User Guide

NetIQ® Security Solutions for iSeries - Privilege Manager

October 22, 2007

Contents

About This Book and the Library

The user guide provides conceptual information about the NetIQ Security Solutions for iSeries - Privilege Manager product (Privilege Manager). This book defines terminology and various related concepts.

Intended Audience

This book provides information for Security Officers or Administrators responsible for escalating users privileges to objects, such as commands, programs, and database files, on System i5, iSeries, and AS/400 servers.

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.

Installation Guide
Provides detailed planning and installation information.

User Guides
Provides conceptual information about the NetIQ Security Solutions for iSeries products. 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

Help
Provides definitions for each field and each window.

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

As an Security Officer, you must often grant users broad authorities to address problems or perform routine maintenance on production servers. Most tasks should require only temporary, limited authorities, but because native tools lack this granular control, you must assign broad access.

For example, to complete routine maintenance on a server subject to Sarbanes-Oxley (SOX) compliance, you may delegate *SECOFR authority, even though the user needs to run only one specific program.

This breadth of access concerns both you and your internal and external auditors. There are several problems you need to address:

- You want to limit the number of team members who have *SECOFR authority.
- You must grant access to someone to perform the maintenance.
- Tracking user authorities to meet regulatory compliance for all your IT personnel is time-consuming.
- You need to ensure server availability, but regulations make you document every change.
- When a server falters, you need to take fast remedial action to meet your Service Level Agreement (SLA).

What is 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 one-time or regularly scheduled maintenance window and assign the task to a specific user or user group.

What User Roles Does Privilege Manager Support?

User roles enforce separation of duties on production servers, and reduce security risks by maintaining strict control over server changes. Privilege Manager provides the following user roles:

Administrators

Administrators are the only users who can configure Privilege Manager and define the escalation model that determines who has authority to managed servers. Administrators use the Privilege Manager main menu to perform these tasks and to monitor activity. The Administrators role in Privilege Manager has no constraints. Privilege Manager Administrators must be members of the PSSecure (PSS) and Privilege Manager (PSP) authorization lists. You can authorize users to products using option 70 (Utilities menu) from the NetIQ Product Access Menu. For more information, see the *Installation Guide for NetIQ Security Solutions for iSeries*.

Users

Privilege Manager users are users that have entitlements to specified commands, programs, and database files on specified managed servers during specified timeframes. Users can access managed servers with escalated privileges using the command line interface. Privilege Manager users are not members of the PSSecure (PSS) and Privilege Manager (PSP) authorization lists and do not have authorities to use the Privilege Manager main menu.

What are Entitlements?

Privilege Manager lets you assign temporary authorities, called **entitlements**, to critical servers so you can define the following:

- Which users can make changes
- Which objects (commands, programs, or files) they can access during the session
- Which library the object is located in on the specified server
- Which swap profile is used to access the objects
- Which servers they can access
- A timeframe to execute the task

The assigned user can then use the NQPRVMGR command to access the command, program, or file on the managed server. While using the NQPRVMGR command, the user can access only the specified objects. When the user completes the command, Privilege Manager revokes all escalated authorities.

While accessing the server, Privilege Manager audits user activity. The Privilege Manager object access failure reports show who attempted to access a command, program, or file to which they were not entitled.

Using an escalated permission access model, you can tightly limit the native authorities individual users have, while still providing the access they need to maintain or troubleshoot managed servers.

How Privilege Manager Helps You

Privilege Manager helps you increase compliance and ensure operational integrity while reducing the cost of compliance for all your managed servers.

Increases 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. Privilege Manager 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.

Ensures Operational Integrity

No server runs continuously without needing attention for troubleshooting, maintenance, or performance tuning. Using Privilege Manager, you can assign the authorities users require to work on servers in need of PTFs or other changes. The escalation of privileges helps reduce the risk associated with widespread distribution of powerful authorities.

Reduces the Cost of Compliance

When you use Privilege Manager, you can quickly reduce the number of user profiles that have access to sensitive commands. The result is fewer profiles you have to audit and track.

Because you can securely escalate only the authorities needed to fix, update, or troubleshoot server problems, Privilege Manager 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. Privilege Manager reports keep you and your auditors up to date, showing all mediated activity for specified servers or users during a specified period.

Chapter 2
Setting Up Your Escalation Model

Privilege Manager offers an escalation model that allows administrators to control who has access where, to which commands, programs, and files, using which swap profile, and when that access is possible. Administrators escalate permissions for users by granting entitlements that define the following criteria:

- Which users can make changes
- Which commands, programs, or files **(objects)** they can access during the session
- Which library the object is located in on the specified server
- Which swap profile is used to access the objects
- Which servers they can access
- A timeframe to execute the task

Administrators must be members of the PSSecure (PSS) and Privilege Manager (PSP) authorization lists. You can authorize users to products using option 70 (Utilities menu) from the NetIQ Product Access Menu. For more information, see the *Installation Guide for NetIQ Security Solutions for iSeries*.

Getting Started

Use the following checklist to start using Privilege Manager and to ensure you set up an escalation model that meets the needs of your organization.

☑	Checklist Items
☐	**1.** Read the topics about entitlements to ensure you understand how Privilege Manager works. For more information, see “Understanding Entitlements” on page 8.
☐	**2.** Define your enterprise workflows. For more information, see “Defining Your Workflows” on page 11.
☐	**3.** Plan and implement the appropriate user groups. For more information, see“Creating User Groups” on page 13.
☐	**4.** Plan and implement the appropriate command, program, and file groups. For more information, see “Creating Object Groups” on page 14.
☐	**5.** Plan and implement the appropriate server groups. For more information, see “Creating Server Groups” on page 15.
☐	**6.** Plan and implement the appropriate swap profile groups. For more information, see “Creating Swap Profile Groups” on page 16.
☐	**7.** Configure the default swap user profile for entitlements. For more information, see “Configuring a Default Swap User Profile” on page 23.
☐	**8.** Start setting up entitlements for users. For more information, see “Creating Entitlements” on page 29.

Understanding Entitlements

A Privilege Manager **entitlement** is a complete set of access rights that you configure. An entitlement consists of one or more users who have access to one or more objects on one or more managed servers during a specified time frame.

One entitlement might allow a single user to access a single managed server using a single command to perform a specific task during a one-time only access window. Another entitlement might allow multiple users to access multiple managed servers to perform common maintenance tasks using several commands and programs during a recurring access window. You can create as many entitlements as necessary to provide granular levels of access to users.

Components of an Entitlement

Privilege Manager allows you to create entitlements to your managed servers. Entitlements include the following components:

Users
: Specifies the staff members who need to access managed servers to perform maintenance or configuration tasks. You can add individual users or groups of users to the entitlement. For more information about creating Privilege Manager user groups, see "Creating User Groups" on page 13.

Objects
: Specifies the commands, programs, and files you want the user to access when performing maintenance or configuration tasks. For more information, see "Creating Object Groups" on page 14.

Libraries
: Specifies the libraries where the specified commands, programs, and files are located on the specified servers.

Object Type
: Specifies whether the listed object is a command, program, or file.

Swap User Profiles
: Specifies the user profile used to authorize a user to the specified objects. The entitlement temporarily escalates the user's authorities by running under the authority of the swap profile instead of the authority of the signed-on user profile. For more information about creating swap profile groups, see "Creating Swap Profile Groups" on page 16.

Server

Specifies the iSeries servers or IP addresses where you want to escalate user authorities to the objects specified in the entitlement. You can add individual servers or groups of servers to the entitlement. For more information about creating Privilege Manager server groups, see "Creating Server Groups" on page 15.

Calendars

Specifies the timeframe during which an entitlement is effective. For more information about creating calendars, see "Creating Calendars" on page 17.

Authentication

Specifies whether users must sign on to gain escalated privileges defined in the entitlement.

Alerting

Specifies whether Privilege Manager sends event notifications to NetIQ Security Solutions for iSeries - PSDetect or NetIQ Security Manager. For more information, see "Configuring Event Notifications" on page 24.

Description

Specifies the reason for the entitlement.

Using Entitlements Effectively

The steps for creating entitlements are simple, but using entitlements most effectively requires analysis and planning. Your privilege escalation model helps you determine how granular access rights should be. You should define your privilege escalation model before creating entitlements.

Defining Your Privilege Escalation Model

The following sections provide guidance for defining your Privilege Manager escalation model.

Defining Your Workflows

The most important step in setting up your escalation model is to identify your organization's workflows. Each workflow determines *who* needs to be able to do *what* on *which* managed servers, and *when* they need to be able to do it. Use your workflow definitions to create the groups and calendars needed for your organization, and then set up the necessary entitlements.

Identify the user profiles and resources in your organization, and then consider the following questions:

- How is your organization structured? Would it make more sense to organize resources geographically (by site), or by business unit?
- Which users need to access these servers, and what tasks do they typically perform?
- Do these users typically do these tasks during a specific timeframe?
- What authorities do these staff members currently have?
- What minimum authorities do these staff members need to do their work?
- What are the users' job functions?

Authority Escalation Worksheet

Use the following worksheet to help you define your workflow:

Users	Swap User Profile	Commands, Programs, and Files	Libraries	Servers	Timeframe

Planning Groups

Before you start creating entitlements, define appropriate groups for users, objects, servers, and swap profiles. Creating groups helps you manage the number of entitlements you need to create and maintain.

Creating User Groups

User groups represent the job function of your staff members or the location where they work, such as night workers or Houston workers. Choose a group structure that maps to the setup of your organization. If you want to manage all entitlements from a single server, create user groups for user profiles on any server where Privilege Manager is installed. For more information, see "Centrally Managing Privilege Manager" on page 41.

To create a user group:

1. From the Privilege Manager main menu, type `2` (Work with PM Groups) and then press Enter.
2. Type `1` (Edit User Group Header) and press Enter.
3. Press F6 (Create).
4. If prompted, specify a reason for editing the header file, and then press Enter.
5. In the **USRGRP** field, specify the name of the user group you want to add, and then press Tab. User group names must start with a colon (:).
6. In the **USRGRPDSC** field, type a brief description of the user group, and then press Enter.
7. Press F3 (Exit).
8. Type `2` (Edit User Group Detail) and press Enter.
9. Press F6 (Create).
10. If prompted, specify a reason for editing the detail file, and then press Enter.

11. In the **USRGRP** field, specify the name of the user group to which you want to add the user profile, and then press Tab. User group names must start with a colon (:).
12. In the **USRNM** field, specify the name of the user profile, and then press Tab.
13. In the **USRDSC** field, type a brief description of the user profile, and then press Enter.
14. Press F3 (Exit).

Creating Object Groups

Object groups represent the commands, programs, and fields your staff members need to access to solve problems or perform required maintenance. If you want to manage all entitlements from a single server, create object groups for objects on any server where Privilege Manager is installed. For more information, see "Centrally Managing Privilege Manager" on page 41.

To create a command and program group:

1. From the Privilege Manager main menu, type `2` (Work with PM Groups) and then press Enter.
2. Type `10` (Edit Object Group Header) and press Enter.
3. Press F6 (Create).
4. If prompted, specify a reason for editing the header file, and then press Enter.
5. In the **OBJGRP** field, specify the name of the command, program, or file group you want to add, and then press Tab. Object group names must start with a colon (:).
6. In the **OBJGRPDSC** field, type a brief description of the command, program, or file group, and then press Enter.
7. Press F3 (Exit).
8. Type `11` (Edit Object Group Detail) and press Enter.
9. Press F6 (Create).

10. If prompted, specify a reason for editing the detail file, and then press Enter.
11. In the **OBJGRP** field, specify the name of the object group to which you want to add the command, program, or file, and then press Tab. Object group names must start with a colon (:).
12. In the **OBJNM** field, specify the command, program, or file, and then press Tab.
13. In the **OBJLB** field, specify the library where the command, program, or file is located, and then press Tab.
14. In the **OBJTYP** field, specify whether the object is a command (`*CMD`), program (`*PGM`), or file (`*FILE`), and then press Tab.
15. Leave the **OBJPARM** field blank.
16. Press F3 (Exit).

Creating Server Groups

Server groups represent a view of your organization, such as organizational hierarchy or physical location of servers. Choose a group structure that maps to the setup of your organization. If you want to manage all entitlements from a single server, create server groups for all servers where Privilege Manager installed. For more information, see "Centrally Managing Privilege Manager" on page 41.

To create a server group:

1. From the Privilege Manager main menu, type `2` (Work with PM Groups) and then press Enter.
2. Type `20` (Edit Server Group Header) and press Enter.
3. Press F6 (Create).
4. If prompted, specify a reason for editing the header file, and then press Enter.
5. In the **SVRGRP** field, specify the name of the server group you want to add, and then press Tab. Server group names must start with a colon (:).
6. In the **SVRDSC** field, type a brief description of the server group, and then press Enter.

7. Press F3 (Exit).
8. Type 21 (Edit Server Group Detail) and press Enter.
9. Press F6 (Create).
10. If prompted, specify a reason for editing the detail file, and then press Enter.
11. In the **SVRGRP** field, specify the name of the server group to which you want to add the server, and then press Tab. Server group names must start with a colon (:).
12. In the **SVRNM** field, specify the name of the server or the IP address of the server, and then press Tab.
13. In the **SVRDSC** field, type a brief description of the server, and then press Enter.
14. Press F3 (Exit).

Creating Swap Profile Groups

Swap profile groups represent user profiles with more authority than the average user. These authorities provide access to the objects specified in the entitlement so users can perform the required maintenance or tasks on the managed server.

If the swap profile group contains the default swap profile defined in the Work with PM Defaults screen, users can access the objects in the entitlement without specifying the swap group. For more information, see "Configuring a Default Swap User Profile" on page 23.

If you want to manage all entitlements from a single server, create swap profile groups for user profiles on any server where Privilege Manager is installed. For more information, see "Centrally Managing Privilege Manager" on page 41.

To create a swap profile group:

1. From the Privilege Manager main menu, type 2 (Work with PM Groups) and then press Enter.
2. Type 30 (Edit Swap Group Header) and press Enter.
3. Press F6 (Create).

4. If prompted, specify a reason for editing the header file, and then press Enter.
5. In the **SWPGRP** field, specify the name of the swap profile group you want to add, and then press Tab. Swap profile group names must start with a colon (:).
6. In the **SWPDSC** field, type a brief description of the swap profile group, and then press Enter.
7. Press F3 (Exit).
8. Type `31` (Edit Swap Group Detail) and press Enter.
9. Press F6 (Create).
10. If prompted, specify a reason for editing the detail file, and then press Enter.
11. In the **SWPGRP** field, specify the name of the swap group to which you want to add the profile, and then press Tab. Swap profile group names must start with a colon (:).
12. In the **SWPUSR** field, specify the name of the profile, and then press Tab.
13. In the **SWPDSC** field, type a brief description of the profile, and then press Enter.
14. Press F3 (Exit).

Creating Calendars

Privilege Manager allows you to define timeframes (calendars) that specify when users can use the entitlement. For example, when creating an entitlement for night workers, you can specify a calendar that allows users to use the entitlement from 5:01 PM to 8:00 AM Monday through Saturday. If a calendar is not defined for an entitlement, the entitlement is valid any time and has no end date.

If you want to manage all entitlements from a single server, create calendars for use on all servers where Privilege Manager installed. For more information, see "Centrally Managing Privilege Manager" on page 41.

To create a calendar:

1. From the Privilege Manager main menu, type `3` (Work with Calendar) and then press Enter.
2. Press F6 (Create).
3. In the **Calendar Name** field, type a descriptive name for the calendar, and then press Tab.
4. In the **Start Date** field, type the beginning date for which the calendar is valid in the *YY/MM/DD* format, where *YY* is the two-digit year, *MM* is the month, and *DD* is the day.
5. Press Tab.
6. In the **Start Time** field, type the beginning time for which the calendar is valid in the *HH:MM:SS* format, where *HH* is the hour in 24-hour time, *MM* is the minute, and *SS* is the second.
7. Press Tab.
8. In the **End Date** field, type the end date for which the calendar is valid in the *YY/MM/DD* format, where *YY* is the two-digit year, *MM* is the month, and *DD* is the day.
9. Press Tab.
10. In the **End Time** field, type the end time for which the calendar is valid in the *HH:MM:SS* format, where *HH* is the hour in 24-hour time, *MM* is the minute, and *SS* is the second.
11. Press Tab.
12. In the **Description** field, type a reason for adding the calendar and press Enter.
13. Press Enter.
14. ***If you want to modify the day of the week and time of day when users can access the associated entitlements***, type `2` (Edit) and press Enter.
15. Type `X` to the right of the days of the week for which the entitlement applies.

16. In the **Start Time** field, type the beginning time that users can use the entitlement on the specified days of the week in the *HH:MM:SS* format, where *HH* is the hour in 24-hour time, *MM* is the minute, and *SS* is the second.

17. In the **End Time** field, type the end time that users can use the entitlement on the specified days of the week in the *HH:MM:SS* format, where *HH* is the hour in 24-hour time, *MM* is the minute, and *SS* is the second.

18. Press Enter.

19. Press Enter.

20. ***If you want to add additional timeframes when users can access the associated entitlements***, repeat Steps **14** through **19**.

21. Press F3 (Exit).

Chapter 3
Configuring Privilege Manager

Privilege Manager offers a number of options for customizing journaling, auditing, access, and notification settings. Administrators can customize these settings any time after installation. Administrators must be members of the PSSecure (PSS) and Privilege Manager (PSP) authorization lists. You can authorize users to products using option 70 (Utilities menu) from the NetIQ Product Access Menu. For more information, see the *Installation Guide for NetIQ Security Solutions for iSeries*.

If you want to manage all entitlements from a single server, the following Privilege Manager configurations apply to all servers where Privilege Manager installed. For more information, see "Centrally Managing Privilege Manager" on page 41.

Configuring Transaction Journaling

You can define the journal to which Privilege Manager journals user actions in NQPRVMGR. Privilege Manager queries these journal entries when running PM Usage Reports.

To configure journaling:

1. From the Privilege Manager main menu, type `10` (Work with PM Defaults) and press Enter.
2. In the **PM Transaction Journal** field, type the name of the journal where you want to log Privilege Manager events, and then press Tab.
3. In the **PM Transaction Journal Library** field, type the name of the library where specified journal is located, and then press Enter.

Configuring Auditing

You can define audit journals to which Privilege Manager journals Administrator actions, such as entitlement configuration. Privilege Manager queries these journal entries when running PM Configuration Changes Reports.

To configure auditing:

1. From the Privilege Manager main menu, type `10` (Work with PM Defaults) and press Enter.
2. In the **Audit PM Configuration Changes?** field, type `Y` and then press Tab.
3. In the **PM Audit Journal** field, type the name of the journal where you want log Privilege Manager auditing, and press Enter.
4. In the **PM Audit Journal Library** field, type the name of the library where the specified journal is located, and press Enter.
5. On the iSeries command line, type `CALL PSCOMMON/PRM0500C` and press Enter.

Configuring a Default Swap User Profile

If you assign a default swap user profile and you assign this profile as a swap profile in an entitlement, users do not need to enter a swap profile when accessing the NQPRVMGR command. For example, if you set the default swap user profile to QSECOFR and add QSECOFR as the swap profile in an entitlement, the user leaves *DEFAULT as the swap profile when using the NQPRVMGR command. The *DEFAULT value prevents users from knowing to which profile they are swapping and what authorities the profile has.

To configure a default swap user profile:

1. From the Privilege Manager main menu, type `10` (Work with PM Defaults) and press Enter.
2. In the **Default Swap User** field, specify the user profile you want associated with the `*DEFAULT` value in the NQPRVMGR command.
3. Press Enter.

Configuring Session Time-out

You can require users to authenticate when using the NQPRVMGR command to gain escalated privileges defined in entitlements. Privilege Manager allows you to specify the length of NQPRVMGR session inactivity before a user must log in to use the NQPRVMGR command.

If a user does not log off the session and leaves the workstation unattended, another user at that workstation could access the NQPRVMGR command. Configuring session time-out helps you prevent unauthorized use of entitlements from a physical workstation.

To configure a default session time-out:

1. From the Privilege Manager main menu, type `10` (Work with PM Defaults) and press Enter.
2. In the **Session Timeout** field, specify the number of minutes the NQPRVMGR command screen can remain inactive before Privilege Manager requires the user to log in to use the NQPRVMGR command.
3. Press Enter.

Configuring 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.

PSDetect monitors iSeries systems for unauthorized attempts to gain access. By reading system logs, PSDetect searches for critical system events that unauthorized access attempts generate. You can define multiple actions for each notification, such as automatic reply, page, execute command, call program, or forward a message to another queue or system. For more information, see the *User Guide for NetIQ Security Solutions for iSeries - PSDetect*.

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. 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, Security Manager sends alerts to the Security Manager consoles and can email or page your staff so they can quickly respond. For more information, see the *User Guide for Security Manager*.

To configure event notifications:

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. ***If you want to send event notifications to Security Manager***, in the **Security Manager IP Address** field, specify the IP address of the Security Manager console where you want to send notifications.
4. ***If you want to send event notifications to PSDetect***, ensure the PSDetect ZPSD subsystem is started. For more information, see the *User Guide for NetIQ Security Solutions for iSeries - PSDetect*.
5. ***If you want to send event notifications to a user-defined message queue***, complete the following steps:
   a. In the **Alert Message Queue** field, specify the name of the message queue where you want to send notifications.
   b. In the **Alert Message Queue Library** field, specify the library where the alert message queue is located.

   Note
   If the **Alert Type** field is set to `*SM` or `*NONE`, the **Alert Message Queue** and **Alert Message Queue Library** fields must be blank.
6. Press Enter.

Defining NQPRVMGR Command Access

Privilege Manager provides the ability to limit the workstation or IP address from which a user can issue the NQPRVMGR command. By default, access to the NQPRVMGR command is granted to all users from any workstation or IP address. As soon as you define command access for a user, Privilege Manager automatically restricts access to the NQPRVMGR command for all users from any workstation or IP address not defined in Privilege Manager.

To define NQPRVMGR command access:

1. From the Privilege Manager main menu, type **4** (Work with Access Control) and then press Enter.
2. Press F6 (Create).
3. If prompted, specify a reason for updating the Work with Access Control file, and then press Enter.
4. In the **RSTUSRNM** field, type the user profile or user profile group for which you want to define NQPRVMGR command access, and then press Tab.
5. In the **RSTADDR** field, type the name of the workstation or the IP address of the workstation where you want the user to access the NQPRVMGR command, and then press Enter.
6. Repeat Steps **4** through **5** for each user you want to define access to the NQPRVMGR command.
7. Press F12.

Defining File Editors

By default, Privilege Manager uses UPDDTA to edit all files accessed through the NQPRVMGR command when a file editor is not specified in the entitlement. If you want to use other file editors with this command, you must add them to the list of valid file editors. If you do not want users to access files using UPDDTA, remove this file editor from the list.

Note

If an entitlement contains a file editor command, the file editor in the entitlement overrides file editors defined in the Work With File Editors screen.

To define file editors:

1. From the Privilege Manager main menu, type **11** (Work with File Editors) and then press Enter.
2. Press F6 (Create).
3. If prompted, specify a reason for modifying the Work with File Editor file, and then press Enter.
4. In the **EDTCMD** field, type the name of the editor you want available for editing files using the NQPRVMGR command, and then press Tab.
5. In the **EDTLIB** field, type the library where the file editor command is located, and then press Enter.
6. In the **EDTPARM** field, type the name of the parameter the file editor uses to specify the file to be edited. For example, in the command `UPDDTA FILE(`*`PDA/TESTFILE`*`) MBR(*FIRST)`, the parameter `FILE` contains the name of the file to be edited.
7. Repeat Steps **4** through **5** for each file editor you want available when issuing the NQPRVMGR command.
8. Press F12.

Chapter 4
Escalating Privileges

By escalating privileges through entitlements, administrators can enable users to use objects (commands, programs, and files) on managed servers to do their work while limiting the authorities granted to each user profile. The following sections provide step-by-step instructions for working with entitlements.

These topics assume you are already familiar with Privilege Manager basic entitlement concepts and that you have created the necessary user, object, and swap profile groups. For more information, see "Getting Started" on page 8.

Administrators must be members of the PSSecure (PSS) and Privilege Manager (PSP) authorization lists. You can authorize users to products using option 70 (Utilities menu) from the NetIQ Product Access Menu. For more information, see the *Installation Guide for NetIQ Security Solutions for iSeries*.

Creating Entitlements

When you start setting up entitlements, refer to your completed Authority Escalation Worksheet. For information about planning entitlements, see "Getting Started" on page 8.

If you want to manage all entitlements from a single server, create entitlements that apply to all servers where Privilege Manager installed. For more information, see "Centrally Managing Privilege Manager" on page 41.

To create entitlements:

1. From the Privilege Manager main menu, type `1` (Work with Entitlements) and press Enter.
2. Press F6 (Add).
3. In the **User** field, type the name of the user profile or Privilege Manager user group for which you want to escalate privileges, and then press Tab. For more information about Privilege Manager user groups, see "Creating User Groups" on page 13.
4. In the **Object** field, type the command, program, file, or object group for which you want to escalate permissions, and then press Tab.
5. In the **Library** field, type the library where the command, program, or file is located. If the entry in the **Object** field is a group name, this field must be left blank.
6. In the **Object Type** field, specify whether the object is a command (*CMD), program (*PGM), or file (*FILE). If the entry in the **Object** field is a group name, this field must be left blank.
7. In the **Swap User** field, type the user profile or Privilege Manager swap profile group used to authorize a user to the objects specified in the entitlement.

   If you want users to access the entitlement using the default swap user profile, ensure you include the default swap user defined in the Work With PM Defaults screen in this field or in the specified swap profile group. For more information, see "Configuring a Default Swap User Profile" on page 23.
8. In the **Calendar** field, type the name of the Privilege Manager calendar that defines when the entitlement is valid.
9. In the **Authentication Required?** field, specify whether the user is required to log in to access the entitlement.
10. In the **Alert Required?** field, specify whether Privilege Manager sends an alert when the entitlement is accessed.
11. In the **Enabled Status** field, specify whether the entitlement is enabled.

12. In the **Server** field, type the name of the server or Privilege Manager server group where you want to escalate the user's authorities to the specified object.
13. In the **Description** field, specify a reason for creating the entitlement.
14. Press Enter.

Copying Entitlements

You can create a new entitlement by copying an existing entitlement. Copying an entitlement provides a quick and easy way to create multiple new entitlements. For example, you can create entitlements for your daytime workers, and then copy these entitlements for your nighttime workers to ensure consistent authority escalation across teams.

To copy an entitlement:

1. From the Privilege Manager main menu, type `1` (Work with Entitlements) and press Enter.
2. Place your cursor in the **Opt** field to the left of the entitlement you want to copy.
3. Type `3` (Copy) and press Enter.
4. Change the values in the appropriate fields, and then press Enter.
5. Press Enter.

Modifying Entitlements

Administrators can modify any entitlement in the Work with Entitlements screen. Changes to entitlements take effect immediately. The NQPRVMGR command accesses the entitlement file each time the command is issued, ensuring Privilege Manager uses the most recent version.

To modify an entitlement:

1. From the Privilege Manager main menu, type `1` (Work with Entitlements) and press Enter.
2. Place your cursor in the **Opt** field to the left of the entitlement you want to modify.
3. Type `2` (Edit) and press Enter.
4. Modify the entitlement as needed.
5. Press Enter.

Viewing Entitlement Details

The Display Entitlements screen allows you to see all components of a single entitlement.

To view entitlement details:

1. From the Privilege Manager main menu, type `1` (Work with Entitlements) and press Enter.
2. Place your cursor in the **Opt** field to the left of the entitlement for which you want to view details.
3. Type `5` (Display) and press Enter.

Disabling Entitlements

Instead of deleting entitlements that you may want to reuse at a later date, you can disable them until they are needed.

To disable an entitlement:

1. From the Privilege Manager main menu, type `1` (Work with Entitlements) and press Enter.
2. Place your cursor in the **Opt** field to the left of the entitlement you want to disable.
3. Type `2` (Edit) and press Enter.
4. In the **Status** field type `N` and press Enter.

Deleting Entitlements

Administrators can permanently delete any entitlement in the Work with Entitlements screen. To temporarily disable an entitlement, see "Disabling Entitlements" on page 33.

To delete an entitlement:

1. From the Privilege Manager main menu, type `1` (Work with Entitlements) and press Enter.
2. Place your cursor in the **Opt** field to the left of the entitlement you want to delete.
3. Type `4` (Delete) and press Enter.
4. Press Enter.

Chapter 5
Accessing Escalated Privileges

Administrators enable their staff members (users) to perform tasks on managed servers by creating entitlements. Entitlements list the users who can access managed servers using the NQPRVMGR command, which commands, programs, or files (objects) they can use to do the work, which profile with escalated privileges (swap profile) is used to access the objects, and the timeframe (calendar) when they can do their work.

You can access escalated privileges to perform maintenance or configuration work as soon as an Administrator grants you the necessary entitlements.

To access escalated privileges:

1. Sign on to the iSeries server where you need to perform or configuration work.
2. On the command line, type `PSCOMMON/NQPRVMGR` and press **Enter**.
3. In the **Command/Program to execute** field, type the command you need to execute, and then press Tab.
4. In the **Swap User** field, type the name of the swap user profile used during this session or leave this field `*DEFAULT` when using the default swap user profile, and then press Tab.
5. If required, type the password for your user profile in the **User Password** field, and then press Tab.
6. In the **Reason for use** field, specify the reason for using the entitlement, and then press Enter.

Chapter 6
Reporting on Privilege Escalation

Privilege Manager reports provide critical information for internal and external auditors, and enable your enterprise to demonstrate regulatory compliance.

Administrators must be members of the PSSecure (PSS) and Privilege Manager (PSP) authorization lists. You can authorize users to products using option 70 (Utilities menu) from the NetIQ Product Access Menu. For more information, see the *Installation Guide for NetIQ Security Solutions for iSeries*.

Understanding Report Types

To help you and your auditors keep up to date with all mediated activity for specified servers or users during a specified period, Privilege Manager provides the following report categories:

- Usage reports
- Configuration Changes reports

Usage Reports

Usage reports provide data on user transactions from the NQPRVMGR command. You can use these reports to easily see the following usage information:

- Objects accessed
- Object access failures
- Entitlement usage details

Usage reports query the user-defined Privilege Manager transaction journal. For more information, see "Configuring Transaction Journaling" on page 22.

Configuration Changes Reports

Configuration Changes reports provide data on Administrator actions performed in the Privilege Manager product screens. You can use these reports to easily see changes made to the following types of information:

- Configuration settings
- Groups
- File editors
- Calendars
- Access controls

Configuration Changes reports query the user-defined Privilege Manager audit journal. For more information, see "Configuring Auditing" on page 22.

Running Reports

The Work With PM Reports screen provides access to all Privilege Manager reports. If you are a member of the PSSecure (PSS) and Privilege Manager (PSP) authorization lists you automatically have permissions to run Usage reports. To run Configuration Changes reports, you must also be a member of the PSAudit (PSA) authorization list.

You can authorize users to products using option 70 (Utilities menu) from the NetIQ Product Access Menu. For more information, see the *Installation Guide for NetIQ Security Solutions for iSeries*.

To run a Privilege Manager report:

1. From the Privilege Manager main menu, type `20` (Work With PM Reports) and press Enter.
2. ***If you want to run a Usage report.***, type `1` (PM Usage Reports) and then press Enter.
3. ***If you want to run a Configuration Changes report***, type `2` (PM Configuration Changes Report) and then press Enter.
4. Complete the screen and press Enter. For more information about each field, see the Help.

Chapter 7
Centrally Managing Privilege Manager

Privilege Manager allows you to transfer all Privilege Manager data, such as entitlements, group information, calendars, and default settings from one iSeries server to another iSeries server where Privilege Manager is installed. This feature allows you to create and maintain all entitlements from a single server and then distribute them to all servers in your environment.

To migrate Privilege Manager data, you must export the data from the system where you create and maintain all entitlements (source server) to the system where you want to update Privilege Manager data (target server). For the update to take effect, you must import the data on the target server.

Administrators must be members of the PSSecure (PSS) and Privilege Manager (PSP) authorization lists. You can authorize users to products using option 70 (Utilities menu) from the NetIQ Product Access Menu. For more information, see the *Installation Guide for NetIQ Security Solutions for iSeries*.

Exporting Privilege Manager Settings

Managing entitlements from a central server can help reduce the number of entitlements, groups, defined file editors, and calendars you need to create. You can export this data as needed to keep your Privilege Manager data current on all servers.

To export Privilege Manager settings:

1. Ensure the FTP server is running on each target server.
2. ***If you use Remote Request Management***, ensure you have a secured entry for the FTP Client on the source server and a secured entry for the FTP Server on the target server.

   For more information, see the *User Guide for NetIQ Security Solutions for iSeries - Remote Request Management*.
3. Log on to the source server with a user profile that is a member of the PSSecure (PSS) and Privilege Manager (PSP) authorization lists.
4. From the Privilege Manager main menu, type `30` (Work with Export/Import), and then press Enter.
5. Type `1` (Export Configuration Data), and then press Enter.
6. In the **System name or address** field, type the name of the server or IP address where you want to migrate Privilege Manager data.
7. In the **User profile** field, type the name of the user profile used to FTP Privilege Manager data.

   This user profile must be a member of the PSSecure (PSS) and Privilege Manager (PSP) authorization lists on the system to which you are exporting data.
8. In the **Password** field, type the password of the specified user profile.
9. In the **Submit to batch** field, specify whether you want to submit the job in batch mode.
10. Press Enter.

Importing Privilege Manager Data

Importing Privilege Manager data ensures you have the most current entitlements, group information, calendars, defined file editors, and default settings. When importing data you can specify whether all Privilege Manager data is overwritten or whether unique entitlements, calendars, groups, and defined file editors are retained on the system.

To determine whether an entitlement, group, calendar, or defined file editor is unique the key fields must be different from the imported data. For example, if an existing entitlement has the same values in the **User**, **Object**, **Library**, **Type**, **Swap User**, and **Server** fields as an imported entitlement, the entitlement is not unique and all remaining fields in the entitlement are updated with the imported data. If one of these seven fields has a different value, the entitlement is unique and all information is retained. The following list provides all key fields for Privilege Manager components:

Privilege Manager Component	Key Fields
Entitlements	User
	Object
	Library
	Type
	Swap User
	Server
User Group Header	User Group
User Group Detail	User Group
	User Name

Privilege Manager Component	Key Fields
Object Group Header	Object Group
Object Group Detail	Object Group
	Object Name
	Object Library
	Object Type
Server Group Header	Server Group
Server Group Detail	Server Group
	Server Name
Swap Group Header	Swap Group
Swap Group Detail	Swap Group
	Swap Name
Calendar	Calendar Name
Calendar Day/Time Access	Calendar Name
	Start Time
	End Time
Access Control	Restricted User
	Restricted Address
File Editor	Editor Command
	Editor Library

When you retain unique entitlements, calendars, groups, and defined file editors, the settings in the Work With PM Defaults screen are updated with the imported data. If users accessed the retained entitlements with *DEFAULT, ensure the value in the **Default Swap User** field has not changed. If the swap default user has changed, users may not be able to access the entitlement using the *DEFAULT value. Ensure the imported swap user profile exists on the system.

To import Privilege Manager settings:

1. Log on to the target server with a user profile that is a member of the PSSecure (PSS) and Privilege Manager (PSP) authorization lists.
2. From the Privilege Manager main menu, type 30 (Work with Export/Import), and then press Enter.
3. Type 2 (Import Configuration Data), and then press Enter.
4. In the **Import action** field, specify whether you want to overwrite all Privilege Manager data (*REPLACE) or keep unique entitlements, calendars, groups, and defined file editors on the system (*MERGE).
5. In the **Submit to batch** field, specify whether you want to submit the job in batch mode.
6. Press Enter.
7. After the import is complete, from the Privilege Manager main menu, type 10 (Work with PM Defaults), and then press Enter.
8. Press F8 (Update).
9. Press Enter.