Installation Guide

NetIQ® Security Solutions for iSeries

September 10, 2008

Contents

About This Book and the Library

The installation guide provides detailed planning and installation information about the NetIQ Security Solutions for iSeries product. This book guides you through the installation process and helps you make the correct decisions.

Intended Audience

This book provides information for individuals responsible for installing NetIQ Security Solutions for iSeries products on an iSeries server.

Other Information in the Library

The library provides the following information resources:

Trial Guide

Provides general information about the product and guides you through the trial and evaluation process.

User Guides

Provide conceptual information about the NetIQ Security Solutions for iSeries product. These books also provide an overview of the user interfaces and the Help. The following user guides are available:

- NetIQ Security Solutions for iSeries - PSAudit
- NetIQ Security Solutions for iSeries - PSSecure
- NetIQ Security Solutions for iSeries - Remote Request Management
- NetIQ Security Solutions for iSeries - PSDetect
- NetIQ Security Solutions for iSeries - PSPasswordManager
- NetIQ Security Solutions for iSeries - Privilege Manager

Help

Provides definitions for each screen and each field.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and CD-ROM titles • Variable names and values • Emphasized words
`Fixed Font`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface
Brackets, such as [*value*]	• Optional parameters of a command
Braces, such as {*value*}	• Required parameters of a command
Logical OR, such as *value1* | *value2*	• Exclusive parameters. Choose one parameter.

About NetIQ Corporation

NetIQ Corporation, an Attachmate business, is a leading provider of comprehensive systems and security management solutions that help enterprises maximize IT service delivery and efficiency. With more than 12,000 customers worldwide, NetIQ solutions yield measurable business value and results that dynamic organizations demand. Best-of-breed solutions from NetIQ Corporation help IT organizations deliver critical business services, mitigate operational risk, and document policy compliance. The company's portfolio of award-winning management solutions includes IT Process Automation, Systems Management, Security Management, Configuration Control and Enterprise Administration. For more information, please visit www.netiq.com

Contacting NetIQ Corporation

Please contact us with your questions and comments. We look forward to hearing from you. For support around the world, please contact your local partner. For a complete list of our partners, please see our Web site. If you cannot contact your partner, please contact our Technical Support team.

Telephone: 713-418-5000
888-323-6768 (only in the United States and Canada)

Sales Email: info@netiq.com

Support: www.netiq.com/support

Web Site: www.netiq.com

Chapter 1
Introduction

Information security is a primary concern for most companies today. You struggle to protect sensitive business information from intentional threats and from accidental damage. New security problems emerge daily. With networks connected to the Internet and intranets, client-server connections, and distributed enterprises, your information is at risk on more fronts than ever before. Supporting remote access services translates into more vulnerabilities that intruders can, and will, exploit.

Many people consider the IBM iSeries to be one of the most secure servers available. The operating system has excellent built-in security features, but you must optimize your iSeries server configuration to guarantee the level of security your business demands. You need to periodically verify the settings to ensure someone else does not undo your effort.

When intruders attempt to gain access to your system or change security settings, you need a mechanism to alert you and immediately respond. The native operating system offers no way to detect or alert you to these possible security breaches. Without event management and response, you could be unaware of intrusions until after damage is done.

NetIQ Security Solutions for iSeries provide the most comprehensive, industry-leading solution for managing security in iSeries environments. This suite of integrated products assesses vulnerabilities, audits and reports on all aspects of security, automates event management and response, secures your iSeries servers, manages user profiles and passwords, and controls access to managed servers through privilege escalation. The product includes award-wining remote server exit point management to monitor and control who can access your iSeries servers.

What Is NetIQ Security Solutions for iSeries?

NetIQ Security Solutions for iSeries is a suite of integrated products including PSAudit, PSSecure, PSDetect, Privilege Manager, and PSPasswordManager. These products simplify security auditing, vulnerability assessment, user access control, event management, and privilege escalation for iSeries servers. NetIQ Security Solutions for iSeries include solutions for managing user profiles and enforcing and strengthening password policies.

These products simplify security management and automate routine security tasks to make securing and maintaining security in iSeries environments manageable. Powerful auditing and reporting, remote and local access control, and real-time incident detection, combined with powerful user profile management, help you minimize security risks and maintain service level agreements for availability.

NetIQ Security Solutions for iSeries reduce security risks and ensures availability by providing the following capabilities:

- Vulnerability assessment and auditing
- Comprehensive library of audit reports
- System hardening and security management
- Remote access control using exit point programs
- Real-time event management and response
- User profile and password management
- Privilege escalation

Besides providing a comprehensive set of security features for iSeries servers, NetIQ Security Solutions for iSeries integrate with other NetIQ Corporation enterprise applications to provide an integrated security solution for heterogeneous environments:

- **NetIQ Secure Configuration Manager** assesses policy compliance, identifies security vulnerabilities, and helps you correct exposures before they result in failed audits, security breaches, or costly downtime. Secure Configuration Manager centralizes vulnerability management across heterogeneous systems and multiple iSeries servers while saving substantial staff time.
- NetIQ Security Solutions for iSeries can send alerts to **NetIQ Security Manager** to monitor security incidents across multiple platforms from a central console. Using NetIQ Security Solutions for iSeries with Security Manager also delivers an archival and forensics solution for managing event logs from iSeries and other servers throughout your enterprise
- Use NetIQ Security Solutions for iSeries with **NetIQ AppManager** to monitor performance and availability of your iSeries and other servers.

For more information about these and other NetIQ products, see the Web site at www.netiq.com.

What NetIQ Security Solutions for iSeries Provide

NetIQ Security Solutions for iSeries provide the following product components that assess, secure, and detect critical changes on your iSeries servers. In addition, the product includes password management to keep your iSeries servers secure and simplify user profile and password management.

You can meet your most demanding security management objectives using NetIQ Security Solutions for iSeries to:

- Assess the current state of security of your iSeries servers
- Maintain security compared to a known baseline state
- Audit changes to files at the field and record level
- Control and log access to applications and data

- Detect and respond to events in real time
- Log and report event activity
- Report users with weak passwords
- Send messages or disable profiles if passwords do not comply
- Implement effective change control on servers
- Run object access failure reports to assure policy and regulatory compliance
- Increase operational security of your servers using just-in-time authorities and granular access control
- Ensure required changes are implemented and validated

Using NetIQ Security Solutions for iSeries, you can configure and maintain your iSeries servers to minimize vulnerabilities and protect your valuable data assets.

NetIQ Security Solutions for iSeries consist of the following products that simplify security auditing, vulnerability assessment, user access control, privilege escalation, and event management for iSeries servers.

PSAudit

Provides scored system check-up, one of almost 200 reports, to analyze system health. You can run reports on demand or on a regular schedule. Audits field and record level changes, storing before and after values of changed data.

Analyzes job logs even for jobs not configured to produce job logs. Security baseline reports check system settings against a saved snapshot to help maintain the security measures you implement.

PSSecure

Uses exit point programs to prevent unauthorized remote access, such as FTP, TELNET, SQL, or ODBC requests. Provides convenient user, command, and IP address groups to simplify access rules. Provides a test environment so you can verify security rules before you roll them out. Simplifies object-level management and compliance using templates.

Locates and addresses unused user profiles. Synchronizes user profiles and passwords across multiple iSeries servers. Controls inactive session termination for each computer rather than by server. Audits changes to edited files. Builds secure menus to control access to applications.

PSDetect

Monitors message queues including the QHST and QSYSOPR queues. Notifies security teams of alerts, such as invalid sign on attempts by powerful users, sign on attempts outside permitted hours, unauthorized FTP access, or unauthorized creation of user profiles. Automatically logs and responds to alerts with email, pages, SNMP traps, or commands.

Sends SNMP traps or alerts to other NetIQ security products including AppManager, or Security Manager. Monitors many events including changes to system values, QSECOFR sign on, or remote access denied by PSSecure.

PSPasswordManager

Identifies and manages users with passwords not meeting rules defined in the QPWD* system values or other rules you define. Includes 124,000-word dictionary that you can customize to check for password strength.

Responds to users with weak passwords by notifying them or disabling their profiles when passwords do not meet defined policy. Includes password validation enforcement for native CHGPWD command.

Privilege Manager

Provides the escalated privilege solution you need to limit widespread authorities, show continuous regulatory compliance, and increase operational integrity. Built-in auditing and reporting help you meet your compliance objectives.

Limits regular access to your sensitive servers to a onetime or regularly scheduled maintenance window and assign the task to a specific user or user group.

How Customers Use NetIQ Security Solutions for iSeries

Many Fortune 500 companies, as well as small and mid-size companies, use NetIQ Security Solutions for iSeries to audit, monitor, and control security in their iSeries environments. See how the following companies put NetIQ Security Solutions for iSeries to work with great results.

Security for Remote Access EFT

A leading provider of integrated computer systems and services for the banking industry provides data processing solutions operating primarily on IBM iSeries servers. The company sells products and services to more than 2,800 financial institutions with assets of up to $10 billion. Their customers demand the highest level of security for every transaction. Many transactions occur over the Internet, through Electronic Funds Transfer (EFT), or from other remote connections.

The company chose NetIQ Security Solutions for iSeries to establish and implement strong auditing and security standards at multiple geographic locations. According to the electronic services general manager:

- *NetIQ Security Solutions for iSeries are critical components in helping us more effectively predict, plan, and manage security and auditing on our iSeries systems, so that we can continue to provide the best, most secure banking transactions and account processing services to our clients.*
- *NetIQ's best-of-breed expertise in iSeries security and auditing gives us the robust, yet easy-to-manage audit and security functions that we need for our iSeries systems, and ensures that our clients' demands for the highest level of security with every transaction are met.*

Result: Consistently audits for vulnerabilities to simply and easily ensure high-level security for client transactions.

Scalable Security for Distributed Installation

A large office superstore business uses NetIQ Security Solutions for iSeries for internal corporate IT security and audits on its 10 IBM iSeries servers and 25,000 user profiles. Using NetIQ Security Solutions for iSeries, the company implemented rigorous auditing and security policies company-wide to prevent unauthorized data access.

Because store managers throughout the United States require remote access to the iSeries servers, it is vital that the security team provide highly secure connectivity to its remote users. The security team uses NetIQ Security Solutions for iSeries to meet the following requirements:

- Ensure appropriate access to internal systems and files
- Track changes to system configuration
- Perform regular, automated system security audits
- Detect and alert on unauthorized activity

The enterprise security manager reports:

- *Providing bulletproof IT security that protects our valuable data assets is my number one priority, but it is a very time-consuming task. My teams spends literally thousands of hours ever year trying to maintain the levels of security that our business demands.*
- *Additionally, with our consistent rapid growth rate of adding a new store approximately every 50 hours, we need a highly scalable security solution that can grow with the demands of our business.*
- *Fortunately, the NetIQ Security Solutions for iSeries enable us to implement highly sophisticated security controls on our iSeries platforms, while at the same time dramatically reduces the amount of time the team must spend managing iSeries security.*

Results: Reduced training and management time to provide top-notch security in a rapidly changing, distributed environment.

Faster, Easier Audit Compliance

A large regional bank relies on NetIQ Security Solutions for iSeries to help meet FDIC audit requirements. The vice president of data processing at the bank shares the problems his team faced before installing NetIQ Security Solutions for iSeries:

- *A few years ago, FDIC auditors recommended that we make our systems more secure. However, the FDIC auditors didn't tell us how to better secure our systems - they just told us we needed to do it.*
- *As a result of their feedback, we hired a consulting company to come in and tell us everything that we needed to check on our systems on a regular basis.*
- *During their engagement, they pointed out a lot of things in the native iSeries environment that we could use to help us with some of our audit reporting, but using the native features turned out to be very time-consuming, labor-intensive, and cumbersome.*

The bank now uses NetIQ Security Solutions for iSeries for daily auditing and exit point control to manage remote access to their systems. The internal auditor can run daily audit reports in minutes to track who is doing what on the iSeries servers when, including:

- Users attempting actions outside their user profile permissions
- Users making changes to or deleting crucial files
- Users attempting to access critical files outside normal application menus or access times

Results: Appropriate remote access security on iSeries servers with faster routine audits.

How NetIQ Security Solutions for iSeries Help You

NetIQ Security Solutions for iSeries deliver powerful vulnerability assessment, access control, security auditing, real-time monitoring, privilege escalation, and user password management to help you eliminate security risks and maintain business continuity across your iSeries servers. The product simplifies security management and automates routine security tasks across your entire iSeries environment to help you achieve the following objectives:

- Ensure and report on compliance with information security policies
- Protect access to information assets on iSeries servers
- Proactively alert you and respond to intrusions or malicious activity
- Increase compliance and ensure operational integrity
- Integrate iSeries systems into company-wide, cross-platform security initiatives

Using NetIQ Security Solutions for iSeries, you can configure and maintain your systems to minimize vulnerabilities, protect critical resources and assets, control user access, and enforce password security.

NetIQ Security Solutions for iSeries also let you detect and respond to intrusions and other security threats in real time. Its award-winning remote access management lets you track, monitor, and control who can access iSeries systems and what resources they can access while connected.

Quickly Assesses Vulnerability and Security

NetIQ Security Solutions for iSeries provide auditing tools to help you assess and report on security of all the iSeries systems in your environment. Use NetIQ Security Solutions for iSeries to meet the following security auditing challenges:

- Reporting on changes to user profiles or object authorities
- Tracking local and remote access activity by user
- Monitoring changes to sensitive files
- Comparing system security settings to a baseline file

NetIQ Security Solutions for iSeries run reports on schedule or on demand to help you quickly audit changes that can indicate unsafe configurations, known vulnerabilities, and other security issues.

Secures Remote Access to iSeries

You need to ensure users can access required services while controlling access to critical data. NetIQ Security Solutions for iSeries let you control who can use specific services on which servers while you maintain secure access to sensitive assets by providing the following access control services:

- Remote access control
- System Object ownership and control
- Application access control

In addition to access control, NetIQ Security Solutions for iSeries synchronize passwords and user profiles across multiple iSeries systems to streamline and simplify these time-consuming user-provisioning tasks.

Leaving a session logged on when users leave their computers is an invitation for intrusions. NetIQ Security Solutions for iSeries let you monitor session activity and automatically log users off after a specified period of inactivity. You can granularly assign session inactivity limits based on user profile instead of for all the computers on a server, providing better control and flexibility for users.

The file editor included with NetIQ Security Solutions for iSeries offer a secure alternative to the IBM Data File Utility (DFU). The NetIQ Security Solutions for iSeries editor records an audit trail to track file modifications so you can identify and report improper file access or changes.

Alerts and Responds to Security Events

NetIQ Security Solutions for iSeries monitor for specified security events and other events and immediately emails, phones, or pages the proper person when a critical event occurs. The NetIQ Security Solutions for iSeries event management provides the following services:

- Monitors system events for security issues, such as stopping auditing functions
- Alerts you to events you specify using criteria you establish
- Logs alerts and sends messages to the console
- Notifies selected staff members by pager, email, or phone
- Can respond to alerts by issuing SNMP traps to shut down access
- Lets you prioritize alerts based on their importance in your environment
- Lets you define criteria for escalating alerts
- Supports rotating notification based on personnel schedule
- Applies alert filters to minimize reports of normal activity
- Helps you implement intrusion detection easily using handy wizard

Ensures Operational Integrity While Increasing Compliance

Regulations, such as the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA), burden IT organizations to track changes to critical data and the systems that store and share that information. NetIQ Security Solutions for iSeries helps you limit general access to managed servers so you can comply with these far-reaching regulations while still maintaining the operational integrity of your servers.

You can limit access by user, server, object, task, and time to granularly control changes to managed servers. This level of granular delegation helps you minimize the risk of unintended or malicious changes to your valuable assets.

Because you can securely escalate only the authorities needed to fix, update, or troubleshoot server problems, NetIQ Security Solutions for iSeries makes your environment more secure and compliant. Automatically documenting the compliance measures you have implemented keeps your costs low while dramatically reducing risk for your assets. NetIQ Security Solutions for iSeries reports keep you and your auditors up to date, showing all mediated activity for specified servers or users during a specified period.

Simplifies User Profile and Password Management

NetIQ Security Solutions for iSeries let you define, verify, and enforce password strength policy so user profiles are no longer your most vulnerable security point. Another common password vulnerability occurs when users choose weak or easily guessed passwords. The NetIQ Security Solutions for iSeries profile and password management features offer the following services:

- Evaluates passwords against dictionaries included with the product
- Lets you customize your password checking dictionary to include industry terms
- Rates passwords as strong or weak
- Authenticates use of historical passwords
- Produces reports to help you implement a plan for improving password security
- Lets security administrators change or disable user profiles if passwords do not meet password strength policy

Integrates with Other NetIQ Products

NetIQ Security Solutions for iSeries also work with other NetIQ security products to deliver centralized enterprise security management for heterogeneous enterprises. Working together, the products offer comprehensive features to address four major aspects of security management:

Vulnerability and Configuration Management

NetIQ Security Solutions for iSeries supply information to Secure Configuration Manager to help you manage vulnerabilities across multiple platforms, including iSeries, Windows, and Unix. Secure Configuration Manager provides built-in security expertise your staff can use to secure your enterprise, educate your staff, and provide facts you need to correct the vulnerabilities.

Incident and Event Management

PSDetect sends alerts to NetIQ Security Manager to monitor and alert you to security events on your iSeries servers. Real-time event notification can help you protect your iSeries assets against attacks, assure servers and staff are compliant with corporate policies, and ensure your iSeries servers are available and performing.

With built-in log management, Security Manager can consolidate raw log and event data, apply automated forensic analysis, quickly pinpoint trends across your enterprise, and create reports that help you easily understand your security and event data.

Policy and Compliance Management

Integrated with VigilEnt Policy Center, NetIQ Security Solutions for iSeries enable security managers to distribute and enforce corporate security policies, government mandates, or industry regulations. Use Secure Configuration Manager to run security checkups that score iSeries servers against corporate security policies and create management-ready compliance reports.

Performance and Availability

NetIQ Security Solutions for iSeries can also send SNMP traps to NetIQ AppManager to assure the performance and availability of your IT systems and services through proactive monitoring and quick diagnostics and recovery.

Chapter 2
Planning to Install NetIQ Security Solutions for iSeries

This chapter provides considerations for installing the NetIQ Security Solutions for iSeries products and components.

Requirements

The following software, hardware, and permissions are required to install and upgrade the NetIQ Security Solutions for iSeries products.

Category	Minimum Requirements
Operating System	OS V5R3 *If you are running OS V6R1*, you must apply IBM PTF MF44237 before accessing the NetIQ Security Solutions for iSeries product.
Disk Space	Installing from a CD: 415 MB Installing from a save file: 1230 MB

Category	Minimum Requirements
Media	• Physical access to the CD-ROM drive in the server • CD-ROM drive device name OR • Downloaded installation save file, SVFPSI00 • Downloaded ISO image installed using a virtual optical drive
QTEMP Storage	*If you are upgrading to the latest product version*, your server must have at least 150 MB of available QTEMP storage.
System Values	QALWOBJRST must be set to *ALL or *ALWPGMADP
User Profile Authorities	User profile that includes *ALLOBJ and *SECADM special authorities to install products or run PSPasswordManager
iSeries Software Components	• Portable Application Solutions Environment (PASE) You can install PASE (option 33) for free from the operating system licensed programs. • Qshell You can install Qshell (option 30) for free from the operating system licensed programs.

Installation Considerations

Before performing a new installation, product upgrade, or Cumulative PTF installation, review the following sections for more information about scheduling an installation, and the changes made to your server during an installation.

The time required to install NetIQ Security Solutions for iSeries can range from five minutes to four hours, depending on the size and speed of your system. To reduce the impact on users, schedule the installation or upgrade after regular work hours.

Installation Changes

This section summarizes the changes that occur to your iSeries system for each NetIQ Security Solutions for iSeries product that is installed or configured.

CPU

Although CPU utilization depends on a number of hardware and software factors, NetIQ Security Solutions for iSeries software usually requires less than 5% average CPU utilization. At times, however, this requirement could be greater.

All iSeries Products

The NetIQ Security Solutions for iSeries installation process makes the following changes on your server:

- Creates the PSINSTALL library
- Creates the PSCOMMON library
- Creates the PSAUDIT authorization list
- Creates the PSSECURE authorization list
- Creates the PSPSSSMS authorization list
- Creates the PSDETECT authorization list
- Creates the PSPWDMGR authorization list
- Creates the PSCOMMON authorization list
- Creates the PSOBJOWN PASSWORD(*NONE) USRCLS(*PGMR) user profile
- Creates PSOBJOWNS PASSWORD(*NONE) USRCLS(*SECOFR) user profile
- Adds a PSOBJOWN user directory entry
- Creates the PSMENU command in the QGPL library
- Creates product library pointers (data areas PSSLIB and PSAMLB) in the library QGPL

PSAudit

The NetIQ Security Solutions for iSeries installation process makes the following changes to your server for PSAudit:

- Creates the PSAUDIT product library
- Creates the following command objects in the QGPL library:
  - ALOG: Enter the SAA Main Menu
  - ALOGPRT: Print the SAA Log of System Accesses
  - BLCRTCLT: Create Baseline Collection
  - BLCMPCLT: Compare Baseline Collection
  - DDRPT: Print the DAR File Changes Report
  - DDRPTA: Print the DAR File Access Report
  - STRAA: Enter the SAR Main Menu
  - STRAAAPI: Run the SAR command interface for reports
  - STRBL: Enter the Baseline Analysis Main Menu
  - STRDD: Enter the DAR Main Menu
- Creates data area (*DTAARA) PSALIB in the QGPL library

PSSecure

The NetIQ Security Solutions for iSeries installation process makes the following changes to your server for PSSecure:

- Creates the PSSECURE product library
- Creates the following commands in the QGPL library:
  - ASO: Enter the ISM Main Menu
  - DBA: Enter the SFE Main Menu
  - DBALOG: Print the SFE log of file changes

- DSPFLD: Display a file's record format layout
- STRMS: Enter the SMS Main Menu
- STROAM: Enter the OAM Main Menu
- STRRRM: Enter the RRM Main Menu
- STRSFE: Enter the SFE Main Menu
- ZPASS: Enter the PPM Main Menu

- Creates product library pointers (data areas PSSLIB and PSAMLB) in the QGPL library

PSDetect

The NetIQ Security Solutions for iSeries installation process makes the following changes to your server for PSDetect:

- Creates the PSDETECT library
- Creates the PSDLIB data area in the QGPL library

PSPasswordManager

The NetIQ Security Solutions for iSeries installation process creates product library PSSECURE on your server for PSPasswordManager.

Privilege Manager

The NetIQ Security Solutions for iSeries installation process makes the following changes to your server for Privilege Manager:

- Creates the NQPRVMGR authorization list
- Creates the NQPRVUSR authorization list
- Creates the STRNPM command in the PSCOMMON library to access the Privilege Manager Main Menu

Chapter 3
Installing NetIQ Security Solutions for iSeries

This chapter describes performing a new, upgrade, or Cumulative PTF installation of the NetIQ Security Solutions for iSeries products:

New Installation

Provides all NetIQ Security Solutions for iSeries products, product options, and PTFs from the most recent Cumulative PTF. For more information about performing a new installation of the NetIQ Security Solutions for iSeries products, see "Installation Checklist" on page 22.

Upgrade

Provides the latest version of NetIQ Security Solutions for iSeries products, while installing all NetIQ Security Solutions for iSeries products, product options, and PTFs from the most recent Cumulative PTF. For more information about upgrading NetIQ Security Solutions for iSeries products, see "NetIQ Security Solutions for iSeries Upgrade Checklist" on page 93.

Cumulative PTF

Provides all PTFs for the NetIQ Security Solutions for iSeries products since the release of the base product, while ensuring all NetIQ Security Solutions for iSeries products and product options are installed on your server. To determine if a Cumulative PTF is available, see the NetIQ Security Solutions for iSeries installation CD or the NetIQ Web site at www.netiq.com/support/iseries.

For more information about performing a Cumulative PTF installation, see "Installing Cumulative PTFs" on page 103.

Installation Checklist

This section provides instructions for performing a new installation of NetIQ Security Solutions for iSeries products. If NetIQ Security Solutions for iSeries products are currently installed on your system, see "NetIQ Security Solutions for iSeries Upgrade Checklist" on page 93.

Note

Perform the installation of NetIQ Security Solutions for iSeries products after regular work hours to reduce the impact on other users. Some operations performed during installation could require you to cycle your remote servers.

☑	Steps
☐	**1.** Back up your system.
☐	**2.** Log on with a user profile with at least *ALLOBJ and *SECADM special authorities.
☐	**3.** Ensure your server meets the software, hardware, and permissions requirements for installing the NetIQ Security Solutions for iSeries products. For more information, see "Requirements" on page 15.

☑	Steps
☐	**4.** Ensure the system value for QALWOBJRST is *ALL or *ALWPGMADP.
☐	**5.** Issue the following command to display the setting of system value QFRCCVNRST. DSPSYSVAL QFRCCVNRST
☐	**6.** *If QFRCCVNRST is not set to 2*, issue the following command to change the setting: CHGSYSVAL QFRCCVNRST VALUE('2') Ensure you note the current value of this setting. After the installation is complete you will reset the system value.
☐	**7.** *If you are running OS V5R3 or later and exit point QIBM_QTMT_WSG is installed*, remove it by performing the procedure outlined in knowledge base article NETIQKB46825.
☐	**8.** *If you are installing the product from media*, load the media in the appropriate iSeries drive.
☐	**9.** *If you are installing the product from media*, on the command line, type the following command and press Enter: RSTLICPGM LICPGM(1PSI001) DEV(*NNNNN*) where *NNNNN* is the name of the optical device that contains the NetIQ Security Solutions for iSeries CD.
☐	**10.** *If you are installing the product from a save file that you downloaded from the NetIQ Web site*, on the command line, type the following command and press Enter: RSTLICPGM LICPGM(1PSI001) DEV(*SAVF) SAVF(*library/file*) where *library/file* is the name of the library and save file that you downloaded from the NetIQ Web site and uploaded to your iSeries server.
☐	**11.** On the command line, type PSINSTALL and press F4 (Prompt).

☑	Steps
☐	**12.** Type the name of the optical device that contains the NetIQ Security Solutions for iSeries CD in the **DEVICE** field, or type `*SAVF` file if you are installing the product from a save file that you downloaded from the NetIQ Web site, and press Enter.
☐	**13.** Review the remaining parameters and make any necessary changes, then press Enter to begin installation. For more information about the parameters, see “Completing PSINSTALL Parameters” on page 26.
☐	**14.** *If the User License Agreement parameter was set to *READ*, PSINSTALL displays the User License Agreement. To accept the license agreement and proceed with the installation, press F6. To decline the agreement and cancel the installation, press F12.
☐	**15.** *If you receive the error message CPA3DD6 Library XXXXXXXXXXX not registered to product PSxxxx... or CPA3DE4 not registered. (C,G)*, type `G` and press Enter.
☐	**16.** *If you have purchased NetIQ Security Solutions for iSeries products*, enter the permanent license codes for the NetIQ Security Solutions for iSeries products. For more information, see “Entering Permanent License Codes” on page 29.
☐	**17.** *If you changed the QFRCCVNRST system value setting*, issue the following command to reset the system value: `CHGSYSVAL QFRCCVNRST VALUE('N')` where *N* is the value you recorded in Step **5**.
☐	**18.** *If you are running i5/OS V6R1*, you must apply IBM PTF MF44237 before accessing the NetIQ Security Solutions for iSeries product.

☑	Steps
☐	**19.** To use PSSecure - Remote Request Management, install the exit programs. For more information about installing exit programs, see “Installing Exit Programs” on page 29. For more information about configuring Remote Request Management, see “Remote Request Management (RRM)” on page 44.
☐	**20.** Authorize users to NetIQ Security Solutions for iSeries products. The user profile used to install the NetIQ Security Solutions for iSeries products is automatically authorized. The user profile QSECOFR can also be used to grant and revoke authority to the NetIQ Security Solutions for iSeries products. For more information, see “Authorizing Users to NetIQ Security Solutions for iSeries Products” on page 31.
☐	**21.** Configure the NetIQ Security Solutions for iSeries components. For more information, see “Configuring NetIQ Security Solutions for iSeries Components” on page 31.

Completing PSINSTALL Parameters

When you execute the PSINSTALL command, all the parameters contain the default values appropriate to the level of installation required for your server. Review the following parameters and make changes as necessary:

Device

Enter the name of the optical device containing the NetIQ Security Solutions for iSeries product CD, or type `*SAVF` if you are installing the product from a save file that you downloaded from the NetIQ Web site.

PTF Save File

If you are installing or upgrading the NetIQ Security Solutions for iSeries product, ensure the value for this field is `*NONE`. This field is used only when installing a Cumulative PTF. The PSINSTALL command displays this field during an installation or upgrade only if you press F9.

If you are installing a Cumulative PTF, enter the name of the save file that was downloaded from the NetIQ Web site. This field is used only if you are installing a Cumulative PTF. To determine if a Cumulative PTF is available, see the NetIQ Security Solutions for iSeries installation CD or the NetIQ Web site at www.netiq.com/support/iseries.

PTF Save File Library

If you are installing or upgrading the NetIQ Security Solutions for iSeries product, ensure the value for this field is `*LIBL`. This field is used only when installing a Cumulative PTF. The PSINSTALL command displays this field during an installation or upgrade only if you press F9.

If you are installing a Cumulative PTF, enter the name of the library where the save file that contains the Cumulative PTF is located. This field is used only if you are installing a Cumulative PTF. To determine if a Cumulative PTF is available, see the NetIQ Security Solutions for iSeries installation CD or the NetIQ Web site at www.netiq.com/support/iseries.

User License Agreement

Determines if the User License Agreement (EULA) is displayed. Valid entries are as follows:

- *READ - The EULA is displayed before installation. From this window, you can accept the agreement and proceed with the installation.
- *ACCEPT - The agreement is accepted, and the EULA is not displayed.

Note

If the EULA has already been accepted, this parameter is automatically set to `*ACCEPT`.

Remove RRM Exit Programs and Cycle Host Servers

This field displays whether the NetIQ Security Solutions for iSeries RRM exit programs are removed, the *FILE, *DATABASE, and *FTP host servers are cycled, and the QSERVER and QUSRWRK subsystems are ended. This parameter is only `*YES` when upgrading the product or applying a Cumulative PTF. For a new installation this parameter is always `*NO`.

Note

This parameter pertains only to RRM Exit Programs. If other exit programs are installed on any NetIQ supported exit points, those exit points are not removed.

Submit install to batch

Determines whether the installation program is run interactively or submitted for batch processing. The default value is `*NO`. If the parameter is `*YES`, the Job Queue, Library, Schedule Date, and Schedule Time parameters are displayed.

If you are upgrading the products and are running in restricted state, ensure this value is `*NO` and press Enter.

If you are upgrading the products and are not running the server in restricted state, type `*YES` and press Tab.

Job Queue

Specifies the job queue from which the PSINSTALL job is submitted. The default value for this parameter is QBATCH. This field is available only if you have entered *YES in the **Submit install to batch** field.

Job Queue Library

Specifies the library where the job queue used to submit the PSINSTALL job is located. This field is available only if you have entered *YES in the **Submit install to batch** field.

Schedule Date

Specifies the date on which the PSINSTALL job is scheduled to begin. The default value is *CURRENT, which is the current date. If you want to begin the job on another date, specify the date you want the job to process. This field is available only if you have entered *YES in the **Submit install to batch** field.

Schedule Time

Specifies the time when the PSINSTALL job is scheduled to begin. The default value is *CURRENT, which indicates that the install is submitted immediately. If you want to schedule the installation to be done at a later time, specify the time you want the job to begin. This field is available only if you have entered *YES in the **Submit install to batch** field.

Note

If you are installing the product from the NetIQ Security Solutions for iSeries product CD and you schedule the PSINSTALL job to begin at another date or time, the NetIQ product CD must be loaded in the optical device specified in the **Device** field prior to the date and time the job is scheduled to start.

Entering Permanent License Codes

After you install the NetIQ Security Solutions for iSeries products, the applications are fully functional for 30 days. If you have purchased the software and have permanent license codes, enter the license codes. If you have not received your permanent license codes, contact your Sales Representative.

Note

If you are evaluating the NetIQ Security Solutions for iSeries products, the NetIQ Security Solutions for iSeries products retain any configuration you implement during the evaluation process when you enter your permanent codes. This capability applies even if the evaluation period has expired.

To enter permanent license codes:

1. Type `PSMENU` on the command line, and press Enter.
2. Type `80` (Access Codes), and press Enter.
3. Type the series of 5-digit license codes for the NetIQ Security Solutions for iSeries products in the **Codes** fields, and press Enter.

Installing Exit Programs

To enable RRM exit programs to restrict remote access, you must install the exit programs by performing the following steps.

Note

If you want to retain non-NetIQ exit programs previously installed on exit points supported by NetIQ Security Solutions for iSeries, see the *User Guide for NetIQ Security Solutions for iSeries Remote Request Management*.

To install RRM exit programs:

1. At the PSSecure Main Menu, type `3` (Remote Request Management) and press Enter.
2. Type `30` (Manage RRM) and press Enter.

3. Type `1` (Work with Exit Programs) and press Enter.
4. Select the exit programs that you want to install by typing `1` (Install RRM Exit) beside each appropriate exit program. To select all the exit programs, type `1` beside the first program listed, and then press F13 (Repeat).
5. Press Enter, then F3.
6. Type `3` (Cycle Remote Servers) and press Enter.
7. Press F9.
8. Type `*FILE` and `*DATABASE` in the **Application Server** fields.
9. Ensure the value in the **Exclude server** field is `*TELNET`.
10. Type `QSERVER` in the **Allow ending subsystems** field.
11. Ensure the value in the **Delay before restart** field is `30`.
12. Press Enter.

Note
If you are connected to the iSeries server using Telnet, your session ends if you choose to cycle all remote servers. Once the Telnet server restarts, start a new session.

For more information about collecting data and implementing RRM, see "Remote Request Management (RRM)" on page 44.

Chapter 4
Configuring NetIQ Security Solutions for iSeries Components

After you have installed the NetIQ Security Solutions for iSeries products, you can customize them for your environment and begin monitoring the security of your servers.

Authorizing Users to NetIQ Security Solutions for iSeries Products

After you have installed the NetIQ Security Solutions for iSeries products, you must authorize users to those products. The NetIQ Security Solutions for iSeries installation process automatically authorizes the user profile that performed the product installation to the NetIQ Security Solutions for iSeries products as an authority administrator. The authority administrator can grant and revoke user authority to the products. The security officer profile QSECOFR can also grant and revoke authority to the NetIQ Security Solutions for iSeries products.

After authorizing users to the products, you must configure the product components as described in the following sections of this chapter.

Note

The security officer cannot grant or revoke authority to PSPasswordManager using this procedure. For information about authorizing uses to PSPasswordManager, see the *User Guide for NetIQ Security Solutions for iSeries PSPasswordManager*.

To authorize users to the NetIQ Security Solutions for iSeries products:

1. On the command line, type `PSMENU` and press Enter.
2. Type `70` (Utilities Menu) and press Enter.
3. Type `1` (Authorize users to products) and press Enter.
4. For each user you want to authorize or prohibit the use of NetIQ iSeries products, specify the following information in the corresponding fields on the Set PentaSafe Authority (PSSETAUT) window:

   User

   Specify one or more user IDs to authorize.

   Product

   Specify a specific product to authorize, or specify `*ALL` to authorize the user to all NetIQ Security Solutions for iSeries products.

   Authority

   Specify whether you are authorizing (*GRANT) or prohibiting (*REVOKE) user authority to the NetIQ Security Solutions for iSeries products.

Authority administrator

Specify whether you want the user to have administrator authority. Administrator authority authorizes the user to grant, change, or revoke other users' authority to the NetIQ Security Solutions for iSeries products.

Users who have Authority Administrator rights also have the following authorities:

- *AUDIT special authority, if authorized to PSAudit
- Ability to perform security administrator functions in PSAudit System Access Analysis (SAA), if authorized to PSAudit
- Special authority to the PSSecure Secure Menuing System (SMS), if authorized to PSSecure, and the ability to perform menu administrator functions

Users who lose Authority Administrator rights lose the following types of authority:

- If you revoke a user profile's authority to PSAudit, you must manually remove *AUDIT special authority from the user profile. For more information, see the *User Guide for NetIQ Security Solution for iSeries PSAudit*.
- If you revoke a user profile's authority to PSAudit, NetIQ Security Solutions for iSeries automatically revoke Security Administrator authority to PSAudit System Access Analysis (SAA) from the user profile.
- If you revoke a user profile's authority to PSSecure, you must manually revoke special authority to the PSSecure Secure Menuing System (SMS) from the user profile. For more information, see the *User Guide for NetIQ Security Solution for iSeries PSSecure*.

Accessing the Products

To access the NetIQ Security Solutions for iSeries products, type `PSMENU` on the command line and press Enter. The PSMENU command is installed in library QGPL.

Configuring PSAudit

PSAudit is a comprehensive product that automates and simplifies the process of monitoring changes to iSeries servers. This product monitors any changes to the operating system, reports on unauthorized accesses and security exposures, provides information about system access and activity of all users, tracks access changes to any file, and compares collections of system information from one date to another.

After installing the NetIQ Security Solutions for iSeries products and authorizing users to PSAudit, read the following sections to configure each PSAudit component:

- "System Auditing and Reporting (SAR)" on page 34
- "System Access Analysis (SAA)" on page 37
- "Data Auditing and Reporting (DAR)" on page 38

For more information about these PSAudit components, see the *User Guide for NetIQ Security Solutions for iSeries PSAudit*.

System Auditing and Reporting (SAR)

SAR provides a scored System Checkup Report for quick analysis of a system's health and delivers approximately 200 reports, which are also available using Secure Configuration Manager.

To configure SAR, perform the tasks listed in this section. Some of these tasks are not required to configure SAR, but have been included to illustrate recommended reporting functions.

Using the PSAudit Configuration Wizard

When you configure SAR, use the PSAudit Configuration Wizard to schedule auditing functions to execute on a regular basis. The PSAudit Configuration Wizard provides an easy way to schedule your auditing functions. The wizard helps you configure the iSeries Security and Auditing functions, and helps you schedule PSAudit/SAR reports and other jobs such as database loads and data purges.

To use the Scheduling Wizard:

1. On the System Auditing and Reporting menu, type `7` (System Setup and Defaults) and press Enter.
2. Type `16` (PSAudit Configuration Wizard) and press Enter to display the first of three windows.
3. Review Screen 1 to ensure system values QAUDCTL and QAUDLVL are set appropriately.

   To set your system to the recommended settings and to start security auditing, press F10. This function modifies QAUDCTL and QAUDLVL system values. Security auditing must be activated before you can generate most PSAudit reports.
4. Press F12 to continue.
5. Review Screen 2 to specify the JOBQ and OUTQ for SAR jobs.
6. Ensure the specified JOBQ and OUTQ are in your current library list, then press Enter.
7. Review Screen 3 to schedule events and reports, and add, remove, or alter the timing of any reports as needed. Pressing F9 displays more detailed information.
8. When the list reflects your needs, press F10 to schedule the jobs and exit the wizard.

Note

If you want to turn off all reports/events, return to the PSAudit Configuration Wizard and press F11 on the last window, or issue the following commands:

RMVJOBSCDE JOB(XA*) ENTRYNBR(*ALL)
RMVJOBSCDE JOB(ZA*) ENTRYNBR(*ALL)

To adjust individual selections, issue the following command:

WRKJOBSCDE

You can filter most reports to alter the selection criteria. For information about filtering, see the *User Guide for NetIQ Security Solutions for iSeries PSAudit*.

Configuring QAUDJRN Logging

PSAudit helps you control the level of auditing on your server by providing a central location for changing auditing system values. PSAudit uses these system values to audit functions that affect your server's security. Changes to these system values take effect immediately for all jobs running on the system. You can also use the PSAudit Configuration Wizard to configure QAUDJRN logging.

For more information about security journaling, see the IBM iSeries documentation.

To use PSAudit to configure QAUDJRN logging:

1. From the **PSAudit Main Menu**, type `1` (System Auditing and Reporting) and press Enter.
2. Type `7` (System Setup and Defaults Menu) and press Enter.
3. Type `4` (Work with Security Journaling) and press Enter.
4. ***If you want to use the NetIQ recommended auditing values***, press `F10` (Set recommended values).
5. ***If you want to define the values for QAUDCTL and QAUDLVL system values***, type `1` next to the appropriate values and press Enter. For more information about the QAUDCTL and QAUDLVL valid values, see the *User Guide for NetIQ Security Solutions for iSeries PSAudit*.
6. Press `F3` until you return to the **NetIQ Product Access Menu**.

Security Checkup Report

The PSAudit Security Checkup Report provides a quick way to perform an audit of 70 aspects of your system security. Using pre-defined thresholds, this report finds potential security weaknesses in your system, rates the security of your system, and gives you recommendations on how to improve your security configuration. The pre-defined thresholds are based on industry standards. You can modify the thresholds to meet your company's security standards. Generate the Security Checkup Report using our pre-defined thresholds first, and then make adjustments as needed to meet the security standards required for your environment.

To generate the full Security Checkup Report using pre-defined thresholds:

1. Type `PSMENU` on the command line and press Enter.
2. Type `1` (PSAudit) and press Enter.
3. Type `1` (System Auditing and Reporting) and press Enter.
4. Type `9` (Summary Reports Menu) and press Enter.
5. Type `5` (Security Checkup) and press Enter.
6. Type `1` (All) and press Enter.
7. Ensure the value in **OUTQ** field and the **JOBQ** field are correct, then press Enter.
8. Press F12 to return to the Summary Reports Menu.
9. To set your own thresholds, type `6` (Security Check-up Configurator) and press Enter.

System Access Analysis (SAA)

SAA is a menu driven product designed to capture and report all details of a user's activity on the iSeries server. SAA provides summary information of interactive and batch jobs executed by users whose activities are being logged. SAA provides details of each job in both online and hard-copy formats, and includes all access attempts, requests, commands, and command messages.

To configure System Access Analysis (SAA):

1. On the command line, type `PSMENU` and press Enter.
2. Type `1` (PSAudit) and press Enter.
3. Type `2` (System Access Analysis) and press Enter.
4. Type `3` (Users/Workstations to be Logged) and press Enter.

5. On the MAINTAIN USERS/WORKSTATIONS TO BE LOGGED window, perform the following steps:

   a. Type the userIDs to monitor in the **User/Job/Workstation** field.

   b. Review the default values shown in the **DEFAULTS** field.

   c. ***If you do not want to use the default values shown***, specify different values and press Enter.

   d. Press F3 to exit.

6. Type `4` (Start Monitor) and press Enter.

7. Type `11` (Configure SAA for Interactive Jobs) and press Enter.

8. On the System Access Analysis Configuration window, type `6` (Apply SAA Capture) beside the **SIGNOFF** and **ENDPASTHR** commands that reside in the QSYS library, and press Enter.

9. Press F3 to exit.

10. To ensure the ZALOG job is active, type 10 (Work With ZALOG Subsystem Jobs) and press Enter.

For more information about SAA reporting and maintenance options, see the *User Guide for NetIQ Security Solutions for iSeries PSAudit*.

Data Auditing and Reporting (DAR)

The Data Auditing and Reporting feature tracks changes made to any iSeries file, and reports on only those files and fields that you specify. Using DAR can save you hundreds of hours in tracking and documenting system activities.

To configure Data Auditing and Reporting (DAR):

1. On the command line, type `PSMENU` and press Enter.

2. Type `1` (PSAudit) and press Enter.

3. Type `3` (Data Auditing and Reporting) and press Enter.

4. Add a file by performing the following steps:

   a. Press F6 (Add).

   b. Specify the name of the file to be journaled.

   c. Specify the name of the library where the file resides.

   d. Press Enter.

5. Locate the appropriate file in the Work with Files list.

6. Type `1` in the **Opt** field beside the specified file, and press Enter to start journaling.

   This configuration process is performed in batch mode. For more information, see the *User Guide for NetIQ Security Solutions for iSeries PSAudit*.

   Note
   If the files selected are locked, auditing is not turned on until the files are available to have the auditing value changed.

7. Type `6` in the **Opt** field beside specified file, and press Enter.

8. Specify the fields included in the report using the following options:

   C=Detect Changes
   The report displays the specified field only when changes occur.

   R=Report Only
   The report displays the specified field.

   N=Remove Selection
   The report does not display the specified field.

9. Press Enter, then press F12 (Previous).

Post-Configuration Procedures

After you have configured PSAudit, you should perform the following post-configuration procedures if they apply to your system:

- ***If you are using Secure Configuration Manager***, see "Configuring Secure Configuration Manager Support" on page 79.
- ***If you are using Security Manager***, see "Configuring Security Manager Support" on page 69.

Configuring PSSecure

PSSecure helps you manage your iSeries servers more efficiently by simplifying security administration and improving system security. With PSSecure, you can control remote access to your system, establish and maintain object level authorizations, and automatically terminate unattended computer sessions. PSSecure helps you prevent security exposures by giving you the tools you need to quickly and easily lock down your system.

After installing the NetIQ Security Solutions for iSeries products and authorizing users to PSSecure, read the following sections to configure each PSSecure component:

- "Profile and Password Management (PPM)" on page 41
- "Remote Request Management (RRM)" on page 44
- "Object Authority Management (OAM)" on page 47
- "Inactive Session Monitor (ISM)" on page 51
- "Secure File Editor (SFE)" on page 53

For detailed information about PSSecure components, see the following guides:

- *User Guide for NetIQ Security Solutions for iSeries PSSecure*
- *User Guide for NetIQ Security Solutions for iSeries Remote Request Management*

Profile and Password Management (PPM)

PPM helps you manage user profiles and control your users' passwords easily, securely, and efficiently on a network of iSeries servers. You can easily delegate creating, changing, and deleting user profiles tasks to a non-technical user or to a System Operator using Profile Templates.

Profile and Password Synchronization

To implement the User Profile Synchronization feature, you must configure SNADS for communications with your iSeries systems, or you can use TCP/IP if appropriate. For more information, contact NetIQ Technical Support.

To configure PPM:

1. On the command line, type `PSMENU` and press Enter.
2. Type `2` (PSSecure) and press Enter.
3. Type `2` (Profile and Password Management) and press Enter.
4. Type `2` (Profile Synchronizer Menu) and press Enter.
5. Type `8` (Profile Synchronizer Installation) and press Enter. When the Profile Synchronizer Installation window is displayed, follow the on-screen instructions and return to the Profile Synchronizer menu when finished.
6. Type `4` (Profile Synchronizer Defaults) and press Enter.
7. Change the default settings as appropriate, and press Enter. For more information about Profile Synchronizer default settings, see the *User Guide for NetIQ Security Solutions for iSeries PSSecure*.
8. Press F3.
9. Type `2` (Distributed Systems) and press Enter.
10. Review the systems listed in the **Target System** column, and change the list as needed. Press Enter to update, then F3 to exit.
11. Press F12 twice to return to the Profile and Password Management menu.

12. Type 4 (AS/400 Password System Values) and press Enter.

    If your system already uses a Password Validation Program (PVP), change the actual program shown in the Password validation program field to call program ZPCL22 in library PSSECURE, passing it the parameters for New Password (10 bytes, character) and User ID (10 bytes, character). If a PVP is not in use, change the value in the **Password validation program** field to ZPPVP and the **Lib** field to PSSECURE.

    Press Enter twice, then press F3. When the process is completed, the Profile and Password Management menu is re-displayed.

    For more information, see "Profile and Password Management" in the *User Guide for NetIQ Security Solutions for iSeries PSAudit*.

User Profile Templates

The following steps provide instructions for creating secure templates to use in creating and changing user profiles. To create user profile templates, you must have a user profile with the user class *SECOFR.

To create a user profile templates:

1. On the command line, type PSMENU and press Enter.
2. Type 2 (PSSecure) and press Enter.
3. Type 2 (Profile and Password Management) and press Enter.
4. Type 3 (Profile Templates Menu) and press Enter.
5. Type 2 (Maintain User Profile Templates) and press Enter.
6. On the Work with User Profile Templates window, press F6 to create a new template. Specify values in the entry fields, and press Enter. To exit, press F3.
7. On the Create a User Profile Template window, press F4 for each parameter for which you want to restrict the permissible values or change the default value.
8. On the Work with User Profile Templates window, type 15 (Edit Authority) next to the template you are creating and press Enter.

9. On the Edit User Profile Template Authority window, press F6 (Add) to authorize a user profile to use the template. Specify the user profile name and whether the user is authorized to create user profiles (CRTUSRPRF = Y) and to change user profiles (CHGUSRPRF = Y). Press Enter, then F3 (Exit).

   Depending on the usage rights and restrictions specified in the CHGUSRPRF and CRTUSRPRF templates, the users that you have specified are now authorized or forbidden to change and create user profiles. The PSCHGUSRPR and PSCRTUSRPR commands control the authorities to change and create these profiles.

User Profile Management

PPM provides automatic disabling, deletion and archiving of unused profiles. You can easily re-activate archived profiles and schedule PPM to delete archived profiles after a specified number of days.

To start using the User Profile Management tool:

1. From the Profile & Password Management Main Menu, type 1 (General Options Menu) and press Enter.
2. To add user profile exclusions, type 17 and press Enter.
3. Enter the user profiles that should not be disabled, such as Q*, and press Enter,
4. Press F3.
5. To change default values, type 16 and press Enter.
6. Specify the appropriate values and press Enter.
7. To schedule the job to disable, delete and archive profiles, press F7.
8. Specify the appropriate job scheduling options and press Enter.

Remote Request Management (RRM)

RRM, which is a subcomponent of PSSecure, manages remote requests on iSeries systems by determining whether incoming transactions are authorized to access the target server. A remote request is a transaction that originates outside the target server. By evaluating exit programs and comparing incoming requests to secured entries, RRM determines whether each request is approved or rejected.

After you complete a new installation of PSSecure/RRM, use the RRM Configuration Wizard to configure the product. Then, perform the tasks described in "Additional RRM Configuration" on page 45.

RRM Configuration Wizard

The RRM Configuration Wizard simplifies the initial setup of primary RRM controls. The wizard prompts you for information about how you want to use RRM and then configures the product.

To run the RRM Configuration Wizard:

1. On the command line, type `PSMENU` and press Enter.
2. Type `2` (PSSecure) and press Enter.
3. Type `3` (Remote Request Management) and press Enter.
4. Type `30` (Manage RRM) and press Enter.
5. Type `30` (RRM Configuration Wizard) and press Enter.
6. Complete the configuration wizard.
7. ***If you want to change an answer to an option***, press F12 until you access the step where you want to make a change.
8. Press Enter. The RRM Configuration Wizard configures the product.

Cycle Remote Servers

If you selected **Install Exit Programs** in the RRM Configuration Wizard, cycle your remote servers to enable all RRM features.

Warning
Cycling your remote servers ends connections to file servers and database servers on the iSeries. If you have any applications that connect to either of these servers, or if you are unsure whether you have applications that connect to either of these servers, you should perform this process after regular work hours.

To cycle your remote servers:

1. On the Manage RRM menu, type `3` (Cycle Remote Servers) and press Enter.
2. In the **Application server** field, specify `*DATABASE` and `*FILE` then press Enter.
3. In the **Allow ending subsystems** field, specify `QSERVER` and press Enter.

   Note
   The job might run for up to five minutes.

Additional RRM Configuration

Complete the following additional configuration tasks for RRM.

- Start the RRM Collection Monitor in your IPL startup routine as follows:

  ```
  PSCOMMON/PSRRMCMON ACTION(*START)
  MONMSG CPF0000.
  ```

  Note
  The collection process only takes effect for an exit point when both the RRM Collection Monitor (subsystem ZPSSMON) is active and the **Collected** parameter for the exit point is set to collect.

- After configuring RRM to collect remote transactions, review how RRM handles remote transactions when security is turned on. The Work With Collected Entries window displays whether the remote transaction is allowed, rejected, or unsecured by RRM. Initially RRM collects all transactions as Unsecured, since no RRM rules are created.
- Continue to review collected remote transactions and create secured entries until you have covered your month end cycle, usually from two to six weeks. Create Secured entries until you do not receive any unplanned rejected or unsecured remote transactions.

Configuration for Integration with ShowCase Suite

If you use ShowCase Suite from SPSS, complete the following configuration tasks for RRM.

- Create the following secured entries to allow you to start the ShowCase server:

```
S  USER     NETWORK     OPERATION        ACTION   OBJECT PATH
Y  QSECOFR  127.0.0.1   RMTCMD_PROGRAM   *PASS    /QSYS.LIB/QUSRUSAT.PGM
Y  QSECOFR  127.0.0.0   SIGNON_INFO      *PASS
```

- Create the following secured entry to allow you to start the Analyzer server:

```
S  USER     NETWORK     OPERATION        ACTION   OBJECT PATH
Y  QSECOFR  127.0.0.1   RMTCMD_COMMAND   *PASS    /QSYS.LIB/ALCOBJ.CMD
```

- Create the following secured entry for each ShowCase user on the iSeries server:

```
S  USER     NETWORK     OPERATION        ACTION   OBJECT PATH
Y  usrname  127.0.0.1   RMTCMD_COMMAND   *PASS    /QSYS.LIB/QMHSNDPM.PGM
```

  where *usrname* is the user profile of the ShowCase user.

- You may need to create secured entries for ShowCase users on the iSeries server to access the following files:
  - /QSYS.LIB/*.LIB/DEFCTRL.FILE
  - /QSYS.LIB/*.LIB/JDBCODBC.FILE
  - /QSYS.LIB/*.LIB/JOBMSGS.FILE
  - /QSYS.LIB/*.LIB/OBATR.FILE

- /QSYS.LIB/*.LIB/OBINST.FILE
- /QSYS.LIB/*.LIB/OBORG.FILE
- /QSYS.LIB/*.LIB/STMTDEF.FILE
- /QSYS.LIB/*.LIB/TGTCOLS.FILE
- /QSYS.LIB/*.LIB/TGTIDX.FILE
- /QSYS.LIB/*.LIB/TRACE2.FILE
- /QSYS.LIB/*.LIB/TRACE3.FILE

Object Authority Management (OAM)

OAM simplifies resource (object-level) management and compliance by using authority templates as a standard to which objects in a library must comply. OAM compares access permissions for objects in a library to authority definitions of a template. After the comparison is complete, you can change the authorities for all objects that do not match the template. You can use a batch job or selectively change the object authorities using an interactive menu option.

Note
To become familiar with the functions of OAM, use a small, non-critical set of libraries or an application used by a small number of users.

To configure OAM:

1. Determine the library or libraries associated with the application for which you want to define a security policy.
2. Determine the user profile to own all the objects in the specified libraries.
3. Determine the user profiles which can access the application and which authorities the user profiles will have.
4. On the command line, type `PSMENU` and press Enter.
5. Type `2` (PSSecure) and press Enter.
6. Type `4` (Object Authority Management) and press Enter.

7. Type 1 (Work with Templates) and press Enter.

8. Press F6 (Add New Template) to create a new authority template:

   a. Specify the name and description. Use a name that describes the template's application.

   b. Specify the profile to own all objects in the libraries covered by the template. The owner has *ALL authority and should not be an application user.

   c. In the **User Profile** field, specify the value for the User Profile attribute of *PGM and *SRVPGM objects. Valid values are as follows:

      ***USER**

      Programs run under the authority of the user who is running the programs attached to this template.

      ***OWNER**

      Programs run under the authority of the user who is running the program and the program owner.

      ***SAME**

      OAM does not change the programs' user profile attribute.

   d. In the **Adopt Authority** field, specify the value for the Use Adopted Authority attribute of *PGM and *SRVPGM objects. Valid values are as follows:

      ***YES**

      *PGM and *SRVPGM objects use the program authority adopted from previous call levels when running programs attached to this template.

      ***NO**

      *PGM and *SRVPGM objects do not use the program authority adopted from previous call levels when running programs.

      ***SAME**

      OAM does not change the Use Adopted Authority attribute.

e. Press F8 (Edit Authorities) to specify user authorities to access the objects. Specify the following authorities:

- Users with *PUBLIC authority should also have *EXCLUDE authority.
- The owner of the template should have *ALL authority.
- All other profiles should have *USE authority.

f. Press F6 (Add New Users) to authorize additional user profiles to access the application.

g. When you have finished adding new users, press F3 to return to the Object Authority Management menu.

9. Generate the authority information for the application by performing the following steps:

a. Create a library to hold the authorities information that OAM collects but does not monitor. For example, to create library PSOAM, type the following command on the command line and press Enter:

CRTLIB LIB(PSOAM) TYPE(*PROD) TEXT('Object Authority Outfiles for VSA for iSeries OAM') AUT(*EXCLUDE) CRTAUT(*EXCLUDE)

b. From the OAM menu, type `3` (Generate Authority File) and press Enter.

c. In the PSAudit Submittal Window, specify the following values:

- Value for the libraries whose objects you want to comply with the template created in Step 8. You can use the filtering feature of PSAudit to exclude an object. For more information about filters, see the *User Guide for NetIQ Security Solutions for iSeries PSSecure*.
- Output file name and library where the report writes information about the current set of authorities. Place output files into a separate library with the same name as the template.

Note

Run the Generate Authority File report after hours during low-activity periods on the iSeries server. If processes are using the object, the report cannot collect object authority information.

If the report displays unwanted object information, create a filter and run the report again. For more information about creating filters, see the *User Guide for NetIQ Security Solutions for iSeries PSSecure*.

d. To submit the Object Authority By Object report, press Enter.

e. To see the list of reports, press F18. PSSecure writes the Object Authority By Object report to the AAOBJAUTO file.

10. After the report is complete, compare the current authorities to the template defined in Step 8 by typing 1 (Work with Templates) from the OAM menu and pressing Enter.

11. Type 5 (Use (Report/Comply)) beside the appropriate template in the **OPT** field and press Enter.

12. Type the name of the Object Authority output file and its library (File/Library) that were specified in the PSAudit Submittal Window.

13. Set the Comply flag to Y to force objects into compliance or N to only audit the objects. The default value is N. The first time you run this report against a library, set this field to N.

14. Specify the job queue (JOBQ) for batch processing or accept the default value QBATCH.

Note

Run the Use (Report/Comply) job after hours during low-activity periods on the iSeries server. If processes are using the object, the report cannot collect object authority information.

If this is a compliance job (Comply flag = Y), OAM replaces all objects in the output file created in Step **9** with the authorities specified in the authority template.

If this is an audit job (Comply flag = N), information is written to a file used by Option 2 (View/Change Non-Compliant Objects).

15. When you finish specifying information, press Enter.
16. Type `2` (View/Change Non-Compliant Objects) and press Enter.
17. Review the objects listed on the Work With Objects Out of Compliance window and use the template authorities to bring the objects into compliance if appropriate.
18. Periodically repeat Steps **9** through Step **17** to audit the application.

Inactive Session Monitor (ISM)

ISM helps you effectively handle the physical security of your inactive computers. Leaving a session signed on at an unoccupied computer is an invitation for intrusions. ISM can help secure computers from unauthorized use, improve availability of communication lines, reduce phone charges by ending inactive dial-up sessions, and decrease software license cost of concurrent users by ending inactive users.

Before configuring ISM, review the Testing section in the "Inactive Session Monitor" chapter of the *User Guide for NetIQ Security Solutions for iSeries - PSSecure*.

To configure Inactive Session Monitor (ISM):

1. On the command line, type `PSMENU` and press Enter.
2. Type `2` (PSSecure) and press Enter.
3. Type `5` (Inactive Session Monitor) and press Enter.

4. Type 6 (Display/Change System Parameters) and press Enter. If a Notice window is displayed, press Enter to continue with the ISM configuration.

5. Change the default values for the following parameters if appropriate:

   - ISM Time Limit

     Note
     The ISM Time Limit value must be less than the system value QINACTITV value.

   - ISM Check Gap
   - Send warning message
   - Subsystems to monitor (F7, *ALL, Enter, F12)

6. Press Enter, then F3 to exit.

7. Specify exceptions to the global default values by performing the following tasks:

- Change Workstation Exclusion:

  a. Type 3 (Change Workstation Exclusions) and press Enter.

  b. Specify the workstations that ISM should exclude or the workstations with default settings that differ from the System Parameters. When finished, press Enter.

  c. Press F3 to Exit.

- Change User Profile Exclusion:

  a. Type 4 (Change User Profile Exclusions) and press Enter.

  b. Specify the user profiles that ISM should exclude or user profiles with default settings that should differ from the System Parameters. When finished, press Enter.

  c. Press F3 to Exit.

8. Type 1 (Start Inactive Session Monitor) and press Enter.

Inactive Session Monitor (ISM) monitors the specified subsystems for idle interactive jobs, which are terminated or suspended according to the rules that you specify. ISM does not monitor sessions started before activating ISM.

Note
Users with privileged profiles, such as security officers, should never leave an interactive session unattended in a physically unsecured location.

Secure File Editor (SFE)

NetIQ Corporation provides the Secure File Editor (SFE) as a secure alternative to the IBM Data File Utility (DFU). SFE automatically creates a detailed log whenever a file alteration occurs. The Security Officer can then print an audit trail containing information of which files were accessed and by whom. This audit log helps identify users who are changing data improperly.

You can operate SFE by using its default values, but you can configure this component to meet the needs of your environment.

To configure SFE:

1. Change the system parameters by performing the following steps:

   a. On the command line, type `PSMENU` and press Enter.

   b. Type `2` (PSSecure) and press Enter.

   c. Type `6` (Secure File Editor) and press Enter.

d. Type `7` (Enter System Parameters) and press Enter.

e. On the Change System Parameters window, specify the following values in the corresponding fields and press Enter when finished:

Field	Value
Log changes to your Database?	Y
Save Before & After Images?	Y
Required entry for reason?	Y

SFE records detailed file changes that you can print using the SFE Show DBA Audit Log (DBALOG) command. If users specify reasons the changes were made, the reasons are printed on the report.

2. Set file authorities by performing the following steps:

a. On the command line, type `PSMENU` and press Enter.

b. Type `2` (PSSecure) and press Enter.

c. Type `6` (Secure File Editor) and press Enter.

d. Type `4` (Maintain File Authorities) and press Enter.

e. Press F6 (Add file record), specify the following values in the corresponding fields, and press Enter when finished:

- file name
- library name
- user profile
- authorization rights (read, add, update, delete)

f. ***If there are no more files to authorize***, press F3 to exit.

SFE uses the file authorities specified when accessing files, regardless of the user's object authority.

3. Disable the DFU Update Data command (UPDDTA) by renaming it, making a copy of the SFE's command for file access (DBA), and naming the copy of DBA "UPDDTA". To disable the DFU UPDDTA command, perform the following steps on the command line:

   a. Type the following command and press Enter:

   ```
   CRTDUPOBJ OBJ(DBA) FROMLIB(PSSECURE)
   ```

   b. Type the following command and press Enter:

   ```
   OBJTYPE(*CMD) TOLIB(QGPL) NEWOBJ(UPDDTA)
   ```

Post-Configuration Procedures

After configuring PSSecure, perform the following post-configuration procedures that apply to your system:

- ***If you plan to use the RRM Plug-in for iSeries Navigator***, perform the appropriate procedures described in "Installing the RRM Plug-in for iSeries Navigator" on page 107.
- ***If you are using Secure Configuration Manager***, see "Configuring Secure Configuration Manager Support" on page 79.

Configuring PSDetect

PSDetect actively monitors your iSeries servers 24 hours a day, 7 days a week and alerts you in real-time if any suspicious activity or potential exposures occur on your systems. PSDetect provides predefined events for your convenience, but is completely configurable, allowing you to choose exactly which events you want to track.

PSDetect QuickStart Wizard

The PSDetect QuickStart Wizard is available from the PSDetect Main Menu to provide easy setup and use of the product. Instead of defining system attributes using menus located throughout PSDetect, you can answer questions about how you want to use your system and let PSDetect configure the product.

Before starting the PSDetect QuickStart Wizard, gather the following information:

Action	Information to gather	Where to locate the information
Email	IP address for corporate e-mail server or router.	Contact your network administrator.
	Name of the corporate e-mail server or router.	Contact your network administrator.
	E-mail address of the user to receive alters.	Contact your network administrator.
Paging	Communication resource name used for paging.	V.24 communication resource with an asynchronous capable modem.
	Model of modem.	Located on the modem.
	Name of your paging service provider.	Contact your network administrator.
	Individual pager phone number, or pager PIN.	Contact your paging service provider.
SNMP Trap	TCP/IP address for the computer listening fro SNMP traps.	Contact your network administrator.
SEC MGR	IP address of the Security Manager central computer.	Contact your network administrator.

To run the PSDetect Quick Start Wizard:

1. On the command line, type `PSMENU` and press Enter.
2. Type `3` (PSDetect) and press Enter.
3. Type `20` (PSDetect QuickStart Wizard) and press Enter.
4. Follow the instructions in the wizard to configure the product.

Additional PSDetect Configuration

The following tasks configure PSDetect for use. To implement these additional configuration tasks, perform the steps in the following sections.

Set Up Monitors

The Work With Monitors window lets you work with each monitor that is running under the ZPSD subsystem. You can view and change the status of each monitor from this central location.

To set up monitors:

1. On the command line, type `PSMENU` and press Enter.
2. Type `3` (PSDetect) and press Enter.
3. Type `4` (Work with Monitors) and press Enter.
4. Press F10 (Verify Status). If any monitors are active, stop them by typing `9` (End) and pressing Enter.
5. In the Alert Monitor **OPT** field, type `20` (System Defaults) and press Enter.
6. On the Work With Alert Monitor Defaults window, ensure the user profile is authorized to all queues to be monitored and is authorized to perform relevant actions, and press Enter to continue.
7. In the Paging Monitor **OPT** field, type `20` (System Defaults) and press Enter.

8. On the Work With Paging Monitor System Defaults window, verify the communication resource name (by pressing F15) and other system defaults (such as Shared Resources & Dialing Prefix), and press Enter.

9. In the E-mail Monitor **OPT** field, type `20` (System Defaults) and, press Enter.

10. Modify the entries to conform to your environment. Function keys are available to configure or review various aspects of e-mail system values. Press Enter to update the e-mail system defaults.

11. Press F12 to continue. The PSDetect Main Menu is displayed.

Create Alert Filters

To help you set up alert filters to monitor messages, PSDetect includes the following predefined alert filters:

PSDAPI
: Checks for messages sent by users.

QHST
: Checks for attempts to sign on using an invalid password.

QSYSOPR
: Checks for hardware failure conditions.

You must maintain these alert filters for user profiles before monitoring message queues. For more information about predefined events, see the *User Guide for NetIQ Security Solutions for iSeries PSDetect.*

To create alert filters:

1. Type `3` (Work with Alert Filters) and press Enter.

2. Press F6 (Create) to define a message queue for filtering, if the appropriate queue does not exist.

3. On the Define Message Queue for Filtering window, provide the appropriate information and press Enter to accept the settings and return to the Work with Alert Filter menu.

4. ***If the Alert Queue is in HOLD status***, type `6` to release it and press Enter.

5. In the new alert filter **Opt** field, type `5` (Work with Filters) and press Enter.
6. Press F6 to create a new filter.
7. On the Work with Alert Filters window, provide the appropriate information and press Enter.
8. On the Alert Filter Selection Criteria window, provide the appropriate information and press Enter.
9. On the Work with Actions window, perform the following steps:
    a. Provide the appropriate information and press Enter.
    b. Specify the appropriate activity and press F4 to display a list of possible choices. Depending on the specified activity, PSDetect displays a secondary window for you to specify additional information.
    c. Provide the activity specific information and press Enter.
10. On the Selection Criteria window, press F12 to re-display the Work with Alert Filters window.
11. Add additional filters as needed.
12. Press F3 to return to the PSDetect Main Menu.
13. Type `4` (Work with Monitors) and press Enter.
14. Type `8` beside each monitor that you want to start, and press Enter.
15. Press Enter then F12.

Post-Configuration Procedures

After configuring PSDetect, perform the following post-configuration procedure if it applies to your system:

- ***If you are using AppManager,*** see "Configuring AppManager Support" on page 65.
- ***If you are using Security Manager***, see "Configuring Security Manager Support" on page 69.

Configuring Privilege Manager

Privilege Manager is a change control solution that lets you control access to managed servers by escalating privileges. Built-in auditing and reporting help you meet your compliance objectives. Offering a rich escalation model, Privilege Manager allows you to:

- Implement effective change control on servers
- Run object access failure reports to assure policy and regulatory compliance
- Increase operational security of your servers using just-in-time authorities and granular access control
- Ensure required changes are implemented and validated

Privilege Manager provides the escalated privilege solution you need to limit widespread authorities, show continuous regulatory compliance, and increase operational integrity.

Using Privilege Manager, you can limit regular access to your sensitive servers to a onetime or regularly scheduled maintenance window and assign the task to a specific user or user group.

To configure Privilege Manager, you must be authorized to PSSecure (PSS) and Privilege Manager (PSP) products. You can authorize users to products using option 70 (Utilities menu) from the NetIQ Product Access Menu. For more information, see "Authorizing Users to NetIQ Security Solutions for iSeries Products" on page 31.

After installing the NetIQ Security Solutions for iSeries products and authorizing users to Privilege Manager, see the *User Guide for NetIQ Security Solutions for iSeries - Privilege Manager.*

Configuring Communication in Heterogeneous Enterprises

NetIQ Security Solutions for iSeries integrate with other NetIQ security products to deliver centralized enterprise security management for heterogeneous enterprises. To allow your iSeries server to communicate with a centralized console, you must specify which computers can connect to the iSeries server, assign the appropriate ports for communication, and start the appropriate subsystem on your iSeries server.

To configure NetIQ Security Solutions for iSeries for use in heterogeneous enterprises, complete the following checklist.

☑	Steps	See Section
☐	**1.** Specify the host systems from which the Agent Communication Subsystem monitors for a connection.	"Authorizing Specific Host Systems" on page 61
☐	**2.** Configure the Agent Communication Subsystem.	"Configuring the Agent Communication Subsystem" on page 62
☐	**3.** Start the Agent Communication Subsystem.	"Starting the Agent Communication Subsystem" on page 63

Authorizing Specific Host Systems

The Agent Communication Subsystem allows you to specify the host systems from which it listens for a connection. The default value allows the Agent Communication Subsystem to listen for connections from any system.

To authorize specific host systems:

1. On the NetIQ Product Access Menu, type `70` (Utilities menu) and press Enter.
2. Type `3` (VigilEnt Agent Access Control) and press Enter.

3. ***If you want to explicitly define the access authority for each system to prevent unauthorized use***, delete the default access authority value (0.0.0.0) by typing `4`, and pressing Enter.

4. Press Enter to confirm the deletion.

5. Perform the following steps for each host that you want to authorize:

   a. Press F6 to add a new entry.

   b. Type the IP address or mask for new host system and press Enter.

6. Press F3 when all entries are complete.

7. ***If the Agent Communication Subsystem (ZPSE) is active***, you must stop and restart it for the changes to take effect. For more information about stopping the ZPSE subsystem, see "Ending the Agent Communication Subsystem" on page 64.

Configuring the Agent Communication Subsystem

Use the PSEnterprise Agent Communication window to change the configuration settings for the Agent Communication Subsystem.

To configure the Agent Communication Subsystem:

1. On the command line, type `PSECONFIG` and press Enter to display the PSEnterprise Agent Configuration window.

2. Make changes to the following fields as necessary:

   Agent Interface
   Specifies which computers can connect to the agent. The default value for this field is *ANY. If you are using Secure Configuration Manager and Security Manager, ensure this field is set to *ANY. To specify specific IP addresses that can connect to the agent, add IP addresses to the VigilEnt Agent Access Control window in the Utilities menu.

   Note
   If you have multiple NIC cards installed on the same network, you may need to specify the IP address of the NIC card registered to Secure Configuration Manager.

Agent Listening Port

Specifies the port where the iSeries Communication Agent listens for incoming requests from Core Services. The default value for this port is 1622.

Note

This port number must match the port specified for the agent in Secure Configuration Manager Console.

Core Listening Port

Specifies the port where the iSeries communication agent returns results to Secure Configuration Manager. The default value for this port is 1621.

Note

This port number must match the port specified in the Core Services Configuration Utility.

Logging Level

Specifies whether message tracking is enabled. Specify **0** to disable message tracking. Specify any other number to enable message tracking.

3. Press **F10** (Update).

Starting the Agent Communication Subsystem

To connect the iSeries server to the Secure Configuration Manager console, start the Agent Communication Subsystem on an iSeries server.

To start the Agent Communication Subsystem:

1. Access the command line on the iSeries server where PSAudit is installed by pressing F10 on any NetIQ Security Solutions for iSeries product menu.
2. Start the agent communication job in a subsystem on the server by typing the following command and pressing Enter:

   ```
   STRSBS PSCOMMON/ZPSE
   ```

   To automatically start this subsystem following an IPL, add the Start Subsystem command (`STRSBS PSCOMMON/ZPSE`) to the program indicated by the system value `QSTRUPPGM`.

Ending the Agent Communication Subsystem

To disconnect the iSeries server from the Secure Configuration Manager console, you must end the Agent Communication Subsystem on the iSeries server.

To end the Agent Communication Subsystem:

1. Access the command line on the iSeries server where PSAudit is installed by pressing F10 on any NetIQ Security Solutions for iSeries product menu.
2. Type the following command and press Enter:

   ENDSBS ZPSE *IMMED

   NetIQ Security Solutions for iSeries displays the following message:

   ```
   Ending of subsystem ZPSE in progress.
   ```

3. Verify the agent has ended by typing `WRKACTJOB SBS(ZPSE)` on the command line and pressing Enter.

   The Agent Communication Subsystem disconnects from the Secure Configuration Manager console when the end subsystem job completes.

Chapter 5
Configuring AppManager Support

The NetIQ AppManager Suite (AppManager) identifies problems in your environment; helps you assess the cause, location, and severity of these problems; and allows you to automatically correct or initiate other appropriate actions when problems occur.

PSDetect actively monitors your iSeries servers and alerts you in real-time if any suspicious activity or potential exposures occur. With the ability to send SNMP traps to AppManager, PSDetect provides real-time alerting to the AppManager centralized console, which monitors activity in your heterogeneous environment.

Perform the following steps to configure your iSeries servers to integrate with AppManager.

☑	**Steps**
☐	**1.** Ensure NetIQ Security Solutions for iSeries is installed on each server from which you want to forward alerts. For more information, see “Installation Checklist” on page 22.
☐	**2.** Configure PSDetect to send SNMP traps to AppManager. For more information see “Configuring SNMP Traps” on page 66.
☐	**3.** Configure AppManager to receive SNMP traps from PSDetect. For more information, see “Checking in the iSeries Knowledge Script” on page 67.

Configuring SNMP Traps

You can quickly and easily configure PSDetect to monitor your iSeries servers for critical events such as storage conditions and QSECOFR activity. When PSDetect detects these critical events, it can send SNMP traps containing event information to AppManager.

Before you begin the PSDetect QuickStart Wizard you need to know the IP address of the AppManager computer monitoring for SNMP traps.

To configure PSDetect to forward alerts to AppManager:

1. At the NetIQ Product Access Menu, type `3` (PSDetect) and press Enter.
2. Type `20` (PSDetect QuickStart Wizard) and press Enter.
3. Press Enter to run the wizard.
4. In step 15 (Configure SNMP Support), type `*YES` and press Enter.
5. In step 16 (SNMP listener address), type the TCP/IP address of the computer where the AppManager management server is installed.
6. Specify the events for which you want to monitor and send an SNMP trap to AppManager.
7. After the final question, the wizard displays a summary of your selections in a two-page window. Press Page Down to view the second page and Page Up to return to the first page.
8. Review your settings. When settings are correct for your environment, press Enter.
9. Press Enter to apply the settings.
10. Press Enter to exit the wizard.

For more information about configuring SNMP traps using PSDetect, see the *User Guide for NetIQ Security Solutions for iSeries PSDetect*.

Checking in the iSeries Knowledge Script

For AppManager to receive SNMP traps from PSDetect, you must check the iSeries JobInfo Knowledge Script into the AppManager repository and run it on the target computer.

To check in the iSeries Knowledge Script:

1. Start the AppManager Operator Console.
2. Click KS > Check In Knowledge Script.
3. Navigate to the JobInfo script that you downloaded from the NetIQ Web site.
4. Select the script and click Open.
5. Click the iSeries tab.
6. Select the JobInfo script from the Knowledge Script pane.
7. Drag the script to the TreeView pane and drop it on the target computer.
8. Set the job properties in the Properties window and press OK to run the script on the target computer.

For more information about using Knowledge Scripts in AppManager, see the NetIQ AppManager documentation.

Chapter 6
Configuring Security Manager Support

Security Manager is an enterprise-scale security monitoring product based on a distributed, tiered architecture that analyzes security incidents, automatically responds to threats, and provides safekeeping of important event information, from a simple-to-use central console.

NetIQ Security Solutions for iSeries integrate with two powerful Security Manager products to provide relief from your worst security event management problems:

Intrusion Manager

Intrusion Manager helps secure your enterprise from internal and external attacks. In real time, the product monitors, analyzes, and consolidates events from log files on monitored iSeries servers to detect a variety of occurrences and alert you of them. When significant events occur, Intrusion Manager sends alerts to the Intrusion Manager consoles and can email or page your staff so they can quickly respond.

With the ability to send real-time alerting to Security Manager, PSDetect provides iSeries data to a powerful enterprise-focused control center that enables you to automate and monitor security in small to large enterprises.

Log Manager

Log Manager provides a powerful, yet simple-to-use solution that collects log data from various sources throughout your enterprise. Log Manager consolidates the events to secure Microsoft SQL Server respositories that provide centralized access, which is critical for meeting audit requirements. Log Manager provides access to your data in the form of Summary, Forensic Analysis, and Trend Analysis reports.

Providing QAUDJRN data to Security Manager delivers an archival and forensics solution for managing event logs from iSeries servers throughout your enterprise in a single, central console.

Detecting Intrusions on iSeries Servers

Intrusion Manager for iSeries allows you to monitor iSeries events in real-time from a single enterprise-focused console. Intrusion Manager for iSeries also provides security knowledge so you can quickly understand and resolve any security issues occurring on your iSeries servers.

Perform the following steps to configure your iSeries servers to send alerts to Intrusion Manager.

☑	Steps
☐	**1.** Ensure NetIQ Security Solutions for iSeries is installed on each server from which you want to forward alerts. For more information, see “Installation Checklist” on page 22.
☐	**2.** Configure NetIQ Security Solutions for iSeries to communicate with Security Manager computers. For more information see “Configuring Communication in Heterogeneous Enterprises” on page 61.
☐	**3.** Configure PSDetect to forward alerts to Security Manager. For more information, see “Configuring PSDetect to Forward Alerts” on page 71.

☑	Steps
☐	**4.** Configure Privilege Manager to send event notifications to Security Manager. For more information, see “Configuring Privilege Manager to Send Event Notifications” on page 76.
☐	**5.** Import the Intrusion Manager for iSeries module into Security Manager. For information about importing a NetIQ module into Security Manager, see the *User Guide for Security Manager*.
☐	**6.** Specify the Security Manager central computer to monitor for iSeries data. For more information, see the *User Guide for Security Manager*.

Configuring PSDetect to Forward Alerts

PSDetect allows you to send important events to Security Manager using SNMP traps. You can easily forward pre-defined events using the PSDetect QuickStart Configuration Wizard or you can forward user-defined events by creating filters in PSDetect.

Forwarding Pre-defined Events

The PSDetect QuickStart Configuration Wizard helps you easily configure your server to send important events to Security Manager by guiding you through questions about pre-defined events you want to monitor, then PSDetect configures the product.

Before you begin the PSDetect QuickStart Wizard you need to know the IP address of the Security Manager central computer monitoring iSeries events.

To forward pre-defined PSDetect events to Security Manager:

1. From the NetIQ Product Access Menu, type `3` (PSDetect) and press Enter.
2. Type `20` (PSDetect QuickStart Wizard) and press Enter.
3. Press Enter to run the wizard.

4. Use the following table as a guide to run the PSDetect QuickStart Wizard. Type your entry and press Enter to move to the next question.

Step	Your Selection
1. Configure email support?	*NO
2. Configure paging support?	*NO
3. Configure Security Manager support?	*YES
4. Security Manager IP address	IP address of the Security Manager central computer
5. Configure SNMP support?	*NO
6. Monitor for storage conditions?	*YES
7. Action for storage condition?	*SEC MGR
8. Monitor changes to QAUDCTL?	*YES
9. Action for QAUDCTL changes?	*SEC MGR
10. Monitor QSECOFR activity?	*YES
11. Action for QSECOFR activity?	*SEC MGR
12. Monitor invalid signon attempts?	*YES
13. Action for invalid signon attempts	*SEC MGR
14. Monitor for rejected remote requests?	*YES
15. Action for rejected remote requests?	*SEC MGR
16. Start the PSDetect Monitors now?	*YES

5. After the final question, the wizard displays a summary of your selections. Press Page Down to view additional summary pages and Page Up to return to the first page.

6. ***If you need to change a setting***, press F12 repeatedly to redisplay the correct wizard page. Correct your selection and complete the wizard.

7. Review your settings. When they are correct for your environment, press Enter.
8. Press Enter to apply the settings.
9. Press Enter to exit the wizard and return to the PSDetect Main Menu.

Forwarding User-Defined Events

PSDetect allows you to create filters for events and forward these as alerts to Security Manager.

To forward user-defined PSDetect events to Security Manager:

1. From the NetIQ Product Access Menu, type `3` (PSDetect) and press Enter.
2. Configure the Trap Action Monitor system defaults by performing the following steps:
   a. From the PSDetect Main Menu, select Option `4` Work With Monitors and press Enter.
   b. Enter `20`=System Defaults next to the **Trap Action Monitor**.
   c. In the **Translate messages** field, enter `*YES`.
   d. Verify the **Test message OID** field contains the value `1.0` (can be changed if desired).
   e. In the **Test message** field, enter the test message that you want to send.
   f. Select `F10=Cfg SNMP`.
   g. Select Option `1`. Change SNMP attributes and press Enter.
   h. In the **Manager internet address** field, enter the IP address of the machine that has Security Manager installed.
   i. In the **Community name** field, type `PSDetect`.
   j. Press F12 once to go back to the Work with Trap System Defaults screen.
   k. Select `F15=Start SNMP`.

3. Start PSDetect subsystem and monitors by performing the following steps:

   a. To start the ZPSD subsystem, on the command line type `STRSBS PSDETECT/ZPSD` and press Enter.

   b. From the PSDetect Main Menu, select Option `4` Work With Monitors and press Enter.

   c. To start the Alert Monitor, Action Monitor and Trap Action Monitor, enter `8`=Start next to each monitor.

4. Create the trap packages by performing the following steps:

   a. From the PSDetect Main Menu, select Option `11`. PSDetect Action Setup Menu and press Enter.

   b. Select Option `10` Work with Trap Packages and press Enter.

   c. Select `F6`=Add.

   d. In the **Trap Package** field, enter a unique name up to 10 characters.

   e. In the **Description** field, enter a description that identifies the trap package.

   f. In the **Trap Number** field, enter any number. Use different numbers for this field if you are creating multiple trap packages.

   g. In the **Variable** field, select `F4`=Prompt to see a list of variables.

   h. To select the variable that you want to monitor, enter `1`=Select next to the variable.

   i. In the **Order** field, type any number and press Enter. The order defines the order of trap variable occurrence in the trap package.

   j. Repeat Steps **h** through **i** as needed.

5. Create PSDetect filter by performing the following steps:

   a. From the PSDetect Main Menu, select Option `3` Work With Alert Filters and press Enter.

   b. Enter `5`=Work with Filters next to the **QHST Alert Queue**.

   c. Select `F6`=Create to create a new filter and press Enter.

   d. In the **Filter sequence** field, enter a unique sequence number.

   e. In the **Filter description** field, enter a description that will help identify the filter.

   f. Type `Any` in the **Alert type** field.

   g. Type `00` in the **Severity filter** field.

   h. In the **Time range** field, enter the time range that you want to monitor.

   i. In the **Monitor on days** fields, enter a Y >in the days you want to monitor and press Enter.

   j. In the **Select or Omit** field, enter `S`=Select.

   k. In the **Message ID** field, enter the CPF message ID you want to monitor.

   l. In the **System name** field, enter `*All`.

   m. In the **Retrieve message description from** fields, enter `QCPFMSG` in the **Message file** field and `QSYS` in the **library** field.

   n. In the **Edit Compare Data** field, enter `N`.

   o. In the **Action** field, select `Trap`.

   p. In the **Delay before action** field, enter `0`.

   q. In the **Perform on system** field, enter `*LOCAL`.

Configuring Privilege Manager to Send Event Notifications

Privilege Manager logs system events to the user-defined audit journal and can generate notifications to NetIQ Security Solutions for iSeries PSDetect (PSDetect) and NetIQ Security Manager.

To send event notifications to Security Manager:

1. From the Privilege Manager main menu, type `10` (Work with PM Defaults) and press Enter.
2. In the **Alert Type** field, specify whether notifications are sent to PSDetect (`*PSDETECT`), Security Manager (`*SM`), both PSDetect and Security Manager (`*BOTH`), or none (`*NONE`), and then press Tab.
3. In the **Security Manager IP Address** field, specify the IP address of the Security Manager console where you want to send notifications.
4. Press Enter.

Auditing iSeries Log Data

Log Manager for iSeries securely provides QAUDJRN data most companies need to meet audit, forensic reporting, and legal requirements. Log consolidation, archival, analysis, and reporting help you understand security-related events across the enterprise while meeting government or company data-retention policies.

Perform the following steps to configure your iSeries servers to send QAUDJRN data to Log Manager.

☑	Steps
☐	**1.** Ensure NetIQ Security Solutions for iSeries is installed on each server from which you want to collect QAUDJRN data. For more information, see “Installation Checklist” on page 22.
☐	**2.** Configure and start the Agent Communication Subsystem. For more information, see “Starting the Agent Communication Subsystem” on page 63.
☐	**3.** Configure the iSeries server to log data to QAUDJRN. For more information, see “Configuring QAUDJRN Logging” on page 36.
☐	**4.** Specify the central computer to manage log data collected from the iSeries agents. For more information, see the *User Guide for Security Manager.*
☐	**5.** Specify the schedule for collecting iSeries log data. For more information, see the *User Guide for Security Manager.*

Chapter 7
Configuring Secure Configuration Manager Support

Secure Configuration Manager is an enterprise-scale configuration and vulnerability management product that analyzes security risks, ensures policy compliance, secures your IT assets, and streamlines the vulnerability management process. This enterprise-scalable product helps you to meet the following key vulnerability management goals:

- Identify vulnerabilities and potential threats across multiple platforms
- Reduce the time required to address vulnerabilities
- Respond quickly to improve policy compliance

With built-in security expertise to identify and help you address hundreds of known vulnerabilities, Secure Configuration Manager simplifies the often complex process of assessing and securing large-scale multi-platform enterprises.

Detecting Vulnerabilities on iSeries Servers

NetIQ Security Solutions for iSeries send QAUDJRN data to Secure Configuration Manager, which helps you manage the following types of vulnerabilities on your iSeries servers from a centralized console:

User profile

Vulnerabilities can occur with any user profile, whether it is a basic user profile or a powerful user profile, such as QSECOFR. Secure Configuration Manager generates reports when you run policy templates, security checks, or task suites. These reports help you identify user profile access and authority so you can immediately correct vulnerabilities. NetIQ Security Solutions for iSeries provide several utilities that help you enforce corrections. You can also correct vulnerabilities by creating and running actions on specific user and group profiles.

Object

Vulnerabilities can occur with any object, whether it is data, an application, or a computer. Secure Configuration Manager generates a report when you run a policy template or task suite. Object Authority Management (OAM) is the primary tool in PSSecure that will easily enable you to implement changes to force compliance to security policies. NetIQ Security Solutions for iSeries provide several utilities that help you enforce corrections. You can correct vulnerabilities by creating and running tasks on specific objects.

Network

Vulnerabilities can occur with any network component. When a network component is vulnerable, your computers and resources are equally vulnerable. The most common network vulnerabilities on the iSeries are a result of remote servers such as file, database, FTP, and TELNET having exit points that are not secure. This leaves transactions such as those done over ODBC wide open to vulnerabilities.

Secure Configuration Manager generates a report when you run a policy template or task suite. NetIQ Security Solutions for iSeries provide several utilities that help you enforce corrections. The PSSecure Remote Request Management (RRM) allows you to collect and view incoming remote transactions on your iSeries and also set up rules to configure object-level access.

Secure Configuration Manager provides built-in security expertise your staff can use to secure your enterprise, increase their knowledge, and obtain facts needed to correct vulnerabilities.

For information about detecting vulnerabilities on your iSeries servers using Secure Configuration Manager reports and security checks, see the *User Guide for Secure Configuration Manager*.

Note
Integration with NetIQ Security Solutions for iSeries 8.1 requires Secure Configuration Manager 5.7 or later.

Perform the following steps to configure support for Secure Configuration Manager.

☑	Steps
☐	**1.** Ensure NetIQ Security Solutions for iSeries is installed on each iSeries server you want to audit. For more information, see “Installation Checklist” on page 22.
☐	**2.** Ensure security journaling is configured and enabled. For more information, see “Configuring QAUDJRN Logging” on page 36.
☐	**3.** Configure NetIQ Security Solutions for iSeries to communicate with Secure Configuration Manager computers. For more information, see “Configuring Communication in Heterogeneous Enterprises” on page 61.
☐	**4.** ***If you are running Secure Configuration Manager 5.7***, update the Secure Configuration Manager console computers to enable NetIQ Security Solutions for iSeries changes. For more information, see “Updating Secure Configuration Manager Console Computers” on page 82.

Updating Secure Configuration Manager Console Computers

Update the Secure Configuration Manager console computers to enable NetIQ Security Solutions for iSeries changes.

To apply the Secure Configuration Manager client update:

1. Log on to the Secure Configuration Manager console computer with a local administrator account.
2. Insert the NetIQ Security Solutions for iSeries product CD.
3. Browse to the SCMUpgrades folder on the installation CD.
4. Run the SCM57_Hotfix70969.exe file.
5. Follow the instructions in the wizard until you have finished installing the hotfix.
6. Repeat Steps **1** through **5** on each Secure Configuration Manager console computer.

Providing IASP Support

Independent Auxiliary Storage Pools (IASPs) are physical collections of disks that are independent from the rest of the storage on a system. Since each IASP contains all necessary system information associated with the data it contains, you can take an IASP offline, bring it online without an IPL, or switch between systems while the system is active.

Secure Configuration Manager task reports provide the name of the IASP from which NetIQ Security Solutions for iSeries gathered QAUDJRN log data. You can specify which ASP groups provide log data to Secure Configuration Manager. For more information, see "Including or Excluding ASP Groups From Task Reports" on page 84. You can also specify which libraries provide log data to Secure Configuration Manager. For more information, see "Including or Excluding Libraries From Task Reports" on page 85.

The following Secure Configuration Manager task reports provide IASP data:

- New Objects
- Restore Objects
- Damaged Objects
- Object Counts by Owner
- Object Counts by System Name
- Unsaved Objects
- Largest Objects
- Object Source
- Missing Objects Source
- Object Usage
- Changed Objects
- Object Creator
- File Needing Reorganization
- File Usage
- Largest Files
- Source Member Changes
- New Source Files
- New Data Files
- Changed Files

- Journaled Files
- Library Analysis by Library
- New Libraries

Including or Excluding ASP Groups From Task Reports

PSAudit allows you to specify which ASP groups provide data to Secure Configuration Manager. If you do not specify ASP groups to include or exclude, only the system ASP groups on your server provide data to Secure Configuration Manager.

To include or exclude ASP groups from task reports:

1. From the PSAudit Main Menu, type 1 (System Auditing and Reporting) and press Enter.
2. Type 1 (Load Auditing Database Menu) and press Enter.
3. Type 3 (Set ASP Group List for Object Load) and press Enter.
4. ***If you want task reports to query all ASP groups except those specified***, type `E` in the **ASP Groups to Exclude/Include** field and press Enter.
5. ***If you want task reports to query only specified ASP groups***, type `I` in the **ASP Groups to Exclude/Include** field and press Enter.
6. Specify the ASP group names you want excluded or included in the **ASP Groups** field.
7. Press `F8`.
8. Type `Y` and press Enter.
9. Press F3 until you return to the PSAudit Main Menu.

For information about running task reports, see the *User Guide for Secure Configuration Manager*.

Including or Excluding Libraries From Task Reports

PSAudit allows you to specify the libraries from which Secure Configuration Manager gathers data. If you do not specify libraries to include or exclude, all libraries within the specified ASP groups on your server provide data to Secure Configuration Manager.

For more information about including or excluding data from ASP groups, see "Including or Excluding ASP Groups From Task Reports" on page 84.

To include or exclude libraries from task reports:

1. From the PSAudit Main Menu, type 1 (System Auditing and Reporting) and press Enter.
2. Type 1 (Load Auditing Database Menu) and press Enter.
3. Type 2 (Set Libraries List for Object Load) and press Enter.
4. ***If you want to manually set the maximum number of active batch jobs run concurrently on your server***, specify a number between 1 and 1000 in the **No. of Concurrent Load Jobs** field. Setting this field to *NOMAX, runs all submitted active batch jobs regardless of size.
5. ***If you want the server to automatically set the maximum number of active batch jobs run concurrently***, type *AUTO in the **No. of Concurrent Load Jobs** field.
6. ***If you want the IASP report to query all libraries except those specified***, type `E` in the **Libraries to Exclude/Include** field and press Enter.
7. ***If you want the IASP report to query only specified libraries***, type `I` in the **Libraries to Exclude/Include** field and press Enter.

   Note
   - If the ASP group containing the specified library has been excluded from Secure Configuration Manager task reports using the Set Auxiliary Storage Pool Defaults screen, data from this library is not returned.
   - NetIQ Security Solutions for iSeries cannot collect data from an inactive IASP.

8. Specify the libraries you want excluded or included in the **Libraries** field.

9. Press F8.
10. Type Y and press Enter.
11. Press F3 until you return to the main menu.

Running an IASP Report from the iSeries Terminal

PSAudit allows you to run the Secure Configuration Manager task reports that contain IASP information from an iSeries command line. PSAudit gathers the report information and provides the results in the specified outfile.

For more information about Secure Configuration Manager reports that contain IASP information, see "Providing IASP Support" on page 82.

To run an IASP report from the iSeries terminal:

1. From the NetIQ Product Access Menu, type 1 (PSAudit) and press Enter.
2. Press F10 (Command entry).
3. Type the following command and press F4:
   `PSRUNPRT REPORTID`
   where *REPORTID* is the ID for the report you want to run.

Report Title	Report ID
New Objects	SAR00001
Restore Objects	SAR00002
Damaged Objects	SAR00003
Object Counts by Owner	SAR00004
Object Counts by System Name	SAR00005
Unsaved Objects	SAR00006
Largest Objects	SAR00007
Object Source	SAR00008

Report Title	Report ID
Missing Objects Source	SAR00009
Object Usage	SAR00010
Changed Objects	SAR00011
Object Creator	SAR00012
File Needing Reorganization	SAR00013
File Usage	SAR00014
Largest Files	SAR00015
Source Member Changes	SAR00016
New Source Files	SAR00017
New Data Files	SAR00018
Changed Files	SAR00019
Journaled Files	SAR00020
Library Analysis by Library	SAR00021
New Libraries	SAR00022

4. Enter the appropriate values for the following parameters:

Report Id
Specifies the code name of the generated report. This field is display only.

Report Description
Specifies the name of the selected report. This field is informational only.

ASP Group Name

Specifies the name of the Auxiliary Storage Pool groups included in the report. This field works in conjunction with the Set Auxiliary Storage Pool Defaults screen. Valid values are as follows:

name - Specifies the name of the ASP group included in the report.

***ALL** - Specifies that the system ASP group and all independent ASP groups are included in the report.

***SYSBAS** - Specifies that only the system ASP group is included in the report.

Library Name

Specifies which libraries within the ASP groups the report includes. This field works in conjunction with the Set Object Load Defaults screen. Valid values are as follows:

name - Specifies a specific library within the ASP group.

generic* - Specifies a generic value for a group of libraries.

***ALL** - Specifies all libraries within the ASP group.

Reload

Specifies whether to reload the database before running the report. Valid values are `*NO` and `*YES`.

Starting Date and Time

Specifies the beginning date and time of the period for which you want report data.

Starting date

Specifies the beginning date of the period for which you want report data. Valid values are as follows:

date - Specifies the date in the *JOB format.Julina date formats are not supported.

***CURR** - Specifies the current date.

***PRVMS** - Specifies the previous month's starting date.

***PRVME** - Specifies the previous month's ending date.

***PRVWK** - Specifies the previous week's starting date (last 7 days).

***PRVDY** - Specifies the previous day's date.

***CURMS** - Specifies the current month's starting date.

Starting time

Specifies the beginning time of the period for which you want report data. Enter the starting time in the `hh:mm:ss` format.

Ending Date and Time

Specifies the ending date and time of the period for which you want report data. Enter the starting time in the `hh:mm:ss` format.

Ending date

Specifies the ending date of the period for which you want report data. Valid values are as follows:

date - Specifies the date in the *JOB format.

***CURR** - Specifies the current date.

***PRVMS** - Specifies the previous month's starting date.

***PRVME** - Specifies the previous month's ending date.

***PRVWK** - Specifies the previous week's starting date (last 7 days).

***PRVDY** - Specifies the previous day's date.

***CURMS** - Specifies the current month's starting date.

Ending Time

Specifies the ending time of the period for which you want report data. Enter the starting time in the `hh:mm:ss` format.

Filter Name

Specifies the name of the user-defined filter to eliminate data from the report. Valid values are as follows:

***NONE** - Specifies that the data is not filtered.

filter name - Specifies the name of the filter to be used. Press F4 to display a list of available filters.

File to Receive Output

Specifies the name of the outfile where you want to write the report data. If a filter and an outfile are specified, then the filter applies to the outfile as well as the report output.

PSRUNRPT writes only to member *FIRST of the output file specified in the OUTFILE parameter, but it supports use of multiple members when the command OVRDBF is issued on an i5/OS command line. Valid values are as follows:

***NONE** - Specifies that the report data will not be placed in a data file.

name - Specifies the name and library of the database file where the output of the command is placed.

Library

Specifies the library where the file is located. Valid values are as follows:

name - Specifies the name of the library.

***LIBL** - Searches the jobs active library list for the file specified in the **File to Receive Output** field.

***CURLIB** - Specifies the library where the outfile is created.

Replace or Add records

Specifies whether data is added to a file or replaces existing data. Valid values are as follows:

***REPLACE** - Replaces existing file data with new reported data.

***ADD** - Adds the new reported data to the end of the existing file.

Spool File
Specifies whether the report generates a spool file. Specify *NO for IASP reports.

Run Interactively
Specifies whether the job is executed interactively or in batch mode. Valid values are as follows:

***NO** - Submits job for batch processing.

***YES** - Executes job interactively.

Synchronize Client
IASP reports do not support this field. This field is available only if you press F9.

Providing IFS Support

The iSeries operating system contains an integrated file system (IFS) which supports stream input/output and storage management similar to operating systems on Unix and personal computers. The integrated file system on the iSeries allows applications on file systems such as Unix and personal computers to access stream files, database files, documents, and other objects stored on your server.

The Secure Configuration Manager task reports provide directory and file information from the iSeries IFS.

Note
*DOC and *FDR IBM special objects are not included in Secure Configuration Manager IFS reports.

The following Secure Configuration Manager task reports and action provide IFS information.

- Files that are set user ID, SUID
- Files that are set group ID, SGID

- Files that are world writeable
- Directories that are world writeable
- World writeable directories that are not sticky
- Load IFS Information

For information about running task reports in Secure Configuration Manager, see the *User Guide for Secure Configuration Manager*.

Appendix A
Upgrading NetIQ Security Solutions for iSeries

This chapter outlines the steps to upgrade NetIQ Security Solutions for iSeries 8.0 products to the most recent version. If NetIQ Security Solutions for iSeries products are not currently installed on your system, see “Installation Checklist” on page 22.

NetIQ Security Solutions for iSeries Upgrade Checklist

When you perform an upgrade, the NetIQ Security Solutions for iSeries installation process installs all NetIQ Security Solutions for iSeries products, product options, and PTFs from the most recent Cumulative PTF on your iSeries server. To determine if a Cumulative PTF is available, see the NetIQ Security Solutions for iSeries installation CD or the NetIQ Web site at www.netiq.com/support/iseries.

If you are using Remote Request Management (RRM) and have exit programs installed, the upgrade process removes the RRM exit programs, cycles the servers, re-installs the exit programs, and cycles the servers again.

You can upgrade your NetIQ Security Solutions for iSeries products by completing the following checklist.

☑	Steps
☐	**1.** Review Release Notes by running the `Setup.exe` file from your installation media on your computer.
☐	**2.** ***If you are running i5/OS V6R1***, must apply IBM PTF MF44237 before accessing the NetIQ Security Solutions for iSeries product.
☐	**3.** Ensure your server meets the software, hardware, and permissions requirements for upgrading the NetIQ Security Solutions for iSeries products. For more information, see “Requirements” on page 15.
☐	**4.** Ensure you upgrade NetIQ Security Solutions for iSeries products after regular work hours to reduce the impact on iSeries users. The PSINSTALL command ends all NetIQ Security Solutions for iSeries processes.
☐	**5.** To prevent processes from running during the upgrade, run the upgrade in restricted state. Processes can potentially lock NetIQ Security Solutions for iSeries objects and cause the upgrade to fail and end abnormally. For more information about running in restricted state, see your IBM documentation.
☐	**6.** ***If you are using Help/Systems' Robot/SCHEDULE and are not upgrading in restricted state***, ensure you hold NetIQ Security Solutions for iSeries tasks and jobs. If you do not hold jobs scheduled by Help/Systems' Robot/SCHEDULE, job processes can potentially lock NetIQ Security Solutions for iSeries objects and cause the upgrade to fail and end abnormally.

☑	Steps
☐	**7.** *If you are using IBM Advanced Job Scheduler and are not upgrading in restricted state*, ensure you hold NetIQ Security Solutions for iSeries jobs and jobs containing the following commands: STRAAAPI, ALOG, ALOGPRT, ASO, BLCRTCLT, DBA, DBALOG, DDRPT, DDRPTA, DSPFLD, PSINSTALL, PSMENU, PSUNINST, STRAA, STRBL, STRDD, STRMS, STROAM, STRRRM, STRSFE, ZPASS. If you do not hold jobs scheduled by IBM Advanced Job Scheduler, job processes can potentially lock NetIQ Security Solutions for iSeries objects and cause the upgrade to fail and end abnormally.
☐	**8.** *If you want to maximize storage space on your server*, backup then purge PSAudit product files ALPF01and ALPF03. For more information, see “Purging PSAudit Product Files” on page 100.
☐	**9.** Back up your system.
☐	**10.** Log on using a user profile with at least `*ALLOBJ` and `*SECADM` special authorities.
☐	**11.** Ensure user profiles PSOBJOWN and PSOBJOWNS are enabled.
☐	**12.** Ensure user profile PSOBJOWNS has a user class of *SECOFR and the following special authorities: • *ALLOBJ • *AUDIT • *IOSYSCFG • *JOBCTL • *SAVSYS • *SECADM • *SERVICE • *SPLCTL

☑	Steps
❑	**13.** Ensure the following product libraries contain at least one physical data file or data area object: • PSAudit • PSCommon • PSDetect • PSSecure
❑	**14.** Ensure library PSCOMMON is not included in your library list.
❑	**15.** Issue the following command to see if exit point QIBM_QTMT_WSG is installed. `WRKREGINF QIBM_QTMT_WSG`
❑	**16.** *If exit point QIBM_QTMT_WSG is installed*, use the Remote Request Management Work with Exit Programs screen to determine if exit program NW0001E is specified for this exit point. For more information about working with exit programs, see the *User Guide for Remote Request Management*.
❑	**17.** *If exit program NW0001E is specified for exit point QIBM_QTMT_WSG*, remove it by performing the procedure outlined in knowledge base article NETIQKB46825.
❑	**18.** Issue the following command to display the setting of system value QFRCCVNRST. `DSPSYSVAL QFRCCVNRST`
❑	**19.** *If QFRCCVNRST is not set to 2*, issue the following command to change the setting: `CHGSYSVAL QFRCCVNRST VALUE('2')` Ensure to note the current value of this setting. After the upgrade is complete you will reset the system value.
❑	**20.** Ensure the CRTLIB command ASP Number parameter is set to 1 by typing `CRTLIB` on the iSeries command line and pressing F4.

☑	Steps
☐	**21.** *If the CRTLIB command ASP Number is not set to 1*, issue the following command to change the setting: `CHGCMDDFT CMD(QSYS/CRTLIB) NEWDFT('ASP(1)')` Ensure to note the current value of this parameter. After the upgrade is complete you will reset the parameter value.
☐	**22.** Note the setting of system value QALWOBJRST on your server. The upgrade program changes this setting to *ALWPGMADP.

☐	**23.** Issue the following commands to ensure there are no locks on product libraries.
	`WRKOBJLCK OBJ(PSAUDIT) OBJTYPE(*LIB)`
	`WRKOBJLCK OBJ(PSCOMMON) OBJTYPE(*LIB)`
	`WRKOBJLCK OBJ(PSDETECT) OBJTYPE(*LIB)`
	`WRKOBJLCK OBJ(PSSECURE) OBJTYPE(*LIB)`

☐	**24.** *If you are installing the product from media*, load the media in the appropriate iSeries drive.
☐	**25.** ***If you are installing the product from media***, on the command line, type the following command and press Enter. `RSTLICPGM LICPGM(1PSI001) DEV(`*NNNNN*`)` where *NNNNN* is the the name of the optical device that contains the NetIQ Security Solutions for iSeries CD.
☐	**26.** *If you are installing the product from a save file downloaded from the NetIQ Web site*, on the command line, type the following command and press Enter. `RSTLICPGM LICPGM(1PSI001) DEV(*SAVF) SAVF(`*library/file*`)` where *library/file* is the name of the library and save file that you downloaded from the NetIQ Web site and uploaded to your iSeries server.
☐	**27.** On the command line, type `PSINSTALL` and press F4 (Prompt).

☑	Steps
☐	**28.** In the **Device** field, type the name of the optical device that contains the NetIQ Security Solutions for iSeries CD. Type *SAVF file if you are installing the product from a save file downloaded from the NetIQ Web site.
☐	**29.** Review the remaining parameters and make any necessary changes, then press Enter. For more information about PSINSTALL parameters, see “Completing PSINSTALL Parameters” on page 26.
☐	**30.** *If you are running in restricted state*, batch job PSCOMAGENT starts running after you come out of restricted state.
☐	**31.** ***If you want to use the RRM Plug-in for iSeries Navigator with PSSecure - RRM***, install iSeries Navigator on your computer. For more information about installing iSeries Navigator, see “New Installation of RRM Plug-in for iSeries Navigator” on page 108.

☑	Steps
☐	**32.** *If you changed the QFRCCVNRST system value setting*, issue the following command to reset the system value: `CHGSYSVAL QFRCCVNRST VALUE('N')` where *N* is the value you recorded in Step **18**.
☐	**33.** *If you are using Robot job scheduler and did not upgrade in restricted state*, ensure you re-activate NetIQ Security Solutions for iSeries tasks and jobs.
☐	**34.** *If you are using IBM Advanced Job Scheduler and did not upgrade in restricted state*, ensure you re-activate NetIQ Security Solutions for iSeries jobs and jobs containing the following commands: STRAAAPI, ALOG, ALOGPRT, ASO, BLCRTCLT, DBA, DBALOG, DDRPT, DDRPTA, DSPFLD, PSINSTALL, PSMENU, PSUNINST, STRAA, STRBL, STRDD, STRMS, STROAM, STRRRM, STRSFE, ZPASS.
☐	**35.** *If you are using ShowCase Suite from SPSS and want to secure the exit point with RRM*, use the RRM Work with Exit Points screen to add exit program PSCOMMON/NW0001E to exit point SC_QUERY_ROW_SEC.
☐	**36.** *If you are using Secure Configuration Manager to detect vulnerabilities on your iSeries servers*, ensure you re-register the iSeries agent and endpoints.
☐	**37.** *If you are using Privilege Manager and journal Administrator actions*, you must turn auditing back on. For more information about turning on auditing, see the *User Guide for Privilege Manager*.

Purging PSAudit Product Files

The retention and removal of system auditing data depends on the size of your iSeries server, the system utilization and workload, the amount of information gathered, and the amount of available DASD storage space. To maximize storage space of your server, you can save the PSAudit product file information to tape and remove the data from the log history.

To purge PSAudit product files:

1. From the NetIQ Product Access Menu, type 1 (PSAudit) and press Enter.
2. Type 2 (System Access Analysis) and press Enter.
3. Type 2 (Purge Logged Data) and press Enter.
4. Review the following parameters and make changes as necessary.

   Save Logged Data Before Purge
   Specifies whether to save the log information before purging.

   Device
   Specifies the tape device name to where the logged data is saved.

   Before Date
   Specifies the date to which the purge will be limited. All logged information before the date entered will be purged. Use the date format MM/DD/YY.

   For Batch Environment
   The date must be enclosed with single quotes. If you are saving the data, the device must also be enclosed with single quotes.

5. Submit the purge log data job using one of the following functions:

Enter
Performs the full purge of summary and detail job log information.

F7=Purge ALL Detail and Access Information
Removes all access summary and detail job log information.

F9=Purge ALL Detail Job Log Information
Removes detail job log information only.

Deleting Temporary Libraries

Do not delete temporary libraries for 90 days after the upgrade. Before deleting temporary libraries, ensure the upgrade was successful, all customization is correct, and the temporary libraries are backed up.

Note
Only delete libraries with TEMP in the library name.

To delete all NetIQ temporary libraries:

1. On the command line, type the following command and press Enter.
   `WRKLIB PS*`
2. Type `4` in the **Opt** field to the left of the libraries you want to delete. The NetIQ Security Solutions for iSeries Upgrade creates temporary libraries with the following formats:

   `PS*TEMP`

   `PS*TEMP##`

   where `*` is the module identification.
3. Press Enter to delete the selected libraries from your system.

Appendix B
Installing Cumulative PTFs

Product Temporary Fixes (PTFs) apply product updates created since the NetIQ Security Solutions for iSeries base release. A Cumulative PTF consists of all individual PTFs created between successive releases of the NetIQ Security Solutions for iSeries products. To determine if a Cumulative PTF is available, see the NetIQ Security Solutions for iSeries installation CD or the NetIQ Web site at www.netiq.com/support/iseries.

Note

When installing a Cumulative PTF, the NetIQ Security Solutions for iSeries installation process installs **all** NetIQ Security Solutions for iSeries products and options on your iSeries server, as well as the PTFs from the Cumulative PTF. For more information about system requirements, see "Requirements" on page 15.

Individual PTFs for NetIQ iSeries products and other support services are available on the NetIQ Web site at: www.netiq.com/support/iseries or by contacting NetIQ Technical Support.

Note

Apply Cumulative PTF maintenance of NetIQ Security Solutions for iSeries products after regular work hours to reduce the impact on other users. The command used to install the Cumulative PTF (PSINSTALL) ends all NetIQ processes.

If you have RRM exit programs installed, this process removes the RRM exit programs, cycles the servers, re-installs the exit programs, and cycles the servers again.

The following procedure provides instructions for applying all PTFs included in the most recent NetIQ Security Solutions for iSeries Cumulative PTF.

☑	**Steps**
☐	**1.** Review the Cumulative PTF by running the `Setup.exe` file from your installation media on your computer.
☐	**2.** Print the Service Pack Release Notes from your Web browser.
☐	**3.** Back up your iSeries system.
☐	**4.** Ensure NetIQ Security Solutions for iSeries libraries are not included in your library list.
☐	**5.** *If you are using Help/Systems' Robot Job Scheduler*, ensure you hold NetIQ Security Solutions for iSeries tasks and jobs. If you do not hold jobs scheduled by Help/Systems' Robot Job Scheduler, job processes can potentially lock NetIQ Security Solutions for iSeries objects and cause the Cumulative PTF to fail and end abnormally.
☐	**6.** *If you are using IBM Advanced Job Scheduler*, ensure you hold NetIQ Security Solutions for iSeries jobs and jobs containing the following commands: ALOG, ALOGPRT, ASO, BLCRTCLT, DBA, DBALOG, DDRPT, DDRPTA, DSPFLD, PSINSTALL, PSMENU, PSUNINST, STRAA, STRAAAPI, STRBL, STRDD, STRMS, STROAM, STRRRM, STRSFE, ZPASS. If you do not hold jobs scheduled by IBM Advanced Job Scheduler, job processes can potentially lock NetIQ Security Solutions for iSeries objects and cause the Cumulative PTF to fail and end abnormally.
☐	**7.** ***If you are installing the product from media***, load the media in the appropriate iSeries drive.

☑	Steps
☐	**8.** Perform all steps listed in the Special Notes / Instructions section of the Cumulative PTF Service Pack that apply to your server.
☐	**9.** Log on to the iSeries using a user profile with at least *ALLOBJ and *SECADM special authorities.
☐	**10.** Ensure the system value for QALWOBJRST is *ALL or *ALWPGMADP.
☐	**11.** On the command line, type PSINSTALL and press F4 (Prompt).
☐	**12.** In the **Device** field, type the name of the optical device that contains the NetIQ Security Solutions for iSeries CD. Type *SAVF file if you are installing the product from a save file downloaded from the NetIQ Web site.
☐	**13.** Review the remaining parameters and make any necessary changes, then press Enter to begin installation. For more information about PSINSTALL parameters, see “Completing PSINSTALL Parameters” on page 26.
☐	**14.** *If you are using Robot job scheduler*, ensure you re-activate NetIQ Security Solutions for iSeries tasks and jobs.
☐	**15.** *If you are using IBM Advanced Job Scheduler*, ensure you re-activate NetIQ Security Solutions for iSeries jobs and jobs containing the following commands: ALOG, ALOGPRT, ASO, BLCRTCLT, DBA, DBALOG, DDRPT, DDRPTA, DSPFLD, PSINSTALL, PSMENU, PSUNINST, STRAA, STRAAAPI, STRBL, STRDD, STRMS, STROAM, STRRRM, STRSFE, ZPASS.

Appendix C
Installing the RRM Plug-in for iSeries Navigator

This chapter discusses considerations for installing the RRM Plug-in for iSeries Navigator, and provides detailed instructions for installation and upgrade.

Before you perform a new installation or an upgrade of the RRM Plug-in for iSeries Navigator, complete all applicable procedures to install and configure PSSecure RRM. For more information about installing PSSecure RRM, see "Installation Checklist" on page 22.

An installation or upgrade of the RRM Plug-in for iSeries Navigator consists of two parts: the server component and the client component.

Use the NetIQ Security Solutions for iSeries product CD to install the server component on your iSeries server. Use iSeries Navigator Selective Setup to install the client component files on a computer.

Requirements

To install or upgrade the RRM Plug-in for iSeries Navigator, your environment must meet the following requirements.

Category	Minimum Requirement
iSeries Server	• i5/OS V5R3 • NetIQ Security Solutions for iSeries 8.1
Client Computer	• Windows XP • Client Access Express Release 5 Version 1 or later • Access to the following IFS path on the server where the Operations Navigator Plug-in files are installed: \QIBM\USERDATA\GUIPLUGIN\PENTASAFE.SECURITY

New Installation of RRM Plug-in for iSeries Navigator

This section provides instructions for performing a new installation of the RRM Plug-in for iSeries Navigator.

For more information about upgrading the RRM Plug-in for iSeries Navigator, see "Client Upgrade Procedure" on page 112.

☑	**Steps**
☐	**1.** Install the client component on each computer that will support the RRM Plug-in for iSeries Navigator. To install the client component, perform the steps in "Client Installation" on page 109.
☐	**2.** Install the AFP Workbench view to view reports using the RRM Plug-in for iSeries Navigator. For more information, see "AFP Workbench Viewer Installation" on page 111.
☐	**3.** Verify the installation of the RRM Plug-in for iSeries Navigator. For more information, see "Verify Installation/Upgrade" on page 110.
☐	**4.** Install the online Help for the RRM Plug-in for iSeries Navigator. For more information, see "Install Help" on page 111.

Client Installation

After installing the server component of the RRM Plug-in for iSeries Navigator, you must install the client component on each computer that supports the RRM Plug-in for iSeries Navigator.

To install the client component:

1. Ensure you have iSeries Navigator Version 5, Release 3 or later installed on the computer. To see the version using the iSeries Navigator Help menu under the topic "About iSeries Navigator."
2. At the Windows Start menu, click **Programs > IBM iSeries Access For Windows > Selective Setup**

   The IBM iSeries Navigator Selective Setup program starts.
3. Click **Next** to enter Setup.

4. ***If iSeries Navigator displays the message Components Cannot Be Installed***, ensure the RRM Plug-in for iSeries Navigator is not listed. Click **Next** to continue. If the RRM Plug-in for iSeries Navigator is listed, contact NetIQ Technical Support.

5. In the Plug-in Selection window, expand **iSeries Navigator**, select the following components, and click **Next**:

   - iSeries Navigator
   - PentaSafe RRM Plug-in For Ops Nav

   If **PentaSafe RRM Plug-in For Ops Nav** is not listed, ensure the server named in Step **4** is the server where the Server component of the RRM Plug-in for iSeries Navigator was installed.

6. On the iSeries Navigator Start Copying Files window, click **Next**.

7. The iSeries Navigator copies the required RRM Plug-in for iSeries Navigator files to the computer. Restart your computer if prompted.

Verify Installation/Upgrade

Verify the successful completion of a new installation or upgrade of the RRM Plug-in for iSeries Navigator.

To verify installation:

1. Open iSeries Navigator.

2. Expand the node for the server where the RRM Plug-in for iSeries Navigator was installed. iSeries Navigator displays a window indicating that it has discovered new instances of the RRM Plug-in for iSeries Navigator.

3. After the scan is complete, select **PentaSafe Security** from the tree. The RRM Plug-in for iSeries Navigator loads the PentaSafe RRM tree nodes, such as **Collected**.

Install Help

The RRM Plug-in for iSeries Navigator Help is a compressed file. The first time you click a Help button on a RRM Plug-in for iSeries Navigator window, you are asked if you want to install Help.

To install online Help:

1. Click **Yes**. The WinZip Self-Extractor displays installation instructions.
2. Click **OK**.
3. Ensure the **Unzip to folder** field value is ".\" and click **Unzip** to install the Help files.
4. When the files are installed, Winzip displays a message showing the number of files installed. Click **OK**.
5. Click **Close**. Windows Explorer displays the selected Help topic.

AFP Workbench Viewer Installation

The RRM Plug-in for iSeries Navigator uses iSeries Navigator's AFP Workbench Viewer to display reports. If you do not have the viewer installed and you want to view reports using iSeries Navigator, you can install the AFP Workbench Viewer from the Client Access installation CD.

To install the AFP Workbench Viewer:

1. Click **Selective Upgrade**.
2. Page down the list of components until you see AFP Workbench Viewer.
3. Select **AFP Workbench Viewer** and complete the installation.

Client Upgrade Procedure

After upgrading the server component of the RRM Plug-in for iSeries Navigator, you must upgrade the client component on each computer that supports the RRM Plug-in for iSeries Navigator.

To upgrade the client component on each computer that will support the RRM Plug-in for iSeries Navigator:

1. Uninstall the RRM Plug-in for iSeries Navigator client by performing the steps in "Uninstall RRM Plug-in for iSeries Navigator" on page 113.
2. At the Windows Start menu, click **Programs > IBM iSeries Access For Windows > Selective Setup**.

   The IBM iSeries Navigator Selective Setup program starts.
3. When the RRM Plug-in for iSeries Navigator is uninstalled, click **Next** on the Selective Setup wizard. You may have to restart your computer.
4. On the Selective Setup Options window, ensure a drive is mapped to the **QIBM** directory on the Plug-in Installation Server. iSeries Navigator determines which components are currently installed.
5. ***If iSeries Navigator displays the message Components Cannot Be Installed***, ensure the RRM Plug-in for iSeries Navigator is *not* listed. Click Next to continue. If the RRM Plug-in for iSeries Navigator is listed, contact NetIQ Technical Support.
6. In the Component Selection window, expand **iSeries Navigator**, select the following components, and click **Next**:

   - iSeries Navigator Base Support
   - PentaSafe RRM Plug-in For Ops Nav

   If the PentaSafe RRM Plug-in For Ops Nav is not listed, ensure the server named in Step **4** is the server where the Server component of the RRM Plug-in for iSeries Navigator was installed.

7. On the iSeries Navigator Start Copying Files window, click **Next**.

8. The iSeries Navigator copies the required RRM Plug-in for iSeries Navigator files to the computer. Restart your computer if prompted.

Uninstall RRM Plug-in for iSeries Navigator

You must uninstall the NetIQ RRM Plug-in for iSeries Navigator from each computer where the RRM Plug-in for iSeries Navigator is installed.

To uninstall the RRM Plug-in for iSeries Navigator:

1. Click **Start > Programs > IBM iSeries Access For Windows > Selective Setup**. The IBM iSeries Navigator Selective Setup program starts.

2. On the Selective Setup Options window, select **Ignore. I'm only going to uninstall components.**

3. Click **Next**.

4. On the Component Selection window, expand **iSeries Navigator**, clear the **PentaSafe RRM Plug-In for iSeries Nav** check box, and click **Next**.

5. On the Start Copying Files confirmation window, click **Next**.

6. If requested, restart the computer.

Appendix D
Uninstalling the Software

If necessary, you can uninstall NetIQ Security Solutions for iSeries products by completing the steps in the following checklist. Performing these steps removes NetIQ exit programs, scheduled jobs referencing NetIQ objects, libraries, authorization lists, user profiles, and commands copied to QGPL during installation.

Note

- To prevent processes from running during the uninstall that can lock NetIQ Security Solutions for iSeries objects, uninstall the NetIQ Security Solutions for iSeries product in restricted state. For more information about running in restricted state, see your IBM documentation.
- Schedule this job after regular work hours to reduce the impact on iSeries users.

☑	Steps
☐	**1.** Log on using a user profile with at least *ALLOBJ and *SECADM authorities.
☐	**2.** *If you are using PSAudit - Data Auditing and Reporting (DAR) and you are journaling activity on a heavily active file*, stop DAR journaling. For more information about DAR, see the *User Guide for NetIQ Security Solutions for iSeries - PSAudit*.
☐	**3.** *If you are using the PSAudit - System Auditing and Reporting (SAR) SQL/Query Auditing feature*, stop the SQL/QRY Monitor.
☐	**4.** *If you are using PSSecure - Remote Request Management (RRM)*, use the Work With Exit Points screen to ensure NetIQ exit programs have been removed from all supported exit points. For more information on RRM exit points, see the *User Guide for NetIQ Security Solutions for iSeries - Remote Request Management*.
☐	**5.** *If you are using the PSSecure - Profile and Password Management (PPM) synchronization feature*, ensure other servers are not synchronizing with the server from which you are uninstalling the software.

☐	**6.** Issue the following commands to ensure there are no locks on product libraries.
	`WRKOBJLCK OBJ(PSAUDIT) OBJTYPE(*LIB)`
	`WRKOBJLCK OBJ(PSCOMMON) OBJTYPE(*LIB)`
	`WRKOBJLCK OBJ(PSDETECT) OBJTYPE(*LIB)`
	`WRKOBJLCK OBJ(PSSECURE) OBJTYPE(*LIB)`

☐	**7.** Ensure NetIQ Security Solutions for iSeries libraries are not included in your library list.

☑	Steps
☐	**8.** *If you are using Help/Systems' Robot Job Scheduler and are not uninstalling in restricted state*, ensure you delete NetIQ Security Solutions for iSeries tasks and jobs. If you do not delete jobs scheduled by Help/Systems' Robot Job Scheduler, job processes can potentially lock NetIQ Security Solutions for iSeries objects and cause the uninstall to fail and end abnormally
☐	**9.** *If you are using IBM Advanced Job Scheduler and are not uninstalling in restricted state*, ensure you delete NetIQ Security Solutions for iSeries jobs and jobs containing the following commands: STRAAAPI, ALOG, ALOGPRT, ASO, BLCRTCLT, DBA, DBALOG, DDRPT, DDRPTA, DSPFLD, PSINSTALL, PSMENU, PSUNINST, STRAA, STRBL, STRDD, STRMS, STROAM, STRRRM, STRSFE, ZPASS. If you do not delete jobs scheduled by IBM Advanced Job Scheduler, job processes can potentially lock NetIQ Security Solutions for iSeries objects and cause the uninstall to fail and end abnormally.
☐	**10.** To prevent processes from running while uninstalling the NetIQ Security Solutions for iSeries product, run the uninstall in restricted state. Processes can potentially lock NetIQ Security Solutions for iSeries objects and cause the uninstall to fail and end abnormally. For more information about running in restricted state, see your IBM documentation.
☐	**11.** Type the following command, and press **F4** (Prompt): `SBMJOB CMD(PSUNINST) JOB(PSUNINST) LOG(4 0 *SECLVL) LOGCLPGM(*YES)`
☐	**12.** Review the parameters and make changes as needed, then press Enter to submit the uninstall job for batch processing and create a job log.

☐	**13.** Since this uninstall process does not destroy existing data, your system might contain data from a previous installation. *If you want to remove all NetIQ data*, delete all libraries that match the following name patterns:
	`PS&TEMP*`
	`ZPS&TEMP*`
	where `&` is A, C, D, or S, and `*` is any letter combination.

☑	Steps
☐	**14.** To delete the installation program, on the command line, type the following command and press Enter. `DLTLICPGM 1PSI001`
☐	**15.** *If you used other exit programs for your remote server and user profile exit points before installing NetIQ Corporation software and you want to continue to use them*, manually reinstall these exit programs.
☐	**16.** *If PS* Authorization lists were not uninstalled*, on the command line, type `WRKAUTL PS*` and press Enter. Delete any linked objects that are no longer needed, and then delete the authorization list. If you are still unable to delete the authorization list, contact IBM or your operating system software maintenance provider to see if a RCLSTG is correct for your environment.