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005440	2	The system must use a remote syslog server (log host).	**Location**
			    /etc/security/pscexpert/dodv2/
			    EnableTrustedLogging
			Compliance action
			    Ensures that the system is using a remote syslog server.

GEN005450	2	The system must use a remote syslog server (log host).	**Location**
			    /etc/security/pscexpert/dodv2/
			    EnableTrustedLogging
			Compliance action
			    Ensures that the system is using a remote syslog server.

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

GEN005460	2	The system must use a remote syslog server (log host).	**Location**
			    `/etc/security/pscexpert/dodv2/`
			    `EnableTrustedLogging`
			
			Compliance action
			    Ensures that the system is using a remote syslog server.

GEN005480	2	The system must use a remote syslog server (log host).	**Location**
			    `/etc/security/pscexpert/dodv2/`
			    `EnableTrustedLogging`
			
			Compliance action
			    Ensures that the system is using a remote syslog server.

GEN005500	2	The SSH daemon must be configured to use only the Secure Shell version 2 (SSHv2) protocol.	**Location**
			    `/etc/security/pscexpert/dodv2/sshDoDconfig`
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005501	2	The SSH client must be configured to use only the SSHv2 protocol.	**Location**
			    `/etc/security/pscexpert/dodv2/sshDoDconfig`
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005504	2	The SSH daemon must only listen on management network addresses, unless it is authorized for uses other than management.	**Location**
			    `/etc/security/pscexpert/dodv2/sshDoDconfig`
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005505	2	The SSH daemon must be configured to use only ciphers that conform to Federal Information Processing Standards (FIPS) 140-2 standards.	**Location**
			    `/etc/security/pscexpert/dodv2/sshDoDconfig`
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005506	2	The SSH daemon must be configured to use only ciphers that conform to FIPS 140-2 standards.	**Location**
			    `/etc/security/pscexpert/dodv2/sshDoDconfig`
			
			Compliance action
			    Ensures that the system meets the specified requirements.

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.	**Location**
			    `/etc/security/pscexpert/dodv2/sshDoDconfig`
			
			Compliance action
			    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

GEN005510	2	The SSH client must be configured to use only MACs with ciphers that conform to FIPS 140-2 standards.	**Location**
			    /etc/security/pscexpert/dodv2/sshDoDconfig
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005511	2	The SSH client must be configured to use only MACs with ciphers that conform to FIPS 140-2 standards.	**Location**
			    /etc/security/pscexpert/dodv2/sshDoDconfig
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005512	2	The SSH daemon must be configured to use only MACs with cryptographic hash algorithms that conform to FIPS 140-2 standards.	**Location**
			    /etc/security/pscexpert/dodv2/sshDoDconfig
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005521	2	The SSH daemon must restrict login to specific users, groups, or both.	**Location**
			    /etc/security/pscexpert/dodv2/sshDoDconfig
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005536	2	The SSH daemon must perform strict mode checking of the home directory configuration files.	**Location**
			    /etc/security/pscexpert/dodv2/sshDoDconfig
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005537	2	The SSH daemon must use privilege separation.	**Location**
			    /etc/security/pscexpert/dodv2/sshDoDconfig
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005538	2	The SSH daemon must not allow rhosts to authenticate by using the Rivest-Shamir-Adleman (RSA) cryptosystem.	**Location**
			    /etc/security/pscexpert/dodv2/sshDoDconfig
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005539	2	The SSH daemon must not allow compression or must allow compression only after a successful authentication.	**Location**
			    /etc/security/pscexpert/dodv2/sshDoDconfig
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005550	2	The SSH daemon must be configured with the DoD logon banner.	**Location**
			    /etc/security/pscexpert/dodv2/sshDoDconfig
			
			Compliance action
			    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

GEN005560	2	Determine whether there is a default gateway that is configured for IPv4.	**Location**
			    `/etc/security/pscexpert/dodv2/chkgtway`
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.
			    Note: If your system is running the IPv6 protocol, ensure that the *ipv6_enabled* setting in the `/etc/security/pscexpert/ipv6.conf` file is set to the value of yes. If system is not using IPv6, then ensure that the *ipv6_enabled* value is set to no.

GEN005570	2	Determine whether there is a default gateway that is configured for IPv6.	**Location**
			    `/etc/security/pscexpert/dodv2/chkgtway`
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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.
			    Note: If your system is running the IPv6 protocol, ensure that the *ipv6_enabled* setting in the `/etc/security/pscexpert/ipv6.conf` file is set to the value of yes. If system is not using IPv6, then ensure that the *ipv6_enabled* value is set to no.

GEN005590	2	The system must not be running any routing protocol daemons, unless the system is a router.	**Location**
			    `/etc/security/pscexpert/dodv2/dodv2cmntrows`
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005590	2	The system must not be running any routing protocol daemons, unless the system is a router.	**Location**
			    `/etc/security/pscexpert/dodv2/dodv2cmntrows`
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN005600	2	IP forwarding for IPv4 must not be enabled unless the system is a router.	**Location**
			    `/etc/security/pscexpert/dodv/ntwkoptsdod`
			Compliance action
			    Sets the value of the `ipforwarding` network option to *0*.

GEN005610	2	The system must not have IP forwarding for IPv6 enabled unless the system is an IPv6 router.	**Location**
			    `/etc/security/pscexpert/dodv/ntwkoptsdod`
			Compliance action
			    Sets the value of the `ip6forwarding` network option to *1*.

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

GEN005820	2	The NFS anonymous UID and GID must be configured to values without permissions.	**Location**
			    /etc/security/pscexpert/dodv2/nfsoptions
			Compliance action
			    Ensures that the specified IDs do not have permissions.

GEN005840	2	The NFS server must be configured to restrict file system access to local hosts.	**Location**
			    /etc/security/pscexpert/dodv2/nfsoptions
			Compliance action
			    Configures NFS server to restrict access to local hosts.

GEN005880	2	The NFS server must not allow remote root access.	**Location**
			    /etc/security/pscexpert/dodv2/nfsoptions
			Compliance action
			    Disables remote root access on the NFS server.

GEN005900	2	The *nosuid* option must be enabled on all NFS client mounts.	**Location**
			    /etc/security/pscexpert/dodv2/nosuid
			Compliance action
			    Enables the *nosuid* option on all NFS client mounts.

GEN006060	2	The system must not run Samba unless it is needed.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2services
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN006380	1	The system must not use UDP for NIS or NIS+.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2cat1
			Compliance action
			    Displays the results of the specified rule tests.

GEN006400	2	The Network Information System (NIS) protocol must not be used.	**Location**
			    /etc/security/pscexpert/dodv2/nisplus
			Compliance action
			    Disables the specified protocol.
			    Note: 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.

GEN006420	2	NIS maps must be protected by using hard-to-guess domain names.	**Location**
			    /etc/security/pscexpert/dodv2/nisplus
			Compliance action
			    Ensures that domain names are not easy to determine.

GEN006460	2	Any NIS+ server must be operating at security level 2.	**Location**
			    /etc/security/pscexpert/dodv2/nisplus
			Compliance action
			    Ensures that the server is at the specified minimum security level.
			    Note: 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.

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

GEN006480	2	The system must be checked weekly for unauthorized `setuid` files, and unauthorized modification to authorized `setuid` files.	**Location**
			    `/etc/security/pscexpert/dodv2/trust`
			
			Compliance action
			    Checks weekly to identify changes to the specified files.

GEN006560	2	The system must be checked weekly for unauthorized `setuid` files, and unauthorized modification to authorized `setuid` files.	**Location**
			    `/etc/security/pscexpert/dodv2/trust`
			
			Compliance action
			    Checks weekly to identify changes to the specified files.

GEN006580	2	The system must use an access control program.	**Location**
			    `/etc/security/pscexpert/dodv2/checktcpd`
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN006600	2	The system's access control program must log each system access attempt.	**Location**
			    `/etc/security/pscexpert/dodv2/chsyslogdod`
			
			Compliance action
			    Ensures that access attempts are logged.

GEN006620	2	The system's access control program must be configured to grant or deny system access to specific hosts.	**Location**
			    `/etc/security/pscexpert/dodv2/chetchostsdod`
			
			Compliance action
			    Configures the `hosts.deny` and `hosts.allow` files to the required settings.

GEN007020	2	The Stream Control Transmission Protocol (SCTP) must be disabled.	**Location**
			    `/etc/security/pscexpert/dodv2/dodv2netrules`
			
			Compliance action
			    Disables the specified protocol.

GEN007700	2	The IPv6 protocol handler must not be bound to the network stack unless it is needed.	**Location**
			    `/etc/security/pscexpert/dodv2/rminet6`
			
			Compliance action
			    Disables the IPv6 protocol handler from the network stack, unless the handler is specified in the `/etc/ipv6.conf` file.
			    Note: If your system is running the IPv6 protocol, ensure that the *ipv6_enabled* setting in the `/etc/security/pscexpert/ipv6.conf` file is set to the value of `yes`. If system is not using IPv6, then ensure that the *ipv6_enabled* value is set to `no`.

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.	**Location** /etc/security/pscexpert/dodv2/rmiface **Compliance action** Disables the specified tunnels. **Note:** 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.
GEN007820	2	The system must not have IP tunnels configured.	**Location** /etc/security/pscexpert/dodv2/rmtunnel **Compliance action** Disables IP tunnels. **Note:** 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.
GEN007840	2	The DHCP client must be disabled if it is not used.	**Location** /etc/security/pscexpert/dodv2/dodv2services **Compliance action** Ensures that the system meets the specified requirements.
GEN007850	2	The DHCP client must not send dynamic DNS updates.	**Location** /etc/security/pscexpert/dodv2/dodv2services **Compliance action** Ensures that the system meets the specified requirements.
GEN007860	2	The system must ignore IPv6 ICMP redirect messages.	**Location** /etc/security/pscexpert/dodv2/ntwkoptsdod **Compliance action** Sets the value of the ipignoreredirects network option to *1*.
GEN007880	2	The system must not send IPv6 ICMP redirects.	**Location** /etc/security/pscexpert/dodv2/ntwkoptsdod **Compliance action** Sets the value of the ipsendredirects network option to *0*.
GEN007900	2	The system must use an appropriate reverse-path filter for IPv6 network traffic, if the system uses IPv6.	**Location** /etc/security/pscexpert/dodv2/chuserstanzadod **Compliance action** Ensures that the system meets the specified requirements.
GEN007920	2	The system must not forward IPv6 source-routed packets.	**Location** /etc/security/pscexpert/dodv2/ntwkoptsdod **Compliance action** Sets the value of the ip6srcrouteforward network option to *0*.

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

GEN007940: GEN003607	2	The system must not accept source-routed IPv4 or IPv6 packets.	**Location**
			    /etc/security/pscexpert/dodv2/ntwkoptsdod
			
			Compliance action
			    Sets the value of the `ipsrcrouterecv` network option to *0*.

GEN007950	2	The system must not respond to ICMPv6 echo requests that are sent to a broadcast address.	**Location**
			    /etc/security/pscexpert/dodv2/ntwkoptsdod
			
			Compliance action
			    Sets the value of the `bcastping` network option to *0*.

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.	**Location**
			    /etc/security/pscexpert/dodv2/ldap_config
			
			Compliance action
			    Ensures that the system meets the specified requirements.

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.	**Location**
			    /etc/security/pscexpert/dodv2/ldap_config
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN008050	2	If the system is using LDAP for authentication or account information, the /etc/ldap.conf file (or equivalent) must not contain passwords.	**Location**
			    /etc/security/pscexpert/dodv2/ldap_config
			
			Compliance action
			    Ensures that the system meets the specified requirements.

GEN008380	2	The system must be checked weekly for unauthorized `setuid` files, and unauthorized modification to authorized `setuid` files.	**Location**
			    /etc/security/pscexpert/dodv2/trust
			
			Compliance action
			    Checks weekly to identify changes to the specified files.

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.	**Location**
			    /etc/security/pscexpert/dodv2/ipsecshunports
			
			Compliance action
			    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

GEN008540	2	The system's local firewall must implement a *deny-all, allow-by-exception* policy.	**Location**
			    `/etc/security/pscexpert/dodv2/ipsecshunhosthls`
			Compliance action
			    Ensures that the system meets the specified requirements.
			    Note: 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:
			    port_number`:`*ip_address*`:`
			    `action`
			
			    where the possible values for *action* are `Allow` or `Deny`.

GEN008600	1	The system must be configured to start only from the system boot configuration.	**Location**
			    `/etc/security/pscexpert/dodv2/dodv2cat1`
			Compliance action
			    Ensures that the starting the system only uses the system boot configuration.

GEN008640	1	The system must not use removable media as the boot loader.	**Location**
			    `/etc/security/pscexpert/dodv2/dodv2cat1`
			Compliance action
			    Ensures that the system does not boot from a removable drive.

GEN009140	1,2,3	The system must not have the `chargen` service active.	**Location**
			    `/etc/security/pscexpert/dodv2/inetdservices`
			Compliance action
			    Disables the required daemons and services by commenting out entries in the `/etc/inetd.conf` file.

GEN009160	1,2,3	The system must not have the `Calendar Management Service Daemon` (CMSD) service active.	**Location**
			    `/etc/security/pscexpert/dodv2/inetdservices`
			Compliance action
			    Disables the required daemons and services by commenting out entries in the `/etc/inetd.conf` file.

GEN009180	1,2,3	The system must not have the `tool-talk database server` (ttdbserver) service active.	**Location**
			    `/etc/security/pscexpert/dodv2/inetdservices`
			Compliance action
			    Disables the required daemons and services by commenting out entries in the `/etc/inetd.conf` file.

GEN009190	1,2,3	The system must not have the `comsat` service active.	**Location**
			    `/etc/security/pscexpert/dodv2/inetdservices`
			Compliance action
			    Disables the required daemons and services by commenting out entries in the `/etc/inetd.conf` file.

GEN009200-9330	1,2,3	The system cannot have other services and daemons active.	**Location**
			    `/etc/security/pscexpert/dodv2/inetdservices`
			Compliance action
			    Disables the required daemons and services by commenting out entries in the `/etc/inetd.conf` file.

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

GEN009210	2	The system must not have the discard service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009220	2	The system must not have the dtspc service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009230	2	The system must not have the echo service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009240	2	The system must not have Internet Message Access Protocol (IMAP) service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009250	2	The system must not have the PostOffice Protocol (POP3) service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009260	2	The system must not have the talk or ntalk services active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009270	2	The system must not have the netstat service active on the InetD process.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009280	2	The system must not have the PCNFS service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009290	2	The system must not have the systat service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

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

GEN009300	2	The `inetd time` service must not be active on the system on the `inetd` daemon.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009310	2	The system must not have the `rusersd` service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009320	2	The system must not have the `sprayd` service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009330	2	The system must not have the `rstatd` service active.	**Location**
			    /etc/security/pscexpert/dodv2/inetdservices
			
			Compliance action
			    Disables the required daemons and services by commenting out entries in the /etc/inetd.conf file.

GEN009340	2	X server login managers must not be running unless they are needed for X11 session management.	**Location**
			    /etc/security/pscexpert/dodv2/dodv2cmntrows
			
			Compliance action
			    This rule disables X Window System connections and XServer login manager.

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/netsvc.conf file must be owned by root.	**Location**
		    /etc/security/pscexpert/dodv2/
		    chowndodfiles
		
		Compliance action
		    Ensures that the specified file is owned by root.

AIX00090	The /etc/netsvc.conf file must be group-owned by bin, sys, or system.	**Location**
		    /etc/security/pscexpert/dodv2/
		    chowndodfiles
		
		Compliance action
		    Ensures that the specified file is group-owned by bin, sys, or system.

AIX00320	The /etc/ftpaccess.ctl file must be owned by root.	**Location**
		    /etc/security/pscexpert/dodv2/
		    chowndodfiles
		
		Compliance action
		    Ensures that the specified file is owned by root.

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
AIX00330	The /etc/ftpaccess.ctl file must be group-owned by bin, sys, or system.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is group-owned by bin, sys, or system.
GEN000250	The time synchronization configuration file (such as /etc/ntp.conf) must be owned by root.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is owned by root.
GEN000251	The time synchronization configuration file (such as /etc/ntp.conf) must be group-owned by bin, sys, or system.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is group-owned by bin, sys, or system.
GEN001160	All files and directories must have a valid owner.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that all files and directories have a valid owner.
GEN001170	All files and directories must have a valid group owner.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that all files and directories have a valid owner.
GEN001220	All system files, programs, and directories must be owned by a system account.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the system files, programs, and directories are owned by a system account.
GEN001240	System files, programs, and directories must be group-owned by a system group.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** All system files, programs, and directories are group-owned by a system group.
GEN001320	Network Information Systems (NIS)/NIS+/yp files must be owned by root, sys, or bin.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified files are owned by root, sys, or bin.

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

GEN001340	NIS/NIS+/yp files must be group-owned by sys, bin, other, or system.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`chowndodfiles`
		
		Compliance action
		Ensures that the specified files are owned by sys, bin, other, or system.

GEN001362	The `/etc/resolv.conf` file must be owned by root.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`chowndodfiles`
		
		Compliance action
		Ensures that the specified file is owned by root.

GEN001363	The `/etc/resolv.conf` file must be group-owned by bin, sys, or system.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`chowndodfiles`
		
		Compliance action
		Ensures that the specified file is group-owned by bin, sys, or system.

GEN001366	The `/etc/hosts` file must be owned by root.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`chowndodfiles`
		
		Compliance action
		Ensures that the specified file is owned by root.

GEN001367	The `/etc/hosts` file must be group-owned by bin, sys, or system.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`chowndodfiles`
		
		Compliance action
		Ensures that the specified file is group-owned by bin, sys, or system.

GEN001371	The `/etc/nsswitch.conf` file must be owned by root.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`chowndodfiles`
		
		Compliance action
		Ensures that the specified file is owned by root.

GEN001372	The `/etc/nsswitch.conf` file must be group-owned by root, bin, sys, or system.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`chowndodfiles`
		
		Compliance action
		Ensures that the specified file is group-owned by root, bin, sys, or system.

GEN001378	The `/etc/passwd` file must be owned by root.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`chowndodfiles`
		
		Compliance action
		Ensures that the specified file is owned by root.

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
GEN001379	The /etc/passwd file must be group-owned by bin, security, sys, or system.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is group-owned by bin, security, sys, or system.
GEN001391	The /etc/group file must be owned by root	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is owned by root.
GEN001392	The /etc/group file must be group-owned by bin, security, sys, or system.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is group-owned by bin, security, sys, or system.
GEN001400	The /etc/security/passwd file must be owned by root.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is owned by root.
GEN001410	The /etc/security/passwd file must be group-owned by bin, security, sys, or system.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is group-owned by bin, security, sys, or system.
GEN001500	All interactive users' home directories must be owned by their respective users.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that all of the interactive users' home directories must be owned by their respective users.
GEN001520	All interactive users' home directories must be group-owned by the home directory owner's primary group.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that all interactive users' home directories are group-owned by the home directory owner's primary group.

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
GEN001540	All files and directories that are contained in the interactive user's home directories must be owned by the home directory's owner.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that all files and directories that are contained in the interactive user's home directories are owned by the home directory's owner.
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.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** 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.
GEN001660	All system start files must be owned by root.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified files are owned by root.
GEN001680	All system start files must be group-owned by sys, bin, other, or system.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified files are group-owned by sys, bin, other, or system.
GEN001740	All global initialization files must be owned by root.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified files are owned by root.
GEN001760	All global initialization files must be group-owned by sys, bin, system, or security.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified files are group-owned by sys, bin, system, or security.
GEN001820	All skeleton files and directories (typically in /etc/skel) must be owned by root or bin.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified files and directories are owned by root or bin.

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
GEN001830	All skeleton files (typically in `/etc/skel`) must be group-owned by security.	**Location** `/etc/security/pscexpert/dodv2/chowndodfiles` **Compliance action** Ensures that the specified files are group-owned by security.
GEN001860	All local initialization files must be owned by the user or root.	**Location** `/etc/security/pscexpert/dodv2/chowndodfiles` **Compliance action** Ensures that the specified files are owned by the user or root.
GEN001870	Local initialization files must be group-owned by the user's primary group or root.	**Location** `/etc/security/pscexpert/dodv2/chowndodfiles` **Compliance action** Ensures that the local initialization files must be group-owned by the user's primary group or root.

GEN002060	All `.rhosts`, `.shosts`, `.netrc`, or `hosts.equiv` files must be accessible by only root or the owner.	**Location**
		`/etc/security/pscexpert/dodv2/chowndodfiles`
		
		`/etc/security/pscexpert/dodv2/fpmdodfiles`
		
		Compliance action
		Ensures that only the root or the owner can access the specified files.

GEN002100	The `.rhosts` file must not be supported by the Pluggable Authentication Module (PAM).	**Location** `/etc/security/pscexpert/dodv2/chowndodfiles` **Compliance action** Ensures that the specified file is not available by using PAM.
GEN002200	All shell files must be owned by root or bin.	**Location** `/etc/security/pscexpert/dodv2/chowndodfiles` **Compliance action** Ensures that the specified files are owned by root or bin.
GEN002210	All shell files must be group-owned by root, bin, sys, or system.	**Location** `/etc/security/pscexpert/dodv2/chowndodfiles` **Compliance action** Ensures that the specified files are group-owned by root, bin, sys, or system.

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

GEN002340	Audio devices must be owned by root.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that all audio devices are owned by root.

GEN002360	Audio devices must be group-owned by root, sys, bin, or system.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that all audio devices are group-owned by root, sys, bin, or system.

GEN002520	All public directories must be owned by root or an application account.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that all public directories are owned by root or an application account.

GEN002540	All public directories must be group-owned by system or an application group.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that all public directories are group-owned by system or an application group.

GEN002680	System audit logs must be owned by root.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified files are owned by root.

GEN002690	System audit logs must be group-owned by bin, sys, or system.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified files are group-owned by bin, sys, or system.

GEN003020	Cron must not run programs in, or subordinate to, world-writable directories.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Prevents cron from running programs in, or subordinate to, world-writable directories.

GEN003040	Crontabs must be owned by root or the crontab creator.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that crontabs are owned by root or by the crontab creator.

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
GEN003050	`Crontab` files must be group-owned by system, cron, or the crontab creator's primary group.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the `crontab` files are group-owned by system, cron, or the crontab creator's primary group.
GEN003110	`Cron` and `crontab` directories must not have extended access control lists.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified directories do not have extended access control lists.
GEN003120	`Cron` and `crontab` directories must be owned by root or bin.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that cron and crontab directories are owned by root or bin.
GEN003140	`Cron` and `crontab` directories must be group-owned by system, sys, bin, or cron.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified directories are group-owned by system, sys, bin, or cron.
GEN003160	Cron logging must be implemented.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that cron logging is implemented.
GEN003240	The `cron.allow` file must be owned by root, bin, or sys.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is owned by root, bin, or sys.
GEN003250	The `cron.allow` file must be group-owned by system, bin, sys, or cron.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is group-owned by system, bin, sys, or cron.
GEN003260	The `cron.deny` file must be owned by root, bin, or sys.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is owned by root, bin, or sys.

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
GEN003270	The cron.deny file must be group-owned by system, bin, sys, or cron.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is group-owned by system, bin, sys, or cron.
GEN003420	The at directory must be owned by root, bin, sys, daemon, or cron.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified directory is owned by root, sys, daemon, or cron.
GEN003430	The at directory must be group-owned by system, bin, sys, or cron.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified directory is group-owned by system, bin, sys, or cron.
GEN003460	The at.allow file must be owned by root, bin, or sys.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is owned by root, bin, or sys.
GEN003470	The at.allow file must be group-owned by system, bin, sys, or cron.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is group-owned by system, bin, sys, or cron.
GEN003480	The at.deny file must be owned by root, bin, or sys.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is owned by root, bin, or sys.
GEN003490	The at.deny file must be group-owned by system, bin, sys, or cron.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is group-owned by system, bin, sys, or cron.
GEN003720	The inetd.conf file, xinetd.conf file, and the xinetd.d directory must be owned by root or bin.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified files and directory are owned by root or bin.

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
GEN003730	The `inetd.conf` file, `xinetd.conf` file, and the `xinetd.d` directory must be group-owned by bin, sys, or system.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified files and directory are group-owned by bin, sys, or system.
GEN003760	The `services` file must be owned by root or bin.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is owned by root or bin.
GEN003770	The `services` file must be group-owned by bin, sys, or system.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is group-owned by bin, sys, or system.
GEN003920	The `hosts.lpd` (or equivalent) file must be owned by root, bin, sys, or lp.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is owned by root, bin, sys, or lp.
GEN003930	The `hosts.lpd` (or equivalent) file must be group-owned by bin, sys, or system.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is group-owned by bin, sys, or system.
GEN003960	The **traceroute** command owner must be root.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the owner of the command is root.
GEN003980	The **traceroute** command must be group-owned by sys, bin, or system.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the command is group-owned by sys, bin, or system.
GEN004360	The `alias` file must be owned by root.	**Location** /etc/security/pscexpert/dodv2/ chowndodfiles **Compliance action** Ensures that the specified file is owned by root.

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

GEN004370	The `aliases` file must be group-owned by sys, bin, or system.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified file is group-owned by sys, bin, or system.

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.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    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.

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.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    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.

GEN004480	The SMTP service log file must be owned by root.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified file is owned by root.

GEN004920	The `ftpusers` file must be owned by root.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified file is owned by root.

GEN004930	The `ftpusers` file must be group-owned by bin, sys, or system.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified file is group-owned by bin, sys, or system.

GEN005360	The `snmpd.conf` file must be owned by root.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified file is owned by root.

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

GEN005365	The `snmpd.conf` file must be group-owned by bin, sys, or system.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified file is group-owned by bin, sys, or system.

GEN005400	The `/etc/syslog.conf` file must be owned by root.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified file is owned by root.

GEN005420	The `/etc/syslog.conf` file must be group-owned by bin, sys, or system.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified file is group-owned by bin, sys, or system.

GEN005610	The system must not have IP forwarding for IPv6 enabled, unless the system is an IPv6 router.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that IP forwarding for IPv6 is not enabled unless the system is being used as an IPv6 router.

GEN005740	The NFS export configuration file must be owned by root.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified file is owned by root.

GEN005750	The NFS export configuration file must be group-owned by root, bin, sys, or system.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified file is group-owned by root, bin, sys, or system.

GEN005800	All NFS-exported system files and system directories must be owned by root.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified file is owned by root.

GEN005810	All NFS-exported system files and system directories must be group-owned by root, bin, sys, or system.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `chowndodfiles`
		
		Compliance action
		    Ensures that the specified files and directories are group-owned by root, bin, sys, or system.

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

GEN006100	The /usr/lib/smb.conf file must be owned by root.	**Location**
		    /etc/security/pscexpert/dodv2/ chowndodfiles
		
		Compliance action
		    Ensures that the specified file is owned by root.

GEN006120	The /usr/lib/smb.conf file must be group-owned by bin, sys, or system.	**Location**
		    /etc/security/pscexpert/dodv2/ chowndodfiles
		
		Compliance action
		    Ensures that the specified file is group-owned by bin, sys, or system.

GEN006160	The /var/private/smbpasswd file must be owned by root.	**Location**
		    /etc/security/pscexpert/dodv2/ chowndodfiles
		
		Compliance action
		    Ensures that the specified file is owned by root.

GEN006180	The /var/private/smbpasswd file must be group-owned by sys or system.	**Location**
		    /etc/security/pscexpert/dodv2/ chowndodfiles
		
		Compliance action
		    Ensures that the specified file is group-owned by sys or system.

GEN006340	Files in the /etc/news directory must be owned by root or news.	**Location**
		    /etc/security/pscexpert/dodv2/ chowndodfiles
		
		Compliance action
		    Ensures that the specified directory is owned by root or news.

GEN006360	The files in /etc/news must be group-owned by system or news.	**Location**
		    /etc/security/pscexpert/dodv2/ chowndodfiles
		
		Compliance action
		    Ensures that the specified files are group-owned by system or news.

GEN008080	If the system is using LDAP for authentication or account information, the /etc/ldap.conf (or equivalent) file must be owned by root.	**Location**
		    /etc/security/pscexpert/dodv2/ chowndodfiles
		
		Compliance action
		    Ensures that the specified file is owned by root.

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.	**Location**
		    /etc/security/pscexpert/dodv2/ chowndodfiles
		
		Compliance action
		    Ensures that the specified file is group-owned by bin, sys, or system.

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
GEN008140	If the system is using LDAP for authentication or account information, the TLS certificate authority file or directory must be owned by root.	**Location** `/etc/security/pscexpert/dodv2/ chowndodfiles` **Compliance action** Ensures that the specified file is owned by root.
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.	**Location** `/etc/security/pscexpert/dodv2/ chowndodfiles` **Compliance action** Ensures that the specified file is group-owned by bin, sys, or system.

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.	**Location** `/etc/security/pscexpert/dodv2/ fpmdodfiles` **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
AIX00340	The `/etc/ftpaccess.ctl` file must have mode 0640 or a mode that is less permissive.	**Location** `/etc/security/pscexpert/dodv2/ fpmdodfiles` **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
GEN000252	The time synchronization configuration file (such as `/etc/ntp.conf`) must have mode 0640 or a mode that is less permissive.	**Location** `/etc/security/pscexpert/dodv2/ fpmdodfiles` **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
GEN000920	The root account's home directory (other than /) must have mode 0700.	**Location** `/etc/security/pscexpert/dodv2/ fpmdodfiles` **Compliance action** Ensures that the directory is set to the specified permission mode, or to one that is less permissive.

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

GEN001140	System files and directories must not have uneven access permissions.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the access permissions are consistent.

GEN001180	All network services daemon files must have mode 0755 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN001200	All system command files must have mode 0755 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN001260	System log files must have mode 0640 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN001280	Manual page files must have mode 0644 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN001300	Library files must have mode 0755 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN001360	The NIS/NIS+/yp files must have mode 0755 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

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

GEN001364	The `/etc/resolv.conf` file must have mode 0644 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/ fpmdodfiles`
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN001368	The `/etc/hosts` file must have mode 0644 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/ fpmdodfiles`
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN001373	The `/etc/nsswitch.conf` file must have mode 0644 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/ fpmdodfiles`
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN001380	The `/etc/passwd` file must have mode 0644 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/ fpmdodfiles`
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN001393	The `/etc/group` file must have mode 0644 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/ fpmdodfiles`
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN001420	The `/etc/security/passwd` file must have mode 0400.	**Location**
		    `/etc/security/pscexpert/dodv2/ fpmdodfiles`
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN001480	All of a user's home directories must have a mode of 0750 or less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/ fpmdodfiles`
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

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

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.	**Location**
		
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN001580	All run control scripts must have mode 0755 or a mode that is less permissive.	**Location**
		
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN001640	Run control scripts must not run world-writable programs or scripts.	**Location**
		
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Checks programs, such as `cron`, for world-writable programs or scripts.

GEN001720	All global initialization files must have mode 0644 or a mode that is less permissive.	**Location**
		
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN001800	All skeleton files (for example, files in /etc/skel) must have mode 0644 or a mode that is less permissive.	**Location**
		
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN001880	All local initialization files must have mode 0740 or a mode that is less permissive.	**Location**
		
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN002220	All shell files must have mode 0755 or a mode that is less permissive.	**Location**
		
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

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
GEN002320	Audio devices must have mode 0660 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the audio devices are set to the specified permission mode, or one that is less permissive,
GEN002560	The system and user default **umask** must be 077.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the specified settings are *077.*
GEN002700	System audit logs must have mode 0640 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the files are set to the specified permission mode, or to one that is less permissive.
GEN002717	System audit tool executable files must have mode 0750 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the files are set to the specified permission mode, or to one that is less permissive.
GEN002980	The cron.allow file must have mode 0600 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
GEN003080	Crontab files must have mode 0600 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the files are set to the specified permission mode, or to one that is less permissive.
GEN003090	Crontab files must not have extended access control lists (ACLs).	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the specified files do not have extended ACLs.

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
GEN003100	Cron and crontab directories must have mode 0755 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the specified directories are set to the specified permissions mode, or to one that is less permissive.
GEN003180	The `cronlog` file must have mode 0600 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
GEN003200	The `cron.deny` file must have mode 0600 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
GEN003252	The `at.deny` file must have mode 0640 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
GEN003340	The `at.allow` file must have mode 0600 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
GEN003400	The `at` directory must have mode 0755 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the directory is set to the specified permission mode, or to one that is less permissive.
GEN003440	At jobs must not set the **umask** parameter to a value less restrictive than 077.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the parameter is set to the specified permission mode, or to one that is less permissive.

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

GEN003740	The `inetd.conf` and `xinetd.conf` files must have mode 0440 or a mode that is less permissive.	**Location**
		    /etc/security/pscexpert/dodv2/ fpmdodfiles
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN003780	The `services` file must have mode 0444 or a mode that is less permissive.	**Location**
		    /etc/security/pscexpert/dodv2/ fpmdodfiles
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN003940	The `hosts.lpd` file (or equivalent) must have mode 0644 or a mode that is less permissive.	**Location**
		    /etc/security/pscexpert/dodv2/ fpmdodfiles
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN004000	The `traceroute` file must have mode 0700 or a mode that is less permissive.	**Location**
		    /etc/security/pscexpert/dodv2/ fpmdodfiles
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN004380	The `alias` file must have mode 0644 or a mode that is less permissive.	**Location**
		    /etc/security/pscexpert/dodv2/ fpmdodfiles
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN004420	Files that are run through a mail `aliases` file must have mode 0755 or a mode that is less permissive.	**Location**
		    /etc/security/pscexpert/dodv2/ fpmdodfiles
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN004500	The SMTP service log file must have mode 0644 or a mode that is less permissive.	**Location**
		    /etc/security/pscexpert/dodv2/ fpmdodfiles
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

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

GEN004940	The `ftpusers` file must have mode 0640 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN005040	All FTP users must have a default **umask** setting of 077.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the setting is correct.

GEN005100	The `TFTP` daemon must have mode 0755 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the daemon is set to the specified mode, or to one that is less permissive.

GEN005180	All `.Xauthority` files must have mode 0600 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN005320	The `snmpd.conf` file must have mode 0600 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

GEN005340	Management Information Base (MIB) files must have mode 0640 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the files are set to the specified permission mode, or to one that is less permissive.

GEN005390	The `/etc/syslog.conf` file must have mode 0640 or a mode that is less permissive.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `fpmdodfiles`
		
		Compliance action
		    Ensures that the file is set to the specified permission mode, or to one that is less permissive.

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
GEN005522	The SSH public host key files must have mode 0644 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the files are set to the specified permission mode, or to one that is less permissive.
GEN005523	The SSH private host key files must have mode 0600 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the files are set to the specified permission mode, or to one that is less permissive.
GEN006140	The /usr/lib/smb.conf file must have mode 0644 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
GEN006200	The /var/private/smbpasswd file must have mode 0600 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
GEN006260	The /etc/news/hosts.nntp file (or equivalent) must have mode 0600 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
GEN006280	The /etc/news/hosts.nntp.nolimit file (or equivalent) must have mode 0600 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.
GEN006300	The /etc/news/nnrp.access file (or equivalent) must have mode 0600 or a mode that is less permissive.	**Location** /etc/security/pscexpert/dodv2/ fpmdodfiles **Compliance action** Ensures that the file is set to the specified permission mode, or to one that is less permissive.

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

GEN006320	The /etc/news/passwd.nntp file (or equivalent) must have mode 0600 or a mode that is less permissive.	**Location**
		
		`/etc/security/pscexpert/dodv2/`
		`fpmdodfiles`
		
		Compliance action
		Ensures that the file is set to the specified permission mode, or to one that is less permissive.

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.	**Location**
		
		`/etc/security/pscexpert/dodv2/`
		`fpmdodfiles`
		
		Compliance action
		Ensures that the file is set to the specified permission mode, or to one that is less permissive.

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.	**Location**
		
		`/etc/security/pscexpert/dodv2/`
		`fpmdodfiles`
		
		Compliance action
		Ensures that the specified file, directories, or both, are set to the specified permission mode, or to one that is less permissive.

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).	**Location**
		
		`/etc/security/pscexpert/dodv2/`
		`acldodfiles`
		
		Compliance action
		Disables the specified extended ACL.
		Note: 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.

AIX00350	The /etc/ftpaccess.ctl file must not have an extended ACL.	**Location**
		
		`/etc/security/pscexpert/dodv2/`
		`acldodfiles`
		
		Compliance action
		Disables the specified extended ACL.
		Note: 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.

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
GEN000253	The time synchronization configuration file (such as /etc/ntp.conf) must not have an extended ACL.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN000930	The root account's home directory must not have an extended ACL.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN001190	All network services daemon files must not have extended ACLs.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN001210	All system command files must not have extended ACLs.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN001270	System log files must not have extended ACLs, except as needed to support authorized software.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.

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

GEN001310	All library files must not have extended ACLs.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `acldodfiles`
		
		Compliance action
		    Disables the specified extended ACL.
		    Note: 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.

GEN001361	NIS/NIS+/yp command files must not have extended ACLs.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `acldodfiles`
		
		Compliance action
		    Disables the specified extended ACL.
		    Note: 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.

GEN001365	The `/etc/resolv.conf` file must not have an extended ACL.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `acldodfiles`
		
		Compliance action
		    Disables the specified extended ACL.
		    Note: 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.

GEN001369	The `/etc/hosts` file must not have an extended ACL.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `acldodfiles`
		
		Compliance action
		    Disables the specified extended ACL.
		    Note: 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.

GEN001374	The `/etc/nsswitch.conf` file must not have an extended ACL.	**Location**
		    `/etc/security/pscexpert/dodv2/`
		    `acldodfiles`
		
		Compliance action
		    Disables the specified extended ACL.
		    Note: 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.

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
GEN001390	The /etc/passwd file must not have an extended ACL.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN001394	The /etc/group file must not have an extended ACL.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN001430	The /etc/security/passwd file must not have an extended ACL.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN001570	All files and directories that are contained in user home directories must not have extended ACLs.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN001590	All run control scripts must have no extended ACLs.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.

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
GEN001730	All global initialization files must not have extended ACLs.	**Location** `/etc/security/pscexpert/dodv2/ acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN001810	Skeleton files must not have extended ACLs.	**Location** `/etc/security/pscexpert/dodv2/ acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN001890	Local initialization files must not have extended ACLs.	**Location** `/etc/security/pscexpert/dodv2/ acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN002230	All shell files must not have extended ACLs	**Location** `/etc/security/pscexpert/dodv2/ acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN002330	Audio devices must not have extended ACLs.	**Location** `/etc/security/pscexpert/dodv2/ acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.

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
GEN002710	All system audit files must not have extended ACLs	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN002990	Extended ACLs should be disabled for the cron.allow and cron.deny files.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN003090	Crontab files must not have extended ACLs.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN003110	Cron and crontab directories must not have extended ACLs.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN003190	The cron log files must not have extended ACLs.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.

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
GEN003210	The `cron.deny` file must not have an extended ACL.	**Location** `/etc/security/pscexpert/dodv2/ acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN003245	The `at.allow` file must not have an extended ACL.	**Location** `/etc/security/pscexpert/dodv2/ acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN003255	The `at.deny` file must not have an extended ACL.	**Location** `/etc/security/pscexpert/dodv2/ acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN003410	The at directory must not have an extended ACL.	**Location** `/etc/security/pscexpert/dodv2/ acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN003745	The `inetd.conf` and `xinetd.conf` files must not have extended ACLs.	**Location** `/etc/security/pscexpert/dodv2/ acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.

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
GEN003790	The services file must not have an extended ACL.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN003950	The hosts.lpd file (or equivalent) must not have an extended ACL.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN004010	The traceroute file must not have an extended ACL.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN004390	The alias file must not have an extended ACL.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN004430	Files that are run through a mail aliases file must not have extended ACLs.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.

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

GEN004510	The SMTP service log file must not have an extended ACL.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`acldodfiles`
		
		Compliance action
		Disables the specified extended ACL.
		Note: 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.

GEN004950	The `ftpusers` file must not have an extended ACL.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`acldodfiles`
		
		Compliance action
		Disables the specified extended ACL.
		Note: 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.

GEN005190	The `.Xauthority` files must not have extended ACLs.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`acldodfiles`
		
		Compliance action
		Disables the specified extended ACL.
		Note: 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.

GEN005350	Management Information Base (MIB) files must not have extended ACLs.	**Location**
		`/etc/security/pscexpert/dodv2/`
		`acldodfiles`
		
		Compliance action
		Disables the specified extended ACL.
		Note: 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.

GEN005375	The `snmpd.conf` file must not have an extended ACL	**Location**
		`/etc/security/pscexpert/dodv2/`
		`acldodfiles`
		
		Compliance action
		Disables the specified extended ACL.
		Note: 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.

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
GEN005395	The `/etc/syslog.conf` file must not have an extended ACL.	**Location** `/etc/security/pscexpert/dodv2/acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN006150	The `/usr/lib/smb.conf` file must not have an extended ACL.	**Location** `/etc/security/pscexpert/dodv2/acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN006210	The `/var/private/smbpasswd` file must not have an extended ACL.	**Location** `/etc/security/pscexpert/dodv2/acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN006270	The `/etc/news/hosts.nntp` file must not have an extended ACL.	**Location** `/etc/security/pscexpert/dodv2/acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN006290	The `/etc/news/hosts.nntp.nolimit` file must not have an extended ACL.	**Location** `/etc/security/pscexpert/dodv2/acldodfiles` **Compliance action** Disables the specified extended ACL. **Note:** 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.

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
GEN006310	The /etc/news/nnrp.access file must not have an extended ACL.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
GEN006330	The /etc/news/passwd.nntp file must not have an extended ACL.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Disables the specified extended ACL. **Note:** 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.
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).	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Ensures that the specified files do not have an extended ACL. **Note:** 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.
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.	**Location** /etc/security/pscexpert/dodv2/ acldodfiles **Compliance action** Ensures that the specified directory or file does not have an extended ACL. **Note:** 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.

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

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

- Change user passwords at least every 90 days.
- Require a minimum password length of 7 characters.
- Use a password that contains both numerals and alphabetic characters.
- Do not allow an individual to submit a new password that is the same as the previous four passwords that were used.
- Limit repeated access attempts by locking out the user ID after six unsuccessful attempts.
- Set the lockout duration to 30 minutes, or until an administrator re-enables the user ID.
- 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.
> 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.
> 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 Standard Edition reduces the configuration management that is required to meet the guidelines that are defined by PCI DSS version 2.0 and PCI DSS version 3.0. 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 Standard 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/pscexpert/bin` directory.

The following table shows how PowerSC Standard Edition address 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 version 2.0 and version 3.0 standards

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
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 by setting the **minage** parameter to a value of 0.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 8.5.9 **PCI version 3** 8.2.4	Change user passwords at least every 90 days.	Sets the maximum number of weeks that a password is valid to 13 weeks by setting the **maxage** parameter to a value of 13.	/etc/security/pscexpert/bin/chusrattr

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
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 by setting the **maxexpired** parameter to a value of 8.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 8.5.10 PCI version 3 8.2.3	Require a minimum password length of at least 7 characters.	Sets the minimum password length to 7 characters by setting the **minlen** parameter to a value of 7.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 8.5.11 PCI version 3 8.2.3	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 by setting the **minalpha** parameter to a value of 1.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 8.5.11 PCI version 3 8.2.3	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 by setting the **minother** parameter to a value of 1.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 2.1 PCI version 3 8.2.2	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 by setting the **maxrepeats** parameter to a value of 8. This setting indicates that a character in a password can be repeated an unlimited number of times when it conforms to the other password limitations.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 8.5.12 PCI version 3 8.2.5	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 by setting the **histexpire** parameter to a value of 52.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 8.5.12 PCI version 3 8.2.5	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 by setting the **histsize** parameter to a value of 4.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 8.5.13 PCI version 3 8.1.6	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 by setting the **loginentries** parameter to a value of 6.	/etc/security/pscexpert/bin/chusrattr

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 2 8.5.13 **PCI version 3** 8.1.6	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 by setting the **logindisable** parameter to a value of 6.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
PCI version 2 8.5.14 **PCI version 3** 8.1.7	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 *logindisable* attribute to 30 minutes by setting the **loginreenable** parameter to a value of 30.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
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.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
8.1.1	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.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
10.2	Enable auditing on the system.	Enables auditing of the binary files on the system.	/etc/security/pscexpert/bin/pciaudit
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include the Common Desktop Environment (CDE).	Disables the CDE function when the layer four traceroute (LFT) is not configured.	/etc/security/pscexpert/bin/comntrows
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include the timed daemon.	Stops the timed daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscexpert/bin/rctcpip
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include the rwhod daemon.	Stops the rwhod daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscexpert/bin/rctcpip
PCI version 2 2.1 **PCI version 3** 2.1.1	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.	/etc/security/pscexpert/bin/rctcpip

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value

PCI version 2
    2.1
 	
PCI version 3
    2.1.1
	Change vendor-supplied defaults before installing a system on the network, which includes disabling the SNMPMIBD daemon.	Disables the SNMPMIBD daemon by commenting out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscexpert/bin/rctcpip

2.1	Change vendor-supplied defaults before installing a system on the network, which includes disabling the AIXMIBD daemon.	Disables the AIXMIBD daemon by commenting out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscexpert/bin/rctcpip
2.1	Change vendor-supplied defaults before installing a system on the network, which includes disabling the HOSTMIBD daemon.	Disables the HOSTMIBD daemon by commenting out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscexpert/bin/rctcpip

PCI version 2
    1.1.5
 	
    2.2.2
 	
PCI version 3
    2.2.2
	Disable unnecessary and insecure services, which include the DPID2 daemon.	Stops the DPID2 daemon and comments out the corresponding entry in the /etc/rc.tcpip file that automatically starts the daemon.	/etc/security/pscexpert/bin/rctcpip

PCI version 2
    2.1
 	
PCI version 3
    2.2.2
	Change vendor-supplied defaults before installing a system on the network, which includes stopping the DHCP server.	Disables the DHCP server.	/etc/security/pscexpert/bin/rctcpip

PCI version 2
    1.1.5
 	
    2.2.2
 	
PCI version 3
    2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/rctcpip

PCI version 2
    1.1.5
 	
    2.2.2
 	
PCI version 3
    2.2.2
	Disable unnecessary and insecure services, which include the rshd daemon.	Stops and disables all instances of the rshd daemon and the shell service, and comments out the corresponding entries in the /etc/inetd.conf file that automatically start the instances.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
    1.1.5
 	
    2.2.2
 	
PCI version 3
    2.2.2
	Disable unnecessary and insecure services, which include the rlogind daemon.	Stops and disables all instances of the rlogind daemon and rlogin service. The AIX Security Expert utility also comments out the corresponding entries in the /etc/inetd.conf file that automatically start the instances.	/etc/security/pscexpert/bin/cominetdconf

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf
2.1	Change vendor-supplied defaults before installing a system on the network, which includes disabling the `netstat` command.	Disables the `netstat` command by commenting out the corresponding entry in the /etc/inetd.conf file.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.3	Disable unnecessary and insecure services, which include the `tftp` daemon.	Stops and disables all instances of the `tftp` daemon. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the daemon.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value

PCI version 2
  1.1.5
 	
  2.2.2
 	
PCI version 3
  2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
  1.1.5
 	
  2.2.2
 	
PCI version 3
  2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
  1.1.5
 	
  2.2.2
 	
PCI version 3
  2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
  1.1.5
 	
  2.2.2
 	
PCI version 3
  2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
  1.1.5
 	
  2.2.2
 	
PCI version 3
  2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
  1.1.5
 	
  2.2.2
 	
PCI version 3
  2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
  1.1.5
 	
  2.2.2
 	
PCI version 3
  2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value

PCI version 2
    1.1.5
    2.2.2
 	
PCI version 3
    2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
    1.1.5
    2.2.2
 	
PCI version 3
    2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
    1.1.5
    2.2.2
 	
PCI version 3
    2.2.3
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
    1.1.5
    2.2.2
 	
PCI version 3
    2.2.3
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
    1.1.5
    2.2.2
 	
PCI version 3
    2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
    1.1.5
    2.2.2
 	
PCI version 3
    2.2.2
	Disable unnecessary and insecure services, which include the ttdbserver service.	Stops and disables all instances of the ttdbserver service. The AIX Security Expert utility also comments out the corresponding entry in the /etc/inetd.conf file that automatically starts the service.	/etc/security/pscexpert/bin/cominetdconf

PCI version 2
    1.1.5
    2.2.2
 	
PCI version 3
    2.2.2
	Disable unnecessary and insecure services, which include 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.	/etc/security/pscexpert/bin/cominetdconf

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 2 2.2.3 **PCI version 3** 2.2.4	Configure system security parameters to prevent misuse.	Removes the Set User ID (SUID) commands by commenting out the corresponding entry in the `/etc/inetd.conf` file that automatically enables the commands.	`/etc/security/pscexpert/bin/rmsuidfrmrcmds`
PCI version 2 2.2.3 **PCI version 3** 2.2.4	Configure system security parameters to prevent misuse.	Enables the lowest security level for the File Permissions Manager.	`/etc/security/pscexpert/bin/filepermgr`
PCI version 2 2.2.3 **PCI version 3** 2.2.4	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.	`/etc/security/pscexpert/bin/nfsconfig`
PCI version 2 2.2.2 **PCI version 3** 2.2.3	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.	`/etc/security/pscexpert/bin/disrmtdmns`
PCI version 2 2.2.2 **PCI version 3** 2.2.3	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.	`/etc/security/pscexpert/bin/rmrhostsnetrc`
PCI version 2 2.2.2 **PCI version 3** 2.2.3	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.	`/etc/security/pscexpert/bin/rmetchostsequiv`
PCI version 2 1.3.6 **PCI version 3** 2.2.3	Implement stateful inspection, or packet filtering, in which only established connections are allowed on the network.	Enables the network **`clean_partial_conns`** option by setting its value to 1.	`/etc/security/pscexpert/bin/ntwkopts`

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value

PCI version 2
    2.2.2
 	
PCI version 3
    2.2.3
	Implement stateful inspection, or packet filtering, in which only established connections are allowed on the network.	Enables TCP security by setting the network **tcp_tcpsecure** option to a value of 7. This setting provides protection against data, reset (RST), and TCP connection request (SYN) attacks.	/etc/security/pscexpert/bin/ntwkopts

1.2	Protect unauthorized access to unused ports.	Configures the system to shun the hosts for 5 minutes to prevent other systems from accessing unused ports.	/etc/security/pscexpert/bin/ ipsecshunhosthls **Note:** 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: *port_number:ip_address: action* where the possible values for *action* are Allow or Deny.
1.2	Protect the host from port scans.	Configures the system to shun vulnerable ports for 5 minutes, which prevents port scans.	/etc/security/pscexpert/bin/ipsecshunports **Note:** 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: *port_number:ip_address: action* where the possible values for *action* are Allow or Deny.
7.1.1	Limit object creation permissions.	Sets the default object creation permissions to 22 by setting the **umask** parameter to a value of 22.	/etc/security/pscexpert/bin/chusrattr
7.1.1	Limit system access.	Ensures that the root ID the only one that is listed in the cron.allow file and removes the cron.deny file from the system.	/etc/security/pscexpert/bin/limitsysacc
6.5.8	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: • .cshrc • .kshrc • .login • .profile	/etc/security/pscexpert/bin/ rmdotfrmpathroot

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
6.5.8	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: • .cshrc • .kshrc • .login • .profile	/etc/security/pscexpert/bin/ rmdotfrmpathnroot
2.2.3	Limit system access.	Adds the root user capability and user name in the /etc/ftpusers file.	/etc/security/pscexpert/bin/chetcftpusers
2.1	Remove the guest account.	Removes the guest account and its files.	/etc/security/pscexpert/bin/execmds
6.5.2	Prevent launching programs in content space.	Enables the stack execution disable (SED) feature.	/etc/security/pscexpert/bin/sedconfig
8.2	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.	/etc/security/pscexpert/bin/chuserstanza

PCI version 2
    8.5.15
 	
PCI version 3
    8.1.8
	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.	/etc/security/pscexpert/bin/autologoff

1.3.5	Limit traffic access to cardholder information.	Sets the TCP traffic regulation to its high setting, which enforces denial-of-service mitigation on ports.	/etc/security/pscexpert/bin/ tcptr_pscexpert
1.3.5	Maintain a secure connection when migrating data.	Enables automated IP Security (IPSec) tunnel creation between Virtual I/O Servers during live partition migration.	/etc/security/pscexpert/bin/cfgsecmig
1.3.5	Limit packets from unknown sources.	Allows the packets from the Hardware Management Console.	/etc/security/pscexpert/bin/ ipsecpermithostorport
5.1.1	Maintain antivirus software.	Maintains the system integrity by detecting, removing, and protecting against known types of malicious software.	/etc/security/pscexpert/bin/ manageITsecurity

PCI version 2
    Section 7
 	
PCI version 3
    Section 7
	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.	/etc/security/pscexpert/bin/EnableRbac

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 2 Not included in version 2 profile, added in version 3. **PCI version 3** 2.3	Implement more security features for any required services, protocols, or daemons that are considered to be insecure.	Uses secured technologies such as Secure Shell (SSH), SSH File Transfer Protocol (S-FTP), Secure Sockets Layer (SSL), or Internet Protocol Security Virtual Private Network (IPsec VPN) to protect insecure services such as NetBIOS, file-sharing, Telnet, and FTP. It also configures the SSH daemon to use only the SSHv2 protocol.	/etc/security/pscexpert/bin/sshPCIconfig
PCI version 2 Not included in version 2 profile, added in version 3. **PCI version 3** 2.3	The SSH Client must be configured to use only the SSHv2 protocol.	Configures the SSH client to use the SSHv2 protocol.	/etc/security/pscexpert/bin/sshPCIconfig
PCI version 2 Not included in version 2 profile, added in version 3. **PCI version 3** 2.3	The SSH daemon must listen only on management network addresses unless it is authorized for uses other than management.	Ensures that the SSH daemon is set up only to listen.	/etc/security/pscexpert/bin/sshPCIconfig
PCI version 2 Not included in version 2 profile, added in version 3. **PCI version 3** 2.3	The SSH daemon must be configured to use only FIPS 140-2 approved ciphers	Ensures that the SSH daemon uses only the FIPS 140-2 ciphers.	/etc/security/pscexpert/bin/sshPCIconfig
PCI version 2 Not included in version 2 profile, added in version 3. **PCI version 3** 2.3	The SSH daemon must be configured to use only Message Authentication Codes (MACs) that employ FIPS 140-2 approved cryptographic hash algorithms.	Ensures that the MACs are running the approved algorithms.	/etc/security/pscexpert/bin/sshPCIconfig
PCI version 2 Not included in version 2 profile, added in version 3. **PCI version 3** 2.3	The SSH daemon must restrict login ability to specific users or groups.	Restricts login on the system to specific users and groups.	/etc/security/pscexpert/bin/sshPCIconfig

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value

PCI version 2
    Not included in version 2 profile, added in version 3.
 	
PCI version 3
    2.3
	The system must display the date and time of the last successful account login upon login.	Maintains the information from the last successful login, and displays it after the next successful login.	/etc/security/pscexpert/bin/sshPCIconfig

PCI version 2
    Not included in version 2 profile, added in version 3.
 	
PCI version 3
    2.3
	The SSH daemon must complete strict mode checking of home directory configuration files.	Ensures that the home directory configuration files are set to the correct modes.	/etc/security/pscexpert/bin/sshPCIconfig

PCI version 2
    Not included in version 2 profile, added in version 3.
 	
PCI version 3
    2.3
	The SSH daemon must use privilege separation.	Ensures that the SSH daemon has the correct amount of separation of its privileges.	/etc/security/pscexpert/bin/sshPCIconfig

PCI version 2
    Not included in version 2 profile, added in version 3.
 	
PCI version 3
    2.3
	The SSH daemon must not allow rhosts to have RSA authentication.	Disables RSA authentication for rhosts when you are using the SSH daemon.	/etc/security/pscexpert/bin/sshPCIconfig

PCI version 2
    1.1.5
 	
    2.2.2
 	
PCI version 3
    10.4
	Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	Enables the ntp daemon.	/etc/security/pscexpert/bin/rctcpip

PCI version 2
    Not included in version 2 profile, added in version 3.
 	
PCI version 3
    8.1.5
	Disable a user account when not in use.	Disables user accounts after 35 days of inactivity.	/etc/security/pscexpert/bin/disableacctpci

PCI version 3 2.2.3	Disable Secure Sockets Layer (SSL) v3 and Transport Layer Security (TLS) v1.0 in applications.	Disable SSLv3 and TLS v1.0 versions in Courier POP3 server (Pop3d) configuration.	/etc/security/pscexpert/bin/disableSSL

Table 6. Settings related to the PCI DSS compliance version 2.0 and version 3.0 standards (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the script that modifies the value
PCI version 3 2.2.3	Disable SSL v3 and TLS v1.0 in applications.	Disable SSLV3 and TLS v1.0 in the Courier IMAP server (imapd).	`/etc/security/pscexpert/bin/disableSSL`
PCI version 3 8.2.1	Disable SSL v3 and TLS v1.0 in applications.	Check the Network Time Protocol (NTP) configuration file for TLS 1.1, or later security adoption.	`/etc/security/pscexpert/bin/checkNTP`
PCI version 3 2.2.3	Disable SSL v3 and TLS v1.0 in applications.	Check the File Transfer Protocol Daemon (FTPD) configuration file for TLS 1.1, or later security adoption.	`/etc/security/pscexpert/bin/secureFTP`
PCI version 3 2.2.3	Disable SSL v3 and TLS v1.0 in applications.	Check the File Transfer Protocol (FTP) configuration file for TLS 1.1, or later security adoption.	`/etc/security/pscexpert/bin/secureFTP`
PCI version 3 2.2.3	Disable SSL v3 and TLS v1.0 in applications.	Disable SSLv3 and TLS v1.0 in sendmail configuration.	`/etc/security/pscexpert/bin/` `sendmailPCIConfig`
PCI version 3 2.2.3	Disable SSL v3 and TLS v1.0 in applications.	Check whether the SSL version on AIX is greater than 1.0.2.	`/etc/security/pscexpert/bin/sslversion`
PCI version 3 8.2.1	Enforce two factor authentication.	Enforce two factor authentication such as SHA-256 or SHA-512.	`/etc/security/pscexpert/bin/pwdalgchk`

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 Standard 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 the following version of the AIX operating system:
- AIX 6.1
- AIX 7.1
- AIX 7.2

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

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/pscexpert/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.	**Command**: **#audit query**. **Return value**: If successful, this command exits with a value of 0. If unsuccessful, the command exits with a value 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) (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.	**Command**: **# audit start >/dev/null 2>&1**. **Return value**: 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: **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**
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.	**Command**: **# efskeymgr -V >/dev/null 2>&1**. **Return value**: 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.	**Command**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT**. **Return value**: If the command fails to find the value **TMOUT=15**, 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.	**Command**: **chsec -f /etc/security/user -s user -a minlen=8**. **Return value**: If successful, this script exits with a value of 0. If unsuccessful, the script 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.	Ensures that all passwords include at least two alphabetic characters, one of which must be capitalized.	**Command**: **chsec -f /etc/security/user -s user –a minalpha=4**. **Return value**: 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 nonalphabetic characters in a password to 2.	**Command**: **#chsec –f /etc/security/user –s user –a minother=2**. **Return value**: 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.	**Command**: **#chsec –f /etc/security/user –s user –a maxrepeats=1**. **Return value**: 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.	**Command**: **#chsec –f /etc/security/user –s user –a histsize=5**. **Return value**: 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.	**Command**: **#chsec –f /etc/security/user –s user –a maxage=8**. **Return value**: 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.	**Command**: **#chsec –f /etc/security/user –s user –a minage=2**. **Return value**: 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 **maxage** parameter set by the user expires.	**Command**: **#chsec –f /etc/security/user –s user –a maxexpired=4**. **Return value**: 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 characters that cannot be repeated from the old password is 4 characters.	**Command**: **#chsec –f /etc/security/user –s user –a mindiff=4**. **Return value**: 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 that the number of days is 5 to wait before the system issues a warning that a password change is required.	**Command**: **#chsec –f /etc/security/user –s user –a pwdwarntime = 5**. **Return value**: 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.	**Command**: **/usr/bin/usrck -y ALL** **/usr/bin/usrck –n ALL**. **Return value**: 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.	**Command**: **#chsec –f /etc/security/user –s user –a loginretries=3**. **Return value**: 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.	**Command**: **chsec -f /etc/security/login.cfg -s default -a logindelay=5**. **Return value**: 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.	**Command**: **chsec -f /etc/security/lastlog -s username -a \ unsuccessful_login_count=10**. **Return value**: 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.	**Command**: **#chsec -f /etc/security/lastlog -s user –a time_last_unsuccessful_ login=60**. **Return value**: 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 after which a port is unlocked and after being disabled, as 30 minutes.	**Command**: **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30**. **Return value**: 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 to type a password as 30 seconds.	**Command**: **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30**. **Return value**: 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.	**Command**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}**. **Return value**: If the command fails to set the value of **account_locked** to **true**, 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.	**Command**: Turns on **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON For example, trustchk –p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON**. **Return value**: 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 **ssh** filesets are installed. If not, displays an error message.	**Command**: **# lslpp –l | grep openssh > /dev/null 2>&1**. **Return value**: If return code for this command is 0, the script exits with a value of 0. If ssh filesets are not installed, the script exits with a value of 1 and displays the error message `Install ssh filesets for secure transmission`.

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 **trcfile** file in the location, /var/adm/ras/trcfile. Sends the errors to **root@<hostname>**.	**Command**: **errpt -d H**. **Return value**: If successful, this command exits with a value of 0. If unsuccessful, the command exits with a value of 1.

Table 8. HIPAA Functions and implementation details (continued)

HIPAA functions	Implementation specification	The aixpert implementation	Commands and return values
FPM enablement	Changes file permissions.	Changes the permission of files from a list of permissions and files by using the **fpm** command.	**Command**: # **fpm -1 <level> -f <commands file>**. **Return value**: If successful, this command exits with a value of 0. If unsuccessful, the command exits with a value of 1.
RBAC enablement	Creates **isso**, **so**, and **sa** users and assigns appropriate roles to the users.	Suggests that you create **isso**, **so**, and **sa** users. Assigns appropriate roles to the users.	**Command**: **/etc/security/pscexpert/bin/ RbacEnablement**.

North American Electric Reliability Corporation compliance

The North American Electric Reliability Corporation (NERC) is a nonprofit corporation that develops standard for the electric power systems industry. PowerSC Standard Edition contains a preconfigured NERC profile, which provides security standards that you can use to protect critical electric power systems.

The NERC profile follows the Critical Infrastructure Protection (CIP) standards.

The NERC profile is located at `/etc/security/aixpert/custom/NERC.xml`. You can reset the CIP requirements that are applied to the NERC profile to the default state by applying the NERC_to_AIXDefault.xml profile that is located in the `/etc/security/aixpert/custom` directory. This process is not the same as the undo operation of the NERC profile.

The following table provides information about the CIP standards that are applied to the AIX operating system, and how PowerSC Standard Edition handles the CIP standards:

Table 9. CIP standards for PowerSC Standard Edition

CIP standard	AIX Security Expert implementation	Location of the script that modifies the value
CIP-003-3 R5.1	Configures system security parameters to prevent problems by removing the set-user identification (SUID) and set-group identification (SGID) attributes from the binary files.	• `/etc/security/pscexpert/bin/filepermgr` • `/etc/security/pscexpert/bin/rmsuidfrmrcmds`
CIP-003-3 R5.1.1	Enables role-based access control (RBAC) by creating system operator, system administrator, and information system security officer user roles with the required permissions.	`/etc/security/pscexpert/bin/EnableRbac`
CIP-005-3a R2.1-R2.4	Enables Secure Shell (SSH) for security access.	`/etc/security/pscexpert/bin/sshstart`
CIP-005-3a R2.5 CIP-007-5 R1.1	Disables the following unnecessary and insecure services: • **lpd** daemon • Common Desktop Environment (CDE)	`/etc/security/pscexpert/bin/comntrows`

Table 9. CIP standards for PowerSC Standard Edition (continued)

CIP standard	AIX Security Expert implementation	Location of the script that modifies the value
CIP-005-3a R2.5 CIP-007-5 R1.1	Disables the following unnecessary and insecure services: • **timed** daemon • **NTP** daemon • **rwhod** daemon • **DPID2** daemon • DHCP agent	/etc/security/pscexpert/bin/rctcpip
CIP-005-3a R2.5 CIP-007-5 R1.1	Disables the following unnecessary and insecure services: • **comsat** daemon • **dtspcd** daemon • **fingerd** daemon • **ftpd** daemon • **rshd** daemon • **rlogind** daemon • **rexecd** daemon • **systat** daemon • **tfptd** daemon • **talkd** daemon • **rquotad** daemon • **rstatd** daemon • **rusersd** daemon • **rwalld** daemon • **sprayd** daemon • **pcnfsd** daemon • **telnet** daemon • cmsd service • ttdbserver service • TCP echo service • TCP discard service • TCP chargen service • TCP daytime service • TCP time service • UDP echo service • UDP discard service • UDP chargen service • UDP daytime service • UDP time service	/etc/security/pscexpert/bin/cominetdconf
CIP-005-3a R2.5 CIP-007-5 R1.1	Enforces the denial of service request for mitigation ports.	/etc/security/pscexpert/bin/tcptr_aixpert
CIP-005-3a R3 CIP-007-3a R5, R6.5 CIP-007-5 R4.4	Enables auditing of the binary files on the system.	/etc/security/pscexpert/bin/pciaudit
CIP-007-3a R3 CIP-007-5 R2.1	Displays a message to enable Trusted Network Connect (TNC).	/etc/security/pscexpert/bin/GeneralMsg

Table 9. CIP standards for PowerSC Standard Edition (continued)

CIP standard	AIX Security Expert implementation	Location of the script that modifies the value
CIP-007-3a R4 CIP-007-5 R3.3	Maintains the system integrity by detecting, removing, and protecting against known types of malicious software.	`/etc/security/pscexpert/bin/manageITsecurity`
CIP-007-3a R5.2.1	Enables the password to be changed at the first login for all default users accounts that are not locked.	`/etc/security/pscexpert/bin/pwdchg`
CIP-007-3a R5.2.2-R5.2.3	Locks all default user accounts.	`/etc/security/pscexpert/dodv2/lockacc_rlogin`
CIP-007-3a R5.3.1	Sets each password to a minimum of 6 characters.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-5 R5.5.1	Sets each password to a minimum of 8 characters.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R5.3.2 CIP-007-5 R5.5.2	Sets each password to a combination of alpha, numeric, and special characters.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R5.3.3 CIP-007-5 R5.6	Changes each password annually.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R7	Displays a message to enable Encrypted File System (EFS).	`/etc/security/pscexpert/bin/GeneralMsg`
CIP-007-5 R5.7	Limit the number of unsuccessful authentication attempts.	`/etc/security/pscexpert/bin/chusrattr`
CIP-010-1 CIP-010-2 R2.1	Displays a message to enable Real Time Compliance (RTC).	`/etc/security/pscexpert/bin/GeneralMsg`

The following list displays information about the CIP standards that are applied to the AIX operating system:

Standard CIP–003–3 — Cyber Security — Security Management Controls

> **R5. Access Control**
>> The Responsible Entity documents and implements a program for managing access to protected Critical Cyber Asset (CCA) information.
>> - **R5.1:** The Responsible Entity maintains a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
>> - **R5.1.1:** Personnel are identified by name, title, and the information for which they are responsible for authorizing access.

Standard CIP–005–3a — Cyber Security — Electronic Security Perimeters

> **R2. Electronic Access Controls**
>> The Responsible Entity implements and documents the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeters.
>> - **R2.1:** These processes and mechanisms use an access control model that denies access by default, such that explicit access permissions must be specified
>> - **R2.2:** At all access points to the Electronic Security Perimeter(s), the Responsible Entity enables only ports and services that are required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and documents, individually or by specified grouping, the configuration of those ports and services.
>> - **R2.3:** The Responsible Entity implements and maintains a procedure for securing dial-up access to the Electronic Security Perimeters.

- **R2.4:** Where external interactive access into the Electronic Security Perimeter is enabled, the Responsible Entity implements strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
- **R2.5:** The required documentation, at a minimum, identify, and describe the following:
  - **R2.5.1:** The processes for access request and authorization.
  - **R2.5.2:** The authentication methods.
  - **R2.5.3:** The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.
  - **R2.5.4:** The controls that are used to secure dial-up accessible connections.

R3. Monitoring Electronic Access

The Responsible Entity implements and documents an electronic or manual process for monitoring and logging access at access points to the Electronic Security Perimeters twenty-four hours a day, seven days a week.

- **R3.1:** For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity implements and documents monitoring processes at each access point to the dial-up device, where technically feasible.
- **R3.2:** Where technically feasible, the security monitoring processes detect and alert for attempts at or actual unauthorized accesses. These alerts provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity reviews or obtains access logs for attempts at or actual unauthorized accesses at least every 90 days.

Standard CIP–007–3a — Cyber Security — Systems Security Management

R2. Ports and Services

The Responsible Entity establishes, documents, and implements a process to ensure that only those ports and services that are required for normal and emergency operations are enabled.

- **R2.1:** The Responsible Entity enables only those ports and services that are required for normal and emergency operations.
- **R2.2:** The Responsible Entity disables other ports and services, including ports that are used for testing purposes, before production use of all Cyber Assets inside the Electronic Security Perimeters.
- **R2.3:** In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity documents the compensating measures that are applied to mitigate risk exposure.

R3. Security Patch Management

The Responsible Entity, either separately or as a component of the documented configuration management process that is specified in CIP-003-3 Requirement R6, establishes, documents, and implements a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeters.

- **R3.1:** The Responsible Entity documents the assessment of security patches and security upgrades for applicability within 30 days of availability of the patches or upgrades.
- **R3.2:** The Responsible Entity documents the implementation of security patches. In any case where the patch is not installed, the Responsible Entity documents the compensating measures that are applied to mitigate risk exposure.

R4. Malicious Software Prevention

The Responsible Entity uses anti-virus software and other malicious software (malware)

prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeters.

- **R4.1:** The Responsible Entity documents and implements anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity documents compensating measures that are applied to mitigate risk exposure.

- **R4.2:** The Responsible Entity documents and implements a process for the update of anti-virus and malware prevention signatures. The process must address testing and installing the signatures.

R5. Account Management

The Responsible Entity establishes, implements, and documents technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

- **R5.1:** The Responsible Entity verifies that individual and shared system accounts and authorized access permissions are consistent with the concept of need to know regarding work functions that are performed.

  - **R5.1.1:** The Responsible Entity reviews, at least annually, user accounts to verify that access privileges are in accordance with Standard CIP-003-3.

  - **R5.1.2:** The Responsible Entity establishes methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of 90 days.

  - **R5.1.3:** The Responsible Entity reviews, at least annually, user accounts to verify that access privileges are in accordance with Standard CIP-003-3.

- **R5.2:** The Responsible Entity implements a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges that include factory default accounts.

  - **R5.2.1:** The policy includes the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords to be changed before putting any system into service.

  - **R5.2.2:** The Responsible Entity identifies those individuals with access to shared accounts.

  - **R5.2.3:** Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts that limits access to only users with authorization, an audit trail of the account use (automated or manual), and steps for securing the account if personnel changes (for example, change in assignment or termination).

- **R5.3:** At a minimum, the Responsible Entity is required to use passwords, subject to the following, as technically feasible:

  - **R5.3.1:** Each password must be a minimum of 6 characters.

  - **R5.3.2:** Each password must consist of a combination of alpha, numeric, and special characters.

  - **R5.3.3:** Each password must be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring

The Responsible Entity ensures that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

- **R6.1:** The Responsible Entity implements and documents the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

- **R6.2:** The security monitoring controls issue automated or manual alerts for detected cyber security incidents.
- **R6.3:** The Responsible Entity maintains logs of system events that are related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.
- **R6.4:** The Responsible Entity retains all logs that are specified in Requirement R6 for 90 days.
- **R6.5:** The Responsible Entity reviews logs of system events that are related to cyber security and maintain records that document the review of the logs.

R7. Disposal or Redeployment
The Responsible Entity establishes and implements formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.

- **R7.1:** Before the disposal of such assets, the Responsible Entity destroys or erases the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
- **R7.2:** Before redeployment of such assets, the Responsible Entity, at a minimum, erases the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

Standard CIP–007–5 — Cyber Security — Systems Security Management

R1: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R1 – Ports and Services. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.].*

- **R1.1:** Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.
- **R1.2:** Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.

R2: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R2 – Security Patch Management. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

- **R2.1:** A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.
- **R2.2:** At least once every 35 calendar days, the Responsible Entity evaluates for applicability security patches that have been released since the last evaluation from the source or sources identified in Part 2.1.
- **R2.3:** For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:
  - Apply the applicable patches; or
  - Create a dated mitigation plan; or
  - Revise an existing mitigation plan.

Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a time frame to complete each plan.

- **R2.4:** For each mitigation plan created or revised in Part 2.3, implement the plan within the time frame specified in the plan, unless a revision to the plan or an extension to the time frame specified in Part 2.3 is approved by the CIP Senior Manager or delegate.

R3: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R3 – Malicious Code Prevention. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

- **R3.1:** Deploy method(s) to deter, detect, or prevent malicious code.
- **R3.2:** Mitigate the threat of detected malicious code.
- **R3.3:** For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.

R4: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R4 – Security Event Monitoring. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.].*

- **R4.1:** Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:
  - **R4.1.1.** Detected successful login attempts;
  - **R4.1.2.** Detected failed access attempts and failed login attempts;
  - **R4.1.3.** Detected malicious code.
- **R4.2:** Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):
  - **R4.2.1.** Detected malicious code from Part 4.1; and
  - **R4.2.2.** Detected failure of Part 4.1 event logging.
- **R4.3:** Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.
- **R4.4:** Review a summary or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.

R5: Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R5 – System Access Controls. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

- **R5.1:** Have a method(s) to enforce authentication of interactive user access, where technically feasible.
- **R5.2:** Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).

- **R5.3:** Identify individuals who have authorized access to shared accounts.
- **R5.4:** Change known default passwords, per Cyber Asset capability.
- **R5.5:** For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:
  - **R5.5.1:** Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset;
  - **R5.5.2:** Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the Cyber Asset.
- **R5.6:** Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.
- **R5.7:** Where technically feasible, either:
  - Limit the number of unsuccessful authentication attempts; or
  - Generate alerts after a threshold of unsuccessful authentication attempts.

CIP–010–1 — Cyber Security — Configuration Change Management and Vulnerability Assessments

R1: The Responsible Entity implements, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts.

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&gt;Implements portions of PCI Section 8.2,
Check group definitions: Verifies the correctness of group definitions
and fixes the errors
</AIXPertDescription
<AIXPertPrereqList&gt;bos.rte.security,bos.rte.date,bos.rte.ILS</AIXPertPrereqList
<AIXPertCommand
/etc/security/aixpert/bin/execmds</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 10. PowerSC commands for AIX

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

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 11. PowerSC commands for the Virtual I/O Server

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

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 fileset. 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 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 Standard Edition version 1.1.4, or later, and it is not part of the base AIX operating system.

To install PowerSC Standard Edition, 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 Standard Edition 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
   - AIX Version 7.2, or later, with AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 7.2.0.0), or later

2. To update or install the PowerSC Standard Edition feature fileset, install the `powerscStd.rtc` fileset from the installation package for PowerSC Standard Edition version 1.1.4, or later.

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.

Related information:

/etc/security/rtc/rtcd.conf file format for real-time compliance

Trusted Boot

The Trusted Boot feature uses the Virtual Trusted Platform Module (VTPM), which is a virtual instance of the Trusted Computing Group's TPM. The VTPM is used to securely store measurements of the system boot for future verification.

Trusted Boot concepts

It is important to understand the integrity of the boot process and how to classify the boot as a trusted boot or a nontrusted boot.

You can configure a maximum of 60 VTPM-enabled logical partitions (LPAR) for each physical system by using the Hardware Management Console (HMC). When configured, the VTPM is unique to each LPAR. When used with the AIX Trusted Execution technology, the VTPM provides security and assurance to the following partitions:

- The boot image on the disk
- The entire operating system
- The application layers

An administrator can view trusted and nontrusted systems from a central console that is installed with the **openpts** verifier that is available on the AIX expansion pack. The **openpts** console manages one or more Power Systems servers, and monitors or attests the trusted state of AIX Profile Manager systems throughout the data center. Attestation is the process where the verifier determines (or attests) if a collector has performed a trusted boot.

Trusted boot status

A partition is said to be trusted if the verifier successfully attests the integrity of the collector. The verifier is the remote partition that determines if a collector has performed a trusted boot. The collector is the AIX partition that has a Virtual Trusted Platform Module (VTPM) attached and the Trusted Software Stack (TSS) installed. It indicates that the measurements that are recorded within the VTPM match a reference set held by the verifier. A trusted boot state indicates whether the partition booted in a trusted manner. This statement is about the integrity of the system boot process and does not indicate the current or ongoing level of the security of the system.

Nontrusted boot status

A partition enters a nontrusted state if the verifier cannot successfully attest the integrity of the boot process. The nontrusted state indicates that some aspect of the boot process is inconsistent with the reference information held by the verifier. The possible causes for a failed attestation include booting from a different boot device, booting a different kernel image, and changing the existing boot image.

Related concepts:

"Troubleshooting Trusted Boot" on page 111
There are some of the common scenarios and remedial steps that are required to help identify the reason for attestation failure when using Trusted Boot.

Planning for Trusted Boot

Learn about the hardware and software configurations that are required to install Trusted Boot.

Trusted Boot prerequisites

The installation of Trusted Boot involves configuring the collector and the verifier.

When you prepare to reinstall the AIX operating system on a system with Trusted Boot already installed, you must copy the /var/tss/lib/tpm/system.data file and use it to overwrite the file in the same location after the reinstallation completes. If you do not copy this file, you must remove the virtualized Trusted Platform Module from the management console and reinstall it on the partition.

Collector

The configuration requirements to install a collector involves the following prerequisites:
- POWER7 hardware that is running on a 740 firmware release.
- Install IBM AIX 6 with Technology Level 7 or install IBM AIX 7 with Technology Level 1.
- Install Hardware Management Console (HMC) version 7.4 or later.
- Configure the partition with the VTPM and a minimum of 1 GB memory.
- Install Secure Shell (SSH), specifically OpenSSH or equivalent.

Verifier

The **openpts** verifier can be accessed from the command-line interface and the graphical user interface that is designed to run on a range of platforms. The AIX version of the OpenPTS verifier is available on the AIX expansion pack. The versions of OpenPTS verifier for Linux and other platforms are available through a web download. The configuration requirements include the following prerequisites:
- Install SSH, specifically OpenSSH or equivalent.
- Establish network connectivity (through SSH) to the collector.
- Install Java™ 1.6 or later to access the **openpts** console from the graphical interface.

Preparing for remediation

The Trusted Boot information that is described here serves as a guide to identifying situations that might require remediation. It does not affect the boot process.

There are many circumstances that can cause an attestation to fail, and it is difficult to predict the circumstance you might encounter. You must decide on the appropriate action depending on the circumstance. However, it is good practice to prepare for some of the severe scenarios and have a policy or a workflow to help you to handle such incidents. Remediation is the corrective action that must be taken when attestation reports one or more collectors are not trusted.

For example, if an attestation failure occurred due to the boot image differing from the verifier's reference, consider having answers to the following questions:
- How can you verify that the threat is credible?
- Was there any planned maintenance that was carried out, an AIX upgrade, or new hardware that was recently installed?
- Can you contact the administrator who has access to this information?
- When was the system last booted in a trusted state?
- If the security threat looks legitimate, what action must you take? (Suggestions include collecting audit logs, disconnecting the system from the network, powering the system off, and alerting users).
- Were there any other systems compromised that must be checked?

Related concepts:
"Troubleshooting Trusted Boot" on page 111
There are some of the common scenarios and remedial steps that are required to help identify the reason for attestation failure when using Trusted Boot.

Migration considerations

Consider these prerequisites before you migrate a partition that is enabled for virtual trusted platform module (VTPM).

An advantage of a VTPM over a physical TPM is that it allows the partition to move between systems while retaining the VTPM. To securely migrate the logical partition, the firmware encrypts the VTPM data before transmission. To ensure a secure migration, the following security measures must be implemented before migration:

- Enable IPSEC between the Virtual I/O Server (VIOS) that is performing the migration.
- Set the trusted system key through the Hardware Management Console (HMC) to control the managed systems that are capable of decrypting the VTPM data after migration. The migration destination system must have the same key as that of the source system to successfully migrate the data.

Related information:

➡ Using HMC

➡ VIOS migration

Installing Trusted Boot

There are some required hardware and software configurations that are required to install Trusted Boot.

Related information:

"Installing PowerSC Standard Edition 1.1.5" on page 7
You must install a fileset for each specific function of PowerSC Standard Edition.

Installing the collector

You must install the collector by using the fileset from the AIX base CD.

To install the collector, install the `powerscStd.vtpm` and `openpts.collector` packages which are on the base CD, by using the **smit** or **installp** command.

Installing the verifier

The OpenPTS verifier component runs on the AIX operating system and on other platforms.

The AIX version of the verifier can be installed from the fileset by using the AIX expansion pack. To install the verifier on the AIX operating system, install the `openpts.verifier` package from the AIX expansion pack by using the **smit** or **installp** command. This installs both the command line and graphical interface versions of the verifier.

The OpenPTS verifier for other operating systems can be downloaded from `Download Linux OpenPTS Verifier For Use With AIX Trusted Boot`.

Related information:

➡ Download Linux OpenPTS Verifier For Use With AIX Trusted Boot

Configuring Trusted Boot

Learn the procedure to enroll a system and to attest a system for Trusted Boot.

Enrolling a system

Learn the procedure to enroll a system with the verifier.

Enrolling a system is the process of providing an initial set of measurements to the verifier, which forms the basis for subsequent attestation requests. To enroll a system from the command line, use the following command from the verifier:

```
openpts -i <hostname>
```

Information about the enrolled partition is located in the $HOME/.openpts directory. Each new partition is assigned with a unique identifier during the enrollment process and information related to the enrolled partitions is stored in the directory corresponding to the unique ID.

To enroll a system from the graphical interface, complete the following steps:

1. Launch the graphical interface by using **/opt/ibm/openpts_gui/openpts_GUI.sh** command.
2. Select **Enroll** from the navigation menu.
3. Enter the host name and the SSH credentials of the system.
4. Click **Enroll**.

Related concepts:

"Attesting a system"
Learn the procedure to attest a system from the command-line and by using the graphical interface.

Attesting a system

Learn the procedure to attest a system from the command-line and by using the graphical interface.

To query the integrity of a system boot, use the following command from the verifier:

```
openpts <hostname>
```

To attest a system from the graphical interface, complete the following steps:

1. Select a category from the navigation menu.
2. Select one or more systems to attest.
3. Click **Attest**.

Enrolling and attesting a system without a password

The attestation request is sent through the Secure Shell (SSH). Install the verifier's certificate on the collector to permit SSH connections without a password.

To set up the verifier's certificate on the collector's system, complete the following steps :

- On the verifier, run the following commands:
  ```
  ssh-keygen     # No passphrase
  scp ~/.ssh/id_rsa.pub <collector>:/tmp
  ```
- On the collector, run the following command:
  ```
  cat /tmp/id_rsa.pub >> ~/.ssh/authorized_keys
  ```

Managing Trusted Boot

Learn the procedure to manage the attestation results of Trusted Boot.

Interpreting attestation results

Learn the procedure to view and understand the attestation results.

An attestation can result in one of following states:

1. Attestation request failed: The attestation request did not complete successfully. See the Troubleshooting section to understand the possible causes for the failure.

2. System integrity valid: The attestation completed successfully, and the system boot matches the reference information that is held by the verifier. This indicates a successful Trusted Boot.

3. System integrity invalid: The attestation request completed, but a discrepancy was detected between the information that is collected during system boot and the reference information that is held by the verifier. This indicates a nontrusted boot.

The attestation also reports whether an update was applied to the collector by using the following message:

System update available: This message indicates that an update was applied on the collector and a set of updated reference information is available that is effective for the next boot. The user is prompted on the verifier to accept or reject the updates. For example, the user can choose to accept these updates if the user is aware of the maintenance occurring on the collector.

To investigate an attestation failure by using the graphical interface, complete the following steps:

1. Select a category from the navigation menu.

2. Select a system to investigate.

3. Double-click the entry corresponding to the system. A properties window is displayed. This window contains log information about the failed attestation.

Deleting systems

Learn the procedure to delete a system from the verifier's database.

To remove a system from the database of the verifier, run the following command:

```
openpts -r <hostname>
```

Troubleshooting Trusted Boot

There are some of the common scenarios and remedial steps that are required to help identify the reason for attestation failure when using Trusted Boot.

The **openpts** command declares a system as invalid if the current boot state of the system does not match the reference information that is held on the verifier. The **openpts** command determines the possible reason for the integrity to be invalid. There are several variables in a full AIX boot, and a failed attestation requires analysis to determine the cause of the failure.

The following table lists some of the common scenarios and remedial steps to identify the reason for the failure:

Table 12. Troubleshooting some of the common scenarios for failure

Reason for failure	Possible causes of failure	Suggested remediation

Attestation did not complete.	• Incorrect host name.
	• No network route between the source and destination.
	• Incorrect security credentials.
		Check the Secure Shell (SSH) connection using the following command:
		`ssh ptsc@hostname`
		
		If the SSH connection is successful, then check for the following reasons for attestation failure:
		• The system that is being attested is not running the **tcsd** daemon.
		• The system that is being attested was not initialized by the **ptsc** command. This process should occur automatically during the system startup but check for the presence of a `/var/ptsc/` directory on the collector. If the `/var/ptsc/` directory does not exist, run the following command on the collector:
		`ptsc -i`

Table 12. Troubleshooting some of the common scenarios for failure (continued)

Reason for failure	Possible causes of failure	Suggested remediation
The CEC firmware was changed.	• A firmware upgrade was applied. • The LPAR was migrated to a system that was running a different version of the firmware.	Check the firmware level of the system that is hosting the LPAR.
The resources allocated to the LPAR changed.	The CPU or memory allocated to the LPAR changed.	Check the partition profile in the HMC.
The firmware changed for the adapters that are available in the LPAR.	A hardware device was added or removed from the LPAR.	Check the partition profile in the HMC.
The list of devices attached to the LPAR was changed.	A hardware device was added or removed from the LPAR.	Check the partition profile in the HMC.
The boot image changed, which includes the operating system kernel.	• An AIX update was applied and the verifier was unaware of the update. • The **bosboot** command was run.	• Confirm with the administrator of the collector whether any maintenance was performed before the latest reboot operation. • Check the logs on the collector for maintenance activity.
The LPAR is booted from a different device.	• Enrollment was carried out immediately after network installation. • The system is booted from a maintenance device.	The boot device and flags can be checked by using the **bootinfo** command. If enrollment was carried out immediately after Network Installation Management (NIM) installation and before the reboot operation, the enrolled details pertain to the network installation and not to the next disk boot. This enrollment can be repaired by removing the enrollment and re-enrolling the logical partition.
The interactive System Management Services (SMS) boot menu was called.		The boot process must run uninterrupted without user interaction for a system to be trusted. Entering the SMS boot menu causes the boot to be invalid.
The trusted execution (TE) database was altered.	• Binary files were added or removed from the TE database. • Binary files in the database were updated.	Run the **trustchk** command to verify the database.

Related concepts:

"Preparing for remediation" on page 108
The Trusted Boot information that is described here serves as a guide to identifying situations that might require remediation. It does not affect the boot process.

"Trusted Boot concepts" on page 107
It is important to understand the integrity of the boot process and how to classify the boot as a trusted boot or a nontrusted boot.

Related information:

➡ Using HMC

Trusted Firewall

The Trusted Firewall feature provides virtualization-layer security that improves performance and resource efficiency when communicating between different virtual LAN (VLAN) security zones on the same Power Systems server. Trusted Firewall decreases the load on the external network by moving the filtering capability of firewall packets meeting specified rules to the virtualization layer. This filtering capability is controlled by easily defined network filter rules, which allow trusted network traffic to cross between VLAN security zones without leaving the virtual environment. Trusted Firewall protects and routes internal network traffic between the AIX, IBM i, and Linux operating systems.

Trusted Firewall concepts

There are some basic concepts to understand when using Trusted Firewall.

Power Systems hardware can be configured with multiple virtual LAN (VLAN) security zones. A user-configured policy, created as a Trusted Firewall filter rule, permits some trusted network traffic to cross VLAN security zones and remain internal to the virtualization layer. This is similar to introducing a network-attached physical firewall into the virtualized environment, which provides a more performance-efficient method of implementing firewall capabilities for virtualized data centers.

With Trusted Firewall, you can configure rules to allow certain types of traffic to transfer directly from one VLAN on a Virtual I/O Server (VIOS) to another VLAN on the same VIOS, while still maintaining a high level of security by limiting other types of traffic. It is a configurable firewall within the virtualization layer of Power Systems servers.

Using the example in Figure 1 on page 114, the goal is to be able to transfer information securely and efficiently from LPAR1 on VLAN 200 and from LPAR2 on VLAN 100. Without Trusted Firewall, information targeted for LPAR2 from LPAR1 is sent out of the internal network to the router, which routes the information back to LPAR2.
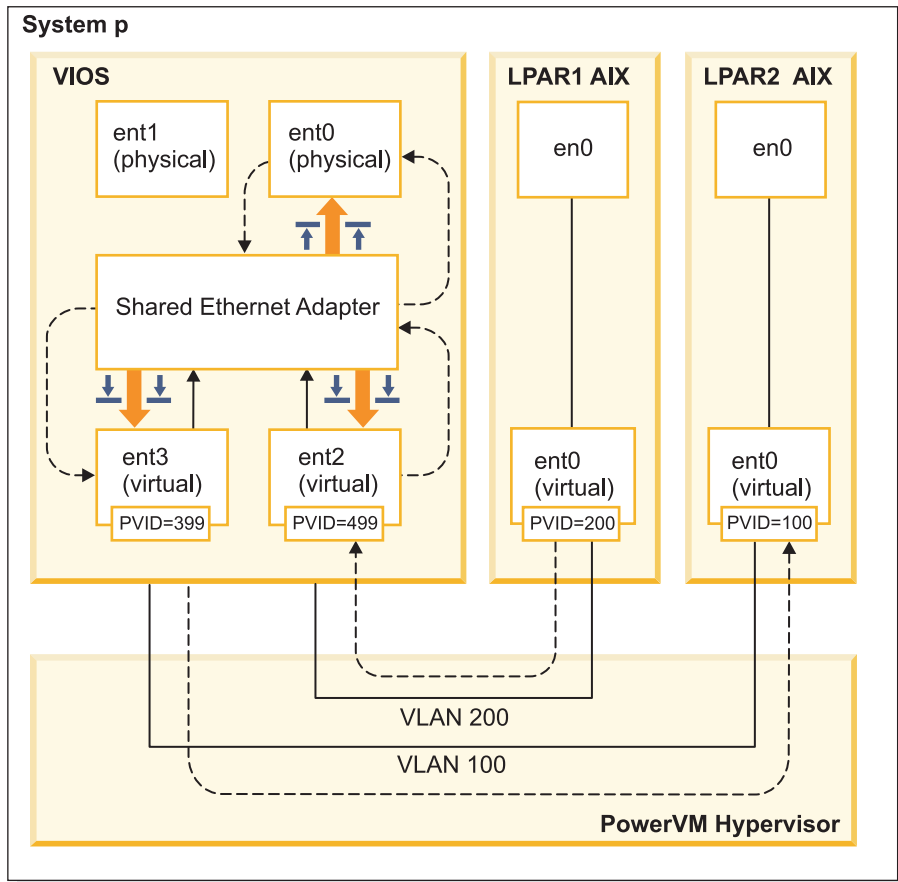
Figure 1. Example of cross-VLAN information transfer without Trusted Firewall

Using Trusted Firewall, you can configure rules to allow the information to pass from LPAR1 to LPAR2 without leaving the internal network. This path is shown in Figure 2 on page 115.
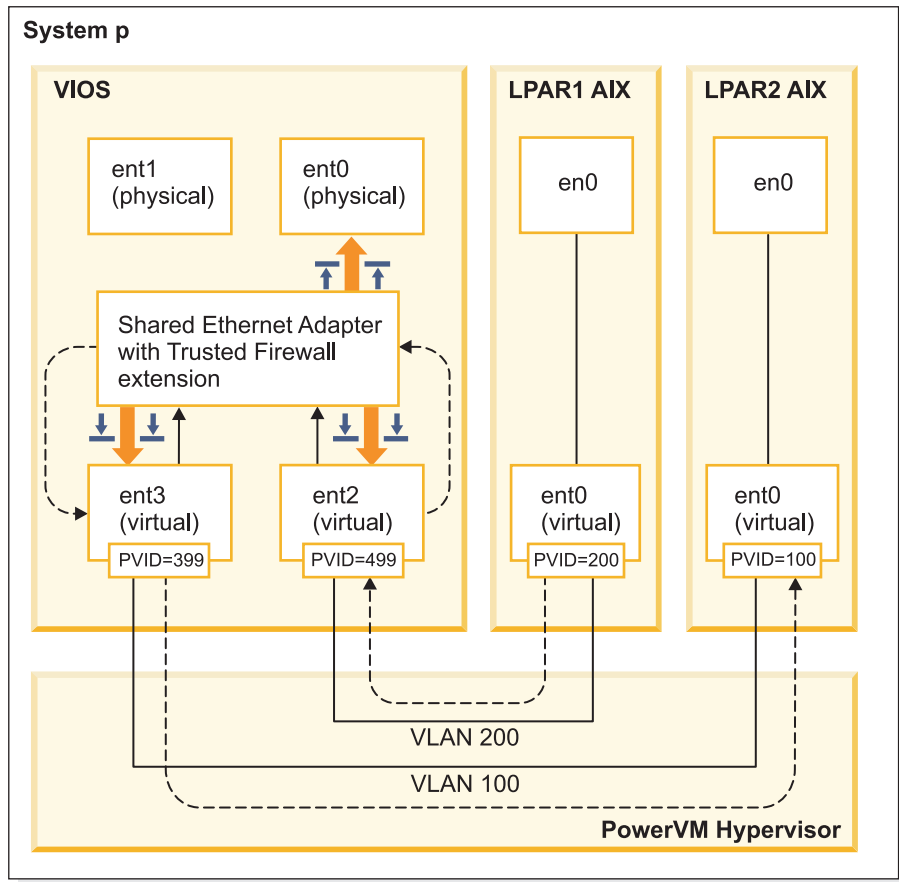
Figure 2. Example of cross-VLAN information transfer with Trusted Firewall

Configuration rules that allow certain information to pass securely across VLANs shorten the path to its destination. The Trusted Firewall uses the Shared Ethernet Adapter (SEA) and the Security Virtual Machine (SVM) kernel extension to enable the communication.

Shared Ethernet Adapter
   The SEA is where the routing begins and ends. When the SVM is registered, the SEA receives the packets and forwards them to the SVM. If the SVM determines that the packet is for an LPAR on the same Power Systems server, it updates the packet's layer 2 header. The packet is returned to the SEA for forwarding to the final destination either within the system or on the external network.

Security Virtual Machine
   The SVM is where the filtering rules are applied. The filtering rules are necessary to maintain security on the internal network. After registering the SVM with the SEA, the packets are forwarded to the SVM before being sent to the external network. Based on the active filter rules, the SVM determines whether a packet stays in the internal network or moves to the external network.

Installing Trusted Firewall

Installing the PowerSC Trusted Firewall is similar to installing other PowerSC features.

Prerequisites:
- PowerSC versions prior to 1.1.1.0 did not have the required fileset to install Trusted Firewall. Ensure that you have the PowerSC installation CD for version 1.1.1.0, or later.

- To take advantage of Trusted Firewall, you must have already used the Hardware Management Console (HMC) or Virtual I/O Server (VIOS) to configure your Virtual LANs (VLANs).

Trusted Firewall is provided as an additional fileset on the PowerSC Standard Edition installation CD. The file name is `powerscStd.svm.rte`. You can add the Trusted Firewall to an existing instance of PowerSC Version 1.1.0.0, or later, or install it as part of a new installation of PowerSC Version 1.1.1.0, or later.

To add the Trusted Firewall function to an existing PowerSC instance:
1. Ensure that you are running VIOS Version 2.2.1.4, or later.
2. Insert the PowerSC installation CD for version 1.1.1.0 or download the image of the installation CD.
3. Use the **oem_setup_env** command for root access.
4. Use the **installp** command or the SMIT tool to install the `PowerscStd.svm.rte` fileset.

Related information:
"Installing PowerSC Standard Edition 1.1.5" on page 7
You must install a fileset for each specific function of PowerSC Standard Edition.

Configuring Trusted Firewall

Additional configuration settings are required for the Trusted Firewall feature after it is installed.

Trusted Firewall Advisor

Trusted Firewall Advisor analyzes system traffic from different logical partitions (LPARs) to provide information for determining whether running Trusted Firewall improves system performance.

If the Trusted Firewall Advisor function records a significant amount of traffic from different virtual LANs (VLANs) that are on the same central electronics complex, enabling Trusted Firewall should benefit your system.

To enable Trusted Firewall Advisor, enter the following command:

```
vlantfw -m
```

To display the results of Trusted Firewall Advisor, enter the following command:

```
vlantfw -D
```

To disable Trusted Firewall Advisor, enter the following command:

```
vlantfw -M
```

Trusted Firewall logging

Trusted Firewall logging compiles a list of network traffic paths within the central electronics complex. The list shows the filters that Trusted Firewall uses to route traffic.

When Trusted Firewall Advisor determines that routing the traffic internally improves efficiency, Trusted Firewall logging maintains a list of paths in the `svm.log` file. The size of the `svm.log` file is limited to 16 MB. If the entries exceed the 16 MB limit, the oldest entries are removed from the log file.

To start Trusted Firewall logging, enter the following command:

```
vlantfw -l
```

To stop Trusted Firewall logging, enter the following command:

```
vlantfw -L
```

You can view the log file at the following location: `/home/padmin/svm/svm.log`.

Note: You can run the commands to start and stop Trusted Firewall logging only when you are authenticated as a root user.

Multiple Shared Ethernet Adapters

You can configure Trusted Firewall on systems that use multiple Shared Ethernet Adapters.

Some configurations use multiple Shared Ethernet Adapters (SEAs) on the same Virtual I/O Server (VIOS). Multiple SEAs can provide benefits of failover protection and resource leveling. Trusted Firewall supports routing across multiple SEAs, provided they are on the same VIOS.

Figure 3 shows an environment using multiple SEAs.
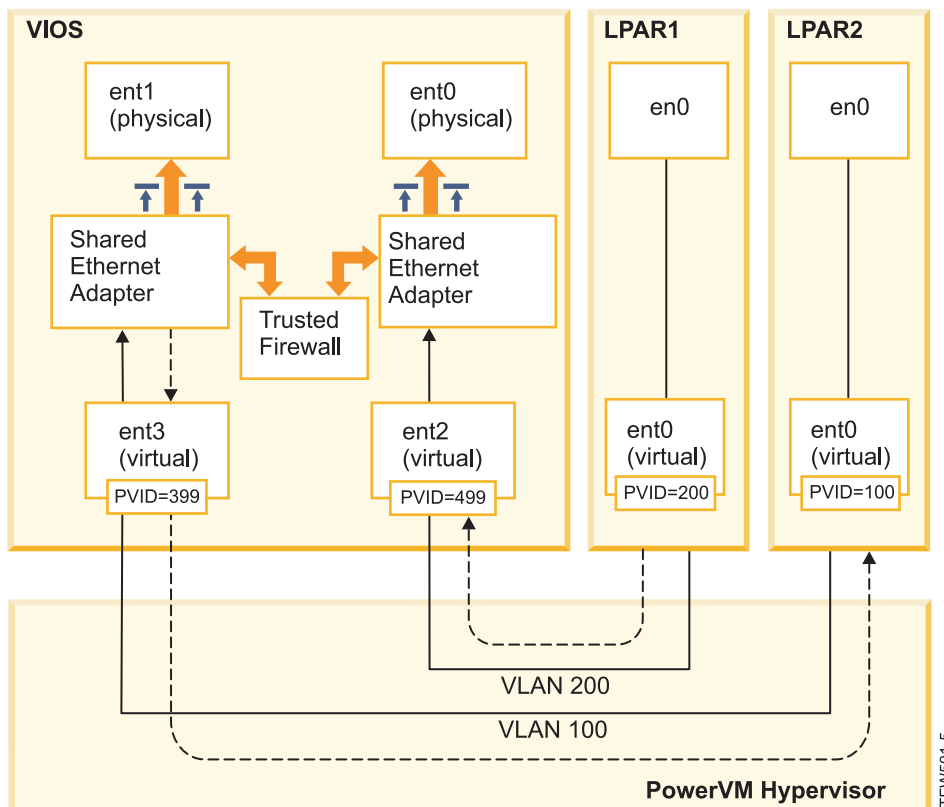
Figure 3. Configuration using multiple Shared Ethernet Adapters on a single VIOS

The following are examples of multiple SEA configurations that are supported by Trusted Firewall:
- The SEAs are configured with trunk adapters on the same Power® hypervisor virtual switch. This configuration is supported because each SEA receives network traffic with different VLAN IDs.
- The SEAs are configured with trunk adapters on different Power hypervisor virtual switches, and each trunk adapter is on a different VLAN ID. In this configuration, each SEA still receives network traffic by using different VLAN IDs.
- The SEAs are configured with trunk adapters on different Power hypervisor virtual switches, and the same VLAN IDs are reused on the virtual switches. In this case, the traffic for both SEAs has the same VLAN IDs.

  An example of this configuration is having LPAR2 on VLAN200 with virtual switch 10 and LPAR3 on VLAN200 with virtual switch 20. Because both LPARs and their corresponding SEAs use the same VLAN ID (VLAN200), both of the SEAs have access to the packets with that VLAN ID.

You cannot enable bridging on more than one VIOS. For this reason, the following multiple SEA configurations are not supported by Trusted Firewall:
- Multiple VIOS and multiple SEA drivers.
- Redundant SEA load sharing: Trunk adapters that are configured for inter-VLAN routing cannot be split between VIOS servers.

Removing Shared Ethernet Adapters

The steps to remove Shared Ethernet Adapter devices from the system must be performed in a specific order.

To remove a Shared Ethernet Adapter (SEA) from your system, complete the following steps:
1. Remove the Security Virtual Machine that is associated with the SEA by entering the following command:

   ```
   rmdev -dev svm
   ```
2. Remove the SEA by entering the following command:

   ```
   rmdev -dev shared ethernet adapter ID
   ```

Note: Removing the SEA before removing the SVM can result in system failure.

Creating rules

You can create rules to enable Trusted Firewall cross-VLAN routing.

To enable the routing features of Trusted Firewall, you must create rules specifying which communications are allowed. For enhanced security, there is no single rule that allows communication between all of the VLANs on the system. Each allowed connection requires its own rule, though each rule that is activated allows communication in both directions for its specified endpoints.

Because the rule creation is created in the Virtual I/O Server (VIOS) interface, additional information about the commands is available in the VIOS topic collection in the Power Systems Hardware Information Center.

To create a rule, complete the following steps:
1. Open the VIOS command-line interface.
2. Initialize the SVM driver by entering the following command:

   ```
   mksvm
   ```
3. Start Trusted Firewall by entering the start command:

   ```
   vlantfw -s
   ```
4. To display all known LPAR IP and MAC addresses, enter the following command:

   ```
   vlantfw -d
   ```

   You will need the IP and MAC addresses of the logical partitions (LPARs) for which you are creating rules.
5. Create the filter rule to allow communication between the two LPARs (LPAR1 and LPAR2) by entering one of the following commands (commands should be entered on one line):

   ```
   genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress]
        -d [lpar2ipaddress]
   ```

   ```
   genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d
        [lpar2ipaddress]-o any -p 0 -O gt -P 23
   ```

   Note: One filter rule allows communication in both directions by default, depending on port and protocol entries. For example, you can enable Telnet for LPAR1 to LPAR2 by running the following command:

```
genvfilt -v4 -a-P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d
    [lpar2ipaddress] -o any -p 0 -O eq -P 23
```

6. Activate all of the filter rules in the kernel by entering the following command:
   ```
   mkvfilt -u
   ```

Note: This procedure activates this rule and any other filtering rules that exist on the system.

Additional examples

The following examples show some other filter rules that you can create by using Trusted Firewall.
- To allow Secure Shell communication from the LPAR on VLAN 100 to the LPAR on VLAN 200, enter the following command:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -o any -p 0 -O eq -P 22 -c tcp
  ```
- To allow traffic between all of the ports 0 - 499, enter the following command:
  ```
  genvfilt -v4 -a P -z 100 -z 200 -o lt -p 500 -O lt -P 500 -c tcp
  ```
- To allow all TCP traffic between the LPARs, enter the following command:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c tcp
  ```

  If you do not specify any ports or port operations, the traffic can use all ports.
- To allow Internet Control Message Protocol messaging between LPARs, enter the following command:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c icmp
  ```

Related concepts:

"Deactivating rules"
You can deactivate rules that enable cross-VLAN routing in the Trusted Firewall feature.

Related reference:

"genvfilt command" on page 152

"mkvfilt command" on page 154

"vlantfw command" on page 170

Related information:

➜ Virtual I/O Server (VIOS)

Deactivating rules

You can deactivate rules that enable cross-VLAN routing in the Trusted Firewall feature.

Because the rules are deactivated in the Virtual I/O Server (VIOS) interface, additional information about the commands and process are available in the VIOS topic collection in the Power Systems Hardware Information Center.

To deactivate a rule, complete the following steps:
1. Open the VIOS command-line interface.
2. To display all active filter rules, enter the following command:
   ```
   lsvfilt -a
   ```

   You can omit the **-a** flag to display all of the filter rules stored in the Object Data Manager.
3. Note the identification number for the filter rule that you are deactivating. For this example, the identification number of the filter rule is 23.
4. Deactivate filter rule 23 when it is active in the kernel by entering the following command:
   ```
   rmvfilt -n 23
   ```

   To deactivate all of the filter rules in the kernel, enter the following command:

```
rmvfilt -n all
```

Related concepts:

"Creating rules" on page 118
You can create rules to enable Trusted Firewall cross-VLAN routing.

Related reference:

"lsvfilt command" on page 153
"rmvfilt command" on page 169

Trusted Logging

PowerVM® Trusted Logging lets AIX logical partitions (LPARs) write to log files that are stored on an attached Virtual I/O Server (VIOS). Data is transmitted to the VIOS directly through the hypervisor, and network connectivity is not required between the client LPAR and the VIOS.

Virtual logs

The Virtual I/O Server (VIOS) administrator creates and manages the log files, and they are presented to the AIX operating system as virtual log devices in the /dev directory, similar to the virtual disks or virtual optical media.

Storing log files as virtual logs increases the level of trust in the records because they cannot be changed by a user with root privileges on the client LPAR where they were generated. Multiple virtual log devices can be attached to the same client LPAR and each log is a different file in the /dev directory.

Trusted Logging lets log data from multiple client LPARs be consolidated into a single file system, which is accessible from the VIOS. Therefore, the VIOS provides a single location on the system for log analysis and archival. The client LPAR administrator can configure applications and the AIX operating system to write data to the virtual log devices, which is similar to writing data to the local files. The AIX Audit subsystem can be configured to direct the audit records to virtual logs, and other AIX services, such as syslog, work with their existing configuration to direct data to virtual logs.

To configure the virtual log, the VIOS administrator must specify a name for the virtual log, which has the following separate components:
- Client name
- Log name

The names of the two components can be set by the VIOS administrator to any value, but the client name is typically the same for all virtual logs that are attached to a given LPAR (for example, the host name of the LPAR). The log name is used to identify the purpose of the log (for example, audit or syslog).

On an AIX LPAR, each virtual log device is present as two functionally equivalent files in the /dev file system. The first file is named after the device, for example, /dev/vlog0, and the second file is named by concatenating a vl prefix with the log name and the device number. For example, if the virtual log device vlog0 has audit as the log name, it is present in the /dev file system as both vlog0 and vlaudit0.

Related information:

➡ Creating virtual logs

Detecting virtual log devices

After a VIOS administrator has created virtual log devices and attached them to a client LPAR, the client LPAR device configuration must be refreshed for the devices to be visible.

The client LPAR administrator refreshes the settings by using one of the following methods:
- Rebooting the client LPAR
- Running the **cfgmgr** command

Run the **lsdev** command to display the virtual log devices. The devices are prefixed with vlog by default. An example of the **lsdev** command output on an AIX LPAR on which two virtual logs devices are present is as follows:

```
lsdev
vlog0  Virtual Log Device
vlog1  Virtual Log Device
```

Inspect the properties of an individual virtual log device by using the `lsattr –El` *<device name>*
command, which produces output that is similar to the following :

```
lsattr –El vlog0
PCM                           Path Control Module         False
client_name    dev-lpar-05 Client Name                    False
device_name    vlsyslog0   Device Name                    False
log_name       syslog      Log Name                       False
max_log_size   4194304     Maximum Size of Log Data File  False
max_state_size 2097152     Maximum Size of Log State File False
pvid           none        Physical Volume Identifier     False
```

This output displays the client name, device name, and the amount of log data that VIOS can store.

The virtual log stores two types of log data, which are:

- Log data: The raw log data generated by applications on the AIX LPAR.
- State data: Information about when the devices were configured, opened, closed, and other operations
  that are used to analyze log activity.

The VIOS administrator specifies the amount of **log data** and **state data** that can be stored for each
virtual log, and the amount is indicated by the `max_log_size`, and `max_state_size` attributes. When the
amount of stored data exceeds the specified limit, the earliest log data is overwritten. The VIOS
administrator must ensure that the log data is collected and archived frequently to preserve the logs.

Installing Trusted Logging

You can install the PowerSC Trusted Logging feature by using the command line interface or the SMIT
tool.

The prerequisites for installing Trusted Logging are VIOS 2.2.1.0, or later, and IBM AIX 6 with Technology
Level 7 or IBM AIX 7 with Technology Level 1.

The file name for installing the Trusted Logging feature is `powerscStd.vlog`, which is included on the
PowerSC Standard Edition installation CD.

To install the Trusted Logging function:

1. Ensure that you are running VIOS Version 2.2.1.0, or later.
2. Insert the PowerSC installation CD or download the image of the installation CD.
3. Use the **installp** command or the SMIT tool to install the `powerscStd.vlog` fileset.

Related information:

You must install a fileset for each specific function of PowerSC Standard Edition.

Configuring Trusted Logging

Learn the procedure to configure Trusted Logging on the AIX Audit subsystem, and syslog.

Configuring the AIX Audit subsystem

The AIX Audit subsystem can be configured to write binary data to a virtual log device in addition to
writing logs to the local file system.

Note: Before you configure the AIX Audit subsystem, you must complete the procedure in "Detecting virtual log devices" on page 121.

To configure the AIX Audit subsystem, complete the following steps:

1. Configure the AIX Audit subsystem to log data in binary (`auditbin`) mode.
2. Activate Trusted Logging for AIX auditing by editing the `/etc/security/audit/config` configuration file.
3. Add a `virtual_log = /dev/vlog0` parameter to `bin:` stanza.

   Note: The instruction is valid if the LPAR administrator wants `auditbin` data to be written to the `/dev/vlog0`.
4. Restart the AIX Audit subsystem in the following sequence:
   ```
   audit shutdown
   audit start
   ```

The audit records are written to Virtual I/O Server (VIOS) through the specified virtual log device in addition to writing logs to the local file system. The logs are stored under control of the existing `bin1` and `bin2` parameters in the `bin:` stanza of the `/etc/security/audit/config` configuration file.

Related information:

Auditing subsystem

Configuring syslog

Syslog can be configured to write messages to virtual logs by adding rules to the `/etc/syslog.conf` file.

Note: Before you configure the `/etc/syslog.conf` file, you must complete the procedure in "Detecting virtual log devices" on page 121.

You can edit the `/etc/syslog.conf` file to match the log messages, which are based on the following criteria:

* Facility
* Priority level

To use the virtual logs for syslog messages, the `/etc/syslog.conf` file must be configured with rules to write the desired messages to the appropriate virtual log in the `/dev` directory.

For example, to send debug-level messages that are generated by any facility to the `vlog0` virtual log, add the following line to the `/etc/syslog.conf` file:

```
*.debug /dev/vlog0
```

Note: Do not use the log rotation facilities that are available in the `syslogd` daemon for any command that writes data to virtual logs. The files in the `/dev` file system are not regular files and they cannot be renamed and moved. The VIOS administrator must configure virtual log rotation within the VIOS.

The `syslogd` daemon must be restarted after the configuration by using the following command:

```
refresh -s syslogd
```

Related information:

syslogd Daemon

Writing data to virtual log devices

Arbitrary data is written to a virtual log device by opening the appropriate file in the `/dev` directory and writing data to the file. A virtual log can be opened by one process at a time.

For example:

To write messages to the virtual log devices by using the **echo** command, enter the following command:
```
 echo "Log Message" > /dev/vlog0
```

To store files to the virtual log devices by using the **cat** command, enter the following command:
```
cat /etc/passwd > /dev/vlog0
```

The maximum individual write size is limited to 32 KB, and programs that attempt to write more data in a single write operation receive an I/O (EIO) error. The command-line interface (CLI) utilities, such as the **cat** command, automatically break up the transfers into 32 KB write operations.

Trusted Network Connect and Patch management

Trusted Network Connect (TNC) is part of the trusted computing group (TCG) that provides specifications to verify the end-point integrity. TNC has defined open solution architecture that helps administrators enforce policies to effectively control access to the network infrastructure.

Trusted Network Connect concepts

Learn about the components, configuring secure communication, and the patch management system of the Trusted Network Connect (TNC).

Trusted Network Connect components

Learn about the components of the Trusted Network Connect (TNC) framework.

The TNC model consists of the following components:

Trusted Network Connect server

The Trusted Network Connect (TNC) server identifies the clients that are added to the network and initiates a verification on them.

The TNC client provides the required fileset level information to the server for verification. The server determines whether the client is at the level that is configured by the administrator. If the client is not compliant, the TNC server notifies the administrator about the remediation that is required.

The TNC server initiates verifications on the clients that are trying to access the network. The TNC server loads a set of integrity measurement verifiers (IMVs) that can request the integrity measurements from clients and verify them. AIX has a default IMV, which verifies the fileset and security patch level of the systems. The TNC server is a framework which loads and manages multiple IMV modules. For verifying a client, it relies on the IMVs to request information from clients and verifies the clients.

Patch management

The Trusted Network Connect (TNC) server integrates with the SUMA to provide a patch management solution.

The AIX SUMA downloads the latest service packs and security fixes available in the IBM ECC and Fix Central. The TNC and patch management daemon pushes the latest updated information to the TNC server, which serves as a baseline fileset to verify the clients.

The **tncpmd** daemon must be configured to manage Service Update Management Assistant (SUMA) downloads and to push fileset information to the TNC server. This daemon must be hosted on a system that is connected to the Internet to be able to download the updates automatically. To use the TNC patch management server without connecting it to the Internet, you can register a user-defined fix repository with the TNC patch management server.

Note: The TNC server and the **tncpmd** daemon can be hosted on the same system.

Trusted Network Connect client

The Trusted Network Connect (TNC) client provides the information that is required by the TNC server for verification.

The server determines whether the client is at the level configured by the administrator. If the client is not compliant, the TNC server notifies the administrator about the updates that are required.

The TNC client loads the IMCs on startup and uses the IMCs to gather the required information.

Trusted Network Connect IP referrer

The Trusted Network Connect (TNC) server can automatically initiate the verification on clients that are part of the network. The IP referrer running on Virtual I/O Server (VIOS) partition detects the new clients that are serviced by the VIOS and sends their IP addresses to the TNC server. The TNC server verifies the client regarding the policy that is defined.

Trusted Network Connect secure communication

The Trusted Network Connect (TNC) daemons communicate over the encrypted channels that are enabled by Transport Layer Security (TLS) or Secure Sockets Layer (SSL).

The secure communication is to ensure that the data and commands that flow in the network are authenticated and secure. Each system must have its own key and certificate, which are generated when the initialization command for the components is run. This process is completely transparent to the administrator and requires less involvement from the administrator.

To verify a new client, the certificate of the client must be imported into the database of the server. The certificate is marked as untrusted initially, and then the administrator uses the **psconf** command to view and mark the certificates as trusted by entering the following command:

```
psconf certadd —i<ip> -t<TRUSTED|UNTRUSTED>
```

To use a different key and certificate, the **psconf** command provides the option to import the certificate.

To import the certificate from the server, enter the following command:

```
psconf import  -S -k<key filename> -f<key filename>
```

To import the certificate from the client, enter the following command:

```
psconf import -C -k<key filename> -f<key filename>
```

Trusted Network Connect protocol

The Trusted Network Connect (TNC) protocol is used with the TNC framework to maintain network integrity.

TNC provides specifications to verify the end-point integrity. The end-points that request access are assessed based on the integrity measurements of critical components that can affect its operational environment. The TNC framework enables administrators to monitor the integrity of the systems in the network. The TNC is integrated with the AIX patch distribution infrastructure to build a complete patch management solution.

TNC specifications must satisfy the requirements of AIX and POWER® family system architecture. The components of TNC are designed to provide a complete patch management solution on the AIX operating system. This configuration enables administrators to efficiently manage the software configuration on AIX deployments. It provides tools to verify the patch levels of the systems and generate a report on the clients that are not compliant. Additionally, patch management simplifies the process of downloading the patches and installing them.

IMC and IMV modules

The Trusted Network Connect (TNC) server or client internally use the integrity measurement collector (IMC) and integrity measurement verifier (IMV) modules for server verification.

This framework allows loading of multiple IMC and IMV modules into the server and clients. The module that performs the operating system (OS) and fileset level verification is shipped with the AIX operating system by default. To access the modules that are shipped with the AIX operating system, use one of the following paths:

* `/usr/lib/security/tnc/libfileset_imc.a`: Collects the OS level and information about the fileset that is installed from the client system and sends it to the IMV (TNC server) for verification.
* `/usr/lib/security/tnc/libfileset_imv.a`: Requests the OS level and fileset information from the client and compares it with the baseline information. It also updates the status of the client into the database of the TNC server. To view the status, enter the following command:

  ```
  psconf list -s<COMPLIANT|IGNORE|FAILED|ALL>-i<ip|ALL> [-c] [-q]
  ```

Related reference:

"psconf command" on page 158

Installing Trusted Network Connect

Installing the components of Trusted Network Connect (TNC) requires you to complete certain steps.

To configure the setup for using the components of TNC, complete the following steps:

1. Identify the IP addresses of the systems to setup the TNC server, the Trusted Network Connect and Patch Management (TNCPM) server, and the TNC IP referrer for the Virtual I/O Server (VIOS).

   Note: The TNC server cannot be configured as a TNC client.
2. Set up the network installation management (NIM) server. The system that is configured as a server is the NIM master, and the `sets:bos.sysmgt.nim.master` filesets must be installed on the client system.
3. Configure the TNCPM server. This configuration can be set up on the NIM system. The TNCPM server uses the SUMA to download the patches from IBM Fix Central and ECC websites. To download the updates, the system must be connected to the Internet. Enter the following command to configure the TNCPM server:

   ```
   pmconf mktncpm [pmport=<port>]tncserver=<host:port>
   ```

   For example:

   ```
   pmconf mktncpm pmport=20000 tncserver=1.1.1.1:10000
   ```
4. Configure the policies on the TNC server. To create the policies for verifying the clients, see "Creating policies for the Trusted Network Connect client" on page 131.
5. Configure the TNC IP referrer on VIOS. This configuration on VIOS triggers the verification on the clients that are connecting to the network. Enter the following command to configure the referrer:

   ```
   psconf mkipref tncport=<port> tncserver=<ip:port>
   ```

   For example:

   ```
   psconf mkipref tncport=10000 tncserver=1.1.1.1:10000
   ```

   Note: The value of the server port and the TNC port, which is a client port, must be the same.
6. Configure the clients by using the following command:

   ```
   psconf mkclient tncport=<port> tncserver=<serverip>:<port>
   ```

   For example:

   ```
   psconf mkclient tncport=10000 tncserver=10.1.1.1:10000
   ```

Related reference:

"psconf command" on page 158

Related information:

You must install a fileset for each specific function of PowerSC Standard Edition.

Installing with NIM

➥ IBM Fix Central

➥ Passport Advantage Online Help Center

Configuring Trusted Network Connect and Patch management

You must configure Trusted Network Connect (TNC) as a patch management daemon. The TNC server integrates with the SUMA to provide a comprehensive patch management solution.

Configuring Trusted Network Connect server

Learn the steps to configure the TNC server.

To configure the TNC server, the /etc/tnccs.conf file must have a value similar to the following:

```
component = SERVER
```

To configure a system as a server, enter the following command:

```
psconf mkserver tncport=<port> pmserver=<ip|hostname[,ip2|hostname2..]:port>
[recheck_interval=<time in mins>]
```

For example:

```
psconf mkserver tncport=10000 pmserver=2.2.2.2:20000 recheck_interval=20
```

Note: The tncport port and the pmserver port must be set to different values, and if the value of the recheck_interval parameter is not provided, a default value of 1440 minutes is used.

The default port value of 42830 minutes is used for the tncport port, and the default value of 38240 minutes is used for the pmserver port.

Related reference:

"psconf command" on page 158

Configuring Trusted Network Connect client

Learn the steps to configure the Trusted Network Connect (TNC) client and the configuration settings that are required for the setup.

To configure the TNC client, the /etc/tnccs.conf file must have a value similar to the following :

```
component = CLIENT
```

To configure a system as a client, enter the following command:

```
psconf mkclient tncport=<port> tncserver=<ip:port>
```

For example:

```
psconf mkclient tncport=10000 tncserver=1.1.1.1:10000
```

Note: The value of the server port and the tncport, which is a client port must be the same.

Related reference:

"psconf command" on page 158

Configuring the patch management server

Learn the steps to configure a system as a patch management server.

The Trusted Network Connect (TNC) patch management server must be configured on the Network Installation Management (NIM) server so the TNC clients can be updated.

To initialize the fix repositories for TNC patch management, enter the following command (enter command on a single line):

```
pmconf init -i <download interval> -l <TL list> [-A] [-P <download path>]
[-x <ifix interval>] [-K <ifix key>]
```

An example of the **pmconf** command follows:

```
pmconf init -i 1440 -l 6100-07,7100-01
```

The **init** command downloads the latest service pack for each technology level, and makes it available for the TNC server. The updated service packs enable the TNC server to run a baseline TNC client verification, and for the TNC patch management server to install the TNC client updates. Specify the **-A** flag to accept all license agreements when running the client updates. By default, the fix repositories that are downloaded by the TNC patch management server are in the /var/tnc/tncpm/fix_repository file. Use the **-P** flag to specify a different directory.

To enable automatic IBM Security Advisory and interim fix downloads, you can specify an interim fix interval. This feature provides automatic notification of newly-published security interim fixes and associated Common Vulnerabilities and Exposures (CVE) identifiers. All security advisories and interim fixes are verified prior to registration with the TNC. The IBM AIX vulnerability public key, which is required to download interim fixes automatically, is available at the IBM AIX Security website. Automatic service pack and interim fix downloads are disabled by setting both the download interval and interim fix interval to 0.

You can also update service pack and interim fix registration manually. To manually register an IBM Security Advisory along with its corresponding interim fixes, enter the following command:

```
pmconf add -y <advisory file> -v <signature file>  -e <ifix tar file>
```

To manually register a stand-alone interim fix, enter the following command:

```
pmconf add -p <SP> -e <ifix file>
```

To register a new technology level and to download its latest service pack, enter the following command:

```
pmconf add -l <TL list>
```

To download a service pack that is not the most current version, or to download a technology level to be used for verification and client updates, enter the following command:

```
pmconf add -l <TL list> -d
pmconf add -s <SP List>
```

To register a service pack or technology level fix repository that exists on the system, enter the following command:

```
pmconf add -s <SP> -p <user_defined_fix_repository>
pmconf add -l <TL> -p <user_defined_fix_repository>
```

To configure a system to serve as a patch management server, enter the following command:

```
pmconf mktncpm [pmport=<port>] tncserver=ip_list[:port]
```

An example of this command follows:

```
pmconf mktncpm pmport=20000 tncserver=1.1.1.1:100000
```

The TNC patch management server always supports the management of security Authorized Problem Analysis Reports (APARs). Enter the following command to configure the TNC patch management to manage other types of APARs:

```
pmconf add -t <APAR_type_list>
```

In the previous example, <APAR_type_list> is a comma-separated list that contains the following types of APARs:

- HIPER
- PE
- Enhancement

To manage the TNCPM Open Package Repositories enter one or more of the following commands:

```
pmconf add -o <package name> -V <version> -T [installp|rqm] -D <User defined path>
pmconf delete -o <package name> -V <version>
pmconf list -o <package name> -V <version>
pmconf list -O [-c] [-q]
```

Open Packages are added to this default directory:

```
/var/tnc/tncpm/fix_repository/packages.
```

User defined path = Package location on the system

The TNC patch management server supports **syslog** for downloading service pack, technology level, and client updates. The facility is `user` and priority is `info`. An example of this is `user.info`.

The TNC patch management server also maintains a log with all of the client updates in the `/var/tnc/tncpm/log/update/<ip>/<timestamp>` directory.

Related reference:

"psconf command" on page 158

Related information:

➥ IBM AIX Security

Configuring Trusted Network Connect server email notification

Learn the procedure to configure email notification for the Trusted Network Connect (TNC) server.

The TNC server views the patch level of the client and if the TNC server finds that the client is not compliant, it sends an email to the administrator with the result and the required remediation.

To configure the email address of the administrator, enter the following command:

```
psconf add –e <email_id>[ipgroup=[±]G1, G2 ..]
```

For example:

```
psconf add –e abc@ibm.com ipgroup=vayugrp1,vayugrp2
```

In the preceding example, the email for IP group *vayugrp1* and *vayugrp2* is sent to the abc@ibm.com email address.

To send an email to a global email address for the IP group that does not have an email address assigned to it, enter the following command:

```
psconf add –e <mailaddress>
```

For example:

```
psconf add –e abc@ibm.com
```

In the preceding example, if an IP group does not have an email address assigned to it, the mail is sent to the abc@ibm.com email address. It acts as a global email address.

Related reference:

"psconf command" on page 158

Configuring IP referrer on VIOS

Learn how to configure the IP referrer on Virtual I/O Server (VIOS) to automatically initiate verification.

Note: You must configure the SVM kernel extension on the Virtual I/O Server (VIOS) before configuring the IP referrer.

To configure the TNC IP Referrer, the `/etc/tnccs.conf` configuration file must have a setting similar to the following `component = IPREF`.

You can configure a system as a client by entering the following command:

`psconf mkipref tncport=<port> tncserver=<ip:port>`

For example:

`psconf mkipref tncport=10000 tncserver=1.1.1.1:10000`

The value of the `tncserver` port and the `tncport`, which is the client port must be the same.

Related reference:

"psconf command" on page 158

Managing Trusted Network Connect and Patch management

Learn how to manage Trusted Network Connect (TNC) to implement tasks, such as adding the clients, policies, logs, verification results, updating clients, and certificates related to TNC.

Viewing the Trusted Network Connect server logs

Learn how to view the logs of the Trusted Network Connect (TNC) server.

The TNC server logs the verification results of all the clients. To view the log, run the **psconf** command:

`psconf list –H –i <ip |ALL>`

Related reference:

"psconf command" on page 158

Creating policies for the Trusted Network Connect client

Learn how to set up policies related to Trusted Network Connect (TNC) client.

The `psconf` console provides the interface that is required to manage the TNC policies. Each client or a group of clients can be associated with a policy.

The following policies can be created:
- An Internet Protocol (IP) group contains multiple client IP addresses.
- Each client IP can belong to only one group.
- The IP group is associated with a policy group.
- A policy group contains different kinds of policies. For example, the fileset policy that specifies what must be the client's operating system level (that is, release, technology level, and service pack). There can be multiple fileset policies in a policy group and the client that refers to this policy must be at the level specified by one of the fileset policies.

The following commands show how to create an IP group, policy group, and fileset policies.

To create an IP group, enter the following command:
```
psconf add –G <ipgrpname> ip=[±]<ip1,ip2,ip3 ...>
```

For example:
```
psconf add –G myipgrp ip=1.1.1.1,2.2.2.2
```

Note: For a group, at least one IP must be provided. Multiple IPs must be separated by a comma.

To create a fileset policy, enter the following command:
```
psconf add –F <fspolicyname> <rel00-TL-SP>
```

For example:
```
psconf add –F myfspol  6100-02-03 aparlist=IY0001,IY0002
```

Note: The build information must be in the `<rel00-TL-sp>` format.

To create a policy and to assign an IP group, enter the following command:
```
psconf add –P <policyname> ipgroup=[±] <ipgrp1, ipgrp2 ...]
```

For example:
```
psconf add –P mypol ipgroup=myipgrp,myipgrp1
```

To assign fileset policy to a policy, enter the following command:
```
psconf add –P <policyname> fspolicy=[±]<fspol1, fspol2 ...>
```

For example:
```
psconf add –P mypol fspolicy=myfspol,myfspol1
```

To add OpenPackage policy, enter the following command:
```
pconf add -O <openpkggrp> <openpkgname:version>
```

The following is an example of adding an OpenPackage policy:
```
psconf add –O opengrp2 openssl:1.0.1.516
```

To assign OpenPackage policy to Fspolicy, enter the following command:
```
psconf add -O opengrp2 fspolicy=fspolicy1
```

Note: If multiple fileset policies are provided, the system enforces the best matching policy on the client. For example, if the client is on 6100-02-01 and you mention the fileset policy as 7100-03-04 and 6100-02-03, then 6100-02-03 is enforced on the client.
Related reference:
"psconf command" on page 158

Starting verification for the Trusted Network Connect client

Learn how to verify the Trusted Network Connect (TNC) client.

Use one of the following methods for client verification:
- The IP referrer daemon on the Virtual I/O Server (VIOS) forwards the client IP to the TNC server: The client LPAR acquires the IP and tries to access the network. The IP referrer daemon on VIOS detects the new IP address and forwards it to the TNC server: The TNC server initiates verification on receiving the new IP address.

- The TNC server verifies the client periodically: The administrator can add the client IPs that are to be verified in the TNC policy database. The TNC server verifies the clients that are in the database. The reverification happens automatically at regular intervals with reference to the `recheck_interval` attribute value that is specified in the `/etc/tnccs.conf` configuration file.
- The administrator initiates the client verification manually: The administrator can initiate the verification manually to verify whether a client is added to the network by running the following command:

```
pconf verify -i <ip>
```

Note: For resources that are not connected to a VIOS, the clients can be verified and updated when they are added manually to the TNC server.

Related reference:

"psconf command" on page 158

Viewing the verification results of the Trusted Network Connect

Learn the procedure to view the verification results of the Trusted Network Connect (TNC) client.

To view the verification results of the clients in the network, enter the following command:

```
psconf list -s ALL -i ALL
```

This command displays all clients that have a **IGNORED**, **COMPLIANT**, or **FAILED** status.
- **IGNORED**: The client IP is ignored in the IP list (that is, the client can be exempt from verification).
- **COMPLIANT**: The client passed the verification (that is, the client is compliant with the policy).
- **FAILED**: The client failed verification (that is, the client is not compliant with the policy and administration action is required).

To determine the reason for the failure, run the **psconf** command with the client IP that has failed:

```
psconf list -s ALL -i <ip>
```

Related reference:

"psconf command" on page 158

Updating the Trusted Network Connect client

The Trusted Network Connect (TNC) server verifies a client and updates the database with the status of the client and the result of verification. The administrator can view the results and take action to update the client.

To update a client that is at a previous level, enter the following command:

```
psconf update -i <ip> -r <buildinfo> [-a apar1,apar2...]
```

For example:

```
psconf update —i 4.4.4.4 —r 6100-02-03 —a IY0004
```

The **psconf** command updates the client with the build and the APAR installations if they are not installed.

To update the client with Open Packages:

```
psconf update -i <ip> -O opengrp2
```

Related reference:

"psconf command" on page 158

Managing patch management policies

The **pmconf** command is used to configure the patch management policies.

The patch management policies provide information, such as the TNC server IP address and the time interval to initiate a SUMA update.

To manage the patch management policy, enter the following command:

```
pmconf mktncpm [pmport=<port>] tncserver=<host:port>
```

For example:

```
pmconf mktncpm pmport=2000 tncserver=10.1.1.1:1000
```

Note: The `pmport` and the `tncserver` ports must be different.

Related reference:

"pmconf command" on page 155

Importing Trusted Network Connect certificates

Learn the procedure to import a certificate and to securely transmit data in the network.

The Trusted Network Connect (TNC) daemons communicate over the encrypted channels enabled by using the Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocol. This daemon ensures that the data and commands that are transported on the network are authenticated and secure. Each system has its own key and certificate, which are generated when the initialization command for the components is run. This process is transparent to the administrator and requires less involvement from the administrator. When a client is being verified for the first time, its certificate is imported into the database of the server. The certificate is marked as untrusted initially, and the administrator uses the **psconf** command to view and to mark the certificates as trusted by entering the following command:

```
psconf certadd -i <ip> -t <TRUSTED|UNTRUSTED>
```

If the administrator wants to use a different key and certificate, the **psconf** command provides the feature to import the key and certificate.

To import the certificate from a server, enter the following command:

```
psconf import  -S -k <key filename> -f <filename>
```

To import the certificate from a client, enter the following command:

```
psconf import -C -k <key filename> -f <filename>
```

Related reference:

"psconf command" on page 158

TNC server reporting

The Trusted Network Connect (TNC) server supports both the comma-separated values (CSV) format and the text output format for its common vulnerabilities and exposures (CVE), IBM Security Advisory, TNC server policies, TNC client security fix, and registered service packs and interim fix reports.

The CVE report displays all of the common exposures and vulnerabilities for the registered service packs. To display the results of this report, enter the following command:

```
psconf report -v {CVEid|ALL} -o {TEXT|CSV}
```

The IBM Security Advisory report displays the known security vulnerabilities on the installed IBM software. To display the results of this report, enter the following command:

```
psconf report -A <advisoryname>
```

The TNC server policies report displays the security policies that are enforced on the TNC server. To display the results of this report, enter the following command:

```
psconf report -P {policyname|ALL} -o {TEXT|CSV}
```

The TNC client fix report displays the installed and missing interim fixes for the TNC client. To display the results of this report, enter the following command:

```
psconf report -i {ip|ALL} -o {TEXT|CSV}
```

You can also run a report that generates a list of registered service packs and the related authorized program analysis reports (APARs) and interim fixes. To display the results of this report, enter the following command:

```
psconf report -B {buildinfo|ALL} -o {TEXT|CSV}
```

| To display a list of registered open source packages, enter the following report command:
| `psconf report -O ALL -o TEXT`

Related reference:

Troubleshooting Trusted Network Connect and Patch management

Learn the possible causes for failure and the steps to troubleshoot the TNC and the patch management system.

To troubleshoot the TNC and the patch management system, verify the configuration settings that are listed in the following table.

Table 13. Troubleshooting the configuration settings for the TNC and Patch management systems

Problem	Solution
TNC server is not starting or responding	Complete the following procedure: 1. Determine whether the TNC server daemon is running by entering the command: `ps -eaf	grep tnccsd`   2. If it is not running, delete the /var/tnc/.tncsock file.   3. Restart the server.    If that does not solve the problem, check the /etc/tnccs.conf configuration file for the `component = SERVER` entry on the TNC server.
The TNC patch management server is not starting or responding	• Determine whether the TNC patch management server daemon is running by entering the following command: `ps -eaf	grep tncpmd`   • Check the /etc/tnccs.conf configuration file for the `component = TNCPM` entry on the TNC patch management server.
TNC client is not starting or responding	• Determine whether the TNC client daemon is running by entering the following command: `ps -eaf	grep tnccsd`   • Check the /etc/tnccs.conf configuration file for the `component = CLIENT` entry on the TNC client.
TNC IP referrer is not running on Virtual I/O Server (VIOS)	• Determine whether the TNC IP referrer daemon is running by entering the following command: `ps -eaf	grep tnccsd`   • Check the /etc/tnccs.conf configuration file for the `component = IPREF` entry on VIOS.

Table 13. Troubleshooting the configuration settings for the TNC and Patch management systems (continued)

Problem	Solution
Unable to configure a system as both a TNC server and client	The TNC server and client cannot run simultaneously on the same system.
Daemons are running but verification does not happen	Enable the log messages for the daemons. Set the `level=info` log in the `/etc/tnccs.conf` file. You can analyze the log messages.

PowerSC graphical user interface (GUI)

This section describes the IBM PowerSC graphical user interface (GUI) including information about how to install, maintain, and use the interface.

The IBM PowerSC GUI improves the usability of the PowerSC Standard Edition product by providing an alternative to command-line and log-file interaction. PowerSC GUI provides a centralized management console for visualization of endpoints and their status; applying, undoing, or checking compliance levels; grouping systems for the application of compliance level actions; and viewing and customizing compliance configuration profiles.

PowerSC GUI concepts

Before using the PowerSC GUI, you should understand the general concepts regarding security and endpoint discovery.

PowerSC GUI security

The PowerSC GUI provides security by using bidirectional HTTPS communication between the PowerSC GUI server and the PowerSC GUI agents on each of the AIX endpoints.

The TLS handshaking process uses certificates that are available on both the PowerSC GUI server and PowerSC GUI agents. The TLS handshaking process supports single authentication in both directions because either the PowerSC GUI agent or the PowerSC GUI server might initiate communication. The agent creates a nonce, which is a random number, that is sent to the PowerSC GUI server during the first connection. The PowerSC GUI server then includes this nonce with every command that is sent to that agent. This nonce provides another layer of confirmation to the endpoint agent that it is running a command that originated from the authentic PowerSC GUI server. The endpoint must ensure that the source of the web service call is trusted. The initial handshake and the nonce ensures the trust.

All communication between the PowerSC GUI agents and the PowerSC GUI server is encrypted by using protocols and cipher suites that are consistent with the security requirements of the protected systems. Currently, the protocol level is TLS 1.2. The PowerSC GUI server interacts with all the PowerSC GUI agents and with all the PowerSC GUI users. Therefore, the PowerSC GUI server must have a certificate that is trusted by all connections from the user's web browsers. For example, certificates from a well-known authority such as Verisign or from an internally trusted certificate authority.

During installation, the PowerSC GUI server creates a self-signed certificate for its own use. This certificate can be used indefinitely, but it is intended for temporary use and can be replaced by a user-provided, widely recognized certificate. The PowerSC GUI server installation also creates a signing certificate that is used to sign all endpoint certificates. A shell script (`generate_endpoint_keystore_uiServer.sh`) is provided that you must use to create a self-signed certificate for each endpoint that is managed by using the PowerSC GUI. Because each endpoint's certificate is signed by the server's signing certificate, the PowerSC GUI server recognizes the validity of every endpoint when a connection is established. In addition to running the script to create a certificate for each endpoint, you must also copy the newly created certificate file from the PowerSC GUI server to the endpoint. The installation process automatically creates a truststore file for each endpoint. The truststore file is the same for every endpoint and must be copied from the PowerSC GUI server to each endpoint. This combination of certificates on both the PowerSC GUI server and endpoints provides a high level of communication security.

More security control is provided by using UNIX Groups. By default any user, whether an LDAP user or a local user who is defined by the operating system, must be a member of the security group to log in to the PowerSC GUI. The administrator can change this required group membership by using the **setLoginGroupName.sh** command.

After you are logged in, you might still be restricted to view-only mode. You can use the user authority function to perform actions against endpoints that are controlled by UNIX group membership. To perform any actions, you must be a member of a UNIX group that has permission to manage the endpoint. For more information, see the Specifying which groups have access topic.

By default, any user who is a member of the security group can manage every endpoint that is visible in the PowerSC GUI. The PowerSC administrator can restrict user access to the individual endpoint level by using the **setGroups.sh** command.

Populating the endpoint content in the compliance page

The PowerSC GUI server and PowerSC GUI agent communicate with the endpoint to discover the compliance level.

Upon startup, and intermittently until successful, the agent attempts to initiate contact with the PowerSC GUI server. When contact is established, a one-time agent-server security handshake is performed. After the agent-to-server security handshake is successfully negotiated the first time, the server creates a domain element with a Unique Identifier (UID) for internal representation of the endpoint, and passes the UID back to the endpoint. The UID is then included with all communication from the agent to the server. This action completes the discovery process. The PowerSC GUI server and the endpoint can communicate securely in either direction.

After completion of the initial discovery handshake, or after the PowerSC GUI agent is restarted, the PowerSC GUI agent attempts to determine the current compliance status information for its endpoint and updates the PowerSC GUI server. The existence of the endpoint and the current compliance information is used to populate the compliance status page of the PowerSC GUI. If no compliance status information can be determined, the entry is blank in the compliance status page.

The PowerSC GUI server contains a representation of all known endpoints, which are automatically created as a result of the initial agent-server connection and communication. As the endpoint agents track changes in compliance status, the changes are passed to the server and retained. All user (from the browser) interaction with an endpoint is performed through the PowerSC GUI. The user interface never interacts directly with any endpoint or endpoint agent.

Installing PowerSC GUI

The PowerSC GUI components are installed during the PowerSC Standard Edition 1.1.5 installation.

PowerSC GUI agents and the PowerSC GUI server are installed from the `installp` filesets, mostly by using the AIX Network Installation Manager (NIM). NIM allows the postinstallation scripts to automatically configure the installed PowerSC GUI agent.

The installation process creates role-based access control (RBAC) role definitions on each endpoint and on the PowerSC GUI server.

The installer also defines default users on the endpoints to run the PowerSC GUI agent and the PowerSC GUI server processes. Setting up default users provides control over the permissions that are granted to the PowerSC GUI processes.

PowerSC GUI agent

The PowerSC GUI agent is installed on every AIX endpoint. The PowerSC GUI agent tracks the endpoint compliance status and provides that information to the PowerSC GUI server.

The PowerSC GUI agent also runs the commands that are triggered from the PowerSC GUI. All communication between PowerSC GUI agents and the PowerSC GUI server is encrypted.

The `installp` command installs the core PowerSC Standard Edition product and the PowerSC GUI agent. The `powerscStd.uiAgent.rte` `installp` fileset is used for the PowerSC GUI agent installation. The following example displays the `installp` command that is run on each endpoint:

Note: In the following example, the installer images are expanded in the `/tmp/inst.images/` directory.

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiAgnet.rte
```

PowerSC GUI server

The PowerSC GUI server can run on any AIX system, it is recommended that you create a dedicated AIX LPAR on which to install and run the PowerSC GUI server.

The **installp** command installs the core PowerSC Standard Edition product and the PowerSC GUI server. The `powerscStd.uiServer.rte` **installp** fileset is used for the PowerSC GUI server installation. The following example displays the **installp** command that is run on an endpoint:

Note: In the following example, the installer images are expanded in the `/tmp/inst.images/` directory.

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiAgnet.rte
```

PowerSC GUI Requirements

Learn about the hardware and software requirements for the PowerSC GUI.

Hardware
- The PowerSC GUI server components should be installed on a separate LPAR, or VM that is running AIX Version 7.2, or later.
- The PowerSC GUI agent components must be installed on each AIX endpoint.

Software
- The PowerSC GUI server requires AIX Version 7.2, or later.

Creating security certificates

After you install the PowerSC GUI agent on the endpoints and after you install the PowerSC GUI server, several shell scripts are provided in the `/opt/powersc/uiServer/bin/` directory for creating or importing security certificates.

The following stores are required and are created by one or more of the shell scripts that are run during installation or by the PowerSC administrator:
- `endpointKeystore.jks`
- `endpointTruststore.jks`
- `serverKeystore.jks`
- `serverTruststore.jks`
- `signingKeystore.jks`

The following table describes each certificate-related shell script that is provided in `/opt/powersc/uiServer/bin/` directory and whether it is run automatically as part of the installation or whether it must

be run by the system administrator after installation is complete:

Table 14. Certificate shell scripts

Shell script	Run by	Description
`generate_server_keystore_uiServer.sh`	Runs automatically during installation.	This script creates the endpoint truststore, the GUI server truststore, and GUI server keystore. The endpoint truststore contains a self-signed security certificate that references the GUI server. • `endpointTruststore.jks` • `serverKeystore.jks` • `serverTruststore.jks`
`generate_signing_keystore_uiServer.sh`	Runs automatically during installation.	This script generates a certificate that is used to sign messages. • `signingKeystore.jks`
`generate_endpoint_keystore_uiServer.sh`	This script must be run once for each endpoint that is monitored through the PowerSC GUI.	Run this script to generate the endpoint keystore. • `endpointKeystore.jks`
`import_well_known_certificate_uiServer.sh`	This script needs to run only if you are providing your own well-known certificate.	If you already have a certificate .pem file from a well-known certificate authority, you can run this script to create the endpoint truststore, import that certificate, create the GUI server truststore, and create the GUI server keystore.

Running the certificate scripts

System administrators must run the provided scripts to create security certificates and certificate stores for the PowerSC GUI server and for each endpoint.

You use the provided scripts to create both truststores and keystores for the PowerSC GUI server and endpoints.

The endpoint truststore enables the endpoints to verify the credentials of the PowerSC GUI server. Depending on the script you choose, the endpoint truststore contains either a certificate from a well-known certificate authority, or a self-signed security certificate that references the PowerSC GUI server. You use the same truststore for all endpoints, but the keystores are endpoint-specific.

1. On the PowerSC GUI server, change directory to /opt/powersc/uiServer/bin/.
2. Choose one of the following scripts to create the endpoint truststore, the GUI server truststore, and the GUI server keystore:
   - If you already have a certificate .pem file from a well-known certificate authority, run the `import_well_known_certificate_uiServer.sh` script to import that certificate:

     `./import_well_known_certificate_uiServer.sh` *wellknowncert.pem*
   - If you do not already have a certificate .pem file from a well-known certificate authority, run the `generate_server_keystore_uiServer.sh` script to create a self-signed certificate.

     `./generate_server_keystore_uiServer.sh` *fully-qualified-UI server-hostname*
3. Generate a certificate (opt/powersc/uiServer/psc_signing_cert.pem) that is used to sign messages and store it in the /etc/security/powersc/uiServer/signingKeystore.jks keystore.

   `./generate_signing_keystore_uiServer.sh`
4. Generate the endpoint keystore in the /etc/security/powersc/uiServer/fully-qualified-hostname/ endpointKeystore.jks file. You must provide the fully qualified host name for the endpoint. The

common name (CN) of the created certificate uses the fully qualified host name to identify the endpoint. This script uses the location of the signing keystore that is created by the `generate_signing_keystore_uiServer.sh` script.

```
./generate_endpoint_keystore_uiServer.sh fully-qualified-endpoint-hostname
```

5. Copy the `/etc/security/powersc/uiServer/fully-qualified-hostname/endpointKeystore.jks` file to the `/etc/security/powersc/uiAgent/endpointKeystore.jks` file on the endpoint you specified by running the following **scp** command:

```
# scp endpointKeystore.jks user@endpoint-host-name:
                            /etc/security/powersc/uiAgent
```

6. Copy the endpoint truststore `/etc/security/powersc/uiServer/endpointTruststore.jks` file to the `/etc/security/powersc/uiAgent/endpointTruststore.jks` file on each endpoint by running the following **scp** command:

```
# scp endpointTruststore.jks user@endpoint-host-name:
                            /etc/security/powersc/uiAgent
```

7. Repeat steps 4 on page 140, 5 and 6 for each endpoint.

8. If you add more endpoints, complete steps 4 on page 140, 5, and 6 for each additional endpoint.

Setting up user accounts

By default any user, whether an LDAP user or a local user who is defined by the operating system, must be a member of the security group to log in to the PowerSC GUI.

The administrator can change this required group membership by using the **setLoginGroupName.sh** command. After logging in to the PowerSC GUI, a user can only view the status of endpoints unless the their user account is a member of a UNIX group that is allowed to manage the endpoint. This setting is a wildcard by default (users who are allowed to login can also manage every endpoint that visible in the GUI). The administrator can change the user account settings for the individual endpoint level by using the **setGroups.sh** command.

Consider the following points:

- A many-to-many relationship exists between endpoints and AIX groups:
  - One AIX group can be associated with many endpoints.
  - One endpoint can be associated with many AIX groups.
- After a user is logged in to the PowerSC GUI, group associations are used to determine whether a user is allowed to run commands to specific endpoints, or whether the user is allowed only to view endpoint status.
  - To run commands against a specific endpoint by using the PowerSC GUI, the user must be associated with one of the groups that is associated with the endpoint.
  - The user's group membership is compared with the set of groups that are associated with each endpoint. If the users's group membership matches groups that are associated with each endpoint, the user is allowed to run commands such as **Apply profiles**, **Undo**, and **Check** against that endpoint. If the users's group membership does not match any groups that are associated with each endpoint, the user can view only the status for that endpoint.

The following shell scripts are available in the PowerSC GUI server in the `/opt/powersc/uiServer/bin/` directory.

Table 15. Group shell scripts

Shell script	Description
setLoginGroupName.sh	Specifies which AIX groups a user must be a member to log in to the PowerSC GUI.
setGroups.sh	Specifies which AIX groups a user must be a member of to run commands on specific endpoints.

Running the group scripts

System administrators must run the provided scripts to specify which operating system groups are allowed to log in to the PowerSC GUI, and to execute commands on specific endpoints.

1. On the PowerSC GUI server, change the directory to /opt/powersc/uiServer/bin/.

2. Run the following command to specify the AIX group in which a user must be a member to log in to the PowerSC GUI. The group that you specify is written to the /etc/security/powersc/uiServer/groups.txt file.

   ./setLoginGroupName.sh *groupname*

   Tip: Before you run the command, you can use the **groups** *username* command to view the groups in which the user is a member.

3. Run the following command to specify the AIX groups in which a user must be a member to run commands on specific endpoints. You must provide fully qualified host names of the endpoints. The groups that you specify are written to the /etc/security/powersc/uiServer/groups.txt file.

   ./setGroups.sh *groupname* "*comma separated list of endpoint host names*"

   Note: Limited wildcards are supported when you are searching for endpoints. For example, the following specifications are valid to query all endpoints that have a name starting with "Boston_" or ending with ".rs.com":

   - ./setGroups.sh groupname "Boston_*"
   - ./setGroups.sh groupname "*.rs.com"

Using the PowerSC GUI

You can use the PowerSC GUI to view the endpoints that are discovered on your system, create customized groups, create customized profiles, copy custom profiles to endpoints, and apply profiles. You can also verify communication between the endpoints and the PowerSC GUI server and stop communication between an endpoint and the PowerSC GUI server.

The main page of the PowerSC GUI contains the following sections:
- **Groups** tray: Lists the groups that are defined for your environment. Groups are collections of endpoints that are grouped based on a commonality. The **All systems** group is created automatically when the endpoints in your environment are discovered. You can create customized groups. For example, you can create a group of endpoints whose commonality is HIPPA.
- **Compliance** page: The **Compliance** page includes three sections:
  - The top pane displays statistical information on the group you selected from the **Groups** tray. The statistical information displays the results of the last compliance levels that were applied to the endpoints in the selected group. For the selected group, you can view the percentage of system passes and failures, the total number of rules that were checked, and the specific rules that failed.
  - The center pane is a taskbar that can be used to perform actions on one or more endpoints. You can apply, undo, or check a compliance level.
  - The bottom pane displays a table that includes all the endpoints or a group of endpoints that are available in your environment. The table includes the following information for each endpoint:
    - System endpoints that are included in the selected group

- Last compliance level for the endpoint
- Time and date that the compliance level was applied to the endpoint
- Time and date that the compliance level was checked on the endpoint
- Compliance level status
- Number of rules on the endpoint that have passed successfully during compliance level checking
- **Configuration** page includes the following tabs:
  - **Group Editor**: You can use this tab to create customized groups of endpoints.
  - **Profile Editor**: You can use this tab to create customized profiles and copy custom profiles to endpoints.
  - **Endpoint Admin**: You can use this tab to verify communication between the endpoints and the PowerSC GUI server. You can also remove endpoints that you do not want to be monitored in the PowerSC GUI.

Specifying the PowerSC GUI language

The PowerSC GUI can be rendered in different languages.

To select the language for the PowerSC GUI, select the language icon that is located to the right in the top of the main page.

Navigating the PowerSC GUI

You can use the PowerSC GUI for all interaction with the PowerSC GUI server and agents.

To navigate the PowerSC GUI, complete the following steps:

1. Open the PowerSC GUI. The PowerSC GUI displays the **Compliance** page. The **Groups** tray is collapsed (hidden) by default.

2. To define groups, create custom profiles, and perform endpoint administrative tasks, select the **Configuration** tab. The **Configuration** notebook displays the **Group Editor** page.
   From the **Configuration** notebook:

   a. Select the **Group Editor** tab to create custom groups of endpoints. For more information, see the "Creating custom groups" on page 144 topic.

   b. Select the **Profile Editor** tab to create custom compliance profiles and copy profiles to endpoints. For more information, see the "Working with compliance profiles" on page 145 topic.

   c. Select the **Endpoint Admin** tab to verify or cease communication between the endpoints and the PowerSC GUI server. For more information, see the "Administering endpoint and server communication" on page 149 topic.

   d. Select the **Compliance** tab to return to the **Compliance** page.

3. All the endpoints for a selected group are displayed in the endpoint table. You can filter the endpoints that are displayed by using the **Filtering by text** text box. Enter the text that you want to filter by in the text box and press Enter. The list of endpoints from the selected group is dynamically filtered to show only rows that contain your text.

4. To refresh the displayed status information, click **Refresh Table**. To set how frequently the display is automatically refreshed, click **Refresh Interval**.

Organizing and grouping endpoints

System administrators can organize and group endpoints based on some common property. Custom groups can be defined and can contain an explicitly selected set of endpoints that are managed by using the PowerSC GUI.

For example, if you have 3 - 4 environments, you might want to create groups that contain production endpoints, test endpoints, and quality assurance endpoints.

A default group that is called **All Systems** is created during installation. This group contains all the endpoints that were discovered in your environment.

Creating custom groups

You can create a custom group with an explicitly selected, enumerated list of endpoints.

To create a custom group, complete the following steps:

1. Open the **Create New Group** dialog box by choosing one of the following methods:
   - From the main page, select **Configuration**. The **Configuration** notebook opens displaying the **Group Editor** page. From the **Group Editor** page, click the **Create New Group** icon.
   - From the **Groups** tray, select **Add New Group**.
   - From the **Profile Editor** tab or the **Endpoint Admin** tab, select the **Group Editor** tab. From the **Group Editor** page, click the **Create New Group** icon.
2. Enter the **Group** name and click **Save**. The new group is added to the **Groups** tray.
3. Add the systems that you want to be included in this group. From the list of available endpoint systems, select the check boxes for the systems that you want to include in the group, and then click the **Save** icon.

Adding systems to an existing group

You can add endpoints to existing groups.

To add a system to an existing group, complete the following steps:

1. Open the **Group Editor** page by choosing one of the following methods:
   - From the main page, select **Configuration**. The **Configuration** notebook opens displaying the **Group Editor** page.
   - From the **Profile Editor** page or the **Endpoint Admin** page, select the **Group Editor** tab.
2. Open the **Groups** tray by selecting the **Groups** tray icon.
3. From the **Groups** tray, select the group to which you want to add system endpoints.
4. Click the **Add Systems to Group** icon. A list of endpoints that are available but not already included in the group is displayed.
5. From the list of available endpoint systems, select the check boxes for the systems that you want to include in the group. Click the **Save** icon.

Deleting systems from a group

You can delete endpoint systems from a group.

To delete a system from a group, complete the following steps:

1. Open the **Group Editor** page by choosing one of the following methods:
   - From the main page, select **Configuration**. The **Configuration** notebook opens displaying the **Group Editor** page.
   - From the **Profile Editor** page or the **Endpoint Admin** page, select the **Group Editor** tab.
2. Open the **Groups** tray by selecting the **Groups** tray icon.
3. From the **Groups** tray, select the group that contains the endpoints that you want to remove from the group.
4. The endpoints for the group are displayed in the endpoints table. Clear the check boxes for the systems that you want to remove from the group.
5. Click the **Save** icon.

Deleting a group

You can delete groups that are no longer applicable.

To delete a group, complete the following steps:
1. Open the **Group Editor** page by choosing one of the following methods:
   - From the main page, select **Configuration**. The **Configuration** notebook opens displaying the **Group Editor** page.
   - From the **Profile Editor** page or the **Endpoint Admin** page, select the **Group Editor** tab.
2. Open the **Groups** tray by selecting the **Groups** tray icon.
3. From the **Groups** tray, select the group that you want to delete.
4. Click the **Delete Group** icon. The group is deleted.

Working with compliance profiles

Using the PowerSC GUI Profile Editor, you can view the built-in compliance profiles, create custom profiles, and copy profiles to system endpoints.

The PowerSC Standard Edition product is delivered with a set of built-in profiles that can be used to configure your system endpoints so that each endpoint meets the following security standards:
- Payment Card Industry - Data Security Standard compliance (PCI)
- Sarbanes-Oxley Act and COBIT compliance (SOX-COBIT)
- US Department of Defense STIG compliance (DoD)
- Health Insurance Portability and Accountability Act (HIPAA)
- North American Electric Reliability Corporation compliance (NERC)

For more information about the built-in profiles, see the "Security and Compliance Automation concepts" on page 9 topic.

Each of the built-in profiles include rules that must be applied to an endpoint to meet security requirements. When you need to apply only a subset of these rules or customize compliance levels, you can create a custom profile.

In most environments, administrators frequently edit compliance files to remove problem rules. After compatibility checks are complete, the compliance rule files are considered stable and are deployed onto production servers.

The PowerSC GUI can be used to create custom profiles by removing rules from built-in (or other custom) profiles.

Note: In PowerSC Standard Edition Version 1.1.5, you can create custom profiles by using the PowerSC GUI, as well as use existing custom profile XML files you might have already created manually. These custom profile XML files can be copied to the PowerSC GUI server. After the files are copied to the PowerSC GUI server, they are considered the same as other custom profiles.

When one of the built-in files is selected, that file is loaded such that the individual rule names are displayed with a check box for turning them off. The Profile Editor then allows the customized file to be saved. When you are saving changes, the file name must be different from an existing built-in profile or level. The newly customized file can be transferred to the default location on selected endpoint.

Using the Profile Editor you can perform the following functions for a selected target endpoint:
- List built-in profiles, custom profiles, and compliance level files. These profiles and compliance levels must be in the standard directory location on the PowerSC GUI server.

- Allow selection and loading of a (XML) file that is associated with a defined profile or level. Loading consists of:
  - Displaying a list of each rule name, all selected by default, with a GUI mechanism that allows individual deselection.
- Allow saving of the file, with deselected rule entries explicitly removed. The following restrictions apply to saving files:
  - Do not allow saving as the name of a pre-defined profile or level file
  - Only save to the proper PowerSC GUI server customization directory
  - A previously customized file could again be loaded and further reduced, then saved again

Viewing compliance profiles

You can view the rules that are included in each of the built-in and custom profiles.

To view compliance profiles, complete the following steps:
1. Open the **Profile Editor** page by choosing one of the following methods:
   - From the main page, select **Configuration**. The **Configuration** notebook opens displaying the **Group Editor** page. Select the **Profile Editor** tab.
   - From the **Group Editor** page or the **Endpoint Admin** page, select the **Profile Editor** tab.
2. Depending on the profile that you want to view, expand either the list of Built-in Profiles or Custom Profiles.
3. Select the profile that you want to view. Each rule that is included in the profile is displayed with its name, type, and a description. For more information about the rules, see the "Security and Compliance Automation concepts" on page 9 topic.
4. All the rules for the selected profile are displayed in the profiles table. You can filter the profiles that are displayed by using the **Filtering by text** text box. Enter the text that you want to filter by in the text box. The list of rules from the selected profile is refreshed.

Creating a custom profile

You can create a custom profile.

To create a custom profile, complete the following steps:
1. Open the **Profile Editor** page by choosing one of the following methods:
   - From the main page, select **Configuration**. The **Configuration** notebook opens displaying the **Group Editor** page. Select the **Profile Editor** tab.
   - From the **Group Editor** page or the **Endpoint Admin** page, select the **Profile Editor** tab.
2. Depending on the profile that you want to customize, expand either the list of **Built-in Profiles** or **Custom Profiles**.
3. Select the profile that you want to customize. The inclusion check box that is associated with each of the rules is checked if the rule is already included in the profile.
4. Select or clear the check boxes for the rules that you want to include or exclude in the custom profile.
5. When you have completed selecting or deselecting the rules, click the **Save as New Custom Profile** icon. The **Create Profile** dialog box opens.
6. Specify the custom name and custom type for the custom profile. Click **Create**.

Copying profiles to group members

You can copy custom profiles to a group of endpoints. After the custom profile is copied to the endpoint, it is available for application to the endpoint. It is also available for checking to verify whether it can be applied to the endpoint without errors.

To copy a custom profile to a group of endpoints, complete the following steps:

1. Open the **Profile Editor** page by choosing one of the following methods:
   - From the main page, select **Configuration**. The **Configuration** notebook opens displaying the **Group Editor** page. Select the **Profile Editor** tab.
   - From the **Group Editor** page or the **Endpoint Admin** page, select the **Profile Editor** tab.
2. Depending on the profile that you want to copy, expand either the list of **Built-in Profiles** or **Custom Profiles**.
3. Select the profile that you want to copy to a group's members.
4. Click the **Copy Profile to Group Members** icon. The **Copy** *profilename* **to Members of** window opens.
5. Each group that you have created for your organization is listed with an associated check box. Select the check box for each group where you want to copy the selected profile.
6. Click **OK**.
7. To apply or check the profile, return to the **Compliance** page by selecting the **Compliance** tab or responding to the prompt.

Deleting a custom profile

You can delete custom profiles.

To delete a custom profile, complete the following steps:

1. Open the **Profile Editor** page by choosing one of the following methods:
   - From the main page, select **Configuration**. The **Configuration** notebook opens displaying the **Group Editor** page. Select the **Profile Editor** tab.
   - From the **Group Editor** page or the **Endpoint Admin** page, select the **Profile Editor** tab.
2. From the **Groups** tray, select the group that includes the endpoints that have the custom profile that you want to delete.
3. Expand the **Custom Profiles** list.
4. Select the profile that you want to delete.
5. Click the **Delete Profile** icon. The Custom Profile that you selected is deleted.

Applying compliance levels and profiles

System administrators can apply, check, undo, or remediate built-in and custom compliance levels and profiles on multiple endpoints.

The following table lists the pre-defined profiles and compliance levels that are supported by PowerSC Standard Edition.

Table 16. Predefined profiles and compliance levels supported by PowerSC Standard Edition

Profiles	Levels
Database	low
DoD	medium
DoD_to_AIXDefault	high
DoDv2	default
DoDv2_to_AIXDefault	
HIPAA	
NERC	
NERC_to_AIXDefault	
NERCv5	
NERCv5_to_AIXDefault	

Table 16. Predefined profiles and compliance levels supported by PowerSC Standard Edition (continued)

Profiles	Levels
PCI	
PCI_to_AIXDefault	
PCIv3	
PCIv3_to_AIXDefault	
SOX-COBIT	

From the **Compliance** page in the PowerSC GUI, you can perform the following tasks:

* Select and apply a defined profile or level to one or multiple endpoints.
* Trigger an undo operation on one or multiple endpoints.
* Check a defined profile or level against the current state for one or multiple endpoints. The check operation does not result in any changes to the endpoint, but sets the **Checked Timestamp** value to indicate when the last check was performed.

Applying compliance levels and profiles

You can apply a compliance level or profile to one or more endpoints in a selected group.

To apply compliance levels and profiles, complete the following steps:

1. From the main page, select the **Compliance** tab. The **Compliance** page opens.
2. From the **Groups** tray, select the group that includes the endpoints to which you want to apply compliance levels and profiles.
3. All the endpoints for a selected group are displayed in the endpoint table. You can filter the endpoints that are displayed by using the **Filtering by text** text box. Enter the text that you want to filter by in the text box and press Enter. The list of endpoints from the selected group is dynamically filtered to show only rows that contain your text.
4. To refresh the displayed status information, click **Refresh**. To set how frequently the display is automatically refreshed, click **Refresh Interval**.
5. From the **Compliance Rule Type** list, you can view the levels and profiles that were copied to the associated endpoint. Select the level or profile that you want to apply to the endpoint. Check the associated check box.
6. Repeat step 5 for each endpoint in the group to which you want to apply compliance levels and profiles.
7. Click the **Apply profiles** icon.
8. The selected compliance levels and profiles are applied to each of the selected endpoints. If one or more rules cannot be applied, it is considered that they failed. If one or more rules fail, the endpoint is flagged with a red bar; and the text **Failed** is displayed in the **#Failed Rules** column.
9. From the **#Failed Rules** list for each flagged endpoint you can see why the rule failed. You can adjust the rules that are applied by creating a custom profile or by editing a custom profile.

Undoing compliance levels

You can undo the last compliance level or profile that has been applied to one or more endpoints in a selected group.

To undo compliance levels, complete the following steps:

1. From the main page, select the **Compliance** tab. The **Compliance** page opens.
2. From the **Groups** tray, select the group that includes the endpoints for which you want to undo the compliance levels and profiles.

3. All the endpoints for a selected group are displayed in the endpoint table. You can filter the endpoints that are displayed by using the **Filtering by text** text box. Enter the text that you want to filter by in the text box and press Enter. The list of endpoints from the selected group is dynamically filtered to show only rows that contain your text.

4. To refresh the displayed status information, click **Refresh**. To set how frequently the display is automatically refreshed, click **Refresh Interval**.

5. To undo a level that was applied to an endpoint:

   a. Check the associated check box for the endpoint.

   b. Click the **Undo** icon.

6. To undo a profile that was applied:

   a. Check the associated check box for the endpoint.

   b. Click the **Undo** icon.

Checking compliance levels and profiles

You can check whether the last compliance level or profile was applied to one or more endpoints in a selected group.

To check compliance levels and profiles, complete the following steps:

1. From the main page, select the **Compliance** tab. The **Compliance** page opens.

2. From the **Groups** tray, select the group that includes the endpoints for which you want to check the compliance levels and profiles.

3. All the endpoints for a selected group are displayed in the endpoint table. You can filter the endpoints that are displayed by using the **Filtering by text** text box. Enter the text that you want to filter by in the text box and press Enter. The list of endpoints from the selected group is dynamically filtered to show only rows that contain your text.

4. To refresh the displayed status information, click **Refresh**. To set how frequently the display is automatically refreshed, click **Refresh Interval**.

5. Select the associated check box for the endpoint system name for which you want to check for the last level or profile that was applied.

6. Repeat step 5 on page 148 for each endpoint in the group for which you want to check the compliance levels and profiles.

7. Click the **Check** icon.

8. The endpoint is checked to see whether the rules that are in the compliance level or profile can be applied. The endpoints are not updated. If any rules cannot be applied, it is considered that they fail when they are applied. If one or more rules fail, the endpoint is flagged with a red bar; and the text **Failed** is displayed in the **#Failed Rules** column.

9. From the **#Failed Rules** list for each flagged endpoint, you can view the message that indicates why the rule failed. You can adjust the rules that are applied by creating a custom profile.

Administering endpoint and server communication

From the **Endpoint Admin** page of the Configuration notebook you can verify or cease communication between the endpoints and the PowerSC GUI server.

Verifying endpoint and server communication

You can verify communication between discovered endpoints and the PowerSC GUI server.

To verify endpoint and server communication, complete the following steps:

1. Open the **Endpoint Admin** page by choosing one of the following methods:

- From the main page, select **Configuration**. The **Configuration** notebook opens displaying the **Group Editor** page. Select the **Endpoint Admin** tab.
- From the **Group Editor** page or the **Profile Editor** page, select the **Profile Editor** tab.

2. From the **Groups** tray, select the group that includes the endpoints that you want to verify. The endpoints for that group are listed in the endpoint table.
3. Select the associated check box for each endpoint that you want to verify.
4. Click the **Verify** icon.
5. A confirmation message about the valid connection is displayed in the **Verified** and **Connectivity Diagnosis** columns.

Removing endpoints from PowerSC GUI monitoring

Once an endpoint is discovered, it is continually monitored. If the endpoint is removed from your environment, you must also remove it from the PowerSC GUI server.

To remove endpoints from being monitored in the PowerSC GUI, complete the following steps:

1. Open the **Endpoint Admin** page by choosing one of the following methods:
   - From the main page, select **Configuration**. The **Configuration** notebook opens displaying the **Group Editor** page. Select the **Endpoint Admin** tab.
   - From the **Group Editor** page or the **Profile Editor** page, select the **Profile Editor** tab.
2. From the **Groups** tray, select the group that includes the endpoints that you want to remove. The endpoints for that group are listed in the endpoint table.
3. Select the associated check box for each endpoint that you want to remove.
4. Click the **Delete** icon.
5. A confirmation message about the deletion of the endpoint is displayed in the **Verified Timestamp** and **Connectivity Diagnosis** columns.

PowerSC Standard Edition commands

PowerSC Standard Edition provides commands that enable communication with the Trusted Firewall component and the Trusted Network Connect component by using the command line.

chvfilt command

Purpose

Changes the values for the existing virtual LAN-crossing filter rule.

Syntax

chvfilt [**-v** <4|6>] **-n fid** [**-a** <D|P>] [**-z** <**svlan**>] [**-Z** <**dvlan**>] [**-s** <**s_addr**>] [**-d** <**d_addr**>] [**-o** <**src_port_op**>] [**-p** <**src_port**>] [**-O** <**dst_port_op**>] [**-P** <**dst_port**>] [**-c** <**protocol**>]

Description

The **chvfilt** command is used to change the definition of a virtual LAN-crossing filter rule in the filter rule table.

Flags

-a   Specifies the action. Valid values follow:
  - D (Deny): Blocks traffic
  - P (Permit): Allows traffic

-c   Specifies different protocols to which the filter rule is applicable. Valid values follow:
  - udp
  - icmp
  - icmpv6
  - tcp
  - any

-d   Specifies the destination address in IPv4 or IPv6 format.

-m   Specifies the source address mask.

-M   Specifies the destination address mask.

-n   Specifies the filter ID of the filter rule that should be modified.

-o   Specifies the source port or the Internet Control Message Protocol (ICMP) type operation. Valid values follow:
  - lt
  - gt
  - eq
  - any

-O   Specifies the destination port or the ICMP code operation. Valid values follow:
  - lt
  - gt
  - eq

- any

-p Specifies the source port or the ICMP type.

-P Specifies the destination port or the ICMP code.

-s Specifies the source address in v4 or v6 format.

-v Specifies the IP version of the filter rule table. Valid values are 4 and 6.

-z Specifies the virtual LAN ID of the source logical partition.

-Z Specifies the virtual LAN ID of the destination logical partition.

Exit Status

This command returns the following exit values:

0 Successful completion.

>0 An error occurred.

Examples

1. To change a valid filter rule that exists in the kernel, type the command as follows:

   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

2. When a filter rule (n=2) does not exist in the kernel, the output is as follows:

   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   The system displays the output as follows:

   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   Cannot Change the filter rule.
   ```

genvfilt command

Purpose

Adds a filter rule for the virtual LAN (VLAN) crossing between logical partitions on the same IBM Power Systems server.

Syntax

genvfilt -v <4|6> -a <D|P> -z <svlan> -Z <dvlan> [-s <s_addr>] [-d <d_addr>] [-o <src_port_op>] [-p <src_port>] [-O <dst_port_op>] [-P <dst_port>] [-c <protocol>]

Description

The **genvfilt** command adds a filter rule for the virtual LAN (VLAN) crossing between logical partitions (LPARs) on the same IBM Power Systems server.

Flags

-a Specifies the action. Valid values follow:
- D (Deny): Blocks traffic
- P (Permit): Allows traffic

-c Specifies different protocols to which the filter rule is applicable. Valid values follow:
- udp
- icmp
- icmpv6

- tcp
- any

-d Specifies the destination address in v4 or v6 format.

-m Specifies the source address mask

-M Specifies the destination address mask.

-o Specifies the source port or the Internet Control Message Protocol (ICMP) type operation. Valid values follow:
- lt
- gt
- eq
- any

-O Specifies the destination port or the ICMP code operation. Valid values follow:
- lt
- gt
- eq
- any

-p Specifies the source port or the ICMP type.

-P Specifies the destination port or the ICMP code.

-s Specifies the source address in IPv4 or IPv6 format.

-v Specifies the IP version of the filter rule table. Valid values are 4 and 6.

-z Specifies the virtual LAN ID of the source LPAR. The virtual LAN ID must be in the range of 1 - 4096.

-Z Specifies the virtual LAN ID of the destination LPAR. The virtual LAN ID must be in the range of 1 - 4096.

Exit Status

This command returns the following exit values:

0 Successful completion.

>0 An error occurred.

Examples

1. To add a filter rule to permit TCP data from a source VLAN ID of 100 to a destination VLAN ID of 200 on specific ports, type the command as follows:

```
genvfilt -v4 -a P -z 100 -Z 200  -o lt -p 345 -O lt -P 345 -c tcp
```

Related reference:

"mkvfilt command" on page 154

"vlantfw command" on page 170

lsvfilt command

Purpose

Lists virtual LAN-crossing filter rules from the filter table.

Syntax

lsvfilt [**-a**]

Description

The **lsvfilt** command is used to list the virtual LAN-crossing filter rules and their status.

Flags

-a Lists only the active filter rules.

Exit Status

This command returns the following exit values:

0 Successful completion.

>0 An error occurred.

Examples

1. To list all the active filter rules in the kernel, type the command as follows:

       lsvfilt -a

Related concepts:

"Deactivating rules" on page 119
You can deactivate rules that enable cross-VLAN routing in the Trusted Firewall feature.

mkvfilt command

Purpose

Activates the virtual LAN-crossing filter rules defined by the **genvfilt** command.

Syntax

mkvfilt -u

Description

The **mkvfilt** command activates the virtual LAN-crossing filter rules defined by the **genvfilt** command.

Flags

-u Activates the filter rules in the filter rule table.

Exit Status

This command returns the following exit values:

0 Successful completion.

>0 An error occurred.

Examples

1. To activate the filter rules in the kernel, type the command as follows:

       mkvfilt -u

Related reference:

pmconf command

Purpose

Reports and manages the trusted network connect patch management (TNCPM) server by registering technology levels and TNC servers for latest fixes and generating reports on TNCPM status.

Note: The TNCPM server must be run only on AIX Version 7.1 with the 7100-02 Technology Level to allow the download of the service pack metadata.

Syntax

pmconf mktncpm [**pmport=**<*port*>] **tncserver=***ip* | hostname **:** *port*

pmconf rmtncpm

pmconf start

pmconf stop

pmconf init -i <*download interval*> **-l** <*TL List*> **-A** [**-P** <*download path*>] [**-x** <*ifix interval*>] [**-K** <*ifix key*>]

pmconf add -l *TL_list*

| **pmconf add -o** <*package name*> **-V** <*version*> **-T [installp|rqm] -D** <*User defined path*>

pmconf add -p <*SP List*> [**-U** <*user-defined SP path*>]

pmconf add -p <*SP*> **-e** <*ifix file*>

pmconf add -y <*advisory file*> **-v** <*signature file*> **-e** <*ifix tar file*>

pmconf delete -l *TL_list*

| **pmconf delete -o** <*package name*> **-V** <*version*>

pmconf delete -p <*SP List*>

pmconf delete -p <*SP*>**-e** *ifix file*

pmconf list -s [-c] [-q]

pmconf list -a *SP*

pmconf list -C

pmconf hist -d

pmconf list -l *SP*

| **pmconf list -o** <*package name*> **-V** <*version*>

| **pmconf list -o** [-c] [-q]

pmconf hist -u

pmconf import -f *cert_filename* **-k** *key_filename*

pmconf export -f *filename*

pmconf modify -i < *download interval*>

pmconf modify -P <*download path*>

pmconf modify -g <*yes or no to accept all licenses*>

pmconf modify -t <*APAR type list*>

pmconf modify -x <*ifix interval*>

pmconf modify -K <*ifix key*>

pmconf delete -l <*TL list*>

pmconf restart

pmconf status

pmconf log loglevel = info | error | none

pmconf chtncpm attribute = *value*

Description

The functions of the **pmconf** command are as follows:

Fix repository management
Registers or unregisters technology levels; unregisters TNC servers. TNCPM creates a fix
repository for each technology level that contains the latest fixes, **lslpp** information (for example,
information about installed file sets or file set updates), and security fix information for that
technology level.

Reporting
Generates reports on the status of TNCPM.

The following operations can be performed by using the **pmconf** command:

Item	Description
add	Registers a new technology level by using TNCPM.
chtncpm	Changes the attributes in the tnccs.conf file. An explicit **start** command is required for the changes to take effect in the TNCPM server.
delete	Unregisters a technology level by using TNCPM.
history	Displays update and download history.
list	Displays the information about TNCPM.
log	Sets the log level for the TNC components.
mktncpm	Creates the TNCPM server.
modify	Modifies the tncpm.conf attributes.
rmtncpm	Removes the TNCPM server.
start	Starts the TNCPM server.
stop	Stops the TNCPM server.

Flags

Item	Description
-A	Accepts all license agreements when performing client updates.
-a <advisory file>	Specifies the advisory file that corresponds to the **ifix** parameter. If the advisory file is not provided, the **ifix** parameter is not viewed as a common vulnerabilities and exposures (CVE) address of the interim fix.
-e <ifix file>	Specifies the interim fixes that are added to the TNCPM.
-i *download_interval*	Specifies the interval that TNCPM checks for a new service pack for the registered technology levels. The interval is an integer value that represents minutes or represents the following format: **d** (no of days): **h** (hours): **m** (minutes). The supported range for the *download_interval* is 30 - 525600 minutes.
-K <ifix key>	Specifies the public key of IBM AIX Product Security Incident Response Tool (PSIRT) that is used to authenticate the downloaded advisories and interim fixes. This public key can be downloaded from a PGP public key server by using the **0x28BFAA12** ID.
-p *SP_list*	Specifies a list of service packs to be downloaded. The list is a comma-separated list in the format, REL00-TL-SP (for example, 6100-01-04 represents the service pack 04 for technology level 01 and version 6.1). When you use the -U flag, specify only one SP.
-t *APAR_type_list*	Specifies the APAR types that the TNCPM supports for the client update and TNC server listing. Security APARs are always supported. APAR_type_list is a comma-separated list of the following types: HIPER, FileNet® Process Engine, Enhancement.
-P *fix_repository_path*	Specifies the download directory for the fix repositories that will be download by TNCPM. The default directory is **/var/tnc/tncpm/fix_repository**.
-U *user_defined_fix_repository*	Specifies the path to the user-defined fix repository. Specify the release, the technology level, and the service pack that are associated with the fix repository that is used for verification and updates of clients.
-s	Generates a report of registered service packs.
-l *SP*	Generates a report of **lslpp** information for the service pack. *SP* is in the format, REL00-TL-SP (for example, 6100-01-04 represents the service pack 04 for technology level 01 and version 6.1).
-u	Generates a report of the client update history.
-d	Generates a report of the service pack download history.
-C	Generates a report for the server certificate.
-a *SP*	Generates a report of security authorized program analysis report (APAR) information for the service pack. *SP* is in the format, REL00-TL-SP (for example, 6100-01-04 represents the service pack 04 for technology level 01 and version 6.1).
-f *filename*	Specifies the certificate file name.
-k *key_filename*	Specifies the file from which the certificate key must be read in case of an import operation.
-c	Displays the user attributes in colon-separated records, as follows: `# name: attribute1: attribute2: ...` `policy: value1: value2: ...`
-v *<signature file>*	Specifies the signature file for the IBM AIX vulnerability advisory.
-y *<advisory file>*	Specifies an IBM AIX vulnerability advisory file.
-q	Suppresses the header information.
-x *<ifix interval>*	Specifies the interval in minutes to check for and download new interim fixes. If this value is set to 0, the automatic interim fix download and notification is disabled. The default interval is every 24 hours. The supported range for the *<ifix interval>* is 30 - 525600 minutes.

Exit Status

This command returns the following exit values:

Item	Description
0	The command ran successfully, and all the requested changes are made.
>0	An error occurred. The printed error message includes more details about the type of failure.

Examples

1. To initialize TNCPM, enter the following command:

   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```

2. To create the TNCPM daemon, enter the following command:

   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```

3. To start the server, enter the following command:

   ```
   pmconf start
   ```

4. To stop the server, enter the following command:

   ```
   pmconf stop
   ```

5. To register a new technology level by using TNCPM, enter the following command:

   `pmconf add -l 6100-01`

6. To unregister a technology level from TNCPM, enter the following command:

   `pmconf delete -l 6100-01`

7. To unregister a TNC server that has an IP address of 11.11.11.11 from TNCPM, enter the following command:

   `pmconf delete -t 11.11.11.11`

8. To register a newer version of an earlier service pack to TNCPM, enter the following command:

   `pmconf add -s 6100-01-04`

9. To unregister an earlier service pack from TNCPM, enter the following command:

   `pmconf delete -s 6100-01-04`

10. To generate a report of fix repositories for each registered technology level, enter the following command:

    `pmconf list -s`

11. To generate a report of a registered technology level **lslpp** information, enter the following command:

    `pmconf list -l 6100-01-02`

12. To generate a report from the update history, enter the following command:

    `pmconf hist -u`

13. To generate a report from the download history, enter the following command:

    `pmconf hist -d`

14. To generate a report of the server certificate, enter the following command:

    `pmconf list -C`

15. To generate a report of a service pack security APAR information, enter the following command:

    `pmconf list -a 6100-01-02`

16. To import a server certificate, enter the following command:

    `pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt`

17. To export the server certificate, enter the following command:

    `pmconf export -f /tmp/server.txt`

psconf command

Purpose

Reports and manages the Trusted Network Connect (TNC) server, the TNC client, the TNC IP Referrer (IPRef), and Service Update Management Assistant (SUMA). It manages fileset and patch management policies regarding endpoint (server and client) integrity at or after network connection to protect the network from threats and attacks.

Syntax

TNC server operations:

psconf mkserver [**tncport=**<*port*>] **pmserver=**<*host*:*port*> [tsserver=<host>] [**recheck_interval=**<*time_in_minutes*> | **d** (days) : **h** (hours) : **m** (minutes)] [**dbpath** = <*user-defined directory*>] [**default_policy=**<*yes* | *no* >] [**clientData_interval=**<*time in mins* > | **d** (days) : **h** (hours) : **m** (minutes)] [**clientDataPath=**<*Full_path* >]

psconf { **rmserver** | **status** }

psconf { **start** | **stop** | **restart** } **server**

psconf chserver attribute = *value*

psconf clientData -i *host* [**-l** | **-g**]

psconf add -F *<FSPolicyname>* **-r** *<buildinfo>* [**apargrp=** [±]*<apargrp1, apargrp2.. >*] [*ifixgrp*=[+|-]*<ifixgrp1,ifixgrp2...>*]

psconf add { **-G** *<ipgroupname>* **ip**=[±]*<host1, host2...>* | {**-A***<apargrp>* [**aparlist**=[±]*apar1, apar2...* | {**-V** *<ifixgrp>* [*ifixlist*=[+|-]*ifix1,ifix2...*]}

psconf add -P *<policyname>* { **fspolicy**=[±]*<f1,f2...>* | **ipgroup**=[±]*<g1,g2...>* }

psconf add -e *emailid* [-E FAIL | COMPLIANT | ALL] [**ipgroup=** [±]*<g1,g2...>*]

psconf add -I ip= [±]*<host1, host2...>*

psconf delete { **-F** *<FSPolicyname>* | **-G** *<ipgroupname>* | **-P** *<policyname>* | **-A** *<apargrp>* | **-V** *<ifixgrp>*}

psconf delete -H -i *<host* | **ALL>* **-D** *<yyyy-mm-dd>*

psconf certadd -i *<host>* **-t** <**TRUSTED** | **UNTRUSTED**>

psconf certdel -i *<host>*

psconf verify -i *<host>* | **-G** *<ipgroup>*

psconf update [**-p**] {**-i***< host >*| **-G** *<ipgroup>* [**-r** *<buildinfo>* | **-a** *<apar1, apar2...>* | [**-u**] **-v** *<ifix1, ifix2,...>* | **-O** *<openpkggrp1, openkggrp2,...>*}

psconf log loglevel=<**info** | **error** | **none**>

psconf import -C -i *<host>* **-f** *<filename>* | **–d** *<import database filename>*

psconf { **import -k** *<key_filename>* | **export**} **-S -f** *<filename>*

| **psconf list** { **-S** | **-G** *< ipgroupname* | **ALL** *>* | **-F** *< FSPolicyname* | **ALL** *>* | **-P** *< policyname* | **ALL** *>* | **-r**
| *< buildinfo* | **ALL** *>* | **-I -i** *< ip* | **ALL** *>* | **-A** *< apargrp* | **ALL** *>* | **-V** *<ifixgrp>* | -O *<openpkggrp|ALL>*}
| [**-c**] [**-q**]

psconf list { **-H** | **-s** <**COMPLIANT** | **IGNORE** | **FAILED** | **ALL**> } **-i** *<host* | **ALL**> [**-c**] [**-q**]

psconf export -d *<path to export directory>*

psconf report -v <**CVEid**|**ALL**> **-o** <**TEXT**|**CSV**>

psconf report -A <**advisoryname**>

psconf report -P <**policyname**|**ALL**> **-o** <**TEXT**|**CSV**>

psconf report -i <**ip**|**ALL**> **-o** <**TEXT**|**CSV**>

psconf report -B <**buildinfo**|**ALL**> **-o** <**TEXT**|**CSV**>

| **psconf clientData** {**-l** | **-g**} **-i** *<ip|host>*

| **psconf add -O** *<openpkggrp>* *<openpkgname:version>*

| **psconf delete -O** *<openpkggrp>* *<openpkgname:version>*

| **psconf delete -O** *<openpkggrp>*

| **psconf delete -O ALL**

| **psconf add -O** *<openpkggrp>* **fspolicy=***<fspolicy name>*

| **psconf report -O ALL -o TEXT**

TNC client operations:

psconf mkclient [**tncport=***<port>*] **tncserver=***<host:port>*

psconf mkclient tncport=*<port>* -T

psconf { **rmclient** | **status** }

psconf {**start** | **stop** | **restart** } **client**

psconf chclient attribute = *value*

psconf list { **-C** | **-S** }

psconf export { **-C** | **-S** } **-f** *<filename>*

psconf import { **-S** | **-C -k** *<key_filename>* } **-f** *<filename>*

TNC IPRef operations:

psconf mkipref [**tncport=***<port>*] **tncserver=**<host:port>

psconf { **rmipref** | **status**}

psconf { **start** | **stop** | **restart**} ipref

psconf chipref attribute = *value*

psconf { **import -k** *<key_filename>* | **export** } **-R -f** *<filename>*

psconf list -R

Description

The TNC technology is an open standard-based architecture for endpoint authentication, platform integrity measurement, and integrating security systems. The TNC architecture inspects endpoints (network clients and servers) for compliance with security policies before allowing them on the protected network. The TNC IPRef notifies the TNC server about any new IPs that are detected on the virtual I/O server (VIOS).

SUMA helps move system administrators away from the task of manually retrieving maintenance updates from the web. It offers flexible options that enable the system administrator to set up an automated interface to download fixes from a fix distribution website to their systems.

The **psconf** command manages the network server and clients by adding or deleting security policies, validating clients as trusted or untrusted, generating reports, and updating the server and the client.

The following operations can be performed by using the **psconf** command:

Item	Description
add	Adds a policy, a client, or the email information on the TNC server.
apargrp	Specifies the APAR group names as part of the fileset policy that are used for verification of TNC clients.
aparlist	Specifies the list of APARs that are part of the APAR group.
certadd	Marks the certificate as trusted or untrusted.
certdel	Deletes the client information.
chclient	Changes the attributes in the `tnccs.conf` file. An explicit **start** command is required for the changes to take effect in the TNC client. The syntax of attribute=value will be same as that of **mkclient**.
chipref	Changes the attributes in the `tnccs.conf` file. An explicit **start** command is required for the changes to take effect in IPRef. The syntax of attribute=value is the same as that of the **mkipref**.
chserver	Changes the attributes in the `tnccs.conf` file. An explicit **start** command is required for the changes to take effect in the TNC server. The syntax of attribute=value is same as that of **mkserver**. **Note:** The **dbpath** attribute cannot be changed by using the **chserver** command. It can be set only while running the **mkserver**.
clientData	Creates a snapshot of information (operating system level and filesets installed) about the TNC client. The *clientDataPath* path identifies where the snapshot collection information is stored. The default location is in the `/var/tnc/clientData/` directory on the TNC server. You can change or set the *clientDataPath* path by using the **chserver** or **mkserver** subcommand. You can initiate the TNC client snapshot collection from the command line by running the **clientData** subcommand from the TNC server. The **clientData** subcommand that is run from the command line is independent of the **clientData_interval** interval.
clientData_interval	You can use the **chserver** or **mkserver** subcommand to configure the snapshot collection to occur at regular intervals by specifying a value for the **clientData_interval** interval. The snapshot collection starts automatically when the **clientData_interval** interval has a value other than 0 (zero). By default, the snapshot collection is disabled by the scheduler. To enable the scheduler, specify a **clientData_interval** value that is greater than or equal to 30. To disable the scheduler, specify a **clientData_interval** value of 0 (zero). The supported range for the **clientData_interval** interval is 30 - 525600 minutes.
dbpath	Specifies the TNC database location. The default value is `/var/tnc`.
default_policy	Enables or disables automatic verification of the TNC clients for the intern fix (ifix) and APARs at the same level as the client. Specify *yes* to enable automatic verification. Specify *no* to disable automatic verification. For more information about the **default_policy** subcommand, see the default_policy table.
delete	Deletes a policy or the client information.
export	Exports the client or server certificate, or database on TNC server.
fspolicy	Specifies the fileset policy of the release, technology level and service pack that are used for verification of TNC Clients.
import	Imports a certificate on client or server, or database on TNC server.

Item	Description
ipgroup	Specifies the Internet Protocol (IP) group that contains multiple client IP addresses or host names.
list	Displays information about the TNC server, the TNC client, or the SUMA.
log	Sets the log level for the TNC components.
mkclient	Configures the TNC client.
mkipref	Configures the TNC IPRef.
mkserver	Configures the TNC server.
Openpkggrp	Specifies the openpkg group name as part of fileset policy that is used to verify clients.
pmport	Specifies the port number on which the **pmserver** listens to. The default value is 38240.
pmserver	Specifies the host name or IP address of the **suma** command that downloads the latest service packs and security fixes available in the IBM® ECC website and the IBM Fix Central website.
recheck_interval	Specifies the interval in minutes or d (days) : h (hours) : m (minutes) format for the TNC server to verify the TNC clients. The supported range for the **recheck_interval** interval is 30 - 525600 minutes. **Note:** A value of **recheck_interval=0** means that the scheduler does not initiate verification of the clients at regular intervals and the registered clients are automatically verified when they start. In such cases, the client can be manually verified.
report	Generates a report that has a .txt or .csv file extension.
restart	Restarts the TNC client, the TNC server, or the TNC IPRef.
rmclient	Unconfigures the TNC client.
rmipref	Unconfigures the TNC IPRef.
rmserver	Unconfigures the TNC srever.
start	Starts the TNC client, the TNC server, or the TNC IPRef.
status	Shows the status of the TNC configuration.
stop	Stops the TNC client, the TNC server, or the TNC IPRef.
tncport	Specifies the port number on which the TNC server listens to. The default value is 42830.
tncserver	Specifies the TNC server that verifies or updates the TNC clients.
tssserver	Specifies the IP or host name of the Trusted Surveyor server.
update	Installs patches on the client.
verify	Initiates a manual verification of the client.

The following table displays the results of configuring the **default_policy** subcommand to either *yes* or *no* values:

Table 17. Results of default_policy subcommand

FSpolicy (Fileset policy)	default policy=*yes*	default policy=*no*
TNC client belongs to a fileset policy with an interim fix (iFix) and APARs groups defined	The default policy is overridden by the iFix and APARs provided in the fileset policy.	The default policy is not used. The iFix and APARs provided in the fileset policy are considered during the verification process for the TNC client.
TNC client belongs to a fileset policy without an iFix and APARs groups defined	The default policy is used with the iFix and APARs during the verification process for the TNC client. Only the iFix and APARs that match the level of the TNC client are used during the verification process.	The default policy is not used.

Flags

Item	Description
-A <advisoryName>	Specifies the advisory name for the report.
-B <buildinfo>	Specifies the build information to prepare a patch report.
-c	Displays the user attributes in colon-separated records as follows:
	`# name: attribute1: attribute2: ...`
	`policy: value1: value2: ...`
-C	Specifies that the operation is for client component.
-d *database file location/dir path of database*	Specifies the file path location for import of the database/specifies the directory path location for export of the database.
-D *yyyy-mm-dd*	Specifies the date for a particular client entry in the log history, where *yyyy* is the year, *mm* in the month, and *dd* is the day.
-e *emailid* **ipgroup=[±]***g1, g2...*	Specifies the email ID followed by a comma-separated IP group name list.
-E ∣ **FAIL** ∣ **COMPLIANT** ∣ **ALL** ∣	Specifies the event for which the emails need to be sent to the configured email id.
	FAIL- Mails are sent when the verification status of the client is FAILED.
	COMPLIANT- Mails are sent when the verification status of the client is COMPLAINT.
	ALL - Mails are sent for all the statuses of the client verification.
-f *filename*	Specifies the file from which the certificate must be read in case of an import operation, or specifies the location to which the certificate must be written in case of an export operation.
-F *fspolicy buildinfo*	Specifies the file system policy name, followed by the build information. The build information can be provided in the following format:
	`6100-04-01`, where `6100` represents version 6.1, `04` is the maintenance level, and `01` is the service pack.
-g	Run the **clientData** subcommand on the specified TNC client. This flag is available only with the **clientData** subcommand.
-G *ipgroupname* **ip=[±]***ip1, ip2...*	Specifies the IP group name followed by a comma-separated IP list.
-H	Lists the history log.
-i *host*	Specifies the IP address or host name.
-I **ip=[±]***ip1, ip2...* ∣ [±] *host1,host2...*	Specifies the IP/host name that must be ignored during verification.
-k *filename*	Specifies the file from which the certificate key must be read in case of an import operation.
-l	Lists the snapshot details on the TNC server for the specified TNC client. This flag is available only with the **clientData** subcommand.
-O <openpkggrp>	Specifies the openpkg group name for the policy.
-p	Previews the TNC client update.
-P <policyName>	Specifies the policy name to prepare a client policy report.
-q	Suppresses the header information.
-r *buildinfo*	Generates the report based on the build information. The build information can be provided in the following format:
	`6100-04-01`, where `6100` represents version 6.1, `04` is the maintenance level, and `01` is the service pack.
-R	Specifies that the operation is for IPRef component.
-s **COMPLIANT** ∣ **IGNORE** ∣ **FAILED** ∣ **ALL**	Displays the client by status as follows:
	COMPLIANT Displays the active clients.
	IGNORE Displays the clients that are excluded from any verification.
	FAILED Displays the clients that have failed verification as per the configured policy.
	ALL Displays all the clients irrespective of their statuses.
-S <host>	Specifies the host name to prepare a client security fix report.
-t **TRUSTED** ∣ **UNTRUSTED**	Marks the specified client as trusted or untrusted. **Note:** Only system administrators can verify the server or client as trusted or untrusted.
-T	Specifies that the client can accept request from any TS server that has a valid certificate.
-u	Uninstalls an interim fix that is installed on a TNC client.
-v	Specifies a comma-separated interim fix list.
-V	Specifies the interim fix group name.

Exit Status

This command returns the following exit values:

Item	Description
0	The command ran successfully, and all the requested changes are made.
>0	An error occurred. The printed error message includes more details about the type of failure.

Examples

1. To start the TNC server, enter the following command:

   `psconf start server`

2. To add a file system policy named `71D_latest` for the build 7100-04-02, enter the following command:

   `psconf add -F 71D_latest 7100-04-02`

3. To delete a file system policy named `71D_old`, enter the following command:

   `psconf delete -F 71D_old`

4. To validate that the client that has an IP address of 11.11.11.11 is **trusted**, enter the following command:

   `psconf certadd -i 11.11.11.11 -t TRUSTED`

5. To delete the client that has an IP address of 11.11.11.11 from the server, enter the following command:

   `psconf certdel -i 11.11.11.11`

6. To verify the client information that has an IP address of 11.11.11.11, enter the following command:

   `psconf verify -i 11.11.11.11`

7. To display the client information that has an IP address of 11.11.11.11, enter the following command:

   `psconf list -i 11.11.11.11`

8. To generate the report for clients that are in **COMPLAINT** status, enter the following command:

   `psconf list -s CPMPLIANT -i ALL`

9. To generate the report for the build 7100-04-02, enter the following command:

   `psconf list -r 7100-04-02`

10. To display the connection history of a client that has an IP address of 11.11.11.11, enter the following command:

    `psconf list -H -i 11.11.11.11`

11. To delete the entry of a client that has an IP address of 11.11.11.11 from the log history older or equal to 1 February, 2009, enter the following command:

    `psconf delete -H -i 11.11.11.11 -D 2009-02-01`

12. To import the client certificate of a client that has an IP address of 11.11.11.11 from the server, enter the following command:

    `psconf import -C -i 11.11.11.11 -f /tmp/client.txt`

13. To export the server certificate from a client, enter the following command:

    `psconf export -S -f /tmp/server.txt`

14. To update the client that has an IP address of 11.11.11.11 to an appropriate level from the server, enter the following command:

    `psconf update -i 11.11.11.11`

15. To display the client statuses, enter the following command:

    `psconf status`

16. To display the client certificate, enter the following command:

    `psconf list -C`

17. To start the client, enter the following command:

    `psconf start client`

18. To display the snapshot information that was gathered with the **clientData** subcommand, enter the following command:

    `psconf clientData -l [ip|host]`

19. To display the history for the TNC client, enter the following command:

    `psconf list —H —i [ip|ALL]`

Security

Attention RBAC users and Trusted AIX users:

This command can perform privileged operations. Only privileged users can run privileged operations. For more information about authorizations and privileges, see Privileged Command Database in Security. For a list of privileges and the authorizations associated with this command, see the **lssecattr** command or the **getcmdattr** subcommand

---

pscxpert command

Purpose

Aids the system administrator in setting the security configuration.

Syntax

pscxpert -l {high|medium|low|default|sox-cobit} [**-p**]

pscxpert -l {h|m|l|d|s} [**-p**]

pscxpert -f Profile [**-p**]

pscxpert -u [-p]

pscxpert -c [**-p**] [-r|-R] [-P Profile] [-l Level]

pscxpert -t

pscxpert -l <Level> [**-p**] <-a *File1* | -n *File2* | -a *File3* -n *File4*>

pscxpert -f Profile **-a** File [**-p**]

pscxpert -d

Description

The **pscxpert** command sets various system configuration settings to enable the specified 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 **-a** flags saves the security settings to a file specified by the *File* parameter. The **-f** flag then applies the new configurations.

After the initial selection, a menu is displayed itemizing all security configuration options that are 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 command.

If you run the **pscxpert** command when another instance of the **pscxpert** command is already running, the **pscxpert** command exits with an error message.

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 specified file in an abbreviated format.
-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 `/etc/security/aixpert/core/appliedaixpert.xml` file are checked. You can run this check against any default profile or custom profile.
-d	Displays the document type definition (DTD).

Item	Description
-f	Applies the security settings that are provided in the specified *Profile* file. The profiles are in the `/etc/security/aixpert/custom` 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.

NERC.xml
> This file contains the requirements for the North American Electric Reliability Corporation (NERC) settings.

NERC_to_AIXDefault.xml
> This file changes the NERC settings to the default AIX 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** flag, the 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	Sets the system security settings to the specified level. This flag has the following options:

h|high Specifies high-level security options.

m|medium
 Specifies medium-level security options.

l|low Specifies low-level security options.

d|default
 Specifies AIX standards-level security options.

s|sox-cobit
 Specifies the Sarbanes-Oxley Act and COBIT security options.
If you specify both the **-l** and **-n** flags, the security settings are not implemented on the system; however, they are only written to the specified file.

All 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.

Attention: When you use the **d|default** flag, the flag can overwrite the configured security settings that you had previously set by using the **pscxpert** command or independently, and restores the system to its traditional open configuration.

Item	Description
-n	Writes the settings with the associated security level options to the specified file.
-p	Specifies that the output of the security rules is displayed by using verbose output. The **-p** flag logs the rules that are processed in to the audit subsystem if the **auditing** option is turned on. This option can be used with any of the **-l**, **-u**, **-c**, and **-f** flags.
-P	Accepts the profile name as input. This option is used along with the **-c** flags. The **-c** and **-P** flags are used to check the compatibility of the system with the profile passed.
-r	Writes the existing settings of the system to the `/etc/security/aixpert/check_report.txt` 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 **-r** flag, but this flag also appends a description about each script or program that is used to implement the configuration setting.
-t	Displays the type of the profile that is applied on the system.
-u	Undoes the security settings that are applied. **Note:** You cannot use the **-u** flag to reverse the application of the DoD, DoDv2, NERC, PCI, or PCIv3 profiles. To remove these profiles after they are added, apply the profile that ends with `_AIXDefault.xml`. For example, to remove the NERC.xml profile, you must apply the NERC_to_AIXDefault.xml profile.

Parameters

Item	Description
File	The output file that stores the security settings. Root permission is required to access this file.
Level	The custom level to check against the previously applied settings.
Profile	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

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

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

   After you run 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 in to the audit subsystem, enter the following command:

   `pscxpert -c -p`

5. To check the custom level of the security settings for the NERC profile on the system, and to log the rules that failed in to the audit subsystem, enter the following command:

   `pscxpert -c -p -l NERC`

6. To generate reports and to write them to the `/etc/security/aixpert/check_report.txt` file, enter the following command:

   `pscxpert -c -r`

Location

Item	Description
/usr/sbin/pscxpert	Contains the **pscxpert** command.

Files

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

rmvfilt command

Purpose

Removes the virtual LAN-crossing filter rules from the filter table.

Syntax

rmvfilt -n [**fid**|**all**>]

Description

The **rmvfilt** command is used to remove the virtual LAN-crossing filter rules from the filter table.

Flags

-n Specifies the ID of the filter rule that will be removed. The `all` option is used to remove all the filter rules.

Exit Status

This command returns the following exit values:

0 Successful completion.

>0 An error occurred.

Examples

1. To remove all the filter rules or to deactivate all the filter rules in the kernel, type the command as follows:

   ```
   rmvfilt -n all
   ```

Related concepts:

"Deactivating rules" on page 119
You can deactivate rules that enable cross-VLAN routing in the Trusted Firewall feature.

vlantfw command

Purpose

Displays or clears the IP and Media Access Control (MAC) mapping information, and controls the logging function.

Syntax

vlantfw -h | **-s** | **-t** | **-d** | **-f** | **-G** | **-q** | **-D** | **-E** | **-F** | **-i** | **-l** | **-L** | **-m** | **-M** | **-N** *integer*

Description

The **vlantfw** command displays or clears the IP and MAC mapping entries. It also provides the ability to start or stop the Trusted Firewall logging facility.

Flags

-d Displays all the IP mapping information.

-D Displays the collected connection data.

-E Displays the connection data between logical partitions (LPARs) on different central processor complexes.

-f Removes all the IP mapping information.

-F Clears the connection data cache.

-G Displays the filter rules that can be configured to route the traffic internally by using Trusted Firewall.

-I Displays the connection data between LPARs that are associated with different VLAN IDs, but share the same central processor complexes.

-l Starts the Trusted Firewall logging facility.

-L Stops the Trusted Firewall logging facility and redirects the trace file contents to the `/home/padmin/svm/svm.log` file.

-m Enables Trusted Firewall monitoring.

-M Disables Trusted Firewall monitoring.

-q Queries the secure virtual machine status.

-s Starts the Trusted Firewall.

-t Stops the Trusted Firewall.

Parameters

-N *integer*
> Displays the filter rule that corresponds to the integer that is specified.

Exit Status

This command returns the following exit values:

0 Successful completion.

>0 An error occurred.

Examples

1. To display all the IP mappings, type the command as follows:

   `vlantfw -d`

2. To remove all the IP mappings, type the command as follows:

   `vlantfw -f`

3. To start the Trusted Firewall logging function, type the command as follows:

   `vlantfw -l`

4. To check the status of a secure virtual machine, type the command as follows:

   `vlantfw -q`

5. To start trusted firewall, type the command as follows:

   `vlantfw -s`

6. To stop trusted firewall, type the command as follows:

   `vlantfw -t`

7. To display the corresponding rules that can be used to generate filters that route traffic within the central processor complex, type the command as follows:

   `vlantfw -G`

Related reference:

"genvfilt command" on page 152

Notices

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

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
US

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

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 jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. 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 provide in any way it believes appropriate without incurring any obligation to you.

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

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 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 Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

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

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

Index

IBM ®

Printed in USA