IBM PowerSC

Express Edition

Version 1.1.0, 1.1.1, and 1.1.2

PowerSC Express Edition

IBM PowerSC

Express Edition

Version 1.1.0, 1.1.1, and 1.1.2

PowerSC Express Edition

Note
Before using this information and the product it supports, read the information in "Notices" on page 35.

This edition applies to IBM PowerSC Express Version 1.1.2.0, or earlier, and to all subsequent releases and modifications until otherwise indicated in new editions.

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 Express Edition 1.1.2, or earlier

Read about new or significantly changed information for the What's new in the PowerSC™ Express Edition 1.1.2, or earlier, topic collection.

How to see what's new or changed

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

May 2013

Added a table that describes how the AIX Security Expert feature ensures compliance with the Payment card industry data security standards to “Payment card industry Data Security Standard compliance” on page 10.

November 2012

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

- Added documentation that describes the Real Time Compliance feature in “PowerSC Real Time Compliance” on page 33.
- Added documentation for the support of the standards as defined by the “Health Insurance Portability and Accountability Act (HIPAA)” on page 22.

PowerSC Express Edition Release Notes Versions 1.1.2, or earlier

The release notes contain information about changes to PowerSC Express Edition Versions 1.1.2, or earlier, that were identified after the documentation was completed.

What's new

- The PowerSC Real Time Compliance feature provides monitoring to ensure that enabled AIX systems remain compliant and secure. You can configure PowerSC Real Time Compliance to send alerts when changes result in a noncompliant system. For more information about PowerSC Real Time Compliance, see "PowerSC Real Time Compliance" on page 33.
- PowerSC supports the compliance of the Health Insurance Portability and Accountability Act (HIPAA) standard. For more information about this support, see "Health Insurance Portability and Accountability Act (HIPAA)" on page 22.

Read this before installation

To view the most current version of the Release Notes, go to the online Release Notes in the Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSNRQU_1.1.2/com.ibm.powersc112.ee/powersc_ee_rn.htm).

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

Note: This software might contain errors that could result in a critical business impact. Install the latest available fixes prior to using this software. To learn more about installing the PowerSC Express Edition software, see "Installing PowerSC Express Edition 1.1.2, or earlier" on page 7.

System requirements

The PowerSC Real Time Compliance feature must be installed on an AIX operating system at the following levels:

- 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

Installation, migration, upgrade, and configuration information

For information about installing PowerSC, see "Installing PowerSC Express Edition 1.1.2, or earlier" on page 7.

Limitations and restrictions

A readme file is installed with the package in the `/etc/security/aixpert` directory and is given the `README.ICEexpress` file name. This file contains the implementation details for all three profiles: Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act and COBIT compliance (SOX/COBIT), and United States Department of Defense (DoD) Security Technical Implementation Guides (STIG).

PowerSC Express Edition 1.1.2, or earlier, concepts

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

PowerSC Express Edition 1.1.2, or earlier, provides security and control of the systems operating within a cloud or in virtualized data centers, and provides an enterprise view and management capabilities. PowerSC Express Edition is a suite of features that includes Security and Compliance Automation and Real Time Compliance. The security technology that is placed within the virtualization layer provides additional security to stand-alone systems.

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

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

Components	Description	Operating system supported	Hardware supported
Security and Compliance Automation	Automates the setting, monitoring, and auditing of security and compliance configuration for the following standards: • 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	• POWER5 • POWER6® • POWER7®
Real Time Compliance	Monitors an enabled AIX system to maintain security and provides alerts when a change to the system violates a rule that is identified in the configuration policy.	• AIX 6.1 • AIX 7.1	There is no specific hardware requirement.

Installing PowerSC Express Edition 1.1.2, or earlier

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

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

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

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

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

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

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 Express Edition installation image.

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

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

Security and Compliance Automation

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

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

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

The PowerSC Express Edition installation package, 5765-G82, must be installed on AIX managed systems. The installation package installs the `powerscExp.ice` fileset that can be implemented on the system by using the AIX Profile Manager or the **aixpert** 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.

Security and Compliance Automation concepts

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

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

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

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

Department of Defense STIG compliance

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

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

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

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 12 commandments.

The 12 commandments of the IT security that are defined by PCI DSS include the following items:

1. Install and maintain a firewall configuration to protect the data of the cardholder.
2. Avoid the use of vendor-supplied defaults for system passwords and other security parameters.
3. Protect the stored data of the cardholder.
4. Encrypt the data of the cardholder, when you transmit the data across open public networks.
5. Use antivirus software or programs and regularly update the applications.
6. Develop and maintain secure systems and applications.
7. Restrict access to the data of the cardholder, depending on the business requirement.
8. Assign a unique ID to each person who has access to the computer.
9. Restrict physical access to the data of the cardholder.
10. Track and monitor all access to network resources and the cardholder data.
11. Regularly test the security systems and processes.
12. Maintain a policy that includes information security for employees and contractors.

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

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

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

Table 2. Settings related to the PCI DSS compliance standard

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
2.1	Always change vendor-supplied defaults before installing a system on the network. For example, include passwords, simple network management protocol community strings, and eliminate unnecessary accounts.	Sets the minimum number of weeks that must pass before you can change a password to 0 weeks.	**Location** /etc/security/aixpert/bin/chusrattr **Compliant value** minage=0
8.5.9	Change user passwords at least every 90 days.	Sets the maximum number of weeks that a password is valid to 13 weeks.	**Location** /etc/security/aixpert/bin/chusrattr **Compliant value** maxage=13
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.	**Location** /etc/security/aixpert/bin/chusrattr **Compliant value** maxexpired=8
8.5.10	Require a minimum password length of at least 7 characters.	Sets the minimum password length to 7 characters.	**Location** /etc/security/aixpert/bin/chusrattr **Compliant value** minlen=7
8.5.11	Use passwords that contain both numeric and alphabetic characters.	Sets the minimum number of alphabetic characters that are required in a password to 1. This setting ensures that the password contains alphabetic characters.	**Location** /etc/security/aixpert/bin/chusrattr **Compliant value** minalpha=1
8.5.11	Use passwords that contain both numeric and alphabetic characters.	Sets the minimum number of non-alphabetic characters that are required in a password to 1. This setting ensures that the password contains nonalphabetic characters.	**Location** /etc/security/aixpert/bin/chusrattr **Compliant value** minother=1
2.1	Always change vendor-supplied defaults before installing a system on the network. For example, include passwords, simple network management protocol community strings, and eliminate unnecessary accounts.	Sets the maximum number of times that a character can be repeated in a password to 8. This setting indicates that a character in a password can be repeated an unlimited number of times as long as it conforms to the other password limitations.	**Location** /etc/security/aixpert/bin/chusrattr **Compliant value** maxrepeats=8
8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	Sets the number of weeks before a password can be reused to 52.	**Location** /etc/security/aixpert/bin/chusrattr **Compliant value** histexpire=52

Table 2. Settings related to the PCI DSS compliance standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	Sets the number of previous passwords that you cannot reuse to 4.	**Location** `/etc/security/aixpert/bin/chusrattr` **Compliant value** histsize=4
8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Sets the number of consecutive unsuccessful login attempts that disables an account to 6 attempts for each non-root account.	**Location** `/etc/security/aixpert/bin/chusrattr` **Compliant value** loginretries=6

8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Sets the number of consecutive unsuccessful login attempts that disables a port to 6 attempts.	**Location**
			`/etc/security/aixpert/bin/chdefstanza`
			`/etc/security/login.cfg`
			Compliant value
			logindisable=6

8.5.14	Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	Sets the duration of time that a port is locked after it is disabled by the *logindisable* attribute to 30 minutes.	**Location**
			`/etc/security/aixpert/bin/chdefstanza`
			`/etc/security/login.cfg`
			Compliant value
			loginreenable=30

12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	Disables the remote root login function by setting its value to false. The system administrator can activate the remote login function as needed, and then deactivate it when the task is complete.	**Location**
			`/etc/security/aixpert/bin/chuserstanza`
			`/etc/security/user`
			Compliant value
			rlogin=false root

8.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	Enables the function that ensures that all users have a unique user name before they can access system components or card holder data by setting that function to a value of true.	**Location**
			`/etc/security/aixpert/bin/chuserstanza`
			`/etc/security/user`
			Compliant value
			login=true root

10.2	Enable auditing on the system.	Enables auditing of the binary files on the system.	**Location** `/etc/security/aixpert/bin/pciaudit` **Compliant value** h
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the `lpd` daemon.	Stops the `lpd` daemon and comments out the corresponding entry in the `/etc/inittab` file that automatically starts the daemon.	**Location** `/etc/security/aixpert/bin/comntrows` **Compliant value** lpd: /etc/inittab : d
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the Common Desktop Environment (CDE).	Disables the CDE function when the layer four traceroute (LFT) is not configured.	**Location** `/etc/security/aixpert/bin/comntrows` **Compliant value** "dt" "/etc/inittab" ":" d

Table 2. Settings related to the PCI DSS compliance standard (continued)

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

Table 2. Settings related to the PCI DSS compliance standard (continued)

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

Table 2. Settings related to the PCI DSS compliance standard (continued)

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

Table 2. Settings related to the PCI DSS compliance standard (continued)

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

Table 2. Settings related to the PCI DSS compliance standard (continued)

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

Table 2. Settings related to the PCI DSS compliance standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes `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.	**Location** `/etc/security/aixpert/bin/cominetdconf` **Compliant value** dtspc tcp `d`
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes 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.	**Location** `/etc/security/aixpert/bin/cominetdconf` **Compliant value** ttdbserver tcp `d`
1.1.5 2.2.2	Disable unnecessary and insecure services, which includes the `cmsd` service.	Stops and disables all instances of the `cmsd` service. The AIX Security Expert utility also comments out the corresponding entry in the `/etc/inetd.conf` file that automatically starts the service.	**Location** `/etc/security/aixpert/bin/cominetdconf` **Compliant value** cmsd udp `d`

2.2.3	Configure system security parameters to prevent misuse.	Removes the Set User ID (SUID) commands.	**Location**
			`/etc/security/aixpert/bin/rmsuidfrmrcmds`
			Compliant value
			`r`

2.2.3	Configure system security parameters to prevent misuse.	Enables the lowest security level for the File Permissions Manager.	**Location**
			`/etc/security/aixpert/bin/filepermgr`
			Compliant value
			`l`

2.2.3	Configure system security parameters to prevent misuse.	Enables the security parameters that are provided by the Network File System protocol.	**Location**
			`/etc/security/aixpert/bin/nfsconfig`
			Compliant value
			`e`

2.2.2	Enable only necessary and secure services, protocols, daemons, and so on, as required for the correct function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	Disables the `rlogind`, `rshd`, and `tftpd` daemons, which are not secure.	**Location**
			`/etc/security/aixpert/bin/disrmtdmns`
			Compliant value
			`d`

Table 2. Settings related to the PCI DSS compliance standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)

2.2.2	Enable only necessary and secure services, protocols, daemons, and so on, as required for the correct function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	Disables the `rlogind`, `rshd`, and `tftpd` daemons, which are not secure.	**Location**
			`/etc/security/aixpert/bin/rmrhostsnetrc`
			Compliant value
			`h`

2.2.2	Enable only necessary and secure services, protocols, daemons, and so on, as required for the correct function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	Disables the `logind`, `rshd`, and `tftpdpci_rmetchostsequiv` daemons, which are not secure.	**Location** `/etc/security/aixpert/bin/rmetchostsequiv` **Compliant value** No compliant value is required.
1.3.6	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.	**Location** `/etc/security/aixpert/bin/ntwkopts` **Compliant value** clean_partial_conns=1 s
1.3.6	Implement stateful inspection, or packet filtering, in which only established connections are allowed on the network.	Enables TCP security by setting the network **`tcp_tcpsecure`** option to a value of 7. This setting provides protection against data, reset (RST), and TCP connection request (SYN) attacks.	**Location** `/etc/security/aixpert/bin/ntwkopts` **Compliant value** tcp_tcpsecure=7 s
	Protect unauthorized access to unused ports.	Sets up the system to shun the hosts for 5 minutes to prevent other systems from accessing unused ports.	**Location** `/etc/security/aixpert/bin/ipsecshunhosthls` **Compliant value** No compliant value is required.
	Protect the host from port scans.	Sets up the system to shun vulnerable ports for 5 minutes, which prevents port scans.	**Location** `/etc/security/aixpert/bin/ipsecshunports` **Compliant value** No compliant value is required.
	Limit object creation permissions.	Sets default object creation permissions to 22.	**Location** `/etc/security/aixpert/bin/chusrattr` **Compliant value** umask=22

	Limit system access.	Makes the root ID the only one that is listed in the `cron.allow` file and removes the `cron.deny` file from the system.	**Location**
			`/etc/security/aixpert/bin/limitsysacc`
			Compliant value
			`h`

Table 2. Settings related to the PCI DSS compliance standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)
	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	**Location** `/etc/security/aixpert/bin/rmdotfrmpathroot` **Compliant value** No compliant value is required.
	Remove dot from the non-root path:	Removes the dots from *PATH* environment variable in the following files that are in the user home directory: • .cshrc • .kshrc • .login • .profile	**Location** `/etc/security/aixpert/bin/rmdotfrmpathnroot` **Compliant value** No compliant value is required.

	Limit system access.	Adds the root user capability and user name in the `/etc/ftpusers` file.	**Location**
			`/etc/security/aixpert/bin/chetcftpusers`
			Compliant value
			`a`

	Remove the guest account.	Removes the guest account and its files.	**Location** `/etc/security/aixpert/bin/execmds` **Compliant value** "rmuser guest; rm -rf /home/guest; ODMDIR=/etc/objrepos odmdelete -qloc0=/home/guest -o inventory"
	Prevent launching programs in content space.	Enables the stack execution disable (SED) feature.	**Location** `/etc/security/aixpert/bin/sedconfig` **Compliant value** No compliant value is required.
	Ensure that the password for root is not weak.	Starts a root password integrity check against the root password, thereby ensuring a strong root password.	**Location** `/etc/security/aixpert/bin/chuserstanza` **Compliant value** /etc/security/user dictionlist=`/etc/security/aixpert/dictionary/English rootpci_rootpwdintchk`

8.5.15	Limit access to the system by setting the session idle time.	Sets the idle time limit to 15 minutes. If the session is idle for longer than 15 minutes, you must reenter the password.	**Location**
			`/etc/security/aixpert/bin/autologoff`
			Compliant value
			`900`

Table 2. Settings related to the PCI DSS compliance standard (continued)

Implements these PCI DSS standards	Implementation specification	The AIX Security Expert implementation	Location of the value and the setting that is required for compliance (when applicable)

	Limit traffic access to cardholder information.	Sets the TCP traffic regulation to its high setting, which enforces denial-of-service mitigation on ports.	**Location**
			`/etc/security/aixpert/bin/tcptr_aixpert`
			Compliant value
			`pci`

	Maintain a secure connection when migrating data.	Enables automated IP Security (IPSec) tunnel creation between Virtual I/O Servers during live partition migration.	**Location**
			`/etc/security/aixpert/bin/cfgsecmig`
			Compliant value
			`on`

1.3.5	Limit packets from unknown sources.	Allows the packets from the Hardware Management Console.	**Location** `/etc/security/aixpert/bin/ipsecpermithostorport` **Compliant value** No compliant value is required.
5.1.1	Maintain antivirus software.	Maintains the system integrity by detecting, removing, and protecting against known types of malicious software.	**Location** `/etc/security/aixpert/bin/manageITsecurity` **Compliant value** No compliant value is required.
	Maintain access on an as needed basis.	Enable role-based access control (RBAC) by creating system operator, system administrator, and information system security officer user roles with the required permissions.	**Location** `/etc/security/aixpert/bin/EnableRbac` **Compliant value** No compliant value is required.

Related information:

Payment card industry DSS compliance

Sarbanes-Oxley Act and COBIT compliance

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

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

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

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

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

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

Related information:

COBIT compliance

Sarbanes-Oxley (SOX) compliance

Health Insurance Portability and Accountability Act (HIPAA)

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

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

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

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

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

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

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

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

Table 3. 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 3. 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 3. 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 3. 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 3. 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 4. 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 4. 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**, **sa** users and assigns appropriate roles to the users.	Suggests that you create **isso**, **so**, **sa** users. Assigns appropriate roles to the users.	**Command**: **/etc/security/aixpert/bin/ RbacEnablement**.

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:

```
aixpert –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 **aixpert** 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 5. PowerSC commands for AIX

Command	Compliance standard
% aixpert -f /etc/security/aixpert/custom/DoD.xml	*US Department of Defense UNIX security technical implementation guide*
% aixpert -f /etc/security/aixpert/custom/PCI.xml	*Payment card industry-Data security standard*
% aixpert -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 6. 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/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 **aixpert** 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 27
Learn about the process of planning and deploying PowerSC Security and Compliance Automation profiles on a group of systems in accordance with the accepted IT governance and compliance procedures.

Configuring PowerSC compliance with AIX Profile Manager

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

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

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

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

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

For the deployment to be successful for DoD, PCI, or SOX, PowerSC Express Edition or PowerSC Standard Edition must be installed at the end point of the AIX system. If the system that is being deployed does not have PowerSC installed, the deployment fails. The IBM Systems Director deploys the configuration template to the selected AIX system end points and configures them according to the compliance requirements.

Related information:

AIX Profile Manager

IBM Systems Director

PowerSC Real Time Compliance

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

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

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

Installing PowerSC Real Time Compliance

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

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

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

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 **aixpert** command, and the other is to use the AIX Profile Manager with IBM Systems Director.

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

Setting alerts for PowerSC Real Time Compliance

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

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

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

Related information:

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

Notices

This information was developed for products and services offered in the U.S.A. This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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
Armonk, NY 10504-1785
U.S.A.

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

IBM Corporation
Dept. LRAS/Bldg. 903
11501 Burnet Road
Austin, TX 78758-3400
U.S.A.

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

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.

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

Index

Printed in USA