Trial Guide

NetIQ® Security Solutions for iSeries

September 4, 2008

Contents

About This Book and the Library

The trial guide describes the benefits and features of using the NetIQ Security Solutions for iSeries products (NetIQ Security Solutions for iSeries). This book includes a guided tour that lets you see how the product can help secure your iSeries enterprise.

Intended Audience

This book helps you become familiar with the benefits of using NetIQ Security Solutions for iSeries in your environment.

If you are responsible for researching, designing, and implementing a comprehensive security solution for iSeries servers, the trial guide can quickly guide you through the process of installing, understanding, and using NetIQ Security Solutions for iSeries.

Other Information in the Library

The library provides the following information resources:

Installation Guide

Guides you through the installation process for all the component products in NetIQ Security Solutions for iSeries. Includes information to help you integrate NetIQ Security Solutions for iSeries with other enterprise-scale security solutions from NetIQ Corporation.

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
Installation

To start evaluating NetIQ Security Solutions for iSeries, plan to install the products on an IBM iSeries server in a test environment, if possible. Ensure the test environment meets the requirements. After you install the products, take the time to do the simple product configuration before you begin the guided tour.

Two key factors determine whether you can install and evaluate the products using the procedures in this Trial Guide:

- You must be installing the NetIQ Security Solutions for iSeries products for the first time on an iSeries server. This trial installation does not support upgrading from a previous version of NetIQ Security Solutions for iSeries.
- Considerations for installing the products in a production environment may be different from the trail installation guidelines. Do not use these procedures to perform a production installation.

For more information about upgrading to the latest version of the product or for installing NetIQ Security Solutions for iSeries products in a production environment, see the Installation Guide.

Prepare for Trial

Install NetIQ Security Solutions for iSeries in a test environment, if possible. If you do not have a test environment, you can reduce the potential impact of installing and running the trial by installing the products when the fewest users require access (during an off shift).

Back up your server before you install the NetIQ Security Solutions for iSeries products.

Note

Some operations performed during the trial installation require you to cycle (stop and restart) some servers. For example:

- If you install and configure PSSecure Remote Request Management, you may have to cycle connected remote *DATABASE, *FILE, and *FTP servers.
- If you later decide to remove the products, you may have to cycle all servers on the local iSeries to completely remove all product components.

Preparation Checklist

Complete the following tasks to prepare for installation, install the products, and configure the products for the feature tour.

☑	Preparation Checklist
☐	**1.** Ensure the iSeries server you use for the trial meets all the requirements. For more information, see “Requirements” on page 17.
☐	**2.** Install the products. For more information, see “Installing NetIQ Security Solutions for iSeries” on page 18.
☐	**3.** Display the NetIQ Security Solutions for iSeries menu. For more information, see “Accessing the NetIQ Security Solutions for iSeries Products” on page 21.

☑	Preparation Checklist
☐	**4.** Determine who needs authorization to run and evaluate the products and authorize them. For more information, see “Authorize Other Users to Run NetIQ Security Solutions for iSeries” on page 22
☐	**5.** Complete the configuration tasks. For more information, see “Configuration Checklist and Tasks” on page 26.

Requirements

The following table identifies the software, hardware, and permissions required to install and evaluate the NetIQ Security Solutions for iSeries products. The iSeries server must not have any version of NetIQ Security Solutions for iSeries previously installed.

NetIQ Security Solutions for iSeries product performance depends on a number of factors. The products typically use less than 5% of available CPU capacity. During some operations, CPU usage can be higher.

Category	Minimum Requirements
Operating System	i5/OS V5R2
Disk Space	375 MB available for product libraries
Media	• Physical access to the CD-ROM drive in the server • CD-ROM drive device name OR • Downloaded installation save file, SVFPSI00
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

If you are not running a 5250 terminal emulator, such as Attachmate Reflection for IBM, on a Windows computer, you can still run the product tour. However, this Trial Guide provides instructions for using FTP from a Windows computer in "Exploring Remote Request Management Rules" on page 41. If you are familiar with using FTP, you can follow the tour from any computer with an accessible FTP client.

Licensing

The trial version of NetIQ Security Solutions for iSeries includes a built-in license key that remains active for 30 days from the day you install the products. Contact your sales representative to obtain permanent product licenses.

When you configure the product according to this Trial Guide, your configuration persists after you add the permanent license, even if the trial period has expired. For more information about permanent licensing, see the *Installation Guide*.

Installing NetIQ Security Solutions for iSeries

Ensure the server meets all installation requirements before you proceed. For more information, see "Requirements" on page 17. Choose an installation method and use one of the following procedures:

- "Installing the Products from CD-ROM" on page 18
- "Installing the Products from a Save File" on page 19

Installing the Products from CD-ROM

You can receive a free trial kit from your NetIQ sales representative that includes the installation CD. Use this procedure to install the products from the CD.

To install NetIQ Security Solutions for iSeries products from CD:

1. Sign on to the iSeries server with a user profile that includes the *ALLOBJ and *SECADM special authorities.
2. Insert the installation kit CD in the appropriate iSeries CD-ROM drive.
3. At the i5/OS command prompt, type the following command and press Enter:

   `RSTLICPGM LICPGM(1PSI001) DEV(`*`device_name`*`)`

   where *`device_name`* is the name of the CD-ROM device, such as OPT01. For example, `RSTLICPGM LICPGM(1PSI001) DEV(OPT01)`.
4. Type `psinstall` and press Enter.
5. Type the CD-ROM device name. For example, type `OPT01` and press Enter.
6. Press Enter to read the user license agreement (EULA).
7. Press F6 to accept the EULA and begin installing the products.
8. The installation process runs without further prompts. When complete, NetIQ Security Solutions for iSeries displays the following message: `Installation of the NetIQ Security Solutions for iSeries completed successfully`.

The installation process may take some time. For example, on an iSeries with a CPW of 700, the installation process takes approximately 20 minutes.

Installing the Products from a Save File

You can download a trial version of the product from the NetIQ Web site. Follow the instructions on the Web site to uncompress the package and FTP it to the iSeries server. Then use this procedure to install the products on your iSeries.

To install NetIQ Security Solutions for iSeries products from a save file:

1. Sign on to the iSeries server with a user profile that includes the *ALLOBJ and *SECADM special authorities.
2. At the i5/OS command prompt, type the following command and press Enter:

   ```
   RSTLICPGM LICPGM(1PSI001) DEV(*SAVF) SAVF(library/filename)
   ```

   where *library/filename* is the location of your transferred save file. For example, `RSTLICPGM LICPGM(1PSI001) DEV(*SAVF) SAVF(QGPL/SVFPSI00)`.
3. Type PSINSTALL and press Enter.
4. Type *SAVF and press Enter.
5. Press Enter to read the user license agreement (EULA).
6. Press F6 to accept the EULA and start installing the products.
7. The installation process runs without further prompts. When complete, NetIQ Security Solutions for iSeries displays the following message: Installation of the NetIQ Security Solutions for iSeries completed successfully.

The installation process may take some time. For example, on an iSeries with a CPW of 700, the installation process takes approximately 20 minutes.

Locating NetIQ Security Solutions for iSeries Documentation

The product autorun provides easy access to the NetIQ Security Solutions for iSeries library of documentation.

To start the autorun and locate the NetIQ Security Solutions for iSeries documentation:

1. Insert the installation kit CD in the CD-ROM drive of a Windows computer. The autorun should start automatically.

   Note
   If the autorun program does not start automatically, run SETUP.EXE in the root folder of the CD.

2. Click the **Documents** tab in the autorun.
3. Click any link to display the corresponding documentation.

Accessing the NetIQ Security Solutions for iSeries Products

NetIQ Security Solutions for iSeries include a secure menu that lets authorized users access the products.

To display the NetIQ Security Solutions for iSeries menu:

1. Sign on to the iSeries with a user profile authorized to use the products.
2. At the i5/OS command prompt, type psmenu and press Enter.

If you installed the products, the installation process authorized you to run NetIQ Security Solutions for iSeries. If you did not install the products, the person who installed it should grant you authority to run the products. For more information, see "Authorize Other Users to Run NetIQ Security Solutions for iSeries" on page 22.

Authorize Other Users to Run NetIQ Security Solutions for iSeries

You may need to grant another person authority to run NetIQ Security Solutions for iSeries. Read the following sections to better understand the product use authorization process and determine if you need to authorize any other users to run the products.

Understanding the Authority Administrator Role

During installation, NetIQ Security Solutions for iSeries automatically authorizes the user profile of the person installing the product as authority administrator. An authority administrator can run or configure the products and also control who else can use the products in what capacity.

In addition to the installer, the product grants the QSECOFR profile authority administrator authorities as a fail-safe measure. If the user profile of the installer is unavailable or disabled, sign on as QSECOFR to authorize other users. For best security, do not run NetIQ Security Solutions for iSeries when signed on as QSECOFR.

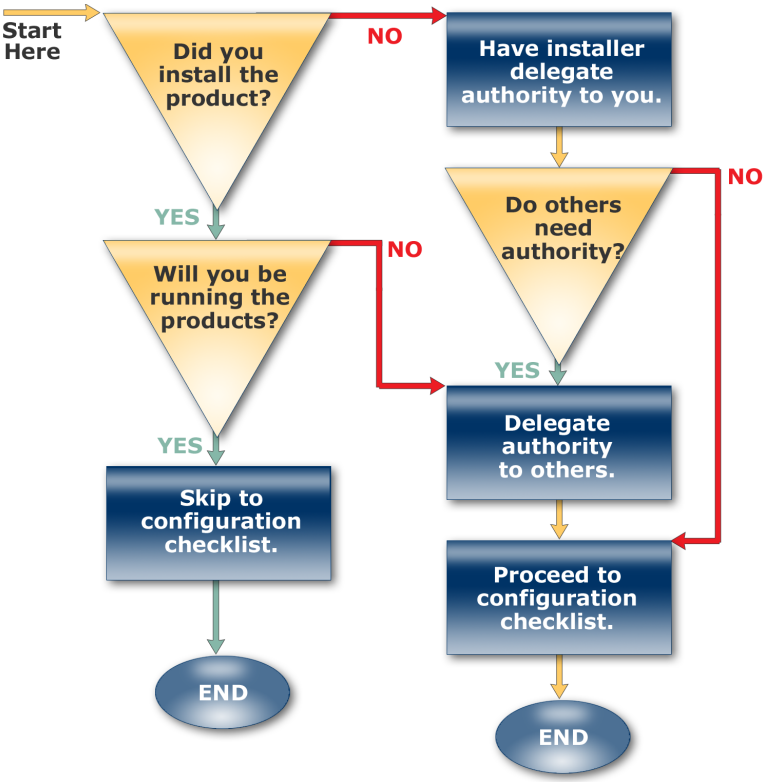
Determine if You Need to Delegate Authority

You may need to authorize other users to run the products. Use the following criteria, or the decision chart that follows, to determine your next step.

- ***If you installed the products, you are evaluating them***, and no one else will be running the products, you do not need to delegate authority to anyone else. In this case, skip the delegation task and go to the configuration checklist. For more information, see "Configuration Checklist and Tasks" on page 26.
- ***If you installed the products, you are evaluating them***, and others will also be running them, you need to delegate authority to those other users. If you installed the products, your user profile automatically has the authorities you need to delegate authority to others. For more information, see "Delegating Authority to Others" on page 24.
- ***If you installed the NetIQ Security Solutions for iSeries products but someone else is evaluating them***, you must explicitly grant authority to the person who will be evaluating the products. In this case, after you install the products, delegate authority to the evaluator to use the products. For more information, see "Delegating Authority to Others" on page 24.

After you delegate authority, instruct the evaluator to configure the products. For more information, the evaluator should see "Configuration Checklist and Tasks" on page 26.

If you are still unsure whether you need to delegate authority to other users, the following decision chart can help you decide how to proceed:



Delegating Authority to Others

If you need to delegate authority to someone else to run the products, complete the following task. Only the person who installed NetIQ Security Solutions for iSeries (or the QSECOFR profile as a fail-safe measure) can initially delegate product authority.

To grant or revoke authority to use the iSeries products:

1. Sign on as the user who installed the products.
2. At the i5/OS command prompt, type `psmenu` and then, press Enter.
3. Type `70` (Utilities Menu) and press Enter.
4. Type `1` (Authorize users to products) and press Enter.
5. Specify the appropriate information for the following items. Press Tab to move to the next field.
   a. **User**: Specify the user profile to authorize. For example, type `VALUSER`.
   b. **Product**: Type `*ALL` to authorize all products.
   c. **Authority**: Type `*GRANT` to authorize access to the specified products.
   d. **Authority administrator:** Type `*YES` to authorize the user as an authority administrator.
6. Check your entries and press Enter.
7. ***If you want to authorize additional users***, repeat Steps 4 through 6.
8. Press F3 to return to the NetIQ Product Access Menu.

Configuration Checklist and Tasks

To gain the most benefit from the guided tours of the NetIQ Security Solutions for iSeries products, configure the products by completing the following tasks:

☑	Configuration Tasks for NetIQ Security Solutions for iSeries Product Tours
☐	**1.** Configure PSSecure Remote Request Management (RRM) by running the RRM Configuration Wizard. RRM lets you control access from remote locations to your iSeries server. For more information, see “Configuring Remote Request Management” on page 27.
☐	**2.** Set RRM to run in secured mode for FTP transactions. For more information, see “Securing FTP Access to Your Server” on page 29.
☐	**3.** Copy the sample data files to your local iSeries server. For more information, see “Copying Sample Data Files” on page 31.
☐	**4.** Configure PSAudit. PSAudit helps security professionals meet system and data auditing and reporting requirements. For more information, see “Configuring Auditing” on page 31.
☐	**5.** Configure PSDetect to monitor the security journal for activities you specify. For more information, see“Running the PSDetect QuickStart Wizard” on page 33.
☐	**6.** Configure the sender's email address for notifications. For more information, see “Configuring Who Sends Notifications” on page 36.
☐	**7.** Create a user profile with a weak password to demonstrate PSPasswordManager. For more information, see“Creating a User Profile” on page 37.

Configuring Remote Request Management

A key component of the PSSecure product, Remote Request Manager (RRM), helps you control access to your iSeries server. A remote request is any transaction that originates from a computer not directly attached to the server but using an i5/OS remote server, such as FTP, TELNET, SQL, or ODBC. RRM determines if incoming transactions are authorized to execute on your server by evaluating them against your security rules, called RRM secured entries.

RRM exit programs enforce security by exiting from transaction requests to verify authority before carrying out the request. RRM exit programs evaluate remote requests and permit or reject requests based on the rules defined in your secured entries.

The RRM Configuration Wizard helps you install and configure the RRM exit programs that permit or reject remote access requests. Run the RRM Configuration Wizard before you begin the guided tour of the product.

Note

- To implement RRM, you must cycle remote servers during the following task.
- Cycling remote servers terminates remote connections to the server, except TELNET connections. Plan to cycle the remote servers when no remote connections are active or during an off shift, if possible.
- Cycling remote servers can take 1 to 5 minutes in most cases.

To complete the RRM configuration wizard:

1. Sign on as a user authorized to configure the products.
2. At the i5/OS command prompt, type `psmenu` and press Enter.
3. Type `2` (PSSecure) and press Enter.
4. Type `3` (Remote Request Management) and press Enter.
5. Type `30` (Manage RRM) and press Enter.
6. Type `30` (RRM Configuration Wizard) and press Enter.
7. Press Enter to continue running the configuration wizard.

8. For steps 1 through 7 in the RRM Configuration Wizard, press Enter to select the default values.

9. For step 8 on the RRM Configuration Wizard, Alert Profile, type your user profile name. For example, type EVALUSER, and press Enter.

10. For steps 10 through 13 of the RRM Configuration Wizard, press Enter to select the default settings.

11. For step 14 of the RRM Configuration Wizard, Simulate Secured Mode, type *NO and press Enter.

12. The wizard displays a summary of your settings. Your settings must match those shown in the following table or be set appropriately for your environment.

Wizard Step	Your Selection
1. Install Exit Programs?	*YES
2. Start Collection?	*YES
3. Retain data for RRM reports?	*YES
4. Retain What If Playback information?	*YES
5. Audit RRM changes?	*YES
6. Send Rejection Alerts?	*YES
7. Specify Profile or Message Queue?	*USER
8. Alert Profile:	EVALUSER
10. Allow Anonymous FTP?	*NO
12. Update last used date/time for FTP profiles?	*YES
13. Allow TELNET auto signon?	*NO
14. Simulate Secured Mode?	*NO

13. Review your settings. When they are correct for your environment, press Enter.

14. Press Enter to apply the settings.
15. Press Enter to exit the wizard and return to the Manage RRM menu.
16. On the Manage RRM menu, type 3 (Cycle Remote Servers) and press Enter.
17. In the Application server field, press the plus key (+) and then press Enter to display additional entry fields.
18. Type `*DATABASE` and press Tab.
19. Type `*FTP` and press Tab.
20. Type `*FILE` and press Enter.

Note
If you have previously installed other exit programs you may have to specify *ALL to cycle all remote servers.

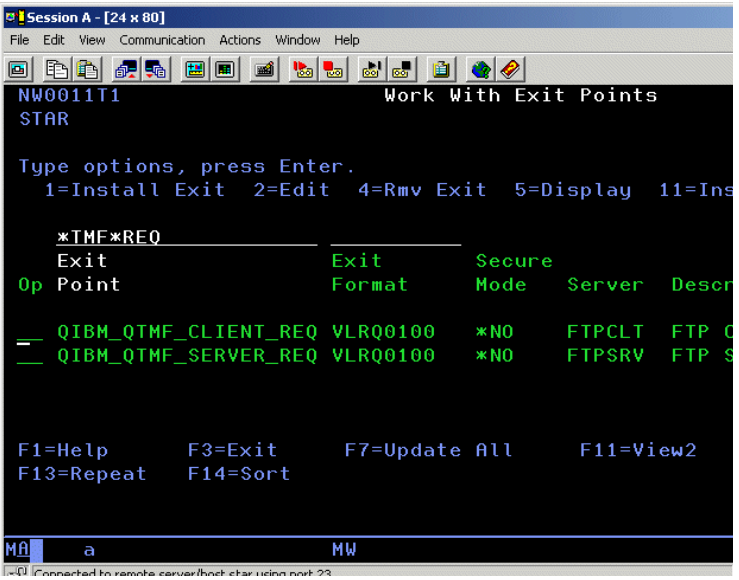
21. Tab to Allow ending subsystems and type QSERVER.
22. Press Enter. NetIQ Security Solutions for iSeries starts cycling the remote servers you specified.
23. When the process is complete, press F12 to return to the Remote Request Management menu.

Securing FTP Access to Your Server

NetIQ Security Solutions for iSeries let you test security rules before you implement them by running in simulated secured mode. After you have tested the rules, you can enforce them by switching to secured mode. For this demonstration, you will enforce the FTP access rules by switching to secured mode for FTP transactions to the server. After the demonstration, you can reset FTP transactions to simulated secured mode if you choose.

To enforce security rules for FTP transactions to the server:

1. From the Remote Request Management menu, type 8 (Work With Exit Points) and press Enter.
2. Press SHIFT+Tab twice to tab back to the Exit Point string search field.
3. Type *TMF*REQ and press Enter. The display should list two FTP exit points.



4. Tab to the QIBM_QTMF_SERVER_REQ exit point.
5. Type 2 and press Enter.
6. Tab to Secured and type *YES for the QIBM_QTMF_SERVER_REQ exit point.
7. Press Enter to review your changes.
8. Press Enter to save your changes.
9. Press F3 to return to the Remote Request Management menu.
10. Press F3 to return to the NetIQ Product Access Menu.

Copying Sample Data Files

The installation kit provides some sample data files to use during the guided tours. The next procedure helps you copy the following files to your server:

- PSEVAL/COMP - sample compensation information
- PSEVAL/CONTACT - sample contact information
- PSEVAL/EXPENSES - sample expense information

To copy the sample data files:

1. At the NetIQ Product Access Menu, type 70 (Utilities) and press Enter.
2. Type 20 (Install trial data) and press Enter. PSSecure copies the sample data files to the PSEVAL library.
3. Press F3 to return to the NetIQ Product Access Menu.

Configuring Auditing

PSAudit reports on security actions, activity, settings, and changes to your iSeries server. PSAudit can also compare collections of system information from different dates to provide baseline auditing. PSAudit includes several reporting capabilities using the following components:

System Auditing and Reporting (SAR)
: Provides reports to help assess the security of your server. Helps managers, auditors, and security administrators who need to quickly and regularly monitor objects, files, libraries, and security settings.

Data Auditing and Reporting (DAR)
: Reports changes to sensitive data that you specify. Can report before and after values for specified files and fields. Use DAR to determine who made changes to sensitive data fields.

System Access Analysis (SAA)
: Reports details of user access activity on your server.

Baseline Analysis

Compares current system, user, and Document Library Objects (DLO) to a saved snapshot (baseline) of these objects and reports the differences.

To prepare for the guided tour of these auditing and reporting features, configure Data Auditing and Reporting (DAR) by selecting files and fields to audit and turn on system value auditing.

To configure DAR:

1. At the NetIQ Product Access Menu, type 1 (PSAudit) and press Enter.
2. Type 3 (Data Auditing and Reporting) and press Enter.
3. Press F6 (Add) and press Enter.
4. Type COMP in the filename field and press Tab.
5. Type PSEVAL in the library name field and press Enter.
6. Type 1 (Journal ON/OFF) in the Opt field next to COMP and press Enter.
7. Press F5 to refresh the display.
8. Type 6 (Work with fields) in the Opt field next to COMP and press Enter.
9. Type C in the Opt field next to each field you want to audit. Press Tab to move to the next field. For example, type C in the Opt field for BASESALARY, BONUS, and OPTIONS. Using option C specifies to store both the original and changed values for changed data fields.
10. When you have identified all the fields you want to audit, press Enter.
11. Press F3 to exit.
12. If you want to specify additional files to audit, repeat Steps 3 through 11 to add files and specify which fields to audit. For example, you may want to specify to monitor fields in another sample file, such as PSEVAL/CONTACT or PSEVAL/EXPENSES.
13. Press F12 to return to the PSAudit Main Menu.
14. Type 1 (System Auditing and Reporting) and press Enter.

15. Type 7 (System Setup and Defaults Menu) and press Enter.

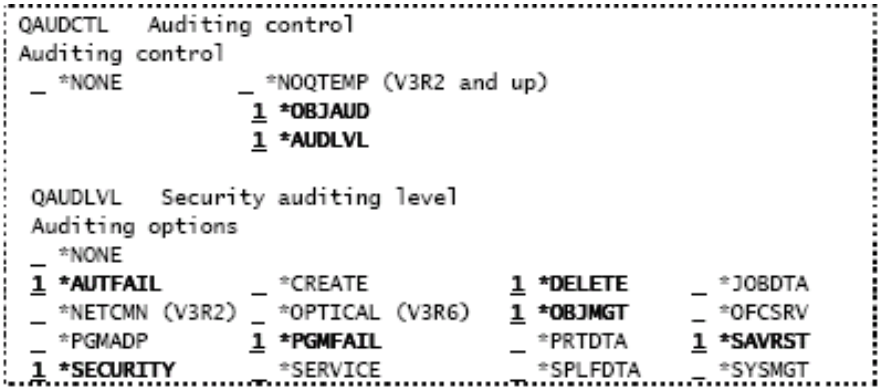
16. Type 4 (Work With Security Journaling) and press Enter.

17. Make a note of the values currently enabled for auditing so you can reset the journal values after you complete the product trial.

Note

To reset Security Journaling to your previous values after the trial, use the CHGSYSVAL command for QAUDCTL and QAUDLVL or repeat this procedure starting at Step 13 from the PSAudit Main Menu.

18. Press F10 (Set recommended values) to enable auditing for the values shown in bold in the following figure.



19.Press F3 twice to return to the NetIQ Product Access Menu.

Running the PSDetect QuickStart Wizard

PSDetect can monitor iSeries servers for a number of events that may indicate possible security issues. For example, the product can monitor sign-on by QSECOFR, changes to the system journaling system value (QAUDCTL), and invalid sign on attempts.

PSDetect identifies important system events, stores the events in the alert log, responds by running a command or sending SNMP traps, and can notify a security team member to take appropriate action. PSDetect can also forward alerts or SNMP traps to other NetIQ products, such as Security Manager and AppManager. You must specify which events to alert on, how to notify you, and whether to forward alerts to other products. To make this configuration easy, run the PSDetect QuickStart wizard.

Before you run the QuickStart wizard, collect the following information about your email server:

- IP address for the email server or router (such as 10.2.11.100)
- Name of the corporate email server or router (such as EXCH_SVR1)

You also need the email address of a user who will receive the alerts. For the trial, you can use your own email address.

To configure PSDetect using the QuickStart Wizard:

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

Wizard Step	Your Selection
1. Configure email support	*YES
2. Configure SMTP?	***If you need to configure SMTP on your iSeries server***, press Enter to accept the default value of *YES. ***If you already have SMTP configured on your iSeries server,*** type *NO and press Enter. The wizard skips Steps 3 and 4.

Wizard Step	Your Selection
3. Mail server IP address	IP address of the mail server. For example, type 10.2.11.100
4. Mail server name	Name of the mail server. For example, type EXCH_SVR1
5. Short name for email user	Type your first name
6. email address	Type your full email address, such as EVALUSER@MyCompany.com
7. Configure paging support?	*NO
13. Configure Security Manager Support?	*NO
15. Configure SNMP Support?	*NO
17. Monitor for storage conditions?	*YES
18. Action for storage condition:	*EMAIL
19. Who should this action notify?	Defaults to your Short name for email
20. Monitor changes to QAUDCTL?	*YES
21. Action for QAUDCTL changes:	*EMAIL
22. Who should this action notify?	Defaults to your Short name for email
23. Monitor QSECOFR activity?	*YES
24. Action for QSECOFR activity:	*EMAIL
25. Who should this action notify?	Defaults to your Short name for email
26. Monitor invalid signon attempts?	*YES
27. Action for invalid signon attempts:	*EMAIL
28. Who should this action notify?	Defaults to your Short name for email

Wizard Step	Your Selection
29. Monitor for rejected remote requests?	*YES ***If you receive a warning message when you select this option**, press Enter to continue.
30. Action for rejected remote requests:	*EMAIL
31. Who should this action notify?	Defaults to your Short name for email
32. 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 press Enter until you return to the summary.
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.

Configuring Who Sends Notifications

PSDetect sends email notifications to the email recipients you specified in the PSDetect QuickStart wizard. If you want to change the sender (reply-to address) of the email notifications, use the following procedure to supply a valid email address.

To identify the sender for PSDetect email notifications:

1. At the PSDetect Main Menu, type 4 (Work with Monitors) and press Enter.
2. Tab to Email Monitor.
3. Type 20 (System Defaults) and press Enter.

4. Type the email address you want to specify as sender. For example, type ActionAlert@MyCompany.com.
5. Review your entry and when correct, press Enter.
6. Press F3 twice to return to the NetIQ Product Access Menu.

Creating a User Profile

To tour PSPasswordManager, create a user profile with a weak password.

To create a user profile with a weak password:

1. Ensure you are signed on as a user with *SECADM authority.
2. At the NetIQ Product Access Menu, press F10 to display an i5/OS command prompt.
3. Type `CRTUSRPRF` and press Enter.
4. In the User profile field type `NETIQ` and press Tab.
5. In the User password field type `SPRMN` (superman with vowels removed).
6. Tab to Limit capabilities and type `*YES`.
7. Press Enter to create the limited capability NETIQ user profile.
8. Press F12 to return to the NetIQ Product Access Menu.

Chapter 3
Tour of NetIQ Security Solutions for iSeries

Now that you have the NetIQ Security Solutions for iSeries products installed and configured, you can begin the guided tour. The first tour demonstrates the Remote Request Manager (RRM) product to understand the following capabilities:

- Controlling access to data on your server by creating a secured entry rule
- Copying the rule and generalizing it to control access to additional files
- Viewing a RRM report

The next tours help you explore System Auditing and Reporting (SAR) and Data Auditing and Reporting (DAR). These tours show you how NetIQ Security Solutions for iSeries tracks and controls changes to your system settings (SAR) and sensitive data files (DAR).

NetIQ Security Solutions for iSeries help track security issues in real time by alerting you to suspicious activity. In the next guided tour, you change the auditing journal setting. PSDetect logs the change in the alert console and sends you an email.

The final tour lets you change the default PSPasswordManager password dictionary and enforces your new password strength policy.

These tours highlight several important capabilities of the products, but represent only a sampling of the security features the products offer. Take a few moments during the tours to explore other product features and to better understand the scope of security issues NetIQ Security Solutions for iSeries help you address.

Explore Remote Access Control Using RRM

Setting up Remote Request Management (RRM) to manage security for remote access requests is simple and fast using the RRM configuration wizard. Be sure you have completed the configuration steps before continuing this tour. For more information, see “Configuring Remote Request Management” on page 27.

RRM uses i5/OS remote server exit points to compare requests with rules, called Secured Entries, that allow or deny access to an iSeries server. If someone attempts to access data on your iSeries server across FTP, TELNET, SQL, ODBC, or other remote servers, RRM determines if the requesting user, network address, time, and access method are authorized and then grants or denies access.

In the tour, you will use FTP to copy (get) a file from the iSeries and let RRM log the transaction. Then, you edit the logged transaction to create a Secured Entry. When you attempt to get the file again, RRM denies your request. Next, you will copy the Secured Entry and modify it slightly to deny access to multiple files using an RRM operation group. When you attempt to get another file, RRM now also blocks that request.

The tour includes instructions for using a Windows computer and the FTP get command. If you cannot FTP to your iSeries from a Windows computer, you can FTP from any computer with an accessible FTP client if you are familiar with the commands to use.

Although not demonstrated in the tour, RRM also lets you operate in a "What If" mode that lets you examine your RRM rules (Secured Entries) before you enforce them in your production environment. In "What If" mode, you can make changes to your rules and configuration settings. Then, use the RRM reports to determine whether the behavior of actual transactions would change. For example, you could look for transactions that previously were accepted (*PASS) and now are rejected (*FAIL). Throughout the process, RRM maintains and enforces the existing rules.

Exploring Remote Request Management Rules

During configuration, you ran the RRM Configuration Wizard. You specified that RRM start collecting all user transactions. You also set FTP transactions to run in secured mode. In the following tour, you will collect a transaction and use it as a starting point for defining a Secured Entry that limits remote access.

First, you run an FTP GET command to your iSeries server from a Windows computer. RRM collects the transaction information. Next, use the collected entry to create a Secured Entry that instructs RRM to fail future transactions like this. When you repeat the FTP get command, RRM denies access to the file.

To explore using RRM to deny a remote FTP request:

1. At a Windows computer, open a Windows command line window.
2. Type `ftp` *`servername`* where *`servername`* is the name of your iSeries server. You can also use the ftp IP address form of the FTP command to connect with your iSeries server.
3. Sign on to your iSeries server at the FTP prompt.
4. Type `get pseval/comp` to download the sample file from the iSeries server. RRM records the transaction request as a collected entry.
5. In the iSeries emulator window at the NetIQ Product Access Menu, type `2` (PSSecure) and press Enter.

Note

To display the NetIQ Product Access Menu, type `psmenu` at the i5/OS command prompt and press Enter.

---

6. Type `3` (Remote Request Management) and press Enter.
7. Type `2` (Work with Collected Entries) and press Enter.
8. ***If the FTPSRV_SEND command that corresponds to your FTP GET transaction is not the first entry in the list***, tab to the **Op** column next to the FTPSRV_SEND command.

9. Type `3` (Create Secured) and press Enter. RRM copies this FTP transaction information so you can edit it to create a secured entry rule.

10. Tab to **Network** and type `*ALL` and clear the rest of the IP address. Specifying *ALL applies this rule to transactions from any IP address.

11. Tab to **Action** and type `*FAIL`. Specifying *FAIL causes RRM to reject transactions that match this rule.

12. Tab to the **Op** field next to /QSYS.LIB/PSEVAL.LIB/COMP.FILE and type `1`. This command selects the PSEVAL/COMP file as the object of the transaction in this rule, protecting this file.

13. ***If you receive the User currently undefined message***, press Enter to add the user to RRM and then, press Enter to continue.

14. Press Enter to review the changes.

15. Press Enter to create the Secured Entry.

16. Press F3 to return to the Remote Request Management main menu.

17. Type `1` (Work with Secured Entries) and press Enter to view the Secured Entry you created. The following entry is an example of a similar Secured Entry:

```
Op S User Network Operation Action Swp Prf
__ Y EVALUSER *ALL FTPSRV_SEND *FAIL >
```

    The greater than symbol (>) at the right indicates the Secured Entry applies to a particular object, in this case, PSEVAL/COMP.

18. ***If you want to view the object associated with this entry***, type `5` (Display) and press Enter. Press F12 to return to the secured entries list.

19. At the Windows FTP command line, type `get pseval/comp`. RRM now denies the FTP request with an error similar to the following message:

```
ftp> get pseval/comp
200 PORT subcommand request successful.
550 Request rejected.
```

The PSDetect QuickStart wizard configured PSDetect to email a notification when RRM rejects remote requests. A few moments after RRM rejected your second attempt to get the file, PSDetect sent an email notification to the address you specified when you ran the wizard.

In this tour, you observed RRM controlling access to a file by a specified user. Using this specific transaction, you can quickly generalize it to create a rule that RRM can apply to remote requests to other files. In the next tour, you will generalize this specific Secured Entry to control access by several access methods to a number of files.

Generalizing an RRM Rule

Creating secured entries to control remote access using RRM is simple. First, collect transactions then use the collected transactions to create the Secured Entry. In the previous tour, you used a transaction to create a specific Secured Entry that identified one user and one file. In the next tour, you will use the same transaction but broaden it using an RRM group.

RRM groups are sets of users, operations (commands), or IP addresses that you identify as a group. You can then use the groups in the Secured Entries you create, simplifying the rules and minimizing the number of rules you need to manage security.

For example, suppose you want to allow the engineering department to access the PLANS library, but deny the accounting department access to this library. You can create engineering and accounting groups and then permit or deny those groups access to the library. Using RRM user, network, and operation groups reduces the number of Secured Entry rules you need to create.

RRM group names always begin with a colon (:). In the following tour, you will use an operation group, the :READONLY group of commands, to instruct RRM to block all forms of change access to selected files, including downloading the file. After you generalize the rule, RRM rejects your request to FTP the file.

To generalize a secured entry rule using RRM groups:

1. In the 5250 terminal or emulator window, press F3 to return to the Remote Request Management main menu.
2. Type `1` (Work with Secured Entries) and press Enter.

3. Tab to the FTPSRV_SEND Secured Entry.
4. Type `3` (Copy) and press Enter.
5. Tab to **Operation** and press F4 (Prompt).
6. Tab to the :READONLY operation group.
7. Type `1` (Select) and press Enter
8. Press F20 (Edit Obj).
9. Change /COMP.FILE to /C*.* and press Enter. Changing the secured entry to /C*.* generalizes the rule to include all files beginning with the letter C.
10. Press Enter to review your changes.
11. Press Enter to save your changes.
12. Press F3 to return to the Remote Request Management menu.
13. At Windows FTP command line, type `get pseval/comp`. RRM now denies the request and PSDetect notifies you by email.
14. Type `get pseval/contact` and press Enter. RRM now also denies this request and PSDetect notifies you by email.
15. Type `get pseval/expenses` and press Enter. RRM accepts this request and allows FTP to transfer the file since the rule applies only to files that start with the letter C.

Exploring RRM Operation Groups

In the following tour, you can delve further into RRM groups, in this case, the :READONLY operation group. The operation groups built in to RRM include sets of commands that have a similar effect, such as changing files or signing on to the server. These convenient operation groups make it easy to protect applications and data from every sort of access, including FTP and database queries.

To view the commands in the :READONLY operation group:

1. From the Remote Request Management menu, type `3` (Work with RRM Groups) and press Enter.
2. Type `3` (Work With Operation Groups) and press Enter.
3. Tab to the :READONLY operation group.
4. Type `5` (Work w/ members) and press Enter.
5. Press Page Down to scroll through the commands in the built-in :READONLY operation group. When a transaction is secured for :READONLY access, if a user issues any of the commands in this group to access the file, RRM denies the request.
6. Press F3 to return to the list of RRM operation groups.
7. Take a few moments to explore the operations included in some of the other operation groups by tabbing to the operation group and using option 5 (Work w/ members).
8. When you have finished exploring operation groups, press F12 to return to the Remote Request Management menu.

You can use RRM groups to simplify and streamline the number of rules you need to create and maintain. You can create user groups, IP address groups called network groups, or operation groups as needed to customize and simplify RRM rules.

Exploring RRM Reports

RRM makes a number of reports available. From the reports, you can easily evaluate how well RRM is working to secure your remote access.

To explore two RRM reports:

1. From the Remote Request Management menu, type `20` (Work with RRM Reports) and press Enter.
2. Type `1` (Transaction Reports) and press Enter.
3. Type `15` (Network Transactions by User) and press Enter.

4. Press Enter to accept the defaults and generate the report.
5. Press F12 to return to the Work With RRM Reports menu.
6. Type **3** (Summary/Statistic Reports) and press Enter.
7. Type **1** (Transaction Summary by Server) and press Enter.
8. Press Enter to accept the default report settings.
9. Press F18 to display the list of spooled files.
10. Tab to the spooled file identified as TransUser in the User Data column.
11. Type **5** in the Opt column.
12. Tab to the spooled file identified as TranSum in the User Data column.
13. Type **5** and press Enter to display the report. The following figure shows a portion of a Network Transactions by User report. Your report must include FTPSRV transactions. RRM passed some transactions but failed others, as the P or F in the first column of the following figure indicates.

```
RRM DMA Entry Job Id                    Incoming   Incoming
P/F P/F Type_ ... User_______ Address______  Server   Function
P   P   DB  ...  EVALUSER    10.21.18.111    SIGNON  INFO
P   P   DM  ...  EVALUSER    10.21.18.223    FTPSRV  LOGON
F   F   DM  ...  EVALUSER    10.21.18.223    FTPSRV  SEND
                          /QSYS.LIB/PSEVAL.LIB/COMP.FILE
P   P   DM  ...  EVALUSER    10.21.18.223    FTPSRV  SEND
```

14. Press F3 to redisplay the spool file list.

15. Press Enter to display the Transaction Summary Report by Server. The highlighted entry in the following report shows total, rejected, and accepted FTP transactions. The Transaction Summary by Server report provides a high-level overview of the remote transaction activity on your iSeries.

Server	Total Transactions	Rejected Transactions	__%__	Accepted Transactions	__%__
Subtotal	327	3	.91	324	99.09
DBINIT	24	0	.00	24	100.00
DBSQL	182	0	.00	182	100.00
FTPCLT	1	0	.00	1	100.00
FTPSRV	13	3	23.07	10	76.93
RMTCMD	46	0	.00	46	100.00
SIGNON	58	0	.00	58	100.00
TELNET	3	0	.00	3	100.00
Subtotal	0	0	.00	0	.00
Grand Total	327	3	.91	324	99.09

16. Press F3 until you return to the NetIQ Product Access Menu.

Explore System and Data Auditing

Before you can secure your iSeries server, you need to assess its current status. PSAudit makes it easy to assess the vulnerability of your iSeries server. PSAudit helps you assess changes to system values, user profiles, and objects on your iSeries server. You can check significant events, such as invalid sign on attempts or sign on by QSECOFR.

Ensure you configured PSAudit before you run the following guided tours. For more information, see "Configuring Auditing" on page 31.

Exploring System Auditing and Reporting (SAR)

System values on the iSeries server control how you implement the built-in security measures i5/OS offers. System Auditing and Reporting (SAR) lets you report on system values, user profiles, and other objects on your server.

In the following tour, you will make some changes to selected system values and then run the Changes to System Values report.

To report changes to system values using SAR:

1. At the NetIQ Product Access Menu, press F10 to display the i5/OS command prompt.
2. Type the following command and press Enter:

   ```
   DSPSYSVAL SYSVAL(QPWDMINLEN)
   ```

3. The iSeries displays the minimum password length, similar to the following figure. Make a note of the current setting so you can later restore it.

   System value . . . . . : QPWDMINLEN

   Description . . . . . : Minimum password length

   Minimum password length: 3 1-128

4. Press Enter to continue.
5. Type the following command to change the password minimum length to 1 and press Enter:

   ```
   CHGSYSVAL SYSVAL(QPWDMINLEN) VALUE(1)
   ```

6. Press F12 to return to the NetIQ Product Access Menu.
7. Type `1` (PSAudit) and press Enter.
8. Type `1` (System Auditing and Reporting) and press Enter.
9. Type `5` (Security Reports Menu) and press Enter.
10. Type `1` (General Security Reports Menu) and press Enter.

11. Type `6` (Changes To System Values) and press Enter.
12. Type `*CURR` for From date and press Tab.
13. Type `*CURR` for To date.
14. Tab to **Run interactively** and type `*YES`.
15. Press Enter to run the report. The following excerpt from the Changes To System Values report shows the original value of the system value for QPWDMINLEN was 3 and that EVALUSER changed the value to 1.

    System User

    Value Date Time Profile

    ~~~~~~~~ ~~~~~~ ~~~~ ~~~~~~~~

    Old Value

    New Value

    ~~~~~~~~~~~~~~~~

    QPWDMINLEN 03/10/08 13:20:23 EVALUSER

    0000000003 (Old value)

    0000000001 (New value)
16. Press F3 to exit from the report.
17. Press Enter to save the report and return to the General Security Reports Menu.
18. Press F12 twice to return to Security Auditing and Reporting.

Explore Other SAR Reports

You can explore additional reports in the following tour. Information in each table helps you navigate to the reports from the System Auditing and Reporting menu. Use the steps from the preceding tour to help you display and review each report that interests you. Use the shortcut key, F18, to access spooled report files within SAR.

Profiles w/Limit Capabilities = *NO

When a user has no capability limits, the user has i5/OS command prompt authority. If you limit user capabilities, they cannot execute commands even if they have a i5/OS command prompt available. You can limit user capabilities by changing their user profiles.

Option	Category or Report Selected
8	User Profile Reports
6	Profiles w/Limit Capabilities = *NO

Profiles w/ *SECADM,*SECOFR, or *ALLOBJ

The powerful profiles report lists users with special authorities. For example, users with *ALLOBJ special authority can read, change, or delete any application or data on a server. Secure your server by minimizing the number of user profiles with these special authorities. Limit users capabilities by changing their user profiles. Find out who to limit using this report.

Option	Category or Report Selected
8	User Profile Reports
7	Profiles w/*SECADM,*SECOFR,*ALLOBJ

Security Checkup Report

The Security Checkup Report provides a scored historical security analysis and serves as a pointer to other, more detailed, reports. This report may take some time to run depending on the number of objects on your server.

Option	Category or Report Selected
9	Summary Reports Menu
5	Security Check-up

Exploring Data Auditing and Reporting (DAR)

Data Auditing and Reporting (DAR) monitors files you specify for changes to specific fields in a file. In the following tour, start by changing a file and then view the DAR change report. DAR reports who made changes to data fields in the specified files and can optionally report before and after data values.

During configuration, you specified to audit the file PSEVAL/COMP. You also selected fields in the file to monitor. To track changes to other files, repeat the configuration steps. For more information, see "Configuring Auditing" on page 31.

To make a change to a monitored file and view the DAR report:

1. At the i5/OS command prompt, type the following command and press Enter:

   ```
   upddta pseval/comp
   ```

2. Press Page Down to view a record in the file.
3. Tab to the BASESALARY, BONUS, or OPTIONS data field and change a data value. For example, change BASESALARY from 35000000 (350,000.00) to 3500000 (35,000.00).
4. Press Tab to move to the next data field.
5. Press F11 (Change).
6. Press F3 (Exit).
7. Press Enter to save the changes.
8. At the i5/OS command prompt, type psmenu and press Enter.
9. Type `1` (PSAudit) and press Enter.
10. Type `3` (Data Access and Reporting) and press Enter.
11. In the Opt field, type 5 (View Data) and press Enter.
12. Press Enter. DAR runs the report query. When complete, the report displays two lines for each file you changed: the first line reports original data and the second line shows the changes. The report includes the user who made the changes and the date and time.

13. If you receive the message, Data too short for specified format, you can ignore it. This message may be displayed when you do not specify start and end dates and times for the report.

14. Press F3 until you return to the NetIQ Product Access Menu.

Exploring Event Management

In a production environment, with many transactions occurring, it is challenging to track security events using only the audit reports. It may also be difficult to differentiate important events from routine occurrences.

PSDetect can automatically notify you when important security events occur. For example, if someone changes the QAUDCTL system value to disable auditing, there may be a valid reason, but more likely it indicates potential malicious activity. PSDetect can email or page you when the auditing status changes so you can investigate this change quickly.

PSDetect lets you identify who to alert and the alert method to use when specified activities take place. When you configured PSDetect using the QuickStart wizard, you set up email notification when changes to the auditing level occur.

In the following tour, you will use PSAudit to turn auditing off and then on again. Then, you will review the alerts in the PSDetect Alert Console. If you configured SMTP email properly when you ran the PSDetect QuickStart wizard, you will also receive email notification of these changes.

To cause PSDetect to create an alert and notify you by email:

1. From the NetIQ Product Access Menu, type 1 (PSAudit) and press Enter.

2. Type 1 (System Auditing and Reporting) and press Enter.

3. Type 7 (System Setup and Defaults Menu) and press Enter.

4. Type 3 (Stop Security Journaling) and press Enter.

5. Type 2 (Setup Security Journaling) and press Enter.

6. Press F3 to return to the NetIQ Product Access Menu.

7. Type 3 (PSDetect) and press Enter.

8. Type 1 (Work With Alert Log) and press Enter.

9. Press F5 to refresh the display until PSDetect displays the new alerts. PSDetect scans the QHST log every 60 seconds to detect new events. You can adjust this interval for your environment. PSDetect issues two alerts corresponding to the two changes you made to journaling (off, then on again). The alert messages may look similar to the following examples:

   System value QAUDCTL changed from *NONE to * AUDLVL *OBJAUD

   System value QAUDCTL changed from *AUDLVL *OBJAUD to *NONE

10. Type 5 (Display) in the Opt field next to one of the alerts and press Enter to view the Display Alert Detail report. The following figure shows an example:

    PSM070R PSDetect 9/29/08 9:57:14

    Display Alert Detail

    Date/time alert entered system . : 9/29/08 9:41:30

    Status . . . . . : CLOSED

    Alert queue . . . . . : QSYS/QHST

    Filter sequence no. processed . . : 0010

    Alert ID . . . . . : CPF1806

    Alert text . . . . . : System value QAUDCTL changed from *NONE to *AUDLVL *OBJAUD.

    Alert type . . . . . : INFO

    Alert severity . . . . . : 00

    Message file . . . . . : *LIBL/QCPFMSG

    System . . . . . : MyiSeriesServer

11. Press F12 to return to the Alert Log window.

12. Type `13` (Action History) in the Opt field next to one of the alerts and press Enter. Your Alert History report may be similar to the following example:

```
PSM070R          PSDetect          9/29/08 9:57:14

                 Alert History

Alert date/time . :   9/29/08 9:41:30

Alert text  . . . :  System value QAUDCTL changed from *NONE to *AUDLVL   *

 Date     Action   Value

 9/29/08 EMAIL    Message to EvalUser passed to Email monitor

 9/29/08 EMAIL    "System value QAUDCTL chang..." sent to email address
EvalUser

_____________________ Outstanding Actions _____________________

Action   Wait System    Action Parameters

  There are no outstanding actions

_____________________ Outstanding Pager Messages _____________

  Date     Time   To Pager   Attempts  Message

  There are no outstanding pager messages
```

13. Press F3 until you return to the NetIQ Product Access Menu.

Check your email for the alert notifications. One of the messages you receive should be similar to the following example.

Exploring Password Management

User passwords are your first line of defense in protecting access to your server. If users can sign on using another person's profile, they could gain access or authority they should not have. PSPasswordManager identifies users with weak or easily guessed passwords and lets you take action, such as emailing users a message to change their passwords, disabling the profile, or expiring their passwords.

In the tour, you will check for profiles with weak passwords and explore sorting the resulting list by various columns to identify the most vulnerable user profiles. Next, you will modify a word list to include additional weak passwords. Depending on how many additions your selections require, this step can take some time. Last, you will disable a sample user profile.

To assess password strength using PSPasswordManager:

1. From the NetIQ Product Access Menu, type `4` (PSPwdMgr) and press Enter.
2. Type your password and press Enter. Password manager requires this extra security step since working with passwords is a sensitive operation. Your user profile must have the *ALLOBJ and *SECADM special authorities to run PSPasswordManager.
3. Type `1` (Work with users with weak passwords) and press Enter. Press Page Down to display additional profiles. Notice that the NETIQ profile you configured is not on the list of users with weak passwords.
4. Press F2 three times to move the sort column identifier (a dot) to the Days column. This sort order helps you identify users with stale passwords. Requiring regular passwords changes is a proactive security measure.
5. Press F2 twice more to sort by Special Authority. This sort order displays user profiles with special authorities at the top. Powerful profiles with weak passwords should be immediately secured or disabled until the password is strengthened.
6. Press F12 to return to the Password Manager Main Menu.
7. Type `4` (Work with word lists) and press Enter.
8. Press F4 (Prompt) and tab to ENGLISH.
9. Type `1` and press Enter.

10. Tab to Remove embedded vowels and type `*YES`.

11. Press Enter. PSPasswordManager displays a progress message while it updates the selected password list. The update can take some time. When complete, the product displays Finished updating word inventory.

12. Press F12 to return to the Password Manager Main Menu.

13. Type `1` (Work with users with weak passwords) and press Enter.

14. Press Page Down until you see the NETIQ profile. With the change you made to the word list, the password for the NETIQ profile is now considered weak. The password was SPRMN, which is superman with the vowels removed.

15. Tab to the Opt column for the NETIQ profile.

16. Type `10` (Act On) and press Enter.

17. Tab to Change User Status.

18. Type `*DISABLED` and press Enter.

19. Press Enter to return to the Work With Selected Passwords menu.

20. Press F5 to refresh the display, and if necessary, press Page Down until you see the NETIQ profile. Notice that the Status is now DISABLED.