# Contents

About This Book and the Library ......................................................................................................................... xi
Conventions ................................................................................................................................................................. xii
About NetIQ Corporation ........................................................................................................................................... xiii

## Chapter 1

**Introduction**

- Features ............................................................................................................................................................... 1
- Functions ............................................................................................................................................................... 4
- User Interface ....................................................................................................................................................... 5
- Security Considerations ....................................................................................................................................... 5
  - Remote Transactions ........................................................................................................................................ 5
  - Previous Security Methods ............................................................................................................................. 7
  - Current Security Methods ................................................................................................................................. 8
- Assessing Security Needs ...................................................................................................................................... 8
- Usage Considerations ........................................................................................................................................... 9
- Reports .................................................................................................................................................................. 10
- Where to Go from Here ....................................................................................................................................... 10

## Chapter 2

**Getting Started**

- Navigation ........................................................................................................................................................... 13
  - Product Screens ............................................................................................................................................. 14
  - Command Screens ........................................................................................................................................ 14
  - Pop-up Windows .......................................................................................................................................... 16
<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Understanding RRM</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production Mode</td>
<td>Production Mode</td>
<td>25</td>
</tr>
<tr>
<td>What If Mode</td>
<td>What If Mode</td>
<td>26</td>
</tr>
<tr>
<td>Groups</td>
<td>Groups</td>
<td>26</td>
</tr>
<tr>
<td>User/Server and User/Object Overrides</td>
<td>User/Server and User/Object Overrides</td>
<td>27</td>
</tr>
<tr>
<td>Calendars</td>
<td>Calendars</td>
<td>28</td>
</tr>
<tr>
<td>Remote Object Authority</td>
<td>Remote Object Authority</td>
<td>28</td>
</tr>
<tr>
<td>Swap Profiles</td>
<td>Swap Profiles</td>
<td>29</td>
</tr>
<tr>
<td>Decision-making Algorithm</td>
<td>Decision-making Algorithm</td>
<td>29</td>
</tr>
<tr>
<td>What If Processing</td>
<td>What If Processing</td>
<td>43</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Product Options</th>
<th>47</th>
</tr>
</thead>
<tbody>
<tr>
<td>RRM Main Menu</td>
<td>RRM Main Menu</td>
<td>48</td>
</tr>
<tr>
<td>Function Key Summary</td>
<td>Function Key Summary</td>
<td>51</td>
</tr>
</tbody>
</table>
Contents 

Work with Secured Entries ................................................................. 53
  Work with User Groups ................................................................. 58
  Work with Network Groups ......................................................... 68
  Work with Operation Groups ....................................................... 74
  Work with Users ........................................................................ 80
  Work with Networks .................................................................. 89
  Work with Operations ............................................................... 92
  Work with Operation Group Members ......................................... 95
  Calendar Maintenance ................................................................. 98

Work with Collected Entries .......................................................... 101
  Create Entry ............................................................................ 106
  Work with Collected Objects ...................................................... 111
  Promote Collected Entries ......................................................... 114

Work with RRM Groups ................................................................. 118
  Work with RRM Object Authorities ............................................ 120
    Object Authority Maintenance .................................................. 123
  Work with Calendars ................................................................. 127
  Work with User/Server Overrides ................................................. 130
  Work with User/Object Overrides .............................................. 133
  Work with Exit Points ............................................................... 136
  Work with RRM Defaults .......................................................... 141
    Work With User/MsgQ Alerts ................................................... 143
  Work with What If Analysis ....................................................... 148
    Work with What If RRM Groups .............................................. 151
  Work With What If Exit Points .................................................. 153
    Playback What If Transaction Database .................................... 157
  What If Reports ......................................................................... 163
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work with RRM Reports</td>
<td>165</td>
</tr>
<tr>
<td>Run Report Command</td>
<td>167</td>
</tr>
<tr>
<td>Transaction Reports</td>
<td>177</td>
</tr>
<tr>
<td>Object Reports</td>
<td>181</td>
</tr>
<tr>
<td>Summary/Statistics Reports</td>
<td>183</td>
</tr>
<tr>
<td>What If Reports</td>
<td>185</td>
</tr>
<tr>
<td>Configuration Reports</td>
<td>187</td>
</tr>
<tr>
<td>All RRM Reports</td>
<td>190</td>
</tr>
<tr>
<td>Work with RRM Report Filters</td>
<td>192</td>
</tr>
<tr>
<td>Manage RRM</td>
<td>200</td>
</tr>
<tr>
<td>Work With Exit Programs</td>
<td>202</td>
</tr>
<tr>
<td>Cycle Remote Servers</td>
<td>205</td>
</tr>
<tr>
<td>Delete Collected Entries</td>
<td>206</td>
</tr>
<tr>
<td>Start/Stop RRM Collection Monitor</td>
<td>209</td>
</tr>
<tr>
<td>Change FTP Attribute</td>
<td>210</td>
</tr>
<tr>
<td>Change Telnet Attribute</td>
<td>212</td>
</tr>
<tr>
<td>RRM Configuration Wizard</td>
<td>214</td>
</tr>
<tr>
<td>Chapter 5</td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td>215</td>
</tr>
<tr>
<td>Reporting Requirements</td>
<td>215</td>
</tr>
<tr>
<td>Report Summary</td>
<td>216</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Transaction Reports</td>
<td>221</td>
</tr>
<tr>
<td>FTP Logon and Server Requests</td>
<td>222</td>
</tr>
<tr>
<td>TCP Signon Server Requests</td>
<td>227</td>
</tr>
<tr>
<td>DDM Request Access</td>
<td>228</td>
</tr>
<tr>
<td>Transfer Function Server Requests</td>
<td>229</td>
</tr>
<tr>
<td>Remote Com/Dist Prog Call Server Requests</td>
<td>230</td>
</tr>
<tr>
<td>File Server Requests</td>
<td>231</td>
</tr>
<tr>
<td>Database Server Requests</td>
<td>232</td>
</tr>
<tr>
<td>Remote SQL Server Requests</td>
<td>235</td>
</tr>
<tr>
<td>Data Queue Original Server Requests</td>
<td>236</td>
</tr>
<tr>
<td>Data Queue Optimized Server Requests</td>
<td>237</td>
</tr>
<tr>
<td>Original Virtual Print Server Request</td>
<td>238</td>
</tr>
<tr>
<td>Network Print Server Entry Requests</td>
<td>239</td>
</tr>
<tr>
<td>Network Print Server Spool File Requests</td>
<td>240</td>
</tr>
<tr>
<td>Network Transactions by Date/Time</td>
<td>241</td>
</tr>
<tr>
<td>Network Transactions by User</td>
<td>242</td>
</tr>
<tr>
<td>Network Transactions by Function</td>
<td>243</td>
</tr>
<tr>
<td>Network Transactions by Server</td>
<td>244</td>
</tr>
<tr>
<td>Network Transactions by Incoming Address</td>
<td>245</td>
</tr>
<tr>
<td>Object Reports</td>
<td>246</td>
</tr>
<tr>
<td>Object Report by Object</td>
<td>246</td>
</tr>
<tr>
<td>Object Report by Date/Time</td>
<td>247</td>
</tr>
<tr>
<td>Object Report by User</td>
<td>248</td>
</tr>
<tr>
<td>Object Report by Function</td>
<td>249</td>
</tr>
<tr>
<td>Object Report by Server</td>
<td>250</td>
</tr>
<tr>
<td>Object Report by Incoming Address</td>
<td>251</td>
</tr>
<tr>
<td>Summary/Statistics Reports</td>
<td>253</td>
</tr>
<tr>
<td>Transaction Summary Report by Server</td>
<td>253</td>
</tr>
<tr>
<td>Transaction Summary Report by User</td>
<td>256</td>
</tr>
<tr>
<td>RRM Audit Report</td>
<td>258</td>
</tr>
<tr>
<td>Collected Entries Report</td>
<td>259</td>
</tr>
</tbody>
</table>
What If Reports ......................................................................................................................... 263
  What If Transactions by Date/Time ............................................................................................. 263
  What If Transaction by User ....................................................................................................... 266
  What If Transaction by Function .............................................................................................. 268
  What If Transaction by Server .................................................................................................. 269
  What If Transaction Summary by Incoming Address .............................................................. 270
Configuration Reports ............................................................................................................ 272
  Secured Entries Report ............................................................................................................. 272
  Exit Point Settings Report ....................................................................................................... 274
  User Groups ............................................................................................................................. 278
  Network Groups ...................................................................................................................... 280
  Operation Groups .................................................................................................................... 281
  Calendars .................................................................................................................................. 282
  Remote Object Authority By User ............................................................................................. 285
  Remote Object Authority By Path ............................................................................................. 286

Chapter 6
Usage Scenarios ........................................................................................................................... 289
  Allow FTP Only Between Multiple iSeries Servers ................................................................. 289
  Restrict Security Officer Activities on a remote PC .............................................................. 292
  Restrict Activities of QSECOFR and All its Members ............................................................ 293
  Prevent the Addition of Objects to a Library ............................................................................ 293
  Enforce Read-Only Access to a Library .................................................................................... 295
  Prevent *ALLOBJ Users From Accessing a File ...................................................................... 296
  Find and Disable a Virus ............................................................................................................ 298

Chapter 7
Operations Navigator Plug-in ................................................................................................... 301
  Features ................................................................................................................................... 301
  Functions ................................................................................................................................. 302
  Documentation ......................................................................................................................... 303
  Operations Navigator GUI ....................................................................................................... 304
Contents

Collected Environment ......................................................................................................... 306
Secured Environment ................................................................................................................ 318
Entries ................................................................................................................................... 319
RRM Groups .......................................................................................................................... 325
Object Authorities ................................................................................................................... 333
Calendars ............................................................................................................................... 340
User/Server Overrides ........................................................................................................... 345
User/Object Overrides ........................................................................................................... 348
Exit Points ............................................................................................................................. 352
What If Environment .............................................................................................................. 357
Entries ................................................................................................................................... 365
RRM Groups .......................................................................................................................... 366
Object Authorities ................................................................................................................... 371
Calendars ............................................................................................................................... 374
User/Server Overrides ........................................................................................................... 376
User/Object Overrides ........................................................................................................... 377
Exit Points ............................................................................................................................. 379
Reports ................................................................................................................................... 381
Report List .............................................................................................................................. 383
Output ................................................................................................................................... 393
Administration ....................................................................................................................... 394
Tools ...................................................................................................................................... 396
User Preferences ..................................................................................................................... 410
RRM Defaults ......................................................................................................................... 412
User Message Alert ................................................................................................................. 417
About This Book and the Library

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

Intended Audience

This book provides information for individuals responsible for managing remote server security by controlling remote requests access to your iSeries server.

Other Information in the Library

The library provides the following information resources:

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

Installation Guide
Provides detailed planning and installation information.

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 - PSDetect
- NetIQ Security Solutions for iSeries - PSPasswordManager
- NetIQ Security Solutions for iSeries - Privilege Manager

Help
Provides definitions for each field and each window.
The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>• Window and menu items</td>
</tr>
<tr>
<td></td>
<td>• Technical terms, when introduced</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>• Book and CD-ROM titles</td>
</tr>
<tr>
<td></td>
<td>• Variable names and values</td>
</tr>
<tr>
<td></td>
<td>• Emphasized words</td>
</tr>
<tr>
<td><strong>Fixed Font</strong></td>
<td>• File and folder names</td>
</tr>
<tr>
<td></td>
<td>• Commands and code examples</td>
</tr>
<tr>
<td></td>
<td>• Text you must type</td>
</tr>
<tr>
<td></td>
<td>• Text (output) displayed in the command-line interface</td>
</tr>
<tr>
<td><strong>Brackets</strong>, such</td>
<td>• Optional parameters of a command</td>
</tr>
<tr>
<td>as <code>[value]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Braces</strong>, such as</td>
<td>• Required parameters of a command</td>
</tr>
<tr>
<td><code>{value}</code></td>
<td></td>
</tr>
<tr>
<td><strong>Logical OR</strong>, such</td>
<td>• Exclusive parameters. Choose one parameter.</td>
</tr>
<tr>
<td>as `value1</td>
<td>value2`</td>
</tr>
</tbody>
</table>
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
RRM is used to manage remote requests on iSeries systems by determining whether incoming transactions are authorized to access the target server. A remote request is a transaction that originates outside the target server. By evaluating exit programs and comparing incoming requests to secured entries, RRM determines whether each request is approved or rejected.

Features

RRM provides the following key features, functions, and benefits:

- **Numerous Reports** — Over 40 reports have been added to help you easily identify who is accessing your servers (successfully or unsuccessfully), when, from where, and what action they are taking. Summary reports are included to show user and server activity during specified time intervals. An activity report is also provided to show who made which changes and when to RRM configuration settings and rules.

- **Simplified Administration** — Depending on the size and complexity of your environment, you may have thousands of collected entries or rules (or more!). RRM provides sorting and filtering capabilities that let you quickly find and work with specific rules.
• **What If? Analysis** — A test (“What If”) environment has been added that lets you set up and use new RRM rules and configuration settings and then run a report to show which transactions from your current business environment would pass and which would fail using the test environment. When you are satisfied that you have configured your new rules properly, you can instantly move those rules into production. When a rule set is promoted, if you are still not satisfied with the changes you can instantly go back to the previous rule set. Throughout the What If? analysis and testing process, your existing RRM rules remain intact and are enforced.

• **Powerful and Flexible Controls** — The decision to allow a remote transaction to be executed can be based on any combination of the following controls:
  - User Profile (who can access the server)
  - Network Address (from where, using TCP/IP and SNA)
  - Operation (what can be done, expressed as a server/function/command combination)
  - Day and Time (when access is approved or denied)
  - Objects (which objects are touched, regardless of file system)

RRM also has the granularity to fully parse (if desired) SQL statements and i5/OS commands to ensure that the user submitting the transaction has the necessary authority to all the objects in the requested operation.

User/server and user/object overrides can be configured to bypass all other rules. These overrides can be useful, for example, when you want to quickly grant or deny a user total access to your iSeries server or to specific objects.

User profile swapping is also supported, which is generally used to temporarily give a user more power to perform a specific operation.

• **Groups** — Use of RRM groups also simplifies administration. RRM provides grouping for users, network addresses, and operations (server/function/command combinations). You can create a single rule, for example, to prevent everyone but users in the Human Resources department from accessing the Payroll file from any server, or to prevent everyone from uploading any file using SQL. Groups can be nested for additional convenience.
• **Object Level Security** — RRM provides the ability to specify read, write, execute, or manage authority for objects with native i5/OS security. To simplify rule administration, directory paths and objects can be specified with generic names using wildcard character (*) support. This capability provides another level of protection in addition to native i5/OS resource security. RRM works with, and does not change, your native i5/OS resource security implementation.

• **Full Integrated File System (IFS) Support** — All objects on your iSeries servers can be secured, regardless of file system.

• **PSDetect Integration** — You can set up PSDetect to notify you in real-time when RRM rejects transactions. PSDetect can be configured so that, when it monitors a rejected RRM transaction, it can send any combination of an e-mail alert, a page, an SNMP trap alert, or an i5/OS command.

• Each remote server can be configured separately so that the task of securing your iSeries systems does not have to be an overwhelming, “all-or-nothing” proposition. This capability lets you secure your TELNET server first, and then work on other servers (such as FTP and SQL) when time allows.

• Controls and secures all IBM remote exit points.

• Supports a GUI user interface for use with IBM’s Operations Navigator.

• Provides an RRM Configuration Wizard that simplifies the initial setup of primary RRM controls.

• Provides an audit trail of changes made within RRM.

• Provides multiple logging levels.

• Provides diagnostics.

• Uses shorter SQL queries.
RRM includes the following primary functions. All of these functions are available through the RRM Main Menu.

**Work with Secured Entries**
Lets you perform maintenance functions for RRM secured entries. For more information, see “Work with Secured Entries” on page 53.

**Work with Collected Entries**
Lets you maintain collected entries. For more information, see “Work with Collected Entries” on page 101.

**Work with RRM Groups**
Lets you maintain RRM groups. For more information, see “Work with RRM Groups” on page 118.

**Work with RRM Object Authorities**
Lets you maintain object authorities. For more information, see “Work with RRM Object Authorities” on page 120.

**Work with Calendars**
Lets you maintain calendar file records. For more information, see “Work with Calendars” on page 127.

**Work with User/Server Overrides**
Lets you maintain user/server overrides. For more information, see “Work with User/Server Overrides” on page 130.

**Work with User/Object Overrides**
Lets you maintain user/object overrides. For more information, see “Work with User/Object Overrides” on page 133.

**Work with Exit Points**
Lets you maintain RRM exit points. For more information, see “Work with Exit Points” on page 136.

**Work with RRM Defaults**
Lets you maintain RRM default values. For more information, see “Work with RRM Defaults” on page 141.
Work with What If Analysis  
   Lets you test the results of a new configuration before you put it into production.  
   For more information, see “Work with What If Analysis” on page 148.

Work with RRM Reports  
   Lets you generate RRM reports. For more information, see “Work with RRM  
   Reports” on page 165.

Manage RRM  
   Lets you perform functions for managing RRM. For more information, see  
   “Manage RRM” on page 200.

User Interface

RRM is provided with two user interfaces: a conventional iSeries 5250 (green screen)  
user interface and a Windows graphical user interface (GUI) that supports IBM’s  
Operations Navigator. For more information about the appearance and operation of  
the Windows GUI interface, see “Operations Navigator Plug-in” on page 301. The 5250  
user interface, along with other aspects of RRM, are described in the other sections of  
this manual. If plan to use the 5250 user interface, you should review all sections of this  
manual except Chapter 7. If plan to use the Windows GUI interface, you should review  
all sections of this manual in addition to Chapter 7.

Security Considerations

This section describes remote transactions and discusses the previous and current  
methods for securing remote iSeries servers.

Remote Transactions

A remote transaction includes a user, a function, an address, and zero to many objects.  
The RRM decision-making Algorithm compares parsed incoming transactions to a set  
of user configurable rules to determine whether transactions are to be approved or  
rejected (*PASS or *FAIL).
Combinations of the following parameters form these rules:

**User Name**
- designated user name.

**Network Address**
- TCP/IP or SNA.

**Operation (server/function/command)**
- The following are examples:
  - DATAQ_READ_*ALL
  - FTP_LIST_*ALL
  - SQL_EXECUTE_INSERT

**Day-Time**
- Restricts access according to the day of week and time.

**Object**
- RRM maintains its own records of object-level authority (it does not change i5/OS object-level authorities).

**Swap Profile**
- Simplifies administration by allowing a transaction to temporarily acquire more or less authority based on the swap-to profile.

The following examples represent some of the commonly encountered forms of remote transactions:

- A financial analyst accessing the accounts receivable file using Microsoft Access.
- The system administrator gaining more disk space by deleting files using Windows Explorer.
- A tax department member using FTP to download accounting information to a PC-based spreadsheet.
- An accounting clerk and a JD Edwards user making changes to financial databases through remote SQL and/or JD Edwards OneWorld.
- A business analysis downloading corporate production information through FTP and/or SQL.
Previous Security Methods

When the iSeries was introduced in 1988, client/server configurations and Internet-based networks were not widely used as computing models, and did not represent the prevailing security issues.

At that time, the iSeries was accessed only through locally attached TWINAX 5250 terminals, and security was controlled (as it still is) through one or more of the following mechanisms:

**Physical security**
- iSeries servers were usually set up in restricted computer rooms.

**System values**
- Global system values such as the following control the system security level:
  - 10 = Physical Security
  - 20 = Password and User-level (special authorities) Security
  - 30 = Resource or Object-level Security (*ALLOBJ not assigned by default)
  - 40 = System Integrity—access to certain MI instructions are blocked
  - 50 = Primarily for DOD C2 Security—parameter validation and so on

**User level authority**
- When a user profile is created using the CRTUSRPRF command, several parameters are provided that control that user's capabilities. For example, a user's special authorities, if any, and a user's ability to execute i5/OS or user-defined commands from the command line are established here.

**Object level authority**
- Using the i5/OS GRTOBJAUT command, any user with *ALLOBJ or *OBJMGT authority can grant other users authority to individual objects. This method of authorization is tedious, but can be greatly simplified by using the templates and groups provided by PSSecure's Object Authority Management (OAM) function set.
Application level authority
Applications are developed to provide users with specific access to data and commands. PSSecure's Secure Menuing System (SMS) allows users to build secure menus for applications and to control the execution of programs and commands for new functions or as a shell to control access to existing applications.

Current Security Methods

Today, most users access the iSeries through remote connections. The use of twinax 5250 devices is now mainly used for system consoles. The increased use of remote connections to access iSeries has led to an increased need to secure those connections. Application-level (or menu-level) security no longer provides adequate security for the iSeries. To adequately secure a typical iSeries environment, the following types of security must be enforced:

- physical security
- user-level authorization
- object-level authorization
- application-level authorization
- remote-access security

Assessing Security Needs

If you have not reviewed your local security requirements and set up a list of approved entries, you should perform the following task.

Before you implement RRM security, review your local security implementation, evaluate the needs of your users, and determine the level of remote access required so that conflicts do not occur between server-level security and local-level security.
For example, if a user is authorized to update databases in a library through iSeries menu options, but is only allowed to download the data through a file transfer application, you should create only the approved entries needed to satisfy the requirements for this download function.

By activating the request collection for a few weeks and analyzing the requests, you can determine the types of transactions being sent to your iSeries server. For more information, see “Work with Exit Points” on page 136. Then, you can decide which records to promote to approved entries and to keep in the RRM Server. For more information, see “Work with Collected Entries” on page 101.

Usage Considerations

Before you start using RRM, you should review the following usage considerations:

- Before RRM can be used to control remote access, PSSecure remote server exit programs must be installed and the required remote servers must be cycled (restarted). To cycle a server, all remote connections defined on the server must be ended.

- Specifying object-level authority in a rule can result in significant additional checking by the Decision-making Algorithm, especially if generic entries are used, such as /QSYS.LIB/CUSTOMER/ORDERS/*.*.

- If groups such as :DEVELOPERS or :MANAGERS are used to simplify administration by reducing the number of specific entries in the rules list, these groups must be evaluated instead of evaluating specific values, such as JAVAPERSON or MANAGERPERSON.

- Logging is required for RRM reporting. For more information about the logging level requirements for reporting, see “Reporting Requirements” on page 215.
Reports

RRM provides the means to produce the following types of reports:

- Transaction Reports
- Object Reports
- Summary/Statistic Reports
- What If Reports
- Configuration Reports

These reports can be generated by using Option 20 on the RRM Main Menu or by issuing commands on the RRM command line. For more information about RRM report output, see “Reports” on page 215.

RRM reports are also available through NetIQ Secure Configuration Manager. For more information, see the NetIQ Security Solutions for iSeries Installation Guide.

Where to Go from Here

After you have read this chapter, we recommend that you read the following sections in the order shown before you begin using RRM:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Understanding RRM” on page 25</td>
<td>Describes the advanced concepts and processes that underlie the functioning of RRM.</td>
</tr>
<tr>
<td>“Product Options” on page 47</td>
<td>Describes the RRM options available through the user interface.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>“Reports” on page 215</td>
<td>Describes the purpose and format of each RRM report.</td>
</tr>
<tr>
<td>“Getting Started” on page 13</td>
<td>Explains what you need to know to start using RRM.</td>
</tr>
<tr>
<td>“Operations Navigator Plug-in” on page 301 (if you plan to use the Operations Navigator Plug-in for RRM)</td>
<td>Describes the RRM options available through the Operations Navigator user interface.</td>
</tr>
</tbody>
</table>
This chapter provides information you need to start using Remote Request Management (RRM).

Navigation

The functions provided in RRM are accessed through a series of screens and screen elements included in the user interface.

To access RRM:

1. On an iSeries command line, type **PSMENU** and press ENTER.

2. On the NetIQ Product Access Menu, type option 2 (PSSecure) and press ENTER.

3. On the PSSecure Main Menu, type option 3 (Remote Request Management) and press ENTER.

On the RRM Main Menu, you can access the major product options. For more information about the RRM options available through the user interface, see “Product Options” on page 47.
Product Screens

RRM product screens display the data and additional options (selection and function key options) that are available to execute the major options selected on the RRM main menu. For more information about all RRM product screens, see “Product Options” on page 47.

<table>
<thead>
<tr>
<th>Operation</th>
<th>User</th>
<th>Network</th>
<th>Operation</th>
<th>Action</th>
<th>Swap Prf</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>*PUBLIC</td>
<td>*ALL</td>
<td>*ALL</td>
<td>*PASS</td>
<td>&gt;</td>
</tr>
<tr>
<td>Y</td>
<td>*PUBLIC</td>
<td>*ALL</td>
<td>*ALL</td>
<td>*FAIL</td>
<td>&gt;</td>
</tr>
<tr>
<td>Y</td>
<td>*PUBLIC</td>
<td>172.16.37.5</td>
<td>*ALL</td>
<td>*PASS</td>
<td>&gt;</td>
</tr>
<tr>
<td>Y</td>
<td>:USRGRP01</td>
<td>172.16.37.5</td>
<td>CENTRAL_CLACT</td>
<td>*FAIL</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>:USRGRP02</td>
<td>172.16.37.5</td>
<td>CENTRAL_CLACT</td>
<td>*FAIL</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>:USRGRP04</td>
<td>172.16.37.5</td>
<td>CENTRAL_CLACT</td>
<td>*FAIL</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>:USRGRP07</td>
<td>172.16.37.5</td>
<td>CENTRAL_CLACT</td>
<td>*FAIL</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>:USRGRP14</td>
<td>172.16.37.5</td>
<td>CENTRAL_CLACT</td>
<td>*FAIL</td>
<td></td>
</tr>
</tbody>
</table>

F1=Help F3=Exit F6=Add F11=View2 F12=Cancel
F13=Repeat F14=Sort
(c) PentaSafe Security Technologies, Inc. 2001

Command Screens

Command screens provide input fields where you can specify additional criteria to perform a desired task such as generating a report. The following figure shows an example of an RRM command screen.
RRM commands can be issued from any i5/OS command line or from within customer-developed programs. For RRM commands to function correctly, the PSCOMMON library must be at the top of the library list.

PentaSafe - Run Report (PSRUNRPT)

Type choices, press Enter.

Report Id . . . . . . . . . . . . . > NW000094   Name, NW000002....
Report Description . . . . . . 'Transaction Summary Report By Server'

Range of Journal Receivers:
Starting journal receiver . . *CURCHAIN Name, *CURRENT, *CURCHAIN
   Library . . . . . . . . . . . . . . . . . . Name, *LIBL, *CURLIB
Ending journal receiver . . . . . . . . . . . . Name, *CURRENT
   Library . . . . . . . . . . . . . . . . . . Name, *LIBL, *CURLIB

Starting Date and Time:
Starting date . . . . . . . . . *CURR Date, *PRVMS, *PRVME...
Starting time . . . . . . . . . . . . . . . . . . Time (hhmmss)

Ending Date and Time:
Ending date . . . . . . . . . . . . *CURR Date, *PRVMS, *PRVME...
Ending time . . . . . . . . . . . . . . . . . . Time (hhmmss)

More...

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
Pop-up Windows

The following figure shows an example of an RRM pop-up window. Pop-up windows provide additional information or caution you about the task that you are performing.

Preparing to Use RRM

Before you start using RRM, it is recommended that you verify product installation and review the product documentation.

Verify Product Installation

RRM is a component of PSSecure. Verify that the most recent version of PSSecure has been installed.
To verify the version:

1. From a command line on the iSeries system where the product was installed, type the IBM command **DSPSFWRSC**.

2. When the list is displayed, page through it until you find the code **1PSS001**.

3. Press F11 to view the library where this product was installed.

When RRM is installed, a set of initial data is also installed that includes settings for groups and other data elements. For more information on installation, see the *NetIQ Security Solutions for iSeries Installation Guide*.

**Review Product Documentation**

To ensure that you understand the operation of RRM, you should read the following chapters in the order shown before you begin using the product:

<table>
<thead>
<tr>
<th>Chapter Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>“Understanding RRM” on page 25</td>
<td>Describes the advanced concepts and processes that underlie the functioning of RRM.</td>
<td></td>
</tr>
<tr>
<td>“Product Options” on page 47</td>
<td>Describes the RRM functions available through the user interface.</td>
<td></td>
</tr>
<tr>
<td>“Reports” on page 215</td>
<td>Describes the purpose and format of each RRM report.</td>
<td></td>
</tr>
<tr>
<td>“Usage Scenarios” on page 289</td>
<td>Provides representative examples that show how to use RRM.</td>
<td></td>
</tr>
</tbody>
</table>
Use RRM Configuration Wizard

After RRM is installed, it is recommended that you use the RRM Configuration Wizard to configure the product. The RRM Configuration Wizard is provided to simplify the initial setup of primary RRM controls. The wizard prompts you for more information about how you want to use RRM and then configures the product accordingly. You can access the wizard by executing the following option string starting at the RRM Main Menu and pressing ENTER:

```
Opt 30 (Manage RRM) > 30 (RRM Configuration Wizard)
```

For more information, see “RRM Configuration Wizard” on page 214.

Recommended Settings

When you start using RRM, it is recommended that you apply the following settings:

Start Collecting Requests

You should start collecting remote requests for use in developing secured entries for your installation. To begin collecting entries, specify *ALL in the Collected field on the Work With Exit Points screen.

Also, ensure that the RRM Collection Monitor is started by selecting the following menu options starting at the RRM Main Menu:

30 (Manage RRM) > 5 (Start/Stop RRM Collection Monitor) > *START.

For more information, see “Start/Stop RRM Collection Monitor” on page 209.

NetIQ Corporation recommends that you collect enough entries to obtain a representative sampling of the remote requests that are sent to your installation. However, you should periodically check the amount of disk space consumed by collected entries.
Start Logging Incoming Transactions

You should start logging incoming transactions to enable logging of What If transactions. To record the incoming transactions used to test a What If entry, you must activate logging of incoming transactions by specifying *YES in the Log Incoming Transactions field on the Work With Exit Points screen. It is recommended that you use the What If analysis for testing new rules because it lets you test the results of a new configuration before you put it into production.

Restrict Powerful Profiles with Calendars

You should restrict powerful user profiles by limiting their availability for remote devices through calendars. To create a calendar, press F6 on the Work With Calendars screen, specify a name, default action, and the times and days when you want powerful profiles to be available.

Build Initial Rule Set

To help secure your iSeries environment, NetIQ Corporation recommends that you build an initial set of secured entry rules.

To build an initial rule set:

1. Install all RRM exit programs by specifying Option 1 (Install RRM Exit) for each exit program listed on the Work with Exit Programs screen. For more information, see “Work with Exit Points” on page 136.

2. Ensure that the RRM Collection Monitor has been started. If the collection monitor has not been started, specify *START in the RRM collection monitor action field for the RRM Collection Monitor Control (PSRRMCMON) command. For more information, see “Start/Stop RRM Collection Monitor” on page 209.
3. For each exit point listed on the Work with Exit Points screen, specify *REJECT in the Collection Mode field and specify *NO in the Secure Mode field. For more information, see “Work with Exit Points” on page 136. These settings cause RRM to collect all remote requests as collected entries, which will form the basis of the initial secured entry rules set.

**Note**
Because *NO is specified in the Secure Mode field, remote transactions are *blocked* instead of rejected. However, when RRM collects transactions, each one is analyzed by the Decision-making Algorithm and marked “REJECTED” or “ALLOWED” in the RRM Collection database. This method of collecting remote requests lets you identify transactions that would be rejected if *YES was specified in the Secure Mode field without actually rejecting any transactions.

4. Review your rejected collected entries periodically to identify transactions that you want RRM to allow or reject. For more information, see “Work with Collected Entries” on page 101. To view your rejected collected entries, press F11 (Toggle view) on the Work with Collected Entries screen until the “REJECTED Entries” view is displayed. For more information, see “Work with Collected Entries” on page 101.

5. For each rejected collected entry that you want to become a secured entry, use Option 3 (Promote/Secure) on the Work with Collected Entries screen to promote it to the secured environment.

6. For each exit point listed on the Work with Exit Points screen, specify *YES in the Secure Mode field. For more information, see “Work with Exit Points” on page 136.

   By continuing to review rejected collected entries periodically, you can identify additional types of transaction that you want RRM to reject, and you can build new rules accordingly.

**Limit IFS Access to Read-Only**

You should limit IFS access to read-only access by reviewing requests with objects that target the IFS, and determining an appropriate level of access for your organization.
To limit access to read-only:

1. Type 10 beside the selected entry on the Work With Collected Entries screen and press ENTER.
2. Type 2 beside the appropriate object and press ENTER.
3. Press F6 to add a remote object authority record.
4. In the User Profile field, specify a user profile, a group, or *PUBLIC.
5. In the Read Rights field, specify Y.
6. In the Secure Status field, specify Y.
7. In all of the remaining fields, specify N.
8. Press ENTER.

Restrict Access to Services that Start Automatically

You should restrict access to services such as Telnet and FTP that start automatically so that these services are available only to authorized users and do not present security exposures to unauthorized users. To restrict access to services that start automatically, create a secured entry with user groups that include all authorized users.

To restrict automatic services access:

1. Access the Work with User Groups screen.
2. Type 1 (Add Group) in the Opt field and press TAB.
3. Type :FTPCLT in the Name field and press TAB.
4. Type a description in the Description field and press ENTER.
5. Repeat Step 1 through 5 substituting :FTPSVR for the name of the group.
6. Type 5 beside :FTPCLT and press ENTER.
7. For each user who you want to authorize to use services that start automatically, type 1 (Add Member) in the Opt field, type the name of the user, and press ENTER.
8. Press F12 (Cancel) to redisplay the Work With User Groups screen, and repeat Step 3 substituting :FTPSVR for the name of the group.


10. Type :FTPCLT in the User field, type *PASS in the Action field, type Y in the Enabled Status field, and press ENTER.

11. Press ENTER.

12. Press F12 (Cancel) to redisplay the Work With Secured Entries screen.

13. Type 6 (UsrGrp) beside the secured entry created in Step 5, and press ENTER.


15. Type :FTPSVR in the Name field and press ENTER.

16. Press ENTER again when prompted.

**Maintaining RRM**

After you start using RRM, it is recommended that you implement the following maintenance procedures in the system operation procedures for your installation.

**Restart RRM Collection Monitor**

When you restart RRM (to perform an IPL, for example), you must restart the RRM Collection Monitor using one of the following methods.

**Select RRM Menu Option**

You can restart the RRM Collection Monitor by selecting the following menu options starting at the RRM Main Menu:

30 (Manage RRM) > 5 (Start/Stop RRM Collection Monitor) > *START.

For more information, see “Start/Stop RRM Collection Monitor” on page 209.
Issue Command at Command Line
You can restart the RRM Collection Monitor by issuing the following command on an i5/OS command line:

`PSRRMCMON`

Put Command in Startup Routine
You can set up your system to automatically restart the RRM Collection Monitor whenever the system is restarted by adding the following command to your startup routine:

`PSCOMMON/PSRRMCMON ACTION(*START)`

Schedule Job to Delete Collected Entries
RRM includes a function that deletes collected entries. For more information, see “Delete Collected Entries” on page 206. This function can be scheduled to execute automatically at the times you specify. It is recommended that you review your collected entries on a regular basis to determine whether each entry should be promoted to a secured entry or discarded. Based on the number of collected entries that accumulate, you should set up a schedule to automatically delete the entries after you have reviewed them. It is important to determine how often collected entries should be deleted because an excessively high number of entries can be difficult to manage and can significantly reduce available disk space.

Save and Restore Files
RRM physical files have associated trigger programs and user index objects. These files cannot be operated without their user index objects. If you perform a SAVE and RESTORE operation with RRM physical files, ensure that the associated user index objects are included with the physical files.
Online Help

RRM is provided with an online help system that provides most of the information contained in the RRM User Guide. Help information is available for each product screen and for every field on every screen.

You can access Help for this product by pressing F1 while the cursor is in the field for which you want Help. This action causes a pop-up Help window to be displayed that contains useful information about the selected field. If you press F1 while the cursor is not in a specific field, Help is displayed for the entire screen.
RRM can be operated in “Production Mode,” which is used to control remote requests on your server, or in “What If Mode,” which lets you test a new configuration before you put it into production.

Production Mode

RRM determines whether remote requests are authorized to execute on the server it controls by comparing incoming requests to secured entry rules and approving (PASS) or rejecting (FAIL) each request. This evaluation process is controlled by the Decision-making Algorithm, which coordinates a series of authority checking tasks that determine whether requests are approved or rejected.

The Decision-making Algorithm begins by extracting user, network address, and operation data from the incoming request and generating lists of each type of data. If the request specifies a user/server override or a user/object override, the override is evaluated and the indicated action (PASS/FAIL) is taken. If the request specifies a swap profile, the user profile authority is “swapped” with the authority of another profile and is examined later in the evaluation process.

From the lists of extracted data, keys to secured entry rules are built. If the keys specify a calendar, the calendar rule is evaluated, and the indicated action (PASS/FAIL) is taken. If the keys specify an object, the request is parsed for remote object authority, and the indicated action (PASS/FAIL) is taken.
Finally, if the request specifies a default action, the action (PASS/FAIL) is taken. Based on the outcome of all applicable authority checking tasks, RRM determines whether the incoming request is approved or rejected.

For more information about the following topics, see the pages indicated:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Decision-making Algorithm”</td>
<td>29</td>
</tr>
<tr>
<td>“User/Server and User/Object Overrides”</td>
<td>27</td>
</tr>
<tr>
<td>“Swap Profiles”</td>
<td>29</td>
</tr>
<tr>
<td>“Calendars”</td>
<td>28</td>
</tr>
<tr>
<td>“Remote Object Authority”</td>
<td>28</td>
</tr>
</tbody>
</table>

**What If Mode**

What If Mode is similar to Production Mode except that the changes made to rules do not affect remote requests until those changes are put into production. Using copies of secured entries, What If Mode lets you make changes to secured entry rules and test them in your environment without affecting existing secured entries or remote transaction security. Then, the What If files can be discarded or promoted to secured entries and put into production. For more information, see “What If Processing” on page 43.

**Groups**

RRM supports the use of groups for users, network addresses, and operations. Groups can contain individual data items (users, network addresses, or operations) or other groups, and those groups can contain other groups or belong to other groups. Groups can be set up for production or What If environments.
The elements of a group—whether individual data items or other groups—are called members. When the RRM Decision-making Algorithm searches a group for matching authority, it starts at the most inclusive level and continues searching for members contained in groups until no more groups containing members can be found and all members have been examined. For an example of this process, see Step 4 in “Decision-making Algorithm” on page 32.

Organizing data items (users, network addresses, and operations) by groups lets you minimize the number of secured entries that must be created and maintained to authorize remote requests. Instead of specifying a unique secured entry to authorize each remote request, you can place the data item of each request in a group that provides the desired authority. Each additional request that needs the same authority can be secured by adding it to the group. When a change must be made to a group of data items, you can change the authorities for all data items in the group by changing the authorities of the group to which the items belong. For this reason, use of groups can be an effective tool for managing changes.

You can set up or maintain production groups through the options provided on the Work With RRM Groups menu. You can set up or maintain What If groups through the options provided on the Work With What If RRM Groups menu. To distinguish between i5/OS groups and RRM groups, RRM groups begin with a colon (:) and i5/OS groups do not.

**User/Server and User/Object Overrides**

RRM supports the use of user/server overrides and user/object overrides. User/server and user/object overrides let you grant or revoke user authority to a specified server or object. These authorities exceed all other authorities. Typically, user/server and user/object overrides are used to apply a temporary and/or quick change to existing remote access authorities until similar authorities can be implemented through secured rules.

You can maintain user/server overrides through the Work With User/Server Overrides screen. You can maintain user/object overrides through the Work With User/Object Overrides screen.
To better understand how user/server overrides and user/object overrides are evaluated by the Decision-making Algorithm, see the figure in “Decision-making Algorithm” on page 29. It depicts the processing flow of remote requests through the Decision-making Algorithm from arrival until a decision is reached.

**Calendars**

RRM supports the use of production or What If calendars for defining the action to be taken when users attempt to access a server controlled by RRM during the days and times specified in the calendar record. For the days and times shown in the record, the action specified in the **Action** field on the Maintain Calendar screen determines whether the user is granted access (*PASS), denied access (*FAIL), or whether access is controlled on the basis of i5/OS object-level authorities (*OBJLIST).

In an RRM environment, calendars exist only in association with collected, secured, or What If entries, but they have rules of their own (based on day, time, and action restrictions) that determine the success or failure of each transaction received. If no existing calendar record applies to the day and time when the transaction is received, the action specified in the **Default Action** field is taken.

You can set up or maintain production or What If calendars through the Work With Calendars screen.

**Remote Object Authority**

RRM controls remote access to objects on the RRM server by checking requests for the following authorities:

**Read**

Authority to read a file (Y=yes or N=no).

**Write**

Authority to change a file (Y=yes or N=no).
Execute
Authority to execute a program or command (Y=yes or N=no).

Operate
Authority to create or delete a file (Y=yes or N=no).

SecS
Secure status. Whether the object has been secured (Y=yes or N=no).

To access an RRM object, the request must have the appropriate authority to perform the specified task. The authorities for RRM objects are recorded on the Remote Object Authority List on the RRM server, and can be managed through the Maintain Remote Object Authority screen.

Swap Profiles

RRM supports the use of swap profiles in remote requests. A swap profile is a user profile that is used to authorize a user to complete a remote request when the other elements of the transaction do not provide enough authority. When a swap profile is specified in a request, the authority of the swap profile is used instead of the authority of the user profile associated with the request. User profile authority can be swapped only if the associated exits are secured.

The swap profile function is available through the Work with Secured Entries screen.

Decision-making Algorithm

The Decision-making Algorithm controls the way RRM searches for secured entry rules to authorize remote requests. The algorithm uses multiple parsing routines and generic search capabilities to determine (“decide”) whether a transaction is rejected or approved. The following figure depicts the processing flow of the Decision-making Algorithm. Following the diagram, each part of the process is described in detail.
Remote request received

Registered exit program starts

Processing exit program extracts data
• User ID
• Network address
• Operation
• Object list

Extracted User ID list generated

Extracted network address list generated

Extracted operation list generated

Extracted object list generated

Keys generated from lists

Usr/Svr Override checked for User ID or *PUBLIC

Usr/Obj Override checked for User ID or *PUBLIC

Was a Usr/Svr override found?

Check secured entries

Check object authority

Are there more objects?

Remote Request Is Approved or Denied
1. Remote Request Received

RRM receives a remote request from an IBM-supported server. Depending on the type of function requested, the request can contain the following information:

- User ID
- Network address
- Operation (server/function/command)
- Object List (containing zero, one, or multiple objects)

2. Registered Exit Program Starts

The registered exit program identifies the processing exit program associated with the exit point and determines the format of the information it receives. The registered exit program then reads an index to find the configuration of the processing exit program. The configuration consists of the processing exit program and any registered exit programs. When the processing exit program is found, it is called by the registered exit program, and then the registered exit program ends.

3. Processing Exit Program Extracts Data

The processing exit program extracts the following data from the request:

- User ID
- Network Address
- Operation (server/function/command)
- Object List

Then, lists are generated that contain the data and any groups that also include the data. The Extracted User ID (EUID) List, Extracted Network (EN) List, and Extracted Operation (EO) List are used to search for matching secured entry rules in the order of most specific to least specific (generic).
4. Extracted User ID List Generated

The EUID List is generated from the extracted user data. The list will include the following types of information:

- User ID
- RRM user groups that include the user as a member

**Note**
RRM user group names begin with a colon (:) to distinguish them from i5/OS group profiles.

- i5/OS group profiles for users that include the user as a member
- RRM user groups that include i5/OS group profiles as a member
- *PUBLIC group

**Example**

The following example illustrates the process used by the Decision-making Algorithm to extract data from the User ID List and to resolve the EUID List.

In this example, the following user IDs were included in the User ID List when RRM was set up:

<table>
<thead>
<tr>
<th>Able</th>
<th>Jed</th>
<th>John</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mable</td>
<td>George</td>
<td>Mark</td>
</tr>
<tr>
<td>Joe</td>
<td>Mary</td>
<td>Bob</td>
</tr>
<tr>
<td>Fred</td>
<td>Shari</td>
<td>Rob</td>
</tr>
<tr>
<td>Mike</td>
<td>Barry</td>
<td></td>
</tr>
</tbody>
</table>
The following table shows the RRM user IDs that are listed in the User ID List and the RRM user groups that include the IDs as members:

<table>
<thead>
<tr>
<th>RRM User IDs</th>
<th>RRM User Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>:AP, :AR, George</td>
<td>:Acctg</td>
</tr>
<tr>
<td>Able, Mable, George</td>
<td>:AP</td>
</tr>
<tr>
<td>Fred, Jed, George</td>
<td>:AR</td>
</tr>
<tr>
<td>Mary, Shari, Barry, Bob</td>
<td>:Execs</td>
</tr>
<tr>
<td>Bob, Rob</td>
<td>:R&amp;D</td>
</tr>
<tr>
<td>Mike, John, Mark</td>
<td>:Sales</td>
</tr>
</tbody>
</table>

The following table shows the i5/OS user IDs in the User ID List and the i5/OS user groups that include the IDs as members:

<table>
<thead>
<tr>
<th>i5/OS User IDs</th>
<th>Group Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Able, Mable, Fred, Jed, Mike, John, Mark</td>
<td>JDE</td>
</tr>
<tr>
<td>Bob, Rob</td>
<td>QPGMR</td>
</tr>
<tr>
<td>Wayne, Marge</td>
<td>CONTRACTOR</td>
</tr>
</tbody>
</table>

When a remote request is received, the user ID is extracted and the Decision-making Algorithm uses the following process to resolve the EUID List:

a. The User ID List is searched to find a match for the extracted user ID. If a match is found, it is added to the EUID List.

b. The User ID List is searched for RRM user groups that include the extracted user ID as a member. Each group found is added to the EUID List.

c. For each RRM user group that was found in the previous step, the User ID List is searched for other RRM user groups that include it as a member. Each group found is added to the EUID List. This process is repeated until there are no more groups that are members of other groups.
d. The i5/OS user profile information for the extracted user ID is retrieved, and its i5/OS group and any supplemental groups are extracted. The User ID List is searched for i5/OS user groups that include the extracted user ID as a member. Each group found is added to the EUID List.

e. The i5/OS Group List and Supplemental Group List are searched for RRM user groups that include other i5/OS Groups and Supplemental Groups as members. Each group found is added to the EUID List.

f. For each RRM user group that was found in the previous step, the i5/OS Group List and Supplemental Group List are searched for other RRM user groups that include other i5/OS groups and supplemental groups as members. Each group found is added to the EUID List. This process is repeated until there are no more groups that are members of other groups.

g. The *PUBLIC entry is added to the EUID List.

The following table shows the user IDs, RRM user groups, and i5/OS user groups that were added to the EUID List during the process of resolving Able, George, Bob, and Wayne:

<table>
<thead>
<tr>
<th>User IDs</th>
<th>User IDs and Groups Added to EUID List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Able</td>
<td>Able, :AP, :Acctg, JDE, *PUBLIC</td>
</tr>
<tr>
<td>George</td>
<td>George, :AP, :AR, :Acctg, *PUBLIC</td>
</tr>
<tr>
<td>Bob</td>
<td>Bob, R&amp;D, Executives, QPGMR, *PUBLIC</td>
</tr>
<tr>
<td>Wayne</td>
<td>Wayne, CONTRACTOR, *PUBLIC</td>
</tr>
</tbody>
</table>

Note
RRM groups begin with a colon (:).
5. Extracted Network List Generated

The EN List is generated from the extracted network address data. The list will include the following types of information:

- IP and SNA addresses
- RRM network groups (which include the extracted addresses as members)
- *ALL network group

Example

The following example illustrates the process used by the Decision-making Algorithm to extract network addresses from the Network List and to resolve the EN List.

In this example, the following IP and SNA addresses were included in the Network List when RRM was set up:

- 173.16.130.5
- 173.16.130.6
- 173.16.130.7
- 173.16.130.10
- 173.16.130.11
- 173.16.130.15
- 173.16.130.16
- 173.16.*.*
- QPADEV*
The following table shows the RRM network addresses and the RRM network groups that include RRM network addresses as members. RRM groups begin with a colon (:).

<table>
<thead>
<tr>
<th>IP/SNA Addresses</th>
<th>Network Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>173.16.130.5</td>
<td>:DEV400</td>
</tr>
<tr>
<td>173.16.130.6</td>
<td></td>
</tr>
<tr>
<td>173.16.130.7</td>
<td></td>
</tr>
<tr>
<td>173.16.130.10</td>
<td>:QA400</td>
</tr>
<tr>
<td>173.16.130.11</td>
<td></td>
</tr>
<tr>
<td>173.16.130.15</td>
<td>:PCS400</td>
</tr>
<tr>
<td>173.16.130.16</td>
<td></td>
</tr>
<tr>
<td>:DEV400</td>
<td>:R&amp;D400</td>
</tr>
<tr>
<td>:QA400</td>
<td></td>
</tr>
<tr>
<td>173.16.<em>.</em></td>
<td>:PENTASAFE</td>
</tr>
<tr>
<td>QPADEV</td>
<td></td>
</tr>
<tr>
<td>PDAOS2</td>
<td>:PDA</td>
</tr>
<tr>
<td>PDAWIN3</td>
<td></td>
</tr>
<tr>
<td>PMAOS201</td>
<td>:PMA</td>
</tr>
<tr>
<td>PMAOS202</td>
<td></td>
</tr>
<tr>
<td>:PDA</td>
<td>:SNA</td>
</tr>
<tr>
<td>:PMA</td>
<td></td>
</tr>
</tbody>
</table>

When a remote request is received, the network address is extracted, and the Decision-making Algorithm uses the following process to resolve the EN List:

a. The Network List is searched to find an exact or partial match for the extracted network address. If a match is found, it is added to the EN List.

b. The Network List is searched for RRM network groups that include the extracted network address as a member. Each group found is added to the EN List.
c. For each RRM network group that was found in the previous step, the Network List is searched for other RRM network groups that include it as a member. Each group found is added to the EN List. This process is repeated until there are no more groups that are members of other groups.

d. The *ALL entry is added to the EN List.

The following table shows the network addresses and RRM network groups that were added to the EN List during the process of resolving remote requests containing the network addresses 173.16.130.5, 173.16.120.5 and 10.10.10.10:

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Network Groups Added</th>
</tr>
</thead>
<tbody>
<tr>
<td>173.16.130.5</td>
<td>173.16.130.5, 173.16.**, DEV400, :R&amp;D400, :PENTASAFE, *ALL</td>
</tr>
<tr>
<td>173.16.120.5</td>
<td>173.16.120.5, :PENTASAFE, *ALL</td>
</tr>
<tr>
<td>10.10.10.10</td>
<td>10.10.10.10, *ALL</td>
</tr>
</tbody>
</table>

6. Extracted Operation List Generated

The EO List is generated from the extracted operation data. An operation consists of server, function, and command data. The list will include the following types of information:

- Operations
- Operation groups that include the operation as a member
- *ALL Operation group

Example

The following example illustrates the process used by the Decision-making Algorithm to extract operation data from the Operation List and to resolve the EO List.
In this example, the following table shows the operations that were listed in the Operation List when RRM was set up:

<table>
<thead>
<tr>
<th>Server</th>
<th>Function</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>*ALL</td>
<td>*ALL</td>
</tr>
<tr>
<td>FTP</td>
<td>PUT</td>
<td>*ALL</td>
</tr>
<tr>
<td>FTP</td>
<td>GET</td>
<td>*ALL</td>
</tr>
<tr>
<td>FTP</td>
<td>CD</td>
<td>*ALL</td>
</tr>
<tr>
<td>FTP</td>
<td>DEL</td>
<td>*ALL</td>
</tr>
<tr>
<td>SQL</td>
<td>*ALL</td>
<td>*ALL</td>
</tr>
<tr>
<td>SQL</td>
<td>EXECIMM</td>
<td>*ALL</td>
</tr>
<tr>
<td>SQL</td>
<td>EXECIMM</td>
<td>SELECT</td>
</tr>
<tr>
<td>SQL</td>
<td>EXECIMM</td>
<td>UPDATE</td>
</tr>
<tr>
<td>SQL</td>
<td>EXECIMM</td>
<td>Insert</td>
</tr>
</tbody>
</table>

The following table shows the operations that are listed in the Operation List and the operation groups that include them as members:

<table>
<thead>
<tr>
<th>Operations</th>
<th>Operation Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP/GET/*ALL</td>
<td>:FTPREAD</td>
</tr>
<tr>
<td>FTP/CD/*ALL</td>
<td></td>
</tr>
<tr>
<td>SQL/EXECIMM/SELECT</td>
<td>:SQLREAD</td>
</tr>
<tr>
<td>FTPREAD</td>
<td></td>
</tr>
<tr>
<td>SQLREAD</td>
<td>:READONLY</td>
</tr>
</tbody>
</table>
When a remote request is received, the operation is extracted and the Decision-making Algorithm uses the following process to resolve the EO List:

a. The Operation List is searched to find an exact or partial match for the extracted operation. If a match is found, it is added to the EO List.

b. The Operation List is searched for RRM operation groups that include the extracted operation as a member. Each group found is added to the EO List.

c. For each RRM operation group that was found in the previous step, the Operation List is searched for other RRM operation groups that include it as a member. Each group found is added to the EO List. This process is repeated until there are no more groups that are members of other groups.

d. If the *ALL command was not included in one of the operations above, *ALL is substituted for the command, and Step a - Step c are repeated.

e. If the *ALL function was not included in one of the operations above, *ALL is substituted for the function, and Step a - Step c are repeated.

f. The *ALL operation is added to the EO List.
The following table shows the operations that were added to the EO List during the process of resolving the operations FTP/CD/*ALL, SQL/EXECIMM/UPDATE, and SQL/EXECIMM/SELECT:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Extracted Operation List</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP/CD/*ALL</td>
<td>FTP/CD/*ALL</td>
</tr>
<tr>
<td></td>
<td>:FTPREAD</td>
</tr>
<tr>
<td></td>
<td>:READONLY</td>
</tr>
<tr>
<td></td>
<td>FTP/*ALL/*ALL</td>
</tr>
<tr>
<td></td>
<td>*ALL</td>
</tr>
<tr>
<td>SQL/EXECIMM/UPDATE</td>
<td>SQL/EXECIMM/UPDATE</td>
</tr>
<tr>
<td></td>
<td>SQL/EXECIMM/*ALL</td>
</tr>
<tr>
<td></td>
<td>SQL/*ALL/*ALL</td>
</tr>
<tr>
<td></td>
<td>*ALL</td>
</tr>
<tr>
<td>SQL/EXECIMM/SELECT</td>
<td>SQL/EXECIMM/SELECT</td>
</tr>
<tr>
<td></td>
<td>:SQLREAD</td>
</tr>
<tr>
<td></td>
<td>:READONLY</td>
</tr>
<tr>
<td></td>
<td>SQL/EXECIMM/*ALL</td>
</tr>
<tr>
<td></td>
<td>SQL/*ALL/*ALL</td>
</tr>
<tr>
<td></td>
<td>*ALL</td>
</tr>
</tbody>
</table>

7. Extracted Object List Generated. The Extracted Object List is generated from the extracted object data.

8. Keys Generated from Extracted Lists. The keys to the secured entry rule are built from the information in the following lists:

- Extracted User ID (EUID) List
- Extracted Network (EN) List
- Extracted Operation (EO) List
- Extracted Object List
When extracted lists are generated, the secured rules are searched for entries that match one of the user/network/operation combinations from these lists. The search proceeds from the most specific combination to the least specific combination.

9. User/Server Override checked for User ID or *PUBLIC. If a user/server override is found, it is checked for a user ID or *PUBLIC authority. If the action is *FAIL, the request is rejected. If the action is *PASS or if an override is not found, the request is checked for an object/server override.

10. Object/Server Override checked for User ID or *PUBLIC. If an object/server override is found, it is checked for a user ID or *PUBLIC authority. If the action is *FAIL, the request is rejected. If the action is *PASS, the request bypasses all other checking until a final *PASS or *FAIL decision is reached.

11. Was a User/Server Override Found? The Decision-making Algorithm checks to see if a user/server override was found in Step 9. If a user/server override was found, the request bypasses checking for secured entry rules. If a user/server override was not found, the Decision-making Algorithm searches for a matching secured entry rule.

12. Secured Entry Rules Searched for Most Specific Match. Using the keys generated in Step 8, the Secured Entry Rules are searched from the most specific rule to the most generic rule. If a rule contains values for user, network address, and operation that match those of a generated key, that match is considered an “exact match,” and the matching rule is considered the most specific rule available. A secured rule containing *PUBLIC for the user, *ALL for the network address, and *ALL for the operation would be the most generic rule available.

Secured entry rules are searched in the order of the lowest numbered key (most specific) to the highest numbered key (most generic). When a secured entry is found, other secured entry rules at that level are evaluated to determine if the remote request is approved or rejected.
If the remote request has an object associated with it, secured rules with associated objects are evaluated at the same level. If none of the objects on the secured rules matches, the object from the remote request followed by secured rules without associated objects are evaluated. If an object is associated with one or more secured entries that match, only those rules with matching objects are evaluated, and rules without associated objects are ignored. If the remote request lists multiple objects, only the first object is used. If the remote request does not specify an object, only secured entries without objects are evaluated. All matching rules are evaluated until one of the following actions occurs:

- A key with the same process order code resolves to *FAIL, causing the transaction to be rejected.
- A key with a higher process order code is read.

If all rules with the same process order code have been read and no rule resolves to *FAIL, the transaction is approved. If no matching rule is found, the transaction resolves to *FAIL.

13. Calendar Rule Is Processed If a calendar rule is found as the action of the matching rule, the calendar is evaluated using the current day of the week and time. A calendar indicates whether an action can be performed and specifies the allowed dates and times to perform the action. If a calendar name is found that allows the request based on the date and time specified, its action is evaluated. The three allowed actions are *PASS, *FAIL, and *OBJLIST.

If the requested time period is not found in the calendar, the default action for the calendar is used.

14. Check Object Authority. Remote object authority is checked for any object found in Step 12. If the authority of the object fails, the request bypasses all other checking until a final *PASS or *FAIL decision is reached. If the authority of the object passes, the Decision-making Algorithm checks to see if there are more objects.

15. Are There More Objects? If more objects are found, the request is sent to Step 10 to be checked for the appropriate authorities. If no more objects are found, the request is submitted for a final *PASS or *FAIL decision.

16. Remote Request is Approved or Denied. Depending on the outcome of the decision-making process, the remote request is approved (*PASS) or denied (*FAIL).
What If Processing

Three sets of files are used to perform What If processing:

**Secured Entry files**
Files that specify the authorities required to access the RRM server. Incoming requests are compared to secured entry files to determine whether the requests have the authorities required to access the RRM server.

**What If files**
Copies of secured entry files that are modified and used to test the effects of a new RRM configuration before it is put into production. For more information, see “What If Processing” on page 43.

**Backup files**
Copies of secured entry files that are kept in case you want to use them to restore the previous RRM configuration.

As shown in the following figure, the process of modifying secured entries involves two primary phases.

---

**Part 1: Copy Phase**

**Secured Entry Files**

↓

**What If Files**

---

**Part 2: Promote Phase**

**Secured Entry Files**

→

**What If Files**

→

**Backup Files**
In the Copy Phase, secured entry files are copied and become “What If” files. These copies of secured entry files (What If files) can be modified and tested without changing the existing configuration to determine the effects of a new configuration. At this point, the What If files can be kept and promoted to secured entry files, or they can be discarded so that the previous secured entry files can continue to be used.

In the Promote Phase, the What If files configured in the Copy Phase are promoted to secured entry files, and the existing secured entry files become backup files. The backup files can be restored to secured entry files at any time if you have not promoted a new set of What If files and overwritten the previous backup files.
What If processing mode is a separate yet interrelated component of the RRM remote request processing facility. The following figure shows the flow of What If processing mode in relation to production processing mode.
What If processing operates by duplicating existing secured entries (which then become What If entries) to allow changes to be made and tested without affecting existing secured entries or remote transaction security. When all changes have been tested, the secured entries can be kept, or they can be replaced with the tested What If entries to put the new configuration into production. What If processing also makes a backup copy of the existing secured entries so that those entries, if desired, can be restored. To prevent simultaneous update of secured entries, only one administrator at a time should check out secured entries for What If processing. Changes to What If entries have no effect on the security of remote access.

Transactions are selected by using the What If Playback function, which provides selection criteria to specify the time of day and network address the transactions will use for testing. For more information, see “Playback What If Transaction Database” on page 157.

What If processing uses copies of the following types of files:

- Exit point configuration
- Secured entries
- Groups
- Network addresses
- Calendars
- Remote Object Authority List
- User exceptions

When the What If process is complete, the administrator can promote the What If files to secured entry files. Promotion can occur while remote security is active and without affecting the processing of remote transactions.

The results of a new configuration can be evaluated by generating What If reports and reviewing the return codes. For more information, see “What If Reports” on page 263.

If desired, the transaction set and new return code can be saved under new serial numbers for a new transaction benchmark. If the selected transactions give undesirable results, changes can be made to What If entries and the transactions can be reprocessed until the desired results are achieved.
This chapter describes the options of Remote Request Management (RRM) that can be performed through the user interface.
RRM Main Menu

The RRM Main Menu provides access to the major functions of the product. Related functions are provided on child screens.

```
PS3            PentaSafe Security Technologies,Inc ANYUSER   Date:  8/16/08
Remote Request Management QPADEV000C Time: 16:52:29

Select one of the following:
1  Work With Secured Entries           10  Work With What If Analysis
2  Work With Collected Entries
3  Work With RRM Groups
4  Work With RRM Object Authorities
5  Work With Calendars
6  Work With User/Server Overrides
7  Work With User/Object Overrides
8  Work With Exit Points
9  Work With RRM Defaults

Enter Option or Function/Type ==>
F1=Help         F3=Exit         F6=Messages     F9=Window       F10=Cmd Line
F12=Previous    F13=Attention   F14=Batch Jobs  F18=Reports
```

This menu includes the following header, menu option, and function key information.

**Header Information**

`function name`

The code for this function, based on the option selected on the preceding menu. In this, case “PS3” indicates that the RRM Main Menu was displayed by selecting Option 3 on the preceding menu, the PSSecure Main Menu.

`panel name`

The name of the panel displayed.

`user`

The user who has accessed the menu.
panel code
The code name used for this panel.

Date
The date when the screen was accessed in the user’s job date format.

Time
The time when the screen was accessed in the format hh:mm:ss.

Menu Option Information

1 Work with Secured Entries
Displays the Work with Secured Entries screen, which is used to maintain Secured Entries. For more information, see “Work with Secured Entries” on page 53.

2 Work with Collected Entries
Displays the Work with Collected Entries screen, which is used to maintain Collected Entries. For more information, see “Work with Collected Entries” on page 101.

3 Work with RRM Groups
Displays the Work with RRM Groups menu, which is used to maintain RRM groups. For more information, see “Work with RRM Groups” on page 118.

4 Work with RRM Object Authorities
Displays the Work with RRM Object Authorities screen, which is used to maintain object authorities. For more information, see “Work with RRM Object Authorities” on page 120.

5 Work with Calendars
Displays the Work with Calendars screen, which is used to maintain calendar file records. For more information, see “Work with Calendars” on page 127.

6 Work with User/Server Overrides
Displays the Work with User/Server Overrides screen, which is used to maintain user/server overrides. For more information, see “Work with User/Server Overrides” on page 130.
7 Work with User/Object Overrides
Displays the Work with User/Object Overrides screen, which is used to maintain user/server overrides. For more information, see “Work with User/Object Overrides” on page 133.

8 Work with Exit Points
Displays the Work with Exit Points screen, which is used to maintain RRM exit points. For more information, see “Work with Exit Points” on page 136.

9 Work with RRM Defaults
Displays the Work with RRM Defaults screen, which is used to maintain RRM default values. For more information, see “Work with RRM Defaults” on page 141.

10 Work with What If Analysis
Displays the Work with What If Analysis menu, which is used to maintain What If Entries and to test the results of a new configuration before putting it into production. For more information, see “Work with What If Analysis” on page 148.

20 Work with RRM Reports
Displays the Work with RRM reports menus, which provides options for generating RRM reports. For more information, see “Work with RRM Reports” on page 165.

30 Manage RRM
Displays the Manage RRM menu, which provides options for managing RRM. For more information, see “Manage RRM” on page 200.

Function Key Information
For more information about the function keys on this screen, see “Function Key Summary” on page 51.
Function Key Summary

The following table describes the function key available on RRM menus and screens.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RRM Menus</td>
<td>RRM Menus</td>
</tr>
<tr>
<td>F1=Help</td>
<td>Displays Help for the field where the cursor is positioned. If the cursor is not positioned in a specific field, Help is displayed for the entire screen.</td>
</tr>
<tr>
<td>F3=Exit</td>
<td>Exits the current application or display.</td>
</tr>
<tr>
<td>F6=Messages</td>
<td>Displays the Display Message screen where all messages that were sent to the user are shown.</td>
</tr>
<tr>
<td>F9=Window</td>
<td>Opens an i5/OS command window, which can be used for performing additional RRM functions.</td>
</tr>
<tr>
<td>F10=Cmd Line</td>
<td>Displays a command line, which can be used for performing additional i5/OS functions.</td>
</tr>
<tr>
<td>F12=Previous</td>
<td>Displays the screen that was previously displayed.</td>
</tr>
<tr>
<td>F13=Attention</td>
<td>Displays the Group Jobs Screen where you can work with group jobs.</td>
</tr>
<tr>
<td>F14=Batch Jobs</td>
<td>Displays the Work with Submitted Jobs screen where the name and status of all jobs submitted by the user are displayed.</td>
</tr>
<tr>
<td>F18=Reports</td>
<td>Displays the Work with All Spooled Files screen where all reports generated by the user are displayed.</td>
</tr>
<tr>
<td>F24=More Keys</td>
<td>Displays additional function keys that do not appear because of space limitations.</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>RRM Screens</strong></td>
<td></td>
</tr>
<tr>
<td>F1=Help</td>
<td>Displays Help for the field where the cursor is positioned. If the cursor is not positioned in a specific field, Help is displayed for the entire screen.</td>
</tr>
<tr>
<td>F3=Exit</td>
<td>Exits the current application or display.</td>
</tr>
<tr>
<td>F4=Prompt</td>
<td>Displays a list of valid values for the current field.</td>
</tr>
<tr>
<td>F5=Refresh</td>
<td>Updates and displays the data for the function being used.</td>
</tr>
<tr>
<td>F6=Add</td>
<td>Lets you add a record to the current file.</td>
</tr>
<tr>
<td>F9=All Parameters</td>
<td>Displays all available parameters for the current command.</td>
</tr>
<tr>
<td>F11=View2</td>
<td>Allows the user to shift views on supported screens.</td>
</tr>
<tr>
<td>F12=Cancel</td>
<td>Cancels the operation and redisplays the previous screen.</td>
</tr>
<tr>
<td>F13=Repeat</td>
<td>Repeats the selection option you typed in the entry fields below your current position in the Op column.</td>
</tr>
<tr>
<td>F14=Sort</td>
<td>Lets you control the sequence of displayed records. To use this function, place the cursor in the column you want to sort and press F14.</td>
</tr>
<tr>
<td>F17=Refresh Defaults</td>
<td>Restores the previously specified default values for RRM.</td>
</tr>
<tr>
<td>F23=More Options</td>
<td>Displays additional options. Because of space limitations, all available options cannot be displayed at the same time.</td>
</tr>
<tr>
<td>F24=More Keys</td>
<td>Displays additional function keys. Because of space limitations, all available function keys cannot be displayed at the same time.</td>
</tr>
</tbody>
</table>
Work with Secured Entries

Depending on the option selected, the Work With Secured Entries screen lets you maintain Secured Entries or What If Entries. Use this screen to maintain RRM Secured Entries. For more information, see “Production Mode” on page 25 and “What If Processing” on page 43.

The Work With Secured Entries screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

**Opt 1 (Secured Entries)**

**Opt 10 (What If Analysis) > 1 (What If Secured Entries)**

The presence of a right angle bracket (>) on the right side of an entry indicates that the entry is associated with an object.

<table>
<thead>
<tr>
<th>Op</th>
<th>S</th>
<th>User</th>
<th>Network</th>
<th>Operation</th>
<th>Action</th>
<th>Swap Prf</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>*PUBLIC</td>
<td>*ALL</td>
<td>*ALL</td>
<td>*PASS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>*PUBLIC</td>
<td>*ALL</td>
<td>*ALL</td>
<td>*FAIL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>*PUBLIC</td>
<td>172.16.37.5</td>
<td>*ALL</td>
<td>*FAIL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>:USRGRP01</td>
<td>172.16.37.5</td>
<td>CENTRAL_CLACT</td>
<td>*FAIL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>:USRGRP02</td>
<td>172.16.37.5</td>
<td>CENTRAL_CLACT</td>
<td>*FAIL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>:USRGRP04</td>
<td>172.16.37.5</td>
<td>CENTRAL_CLACT</td>
<td>*FAIL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>:USRGRP07</td>
<td>172.16.37.5</td>
<td>CENTRAL_CLACT</td>
<td>*FAIL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>:USRGRP14</td>
<td>172.16.37.5</td>
<td>CENTRAL_CLACT</td>
<td>*FAIL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This screen includes the following header, selection option, Secured Entry, and function key information.
Header Information

screen format
The name of the format used for this panel.

server
The name of the server being used.

panel name
The name of the panel displayed.

time
The current time in the format hh:mm:ss.

date
The current date in the user’s job date format.

mode
The current mode being used for this RRM function. In this example, the mode is “Review”.

Selection Option Information

2=Edit
Lets you edit the selected Secured Entry.

3=Copy
Lets you copy the selected Secured Entry.

4=Delete
Lets you delete the selected Secured Entry.

5=Display
Shows the data for the selected Secured Entry.

6=UsrGrp
If a user group is present, the Work with User Groups screen is displayed, which lets you manage members of user groups.
7=NetGrp
If a network group is present, the Work with Network Groups screen is displayed, which lets you manage members of network groups.

8=OprGrp
If an operation group is present, the Work with Operation Groups screen is displayed, which lets you manage members of operation groups.

9=Cal
If a calendar is associated with the entry, the Maintain Calendar screen is displayed, which lets you manage calendar files.

**Secured Entry Information**

**Position To**
Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the **Position To** field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

**Op**
To issue a selection option, type the number of the option and press Enter.

**S (Status) Subset**
Using the input field above “S,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

**S (Status)**
Indicates the Enabled Status of the selected entry (Y=enabled, N=disabled). If an entry is disabled (N), it will not be examined by the Decision-making Algorithm. By specifying N in this field, you can temporarily disable the Secured entry so that you can re-enabled it later, instead of having to delete and re-create the entry.
User Subset
Using the input field above “User,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

User
The name of the user who submitted the transaction.

Network Subset
Using the input field above “Network,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Network
The name of the network address where the transaction originated.

Operation Subset
Using the input field above “Operation,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Operation
The operation associated with the transaction.

Action Subset
Using the input field above “Action,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Action
The action associated with the transaction.

The following values are valid:

- **PASS**: The transaction is allowed.
- **FAIL**: The transaction is rejected.
- **OBJLIST**: The Remote Object Authority tables are searched to determine if the user is authorized to access the object.
- **calendar**: The name of the calendar associated with the transaction.

Swap Prof Subset
Using the input field above “Swap Prof,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.
Swap Prof
The profile used to execute the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming user.

Object Path
The path for objects associated with the Secured Entry. You can specify generic entries in the path. If this field has a value of *NONE, the specified operation, user, or network can access any file on the system for the operation.

Function Key Information
F11=View2
Displays additional information that could not be displayed because of space limitations.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Using Subset Fields
Subset fields are identified by a line above a column heading. These fields let you select a subset of entries containing information that matches the value specified. Information is selected by typing a subset value in this field that matches other values in the column or by typing a value that includes matching characters and the special characters asterisk (*), underscore (_), or both, and then pressing Enter.

An asterisk represents zero, one, or multiple characters at the beginning or end of a value. An underscore represents one character only, and can be placed anywhere within a value.

When searching for values that have a leading asterisk, you must include a leading asterisk in the search criteria.

You can also select a subset of entries by specifying subset values in multiple columns at the same time. The entries that are displayed are determined by the information they contain that matches the subset values specified.
Examples

The following table shows examples of subset values used to select entries with matching information based on the given user data:

<table>
<thead>
<tr>
<th>User Data</th>
<th>Subset Value</th>
<th>Matching Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>*PUBLIC</td>
<td>PUB*</td>
<td>PUB</td>
</tr>
<tr>
<td>ARP</td>
<td></td>
<td>PUBBY</td>
</tr>
<tr>
<td>CLP</td>
<td><em>PUB</em></td>
<td>*PUBLIC</td>
</tr>
<tr>
<td>PMB</td>
<td></td>
<td>PUB</td>
</tr>
<tr>
<td>PUB</td>
<td></td>
<td>PUBBY</td>
</tr>
<tr>
<td>PUBBY</td>
<td>__P*</td>
<td>ARP</td>
</tr>
<tr>
<td>QTCP</td>
<td></td>
<td>CLP</td>
</tr>
</tbody>
</table>

Work with User Groups

Depending on the option selected, the Work with User Groups screen lets you maintain Secured or What If User Groups.
Using user groups to organize Secured Entries lets you minimize the number of Secured Entries that must be created and maintained to authorize remote requests. Instead of specifying a unique Secured Entry to authorize each remote request, you can place the user of each request in a user group that provides the desired user authority. Each additional request that needs the same user authority can be secured by adding it to the group. When a change must be made to a group of users, you can change the authorities for all users in the group by changing the authorities of the group to which the users belong.

The Work with User Groups screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 1 (Work With Secured Entries)</th>
<th>&gt; 6 (UsrGrp)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 3 (Work With RRM Groups)</td>
<td>&gt; 1 (Work With User Groups)</td>
</tr>
<tr>
<td>Opt 10 (Work With What If Analysis)</td>
<td>&gt; 3 (Work With What If RRM Groups)</td>
</tr>
</tbody>
</table>

NW0067T1                  Work with User Groups           10:29:26   7/18/2008

Member Hierarchy : /*PUBLIC

Type options, press Enter.                          Position To: 1=Add to Group  4=Remove from Group  5=Display Groups  10=Work w/ Obj Au

<table>
<thead>
<tr>
<th>Opt</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CONTAINS</td>
<td>contains all groups</td>
</tr>
<tr>
<td></td>
<td>CONTAINSA</td>
<td>contains a</td>
</tr>
<tr>
<td></td>
<td>CONTAINSB</td>
<td>contains b</td>
</tr>
<tr>
<td></td>
<td>CONTAINSC</td>
<td>contains c</td>
</tr>
<tr>
<td></td>
<td>CONTAINSD</td>
<td>contains d</td>
</tr>
<tr>
<td></td>
<td>CONTAINSE</td>
<td>contains e</td>
</tr>
<tr>
<td></td>
<td>CONTAINSF</td>
<td>contains f</td>
</tr>
<tr>
<td></td>
<td>CONTAINSG</td>
<td>contains g</td>
</tr>
<tr>
<td></td>
<td>CONTAINSH</td>
<td>contains h</td>
</tr>
<tr>
<td></td>
<td>CONTAINSI</td>
<td>contains i</td>
</tr>
<tr>
<td></td>
<td>CONTAINSJ</td>
<td>contains j</td>
</tr>
<tr>
<td></td>
<td>CONTAINSK</td>
<td>contains k</td>
</tr>
</tbody>
</table>

More...

F1=Help       F3=Exit       F4=Prompt      F5=Refresh      F12=Cancel
F13=Repeat    F14=Sort      F17=Top        F18=Bottom

Chapter 4 • Product Options   59
This screen includes the following header, selection option, group/member, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

**Selection Option Information**

1=Add to Group
   Lets you add a user to a user group.

4=Remove from Group
   Lets you remove a user from a user group.

5=Display Groups
   Displays the groups contained in the selected user group.

10=Work w/ Obj Au
   Displays the Remote Object Authority by User screen, which lets you work with Remote Object Authority members of the selected User Group.
Group/Member Information

Group Hierarchy
The hierarchy of groups containing other groups that includes the selected group.

Position To
Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

Opt
To issue a selection option, type the number of the option and press Enter.

Name Subset
Using the input field above “Name,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Name
The name of the user group.

Description Subset
Using the input field above “Description,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Description
A description of the group.

Add Row
This field above the entries lets you add User Groups.
**Function Key Information**

**F17=Top**
Redisplays the list being sorted so that the first record is shown at the top of the list.

**F18=Bottom**
Redisplays the list being sorted so that the last record is shown at the top of the list.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

**Work with User Group Members**

Depending on the option selected, the Work with User Group Members screen lets you maintain Secured or What If members of User Groups.
The Work with User Group Members screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 1 (Secured Entries)</th>
<th>&gt; 6 (UsrGrp)</th>
<th>&gt; 5 (Work w/ Group Mbrs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 3 (RRM Groups)</td>
<td>&gt; 1 (User Groups)</td>
<td>&gt; 5 (Work w/ Group Mbrs)</td>
</tr>
<tr>
<td>Opt 10 What If Analysis</td>
<td>&gt; 3 (What If RRM Groups)</td>
<td>&gt; 1 (What If User Groups)</td>
</tr>
</tbody>
</table>

NW0065T1              Work with User Group Members        10:02:32   3/27/2008
Group Hierarchy . : /:GROUP1
Type options, press Enter.                          Position To: 1=Add Member 4=Remove Member 5=Work w/ Group Mbrs 10=Work w/ Obj Aut
Opt  Name       Description

F1=Help        F3=Exit        F4=Prompt        F5=Refresh        F12=Cancel
F13=Repeat     F14=Sort       F17=Top          F18=Bottom

No records found

This screen includes the following header, selection option, member, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

1=Add Member
   Lets you add a new User Group member.

3=Copy Member
   Lets you create a copy of the selected User Group member using a different name.

4=Remove Member
   Lets you delete the selected User Group member.

5=Work w/ Members
   If the selected member is a group, the Work With User Groups screen is displayed. This screen lets you work with members of the selected User Group.

10=Work w/ Obj Aut
   Displays the Remote Object Authority by User screen, which lets you work with Remote Object Authority members of the selected User Group.

Member Information

Group Hierarchy
   The hierarchy of groups that contains the selected member.

Position To
   Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

   Only sortable columns with an underlined field above the column heading can be positioned using this function.

Opt
   To issue a selection option, type the number of the option and press ENTER.
Name Subset
Using the input field above “Name,” you can select a subset of the list below.
For more information, see “Using Subset Fields” on page 57.

Name
The name of the User Group member. All RRM groups begin with a colon (:).

Description Subset
Using the input field above “Description,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Description
A description of the User Group member.

Add Row
This field above the entries lets you add User Group members.

Function Key Information

F4=Prompt
Displays the Select Screen, which list all valid Users and User Groups that you can select.

F17=Top
Redisplays the list being sorted so that the first record is shown at the top of the list.

F18=Bottom
Redisplays the list being sorted so that the last record is shown at the top of the list.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.
Select Group Value

If you press F4 (Prompt) on one of the Work with Group Members screens while the cursor is in the Name field, the Select Screen is displayed. The Select Screen lets you select Secured or What If User, Network, or Operation Groups and Group Members.

This screen includes the following header, selection option, group/member, and function key information.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type options, press Enter.</td>
<td>Position To: ________</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1=Select</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opt</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>:GROUP1</td>
<td>Group 1</td>
</tr>
<tr>
<td></td>
<td>*PUBLIC</td>
<td>*Public</td>
</tr>
</tbody>
</table>

F1=Help  F3=Exit  F5=Refresh  F7=Reload  F12=Cancel
F13=Repeat  F14=Sort  F17=Top  F18=Bottom

Header Information

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

Selection Option Information

1=Select

Lets you select groups and group members.
Group/Member Information

Position To
Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

Opt
To issue a selection option, type the number of the option and press ENTER.

Name Subset
Using the input field above “Name,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Name
The name of the member or group member. All RRM groups begin with a colon (:).

Description Subset
Using the input field above “Description,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Description
A description of the member or group member.

Function Key Information

F17=Top
Redisplays the list being sorted so that the first record is shown at the top of the list.

F18=Bottom
Redisplays the list being sorted so that the last record is shown at the top of the list.
For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work with Network Groups

Depending on the option selected, the Work with Network Groups screen lets you maintain Secured or What If Network Address Groups.

Using network groups to organize Secured Entries lets you minimize the number of Secured Entries that must be created and maintained to authorize remote requests. Instead of specifying a unique Secured Entry to authorize each remote request, you can place the network address of each request in a network address group that provides the desired authority. Each additional request that needs the same network address authority can be secured by adding it to the group. When a change must be made to a group of network addresses, you can change the authorities for all addresses in the group by changing the authorities of the group to which the addresses belong.
The Work with Network Groups screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 1 (Work With Secured Entries)</th>
<th>&gt; 7 (NetGrp)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 3 (Work With RRM Groups)</td>
<td>&gt; 2 (Work With Network Groups)</td>
</tr>
<tr>
<td>Opt 10 (Work With What If Analysis)</td>
<td>&gt; 3 (Work With What If RRM Groups)</td>
</tr>
</tbody>
</table>

This screen includes the following header, selection option, group/member, and function key information.

### Header Information

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

1=Add Group
   Lets you add a Network Address Group.

2=Edit Group
   Lets you edit a Network Address Group.

3=Copy Group
   Lets you copy a Network Address Group.

4=Delete
   Lets you delete a Network Address Group.

5=Work w/ Members
   Displays the Work With Network Group Members screen, which lets you work
   the members contained in the selected Network Group.

Group/Member Information

Position To
   Locates the desired record and positions it at the top of the column being
   sorted. To locate a record, place the cursor in the field above the column to be
   sorted, and type the name or name pattern of the record in the Position To
   field. Then press ENTER. The record is displayed at the top of the column, and
   the other records are listed below in ascending order.

   Only sortable columns with an underlined field above the column heading can
   be positioned using this function.

Opt
   To issue a selection option, type the number of the option and press ENTER.

Name Subset
   Using the input field above “Name,” you can select a subset of the list below.
   For more information, see “Using Subset Fields” on page 57.

Name
   The name of the network address group. All RRM groups begin with a
   colon (:).
Description Subset
Using the input field above “Description,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Description
A description of the network address group.

Add Row
This field above the entries lets you add Network Groups.

Function Key Information

F17=Top
Redisplays the list being sorted so that the first record is shown at the top of the list.

F18=Bottom
Redisplays the list being sorted so that the last record is shown at the top of the list.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work with Network Group Members

Depending on the option selected, the Work with Network Group Members screen lets you maintain Secured or What If members of Network Groups.
The Work with Operation Group Members screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 1 (Secured Entries)</th>
<th>&gt; 7 (NetGrp)</th>
<th>&gt; 5 (Work w/ Members)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 3 (RRM Groups)</td>
<td>&gt; 2 (Network Groups)</td>
<td>&gt; 5 (Work w/ Members)</td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 3 (What If RRM Groups)</td>
<td>&gt; 2 (What If Network Groups)</td>
</tr>
</tbody>
</table>

| NW0064T1 | Work with Network Group Members | 14:37:54 | 3/27/2008 |

Group Hierarchy : /:NET3

Type options, press Enter. Position To: 
1=Add Member  4=Remove Member  5=Work w/ Members

<table>
<thead>
<tr>
<th>Opt</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>:NET4</td>
<td>network4</td>
</tr>
<tr>
<td></td>
<td>:NET5</td>
<td>network5</td>
</tr>
</tbody>
</table>

F1=Help         F3=Exit         F4=Prompt     F5=Refresh      F12=Cancel
F13=Repeat      F14=Sort        F17=Top       F18=Bottom

This screen includes the following header, selection option, member, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

1=Add Member
   Lets you add a new Network Address or Network Address Group.

4=Remove Member
   Lets you delete the selected Network Address or Network Address Group.

5=Work w/ Members
   If the selected member is a group, the members of the selected group are displayed.

Member Information

Group Hierarchy
   The hierarchy of groups that contains the selected member.

Position To
   Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

Opt
   To issue a selection option, type the number of the option and press Enter.

Name Subset
   Using the input field above “Name,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Name
   The name of the Network Group member. All RRM groups begin with a colon (:).
Description Subset
Using the input field above “Description,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Description
A description of the Network Group member.

Add Row
This field above the entries lets you add Network Group members.

Function Key Information

F4=Prompt
Displays the Select Screen, which list all valid Network Addresses and Network Address Groups that you can select.

F17=Top
Redisplays the list being sorted so that the first record is shown at the top of the list.

F18=Bottom
Redisplays the list being sorted so that the last record is shown at the top of the list.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work with Operation Groups

Depending on the option selected, the Work with Operation Groups screen lets you maintain Secured or What If Operation Groups.
Using operation groups to organize Secured Entries lets you minimize the number of Secured Entries that must be created and maintained to authorize remote requests. Instead of specifying a unique Secured Entry to authorize each remote request, you can place the operation of each request in an operation group that provides the desired operation authority. Each additional request that needs the same operation authority can be Secured by adding it to the group. When a change must be made to a group of operations, you can change the authorities for all operations in the group by changing the authorities of the group to which the operations belong.

The Work with Operation Groups screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

| Opt 1 (Work With Secured Entries) | > 8 (OprGrp) |
| Opt 3 (Work With RRM Groups) | > 3 (Work With Operation Groups) |
| Opt 10 (Work With What If Analysis) | > 3 Work With What If RRM Groups) | > 3 (What If Operation Groups) |

```
NW0067T1                Work with Operation Groups        13:49:47   7/18/2008
Member Hierarchy : /CENTRAL_*ALL_*ALL
Type options, press Enter.                          Position To:
   1=Add to Group  4=Remove from Group  5=Display Groups
Opt   Name       Description
   ___          ___
   1 :CHANGE    Change
   1 :CHANGE1   Change
   1 :CMDCALL   Commands & Calls
   1 :CRTOBJ    Create Objects
   1 :DLTOBJ    Delete Objects
   1 :FTP       FTP Client & Server
   1 :FTPSERVER FTP Server
   1 :READONLY  Read Only
   1 :SIGNON    Signon
   1 :SQL       SQL Servers
   1 :SQLCOPY   SQL Servers

F1=Help         F3=Exit         F4=Prompt     F5=Refresh      F12=Cancel
F13=Repeat      F14=Sort       F17=Top       F18=Bottom
```
This screen includes the following header, selection option, member, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

**Selection Option Information**

1=Add to Group
   Lets you add an Operation to the selected Operation Group.

4=Remove from Group
   Lets you remove an Operation from the selected Operation Group.

5=Display Groups
   Displays the Work With Operation Group Members screen, which lets you work with members of the selected Operation Group.

**Group Information**

**Position To**

Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the **Position To** field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

**Opt**

To issue a selection option, type the number of the option and press ENTER.
Name Subset
Using the input field above “Name,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Name
The name of the operation group. All RRM groups begin with a colon (:).

Description Subset
Using the input field above “Description,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Description
A description of the operation group.

Add Row
This field above the entries lets you add Operation Groups.

Function Key Information

F17=Top
Redisplays the list being sorted so that the first record is shown at the top of the list.

F18=Bottom
Redisplays the list being sorted so that the last record is shown at the top of the list.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work with Operation Group Members
Depending on the option selected, the Work with Operation Group Members screen lets you maintain Secured or What If members of Operation Groups.
The Work with Operation Group Members screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 1 (Secured Entries)</th>
<th>&gt; 8 (OprGrp)</th>
<th>&gt; 5 (Work w/ Members)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 3 (RRM Groups)</td>
<td>&gt; 3 (Operation Groups)</td>
<td>&gt; 5 (Work w/ Members)</td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 3 (What If RRM Groups)</td>
<td>&gt; 3 (What If Operation Groups)</td>
</tr>
</tbody>
</table>

This screen includes the following header, selection option, member, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

1=Add Member
Let you add a new Operation Group member.

3=Copy Member
Let you create a copy of the selected Operation Group member using a different name.

4=Remove Member
Let you delete the selected Operation Group member.

5=Work w/ Members
If the selected member is a group, the Work With Operation Groups screen is displayed. This screen lets you work with members of the selected Operation Group.

Member Information

Group Hierarchy
The hierarchy of groups that contains the selected member.

Position To
Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

Opt
To issue a selection option, type the number of the option and press ENTER.

Name Subset
Using the input field above “Name,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.
Name
The name of the Operation Group member. All RRM groups begin with a colon (:).

Description Subset
Using the input field above “Description,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Description
A description of the Operation Group member.

Add Row
This field above the entries lets you add Operation Group members.

Function Key Information

F4=Prompt
Displays the Select Screen, which list all valid Network Addresses and Network Address Groups that you can select.

F17=Top
Redisplays the list being sorted so that the first record is shown at the top of the list.

F18=Bottom
Redisplays the list being sorted so that the last record is shown at the top of the list.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work with Users

Depending on the option selected, the Work with Users screen lets you maintain Secured or What If user groups.
Using user groups to organize Secured Entries lets you minimize the number of Secured Entries that must be created and maintained to authorize remote requests. Instead of specifying a unique Secured Entry to authorize each remote request, you can place the user of each request in a user group that provides the desired user authority. Each additional request that needs the same user authority can be secured by adding it to the group. When a change must be made to a group of users, you can change the authorities for all users in the group by changing the authorities of the group to which the users belong.

The Work with Users screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 1 (Work With Secured Entries)</th>
<th>&gt; 6 (UsrGrp)</th>
<th>&gt; 5 (Work w/ Members)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 3 (Work With RRM Groups)</td>
<td>&gt; 4 (Work With Users)</td>
<td></td>
</tr>
<tr>
<td>Opt 10 (Work With What If Analysis)</td>
<td>&gt; 3 (Work With What If RRM Groups)</td>
<td>&gt; 4 (Work With What If Users)</td>
</tr>
</tbody>
</table>

```
NW0062T1                     Work with Users              18:47:22   3/26/2008
Type options, press Enter.                          Position To: |
1=Add User  2=Edit User  3=Copy User  4=Delete User  5=Display Groups
Opt  Name       Description
---  ----------  ------------------------------------------
   *PUBLIC    *Public                                  |
   AA         No description found                     |
   ABC        No description found                     |
   ACMSDEMO   No description found                     |
   ACMSDMOOWN No description found                     |
   ALDON      No description found                     |
   ALERT01    ALERT - NETWORK MESSAGER                 |
   ANONFTP    No description found                     |
   ANONYMOUS  No description found                     |
   ANOTHERTES No description found                    |
   AAA        User1                                    |
   BBB        User2                                    |
More...
F1=Help         F3=Exit         F5=Refresh       F7=Reload      F12=Cancel
F13=Repeat      F14=Sort        F17=Top          F18=Bottom     F23=More Opts
```
This screen includes the following header, selection option, group/member, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

**Selection Option Information**

1=Add User
   Lets you add a new user based on the selected user.

2=Edit User
   Lets you edit the selected user.

3=Copy User
   Lets you create a copy of the selected user with a different name.

4=Delete User
   Lets you remove a user from the group.

5=Display Groups
   Displays the Work with User Groups screen, which lets you work with the User Groups that contain the selected user.

**Group/Member Information**

**Position To**

Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the **Position To** field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.
Opt

To issue a selection option, type the number of the option and press ENTER.

Name Subset

Using the input field above “Name,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Name

The name of the user.

Description Subset

Using the input field above “Description,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Description

A description of the user.

Add Row

This field above the entries lets you add Users and User Groups.

Function Key Information

F17=Top

Redisplays the list being sorted so that the first record is shown at the top of the list.

F18=Bottom

Redisplays the list being sorted so that the last record is shown at the top of the list.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work With User Group Members

Depending on the option selected, the Work With User Group Members screen lets you maintain Secured or What If User Groups.
The Work With User Group Members screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 3 (RRM Groups)</th>
<th>&gt; 4 (Users)</th>
<th>&gt; 5 (Display Groups)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 3 (What If RRM Groups)</td>
<td>&gt; 4 (What If Users)</td>
</tr>
<tr>
<td>Opt 3 (RRM Groups)</td>
<td>&gt; 5 (Networks)</td>
<td>&gt; 5 (Display Groups)</td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 3 (What If RRM Groups)</td>
<td>&gt; 5 (What If Networks)</td>
</tr>
<tr>
<td>Opt 3 (RRM Groups)</td>
<td>&gt; 6 (Operations)</td>
<td>&gt; 5 (Display Groups)</td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 3 (What If RRM Groups)</td>
<td>&gt; 6 (What If Operations)</td>
</tr>
</tbody>
</table>

NW0065T1  Work with User Group Members   10:10:56   7/09/2008

Group Hierarchy . : /:ADDNEWGRP

Type options, press Enter.  Position To:  
1-Add Member  4=Remove Member  5=Work w/ Group Mbrs  10=Work w/ Obj Aut

<table>
<thead>
<tr>
<th>Opt</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ACMSDEMO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AERSSER</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>AKTEST131</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AKTEST132</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALDON</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALDONCMS</td>
<td></td>
</tr>
</tbody>
</table>

F1=Help          F3=Exit          F4=Prompt          F5=Refresh          F12=Cancel
F13=Repeat       F14=Sort         F17=Top           F18=Bottom

This screen includes the following header, selection option, group, and function key information.
Header Information

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

Selection Option Information

1=Add Member
   Lets you add a user group member.

4=Remove Member
   Lets you remove a user group member.

5=Work w/Group Mbrs
   If the selected member is a group, the members of the group are displayed.

10=Work w/ Obj Aut
   Displays the Remote Object Authority by User screen, which lets you work with Remote Object Authorities if the selected user has an object.

Group Information

Member Hierarchy
   The hierarchy of groups that contains the selected member.

Position To
   Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

   Only sortable columns with an underlined field above the column heading can be positioned using this function.

Opt
   To issue a selection option, type the number of the option and press ENTER.
**Name Subset**
Using the input field above “Name,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

**Name**
The name of the member or group.

**Description Subset**
Using the input field above “Description,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

**Description**
A description of the member or group.

---

**Function Key Information**

**F4=Prompt**
Displays the Select Screen, which list all valid members and groups that you can select.

**F17=Top**
Redisplays the list being sorted so that the first record is shown at the top of the list.

**F18=Bottom**
Redisplays the list being sorted so that the last record is shown at the top of the list.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

---

**Object Authority Maintenance**
Depending on the option selected, the Remote Object Authority by User screen lets you maintain Secured or What If RRM Object Authorities.
The Remote Object Authority screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 1 (Secured Entries)</th>
<th>&gt; 6 (UsrGrp)</th>
<th>&gt; 5 (Members)</th>
<th>&gt; 10 (Work w/ Obj Aut)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 3 (RRM Groups)</td>
<td>&gt; 4 (Work With Users)</td>
<td>&gt; 10 (Work w/ Obj Aut)</td>
<td></td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 3 (What If RRM Groups)</td>
<td>&gt; 4 (What If Users)</td>
<td>&gt; 10 (Work w/ Obj Aut)</td>
</tr>
</tbody>
</table>

This screen includes the following header, selection option, object, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

2=Work With Remote Aut
   Lets you work with the authorities of remote objects associated with the selected user.

4=Delete
   Lets you delete a Remote Object Authority record.

10=Edit User Aut
   Lets you change the authority of the user associated with the selected object.

22=Display Path
   Displays the path of the selected object authority file or directory.

Object Information

Op
   To issue a selection option, type the number of the option and press ENTER.

Object
   The object (and its full IFS path) collected.

R (read):
   Authority to read a file (Y=yes or N=no).

W (write):
   Authority to change a file (Y=yes or N=no).

E (execute):
   Authority to execute a program or command (Y=yes or N=no).

O (operate):
   Authority to create or delete a file (Y=yes or N=no).

S (status):
   Whether the decision-making process that controls remote request access to RRM is enabled or disabled for the selected entry associated with the object (Y=enabled or N=disabled).
Function Key Information

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work with Networks

Depending on the option selected, the Work with Networks screen lets you maintain Secured or What If Network Address Groups.

Using network groups to organize Secured Entries lets you minimize the number of Secured Entries that must be created and maintained to authorize remote requests. Instead of specifying a unique Secured Entry to authorize each remote request, you can place the network address of each request in a network address group that provides the desired authority. Each additional request that needs the same network address authority can be secured by adding it to the group. When a change must be made to a group of network addresses, you can change the authorities for all addresses in the group by changing the authorities of the group to which the addresses belong.
The Work with Networks screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 1 (Secured Entries)</th>
<th>&gt; 7 (NetGrp)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 3 (RRM Groups)</td>
<td>&gt; 5 (Work/w Networks)</td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 3 (What If RRM Groups)</td>
</tr>
</tbody>
</table>

This screen includes the following header, selection option, group/member, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

1 = Add Network
   Lets you add a Network Address.

2 = Edit Network
   Lets you edit the description of a Network Address.

3 = Copy Network
   Lets you copy a Network Address.

4 = Delete Network
   Lets you delete a Network Address.

Group/Member Information

Group Hierarchy
   The hierarchy of groups containing the selected Network Address or Network Address group.

Position To
   Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

   Only sortable columns with an underlined field above the column heading can be positioned using this function.

Opt
   To issue a selection option, type the number of the option and press ENTER.

Name Subset
   Using the input field above “Name,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Name
   The name of the Network Address (IP address).
Description Subset  
Using the input field above “Description,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Description  
A description of the Network Address.

Add Row  
This field above the entries lets you add Networks and Network Address groups.

Function Key Information

F17=Top  
Redisplays the list being sorted so that the first record is shown at the top of the list.

F18=Bottom  
Redisplays the list being sorted so that the last record is shown at the top of the list.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work with Operations

Depending on the option selected, the Work with Operations screen lets you maintain Secured or What If Operations.

Using operation groups to organize Secured Entries lets you minimize the number of Secured Entries that must be created and maintained to authorize remote requests. Instead of specifying a unique Secured Entry to authorize each remote request, you can place the operation of each request in an operation group that provides the desired operation authority. Each additional request that needs the same operation authority can be Secured by adding it to the group. When a change must be made to a group of operations, you can change the authorities for all operations in the group by changing the authorities of the group to which the operations belong.
The Work with Operations screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 1 (Secured Entries)</th>
<th>&gt; 8 (OprGrp)</th>
<th>&gt; 5 (Work w/ Members)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 3 (RRM Groups)</td>
<td>&gt; 3 (What If Operation Groups)</td>
<td>&gt; 5 (Work w/ Members)</td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 3 (What If RRM Groups)</td>
<td>&gt; 3 (What If Operation Groups)</td>
</tr>
</tbody>
</table>

This screen includes the following header, selection option, member, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

5=Display Groups
Displays the Work with Operation Groups screen, which lets you work with the Operation Groups that contain this Operation.

4=Remove Member
Lets you remove an Operation Group member.

5=Work w/ Members
Displays the members contained in the selected Operation Group.

Member Information

Position To
Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

Opt
To issue a selection option, type the number of the option and press ENTER.

Name Subset
Using the input field above “Name,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Name
The name of the operation. All RRM groups begin with a colon (:).

Description Subset
Using the input field above “Description,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Description
A description of the operation group member.
Function Key Information

F17=Top
Redisplays the list being sorted so that the first record is shown at the top of the list.

F18=Bottom
Redisplays the list being sorted so that the last record is shown at the top of the list.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work with Operation Group Members

Depending on the option selected, the Work with Operation Group Members screen lets you maintain Secured or What If Operation Group Members.

Using operation groups to organize Secured Entries lets you minimize the number of Secured Entries that must be created and maintained to authorize remote requests. Instead of specifying a unique Secured Entry to authorize each remote request, you can place the operation of each request in an operation group that provides the desired operation authority. Each additional request that needs the same operation authority can be Secured by adding it to the group. When a change must be made to a group of operations, you can change the authorities for all operations in the group by changing the authorities of the group to which the operations belong.
The Work with Operations screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 1 (Secured Entries)</th>
<th>&gt; 8 (OprGrp)</th>
<th>&gt; 5 (Work w/ Members)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 3 (RRM Groups)</td>
<td>&gt; 3 (What If Operation Groups)</td>
<td>&gt; 5 (Work w/ Members)</td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 3 (What If RRM Groups)</td>
<td>&gt; 5 (Work w/ Members)</td>
</tr>
</tbody>
</table>

---

NW0066T1            Work with Operation Group Members     11:26:16   7/17/2008

Group Hierarchy . : /:CMDCALL

Type options, press Enter.                          Position To:  
1=Add Member   4=Remove Member   5=Work w/ Members

Opt Name                    Description
__ DBSQL_EXECIMM_*ALL_CALL
__ DBSQLSCRIBE_*ALL_CALL
__ DBSQL_PRPDESC_*ALL_CALL
__ DBSQL_PRPEXEC_*ALL_CALL
__ DDM_COMMAND
__ FTPCLT_COMMAND
__ FTPSRV_COMMAND
__ REXEC_*ALL
__ REXEC_COMMAND
__ REXEC_INIT

F1=Help         F3=Exit         F4=Prompt     F5=Refresh      F12=Cancel
F13=Repeat      F14=Sort        F17=Top       F18=Bottom

This screen includes the following header, selection option, member, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

1=Add Member
   Lets you add an Operation Group member.

4=Remove Member
   Lets you remove an Operation Group member.

5=Work w/ Members
   Displays the members contained in the selected Operation Group.

Member Information

Position To
   Locates the desired record and positions it at the top of the column being
   sorted. To locate a record, place the cursor in the field above the column to be
   sorted, and type the name or name pattern of the record in the Position To
   field. Then press ENTER. The record is displayed at the top of the column, and
   the other records are listed below in ascending order.

   Only sortable columns with an underlined field above the column heading can
   be positioned using this function.

Opt
   To issue a selection option, type the number of the option and press ENTER.

Name Subset
   Using the input field above “Name,” you can select a subset of the list below.
   For more information, see “Using Subset Fields” on page 57.

Name
   The name of the operation. All RRM groups begin with a colon (:).

Description Subset
   Using the input field above “Description,” you can select a subset of the list
   below. For more information, see “Using Subset Fields” on page 57.

Description
   A description of the operation group member.
Function Key Information

F17=Top
Redisplays the list being sorted so that the first record is shown at the top of the list.

F18=Bottom
Redisplays the list being sorted so that the last record is shown at the top of the list.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Calendar Maintenance

Depending on the option selected, the Maintain Calendar screen lets you maintain production or What If calendar records. Use this screen to add or maintain RRM calendar records.

For the days and times shown in the record, the action specified in the Action field determines whether the user is granted access (*PASS), denied access (*FAIL), or whether access is controlled on the basis of i5/OS object-level authorities (*OBJLIST).

RRM calendars exist only in association with Collected, Secured, or What If Entries, but they have rules of their own (based on day, time, and action restrictions) that determine the success or failure of each transaction received. You can define as many calendars as you want as long as no conflict or redundancy exists between records.
The Maintain Calendar screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 5 (Calendars)</th>
<th>&gt; 2 (Edit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 5 (What If Calendars) &gt; 2 (Edit)</td>
</tr>
</tbody>
</table>

This screen includes the following header, selection option, calendar, and function key information.

### Header Information

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

This screen includes the same types of selection option information shown on the Work with User Groups Screen. For descriptions of the selection option information on this screen, see “Work with User Groups” on page 58.

Calendar Information

Calendar Name
The name of the calendar.

Dft. Action
The action to be taken if a matching calendar record is not found. If no existing calendar record applies to the day and time when the transaction is received, the action specified in the Default Action field is taken.

S
Whether the calendar is in effect Sunday.

M
Whether the calendar is in effect Monday.

T
Whether the calendar is in effect Tuesday.

W
Whether the calendar is in effect Wednesday.

T
Whether the calendar is in effect Thursday.

F
Whether the calendar is in effect Friday.

S
Whether the calendar is in effect Saturday.

Start
The starting time for a specified period when the calendar is in effect.
End
The ending time for a specified period when the calendar is in effect.

Action
The action associated with this calendar.
The following values are valid:
• *PASS—The transaction is allowed.
• *FAIL—The transaction is rejected.
• *OBJLIST—An object is associated with the transaction.

Function Key Information
F11=Toggle Default Action
Changes the value of the Dft. Action field to “*PASS”, “*FAIL”, or “*OBJLIST”.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work with Collected Entries
The Work With Collected Entries screen lets you maintain Collected Entries. This screen is displayed by executing the following option at the RRM Main Menu:

| Opt 2 (Collected Entries) |   |
The presence of a right angle bracket (>) on the right side of an entry indicates that the entry is associated with an object.

<table>
<thead>
<tr>
<th>NW0007T1</th>
<th>Work With Collected Entries</th>
<th>15:54:17</th>
<th>2/21/2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
<td></td>
<td>Review</td>
<td></td>
</tr>
</tbody>
</table>

Type options, press Enter. Position To: ___________

3=Create Secured  31=Create What If  4=Delete  5=Display  10=Object
14=Reset Count

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>__</td>
<td>__</td>
<td>__</td>
<td>__</td>
<td>__</td>
<td>__</td>
<td>__</td>
<td>__</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>FTPCLT</td>
<td>INIT</td>
<td>QSECOFR</td>
<td>10.21.17.26</td>
<td>A</td>
<td>2003/02/03.11:35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>TELNET</td>
<td>INIT</td>
<td>ANONYMOUS</td>
<td>10.21.16.49</td>
<td>R</td>
<td>2003/02/03.11:17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U</td>
<td>TELNET</td>
<td>INIT</td>
<td>ANONYMOUS</td>
<td>10.21.17.26</td>
<td>U</td>
<td>2003/02/03.10:03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARU</td>
<td>RMTCMD</td>
<td>PROGRAM</td>
<td>SJONES</td>
<td>10.21.17.26</td>
<td>U</td>
<td>2003/02/03.10:03 &gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>TELNET</td>
<td>INIT</td>
<td>ANONYMOUS</td>
<td>10.21.72.10</td>
<td>R</td>
<td>2003/02/03.09:55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>TELNET</td>
<td>INIT</td>
<td>ANONYMOUS</td>
<td>10.21.17.134</td>
<td>R</td>
<td>2003/02/03.09:46</td>
<td></td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>TELNET</td>
<td>INIT</td>
<td>ANONYMOUS</td>
<td>10.21.72.18</td>
<td>R</td>
<td>2003/02/03.08:37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AR</td>
<td>FILE</td>
<td>LISTATT</td>
<td>KJAMES</td>
<td>10.21.20.153</td>
<td>A</td>
<td>2003/01/31.12:42 &gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

More...

F1=Help  F3=Exit  F5=Refresh  F7=Create Subset
F11=View 2  F12=Cancel  F13=Repeat  F14=Sort

This screen includes the following header, selection option, Collected Entry, and function key information.

**Header Information**

For descriptions of the other types of header information shown on this screen, see “Work with Secured Entries” on page 53.

**Selection Option Information**

3=Create Secured

Lets you create a Secured Entry from a Collected Entry.

4=Delete

Lets you delete a Collected Entry.
5=Display
Shows the data for a Collected Entry.

10=Objects
Displays the Work with Collected Objects screen, which lets you maintain objects associated with a Collected Entry.

14=Reset Counts
This selection option lets you reset the Trans. Count field on the Work With Collected Entries screen to a value of 1 for a specified transaction. Selecting this option also resets the Transaction Counts fields on the Work With Collected Entries - Display screen and the associated Obj Count fields on the Work with Collected Objects screen to a value of 1 for the specified transaction.

31=Create What If
Lets you create a What If Entry from a Collected Entry.

Collected Entry Information

Position To
Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

Op
To issue a selection option, type the number of the option and press ENTER.

Rsn Subset
Using the input field above “Rsn,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Rsn
This column provides the RRM Collection reason code for the transaction with the associated object path. The following codes represent how RRM handles transaction requests based on the rules you created.
A
The transaction was allowed by RRM.

R
The transaction was rejected by RRM.

U
The transaction was unsecured by RRM. Unsecured transactions are rejected because an RRM rule does not exist for the transaction, therefore the default action is to reject the transaction.

Note
RRM sets the reason code based on the user-defined rules regardless of the secured mode setting. Therefore, if security is not turned on you can use the reason code to determine how RRM would handle the transaction if the exit point was secured. If the exit point is secured then the reason code indicates if the transaction was allowed or rejected by RRM.

Server Subset
Using the input field above “Server,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Server
The name of the server where the request originated.

Func (Function) Subset
Using the input field above “Func,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Func
The function requested in the transaction.

Note
If the TELNET/INIT server/function is included in the transaction, a user profile is not displayed unless the Autosignon function was used during initialization of the TELNET session. See “Change Telnet Attribute” on page 212.
Cmd (Command) Subset
Using the input field above “Cmd,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Cmd
The command requested in the transaction.

User Subset
Using the input field above “User,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

User
The name of the user who submitted the request.

Network Subset
Using the input field above “Network,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Network
The network address where the request originated.

R
This column displays the most recent reason code collected for this transaction. This value corresponds to the entry in the Time Stamp field.

Time Stamp Subset
Using the input field above “Time Stamp,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Time Stamp
The time when the transaction was received by RRM, in YYYY-MM-DD-HH.MM format, sorted in descending order.

Trans Count
This column displays the total number of times the transaction has been received by RRM since the last time the column was reset. The Trans. Count column for the specified transaction can be reset to a value of 1 by selecting option 14 (Reset Count). To access the column, press F11 (View 2). To re-display the Time Stamp column, press F11 (View 1).
**Function Key Information**

F7=Create Subset
Invokes the Create Collected Entries (PSRRMPCOL) command, which lets you create Secured Entries or What If Entries from a subset of Collected Entries.

F11=View 2
Toggles the information displayed in the last column. View 1 displays the timestamp when the transaction was received by RRM. View 2 displays the transaction count, which is the number of times the transaction has been received by RRM.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

**Create Entry**

The Create Entry screen lets you create a Secured or What if Entry from a Collected Entry, depending on the option selected (3= Create Secured or 31=Create What If). When a Collected Entry is used to create a Secured Entry, it can be used to authorize other incoming requests with matching security-related characteristics. When a Collected Entry is used to create a What If entry, the What If entry can be used to test the rules of a new configuration before you put it into production.
As shown in the following figure, if an object is associated with an entry, object paths and options for securing objects are displayed on the lower half of the screen.

**Note**

If multiple objects are selected from the lower half of the screen, multiple entries will be created.

---

The presence of a plus sign (+) beside a field indicates that you can press F4 (Prompt) to display a list of valid values. To indicate the type of entry created, “Secured” or “What If” is displayed in the title of the dialog box.

This screen is displayed by executing the following option at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 2 (Collected Entries)</th>
<th>&gt; 3 (Create Secured)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 2 (Collected Entries)</td>
<td>&gt; 31 (Create What If)</td>
</tr>
</tbody>
</table>
This screen includes the following header, Collected Entry, object, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

**Collected Entry Information**

**User**
The name of the user who submitted the transaction.

**Network**
The name of the network address where the transaction originated.

**Operation**
The operation associated with the transaction.

**Object Path**
The path for objects associated with the Collected Entry.

**Action**
The action associated with the transaction.

**Swap Profile**
The profile used to execute the job. If a transaction has a swap profile, the transaction is executed using the swap profile instead of the profile associated with the incoming user.

**Enabled Status**
Whether the decision-making process that controls remote request access to RRM is enabled or disabled for the selected entry (Y=enabled, N=disabled).
Object Information

If an object is associated with the entry, the following fields are displayed on the lower half of the screen:

1=Set as Obj. Path
   Specifies the selected path as the path of the associated object.

2=Work With Remote Authorities
   Displays the Maintain Remote Object Authority screen, which lets you maintain the Remote Object Authorities of the selected object.

5=Display Obj
   Displays the full path of the selected object authority file or directory.

Op
   To issue a selection option, type the number of the option and press ENTER.

Object
   The path for objects associated with the Collected Entry.

Rsn
   This column provides the RRM Collection reason code for the transaction with the associated object path. The following codes represent how RRM handles transaction requests based on the rules you created.

   A
   The transaction was allowed by RRM.

   R
   The transaction was rejected by RRM.
The transaction was unsecured by RRM. Unsecured transactions are rejected because an RRM rule does not exist for the transaction, therefore the default action is to reject the transaction.

Note
RRM sets the reason code based on the user-defined rules regardless of the secured mode setting. Therefore, if security is not turned on you can use the reason code to determine how RRM would handle the transaction if the exit point was secured. If the exit point is secured then the reason code indicates if the transaction was allowed or rejected by RRM.

Time Stamp
This column displays the time when the transaction was received by RRM in the YYYY/MM/DD HH:MM format, where YYYY is the four-digit year, MM is the month, DD is the day, HH is the hour in 24-hour time, and MM is the minute.

Obj. Count
This column displays the number of times the transaction and associated object have been received by RRM since the last time the column was reset. The Object Count column for the specified transaction and object can be reset to a value of 1 by selecting option 14 (Reset Count) from the Work With Collected Entries screen.

Function Key Information

F14=Sort
Lets you control the sequence of displayed records. To use this function, place the cursor in the column you want to sort and press F14

F19=Rmv Obj
Removes the object from the Remote Object Authority Table.

F20=Edit Obj
Lets you change the object path.
F21=Drill Obj
Displays the Maintain Remote Object Authority Screen, which lets you display or maintain remote object authorities.

F22=Display Obj
Displays the path of an object.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

**Work with Collected Objects**

The Work with Collected Objects screen lets you maintain objects associated with a Collected Entry. This screen is displayed by executing the following option string starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 2 (Collected Entries)</th>
<th>&gt; 10 (Objects)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NW0004T1</td>
<td>Work With Collected Objects 8:10:17 6/19/2008</td>
</tr>
<tr>
<td>ISHTAR</td>
<td>Review</td>
</tr>
<tr>
<td>Server</td>
<td>Func.</td>
</tr>
<tr>
<td>FTPSRV</td>
<td>COMMAND</td>
</tr>
</tbody>
</table>

Type options, press Enter.
2=Work With Remote Authorities 4=Delete 5=Display Obj

<table>
<thead>
<tr>
<th>Op Object</th>
<th>Rsn</th>
<th>Time Stamp</th>
<th>Obj. Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>/QSYS.LIB/SBMJOB.CMD</td>
<td>R</td>
<td>2003/06/19.07:01</td>
<td>4</td>
</tr>
<tr>
<td>/QSYS.LIB/QGPL.LIB/LPX.CMD</td>
<td>R</td>
<td>2003/06/19.07:01</td>
<td>14</td>
</tr>
<tr>
<td>/QSYS.LIB/DSPSYSSTS.CMD</td>
<td>R</td>
<td>2003/06/19.07:01</td>
<td>2</td>
</tr>
<tr>
<td>/QSYS.LIB/ENDJOB.CMD</td>
<td>R</td>
<td>2003/06/19.07:01</td>
<td>4</td>
</tr>
<tr>
<td>/QSYS.LIB/PSTOOLS.LIB/PSLIB.CMD</td>
<td>R 2003/06/19.07:01</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>/QSYS.LIB/PSTOOLS.LIB/PSWRKSPLF.CMD</td>
<td>R 2003/06/19.07:01</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>/QSYS.LIB/DSPOBJD.CMD</td>
<td>R</td>
<td>2003/06/19.06:07</td>
<td>4</td>
</tr>
<tr>
<td>/QSYS.LIB/DSPSYSVAL.CMD</td>
<td>R</td>
<td>2003/06/19.06:07</td>
<td>2</td>
</tr>
</tbody>
</table>

F1=Help       F3=Exit       F12=Cancel       F13=Repeat       F14=Sort

This screen includes the following header, selection option, path, and function key information.
Header Information

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

Server
The name of the server where the request originated.

Func
The function requested in the transaction.

Cmd
The command requested in the transaction.

User
The name of the user who submitted the request.

Network
The network address where the request originated.

Selection Option Information

2=Work With Remote Authorities
   Lets you maintain the authorities of remote objects associated with a Collected Entry.

4=Delete
   Lets you delete the selected object path.

5=Display Obj
   Displays the full path of the selected object authority file or directory to a maximum capacity of 16 MB of data.
Path Information

Op
To issue a selection option, type the number of the option and press ENTER.

Object
This column has been modified to display up to 45 characters of the path for objects associated with the collected entry. If an object path is larger than 45 characters long, then the object path begins with an ellipses (...) to show that the object path is truncated, and the last 42 characters of the object path are displayed. To view the entire object path, type 5 (Display Obj) in the Op field for the desired object and press Enter.

Rsn
This column provides the RRM Collection reason code for the transaction with the associated object path. The following codes represent how RRM handles transaction requests based on the rules you created.

A
The transaction was allowed by RRM.

R
The transaction was rejected by RRM.

U
The transaction was unsecured by RRM. Unsecured transactions are rejected because an RRM rule does not exist for the transaction, therefore the default action is to reject the transaction.

---

Note
RRM sets the reason code based on the user-defined rules regardless of the secured mode setting. Therefore, if security is not turned on you can use the reason code to determine how RRM would handle the transaction if the exit point was secured. If the exit point is secured then the reason code indicates if the transaction was allowed or rejected by RRM.

---

Chapter 4 • Product Options 113
Time Stamp
This column displays the time when the transaction was received by RRM in the YYYY/MM/DD HH:MM format, where YYYY is the four-digit year, MM is the month, DD is the day, HH is the hour in 24-hour time, and MM is the minute.

Obj. Count
This column displays the number of times the transaction and associated object have been received by RRM since the last time the column was reset. The Object Count column for the specified transaction and object can be reset to a value of 1 by selecting option 14 (Reset Count) from the Work With Collected Entries screen.

Function Key Information
For more information about the function keys on this screen, see “Function Key Summary” on page 51.

F14=Sort
Lets you control the sequence of displayed records. To use this function, place the cursor in the column you want to sort and press F14.

Promote Collected Entries
The Promote Collected Entries (PSRRMPCOL) command lets you promote a subset of Collected Entries to Secured Entries or What If Entries.
This command is invoked by executing the following option string starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 2 (Collected Entries)</th>
<th>&gt; F7 (Promote Subset)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RRM Promote Collected Entries (PSRRMPCOL)</td>
<td></td>
</tr>
<tr>
<td>Type choices, press Enter.</td>
<td></td>
</tr>
<tr>
<td>Promote to environment . . . .</td>
<td>*SECURED</td>
</tr>
<tr>
<td>Action . . . . . . . . . .</td>
<td>*PASS</td>
</tr>
<tr>
<td>Swap to profile . . . . . .</td>
<td>*NONE</td>
</tr>
<tr>
<td>Secured status . . . . . .</td>
<td>*YES</td>
</tr>
<tr>
<td>Add objects to ROA . . . . .</td>
<td>*YES</td>
</tr>
<tr>
<td>Add object to Secured Entry .</td>
<td>*NO</td>
</tr>
<tr>
<td>Delete Collected Entry? . . . .</td>
<td>*NO</td>
</tr>
<tr>
<td>Run interactively? . . . . .</td>
<td>*NO</td>
</tr>
<tr>
<td>Job queue . . . . . . . . .</td>
<td>QBATCH</td>
</tr>
<tr>
<td>Library . . . . . . . . .</td>
<td>*LIBL</td>
</tr>
</tbody>
</table>

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display  F24=More keys

This command includes the following parameter:

**Promote to environment**

The Secured or What If environment to which the Collected Entries will be promoted. When a subset of Collected Entries is promoted to the Secured environment, new Secured Entries are created. When a subset of Collected Entries is promoted to the What If environment, new What If Secured Entries are created.
The possible values are:

- *SECURED - Promotes the Entries to the Secured environment.

**Note**

When Collected Entries are promoted to the Secured environment, the Secured Entries created immediately take effect.

- *What If - Promotes the entries to the What If environment.

**Action**

The action of the resulting Secured Entries. The possible values are:

- *PASS - The transactions are allowed.
- *FAIL - The transactions are rejected.

**Swap to profile**

The user profile to be used to execute the transaction. The possible values are:

- *NONE - A swap profile is not used.
- name - The user profile to use when the transaction is executed.

**Enabled status**

Whether the decision-making process that controls remote request access to RRM is enabled or disabled for the selected entry. The possible values are:

- *YES - The Secured Entry is “enabled”.
- *NO - The Secured Entry is not “disabled”.

**Add objects to ROA**

Whether all objects are added to the Remote Object Authority (ROA) table. The possible values are:

- *YES - The objects are added to the ROA.
- *NO - The objects are not added to the ROA.
Add object to secured entry
Whether an object, if found, is added to the resulting Secured Entry.

Note
If multiple objects were Collected, only one object is added to the Secured Entry.

The possible values are:

- *YES - An object, if found, is added to each resulting Secured Entry.
- *NO - No object is added to each resulting Secured Entry.

Delete Collected Entry
Whether each Collected Entry will be deleted after it is promoted to a Secured Entry. The possible values are:

- *YES - Each Collected Entry is deleted after it is promoted to a Secured Entry.
- *NO - Each Collected Entry is not deleted after it is promoted to a Secured Entry.

Run Interactively
Whether the job should be executed interactively or in batch mode. The following values are valid:

- *YES - Executes job interactively.
- *NO - Submits job for batch processing.

Job queue
The name of the job queue where you want to place the jobs. The following values are valid:

- *QBATCH - The name of the job queue where the jobs will be placed. “QBATCH” is the default name of the job queue, but you can change this name.
- *NONE - The job’s data will not be placed into a job queue.
Library
The name of the library where you want to place the job queue. The following values are valid:

- **name** - The name of the library.
- ***LIBL** - A list of valid libraries from which you can choose.
- ***CURLIB** - The current library.

Work with RRM Groups

The Work with RRM Groups menu lets you select options to maintain RRM groups. This menu is displayed by executing the following option at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 3 (RRM Groups)</th>
</tr>
</thead>
</table>

```
P36       PentaSafe Security Technologies, Inc  ANYUSER  Date:  3/24/08
          Work With RRM Groups  QPADEV0012  Time: 12:49:06
```

Select one of the following:

1  Work With User Groups
2  Work With Network Groups
3  Work With Operation Groups
4  Work With Users
5  Work With Networks
6  Work With Operations

Enter Option or Function/Type ==> _______  _____

F1=Help  F3=Exit  F6=Messages  F9=Window  F10=Cmd Line
F12=Previous  F13=Attention  F14=Batch Jobs  F18=Reports
This menu includes the following header, menu option, and function key information.

**Header Information**

This screen includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this screen, see “RRM Main Menu” on page 48.

**Menu Option Information**

1  **Work with User Groups**
   Displays the Work with User Groups screen, which lets you work with User Groups. Depending on the option selected, this screen lets you work with Secured or What If User Groups. For more information, see “Work with User Groups” on page 58.

2  **Work with Network Groups**
   Displays the Work with Network Groups screen, which lets you work with Network Address Groups. Depending on the option selected, this screen lets you work with Secured or What If Network Address Groups. For more information, see “Work with Network Groups” on page 68.

3  **Work with Operation Groups**
   Displays the Work with Operation Groups screen, which lets you work with Operation Groups. Depending on the option selected, this screen lets you work with Secured or What If Operation Groups. For more information, see “Work with Operation Groups” on page 74.

4  **Work with Users**
   Displays the Work with Users screen, which lets you work with members of User Groups. Depending on the option selected, this screen lets you work with members of Secured or What If User Groups. For more information, see “Work with Users” on page 80.
5 Work with Networks
Displays the Work with Networks screen, which lets you work with members of
Network Address Groups. Depending on the option selected, this screen lets
you work with members of Secured or What If Network Address Groups. For
more information, see “Work with Networks” on page 89.

6 Work with Operations
Displays the Work with Operations screen, which lets you work with
Operations. Depending on the option selected, this screen lets you work with
Secured or What If Operations. For more information, see “Work with
Operations” on page 92.

Function Key Information
For more information about the function keys on this screen, see “Function Key
Summary” on page 51.

Work with RRM Object Authorities
Depending on the option selected, the Work With RRM Object Authorities screen lets
you maintain Secured or What If RRM Object Authorities. Use this screen to maintain
any RRM object authorities.
The Work With RRM Object Authorities screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 2 (Collected Entries)</th>
<th>&gt; 3 (Create Secured)</th>
<th>&gt; F21 (Drill Obj)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 2 (Collected Entries)</td>
<td>&gt; 31 (Create What If)</td>
<td>&gt; F21 (Drill Obj)</td>
</tr>
<tr>
<td>Opt 4 (RRM Object Authorities)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 1 (What If Entries)</td>
<td>&gt; 2 (Edit)</td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 4 (What If RRM Obj Auth)</td>
<td></td>
</tr>
</tbody>
</table>

This screen includes the following header, selection option, object, and function key information.
Header Information

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

Selection Option

2=Edit
   Lets you edit a selected record.

4=Delete
   Lets you delete a selected record.

5=Next Level
   For directories (D), displays the contents of the next level in a directory structure. For files (F), no data is displayed.

10=Mntn Obj Aut
   Displays the Remote Object Maintenance screen, which lets you maintain an object authority record.

22=Dsp Path
   Displays the full path of the selected object to a maximum capacity of 16 MB of data.

Object Information

Position To
   Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

   Only sortable columns with an underlined field above the column heading can be positioned using this function.
Op
To issue a selection option, type the number of the option and press ENTER.

Path Subset
Using the input field above “Path,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Path
Displays the path segment.

Function Key Information

F7=Maintain Root Authority
Lets you maintain object authorities in the root file system.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Object Authority Maintenance

Depending on the option selected, the Maintain Remote Object Authority screen lets you maintain Secured or What If RRM object authorities. Use this screen to maintain RRM object authorities.
The Maintain Remote Object Authority screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 1 (Secured Entries)</th>
<th>&gt; 2 (Edit)</th>
<th>&gt; F20 (Edit Obj)</th>
<th>&gt; 10 (Mntn Obj Aut)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 2 (Collected Entries)</td>
<td>&gt; 3 (Create Secure)</td>
<td>&gt; F20 (Edit Obj)</td>
<td>&gt; 10 (Mntn Obj Aut)</td>
</tr>
<tr>
<td>Opt 2 (Collected Entries)</td>
<td>&gt; 10 (Objects)</td>
<td>&gt; 2 (Work With Remote Authorities)</td>
<td></td>
</tr>
<tr>
<td>Opt 2 (Collected Entries)</td>
<td>&gt; 31 (Create What If)</td>
<td>&gt; F20 (Edit Obj)</td>
<td>&gt; 10 (Mntn Obj Aut)</td>
</tr>
<tr>
<td>Opt 4 (RRM Object Auth)</td>
<td>&gt; 10 (Mntn Obj Aut)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 1 (What If Entries)</td>
<td>&gt; 2 (Edit)</td>
<td>&gt; F20 (Edit Obj)</td>
</tr>
<tr>
<td>Opt 10 (What If Analysis)</td>
<td>&gt; 4 (What If RRM Obj Auth)</td>
<td>&gt; 10 (Mntn Obj Aut)</td>
<td></td>
</tr>
</tbody>
</table>
This screen includes the following header, selection option, object authority, and function key information.

### Header Information

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

### Selection Option Information

This screen includes the same types of selection option information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Object Authority Information

Position To
Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

Op
To issue a selection option, type the number of the option and press ENTER.

User Subset
Using the input field above “User,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

User
The name of the user associated with the object.

Read Subset
Using the input field above “Read,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Read:
Authority to read a file (Y=yes or N=no).

Write Subset
Using the input field above “Write,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Write:
Authority to change a file (Y=yes or N=no).

Exec Subset
Using the input field above “Exec,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.
Exec: Authority to execute a program or command (Y=yes or N=no).

Oper Subset
Using the input field above “Oper,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Oper:
Authority to create or delete a file (Y=yes or N=no).

Enabl Subset
Using the input field above “Enabled,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Enabl:
Enabled status. Whether the decision-making process that controls remote request access to RRM is enabled or disabled for the selected entry associated with the object (Y=enabled or N=disabled).

Function Key Information

F22=Display Object:
Displays the path of the selected object.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work with Calendars

Depending on the option selected, the Work With Calendars screen lets you maintain production or What If calendar file records. Use this screen to maintain RRM calendar file records. Calendars define the action to be taken when users attempt to access a server controlled by RRM during the days and times specified in the calendar record. You can define as many calendars as you want as long as no conflict or redundancy exists between records.
The Work With Calendars screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 5 (Calendars)</th>
<th>Opt 10 (What If Analysis)</th>
<th>&gt; 5 (What If Calendars)</th>
</tr>
</thead>
</table>

This screen includes the following header, selection option, calendar, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
**Selection Option Information**

2=Edit
Displays the Maintain Calendar screen, which lets you edit the selected record.

4=Delete
Lets you delete the selected record.

5=Display
Lets you display the attributes of the selected record.

**Calendar Information**

**Position To**
Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the **Position To** field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

**Op**
To issue a selection option, type the number of the option and press ENTER.

**Action or Calendar Subset**
Using the input field above “Action or Calendar,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

**Action or Calendar**
The name of the selected calendar file.

**Default Action Subset**
Using the input field above “Default Action,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

**Default Action**
The default action to be taken if a matching calendar file cannot be found.
Function Key Information
For more information about the function keys on this screen, see “Function Key Summary” on page 51.

Work with User/Server Overrides

Depending on the option selected, the Work With User/Server Overrides screen lets you maintain production or What If user/server overrides. Use this screen to maintain RRM user/server overrides. Typically, this function is used to grant or revoke user authority that exceeds all other authorities to a specified server.

The Work With User/Server Overrides screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 6 (User/Server Overrides)</th>
<th>Opt 10 (What If Analysis)</th>
<th>&gt; 6 (What If Usr/Svr Overrds)</th>
</tr>
</thead>
</table>

<p>| NW0052T1 | Work With User/Server Overrides | 11:57:03 | 5/26/2008 |
| ANYSERVER | Review |
| Type options, press Enter. | Position To: | 2=Edit 3=Copy 4=Delete 5=Display |</p>
<table>
<thead>
<tr>
<th>Op</th>
<th>User</th>
<th>Server</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>XYZ</td>
<td>FTPCLT</td>
<td>*PASS</td>
</tr>
<tr>
<td>2</td>
<td>XYZ</td>
<td>FTPSRV</td>
<td>*PASS</td>
</tr>
<tr>
<td>2</td>
<td>XYZ</td>
<td>SIGNON</td>
<td>*PASS</td>
</tr>
<tr>
<td>2</td>
<td>XYZ</td>
<td>FTPSRV</td>
<td>*PASS</td>
</tr>
<tr>
<td>2</td>
<td>JSMIT</td>
<td>FTPSRV</td>
<td>*TRUSTED</td>
</tr>
<tr>
<td>F1=Help</td>
<td>F3=Help</td>
<td>F6=Add</td>
<td>F12=Cancel</td>
</tr>
<tr>
<td>F13=Repeat</td>
<td>F14=Sort</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This screen includes the following header, selection option, override, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

**Selection Option Information**

1. **2=Edit**
   - Lets you edit the selected override record.

2. **3=Copy**
   - Lets you copy the selected override record.

3. **4=Delete**
   - Lets you delete the selected override record.

4. **5=Display**
   - Shows the attributes of the selected override record.

**Override Information**

**Position To**

Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the **Position To** field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

**Op**

To issue a selection option, type the number of the option and press ENTER.
User Subset
Using the input field above “User,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

User
The user who has override authority to the specified server.

Server Subset
Using the input field above “Server,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Server
The server to which the specified user has override authority.

Action Subset
Using the input field above “Action,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Action
The action specified for this override record. Valid actions are as follows:

- *PASS - The transaction is allowed.
- *FAIL - The transaction is rejected.
- *TRUSTED - Transaction information is not gathered by RRM.

RRM allows the transaction to proceed, bypassing all other RRM processing except for running the Customer Exit Programs. This special action is only valid for User/Server Overrides and is provided to significantly increase the performance of remote transactions that do not need or require the security and auditing advantages provided by RRM.
For example, the *TRUSTED action can be used when running a PC-based virus scanner against iSeries Integrated File System (IFS) objects to eliminate the overhead associated with RRM gathering transaction information, verifying security rules, and generating auditing information.

**Note**
Since *TRUSTED bypasses all RRM processing, remote transactions covered by a User/Server Override with the *TRUSTED action will not appear in RRM reports, the Work with Collected Entries screen, or be available for playback with RRM's What If feature.

**Function Key Information**
For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

**Work with User/Object Overrides**
Depending on the option selected, the Work With User/Object Overrides screen lets you maintain production or What If user/object overrides. Use this screen to maintain RRM user/object overrides. Typically, this function is used to grant or revoke user authority that exceeds all other authorities for a specified object.
The Work With User/Object Overrides screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 7 (User/Object Overrides)</th>
<th>Opt 10 (What If Analysis)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; 7 (What If Usr/Obj Overrds)</td>
<td></td>
</tr>
</tbody>
</table>

This screen includes the following header, selection option, override, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

2=Edit
   Lets you edit the selected override record.

3=Copy
   Lets you copy the selected override record.

4=Delete
   Lets you delete the selected override record.

5=Display Entry
   Lets you display the attributes of the selected override record.

22=Display Object
   Lets you display the path of a selected object.

Override Information

Position To
   Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

Op
   To issue a selection option, type the number of the option and press ENTER.

User Subset
   Using the input field above “User,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

User
   The user who has override authority to the specified server.

Object Path
   The object to which the specified user has override authority.
Action Subset
Using the input field above “Action,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Action
The action (*PASS or *FAIL) specified for this override record.

Function Key Information
For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work with Exit Points
The Work With Exit Points screen lets you register and configure the NetIQ Security Solutions for iSeries exit programs.
The Work With Exit Points screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 8 (Exit Points)</th>
<th>&gt; 8 (Exit Points)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 30 (Manage RRM)</td>
<td>&gt; 8 (Exit Points)</td>
</tr>
</tbody>
</table>

```
NW001IT1  Work With Exit Points  11:27:59  9/12/2008
ANYSYSTEM   Review

Type options, press Enter.
1=Install Exit  2=Edit  4=Rmv Exit  5=Display  11=Install/Retain Exit

<table>
<thead>
<tr>
<th>Exit</th>
<th>Exit</th>
<th>Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Op Point</td>
<td>Format</td>
<td>Mode</td>
</tr>
<tr>
<td>DDMACC</td>
<td>DDM</td>
<td>*NO</td>
</tr>
<tr>
<td>DDMACC</td>
<td>DRDA</td>
<td>*NO</td>
</tr>
<tr>
<td>QIBM_QHQ_DTAQ</td>
<td>DTAQ0100</td>
<td>*NO</td>
</tr>
<tr>
<td>QIBM_QLQP_LICENSE</td>
<td>LICM0100</td>
<td>*NO</td>
</tr>
<tr>
<td>QIBM_QMF_MESSAGE</td>
<td>MESS0100</td>
<td>*NO</td>
</tr>
<tr>
<td>QIBM_QNPS_ENTRY</td>
<td>ENTR0100</td>
<td>*NO</td>
</tr>
<tr>
<td>QIBM_QNPS_SPLF</td>
<td>SPLF0100</td>
<td>*NO</td>
</tr>
<tr>
<td>QIBM_QPWFS_FILE_SERV</td>
<td>PWFS0100</td>
<td>*NO</td>
</tr>
<tr>
<td>QIBM_QRQ_SQL</td>
<td>RSQL0100</td>
<td>*NO</td>
</tr>
<tr>
<td>QIBM_QTF_TRANSFER</td>
<td>TRAN0100</td>
<td>*NO</td>
</tr>
</tbody>
</table>

F1=Help   F3=Exit   F7=Update All   F11=View2   F12=Cancel
F13=Repeat   F14=Sort
```

This screen includes the following header, selection option, exit point, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

1=Install Exit
Displays a confirmation dialog box to verify whether you want to install the Exit Program at the selected Exit Point.

2=Edit
Lets you edit the selected Exit Point.

4=Rmv Exit
Lets you remove the Exit Program from the selected Exit Point.

5=Display
Lets you display the Exit Point Configuration file.

11=Install/Retain Exit
Installs an RRM Exit Program at sequence 1, and the custom Exit Program is retained as a customer Exit Program to be called by the RRM Exit Program. When the RRM Exit Program is called, this option causes RRM to pass the original transaction and the RRM decision to the customer Exit Program. The customer exit program can keep or reverse the original RRM decision. RRM will then enforce the decision made by the customer Exit Program.

Exit Point Information

Op
To issue a selection option, type the number of the option and press ENTER.

Exit Point Subset
Using the input field above “Exit Point,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Exit Point
The name of the exit point.

Exit Format Subset
Using the input field above “Exit Format,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.
Exit Format
The format of the exit point.

Secure Mode
Whether the exit point function that restricts access to incoming requests is enabled (*YES) or disabled (*NO).

Server
The server where the exit point resides.

Description
A description of the exit point.

User Exit Program
The exit program associated with this exit point.

Exit Pgm Library
The library that contains any exit programs associated with this exit point.

Collection Mode
The collection mode specified for the selected exit point. The following values are valid:

• *All - All incoming entries are collected.
• *None - No incoming entries are collected.
• *Reject - Rejected entries only are collected.
• *Unsecured - Unsecured entries only are collected.

Check Prm Grp
Whether the primary group should be searched (*Yes/*No).

Check Sup Grp
Whether supplemental groups should be searched (*Yes/*No).

Check RRM Grp
Whether RRM groups should be searched (*Yes/*No).

Allow Swap
Whether use of a swap profile is allowed (*Yes/*No).
Parse Max Dep
The maximum number of objects to be parsed (0-99).

Log Inc Tran
Whether you want What If Playback transactions to be logged (*Yes/*No). To log What If Playback transactions, you must specify *Yes in this field.

Log Tr Pass
Whether you want transactions that were processed and passed to be logged (*Yes/*No).

Log Tr Fail
Whether you want transactions that were processed and failed to be logged (*Yes/*No).

Log Ob Pass
Whether transactions with objects that were processed and passed should be logged (*Yes/*No).

Log Ob Fail
Whether transactions with objects that were processed and failed should be logged (*Yes/*No).

Function Key Information

F7=Update All
Lets you change the values of all exit points that were listed before F7 was pressed according to the new values specified.

When F7 (Update All) is pressed, all applicable fields for RRM exit points are assigned the value “*SAME”. The fields Customer Exit Program, Customer Exit Program Lib, and Maximum Parsing Depth cannot be globally updated and are assigned a value of “na” (not applicable). In each applicable field, you can retain the value *SAME or change it to a different valid value. The value specified will be assigned to the same field for all other exit points that were displayed before F7 was pressed.

F11=View2
Displays additional information that could not be displayed because of space limitations.
Work with RRM Defaults

The Work with RRM Defaults screen lets you maintain RRM default values. The presence of a plus sign (+) beside a field indicates that you can press F4 (Prompt) to display a list of valid values. This menu is displayed by executing the following option at the RRM Main Menu:

This screen includes the following header, default setting, and function key information.
**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

**Default Setting Information**

**RRM Transaction Journal**
The name of the RRM transaction journal. The following values are valid:

- *PentaSafe - The PentaSafe transaction journal is used.
- *IBM - The IBM transaction journal is used.

**RRM Audit Journal**
The name of the RRM audit journal to be used. The following values are valid:

- *PentaSafe - The PentaSafe audit journal is used.
- *IBM - The IBM audit journal is used.
- *NONE - Audit journaling is disabled. No audit journal is used.

---

**Note**
If audit journaling is disabled, RRM will not record who has made changes to your RRM configuration.

**Exit Program Library**
The name of the library where the exit program resides.

**Alert**
The alert notification action to be used. The following values are valid:

- B = *Both - Use PSDetect to notify specified person and send alert messages to the message queue.
- D = *PSDetect - Use PSDetect to notify specified person.
- M = *Msgq - Send alert messages to the message queue.
- N = *None - No action is taken.
Output Queue
The name of the output queue.

Output Queue Library
The name of the library where the output queue resides.

Days Collected Retained
The number of days (0-999) that the Collected Entries will be kept. If you do not want to keep Collected Entries for any length of time, specify 0.

Note
If *DFT is specified in the Number of Days to Purge field on the Delete Collected Entries screen, the value specified in the Days Collected Retained field is used.

Function Key Information

F15=UsrPrf/MsgQAlert
Displays the RRM Defaults - UsrPrf/MsgQ screen, which lets you set up the message notification actions to be used.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Work With User/MsgQ Alerts

The Work With User/MsgQ Alerts screen lets you set up the user profile/message queue alert notification actions to be used when working with PSDetect or some other message notification product. If you want to use PSDetect for alert notification, see “Setting Up PSDetect” on page 146.
The Work With User/MsgQ Alerts screen is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 9 (RRM Defaults)</th>
<th>&gt; F15 (UsrPrf/MsgQ Alert)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 30 (Manage RRM)</td>
<td>&gt; 10 (Work With User/MsgQ Alerts)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NW0055T1</th>
<th>Work With User/MsgQ Alerts</th>
<th>9:39:32</th>
<th>3/18/2008</th>
<th>Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANYSERVER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type options, press Enter.  
2=Edit  4=Delete  5=Display

Position To: ________

<table>
<thead>
<tr>
<th>Op</th>
<th>Alert Type</th>
<th>UserPrf/MsgQ Library</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MSGQ</td>
<td>QSYSOPR QSYS</td>
</tr>
<tr>
<td></td>
<td>USRPRF</td>
<td>MBY</td>
</tr>
<tr>
<td></td>
<td>USRPRF</td>
<td>SPIER</td>
</tr>
</tbody>
</table>

F1=Help  F3=Exit  F6=Add  F12=Cancel  
F13=Repeat  F14=Sort  

This screen includes the following header, alert notification, and function key information.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Selection Option Information

This screen includes the same types of selection option information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

Alert Notification Information

Position To
Locates the desired record and positions it at the top of the column being sorted. To locate a record, place the cursor in the field above the column to be sorted, and type the name or name pattern of the record in the Position To field. Then press ENTER. The record is displayed at the top of the column, and the other records are listed below in ascending order.

Only sortable columns with an underlined field above the column heading can be positioned using this function.

Op
To issue a selection option, type the number of the option and press ENTER.

Alert Type Subset
Using the input field above “Alert Type,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

Alert Type
The type of message notification to be used. The following values are valid:

- *MSGQ - Causes messages to be sent to a message queue.
- *USRPRF - Causes messages to be sent to the message queue of a user.

UserPrf/MsgQ Subset
Using the input field above “UserPrf/MsgQ,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

UserPrf/MsgQ
The user profile or the message queue of the user specified to receive messages.
**MsgQ Library Subset**
Using the input field above “MsgQ Library,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

**MsgQ Library**
The message queue library to receive alert messages if *MSGQ is specified in the Alert Type field. If *USRPRF is specified in the Alert Type field, the MsgQ Library field will not accept input.

**Function Key Information**

**F6=Add**
Lets you add a user profile/message queue alert notification record.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

**Setting Up PSDetect**

To set up PSDetect to send alert messages for messages from RRM, you must create a PSDetect filter for the PSDAPI alert queue.

**To set up PSDetect to send alert messages:**

1. On the PSDetect Main Menu, type 3 (Work with Alert Filters) and press ENTER.

2. On the Work With Alert Filters screen, type 5 (Work with Filters) beside the PSDAPI alert queue and press ENTER.

3. On the next screen displayed, press F6 to begin creating a filter.

4. On the next screen displayed, specify a value in the **Filter sequence** field, type a description in the **Filter description** field, and press ENTER.

5. On the Alert Filter Selection Criteria screen, type **PS10001** in the Message ID field, **PSRRMMSG** in the Message file field, **PSCOMMON** in the Library field, and press ENTER.

6. In the **Edit Compare Data?** popup window, type **Y** and press ENTER.
7. When the Alert Filter Compare Data Variables screen is displayed, press F4 (List variables), select the variable to be used by typing 1 beside it, and press ENTER.

In the **Equal to Compare Data** field, specify the selection criteria for the variable selected and press ENTER. Descriptions of the variables are shown in the following table.

After you have selected the data variables, press ENTER again.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;1</td>
<td>*CHAR</td>
<td>10</td>
<td>User ID</td>
</tr>
<tr>
<td>&amp;2</td>
<td>*CHAR</td>
<td>20</td>
<td>Exit Point Name</td>
</tr>
<tr>
<td>&amp;3</td>
<td>*CHAR</td>
<td>8</td>
<td>Exit Point Format Name</td>
</tr>
<tr>
<td>&amp;4</td>
<td>*CHAR</td>
<td>15</td>
<td>IP Address</td>
</tr>
<tr>
<td>&amp;5</td>
<td>*CHAR</td>
<td>7</td>
<td>Server Name</td>
</tr>
<tr>
<td>&amp;6</td>
<td>*CHAR</td>
<td>7</td>
<td>Function Name</td>
</tr>
<tr>
<td>&amp;7</td>
<td>*CHAR</td>
<td>7</td>
<td>Command</td>
</tr>
</tbody>
</table>

8. On the Work with Actions screen, press F4 (List) to list the available actions, select the action to be used by typing 1 beside it, and press ENTER.

If desired, specify different values in the **Delay before action** field and in the **Perform on system** field.

After you have selected the action(s), press ENTER again.

9. On the Work With Exit Points screen in RRM, ensure that *YES is specified in the **Secure Mode** field for each exit point to be used for providing alert notification.

10. On the Work With RRM Defaults screen, specify *PSDetect or *Both in the **Alert** field.

For additional information, see “Work With Alert Filters” in the *NetIQ Security Solutions for iSeries–PSDetect User Guide.*
Work with What If Analysis

The Work with What If Analysis menu lets you select options to test the results of a new configuration before you put it into production. For more information about What If processing, see “What If Processing” on page 43.

The Work with What If Analysis menu is displayed by executing the following option at the RRM Main Menu:

Opt 10 (What If Analysis)

Select one of the following:

1  Work With What If Entries
10  Copy Secured to What If
11  Promote What If Files
3  Work With What If RRM Groups
12  Demote What If Files
4  Work With What If RRM Obj Auth
13  Clear What If Files
5  Work With What If Calendars
14  Playback What If Trans DB
6  Work With What If Usr/Svr Overrds
20  What If Reports
7  Work With What If Usr/Obj Overrds
8  Work With What If Exit Points

This menu includes the following header, menu option, and function key information.

Header Information

This screen includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this screen, see “RRM Main Menu” on page 48.
Menu Option Information

1 Work With What If Entries
   Displays the Work With Entries screen, which lets you maintain What If
   Entries. Depending on the option selected, this screen lets you maintain
   Secured Entries or What If Entries. For more information, see “Work with
   Secured Entries” on page 53.

3 Work With What If RRM Groups
   Displays the Work with What If RRM Groups menu, which provides options
   that let you manage What If RRM groups.

4 Work With What If RRM Obj Auth
   Displays the Work With RRM Object Authorities Screen, which lets you
   maintain What If RRM object authorities. Depending on the option selected,
   this screen lets you maintain Secured or What If RRM Object Authorities. For
   more information, see “Work with RRM Object Authorities” on page 120.

5 Work With What If Calendars
   Displays the Work with Calendars screen, which lets you maintain What If
   calendar records. Depending on the option selected, this screen lets you
   maintain production or What If calendar records. For more information, see
   “Work with Calendars” on page 127.

6 Work With What If Usr/Svr Ovrrds
   Displays the Work with User/Server Overrides screen, which lets you maintain
   What If user/server override records. Depending on the option selected, this
   screen lets you maintain production or What If user/server overrides. For more
   information, see “Work with User/Server Overrides” on page 130.

7 Work With What If Usr/Obj Ovrrds
   Displays the Work with User/Object Overrides screen, which lets you maintain
   What If user/object override records. Depending on the option selected, this
   screen lets you maintain production or What If user/object overrides. For more
   information, see “Work with User/Object Overrides” on page 133.

8 Work With What If Exit Points
   Displays the Work With What If Exit Points screen, which is used to maintain
   What If exit points.
10 Copy Secured to What If
Displays a pop-up confirmation text box that instructs you to press ENTER if you want to copy Secured Entries to What If files.

11 Promote What If Files
Displays a pop-up confirmation text box that instructs you to press ENTER if you want to promote What If files to Secured Entries. This function replaces the current Secured Entry files with What If files, and saves the Secured Entry files in a backup directory. You can restore the Secured Entry files and What If files to their previous status by using Option 12 (Demote What If files).

12 Demote What If Files
Displays a pop-up confirmation text box that instructs you to press ENTER if you want to demote What If files. This function reverses the effect of the promote function by restoring What If Entries from Secured status to What If status.

13 Clear What If Files
Displays a pop-up confirmation text box that instructs you to press ENTER if you want to remove What If files. This function clears the What If files.

14 Playback What If Trans DB
Displays the What If Playback screen, which lets you create a database of What If transactions for use in testing or verifying the new What If configuration.

20 What If Reports
Displays the What If Reports menu, which provides options that let you generate What If reports.

Function Key Information
For more information about the function keys on this screen, see “Function Key Summary” on page 51.
Work with What If RRM Groups

The Work with What If RRM Groups menu lets you select options to make changes to What If RRM groups. This menu is displayed by executing the following option string starting at the RRM Main Menu:

```
Opt 10 (What If Analysis) > 3 (What If RRM Groups)
```

The following header, menu option, and function key information is available on this menu.

**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.
Menu Option Information

1 Work with User Groups
Displays the Work with User Groups screen, which lets you work with What If User Groups. Depending on the option selected, this screen lets you work with Secured or What If User Groups. For more information, see “Work with User Groups” on page 58.

2 Work with Network Groups
Displays the Work with Network Groups screen, which lets you work with What If Network Address Groups. Depending on the option selected, this screen lets you work with Secured or What If Network Address Groups. For more information, see “Work with Network Groups” on page 68.

3 Work with Operation Groups
Displays the Work with Operation Groups screen, which lets you work with What If Operation Groups. Depending on the option selected, this screen lets you work with Secured or What If Operation Groups. For more information, see “Work with Operation Groups” on page 74.

4 Work with Users
Displays the Work with Users screen, which lets you work with members of What If User Groups. Depending on the option selected, this screen lets you work with members of Secured or What If User Groups. For more information, see “Work with Users” on page 80.

5 Work with Networks
Displays the Work with Networks screen, which lets you work with members of What If Network Address Groups. Depending on the option selected, this screen lets you work with members of Secured or What If Network Address Groups. For more information, see “Work with Networks” on page 89.

6 Work with Operations
Displays the Work with Operations screen, which lets you work with members of What If Operation Groups. Depending on the option selected, this screen lets you work with members of Secured or What If Operation Groups. For more information, see “Work with Operation Group Members” on page 95.
Function Key Information

For more information about the function keys on this screen, see “Function Key Summary” on page 51.

Work With What If Exit Points

The Work With Exit Points screen lets you configure NetIQ Security Solutions for iSeries exit programs for the “What If” environment.

The Work With Exit Points screen is displayed by executing the following option string starting at the RRM Main Menu:

Opt 10 (What If Analysis) > 8 (What If Exit Points)

<table>
<thead>
<tr>
<th>Exit Op Point</th>
<th>Exit Format</th>
<th>Secure Mode</th>
<th>Server</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDMACC</td>
<td>DDM</td>
<td>*YES</td>
<td>DDM</td>
<td></td>
</tr>
<tr>
<td>DDMACC</td>
<td>DRDA</td>
<td>*YES</td>
<td>DRDA</td>
<td></td>
</tr>
<tr>
<td>QIBM_QHQ_DTAQ</td>
<td>DTAQ0100</td>
<td>*YES</td>
<td>DATAQ</td>
<td>Original Data Queue Server</td>
</tr>
<tr>
<td>QIBM_QLZP_LICENSE</td>
<td>LICM0100</td>
<td>*YES</td>
<td>LICENSE</td>
<td>Original License Mgmt Server</td>
</tr>
<tr>
<td>QIBM_QMF_MESSAGE</td>
<td>MESS0100</td>
<td>*YES</td>
<td>MSGSRV</td>
<td>Original Message Server</td>
</tr>
<tr>
<td>QIBM_QNPS_ENTRY</td>
<td>ENTR0100</td>
<td>*YES</td>
<td>NETPRT</td>
<td>Network Print Server -</td>
</tr>
<tr>
<td>QIBM_QNPS_SPLF</td>
<td>SPLF0100</td>
<td>*YES</td>
<td>NETPRT</td>
<td>Network Print Server -</td>
</tr>
<tr>
<td>QIBM_QPWS_FILE_SERV</td>
<td>PWFS0100</td>
<td>*YES</td>
<td>FILE</td>
<td>File Server</td>
</tr>
<tr>
<td>QIBM_QRQ_SQL</td>
<td>RSQL0100</td>
<td>*YES</td>
<td>RMTSQL</td>
<td>Original Remote SQL Server</td>
</tr>
<tr>
<td>QIBM_QTF_TRANSFER</td>
<td>TRAN0100</td>
<td>*YES</td>
<td>FILETFR</td>
<td>Original File Transfer</td>
</tr>
</tbody>
</table>

F1=Help       F3=Exit       F7=Update All   F11=View2   F12=Cancel
F13=Repeat    F14=Sort

This screen includes the following header, selection option, exit point, and function key information.
**Header Information**

This screen includes the same types of header information shown on the Maintain Secured Entries Screen. For more information about the header information on this screen, see “Work with Secured Entries” on page 53.

**Selection Option Information**

2=Edit
   Lets you edit the selected exit point.

5=Display
   Lets you display the Exit Point Configuration file.

**Exit Point Information**

**Op**
   To issue a selection option, type the number of the option and press ENTER.

**exit point subset**
   Using the input field above “Exit Point,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

**Exit Point**
   The name of the exit point.

**exit format subset**
   Using the input field above “Exit Format,” you can select a subset of the list below. For more information, see “Using Subset Fields” on page 57.

**Exit Format**
   The format of the exit point.

**Secure Mode**
   Whether the exit point function that restricts access to incoming requests is enabled (*YES) or disabled (*NO).

**Server**
   The server where the exit point resides.
Description
A description of the exit point.

User Exit Program
The exit program associated with this exit point.

Exit Pgm Library
The library that contains any exit programs associated with this exit point.

Collection Mode
The collection mode specified for the selected exit point. The following values are valid:

- *All - All incoming entries are collected.
- *None - No incoming entries are collected.
- *Reject - Rejected entries only are collected.
- *Unsecured - Unsecured entries only are collected.

Check Prm Grp
Whether the primary group should be searched (*Yes/*No).

Check Sup Grp
Whether supplemental groups should be searched (*Yes/*No).

Check RRM Grp
Whether RRM groups should be searched (*Yes/*No).

Allow Swap
Whether use of a swap profile is allowed (*Yes/*No).

Parse Max Dep
The maximum number of objects to be parsed (0-99).

Log Inc Tran
Whether you want What If Playback transactions to be logged (*Yes/*No). To log What If Playback transactions, you must specify *Yes in this field.

Log Tr Pass
Whether you want transactions that were processed and passed to be logged (*Yes/*No).
Log Tr Fail
Whether you want transactions that were processed and failed to be logged (*Yes/*No).

Log Ob Pass
Whether transactions with objects that were processed and passed should be logged (*Yes/*No).

Log Ob Fail
Whether transactions with objects that were processed and failed should be logged (*Yes/*No).

**Function Key Information**

**F7=Update All**
Lets you change the values of all exit points that were listed before F7 was pressed according to the new values specified.

When F7 (Update All) is pressed, all applicable fields for RRM exit points are assigned the value “*SAME”. The fields **Customer Exit Program**, **Customer Exit Program Lib**, and **Maximum Parsing Depth** cannot be globally updated and are assigned a value of “na” (not applicable). In each applicable field, you can retain the value *SAME or change it to a different valid value. The value specified will be assigned to the same field for all other exit points that were displayed before F7 was pressed.

**F11=View2**
Displays additional information that could not be displayed because of space limitations.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.
Playback What If Transaction Database

The What If Playback (PSWIPLAYBK) command is used to create a database of What If transactions and to test or verify the new What If configuration using the Decision-making Algorithm. After you execute What If Playback, you can review the effects of the new configuration by generating What If reports. If the results are not acceptable, you can make changes and execute What If Playback again until you achieve the desired results. Then, the What If Entries can be promoted to Secured Entries and put into production.

The What If Playback command is invoked by executing the following option string starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 10 (What If Analysis)</th>
<th>&gt; 14 (Playback What If Trans DB)</th>
</tr>
</thead>
</table>

You can also perform this function by issuing PSWIPLAYBK at an i5/OS command line.

---

PentaSafe - WhatIf Playback (PSWIPLAYBK)

Type choices, press Enter.

- Input Type: *JOURNAL, *FILE
- Transaction Type: *ALL, *ALL, *DDM, *DRDA...
- Range of Journal Receivers:
  - Starting journal receiver: *CURRENT, Name, *CURRENT, *CURCHAIN
  - Ending journal receiver: Name, *LIBL, *CURLIB
- Library: Name, *LIBL, *CURLIB
- Starting Date and Time:
  - Starting date: Date (job date format)
  - Starting time: Time (hhmmss)
- Ending Date and Time:
  - Ending date: Date (job date format)
  - Ending time: Time (hhmmss)
- File Name: *NONE, Name, *NONE
- Library: *LIBL, Name, *LIBL, *CURLIB
- Replace or Add records: *REPLACE, *ADD
- Run interactively?: *NO, *YES, *NO
- Job queue: QBATCH, Name, *NONE
- Library: *LIBL, Name, *LIBL, *CURLIB

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
To ensure that reports are generated with current data, execute the What If Playback (PSWIPLAYBK) command before you generate What If reports. Then, reports can be generated by selecting options on the What If Reports menu.

This command includes the following parameters:

**Input Type**
Whether the type of input used for Playback is a journal (*JOURNAL) or a file (*FILE).

**Transaction Type**
The type of transaction to be processed in Playback mode. The following values are valid:

- ***ALL** - All transactions are processed.
- ***CENTRAL** - Central Server transactions are processed.
- ***DDM** - Distributed Data Management (DDM) transactions are processed.
- ***DRDA** - Distributed Relational Database Architecture (DRDA) transactions are processed.
- ***DBINIT** - Database Initialization (DBINIT) transactions are processed.
- ***DBNDB** - Database Server transactions are processed.
- ***DBROI** - Database Server Object Information transactions are processed.
- ***DBSQL** - Database Structured Query Language (DBSQL) transactions are processed.
- ***DTAQ** - Original Data Queue Server transactions are processed.
- ***FILE** - File Server transactions are processed.
- ***FILETFR** - Original File Transfer transactions are processed.
- ***FTPCLT** - Client File Transfer Protocol transactions are processed.
- ***FTPSRV** - Server File Transfer Protocol transactions are processed.
- ***LICENSE** - Original License Management transactions are processed.
- ***MSGSRV** - Original Message Server transactions are processed.
- ***NETPRT** - Network Printer Server transactions are processed.
• *REXEC - REXEC transactions are processed.
• *RMTCMD - Remote Command transactions are processed.
• *RMTSQXL - Remote Structured Query Language (DBSQL) transactions are processed.
• *TELNET - Telnet transactions are processed.
• *VRTPRT - Original Virtual Printer Server transactions are processed.
• *WSG - Workstation Gateway Server Signon Validation transactions are processed.
• + for more values - Displays additional input fields where you can specify more servers to restart.

Range of Journal Receivers
The starting (first) and ending (last) journal receivers that contain the journal entries to be included, and the library that contains them. RRM starts with the starting journal receiver (specified by the first value) and proceeds through the receiver chain until the ending receiver (specified by the last value) is processed. If dual receivers are used at any time, the first of the receivers is used when chaining through the receivers. The Work with Journal Attributes (WRKJRNAS) command can be used to show the order of the receivers in the receiver chain.

Starting journal receiver
The name of the first journal receiver in a series of journal receivers that stores journal entries. The following values are valid:

*CURRENT - The journal receiver that is attached when conversion of journal entries starts.

*CURCHAIN - The journal receiver chain that includes the journal receiver that is attached when conversion of journal entries starts. This receiver chain does not cross a break in the chain. If there is a break in the chain, the receiver range includes the most recent break in the chain through the receiver that is attached when conversion of journal entries starts.

journal receiver - The name of the journal receiver whose entries are converted for output.
Library - The name of the library where the starting journal receiver is located. The following values are valid:

name - The name of the library.

*LIBL - A list of valid libraries from which you can choose.

*CURLIBL - The current library.

Ending journal receiver
The name of the last journal receiver in a series of journal receivers that stores journal entries.

The following values are valid:

*CURRENT - The journal receiver that is attached when conversion of journal entries starts.

journal receiver - The name of the journal receiver whose entries are converted for output.

Library
The name of the library where the ending journal receiver is located. The following values are valid:

name - The name of the library.

*LIBL - A list of valid libraries from which you can choose.

*CURLIBL - The current library.
Starting Date and Time
The beginning date and time of the period for which you want report data.

Starting date
The specified starting date in your jobs date format (*JOB).

Note
NetIQ Corporation products do not support Julian dates.

Starting time
The specified starting time in the format hh:mm:ss.

Ending Date and Time
The ending date and time of the period for which you want report data.

Ending date
The specified ending date in your job date format.

Ending time
The specified ending time in the format hh:mm:ss.

File Name
The name of the file where you want to place the data. The following values are valid:

*NONE
The reported data will not be placed in a data file.

name
The file where the data will be placed.

Library
The name of the library where the data file is located. The following values are valid:

name - The name of the library.

*LIBL - A list of valid libraries from which you can choose.

*CURLIB - The current library.
Replace or Add Records
Whether you want the generated output to replace (*REPLACE) the existing report or to be appended to the end of (*ADD) the existing report.

Run Interactively
Whether the job should be executed interactively or in batch mode. The following values are valid:

- *NO - Submits job for batch processing.
- *YES - Executes job interactively.

Job queue
The name of the job queue where you want to place the jobs. The following values are valid:

- *QBATCH - The name of the job queue where the jobs will be placed. “QBATCH” is the default name of the job queue, but you can change this name.
- *NONE - The job’s data will not be placed into a job queue.
- Library - The name of the library where you want to place the job queue. The following values are valid:

  - name - The name of the library.
  - *LIBL - A list of valid libraries from which you can choose.
  - *CURLIB - The current library.
**What If Reports**

The What If Reports menu lets you select options to generate What If Reports. This menu is displayed by executing the following option string starting at the RRM Main Menu:

```
Opt 10 (What If Analysis) > 20 (What If Reports)
```

```
PS3204 PentaSafe Security Technologies,Inc ANYUSER Date: 6/18/08
What If Reports QPADEV000D Time: 12:01:40
```

Select one of the following:

1. What If Transactions By Date/Time
2. What If Transactions By User
3. What If Transactions By Function
4. What If Transactions By Server
5. What If Transactions By Address

Enter Option or Function/Type ==> __________

F1=Help F3=Exit F6=Messages F9=Window F10=Cmd Line
F11=Filters F12=Previous F13=Attention F14=Batch Jobs F24=More Keys

The following menu options and function keys are available on this screen.

**Header Information**

This screen includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this screen, see “RRM Main Menu” on page 48.
Menu Option Information

1 What If Transactions By Date/Time
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort What If transactions by date and time.

2 What If Transactions By User
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort What If transactions by user.

3 What If Transactions By Function
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort What If transactions by function.

4 What If Transactions By Server
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort What If transactions by server.

5 What If Transactions By Address
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort What If transactions by network address.

Function Key Information

F11=Filters
   Displays the Work with Filters screen, which lets you maintain filters.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.
Work with RRM Reports

The Work with RRM Reports menu lets you select options to generate RRM reports. This menu is displayed by executing the following option at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 20 (RRM Reports)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>PS320</th>
<th>PentaSafe Security Technologies, Inc</th>
<th>XYZ</th>
<th>Date: 7/20/08</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Work With RRM Reports</td>
<td>QPADEV000B</td>
<td>Time: 13:56:30</td>
</tr>
</tbody>
</table>

Select one of the following:

1. Transaction Reports
2. Object Reports
3. Summary/Statistic Reports
4. What If Reports
5. Configuration Reports
6. All RRM Reports
10. Work with RRM Report Filters

Enter Option or Function/Type ==> ______________________

F1=Help   F3=Exit   F6=Messages   F9=Window   F10=Cmd Line
F11=Filters F12=Previous F13=Attention F14=Batch Jobs F24=More Keys

This menu includes the following header, menu option, and function key information.

Header Information

This screen includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this screen, see “RRM Main Menu” on page 48.
Menu Option Information

1 Transaction Reports
   Displays the Transaction Reports menu, which provides options to generate
   transaction reports.

2 Object Reports
   Displays the Object Reports menu, which provides options to generate object
   reports.

3 Summary/Statistic Reports
   Displays the Summary/Statistic Reports menu, which provides options to
   generate summary/statistic reports.

4 What If Reports
   Displays the What If Reports menu, which provides options to generate
   analysis reports.

5 Configuration Reports
   Displays the Configuration Reports menu, which provides options to generate
   configuration reports.

6 All RRM Reports
   Displays the All RRM Reports menu, which provides options to generate any
   RRM report.

10 Work with RRM Report Filters
   Displays the Work with Filters screen, which lets you maintain filters.

Function Key Information

F11=Filters
   Displays the Work with Filters screen, which lets you maintain filters.

For more information about the function keys on this screen, see “Function Key
Summary” on page 51.
Run Report Command

The Run Report (PSRUNRPT) command is invoked whenever you execute an option to generate a production or What If report. This command lets you specify report parameters and generate the desired report.

<table>
<thead>
<tr>
<th>Type choices, press Enter.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Id . . . . . . . . &gt; NW000007 Name, NW000002...</td>
</tr>
<tr>
<td>Report Description . . . . 'FTP Logon and Server Requests'</td>
</tr>
<tr>
<td>User Name . . . . . . . . <em>ALL Name, generic</em>, *ALL</td>
</tr>
<tr>
<td>Transactions . . . . . . . *ALL *ALL, *PASS, *FAIL</td>
</tr>
<tr>
<td>Starting Date and Time:</td>
</tr>
<tr>
<td>Starting date . . . . . . . *CURR Date, *PRVMS, *PRVME...</td>
</tr>
<tr>
<td>Starting time . . . . . . . Time (hhmms)</td>
</tr>
<tr>
<td>Ending Date and Time:</td>
</tr>
<tr>
<td>Ending date . . . . . . . *CURR Date, *PRVMS, *PRVME...</td>
</tr>
<tr>
<td>Ending time . . . . . . . Time (hhmms)</td>
</tr>
<tr>
<td>Filter Name . . . . . . . *NONE Name,...</td>
</tr>
<tr>
<td>Print Exceptions Only . . *YES *YES, *NO</td>
</tr>
<tr>
<td>Range of Journal Receivers:</td>
</tr>
<tr>
<td>Starting journal receiver . . . *CURRENT Name, *CURRENT, *CURCHAIN</td>
</tr>
<tr>
<td>Library . . . . . . . . . Name, *LIBL, *CURLIB</td>
</tr>
<tr>
<td>Ending journal receiver . . . *CURRENT Name, *CURRENT</td>
</tr>
<tr>
<td>Library . . . . . . . . . Name, *LIBL, *CURLIB</td>
</tr>
<tr>
<td>Print Summary Totals . . . . *YES *YES, *NO</td>
</tr>
<tr>
<td>Print Summary Averages . . . *YES *YES, *NO</td>
</tr>
<tr>
<td>Lower Threshold . . . . . . 30 Percent</td>
</tr>
<tr>
<td>Print First Level Detail . . . *YES *YES, *NO</td>
</tr>
<tr>
<td>Print Second Level Detail . . . *YES *YES, *NO</td>
</tr>
<tr>
<td>File to Receive Output . . . *NONE Name, *NONE</td>
</tr>
<tr>
<td>Library . . . . . . . . . *LIBL Name, *LIBL, *CURLIB</td>
</tr>
<tr>
<td>Replace or Add records . . . *REPLACE *REPLACE, *ADD</td>
</tr>
<tr>
<td>Run interactively? . . . . . *NO *YES, *NO</td>
</tr>
<tr>
<td>Output queue . . . . . . . QPRINT Name, *CURRENT, *USRPRF...</td>
</tr>
<tr>
<td>Library . . . . . . . . . *LIBL Name, *LIBL</td>
</tr>
<tr>
<td>Hold report on output queue . . . *NO *YES, *NO</td>
</tr>
<tr>
<td>Job queue . . . . . . . . . QBATCH Name, *NONE</td>
</tr>
<tr>
<td>Library . . . . . . . . . *LIBL Name, *LIBL, *CURLIB</td>
</tr>
<tr>
<td>Schedule job? . . . . . . . *NO *YES, *NO</td>
</tr>
<tr>
<td>Synchronize Client . . . . . *YES *YES, *NO</td>
</tr>
</tbody>
</table>

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display  F24=More keys
The Run Report command is invoked by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 10 (What If Analysis)</th>
<th>&gt; 20 (What If Reports)</th>
<th>&gt; selected report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 20 (RRM Reports)</td>
<td>&gt; 1 (Transaction Reports)</td>
<td>&gt; selected report</td>
</tr>
<tr>
<td>Opt 20 (RRM Reports)</td>
<td>&gt; 2 (Object Reports)</td>
<td>&gt; selected report</td>
</tr>
<tr>
<td>Opt 20 (RRM Reports)</td>
<td>&gt; 3 (Summary/Statistic Reports)</td>
<td>&gt; selected report</td>
</tr>
<tr>
<td>Opt 20 (RRM Reports)</td>
<td>&gt; 4 (What If Reports)</td>
<td>&gt; selected report</td>
</tr>
<tr>
<td>Opt 20 (RRM Reports)</td>
<td>&gt; 5 (What If Reports)</td>
<td>&gt; selected report</td>
</tr>
<tr>
<td>Opt 20 (RRM Reports)</td>
<td>&gt; 6 (All RRM Reports)</td>
<td>&gt; selected report</td>
</tr>
</tbody>
</table>

You can also invoke this command by issuing PSRUNRPT at an i5/OS command line or by issuing it from your own programs or automatic job scheduling systems.

This command includes the following parameters:

**Report Id**

The code name of the report to be generated. All valid RRM report IDs are listed in “Report IDs” on page 175. To generate an RRM report from an i5/OS command line, you must specify the correct report ID for the desired report.

**Report Description**

A description of the report to be generated.

**User Name**

The name of the user who is generating the report.
Transactions
The type of transactions for which you want report data. The following values are valid:

- *ALL - All Transactions are included in the report data.
- *PASS - Only transactions that were allowed are included in the report.
- *FAIL - Only transactions that were rejected are included in the report.

Starting Date and Time
The beginning date and time of the period for which you want report data.

Starting date
The beginning date of the period for which you want report data. The following values are valid.

date - A date in the *JOB format.

Note
NetIQ Corporation products do not support Julian dates.

*CURR - The current date.

*PRVMS - The previous month's starting date.

*PRVME - The previous month's ending date.

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

*PRVDY - The previous day’s date.

*CURMS - The current month’s starting date.

Starting time
The beginning time of the period for which you want report data in the format hh:mm:ss.

Ending Date and Time
The ending date and time of the period for which you want report data.
Ending date
The ending date of the period for which you want report data. The following values are valid.

date - A date in the *JOB format.
*CURR - The current date.
*PRVMS - The previous month's starting date.
*PRVME - The previous month's ending date.
*PRVWK - The previous week's starting date (last 7 days).
*PRVDY - The previous day's date.
*CURMS - The current month’s starting date.

Ending Time
The ending time of the period for which you want report data in the format hh:mm:ss.

Filter
The name of the user-defined filter to be used to select data to include in the report. The possible values are:

• *NONE - The data is not filtered.
• filter name - The name of the filter to be used. Press F4 to display a list of available filters.

Print Exceptions Only
Whether you want to print only the report exceptions (*YES or *NO). This field is displayed for What If Reports only.
Range of Journal Receivers
The starting (first) and ending (last) journal receivers that contain the journal entries to be included, and the libraries that contain them. RRM starts with the starting journal receiver (specified by the first value) and proceeds through the receiver chain until the ending receiver (specified by the last value) is processed. If dual receivers are used at any time, the first of the receivers is used when chaining through the receivers. The Work with Journal Attributes (WRKJRNA) command can be used to show the order of the receivers in the receiver chain.

Starting journal receiver
The name of the first journal receiver in a series of journal receivers that stores journal entries. The following values are valid:

- **journal receiver** - The name of the journal receiver whose entries are converted for output.

- **CURRENT** - The journal receiver is used that is attached when starting to convert journal entries.

- **CURCHAIN** - Uses the journal receiver chain that includes the journal receiver that is attached when starting to convert journal entries. This receiver chain does not cross a break in the chain. If there is a break in the chain, the receiver range includes the most recent break in the chain through the receiver that is attached when starting to convert journal entries.

- **Library** - The name of the library where the starting journal receiver is located. The following values are valid:

- **name** - The name of the library.

- **LIBL** - A list of valid libraries from which you can choose.

- **CURLIBL** - The current library.

Ending journal receiver
The name of the last journal receiver in a series of journal receivers that stores journal entries. The following values are valid:

- **CURRENT** - The journal receiver is used that is attached when starting to convert journal entries.
**journal receiver** - The name of the journal receiver whose entries are converted for output.

**Library** - The name of the library where the ending journal receiver is located. The following values are valid:

- **name** - The name of the library.
- ***LIBL** - A list of valid libraries from which you can choose.
- ***CURLIBL** - The current library.

**Time Interval**
The time interval to be used for summarizing transaction activity. For example, if the time interval is ***DAY**, transaction activity will be summarized by server once each day. This field is displayed only for Summary/Statistic reports. The following values are valid:

- ***DAY** - Transaction activity is summarized by server on a daily basis.
- ***HOUR** - Transaction activity is summarized by server on an hourly basis.
- ***WEEK** - Transaction activity is summarized by server on a weekly basis.
- ***Monthly** - Transaction activity is summarized by server on a monthly basis.

**Print Summary Totals**
Whether you want summary totals to be printed (**YES** or **NO**). This field is displayed for Summary/Statistic reports only.

**Print Summary Averages**
Whether you want summary averages to be printed (**YES** or **NO**). This field is displayed for Summary/Statistic reports only.

**Lower Threshold**
The lower level threshold percentage to omit from averages. Specify a value from 0 to 99. This field is displayed for Summary/Statistic reports only.

**Print First Level Detail**
Whether you want to print the first level of details (**YES** or **NO**). This field is displayed for Summary/Statistic reports only.
Print Second Level Detail
Whether you want to print the second level of details (*YES or *NO). This field is displayed for Summary/Statistic reports only.

File to Receive Output
The name of the data file (outfile) where you want to place the report data. If a filter and an output file are specified, then the filter applies to the output file (outfile) as well as the report output.

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

The following values are valid:

• *NONE - The report data will not be placed in a data file.
• outfile name - The name and library of the database file where the output of the command is placed.
• Library name - The library where the file is located. The following values are valid:

  name - The name of the library.
  *LIBL - A list of valid libraries from which you can choose.
  *CURLIBL - The current library.

Replace or Add records
Whether you will be adding data to a file or replacing the existing data.

The following values are valid:

• *REPLACE - Replaces existing file data with new reported data.
• *ADD - Adds the new reported data to the end of the existing file.
**Run Interactively**

Whether the job should be executed interactively or in batch mode. The following values are valid:

- *NO - Submits job for batch processing.
- *YES - Executes job interactively.

**Output queue**

The qualified name of the output queue to be used for spooled files. The following values are valid:

- *name* - The name of the output queue to be used as the default output queue by the submitted job.
- *CURRENT* - The name of the current output queue.
- *USRPRF* - The name of the output queue defined in the user’s user profile.
- *DEV* - The name of the output queue defined in the printer attributes.
- *JOBD* - The name of the output queue defined in the job description.
- *Library* - The name of the library where the output queue is located.

**Hold report on output queue**

Whether reports are to be held on the output queue (*YES/*NO). Reports that are not held are usually directed to a specified printer.

**Job queue**

The job queue to be used to hold submitted report jobs. The following values are valid:

- *name* - If operating in batch mode, the name of the job queue to be used.
- *NONE* - If operating interactively, no job queue is specified.
- *Library* - The name of the library where the job queue is located.
Schedule job
Specifies whether you want to use a scheduler to schedule report jobs to have the jobs executed in batch mode. The following values are valid:

- **YES** - If operating interactively, the job is scheduled through IBM’s job scheduler or Help/ System's Robot, based on the job scheduler selected in the system menu.
- **NO** - If operating in batch mode, the job is submitted to batch.

Synchronize Client
Specifies whether the report is available using the RRM Plug-in for iSeries Navigator.

Report ID
To generate an RRM report from a command line, you must specify the correct report ID, as shown in the following table, in the **Report name** field of the Run Report command.

<table>
<thead>
<tr>
<th>Report ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NW000002</td>
<td>Database Server Requests</td>
</tr>
<tr>
<td>NW000003</td>
<td>DDM Request Access</td>
</tr>
<tr>
<td>NW000004</td>
<td>Data Queue Optimized Server Requests</td>
</tr>
<tr>
<td>NW000005</td>
<td>Data Queue Original Server Requests</td>
</tr>
<tr>
<td>NW000006</td>
<td>File Server Requests</td>
</tr>
<tr>
<td>NW000007</td>
<td>FTP Logon and Server Requests</td>
</tr>
<tr>
<td>NW000008</td>
<td>Original Virtual Print Server Request</td>
</tr>
<tr>
<td>NW000009</td>
<td>Network Print Server Entry Requests</td>
</tr>
<tr>
<td>NW000010</td>
<td>Network Print Server Spool file Requests</td>
</tr>
<tr>
<td>NW000011</td>
<td>Remote Command/Distributed Program Call Server Requests</td>
</tr>
<tr>
<td>Report ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>NW000012</td>
<td>Remote SQL Server requests</td>
</tr>
<tr>
<td>NW000013</td>
<td>TCP Signon Server requests</td>
</tr>
<tr>
<td>NW000014</td>
<td>Transfer Function Server Requests</td>
</tr>
<tr>
<td>NW000015</td>
<td>Network Transactions by Incoming Address</td>
</tr>
<tr>
<td>NW000016</td>
<td>Network Transactions by Date/Time</td>
</tr>
<tr>
<td>NW000017</td>
<td>Network Transactions by Function</td>
</tr>
<tr>
<td>NW000018</td>
<td>Network Transactions by Server</td>
</tr>
<tr>
<td>NW000019</td>
<td>Network Transactions by User</td>
</tr>
<tr>
<td>NW000083</td>
<td>Object Reports by Incoming Address</td>
</tr>
<tr>
<td>NW000084</td>
<td>Object Reports by Server</td>
</tr>
<tr>
<td>NW000085</td>
<td>Object Report by Function</td>
</tr>
<tr>
<td>NW000086</td>
<td>Object Report by User</td>
</tr>
<tr>
<td>NW000087</td>
<td>Object Report by Date/Time</td>
</tr>
<tr>
<td>NW000088</td>
<td>Object Report by Object</td>
</tr>
<tr>
<td>NW000089</td>
<td>Secured Entries</td>
</tr>
<tr>
<td>NW000090</td>
<td>User Groups</td>
</tr>
<tr>
<td>NW000091</td>
<td>Network Groups</td>
</tr>
<tr>
<td>NW000092</td>
<td>Operation Groups</td>
</tr>
<tr>
<td>NW000093</td>
<td>Calendars</td>
</tr>
<tr>
<td>NW000094</td>
<td>Transaction Summary by Server</td>
</tr>
<tr>
<td>NW000095</td>
<td>Transaction Summary by User</td>
</tr>
<tr>
<td>NW000096</td>
<td>What If Transactions by Date/Time</td>
</tr>
<tr>
<td>NW000097</td>
<td>What If Transactions by User</td>
</tr>
</tbody>
</table>
Transaction Reports

The Transaction Reports menu provides options to generate RRM transaction reports. This menu is displayed by executing the following option string starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Report ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NW000098</td>
<td>What If Transactions by Function</td>
</tr>
<tr>
<td>NW000099</td>
<td>What If Transactions by Server</td>
</tr>
<tr>
<td>NW000100</td>
<td>What If Transactions by Incoming Address</td>
</tr>
<tr>
<td>NW000101</td>
<td>RRM Audit Report</td>
</tr>
</tbody>
</table>

This menu includes the following header, menu option, and function key information.
Header Information

This menu includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this menu, see “RRM Main Menu” on page 48.

Menu Option Information

When a menu option is selected, the Run Report (PSRUNRPT) command is invoked. This command is loaded with report parameters and lets you specify additional criteria. After you submit the report job, you can view the output on the Spool Display Facility by pressing F14, or view it directly by pressing F18.

1 FTP Logon and Server Requests
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort FTP logon and server requests to generate this report. An example of the output is shown in “FTP Logon and Server Requests” on page 222.

2 TCP Signon Server Requests
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort TCP signon server requests to generate this report. An example of the output is shown in “TCP Signon Server Requests” on page 227.

3 DDM Request Access
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort DDM requests for access to generate this report. An example of the output is shown in “DDM Request Access” on page 228.

4 Transfer Function Server Requests
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort transfer function server requests to generate this report. An example of the output is shown in “Transfer Function Server Requests” on page 229.

5 Remt Cmd/Dstrbtd Pgm Call Svr Rqsts
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort remote command/distributed program call server requests to generate this report. An example of the output is shown in “Remote Com/Dist Prog Call Server Requests” on page 230.
6 File Server Requests
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort file server requests to generate this report. An example of the output is shown in “File Server Requests” on page 231.

7 Database Server Requests
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort database server requests to generate this report. An example of the output is shown in “Database Server Requests” on page 232.

8 Remote SQL Server Requests
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort Remote SQL server requests to generate this report. An example of the output is shown in “Remote SQL Server Requests” on page 235.

9 Data Queue Original Server Requests
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort data queue original server requests to generate this report. An example of the output is shown in “Data Queue Original Server Requests” on page 236.

10 Data Queue Optimized Server Requests
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort data queue optimized server requests to generate this report. An example of the output is shown in “Data Queue Optimized Server Requests” on page 237.

11 Original Virtual Print Svr Requests
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort original virtual print server requests to generate this report. An example of the output is shown in “Original Virtual Print Server Request” on page 238.

12 Network Print Server Entry Requests
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort network print server entry requests to generate this report. An example of the output is shown in “Network Print Server Entry Requests” on page 239.
13 Network Print Server Spool Requests
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort network print server spool file requests to generate this report. An example of the output is shown in “Network Print Server Spool File Requests” on page 240.

14 Network Transactions by Date/Time
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort network transactions by date and time to generate this report. An example of the output is shown in “Network Transactions by Date/Time” on page 241.

15 Network Transactions by User
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort network transactions by user to generate this report. An example of the output is shown in “Network Transactions by User” on page 242.

16 Network Transactions by Function
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort network transactions by function to generate this report. An example of the output is shown in “Network Transactions by Function” on page 243.

17 Network Transactions by Server
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort network transactions by server to generate this report. An example of the output is shown in “Network Transactions by Server” on page 244.

18 Network Transactions by Incoming Address
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort network transactions by incoming address to generate this report. An example of the output is shown in “Transaction Summary Report by User” on page 256.

Function Key Information

F11=Filters
Displays the Work with Filters screen, which lets you maintain filters.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.
Object Reports

The Object Reports menu provides options to generate RRM object reports. This menu is displayed by executing the following option string starting at the RRM Main Menu:

```
Opt 20 (RRM Reports) > 2 (Object Reports)

PS3202 PentaSafe Security Technologies, Inc XYZ Date: 6/04/08
Object Reports QPADEV000G Time: 15:31:11

Select one of the following:
1  Object Report by Object
2  Object Report by Date/Time
3  Object Report by User
4  Object Report by Function
5  Object Report by Server
6  Object Report by Incoming Address

Enter Option or Function/Type ==>

F1=Help         F3=Exit         F6=Messages     F9=Window       F10=Cmd Line
F11=Filters     F12=Previous    F13=Attention   F14=Batch Jobs  F24=More Keys
```

This menu includes the following header, menu option, and function key information.

**Header Information**

This menu includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this menu, see “RRM Main Menu” on page 48.
Menu Option Information

When a menu option is selected, the Run Report (PSRUNRPT) command is invoked. This command is loaded with report parameters and lets you specify additional criteria. After you submit the report job, you can view the output on the Spool Display Facility by pressing F14, or view it directly by pressing F18.

1 Object Report by Object
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort objects to generate this report. An example of the output is shown in “Object Report by Object” on page 246.

2 Object Report by Date/Time
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort objects by date and time to generate this report. An example of the output is shown in “Object Report by Date/Time” on page 247.

3 Object Report by User
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort objects by user to generate this report. An example of the output is shown in “Object Report by User” on page 248.

4 Object Report by Function
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort objects by function to generate this report. An example of the output is shown in “Object Report by Function” on page 249.

5 Object Report by Server
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort objects by server to generate this report. An example of the output is shown in “Object Report by Server” on page 250.

6 Object Report by Incoming Address
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort objects by incoming address to generate this report. An example of the output is shown in “Object Report by Incoming Address” on page 251.
Function Key Information

F11=Filters
   Displays the Work with Filters screen, which lets you maintain filters.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

Summary/Statistics Reports

The Summary/Statistics Reports menu provides options to generate RRM summary/statistics reports. This menu is displayed by executing the following option string starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 20 (RRM Reports)</th>
<th>&gt; 3 (Summary/Statistic Reports)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS3203</td>
<td>NetIQ Corporation</td>
</tr>
<tr>
<td>ANYUSER</td>
<td>Date: 6/18/08</td>
</tr>
<tr>
<td>Summary/Statistic Reports</td>
<td>QPADEV000D Time: 17:53:03</td>
</tr>
</tbody>
</table>

Select one of the following:

1  Transaction Summary by Server
2  Transaction Summary by User
3  RRM Audit Report
11 Collected Entries Report

Enter Option or Function/Type ==> __________   __
F1=Help     F3=Exit     F6=Messages     F9=Window     F10=Cmd Line
F11=Filters F12=Previous F13=Attention F14=Batch Jobs F24=More Keys

This menu includes the following header, menu option, and function key information.
Header Information

This menu includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this menu, see “RRM Main Menu” on page 48.

Menu Option Information

When a menu option is selected, the Run Report (PSRUNRPT) command is invoked. This command is loaded with report parameters and lets you specify additional criteria. After you submit the report job, you can view the output on the Spool Display Facility by pressing F14, or view it directly by pressing F18.

1 Transaction Summary by Server
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort transactions by server to generate this report. An example of the output is shown in “Transaction Summary Report by Server” on page 253.

2 Transaction Summary by User
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort transactions by user to generate this report. An example of the output is shown in “Transaction Summary Report by User” on page 256.

3 RRM Audit Report
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort RRM configuration changes by date to generate this report. An example of the output is shown in “RRM Audit Report” on page 258.

11 Collected Entries Report
   Invokes the NetIQ Collection Report (PSRRMCRPT) command and allows you to specify the type of output, such as *, *PRINT, or *OUTFILE, in the OUTPUT parameter. An example of the output is shown in “Collected Entries Report” on page 259.

Function Key Information

F11=Filters
   Displays the Work with Filters screen, which lets you maintain filters.
For more information about the other function keys on this screen, see “Function Key Summary” on page 51.

What If Reports

The What If Reports menu provides options to generate What If Reports. This menu is displayed by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 10 (What If Analysis)</th>
<th>&gt; 20 (What If Reports)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opt 20 (RRM Reports)</td>
<td>&gt; 4 (What If Reports)</td>
</tr>
</tbody>
</table>

This menu includes the following header, menu option, and function key information.

Header Information

This menu includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this menu, see “RRM Main Menu” on page 48.
Menu Option Information

When a menu option is selected, the Run Report (PSRUNRPT) command is invoked. This command is loaded with report parameters and lets you specify additional criteria. After you submit the report job, you can view the output on the Spool Display Facility by pressing F14, or view it directly by pressing F18.

1 What If Transactions By Date/Time
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort What If transactions by date and time to generate this report. An example of the output is shown in “What If Transactions by Date/Time” on page 263.

2 What If Transactions By User
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort What If transactions by user to generate this report. An example of the output is shown in “What If Transaction by User” on page 266.

3 What If Transactions By Function
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort What If transactions by function to generate this report. An example of the output is shown in “What If Transaction by Function” on page 268.

4 What If Transactions By Server
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort What If transactions by server to generate this report. An example of the output is shown in “What If Transaction by Server” on page 269.

5 What If Transactions By Address
   Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort What If transactions by address to generate this report. An example of the output is shown in “What If Transaction Summary by Incoming Address” on page 270.

Function Key Information

F11=Filters
   Displays the Work with Filters screen, which lets you maintain filters.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.
Configuration Reports

The Configuration Reports menu provides options to generate reports that describe the current and past configurations of RRM. This menu is displayed by executing the following option string starting at the RRM Main Menu:

Opt 20 (RRM Reports) > 5 (Configuration Reports)

This menu includes the following header, menu option, and function key information.

Header Information

This menu includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this menu, see “RRM Main Menu” on page 48.
Menu Option Information

When a menu option is selected, the Run Report (PSRUNRPT) command is invoked. This command is loaded with report parameters and lets you specify additional criteria. After you submit the report job, you can view the output on the Spool Display Facility by pressing F14, or view it directly by pressing F18.

1 Secured Entries Reports
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort Secured Entries to generate this report. An example of the output is shown in “Secured Entries Report” on page 272.

2 User Groups Report
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort user groups to generate this report. An example of the output is shown in “User Groups” on page 278.

3 Network Groups Report
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort network groups to generate this report. An example of the output is shown in “Network Groups” on page 280.

4 Operation Groups Report
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort operation groups to generate this report. An example of the output is shown in “Operation Groups” on page 281.

5 Calendar Report
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort calendar records to generate this report. An example of the output is shown in “Calendars” on page 282.
6 Remote Object Authority By User
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort remote object authority records by user to generate this report. An example of the output is shown in “Remote Object Authority By User” on page 285.

7 Remote Object Authority By Path
Invokes the Run Report (PSRUNRPT) command loaded with parameters that sort remote object authority records by path to generate this report. An example of the output is shown in “Remote Object Authority By Path” on page 286.

Function Key Information

F11=Filters
Displays the Work with Filters screen, which lets you maintain filters.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.
The All RRM Reports menu provides options to generate any RRM report. This menu is displayed by executing the following option string starting at the RRM Main Menu:

```
Opt 20 (RRM Reports) > 6 (All RRM Reports)
```

Select one of the following:

```
------ Transaction Reports -------
1 FTP Logon and Server Requests
2 TCP Signon Server Requests
3 DDM Request Access
4 Transfer Function Server Requests
5 Rmt Cmd/Datrbd Pgm Call Svr Rqsts
6 File Server Requests
7 Database Server Requests
8 Remote SQL Server Requests
9 Data Queue Original Server Request
10 Data Queue Optimized Server Reqsts
11 Original Virtual Print Svr Request
12 Network Print Server Entry Reqsts
13 Network Print Server Splf Requests
14 Network Transactions by Date/Time
15 Network Transactions by User
16 Network Transactions by Function
17 Network Transactions by Server
18 Network Trans by Incoming Address

--------- Object Reports ---------
19 Object Report by Object
20 Object Report by Date/Time
21 Object Report by Date/Time
22 Object Report by User
23 Object Report by Function
24 Object Report by Server
25 Object Report by Incoming Address

--- Summary/Statistic Reports ----
26 Object Report by Incoming Address

31 Transaction Summary by Server
32 Transaction Summary by User
33 RRM Audit Report
34 Transaction Summary by Server
35 RRM Audit Report
36 Transaction Summary by User
37 RRM Audit Report
38 Summary Report
39 Summary Report
40 Summary Report

-------- What If Reports --------
41 What If Transactions By Date/Time
42 What If Transactions By User
43 What If Transactions By Function
44 What If Transactions By Server
45 What If Transactions By Address
46 What If Transactions By Address
47 What If Transactions By Address
48 What If Transactions By Address
49 What If Transactions By Address
50 What If Transactions By Address

Enter Option or Function/Type ==> ________________
```

This menu includes the following header, menu option, and function key information.
Header Information

This menu includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this menu, see “RRM Main Menu” on page 48.

Menu Option Information

Transaction Reports
For more information about transaction report options, see “Transaction Reports” on page 177.

Object Reports
For more information about object report options, see “Object Reports” on page 181.

Summary/Statistic Reports
For more information about summary/statistic report options, see “Summary/Statistics Reports” on page 183.

What If Reports
For more information about analysis report options, see “What If Reports” on page 185.

Configuration Reports-
For more information about configuration report options, see “Configuration Reports” on page 187.

Function Key Information

F11=Filters
Displays the Work with Filters screen, which lets you maintain filters.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.
Work with RRM Report Filters

The Work With Filters screen lets you maintain RRM report filters. This screen is displayed by executing the following option string starting at the RRM Main Menu:

```
AP0710R-01                    Work with Filters           14:29:41   7/19/08
                      ANYSERVER

Type options, press Enter.
2=Update   4=Delete   6=Change Alert/Desc

Opt   Filter Name    Description                               Data Source
      TEST1            Test 1                                    NW0720F
      TEST123           Test Filter 34                          NW0720F
      TestFil1          Test Filter 2                             NW0720F
      TestFil2          Test Filter 34                          NW0720F

F1=Help   F3=Exit   F6=Add New Filter   F12=Return
```

This screen includes the following header, selection option, filter, and function key information.

Header Information

This menu includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this menu, see “RRM Main Menu” on page 48.
Selection Option Information

2=Update
   Lets you change a filter.

4=Delete
   Lets you delete a filter.

---

**Note**
No delete confirmation message is displayed.

6=Change Alert/Desc
Displays the Filter/Threshold Definition screen, which lets you change the filter description, or specify an alert to be sent if the threshold is exceeded.

Filter Information

Op
To issue a selection option, type the number of the option and press ENTER.

Filter Name
The name of the filter.

Description
A description of the filter.

Data Source
The name of the file being searched for the query.

Function Key Information

F6=Add New Filter
Displays the Filter/Threshold Definition screen, which lets you define a new filter, and a pop-up window that lets you specify the data source.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.
Filter Definition

The Filter Definition screen lets you change RRM report filter definitions. This screen is displayed by executing the following option string starting at the RRM Main Menu:

```
Opt 20 (RRM Reports) > 10 (RRM Report Filters) > 2 (Update)
```

This screen includes the following header, selection option, filter, and function key information.

Header Information

This menu includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this menu, see “RRM Main Menu” on page 48.
Selection Option Information

4=Delete
   Lets you delete a filter.

Note
No delete confirmation message is displayed.

Filter Information

Data Source
   The name of the file to be searched for the query.

Filter Name
   The name of this filter.

Description
   A description of this filter.

Op
   To issue a selection option, type the number of the option and press ENTER.

AND/OR
   Indicates whether field values must be displayed as pairs (AND) or whether they can be displayed separately (OR). Use the AND and OR values, as needed, between pairs of comparison tests to indicate how the comparisons are to be related and grouped. Leave this column blank if you define only one comparison for this query.

   An AND value indicates that the pair of tests must both be true before the results of the AND can be true. An OR value indicates that only one of the tests needs to be true for the results of the OR to be true. For each pair of comparisons, the query assumes an AND value if you do not specify one for a comparison test.

   If no ORs are specified, only records that meet all of the defined comparison tests are selected for the query. If you want to select all records that meet at least one of the tests, specify ORs to connect each one of the tests.
When you use both ANDs and ORs, each OR separates groups of comparisons connected by ANDs. Starting from the first comparison test, if the results of all the AND comparisons done between two ORs are all true, the query stops comparing and selects that record. If the test results are not all true, the query continues comparing the next group of ANDs. For more information and examples on using AND and OR, see IBM’s Query User's Guide.

Field Name
The value that determines the name of the field specified in the query. 1-50 select/omit criteria can be specified for each filter.

Operator Value
A specified value that modifies a comparison query. A list of valid values and their descriptions can be displayed by pressing F10. The following values are valid. To specify the “like” operator value for a filter, you must include a percent sign (%) before and after the operator value.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Greater Than</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less Than</td>
</tr>
<tr>
<td>&gt; =</td>
<td>Greater or Equal To</td>
</tr>
<tr>
<td>&lt; =</td>
<td>Less Than or Equal To</td>
</tr>
<tr>
<td>=</td>
<td>Equal To</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Not Equal To</td>
</tr>
<tr>
<td>¬ &gt;</td>
<td>Not Greater Than</td>
</tr>
<tr>
<td>¬ &lt;</td>
<td>Not Less Than</td>
</tr>
<tr>
<td>like</td>
<td>Like</td>
</tr>
<tr>
<td>not like</td>
<td>Not Like</td>
</tr>
</tbody>
</table>

Value
A value specified as search criteria in the fields identified.
Function Key Information

F4=Select Fields
Displays a pop-up window that lets you select the fields to be included in the filter.

F9=Insert Line
Inserts another line for the query where the cursor is placed.

F10=Display Op Codes
Displays a pop-up window with descriptions of operator codes (listed above) that can be specified in the Operator Value field.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.
Filter/Threshold Definition

The Filter/Threshold Definition screen lets you add an RRM report filter. This screen is displayed by executing the following option string starting at the RRM Main Menu:

```
Opt 20 (RRM Reports) > 10 (RRM Report Filters) > F6 (Add)
```

<table>
<thead>
<tr>
<th>AP0710R-02</th>
<th>Filter / Threshold Definition</th>
<th>10:10:30</th>
<th>7/27/08</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANYSERVER</td>
<td>Data Source.: NW0720F</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Filter Name.: TestFill</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description.: Test Filter 34</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action......: _ (Y=Send Alert</td>
<td>N=Report</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threshold....: _____ 0 (Alert</td>
<td>Only)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threshold ID: ______ (ID sent</td>
<td>to PSDetect)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Message......: __________ (Message sent to PSDetect)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

F3=Exit  F4=Select Data Source  F12=Return

This screen includes the following header, filter, and function key information.

Header Information

This menu includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this menu, see “RRM Main Menu” on page 48.
Filter Information

Data Source
The name of the file to be searched for the query. A list of possible data sources can be displayed and used for selecting the data source(s) by pressing F4.

Filter Name
The name of the filter.

Description
A description of the filter.

Action
Indicates whether to use PSDetect to send alerts, or to send only product reports (Y=Send Alert, N=Report Only).

Threshold
The number of occurrences you specify as a threshold value for this filter.

Threshold ID
The message ID you specify for directing message alerts.

Message
The message you specify to accompany message alerts.

Function Key Information

F4=Select Data Source
Displays a pop-up window that lets you select the source of the data to be filtered.

For more information about the other function keys on this screen, see “Function Key Summary” on page 51.
Manage RRM

The Manage RRM menu provides options for maintaining RRM. This menu is displayed by executing the following option at the RRM Main Menu:

Select one of the following:

1  Work with Exit Programs
2  Remove All Exit Programs
3  Cycle Remote Servers
4  Delete Collected Entries
5  Start/Stop RRM Collection Monitor
6  Switch Job Scheduler (IBM/ROBOT)
7  Work With Exit Points
8  Work With RRM Defaults
9  Work With User/MsgQ Alerts
10 Work With User/MsgQ Alerts

Enter Option or Function/Type ==> ________________

F1=Help        F3=Exit        F6=Messages       F9=Window       F10=Cmd Line
F12=Previous   F13=Attention  F14=Batch Jobs    F18=Reports

This menu includes the following header, menu option, and function key information.

Header Information

This screen includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this screen, see “RRM Main Menu” on page 48.
Menu Option Information

1. **Work with Exit Programs**
   Displays the Work With Exit Programs screen, which lets you manage Remote Request Management (RRM) exit programs at the exit points supported by your iSeries.

2. **Remove All Exit Programs**
   Displays a pop-up confirmation text box that instructs you to press ENTER if you want to remove all RRM exit programs. This function removes the exit programs and restores the network attributes for parameters DDMACC and PCSACC to their original values.

3. **Cycle Remote Servers**
   Invokes the Restart TCP Server (PSCYCLESVR) command, which lets you restart one or more Client Access or TCP servers.

4. **Delete Collected Entries**
   Invokes the Delete Collected Entries (PSRRMDLTC) command, which lets you specify parameters and schedules for deleting Collected Entries.

5. **Start/Stop RRM Collection Monitor**
   Invokes the RRM Collection Monitor Control (PSRRMCMON) command, which lets you manage RRM collection monitors.

7. **Switch Job Scheduler (IBM/ROBOT)**
   Displays a pop-up confirmation text box that instructs you to press ENTER if you want to switch from one job scheduler to another. The choices include IBM and ROBOT.

8. **Work With Exit Points**
   Displays the Work With Exit Points screen, which lets you manage RRM exit points.

9. **Work With RRM Defaults**
   Displays the Work With RRM Defaults screen, which lets you manage RRM default values.

10. **Work With User/MsgQ Alerts**
    Displays the Work With User/MsgQ Alerts screen, which lets you set up alert message notification through PSDetect.
20 Change FTP Attribute
Invokes the Change FTP Attribute (PSCHGFTPA) command, which lets you change the FTP attribute to allow anonymous access.

21 Change Telnet Attribute
Invokes the Change Telnet Attribute (PSCHGTELA) command, which lets you change the Telnet attribute to allow Autosignon access.

30 RRM Configuration Wizard
Displays a pop-up text box that prompts you For more information about how you want to use RRM and then configures the product accordingly.

Function Key Information
For more information about the function keys on this screen, see “Function Key Summary” on page 51.

Work With Exit Programs
The Work With Exit Programs Screen lets you manage Remote Request Management (RRM) exit programs at supported exit points. Only exit programs at sequence number 1 can be maintained by your iSeries system.

When this option is executed, the network attributes are changed for parameters DDMACC and PCSACC, and some exit points in the Registration Facility are assigned exit programs. Also, the network attributes for parameters DDMACC and PCSACC are printed for future reference.

Note
The IBM-supplied authorization list QPWFSERVER (for the file server) is ignored if Exit Programs are installed.
This command is invoked by executing the following option string starting at the RRM Main Menu:

```
Opt 30 (Manage RRM) > 1 (Work With Exit Programs)
```

<table>
<thead>
<tr>
<th>NW0500S1</th>
<th>Work with Exit Programs</th>
<th>6:19:02</th>
<th>6/19/2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANYSYSTEM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Type options, press Enter.
1=Install RRM Exit  4=Remove Exit  11=Install RRM Exit & Retain Current

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Exit Format</th>
<th>Exit Program</th>
<th>Exit Library</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDMACC</td>
<td>DDM</td>
<td>*NONE</td>
<td>UNSECURED</td>
<td></td>
</tr>
<tr>
<td>DDMACC</td>
<td>DRDA</td>
<td>*NONE</td>
<td>UNSECURED</td>
<td></td>
</tr>
<tr>
<td>QIBM_QHQ_DTAQ</td>
<td>DTAQ0100</td>
<td>*NONE</td>
<td>UNSECURED</td>
<td></td>
</tr>
<tr>
<td>QIBM_QLP_LICENSE</td>
<td>LICM0100</td>
<td>*NONE</td>
<td>UNSECURED</td>
<td></td>
</tr>
<tr>
<td>QIBM_QMF_MESSAGE</td>
<td>MESS0100</td>
<td>*NONE</td>
<td>UNSECURED</td>
<td></td>
</tr>
<tr>
<td>QIBM_QNPS_ENTRY</td>
<td>ENTR0100</td>
<td>*NONE</td>
<td>UNSECURED</td>
<td></td>
</tr>
<tr>
<td>QIBM_QNPS_SPLF</td>
<td>SPLF0100</td>
<td>*NONE</td>
<td>UNSECURED</td>
<td></td>
</tr>
<tr>
<td>QIBM_QPWFS_FILE_SERV</td>
<td>PWFS0100</td>
<td>*NONE</td>
<td>UNSECURED</td>
<td></td>
</tr>
<tr>
<td>QIBM_QRQ_SQL</td>
<td>RSQL0100</td>
<td>*NONE</td>
<td>UNSECURED</td>
<td></td>
</tr>
<tr>
<td>QIBM_QTF_TRANSFER</td>
<td>TRAN0100</td>
<td>*NONE</td>
<td>UNSECURED</td>
<td></td>
</tr>
<tr>
<td>QIBM_QTG_DEVINIT</td>
<td>INIT0100</td>
<td>*NONE</td>
<td>UNSECURED</td>
<td></td>
</tr>
</tbody>
</table>

F1=Help    F3=Exit    F5=Refresh    F12=Cancel    F13=Repeat

This menu includes the following header, selection option, exit program, and function key information.

**Header Information**

This menu includes the same types of header information shown on the RRM Main Menu. For more information about the header information on this menu, see “RRM Main Menu” on page 48.
Selection Option Information

1=Install RRM Exit
   Installs the PSCOMMON/NW0001E RRM exit program. Any exit program
   installed at sequence 1 will be replaced by the RRM exit program
   PSCOMMON/NW0001E.

4=Remove Exit
   Removes any exit program currently installed at sequence 1.

11=Install RRM Exit & Retain Current
   An RRM exit program is installed at sequence 1, and the custom exit program
   is retained as a customer exit program to be called by the RRM exit program.
   Thus, the RRM exit program will be called, and RRM will pass the original
   transaction and the RRM decision to the customer exit program. The customer
   exit program can keep or reverse the original RRM decision. RRM will then
   enforce the decision made by the customer exit program.

Exit Program Information

Exit Point
   The name of the exit point. Only the exit points supported by the version of
   i5/OS currently installed on the system are shown.

Exit Format
   The format of the exit point where the exit program is specified.

Exit Program
   The name of the exit program.

Exit Library
   The library where the exit program resides.

Remarks
   Indicates whether an exit program is installed at sequence 1 and, if so, if it is a
   NetIQ Security Solutions for iSeries program or a custom exit program.
Function Key Information

For more information about the function keys on this screen, see “Function Key Summary” on page 51.

Cycle Remote Servers

The Restart TCP/IP Server (PSCYCLESVR) command lets you cycle (end and restart) one or more Client Access or TCP servers. Usually, these servers need to be cycled only when adding or removing NetIQ Security Solutions for iSeries registered exit programs. When you add or remove these exit programs you must cycle the *FILE and *DATABASE servers, and end the QServer subsystem.

This command is invoked by executing the following option string starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 30 (Manage RRM)</th>
<th>&gt; 3 (Cycle Remote Servers)</th>
</tr>
</thead>
</table>

You can also perform this function by issuing PSCYCLESVR at an i5/OS command line.

```
Restart TCP/IP Server (PSCYCLESVR)

Type choices, press Enter.

Application server ........... *CENTRAL, *DATABASE, *DDM, *DT
+ for more values

Excluded servers ........... *TELNET *CENTRAL, *DATABASE, *DDM, *DT
+ for more values

Allow ending subsystems ...... *NONE *NONE, QSERVER
+ for more values

Delay before restart ....... 30 0-3600

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```
This command includes the following parameters:

**Application server**
The names of the servers that you want to cycle.

- + for more values - Displays additional input fields where you can specify more servers to cycle.

**Excluded servers**
The names of the servers that you want to exclude from the cycling process.

- + for more values - Displays additional input fields where you can specify more servers to exclude from the cycling process.

**Allow ending subsystems**
A list of subsystems that you specify to be ended if necessary. This parameter is required when a subsystem must be ended to cycle a server. This parameter also serves to remind you that a subsystem must be ended to cycle the specified server(s). The following values are valid:

- *NONE - No subsystems can be ended.
- QSERVER - The QSERVER subsystems can be ended if necessary. If the *FILE server or the *DATABASE server is selected, QSERVER must be ended.
- + for more values - Displays additional input fields where you can specify more servers to cycle.

**Delay before restart**
Lets you specify a delay period (0-3600 seconds) before each selected server is cycled.

**Delete Collected Entries**
The Delete Collected Entries (PSRRMDLTC) command lets you specify options to control the deletion of Collected Entries.
This command is invoked by executing the following option string starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 30 (Manage RRM)</th>
<th>&gt; 4 (Delete Collected Entries)</th>
</tr>
</thead>
</table>

You can also perform this function by issuing PSRRMDLTC at an i5/OS command line.

```
Delete Collected Entries (PSRRMDLTC)

Type choices, press Enter.

Number of Days to Retain . . . .  *DFT Character value, *DFT
Run interactively? . . . . . . .  *NO *YES, *NO
Job queue . . . . . . . . . . .  QBATCH Name, *NONE
  Library . . . . . . . . . . .  *LIBL Name, *LIBL, *CURLIB
Schedule job? . . . . . . . . .  *NO *YES, *NO

F9=All parameters  F11=Keywords  F14=Command string  F24=More keys
```

This command includes the following parameters:

**Number of Days to Retain**

The number of days until Collected Entries will be deleted. The following values are valid:

- `*DFT` - The value specified in the **Days Collected Retained** field on the **Work With RRM Defaults** screen.
- `number of days` - Specify a number from 1 to 999.
Run Interactively?
Whether you want the purge Collected Entries program to be executed interactively. The following values are valid:

- *NO - The job is submitted for batch processing.
- *YES - The job is executed interactively.

Job queue
The job queue that holds the batch purge jobs if *NO was specified for Run Interactively? The following values are valid:

- QBATCH - The name of the job queue where the jobs will be placed. “QBATCH” is the default name of the job queue, but you can change this name.
- *NONE - No job queue is specified.
- Library - The name of the library where you want to place the job queue. The following values are valid:

  name: The name of the library that you specify.
  *LIBL: A list of valid libraries from which you can choose.
  *CURLIBL: The name of the current library.

Schedule job?
Whether you want to set up a calendar for deleting Collected Entries. If you specify *YES, the Work with Calendars screen is displayed so that you can set up a calendar. The following values are valid:

- *NO - If operating in batch mode, the job is submitted to batch.
- *YES - If operating interactively, the job is scheduled through IBM's job scheduler or Help/ System's Robot, based on the job scheduler selected in the system menu.
Start/Stop RRM Collection Monitor

The RRM Collection Monitor Control (PSRRMCMON) command lets you stop and start RRM collection monitors.

This command is invoked by executing the following option string starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 30 (Manage RRM)</th>
<th>&gt; 5 (Start/Stop RRM Collection Monitor)</th>
</tr>
</thead>
</table>

You can also perform this function by issuing PSRRMCMON at an i5/OS command line.

```
RRM Collection Monitor Control (PSRRMCMON)
Type choices, press Enter.
How to stop . . . . . . . . . . *CNTRLD *CNTRLD, *IMMED
```

This command includes the following parameters:
RRM collection monitor action:
The action that you want the collection monitor to take. The following values are valid:

- **SWITCH** - Switches the state of the RRM Collection Monitor between running and stopped (controlled).
- **START** - Starts the RRM Collection Monitor.
- **STOP** - Stops the RRM Collection Monitor.

How to stop:
If you specified a value in the RRM collection monitor action field that will cause the collection monitor to stop, this parameter indicates how you want it to stop. The following values are valid:

- **CNTRLD** - Stops the monitor only if no exit points are set to collect remote transaction information. If one or more exits are configured to collect, the collection monitor will not be stopped.
- **IMMED** - Stops the RRM Collection Monitor immediately, even if exit points are configured to collect remote transaction information.

**Note**
If one or more exit points are configured to collect remote transaction information and the collection monitor is not running, the transaction data will be queued and retained until the collection monitor is started. However, if the collection monitor is filled before the collection queue is started, the collection monitor will wrap and lose information.

Change FTP Attribute
The Change FTP Attribute (PSCHGFTPA) command lets you specify whether RRM will allow anonymous access through FTP. This command is invoked by executing the following option string starting at the RRM Main Menu:

| Opt 30 (Manage RRM) | > 20 (Change FTP Attribute) |
You can also perform this function by issuing PSCHGFTP at an i5/OS command line.

This command includes the following parameters:

**Anonymous profile**

The profile name to use when a user logs on anonymously. The following values are valid:

- *NONE - Anonymous logon is not allowed.
- *user profile - The user profile to use to log on if anonymous logon is allowed.

**Default library:**

The initial library to be used after logon. The following values are valid:

- *USRPRF - Uses the current library (CURLIB) specified in the user profile.
- *library name - The name of a library that you specify.
Default directory:
The initial directory to be used after logon. The following values are valid:

- *USRPRF* - Uses the home directory (HOMEDIR) specified in the user profile.
- *directory name* - The name of an IFS directory that you specify.

Update profile last used date:
Whether you want to set the last-used date of the i5/OS user profile to today’s date. The following values are valid:

- *NO* - The user profile last-used date is not changed.
- *YES* - The user profile last-used date is set to today’s date.

**Change Telnet Attribute**

The Change Telnet Attribute (PSCHGTELA) command lets you specify whether RRM will allow AutoSignon access through Telnet. This command is invoked by executing the following option string starting at the RRM Main Menu:

```
Opt 30 (Manage RRM)  > 21 (Change Telnet Attribute)
```
You can also perform this function by issuing PSCHGTELA at an i5/OS command line.

This command includes the following parameters:

**AutoSignon Control**
The level of authentication required for AutoSignon. The following values are valid:

- **NONE** - Autosignon is not allowed.
- **ANY** - The password does not require validation.
- **PWDRQD** - The plain-text password must be validated.
- **ENCPWD** - The encrypted password must be validated.

**Allow printer sessions**
Whether printer sessions are allowed to be serviced through telnet (**YES** or **NO**).

**Allow printer device creation**
Whether new printer devices can be autocreated by the telnet server (**YES** or **NO**).
Allow display device naming
Whether the client can name their display device (*YES or *NO).

RRM Configuration Wizard

The RRM Configuration Wizard is provided to simplify the initial setup of primary RRM controls. The wizard prompts you for more information about how you want to use RRM and then configures the product accordingly. This command is invoked by executing the following option string starting at the RRM Main Menu and then pressing ENTER.

The configuration changes you specify are not applied until the wizard completes its cycle. Until you apply the changes, you can cancel them at any time by pressing F3.
This chapter describes the reports available with Remote Request Management (RRM) and explains how to use them.

Reporting Requirements

To generate RRM reports, logging must be activated through the settings on the Work With Exit Points screen. You can access the Work With Exit Points screen by executing one of the following option strings starting at the RRM Main Menu:

<table>
<thead>
<tr>
<th>Opt 8 (Exit Points)</th>
<th>Opt 10 (What If Analysis)</th>
<th>Opt 30 (Manage RRM)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&gt; 8 (What If Exit Points)</td>
<td>&gt; 8 (Exit Points)</td>
</tr>
</tbody>
</table>

After you submit the report job, you can view the output on the Spool Display Facility by pressing F14, or view it directly by pressing F18.

You can also generate reports by issuing the command PSRUNRPT at an i5/OS command line. For more information, see the “Run Report Command” on page 167.
# Report Summary

The following table describes the types of reports available with RRM and lists the locations in this chapter where they are discussed.

<table>
<thead>
<tr>
<th>Report</th>
<th>Purpose</th>
<th>Report ID</th>
<th>Path from Main Menu</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transaction Reports</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP Logon and Server Requests</td>
<td>Lists attempts to access the TCP/IP FTP client and server programs, and the FTP server.</td>
<td>NW000007</td>
<td>20 &gt; 1 &gt; 1</td>
<td>222</td>
</tr>
<tr>
<td>TCP Signon Server Requests</td>
<td>Lists sign-on requests for users with expired passwords.</td>
<td>NW000013</td>
<td>20 &gt; 1 &gt; 2</td>
<td>227</td>
</tr>
<tr>
<td>DDM Request Access</td>
<td>Lists attempts to access DDM.</td>
<td>NW000003</td>
<td>20 &gt; 1 &gt; 3</td>
<td>228</td>
</tr>
<tr>
<td>Transfer Function Server Requests</td>
<td>Lists file transfers between the RRM server and other systems.</td>
<td>NW000014</td>
<td>20 &gt; 1 &gt; 4</td>
<td>229</td>
</tr>
<tr>
<td>Remote Command/ Distributed Program Call Server Requests</td>
<td>Lists attempts to access the RRM server through remote commands and distributed program call requests.</td>
<td>NW000011</td>
<td>20 &gt; 1 &gt; 5</td>
<td>230</td>
</tr>
<tr>
<td>File Server Requests</td>
<td>Lists file server requests that have accessed the optimized file server.</td>
<td>NW000006</td>
<td>20 &gt; 1 &gt; 6</td>
<td>231</td>
</tr>
<tr>
<td>Database Server Requests</td>
<td>Lists attempts to access database servers for such functions as database query GUI, ODBC driver, new file transfer, remote SQL, and ODBC APIs.</td>
<td>NW000002</td>
<td>20 &gt; 1 &gt; 7</td>
<td>232</td>
</tr>
<tr>
<td>Report</td>
<td>Purpose</td>
<td>Report ID</td>
<td>Path from Main Menu</td>
<td>Page</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------</td>
<td>---------------------</td>
<td>------</td>
</tr>
<tr>
<td>Remote SQL Server requests</td>
<td>Lists attempts to access the original remote SQL server, which enables PC-iSeries database access by remote SQL APIs.</td>
<td>NW000012</td>
<td>20 &gt; 1 &gt; 8</td>
<td>235</td>
</tr>
<tr>
<td>Data Queue Original Server Requests</td>
<td>Lists attempts to access the data queue original server.</td>
<td>NW000005</td>
<td>20 &gt; 1 &gt; 9</td>
<td>236</td>
</tr>
<tr>
<td>Data Queue Optimized Server Requests</td>
<td>Lists attempts to access the data queue optimized server.</td>
<td>NW000004</td>
<td>20 &gt; 1 &gt; 10</td>
<td>237</td>
</tr>
<tr>
<td>Original Virtual Print Server Request</td>
<td>Lists attempts to access the original virtual print server, which lets the iSeries provide virtual printer support.</td>
<td>NW000008</td>
<td>20 &gt; 1 &gt; 11</td>
<td>238</td>
</tr>
<tr>
<td>Network Print Server Entry Requests</td>
<td>Lists attempts to access the optimized network print server. This print server replaces and enhances the original virtual print server, but only supports the CA/400 Optimized for OS/2 client.</td>
<td>NW000009</td>
<td>20 &gt; 1 &gt; 12</td>
<td>239</td>
</tr>
<tr>
<td>Network Print Server Spool file Requests</td>
<td>Lists attempts to access the optimized network spool file print server. This print server replaces and enhances the original virtual spool file print server, but only supports the CA/400 Optimized for OS/2 client.</td>
<td>NW000010</td>
<td>20 &gt; 1 &gt; 13</td>
<td>240</td>
</tr>
<tr>
<td>Report</td>
<td>Purpose</td>
<td>Report ID</td>
<td>Path from Main Menu</td>
<td>Page</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------</td>
<td>---------------------</td>
<td>------</td>
</tr>
<tr>
<td>Network Transactions by Date/Time</td>
<td>Lists transactions by date and time that originate from network addresses outside the RRM server.</td>
<td>NW000016</td>
<td>20 &gt; 1 &gt; 14</td>
<td>241</td>
</tr>
<tr>
<td>Network Transactions by User</td>
<td>Lists transactions by user that originate from network addresses outside the RRM server.</td>
<td>NW000019</td>
<td>20 &gt; 1 &gt; 15</td>
<td>242</td>
</tr>
<tr>
<td>Network Transactions by Function</td>
<td>Lists transactions by function that originated from network addresses outside the RRM server.</td>
<td>NW000017</td>
<td>20 &gt; 1 &gt; 16</td>
<td>243</td>
</tr>
<tr>
<td>Network Transactions by Server</td>
<td>Lists transactions by server that originated from network addresses outside the RRM server.</td>
<td>NW000018</td>
<td>20 &gt; 1 &gt; 17</td>
<td>244</td>
</tr>
<tr>
<td>Network Transactions by Incoming Address</td>
<td>Lists transactions that originate from network addresses outside the RRM server that are sorted by incoming address.</td>
<td>NW000015</td>
<td>20 &gt; 1 &gt; 18</td>
<td>245</td>
</tr>
<tr>
<td><strong>Object Reports</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Object Report by Object</td>
<td>Lists attempts by object and library to access objects in the RRM server.</td>
<td>NW000088</td>
<td>20 &gt; 2 &gt; 1</td>
<td>246</td>
</tr>
<tr>
<td>Object Report by Date/Time</td>
<td>Lists attempts by date and time submitted to access the objects in the RRM server.</td>
<td>NW000087</td>
<td>20 &gt; 2 &gt; 2</td>
<td>247</td>
</tr>
<tr>
<td>Object Report by User</td>
<td>Lists attempts by user to access the objects in the RRM server.</td>
<td>NW000086</td>
<td>20 &gt; 2 &gt; 3</td>
<td>248</td>
</tr>
<tr>
<td>Report</td>
<td>Purpose</td>
<td>Report ID</td>
<td>Path from Main Menu</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------</td>
<td>---------------------</td>
<td>------</td>
</tr>
<tr>
<td>Object Report by Function</td>
<td>Lists attempts by function to access the objects in the RRM server.</td>
<td>NW000085</td>
<td>20 &gt; 2 &gt; 4</td>
<td>249</td>
</tr>
<tr>
<td>Object Report by Server</td>
<td>Lists attempts by server to access objects in the RRM server.</td>
<td>NW000084</td>
<td>20 &gt; 2 &gt; 5</td>
<td>250</td>
</tr>
<tr>
<td>Object Report by Incoming Address</td>
<td>Lists attempts by incoming address to access the objects in the RRM server.</td>
<td>NW000083</td>
<td>20 &gt; 2 &gt; 6</td>
<td>251</td>
</tr>
<tr>
<td><strong>Summary/Statistics Reports</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction Summary Report by Server</td>
<td>Summarizes all transactions by server.</td>
<td>NW000094</td>
<td>20 &gt; 3 &gt; 1</td>
<td>253</td>
</tr>
<tr>
<td>Transaction Summary Report by User</td>
<td>Summarizes all transactions by user.</td>
<td>NW000095</td>
<td>20 &gt; 3 &gt; 2</td>
<td>192</td>
</tr>
<tr>
<td>RRM Audit Report</td>
<td>Lists the dates when the configuration of RRM was changed and indicates the files that were changed.</td>
<td>NW0000101</td>
<td>20 &gt; 3 &gt; 3</td>
<td>258</td>
</tr>
<tr>
<td>Collected Entries Report</td>
<td>Lists all RRM collected entries.</td>
<td>NW0810K</td>
<td>20 &gt; 3 &gt; 11</td>
<td>259</td>
</tr>
<tr>
<td><strong>What If Reports</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What If Transactions by Date/Time</td>
<td>Lists What If transactions by date and time.</td>
<td>NW000096</td>
<td>20 &gt; 4 &gt; 1</td>
<td>263</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10 &gt; 20 &gt; 1</td>
<td></td>
</tr>
<tr>
<td>What If Transactions by User</td>
<td>Lists What If transactions by date and user.</td>
<td>NW000097</td>
<td>20 &gt; 4 &gt; 2</td>
<td>266</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10 &gt; 20 &gt; 2</td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td>Purpose</td>
<td>Report ID</td>
<td>Path from Main Menu</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------</td>
<td>-----------------------</td>
<td>------</td>
</tr>
<tr>
<td>What If Transactions by Function</td>
<td>Lists What If transactions by date and function.</td>
<td>NW000098</td>
<td>20 &gt; 4 &gt; 3 — and — 10 &gt; 20 &gt; 3</td>
<td>268</td>
</tr>
<tr>
<td>What If Transactions by Server</td>
<td>Lists What If transactions by date and server.</td>
<td>NW000099</td>
<td>20 &gt; 4 &gt; 4 — and — 10 &gt; 20 &gt; 4</td>
<td>269</td>
</tr>
<tr>
<td>What If Transactions by Incoming Address</td>
<td>Lists What If transactions by date and incoming address.</td>
<td>NW000100</td>
<td>20 &gt; 4 &gt; 5 — and — 10 &gt; 20 &gt; 5</td>
<td>270</td>
</tr>
<tr>
<td>Configuration Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secured Entries</td>
<td>Lists the secured entries included in the current RRM configuration.</td>
<td>NW000089</td>
<td>20 &gt; 5 &gt; 1</td>
<td>272</td>
</tr>
<tr>
<td>Exit Point Setting</td>
<td>Lists the exit point settings in the current RRM configuration.</td>
<td>NW000104</td>
<td>20 &gt; 5 &gt; __</td>
<td>274</td>
</tr>
<tr>
<td>User Groups</td>
<td>Lists the user groups included in the current RRM configuration.</td>
<td>NW000090</td>
<td>20 &gt; 5 &gt; 2</td>
<td>278</td>
</tr>
<tr>
<td>Network Groups</td>
<td>Lists the network address groups included in the current RRM configuration.</td>
<td>NW000091</td>
<td>20 &gt; 5 &gt; 3</td>
<td>280</td>
</tr>
<tr>
<td>Operation Groups</td>
<td>Lists the operation groups included in the current RRM configuration.</td>
<td>NW000092</td>
<td>20 &gt; 5 &gt; 4</td>
<td>281</td>
</tr>
</tbody>
</table>
### Transaction Reports

RRM provides the following Transaction reports:

- FTP Logon and Server Requests
- TCP Signon Server Requests
- DDM Request Access
- Transfer Function Server Requests
- Remt Cmd/Dstrbtd Pgm Call Svr Rqsts
- File Server Requests
- Database Server Requests
- Remote SQL Server Requests
- Data Queue Original Server Requests
- Data Queue Optimized Server Requests
- Original Virtual Print Svr Requests
- Network Print Server Entry Reqst
• Network Print Server Splf Requests
• Network Transactions by Date/Time
• Network Transactions by User
• Network Transactions by Function
• Network Transactions by Server
• Network Transactions by Incoming Address

You can generate these reports by executing options on the Transaction Reports menu (page 177).

Note
If the TELNET/INIT server/function is included in the transaction, a user profile is not displayed unless the Auto-Signon function was used during initialization of the TELNET session.

FTP Logon and Server Requests

The FTP Logon and Server Requests report lists the number of attempts made to log on to a specified FTP server and the number of attempts to perform FTP client and server requests. This report is generated by typing Option 1 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the TCP/IP FTP client and server programs and to monitor logon access to the FTP server. To use this report, Audit Transactions must be turned on through RRM and the NetIQ Security Solutions for iSeries exit program NW0001E must be registered in the following exit points:

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>QIBM_QTMF_CLIENT_REQ</td>
<td>VLRQ0100</td>
</tr>
<tr>
<td>QIBM_QTMF_SERVER_REQ</td>
<td>VLRQ0100</td>
</tr>
<tr>
<td>QIBM_QTMF_SVR_LOGON</td>
<td>TCPL0100</td>
</tr>
</tbody>
</table>

The following figure shows an example of the FTP Logon and Server Requests Report.
The presence of a right angle bracket (>) on the right side of the report indicates that the entry is associated with an object.

This report includes the following header and transaction information.

**Header Information**

**Rpt Id**
- The identification number of the report.

**System**
- The system where the report was generated.

**Report title**
- The title of the report.

**Date**
- The date when the report was generated in the user’s job date format.

**Time**
- The time when the report was generated in the format hh:mm:ss.

**Page**
- The current page number of the report.
Transaction Information

Selection Criteria
The selection criteria associated with the request.

• **From Date/Time** - The starting date and time of the period when transactions were reported.

• **To Date/Time** - The ending date of the period when transactions were reported.

• **Filter name** - The name of the filter that was selected to generate the report. *NONE means that no filter was used.

• **Filter criteria** - If a filter is defined, the following search criteria for each record is displayed: AND/OR, Field Name, Operator Value, and Value.

Date
The date when the transaction was received, in the user’s job date format.

Time
The time when the transaction was received, in the format hh:mm:ss.

RRM P/F
The pass/fail status (P=Pass, or F=Fail) of the transaction after it has been processed by RRM and the pass/fail status of any customer exit programs.

DMA P/F
The pass/fail status (P=Pass, or F=Fail) of the transaction after it has been processed by the Decision-making Algorithm.

Entry Type
The journal entry code for the type of transaction. The following code values are valid:

<table>
<thead>
<tr>
<th>Code</th>
<th>System Type Used</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA</td>
<td>Original Client Access</td>
<td>Data Queue Server</td>
</tr>
<tr>
<td>DB</td>
<td>Optimized Client Access</td>
<td>Signon Server</td>
</tr>
<tr>
<td>DC</td>
<td>Optimized Client Access</td>
<td>Central Server</td>
</tr>
<tr>
<td>Code</td>
<td>System Type Used</td>
<td>Function</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>DD</td>
<td>Optimized Client Access</td>
<td>Database Server Initialization</td>
</tr>
<tr>
<td>DE</td>
<td>Optimized Client Access</td>
<td>Native Database Requests</td>
</tr>
<tr>
<td>DF</td>
<td>Optimized Client Access</td>
<td>Retrieve Object Information</td>
</tr>
<tr>
<td>DG</td>
<td>Optimized Client Access</td>
<td>SQL Requests</td>
</tr>
<tr>
<td>DI</td>
<td>Optimized Client Access</td>
<td>File Server</td>
</tr>
<tr>
<td>DJ</td>
<td>Optimized Client Access</td>
<td>Remote Command and Distributed Program Call</td>
</tr>
<tr>
<td>DK</td>
<td>Other</td>
<td>Distributed Data Management (DDM)</td>
</tr>
<tr>
<td>DL</td>
<td>Other</td>
<td>Distributed Relational Database Architecture (DRDA)</td>
</tr>
<tr>
<td>DM</td>
<td>TCP/IP</td>
<td>FTP Server Logon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FTP Server Anonymous Logon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FTP Server Request Validation</td>
</tr>
<tr>
<td>DN</td>
<td>TCP/IP</td>
<td>FTP Client Request Validation</td>
</tr>
<tr>
<td>DO</td>
<td>TCP/IP</td>
<td>REXEC Server Request Validation</td>
</tr>
<tr>
<td>DP</td>
<td>TCP/IP</td>
<td>REXEC Server Logon</td>
</tr>
<tr>
<td>DQ</td>
<td>TCP/IP</td>
<td>Telnet Device Initialization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Telnet Device Termination</td>
</tr>
<tr>
<td>DR</td>
<td>Original Client Access</td>
<td>Remote SQL Request</td>
</tr>
<tr>
<td>DT</td>
<td>Original Client Access</td>
<td>File Transfer Function</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Message Function Server</td>
</tr>
<tr>
<td>DU</td>
<td>Original Client Access</td>
<td>Virtual Print Server</td>
</tr>
<tr>
<td>DV</td>
<td>Original Client Access</td>
<td>License Management</td>
</tr>
</tbody>
</table>
Job ID

The following job identification information associated with the transaction:

- **Name** - The name of the job.
- **User** - The name of the user who submitted the job.
- **Nbr** - The job number.

Incoming User

The name of the user who submitted the request.

Incoming Address

The address where the transaction originated.

Operations

Information about the resources used to execute the transaction.

- **Server** - The server used to execute the transaction.
- **Function** - The function used to execute the transaction.
- **Command** - The command used to execute the transaction.

Swap Profile

The profile used to execute the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming user.

System

The system where the transaction originated.

---

<table>
<thead>
<tr>
<th>Code</th>
<th>System Type Used</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>DW</td>
<td>Other</td>
<td>ShowCase Suite</td>
</tr>
<tr>
<td>DX</td>
<td>Optimized Client Access</td>
<td>Data Queue Server</td>
</tr>
<tr>
<td>DY</td>
<td>Optimized Client Access</td>
<td>Network Print Server</td>
</tr>
</tbody>
</table>
TCP Signon Server Requests

The TCP Signon Server Requests report lists sign-on server transactions that were submitted through the TCP/IP server. These transactions are logged by exit point QIBM_QZSO_SIGNONSRV.

This report is generated by typing Option 2 and pressing ENTER on the Transaction Reports menu. Use this report to manage access to the TCP Signon Server through the sign-on server function. The following figure shows an example of the TCP Signon Server Requests Report.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
DDM Request Access

The DDM Request Access report lists the Distributed Data Management (DDM) transactions that have occurred on the RRM server. The transactions in this report are logged by exit point DDMACC. This report is generated by typing Option 3 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to DDM on the RRM server. The following figure shows an example of the DDM Request Access report.

This report includes the following header and transaction information.

Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

Transaction Information

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Transfer Function Server Requests

The Transfer Function Server Requests report lists file transfers between the RRM server and other systems. The transactions in this report are logged by exit point QIBM_QTF_TRANSF.ER. This report is generated by typing Option 4 and pressing ENTER on the Transaction Reports menu.

Use this report to manage file transfers between the RRM server and other systems. The following figure shows an example of the Transfer Function Server Requests report.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Remote Com/Dist Prog Call Server Requests

The Remote Command/Distributed Program Call Server Requests report lists the number of remote command/distributed program call server requests that occurred on the RRM server. The transactions in this report are logged by exit point QIBM_QZRC_RMT. This report is generated by typing Option 5 and pressing ENTER on the Transaction Reports menu.

Use this report to manage the access of remote commands and distributed program calls to the RRM server. The following figure shows an example of the Transaction Summary Report.

This report includes the following header and transaction information.

### Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.
Transaction Information

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.

File Server Requests

The File Server Requests report lists the file server requests that have accessed the optimized the file server. The transactions in this report are logged by exit point QIBM_QPNFS_FILE_SERV. This report is generated by typing Option 6 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the optimized file server. The following figure shows an example of the File Server Requests report.

This report includes the following header and transaction information.

Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.
Transaction Information

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.

Database Server Requests

The Database Server Requests report lists transactions that have occurred on the RRM server for supported database functions such as the following:

- Database query GUI
- ODBC driver
- New file transfer
- Remote SQL
- ODBC APIs

This report is generated by typing Option 7 and pressing ENTER on the Transaction Reports menu. The following figure shows an example of the Database Server Requests Report.
Use this report to manage access to supported database functions on the RRM server. To use this report, logging must be turned on through RRM and the following exit points must be registered in i5/OS:

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QIBM_QZDA_INIT</td>
<td>Performs server initiation.</td>
</tr>
<tr>
<td>QIBM_QZDA_NDB1</td>
<td>Performs native database requests.</td>
</tr>
<tr>
<td>QIBM_QZDA_SQL1</td>
<td>Performs SQL requests.</td>
</tr>
<tr>
<td>QIBM_QZDA_ROI1</td>
<td>Retrieves the following object information requests and SQL catalog functions:</td>
</tr>
<tr>
<td></td>
<td>• Create source physical file</td>
</tr>
<tr>
<td></td>
<td>• Create database file, based on existing file</td>
</tr>
<tr>
<td></td>
<td>• Add, clear, delete database file member</td>
</tr>
<tr>
<td></td>
<td>• Override database file</td>
</tr>
<tr>
<td></td>
<td>• Delete database file override</td>
</tr>
<tr>
<td></td>
<td>• Delete file</td>
</tr>
<tr>
<td></td>
<td>• Prepare</td>
</tr>
<tr>
<td></td>
<td>• Open</td>
</tr>
<tr>
<td></td>
<td>• Execute</td>
</tr>
<tr>
<td></td>
<td>• Connect</td>
</tr>
<tr>
<td></td>
<td>• Create package</td>
</tr>
<tr>
<td></td>
<td>• Clear Package</td>
</tr>
<tr>
<td></td>
<td>• Execute immediate</td>
</tr>
<tr>
<td></td>
<td>• Prepare and describe</td>
</tr>
<tr>
<td></td>
<td>• Prepare and execute or prepare and open</td>
</tr>
<tr>
<td></td>
<td>• Open and fetch</td>
</tr>
<tr>
<td></td>
<td>• Execute or open</td>
</tr>
<tr>
<td></td>
<td>• Library (or collection)</td>
</tr>
<tr>
<td></td>
<td>• File (or table)</td>
</tr>
<tr>
<td></td>
<td>• Field (or column)</td>
</tr>
<tr>
<td></td>
<td>• Index</td>
</tr>
<tr>
<td></td>
<td>• Relational database (or RDB)</td>
</tr>
<tr>
<td></td>
<td>• SQL package</td>
</tr>
<tr>
<td></td>
<td>• SQL package statement</td>
</tr>
<tr>
<td></td>
<td>• File member</td>
</tr>
<tr>
<td></td>
<td>• Record format</td>
</tr>
<tr>
<td></td>
<td>• Special columns</td>
</tr>
<tr>
<td></td>
<td>• Foreign keys</td>
</tr>
<tr>
<td></td>
<td>• Primary keys</td>
</tr>
</tbody>
</table>

If the SQL-specific data is blank, transactions for the Open/Describe function (X’1804’) and the Execute function (X’1805’) are not written to the security journal.
This server supports the following clients:

- Support for remote SQL access.
- Access to data through ODBC interfaces.
- Native database functions (such as creating and deleting files and adding and removing file members).
- Retrieval functions to obtain information about database files that exist on the system (such as SQL catalog functions).

The following products use the database server with APPC support:

- Client Access for Windows 95
  - Access to iSeries database through ODBC interface
- Client Access for Optimized OS/2
  - Access to iSeries database through ODBC interface
  - Access to iSeries database through remote SQL interface
  - File transfer APIs
- Client Access for Windows 3.1
  - Access to iSeries database through ODBC interface

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Remote SQL Server Requests

The Remote SQL Server Requests report lists attempts to access the original remote SQL server, which enables PC-iSeries database access by remote SQL APIs. The transactions in this report are logged by exit point QIBM_QRQ_SQL. This report is generated by typing Option 8 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the original remote SQL server. The following figure shows an example of the Remote SQL Server Requests report.

This report includes the following header and transaction information.

Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

Transaction Information

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
The Data Queue Original Server Requests report lists attempts to access the data queue original server. The transactions in this report are logged by exit point QIBM_QHQ_DTAQ. This report is generated by typing Option 9 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the data queue original server. The following figure shows an example of the Data Queue Original Server Requests report.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Data Queue Optimized Server Requests

The Data Queue Optimized Server Requests report lists attempts to access the data queue optimized server. The transactions in this report are logged by exit point QIBM_Q2HQ_DATA_QUEUE. This report is generated by typing Option 10 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the data queue optimized server. The following figure shows an example of the Data Queue Optimized Server Requests report.

This report includes the following header and transaction information.

Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

Transaction Information

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
The Original Virtual Print Server Requests report lists attempts to access the original virtual print server. The transactions in this report are logged by exit point QIBM_QVP_PRINTERS. This report is generated by typing Option 11 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the original virtual print server. The following figure shows an example of the Original Virtual Print Server Requests report.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Network Print Server Entry Requests

The Network Print Server Entry Requests report lists attempts to access the network print server. The transactions in this report are logged by exit point QIBM_QNPS_ENTRY. This report is generated by typing Option 12 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the network print server. The following figure shows an example of the Network Print Server Entry Requests report.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Network Print Server Spool File Requests

The Network Print Server Spool File Requests report lists attempts to access the network print server spool file. The transactions in this report are logged by exit point QIBM_QNPS_SPLF. This report is generated by typing Option 13 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the network print server spool file print server. The following figure shows an example of the Network Print Server Spool File Requests report.

This report includes the following header and transaction information.

Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

Transaction Information

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Network Transactions by Date/Time

The Network Transactions by Date/Time report lists the transactions that have occurred on the RRM server sorted by date and time. This report is generated by typing Option 14 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the RRM server based on transactions sorted by date and time. The following figure shows an example of the Network Transactions by Date/Time Report.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Network Transactions by User

The Network Transactions by User report lists the transactions that have occurred on the RRM server sorted by user. This report is generated by typing Option 15 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the RRM server based on transactions sorted by users. The following figure shows an example of the Network Transactions by User report.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Network Transactions by Function

The Network Transactions by Function report lists transactions sorted by function that have occurred on the RRM server. This report is generated by typing Option 16 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the RRM server based on transactions sorted by function. The following figure shows an example of the Network Transactions by Function report.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Network Transactions by Server

The Network Transactions by Server report lists transactions sorted by the server name that have occurred on the RRM server. This report is generated by typing Option 17 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the RRM server based on transactions sorted by the originating server. The following figure shows an example of the Network Transactions by Server report.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Network Transactions by Incoming Address

The Network Transactions by Incoming Address report lists transactions sorted by incoming address that have occurred on the RRM server. This report is generated by typing Option 18 and pressing ENTER on the Transaction Reports menu.

Use this report to manage access to the RRM server based on transactions sorted by incoming address. The following figure shows an example of the Network Transactions by Incoming Address report.

This report includes the following header and transaction information.

Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

Transaction Information

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Object Reports

RRM provides the following object reports:

- Object Report by Object
- Object Report by Date/Time
- Object Report by User
- Object Report by Function
- Object Report by Server
- Object Report by Incoming Address

You can generate these reports by executing options on the Object Reports menu.

Object Report by Object

The Object Report by Object lists transactions with objects that occurred on the RRM server sorted by the requested library and object. This report is generated by typing Option 1 and pressing ENTER on the Object Reports menu.
Use this report to manage access to the RRM server based on transactions sorted by the requested library and object. The following figure shows an example of the Object Report by Object.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Object Report by Date/Time**

The Object Report by Date/Time lists transactions with objects sorted by date and time that occurred on the RRM server. This report is generated by typing Option 2 and pressing ENTER on the Object Reports menu.
Use this report to manage access to objects on the RRM server based on transactions sorted by date and time. The following figure shows an example of the Object Report by Date/Time.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Object Report by User**

The Object Report by User lists transactions with objects sorted by user that occurred on the RRM server. This report is generated by typing Option 3 and pressing ENTER on the Object Reports menu.
Use this report to manage access to objects on the RRM server based on transactions sorted by user. The following figure shows an example of the Object Report by User.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Object Report by Function**

The Object Report by Function lists transactions with objects sorted by function that occurred on the RRM server. This report is generated by typing Option 4 and pressing ENTER on the Object Reports menu.
Use this report to manage access to objects on the RRM server based on transactions sorted by function. The following figure shows an example of the Object Report by Function.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Object Report by Server**

The Object Report by Server lists transactions with objects sorted by server that occurred on the RRM server. This report is generated by typing Option 5 and pressing ENTER on the Object Reports menu.
Use this report to manage access to objects on the RRM server based on transactions sorted by server. The figure below shows an example of the Object Reports by Server.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Object Report by Incoming Address**

The Object Report by Incoming Address lists transactions with objects sorted by incoming address that occurred on the RRM server. This report is generated by typing Option 6 and pressing ENTER on the Object Reports menu.
Use this report to manage access to objects on the RRM server based on transactions sorted by incoming address. The figure below shows an example of the Object Reports by Incoming Address.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the FTP Logon and Server Requests Report. For more information about the transaction information contained in this report, see “FTP Logon and Server Requests” on page 222.
Summary/Statistics Reports

RRM provides the following Summary/Statistics reports:

- Transaction Summary Report By Server
- Transaction Summary Report By User
- RRM Audit Report
- Collected Entries Report

You can generate these reports by executing options on the Summary/Statistics Reports menu (page 183).

Transaction Summary Report by Server

The Transaction Summary Report by Server summarizes RRM transactions for each server by date range. This report is generated by typing Option 1 and pressing ENTER on the Summary/Statistics Reports menu.
Use this report to manage access to RRM based on transactions sorted by server and date range. The figure below shows an example of this report.

<table>
<thead>
<tr>
<th>Start Date</th>
<th>Start Time</th>
<th>End Date</th>
<th>End Time</th>
<th>Server</th>
<th>Transactions</th>
<th>Rejected</th>
<th>Accepted</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/03/01</td>
<td>11:00:00</td>
<td>08/03/01</td>
<td>11:59:59</td>
<td>Subtotal</td>
<td>18</td>
<td>0 .00</td>
<td>18 100.00</td>
</tr>
<tr>
<td>08/03/01</td>
<td>12:00:00</td>
<td>08/03/01</td>
<td>12:59:59</td>
<td>Subtotal</td>
<td>0</td>
<td>0 .00</td>
<td>0 .00</td>
</tr>
<tr>
<td>08/03/01</td>
<td>13:00:00</td>
<td>08/03/01</td>
<td>13:59:59</td>
<td>Subtotal</td>
<td>0</td>
<td>0 .00</td>
<td>0 .00</td>
</tr>
<tr>
<td>08/03/01</td>
<td>14:00:00</td>
<td>08/03/01</td>
<td>14:59:59</td>
<td>Subtotal</td>
<td>11</td>
<td>0 .00</td>
<td>11 100.00</td>
</tr>
<tr>
<td>08/03/01</td>
<td>14:00:00</td>
<td>08/03/01</td>
<td>14:59:59</td>
<td>Subtotal</td>
<td>11</td>
<td>0 .00</td>
<td>11 100.00</td>
</tr>
<tr>
<td>08/03/01</td>
<td>14:00:00</td>
<td>08/03/01</td>
<td>14:59:59</td>
<td>Subtotal</td>
<td>11</td>
<td>0 .00</td>
<td>11 100.00</td>
</tr>
<tr>
<td>08/03/01</td>
<td>14:00:00</td>
<td>08/03/01</td>
<td>14:59:59</td>
<td>Subtotal</td>
<td>11</td>
<td>0 .00</td>
<td>11 100.00</td>
</tr>
<tr>
<td>08/03/01</td>
<td>14:00:00</td>
<td>08/03/01</td>
<td>14:59:59</td>
<td>Subtotal</td>
<td>11</td>
<td>0 .00</td>
<td>11 100.00</td>
</tr>
<tr>
<td>08/03/01</td>
<td>11:00:00</td>
<td>08/03/01</td>
<td>14:59:59</td>
<td>Grand Total</td>
<td>58</td>
<td>0 .00</td>
<td>58 100.00</td>
</tr>
<tr>
<td>08/03/01</td>
<td>11:00:00</td>
<td>08/03/01</td>
<td>14:59:59</td>
<td>Average (&gt;= 30%)</td>
<td>14</td>
<td>0 .00</td>
<td>14 100.00</td>
</tr>
</tbody>
</table>

This report includes the following header and transaction information.
Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

Transaction Information

Selection Criteria

The following selection criteria associated with the request:

From Date/Time
The starting date of the period, in the user’s job date format, when transactions were reported.

To Date/Time
The ending date of the period, in the user’s job date format, when transactions were reported.

Time Interval
The time interval used for summarizing transaction activity. For example, if the time interval was *DAY, transaction activity was summarized once each day. The following values are valid:

*DAY - Transaction activity is summarized on a daily basis.

*HOUR - Transaction activity is summarized on an hourly basis.

*WEEK - Transaction activity is summarized on a weekly basis.

*MONTHLY - Transaction activity is summarized on a monthly basis.

Filter Name
The name of the filter that was selected to generate the report. *NONE means that no filter was used.

Filter Criteria
If a filter was defined, the following search criteria for each record is displayed: AND/OR, Field Name, Operator Value, and Value.
Start_Date Start_Time
The starting date and time for this reporting period.

End_Date End_Time
The ending date and time for this reporting period.

Server Subtotal
The subtotal of transactions by server for this reporting period.

Grand Total
The combined total of all server subtotals for this reporting period.

Total Transactions
The total number of transactions (rejected and accepted) for this reporting period.

Rejected Transactions
The number and percentage of rejected transactions for this reporting period.

Accepted Transactions
The number and percentage of accepted transactions for this reporting period.

Transaction Summary Report by User

The Transaction Summary Report by User summarizes RRM transactions for each user by date range. This report is generated by typing Option 2 and pressing ENTER on the Summary/Statistics Reports menu.
Use this report to manage access to RRM based on transactions sorted by user and date range. The figure below shows an example of the Transaction Summary Report by User.

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.
Transaction Information

This report includes the same types of transaction information shown on the Transaction Summary Report by Server. For more information about the transaction information contained in this report, see “Transaction Summary Report by Server” on page 253.

RRM Audit Report

The RRM Audit Report summarizes the dates and changes when the configuration of the RRM server was modified. This report is generated by typing Option 3 and pressing ENTER on the Summary/Statistics Reports menu.

Use this report to manage configuration changes to RRM files. The figure below shows an example of the RRM Audit Report.

This report includes the following header and configuration information.

Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.
Configuration Information

Selection Criteria
The selection criteria used to generate this report.

- **From Date/Time** - The starting date and time of the period when configuration data was gathered.
- **To Date/Time** - The ending date and time of the period when configuration data was gathered.
- **Filter name** - The name of the filter that was selected to generate the report. *NONE means that no filter was used.
- **Filter criteria** - If a filter is defined, the following search criteria for each record is displayed: AND/OR, Field Name, Operator Value, and Value.

**TimeStamp**
The date and time when the values for the indicated function were changed, in the format year-month-day-hour-minutes-seconds-milliseconds.

**User**
The user who made the change.

**Function**
The default value of the function that was changed.

**Before**
The settings of the function before the change occurred.

**After**
The settings of the function after the change occurred.

Collected Entries Report

The Collected Entries Report provides details about all RRM collected entries. This report is generated by typing Option **11** and pressing ENTER on the Summary/Statistics Reports menu.
Use this report to manage access to RRM based on collected entries. The figure below shows an example of the Collected Entries Report.

<table>
<thead>
<tr>
<th>Obj Path</th>
<th>Func.</th>
<th>Cmd.</th>
<th>User</th>
<th>Network</th>
<th>R Time Stamp</th>
<th>Trans Cnt</th>
<th>Rsn Time Stamp</th>
</tr>
</thead>
</table>

This report includes the following header and configuration information.

**Header Information**

- **report title**
  The title of the report.

- **date**
  The date when the report was generated in the user’s job date format.

- **time**
  The time when the report was generated in the format *hh:mm:ss*.

- **page**
  The current page number of the report.
### Collected Entry Information

**Rsn**

This column provides the RRM Collection reason code for the transaction. The following codes represent how RRM handles transaction requests based on the rules you created. If a transaction has been collected multiple times with different reason codes, then more than one entry will be displayed in this column.

- **A** = The transaction was allowed by RRM.
- **R** = The transaction was rejected by RRM.
- **U** = The transaction was unsecured by RRM. Unsecured transactions are rejected because an RRM rule does not exist for the transaction, therefore the default action is to reject the transaction.

RRM sets the reason code based on the user-defined rules regardless of the secured mode setting. If security is not turned on you can use the reason code to determine how RRM would handle the transaction if the exit point were secured. If the exit point is secured then the reason code indicates if the transaction was allowed or rejected by RRM.

**Server**

The name assigned by RRM to the server where the remote request originated.

**Func**

The function requested in the transaction. If the TELNET/INIT server/function is included in the transaction, a user profile is not displayed unless the Autosignon function was used during initialization of the TELNET session.

**Cmd**

The command requested in the transaction. Most transactions do not include a command.

**User**

The name of the user profile used by the server job to submit the remote request.
Network
The network address where the request originated. This can be device name, system name, or an IP address.

R
This column displays the most recent reason code collected for this transaction. This value corresponds to the entry in the Time Stamp field.

A = The transaction was allowed by RRM
R = The transaction was rejected by RRM
U = The transaction was unsecured by RRM
blank = The most recent reason code is being determined.

Collection data must be completely processed before this field displays the appropriate code. Press F5 (Refresh) to update this field.

TimeStamp
The time when the transaction was received by RRM, in YYYY-MM-DD-HH.MM format, in descending order.

Trans Cnt
The total number of transactions collected for the Server/Function/Command/User/Network combination.

Obj Rsn
The reason code associated with the collected object.

Obj Time Stamp
The time when the transaction specific to the object was received by RRM, in YYYY-MM-DD-HH.MM format, in descending order.

Obj Path
The name of the collected object shown in IFS notation.
What If Reports

RRM provides the following What If reports:

• What If Transaction by Date/Time
• What If Transaction by User
• What If Transaction by Function
• What If Transaction by Server
• What If Transaction by Address

Before you generate these reports, execute the What If Playback function to ensure that the reports are generated with current data (see “Playback What If Transaction Database” on page 157). Then, the reports can be generated by executing options on the What If Reports menu.

What If Transactions by Date/Time

The What If Transactions by Date/Time report lists RRM What If transactions sorted by date and time. This report is generated by typing Option 1 and pressing ENTER on the What If Reports menu.
Use this report to review the effects of What If transactions sorted by date and time. The figure below shows an example of the What If Transactions by Date/Time report.

**Note**

Execute the What If Playback function before you generate the report (see “Playback What If Transaction Database” on page 157).

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information in this report, see “FTP Logon and Server Requests” on page 222.
Transaction Information

----- What If -----

Selection Criteria
The selection criteria associated with the request.

- **From Date/Time** - The starting date and time of the period when transactions were reported.
- **To Date/Time** - The ending date and time of the period when transactions were reported.
- **Filter name** - The name of the filter that was selected to generate the report. *NONE means that no filter was used.
- **Filter criteria** - If a filter is defined, the following search criteria for each record is displayed: AND/OR, Field Name, Operator Value, and Value.

Date
The date when the secured entry was copied to a What If file.

Time
The time when the secured entry was copied to a What If file.

Incoming User
The name of the user associated with the transaction.

Incoming Address
The address where the transaction originated.

Operations
Information about the resources used to execute the transaction.

- **Server** - The server used to execute the transaction.
- **Function** - The function used to execute the transaction.
- **Command** - The command used to execute the transaction.

RRM P/F
The pass/fail status (P=Pass, or F=Fail) of the transaction and any customer exit programs after the transaction has been processed by RRM.
DMA P/F
The pass/fail status (P=Pass, or F=Fail) of the transaction after it has been processed by the RRM Decision-making Algorithm.

Swap Profile
The swap profile used to execute the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming user.

----- Secure ------

Date
The date when the secured entry was copied to a What If file in the user’s job-date format.

Time
The time when the secured entry was copied to a What If file in the format hh:mm:ss.

RRM P/F
The pass/fail status (P=Pass, or F=Fail) of the transaction and any customer exit programs after the transaction has been processed by RRM.

DMA P/F
The pass/fail status (P=Pass, or F=Fail) of the transaction after it has been processed by the RRM Decision-making Algorithm.

Swap Profile
The swap profile used to execute the job. If a transaction has a swap profile, the transaction is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming user.

What If Transaction by User
The What If Transaction by User report lists RRM What If transactions sorted by user. This report is generated by typing Option 2 and pressing ENTER on the What If Reports menu.
Use this report to review the effects of What If transactions by user that occurred on the RRM server. The figure below shows an example of the What If Transaction by User report.

**Note**
Execute the What If Playback function before you generate the report (see “Playback What If Transaction Database” on page 157).

This report includes the following header and transaction information.

### Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests report. For more information about the header information in this report, see “FTP Logon and Server Requests” on page 222.

### Transaction Information

This report includes the same types of transaction information shown on the What If Transaction by Date/Time report. For more information about the transaction information contained in this report, see “What If Transactions by Date/Time” on page 263.
What If Transaction by Function

The What If Transaction by Function report lists RRM What If transactions sorted by function. This report is generated by typing Option 3 and pressing ENTER on the What If Reports menu.

Use this report to review the effects of What If transactions by function that occurred on the RRM server. The figure below shows an example of the What If Transaction by Function report.

Note

Execute the What If Playback function before you generate the report (see “Playback What If Transaction Database” on page 157).

This report includes the following header and transaction information.

Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information in this report, see “FTP Logon and Server Requests” on page 222.
Transaction Information

This report includes the same types of transaction information shown on the What If Transaction by Date/Time report. For more information about the transaction information contained in this report, see “What If Transactions by Date/Time” on page 263.

What If Transaction by Server

The What If Transaction by Server report lists RRM What If transactions sorted by server. This report is generated by typing Option 4 and pressing ENTER on the What If Reports menu.

Use this report to review the effects of What If transactions sorted by server. The figure below shows an example of the What If Transaction by Server report.

Note

Execute the What If Playback function before you generate the report (see “Playback What If Transaction Database” on page 157).

This report includes the following header and transaction information.
Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information in this report, see “FTP Logon and Server Requests” on page 222.

Transaction Information

This report includes the same types of transaction information shown on the What If Transaction by Date/Time report. For more information about the transaction information contained in this report, see “What If Transactions by Date/Time” on page 263.

What If Transaction Summary by Incoming Address

The What If Transaction by Incoming Address report lists RRM What If transactions sorted by incoming address. This report is generated by typing Option 5 and pressing ENTER on the What If Reports menu.
Use this report to review the effects of What If transactions by incoming address. The figure below shows an example of the What If Transaction by Incoming Address report.

**Note**

Execute the What If Playback function before you generate the report (see “Playback What If Transaction Database” on page 157).

---

Note

Execute the What If Playback function before you generate the report (see “Playback What If Transaction Database” on page 157).

---

This report includes the following header and transaction information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information in this report, see “FTP Logon and Server Requests” on page 222.

**Transaction Information**

This report includes the same types of transaction information shown on the What If Transaction by Date/Time report. For more information about the transaction information contained in this report, see “What If Transactions by Date/Time” on page 263.
Configuration Reports

RRM provides the following Configuration reports:

- Secured Entries Report
- Exit Point Settings Report
- User Groups Report
- Address Groups Report
- Function Groups Report
- Calendar Report
- Remote Object Authority by User Report
- Remote Object Authority by Path Report

You can generate these reports by executing options on the Configuration Reports menu.

Secured Entries Report

The Secured Entries report lists the secured entries included in the current RRM configuration. This report is generated by typing Option 1 and pressing ENTER on the Configuration Reports menu.

Use this report to manage changes to secured entries on the RRM server. The figure below shows an example of the Secured Entries report.
The presence of a right angle bracket (>) on the right side of an entry indicates that the entry is associated with an object.

This report includes the following header and secured entry information.

### Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

### Secured Entry Information

#### Selection Criteria

The following selection criteria was used to gather data:

- **Filter name** - The name of the filter that was selected to generate the report. *NONE means that no filter was used.
- **Filter criteria** - If a filter is defined, the following search criteria for each record is displayed: AND/OR, Field Name, Operator Value, and Value.

#### User/Group

The user or user group associated with the secured entry. Group names begin with a colon (:).
Address
The address associated with the secured entry.

Operation
The operation associated with the secured entry.

Action
The action associated with the secured entry.

Swap Profile
The profile used to execute the job. If a transaction has a swap profile, the transaction is executed using the swap profile instead of the profile associated with the incoming user.

Enabled
Whether the swap profile specified for the transaction is enabled (*YES or *NO)

Path
The path for objects associated with the secured entry.

Exit Point Settings Report

The Exit Point Settings report lists the exit point settings in the current RRM configuration. This report is generated by typing Option 1 and pressing ENTER on the Configuration Reports menu.
Use this report to manage changes to RRM exit point settings. The figure below shows an example of the Exit Point Settings report.

This report includes the following header and exit point information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.
Exit Point Information

Exit Point
The name of the exit point.

Format
The format of the exit point.

Secure Mode
Whether the exit point function that restricts access to incoming requests is enabled (*YES) or disabled (*NO).

Collect Mode
The collection mode specified for the selected exit point. The following values are valid:

- *All - All incoming entries are collected.
- *None - No incoming entries are collected.
- *Reject - Rejected entries only are collected.
- *Unsecured - Unsecured entries only are collected.

Exit Program
The exit program associated with this exit point.

Customer Exit
The exit program provided by the customer that is invoked by the NetIQ Security Solutions for iSeries exit program associated with this exit point.

Customer Exit Lib
The library that contains any customer exit programs associated with this exit point.

Prm Grp
Whether the primary group should be searched (*Yes/*No).

Sup Grp
Whether supplemental groups should be searched (*Yes/*No).

RRM Grp
Whether RRM groups should be searched (*Yes/*No).
Swap Prf
Whether use of a swap profile is allowed (*Yes/*No).

Parse Depth
The maximum number of objects to be parsed (0-99).

Log TA
Whether you want What If Playback transactions to be logged (*Yes/*No). To log What If Playback transactions, you must specify *Yes in this field.

Log TAP
Whether you want transactions that were processed and passed to be logged (*Yes/*No).

Log TAF
Whether you want transactions that were processed and failed to be logged (*Yes/*No).

Log ObP
Whether transactions with objects that were processed and passed should be logged (*Yes/*No).

Log ObF
Whether transactions with objects that were processed and failed should be logged (*Yes/*No).

Secured Entry Information

Exit Point
The name of the exit point.

Format
The format of the exit point.

Server
The server where the exit point resides.

Description
more information about the exit point.
User Groups

The User Group report lists the user groups included in the current RRM configuration. This report is generated by typing Option 2 and pressing ENTER on the Configuration Reports menu.

Use this report to manage changes to user groups on the RRM server. The figure below shows an example of the User Group report.

This report includes the following header information and user group information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.
User Group Information

Selection Criteria
The selection criteria used to gather data:

- **From Date/Time** - The starting date and time of the period when data was reported.
- **To Date/Time** - The ending date and time of the period when data was reported.
- **Filter name** - The name of the filter that was selected to generate the report. *NONE means that no filter was used.
- **Filter criteria** - If a filter is defined, the following search criteria for each record is displayed: **AND/OR**, **Field Name**, **Operator Value**, and **Value**.

Group Entity
The user group or entity reported. Group names begin with a colon (:).

Description
more information about the entity or user group.

Status
Whether the selected user profile is enabled or disabled.

Expiration
The date when the selected user profile will be disabled.

Limit Capability
Whether you want to limit the capability of the selected user profile.

Special Authorities
Whether the following special authorities are granted (Y = yes or N = no):

- **ALL** = **ALLOBJ** - ALL object special authority.
- **AUD** = **AUDCTL** - Auditing control special authority.
- **IOS** = **IOSYSCFG** - System configuration special authority.
- **JOB** = **JOBCTL** - Job control special authority.
- **SAV** = **SAVSYS** - Save system control special authority.
- SEC = SECADM - Security administrator special authority.
- SRV = SERVICE - Service control special authority.
- SPL = SPLCTL - Spool control special authority.

Network Groups

The Network Groups report lists the network address groups included in the current RRM configuration. This report is generated by typing Option 3 and pressing ENTER on the Configuration Reports menu.

Use this report to manage changes to address groups on the RRM server. The figure below shows an example of the Network Groups report.

This report includes the following header and network address group information.

Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.
Network Group Information

Selection Criteria
The selection criteria used to gather data:

• **From Date/Time** - The starting date and time of the period when data was reported.

• **To Date/Time** - The ending date and time of the period when data was reported.

• **Filter name** - The name of the filter that was selected to generate the report. *NONE means that no filter was used.

• **Filter criteria** - If a filter is defined, the following search criteria for each record is displayed: AND/OR, Field Name, Operator Value, and Value.

Group Entity
The user group or entity reported. Group names begin with a colon (:).

Description
more information about the selected network address group.

Operation Groups

The Operation Groups report lists the operation groups included in the current RRM configuration. This report is generated by typing Option 4 and pressing ENTER on the Configuration Reports menu.
Use this report to manage changes to operation groups on the RRM server. The figure below shows an example of the Operation Group report.

This report includes the following header and operation group information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Operation Group Information**

This report includes the same types of header information shown on the Network Groups report. For more information about the header information contained in this report, see “Network Groups” on page 280.

**Calendars**

The Calendar report lists the calendars included in the current configuration of RRM. This report is generated by typing Option 5 and pressing ENTER on the Configuration Reports menu.
Use this report to manage changes to calendars on the RRM server. The figure below shows an example of the Calendar report.

<table>
<thead>
<tr>
<th>Calender Name</th>
<th>Default</th>
<th>Start Time</th>
<th>End Time</th>
<th>Sunday</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Saturday</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>EHD</td>
<td><em>PASS</em></td>
<td>8:00</td>
<td>17:00</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td><em>PASS</em></td>
</tr>
</tbody>
</table>

This report includes the following header and calendar information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Calendar Information**

**Selection Criteria**

The selection criteria used to gather data:

- **From Date/Time** - The starting date and time of the period when data was reported.
- **To Date/Time** - The ending date and time of the period when data was reported.
• **Filter name** - The name of the filter that was selected to generate the report. *NONE means that no filter was used.

• **Filter criteria** - If a filter is defined, the following search criteria for each record is displayed: AND/OR, Field Name, Operator Value, and Value.

**Calendar Name**
The name of the selected calendar.

**Default Action**
The default action to be taken (*PASS or *FAIL) if a matching calendar file cannot be found.

**Start Time**
The starting time for a specified period when the calendar is in effect.

**End Time**
The ending time for a specified period when the calendar is in effect.

**Sunday**
Whether the period specified by the calendar includes Sunday.

**Monday**
Whether the period specified by the calendar includes Monday.

**Tuesday**
Whether the period specified by the calendar includes Tuesday.

**Wednesday**
Whether the period specified by the calendar includes Wednesday.

**Thursday**
Whether the period specified by the calendar includes Thursday.

**Friday**
Whether the period specified by the calendar includes Friday.

**Saturday**
Whether the period specified by the calendar includes Saturday.

**Action**
The action (*PASS or *FAIL) associated with this calendar.
Remote Object Authority By User

The Remote Object Authority By User report shows the remote object authority records listed in the Remote Object Authority Table, sorted by user. This report is generated by typing Option 6 and pressing ENTER on the Configuration Reports menu.

Use this report to manage remote access to objects on the RRM server. For more information about remote object authority, see “Remote Object Authority” on page 28. The figure below shows an example of the Remote Object Authority By User report.

This report includes the following header and authority information.

Header Information

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.
Authority Information

Selection Criteria
The selection criteria associated with the request.

- **Filter name** - The name of the filter that was selected to generate the report. "NONE means that no filter was used.

- **Filter criteria** - If a filter is defined, the following search criteria for each record is displayed: **AND/OR, Field Name, Operator Value, and Value.**

User Name
The name of the user ID associated with the remote object authority record.

Path
The path of the remote object.

Read:
Authority to read a file (indicated by an “X”).

Write:
Authority to change a file (indicated by an “X”).

Execute:
Authority to execute a program or command (indicated by an “X”).

Operation:
Authority to create or delete a file (indicated by an “X”).

Secure:
Whether the object is secured (Y=yes or N=no).

Remote Object Authority By Path

The Remote Object Authority By Path report shows the remote object authority records listed in the Remote Object Authority Table, sorted by path. This report is generated by typing Option 7 and pressing ENTER on the Configuration Reports menu.
Use this report to manage remote access to objects on the RRM server. For more information about remote object authority, see “Remote Object Authority” on page 28. The figure below shows an example of the Remote Object Authority By Path report.

This report includes the following header and authority information.

**Header Information**

This report includes the same types of header information shown on the FTP Logon and Server Requests Report. For more information about the header information contained in this report, see “FTP Logon and Server Requests” on page 222.

**Authority Information**

This report includes the same types of authority information shown on the Remote Object Authority By User report. For more information about the authority information contained in this report, see “Remote Object Authority By User” on page 285.
This collection of usage scenarios is provided to introduce you to some of the major functions of RRM. These scenarios present typical situations that you might encounter using RRM, and demonstrate how to use RRM to manage them. Each scenario presents one method of accomplishing its intended purpose. For each scenario, however, multiple methods can be used to accomplish the same task.

**Allow FTP Only Between Multiple iSeries Servers**

This scenario relies on grouping and does not require object authority records. All FTP activity that cannot be controlled by this scenario must be prevented with a rule such as Network=*ALL, User=*PUBLIC, *ALL, Operation=:FTP, Action=*FAIL, Secure=Y.

To allow FTP only between multiple iSeries servers:

1. Create a network group and put the network addresses for all iSeries computers in the group by performing the following steps:
   a. On the RRM Main menu, type 3 and press ENTER.
   b. Type 2 and press ENTER.
   c. Press F6 (Create Group). The detailed view of the Work With Networks screen is displayed.
d. In the **Name** field, type the name of the network group you are adding.

e. In the **Description** field, type a description of the network group you are adding.

f. Press ENTER.

g. When prompted, press ENTER again.

h. Add the network addresses for all desired iSeries systems to this group.

2. For all FTP client functions, create a secured entry that includes User=*PUBLIC and the network group created in Step 1. Perform the following steps:

   a. On the RRM Main menu, type `1` and press ENTER.

   b. Press F6 (Add).

   c. In the **User** field, type *PUBLIC.

   d. In the **Network** field, type the network group created in Step 1.

   e. In the **Operation** field, type FTPCLT_*ALL.

   f. In the **Action** field, type *PASS.

   g. In the **Secure Status** field, type Y.

   h. Press ENTER.

   i. When prompted, press ENTER again.

3. For all FTP server functions, create a secured entry that includes User=*PUBLIC. Perform the following steps:

   a. Press F6 (Add).

   b. In the **User** field, type *PUBLIC.

   c. In the **Network** field, type *ALL.

   d. In the **Operation** field, type :FTP.

   e. In the **Action** field, type *FAIL.
f. In the **Secure Status** field, type Y.

g. Press ENTER.

h. When prompted, press ENTER again.

4. Set the exit point for the FTP client to Secured=*Yes by performing the following steps:

   a. On the RRM Main menu, type 8 and press ENTER.

   b. Beside the exit point QIBM_QTMF_CLIENT_REQ, type 2 (Edit) and press ENTER.

   c. In the **Secured** field, type *Yes and press ENTER.

5. For exit point QIBM_QTMF_SERVER_REQ, repeat Step b and Step c.

The secured entries that were created by this process are shown in the following figure.
Restrict Security Officer Activities on a remote PC

If you want to restrict security officer authority (QSECOFR) so that it can only be used to work from a local terminal, you can accomplish this by creating user/server override records that exclude QSECOFR from the specified server(s).

Note
User/server overrides do not check members of groups. To restrict QSECOFR, all its members, and any other profiles with security officer authority, see “Restrict Activities of QSECOFR and All its Members” on page 293.

To restrict security officer activities on a remote PC:

1. On the RRM Main menu, type 6 and press ENTER.


3. In the User field, type QSECOFR.

4. In the Server field, specify the server where you want to restrict the user’s actions. A value of *ALL will restrict all activity beyond a twinax-connected terminal.

5. In the Action field, type *FAIL. This value will reject all requests submitted by the user to the specified server(s).

6. Press ENTER.

7. When prompted, press ENTER again.

If you want to use the QSECOFR profile to perform some tasks remotely, remove the user/server override for QSECOFR on the appropriate server(s). If *ALL was specified for a user/server override, you must delete this override and replace it with a more specific user/server override.
Restrict Activities of QSECOFR and All its Members

If you want to restrict the activities of QSECOFR, all its members, and any other profiles with security officer authority, you can accomplish this by creating a secured entry.

To restrict security officer activities on a remote PC:

1. On the RRM Main menu, type 1 and press ENTER.
2. In the User field, type QSECOFR.
3. In the Network field, type *ALL.
4. In the Operation field, type *ALL.
5. In the Action field, type *FAIL.
6. In the Secure Status field, type Y.
7. Press ENTER.
8. When prompted, press ENTER again.
9. On the Work With Exit Points screen, for each exit point listed, set the Check Primary Group and the Check Supplemental Groups fields to *YES.

Prevent the Addition of Objects to a Library

In this scenario, a secured entry with an object authority record is used to prevent objects from being added to a specified library or directory.

To prevent the addition of objects to a library:

1. On the RRM Main menu, type 1 and press ENTER.
2. Press F6 (Add).
3. In the **User** field, type *PUBLIC.

4. In the **Network** field, type *ALL.

5. In the **Operation** field, type :CRTOBJ.

6. In the **Object Path** field, press F21 (Drill Obj) to display the Work With RRM Object Authorities screen, and perform the following steps:
   a. Locate the appropriate object path.
   b. If the object path is not listed, press F6 to add it.
   c. Type 1 in entry field beside the object path and press ENTER.

7. In the **Action** field, type *FAIL.

8. In the **Secure Status** field, type Y.

9. Press ENTER.

10. When prompted, press ENTER again. The resulting secured entry is shown in the following figure.

```
NW0015B  Work With Secured Entries  15:43:28  10/30/2008
ANYSERVER

User . . . . . . . . . . . . . . . . *PUBLIC + Name, :Group, *PUBLIC
Network . . . . . . . . . . . . . . . . *ALL            +
Operation . . . . . . . . . . . . . . . . :CRTOBJ            +
Object Path . . . . . . . . . . . . . . . /QSYS.LIB/PAYROLL.LIB
Action . . . . . . . . . . . . . . . . *FAIL        + *PASS, *FAIL, *OBJLIST, cal
Swap Profile . . . . . . . . . . . . . . .            Name
Enabled Status . . . . . . . . . . . . . . . . Y + Y, N

F1=Help         F3=Exit         F4=Prompt         F5=Refresh
F12=Cancel      F19=Rmv Obj     F20=Edit Obj      F21=Drill Obj      F22=Disp Obj
```
Enforce Read-Only Access to a Library

In this scenario, a secured entry with an object authority record is used to enforce read-only access to a specified library or directory. This scenario assumes that no other rules exist that grant access to objects with the selected object path (/QSYS.LIB for this example).

To enforce read-only access to files in a library:

1. On the RRM Main menu, type 1 and press ENTER.
2. Press F6 (Add).
3. In the User field, type *PUBLIC.
4. In the Network field, type *ALL.
5. In the Operation field, type :READONLY.
6. In the Object Path field, press F21 (Drill Obj) to display the Work With RRM Object Authorities screen, and perform the following steps:
   a. Locate the appropriate object path.
   b. If the object path is not listed, press F6 to add it.
   c. Type 1 in entry field beside the object path and press ENTER.
7. In the Action field, type *PASS.
8. In the Secure Status field, type Y.
9. Press ENTER.

10. When prompted, press ENTER again. The resulting secured entry is shown in the following figure.

```
NW0015B                   Work With Secured Entries       12:01:45   9/08/2008
ISR24                       Add

User . . . . . . . . . . . . . . *PUBLIC   + Name, :Group, *PUBLIC
Network . . . . . . . . . . . . . . *ALL        +
Operation . . . . . . . . . . . :READONLY   +
Object Path . . . . . . . . . . . /QSYS.LIB
Action . . . . . . . . . . . . . . *PASS       + *PASS, *FAIL, *OBJLIST, cal
Swap Profile . . . . . . . . . . . Name
Enabled Status . . . . . . . . . Y + Y, N

F1=Help         F3=Exit         F4=Prompt       F5=Refresh
F12=Cancel      F20=Edit Obj    F21=Drill Obj
```

**Prevent *ALLOBJ Users From Accessing a File**

In this scenario, a secured entry and an object authority record are used to prevent users with *ALLOBJ authority from accessing a file.

To prevent *ALLOBJ users from accessing a file remotely:

1. On the RRM Main menu, type 3 and press ENTER.
2. Type 1 and press ENTER.
3. Press F6 (Create Group) to display the detail view of the Work With Users screen, and perform the following steps:

   a. In the Name field, type \texttt{:ALLOBJ}.

   b. In the Description field, type \texttt{*ALLOBJ Users}.

   c. Press ENTER.

   d. When prompted, press ENTER again.

   e. On the Work With Users screen, list all profiles that have \texttt{*ALLOBJ} authority and place them in the :ALLOBJ group.

   f. Press F12 until the RRM Main menu is redisplayed.

4. On the RRM Main menu, type \texttt{1} and press ENTER.

5. Press F6 (Add).

6. In the User field, type \texttt{:ALLJOB}.

7. In the Network field, type \texttt{*ALL}.

8. In the Operation field, type \texttt{*ALL}.

9. In the Object Path field, use the default value \texttt{*NONE}.

   To specify a library or directory containing an object, press F21 (Drill Obj) to display the Work With RRM Object Authorities screen and perform the following steps:

   a. Locate the appropriate object path.

   b. If the object path is not listed, press F6 to add it.

   c. Type \texttt{1} in entry field beside the object path and press ENTER.

10. In the Action field, type \texttt{*FAIL}.

11. In the Secure Status field, type \texttt{Y}.
12. Press ENTER.

13. When prompted, press ENTER again. The resulting secured entry is shown in the following figure.

Find and Disable a Virus

In this scenario, a Nimda virus infected files in the Integrated File System (IFS) through a remote PC. When other remote PC users accessed the infected objects in the IFS, the virus was spread throughout the organization.

By running an RRM report to list the objects that have been accessed, you can identify all the PCs that were used to access the infected object.
To find and disable virus:

1. Using a powerful profile whose special authorities include *ALLOBJ or *SECADM, map a drive to the IFS from any PC.

2. Using your antivirus software, scan the IFS for the infected object.

3. If an infected object is found, record the path for reference.

4. On an iSeries command line, run the RRM Object Report by Object and identify the users who have accessed the infected files.

5. Find and record all entries with an object path that matches the path of the infected file.

6. Give your network support group the list of infected computers so that those computers can be cleaned.
Chapter 7
Operations Navigator Plug-in

The Operations Navigator plug-in for RRM lets you perform RRM functions from a Windows interface using the IBM Operations Navigator. This chapter describes the appearance and operation of the RRM plug-in within the Operations Navigator environment.

Operations Navigator is included as part of IBM’s Client Access Express for Windows. For more information about Operations Navigator, see the appropriate IBM documentation.

Additional information about each RRM function provided through the Operations Navigator GUI is available in other chapters of the NetIQ Security Solutions for iSeries RRM User Guide.

Features

The Operations Navigator plug-in for RRM has the following features:

- Provides an easy-to-use Windows user interface that facilitates the management and administration of iSeries and iSeries servers.
- Provides the same functions as PSSecure 7.0/RRM, but with additional ease of use.
- Lets you import the configuration and secured entries from one environment to the What If environment of one or more other servers. This capability significantly reduces the time required to secure multiple servers, and reduces errors caused by manually configuring multiple servers.
Functions

Through the Operations Navigator plug-in for RRM, you can perform the following types of RRM functions:

- Collected Environment
- Secured Environment
  - Entries
  - RRM Groups
  - Object Authorities
  - Calendars
  - User/Server Overrides
  - User/Object Overrides
  - Exit Points

- What If Environment
  - Entries
  - RRM Groups
  - Object Authorities
  - Calendars
  - User/Server Overrides
  - User/Object Overrides
  - Exit Points
• Reports
  - Report List
  - Output

• Administration
  - Tools
  - RRM Defaults
  - User Message Alert

Documentation


The rest of the RRM documentation describes the functioning and appearance of RRM in the 5250 (“green screen”) environment, and explains other important aspects of the product. For additional information about understanding and using RRM, see the other chapters and sections of the NetIQ Security Solutions for iSeries Remote Request Management User Guide.
Operations Navigator GUI

The graphical user interface (GUI) provided with the Operations Navigator plug-in for RRM consists of the List Pane, Detail Pane, and the Environmental Pane.
List Pane

The List Pane, in the upper left portion of the GUI, displays the Operations Navigator directory tree. The List pane contains the primary i5/OS environment where RRM is being operated. The RRM Plug-in is accessed from this pane by clicking the PentaSafe Security icon in the directory tree.

Directory Tree

The directory tree in the Operations Navigator GUI is operated by clicking (left mouse button) and right-clicking (right mouse button) icons and entries, and selecting options from associated pull-down menus.

Click Options

Clicking an icon or entry expands the directory tree by listing its contents in the Detail Pane.

When some icons are clicked, a filter is displayed that lets you specify criteria for gathering and listing information. If no criteria is specified, all existing entries of the type selected are listed.

Right-click Options

Right-clicking an icon or entry lists the available options on a pull-down menu. A listed option can be executed by selecting it.

Detail Pane

The Detail Pane, in the upper right portion of the GUI, displays the contents of the item selected in the Environment List pane. When you click a folder in the List pane, the processing icon is displayed to show that the requested information is being gathered.
When the information has been gathered, the contents of the icon that was clicked in the List Pane is shown in the Detail Pane. In the Detail Pane, you can perform actions to display and manage the selected information.

**Environment Pane**

The *Environment Pane*, in the lower portion of the GUI, lists tasks that you can perform to configure your current i5/OS environment.

**Collected Environment**

The *Collected* icon represents the RRM Collected Environment. The Collected Environment contains remote transaction data, and provides functions to manage the data.

For more information about the Collected Environment, see “Work with Collected Entries” on page 101.
Right-click Options

By right-clicking Collected, the following functions are available:

**Explore**
Displays the Collected environment configuration in the Detail Pane.

**Open**
Displays the Collected environment configuration in a new window.

**Create Shortcut**
Creates a shortcut to the Collected environment on the selected server and places it on your desktop.

**Start RRM Collection Monitor**
Displays the Start/Stop Collection Monitor dialog box, which lets you start the Collection Monitor. This action causes RRM to start collecting transactions.

**Stop RRM Collection Monitor**
Displays the Start/Stop Collection Monitor dialog box, which lets you stop the Collection Monitor. This action causes RRM to stop collecting transactions.

**Note**
If one or more exit points are configured to collect remote transaction information and the Collection Monitor is not running, the transaction data will be queued and retained until the collection monitor is started. However, if the collection queue is filled before the Collection Monitor is started, the collection queue will wrap and lose information.

**Filter Entries**
Displays the Collected Entries Filter dialog box, which lets you specify filter criteria for selecting entries.

Click Options

By clicking Collected, the Define Collected Entries Filter dialog box is displayed for use in selecting Collected Entries (see “Collected Entries Filter” on page 309). After the filter is applied, Collected Entries are listed. Each time Collected Entries are listed, the same filter criteria is used until new filter criteria is specified.
Available Options

By right-clicking **Collected**, the following options are available:

**View Objects**
- Displays the View Objects for Collected Entry dialog box, which lists the objects associated with the selected entry.

**Delete**
- Displays a confirmation dialog box to verify whether you want to delete the selected entries.

**Create Secured Entry**
- Displays the Create Entry dialog box, which lets you create one or more Secured Entries from one or more Collected Entries.

**Create What If Entry**
- Displays the Create Entry dialog box, which lets you create a Secured Entry in the What If Entry environment from a Collected Entry.

**Filter**
- Displays the Collected Entries Filter dialog box, which lets you specify criteria for listing Collected Entries.
Collected Entries Filter

The first time you click the Collected icon or right-click a Collected Entry and select Filter, the Define Collected Entries Filter dialog box is displayed. This dialog box lets you specify the criteria to use for listing Collected Entries. When the filter is applied, the requested Collected Entries are listed in the Detail Pane of the GUI. If no selection criteria are specified, all Collected Entries are listed.

The Define Collected Entries Filter dialog box includes the following fields:

**Value Filters**
Filter criteria that specifies the operation and user.

- **Server**
  A list of possible names of the server where the request originated.

- **Function**
  A list of possible functions requested in the transaction.

- **Command**
  A list of possible commands requested in the transaction.
User
A list of possible names of users who submitted the request.

Reason
The reason why the entry was collected by the Collection Monitor.

Date Range Filter
Filter criteria that specifies the date range for which you want Collected Entries.

From Date/Time
The beginning date and time of the period for which you want Collected Entries. The following values are valid:

*PRVMS - The previous month's starting date.
*PRVME - The previous month's ending date.
*PRVWK - The previous week's starting date (last 7 days).
*PRVDY - The previous day’s date.
*CURMS - The current month’s starting date.
*CURR - The current date.

actual date and time - Type the date and time in the YYYY/MM/DD and HH:MM:SS formats, where YYYY is the four-digit year, MM is the month, DD is the day, HH is the hour in 24-hour time, MM is the minute, and SS is the second.

To Date/Time
The ending date and time of the period for which you want Collected Entries. The following values are valid:

*PRVMS - The previous month's starting date.
*PRVME - The previous month's ending date.
*PRVWK - The previous week's starting date (last 7 days).
*PRVDY - The previous day’s date.
*CURMS - The current month’s starting date.
*CURR - The current date.

**actual date and time** - Type the date and time in the YYYY/MM/DD and HH:MM:SS formats, where YYYY is the four-digit year, MM is the month, DD is the day, HH is the hour in 24-hour time, MM is the minute, and SS is the second.

**Help**
Displays a window containing Help information.

**Apply**
Applies the selection criteria you specify for selecting Collected Entries.

**Cancel**
Closes the dialog box and applies the previously defined filter criteria, or no filter criteria if this is the first time in this session that the dialog box was displayed.

**View Objects**
If you double-click a Collected Entry, the Work With Collected Entry Objects dialog box is displayed. Use this dialog box to maintain objects associated with Collected Entries.

The Work With Collected Entry Objects dialog box includes the following fields:
Collected Objects

By clicking the following buttons, you can perform the corresponding actions to the collected objects you select:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Set Remote Object Authority" /></td>
<td>Displays the Maintain Remote Object Authority dialog box, which lets you manage the Remote Object Authorities of the selected object.</td>
</tr>
<tr>
<td><img src="image" alt="Add User/Object Override" /></td>
<td>Displays the User/Object Override dialog box, which lets you add a User/Object Override for the selected object.</td>
</tr>
<tr>
<td><img src="image" alt="Remove Object from Collected Entry" /></td>
<td>Displays a confirmation dialog box to verify whether you want to delete the selected object.</td>
</tr>
<tr>
<td><img src="image" alt="View Full Path" /></td>
<td>Displays the View Full Path window, which shows the full path of the selected object. Use this function when the object exceeds the maximum value for the window.</td>
</tr>
</tbody>
</table>

**collected object pane**

Lists the objects associated with the selected entry.

**Help**

Displays a window containing Help information.

**Close**

Closes the dialog box.

**Create Entry**

If you right-click a Collected Entry and select Create Secured Entry or Create What If Entry, the Create Entry dialog box is displayed. Depending on the option selected, this dialog box lets you create a Secured or What If Entry from a Collected Entry. To indicate the type of entry created, “Secured Environment” or “What If Environment” is displayed in the title of the dialog box.
All newly created or modified entries must have a unique key (user/network address/operation), or they cannot be saved.
The Create Entry dialog box includes the following fields:

**User or Group**
The RRM user or user group to which the entry applies. The pull-down list contains the currently defined users. You can select a user or user group from the list, or you can specify a new name if the **Add new user if necessary** option is checked.

**Network**
The network (IP) address to which this entry applies. The pull-down list contains the currently defined network addresses. You can select a network address from the list, or you can specify a new network address if the **Add new network if necessary** option is checked.

**Operation**
The operation to which the entry applies. The pull-down list contains the currently defined operations. You can select an operation from the list.

**Object Path**
The object path to which the entry applies.

**object browser button**
Displays the Browse Object dialog box, which lets you browse for the path of the object associated with the entry being created.

**Action**
The action taken when a remote request finds a matching Secured Entry. The following values are valid:

- ***PASS** - The remote request succeeds.
- ***FAIL** - The remote request fails.
- ***OBJLIST** - The Remote Object Authority tables are searched to determine if the user is authorized to access the object.
- **calendar** - The name of the calendar associated with the Secured or What If Entry. The calendar applies additional selection criteria based on the day of the week and time of day when the request is received.
Swap Profile
The profile used to execute the remote request. If a request has a swap profile, the request is executed using the authority of the swap profile instead of the authority of the profile associated with the incoming user.

Enabled Status
Whether the decision-making process that controls remote request access to RRM is enabled or disabled for the selected entry. The following values are valid:

Enabled
The decision-making process that controls remote request access is turned on for the selected entry.

Disabled
The decision-making process that controls remote request access is turned off for the selected entry.

Add new user or group if necessary
When selected, this option lets you dynamically create a new RRM user or user group from the value specified in the User field.

Add new network if necessary
When selected, this option lets you dynamically create a new RRM network address or network address group from the value specified in the Network field.

Delete collect entry(s)
Deletes all collected entries.
Collected Objects

By clicking the following buttons, you can perform the corresponding actions to the collected objects you select:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Select Object to Promote" /></td>
<td>Specifies the highlighted object in the <strong>Object Path</strong> field.</td>
</tr>
<tr>
<td><img src="image" alt="Set Remote Object Authority" /></td>
<td>Displays the Maintain Remote Object Authority dialog box, which lets you manage the Remote Object Authorities of the selected object.</td>
</tr>
<tr>
<td><img src="image" alt="Add User/Object Override" /></td>
<td>Displays the User/Object Override dialog box, which lets you add a User/Object Override for the selected object.</td>
</tr>
<tr>
<td><img src="image" alt="Remove Object from Collected Entry" /></td>
<td>Displays a confirmation dialog box to verify whether you want to delete the selected object.</td>
</tr>
<tr>
<td><img src="image" alt="View Full Path" /></td>
<td>Displays the View Full Path window, which shows the full path of the selected object. Use this function when the object exceeds the maximum value for the window.</td>
</tr>
</tbody>
</table>

**Help**

Displays a window containing Help information.
Create
Creates a Secured Entry in the designated environment.

Cancel
Cancels the operation.

After you specify the desired criteria and click Create, a confirmation dialog box is displayed.

Browse Objects
If you click the object browser button on the Create Entry dialog box, the Object Browser dialog box is displayed. This dialog box lets you browse for the path of the object associated with the entry being created.

The Object Browser dialog box includes the following fields:

object pane
Displays the paths of objects associated with the entry being created.

Help
Displays a window containing Help information.
Select
Selects the highlighted object path.

Close
Closes the dialog box.

Secured Environment

The Secured icon represents the RRM Secured Environment. The Secured Environment contains rules for controlling remote requests, and provides functions to manage the rules.

For more information about the Secured environment, see “Work with Secured Entries” on page 53.
Right-click Options

By right-clicking Secured, the following options are available:

Explore
Displays the Secured Environment configuration in the Detail Pane.

Open
Displays the Secured Environment configuration in a new window.

Create Shortcut
Creates a shortcut to the Secured icon and places it on your desktop.

Click Options

By clicking Secured, icons representing other types of Secured options are displayed.

Entries

The Entries icon represents a repository of RRM Secured or What If Entries, and provides functions to manage the entries.
Right-click Options

By right-clicking Entries, the following options are available:

**Explore**
Displays the Secured Entries in the Detail Pane.

**Open**
Displays the Secured Entries in a new window.

**Create Shortcut**
Creates a shortcut to the Entries icon and places it on your desktop.

**New**
Displays the Work With Entries dialog box, which lets you define a new Secured or What If Entry. For more information, see “Work With Entries” on page 323.

**Filter**
Displays the Entries Filter dialog box, which lets you specify criteria for selecting Secured or What If Entries.

Click Options

By clicking Entries, the Entries Filter dialog box is displayed for use in selecting Entries (see “Filter Entries”). After the filter is applied, entries with options that you can perform are listed in the Detail Pane.

Available Options

By right-clicking an entry and selecting an option, the following options are available:

**Edit**
Displays the Work With Entries dialog box, which lets you edit the selected entry.

**Copy**
Displays the Work With Entries dialog box, which lets you create a new entry based on the selected entry.
Delete
Displays a confirmation dialog box to verify whether you want to delete the selected entries.

Filter
Displays the Entries Filter dialog box, which lets you specify filter criteria for selecting entries.

Filter Entries
If you right-click an entry or the Entries icon and select Filter from the pull-down menu, the Entries Filter dialog box is displayed. Depending on the type of entries selected (Secured or What If Entries), this dialog box lets you specify criteria to use for listing Secured or What If Entries in the Detail Pane. If no selection criteria are specified, all entries of the selected type are listed. To indicate the type of entries selected, “Secured” or “What If” is displayed in the title of the dialog box.
The Entries Filter dialog box includes the following fields:

**Enabled Status**
Whether the entries selected will be “Enabled” or “Disabled.” This status indicates whether the decision-making process that controls remote request access to RRM is active. The following values are valid:

- **<No Filter>** - No filter will be used to select entries.
- **Disabled** - Only entries with Disabled status will be selected.
- **Enabled** - Only entries with Enabled status will be selected.

**User or Group**
A user name or group that can be used to select entries.

**Network**
A network addresses that can be used to select entries.

**Operation**
An operation that can be used to select entries.

**Action or Calendar**
An action or calendar that can be used to select entries.

**Swap Profile**
A swap profile that can be used to select entries.

**Help**
Displays a window containing Help information.

**Apply**
Applies the criteria you specify for selecting entries.

**Cancel**
Cancels the selection operation.
Work With Entries

The Work With Entries dialog box lets you edit or copy an entry. Depending on the type of entry selected (Secured or What If Entry), this dialog box lets you maintain a Secured or What If Entry. To indicate the type of entry selected, “Secured” or “What If” is displayed in the title of the dialog box.

If you copy an entry, the key (user/network/operation) of the new entry must be unique.

![Work With Entries - Edit (Secured)](image)

The Work With Entries dialog box includes the following fields:

**User or Group**

The user or group of the selected entry.

**Network**

The network address of the selected entry.
Operation
The operation of the selected entry.

Object Path
The path of any objects associated with the selected entry.

Object browser button
Displays the Browse Object dialog box, which lets you browse for the path of the object associated with the entry being created.

Action
The action of the selected entry.

Swap Profile
The swap profile (if one exists) of the selected entry.

Enabled Status
The Enabled status of the selected entry. The following values are valid:

- Enabled - The decision-making process that controls remote request access is turned on for the selected entry.
- Disabled - The decision-making process that controls remote request access is turned off for the selected entry.

Add new user or group if necessary
When selected, this option lets you dynamically create a new RRM user or user group from the value specified in the User field.

Add new network if necessary
When selected, this option lets you dynamically create a new RRM network address or network address group from the value specified in the Network field.

Help
Displays a window containing Help information.

Save
Saves the changed or copied entry and displays a confirmation dialog box that indicates the operation was completed.

Cancel
Cancels the operation.
RRM Groups

The RRM Groups icon represents a repository of RRM Group records, and provides functions to manage the records.

For more information about the RRM Groups, see “Work with RRM Groups” on page 118.

Right-click Options

By right-clicking RRM Groups, the following options are available:

Explore
  Displays the available types of RRM Groups in the Detail Pane.

Open
  Displays the available types of RRM Groups in a new window.

Create Shortcut
  Creates a shortcut to the RRM Groups icon and places it on your desktop.

Group Browser
  Displays the Group Browser dialog box, which lets you perform maintenance functions on RRM Groups and Entities.
Click Options

By clicking RRM Groups, the available types of RRM Groups are listed. When you click one of these Group icons (Network, User, or Operation), the associated entries are listed in the Detail Pane.

Network/User/Operation Groups

The Network, User, and Operation icons represent repositories for each type of RRM Group, and they provide functions to manage the records.

Right-click Options

By right-clicking Network, User, or Operation, the following options are available:

Explore
Displays the selected type of RRM Group entries in the Detail Pane.

Open
Displays the selected type of RRM Group entries in a new window.

Create Shortcut
Creates a shortcut to the selected Group icon and places it on your desktop.
New Group
Displays the Work with Group/Member dialog box, which lets you create a new group based on the selected group. New groups are created without the contents of the original group.

New Member
Displays the Work with Group/Member dialog box, which lets you create a new member in the selected group.

Group Browser
Displays the Maintain RRM Groups and Entities dialog box, which lets you perform maintenance functions on RRM Groups and Members.

Click Options
By clicking Network, User, or Operation, all entries for the selected type of group are listed.

Available Options
By right-clicking a group entry, the following options are available:

Explore
Displays the contents of the selected group in the Detail Pane.

Open
Displays the contents of the selected group in a new window.

Create Shortcut
Creates a shortcut to the selected Group icon and places it on your desktop.

Edit
Displays the Work with Group/Member dialog box, which lets you edit the selected group or member.

New
Displays the Work with Group/Member dialog box, which lets you create a new group or member based on the selected group or member. New groups are created without the contents of the original group.
Copy
Displays the Work with Group/Member dialog box, which lets you create a copy of a selected group or member using a different name. For groups, the contents of the original group are also copied.

Delete
Displays a confirmation dialog box to verify whether you want to delete the selected groups or members.

Group Browser
Displays the Maintain RRM Groups and Entities dialog box, which lets you perform maintenance functions on RRM Groups and Members.
**Work with Network**

If you right-click a Group entry in the Detail Pane and select **Edit**, **New**, or **Copy** from the pull-down menu, the Work with Network dialog box is displayed. This dialog box lets you create, delete, or maintain RRM Groups and Members. To indicate the type of Groups and Members selected, “Secured” or “What If” is displayed in the title of the dialog box.
The Work with Group or Member dialog box includes the following fields:

**Basic Attributes**
Descriptive information about the Group selected.

- **Member Name**
The name of the Group selected.

**Group List**
Lists the Groups that you can select and the members of a selected Group.

- **Available**
Lists the Groups that you can select.

  ```
  ==> 
  ```

  Moves a Group from the *Available* field to the *Member of* field to show the members it contains.

- **<=**
Moves the members of a Group from the *Member of* field to the *Available* field to show the Group that contains the members.

- **Select All**
Moves all Groups listed in the *Available* field to the *Member of* field to show the members they contain.

- **Select All**
Moves all Groups listed in the *Member of* field to the *Available* field to show the Groups that contain the members.

- **Member of**
Lists the members of the selected Group.

**Help**
Displays a window containing Help information.

**Save**
Saves the Group or Member.

**Cancel**
Cancels the selected operation.
Group Browser

If you right-click a group icon (User, Network, or Operation) or a Group entry and selected Group Browser from the pull-down menu, the Group Browser dialog box is displayed. This dialog box lets you create, delete, and maintain Secured or What If RRM Groups and Entities. To indicate the type of Groups and Members selected, “Secured” or “What If” is displayed in the title of the browser.
By clicking the following buttons, you can perform the corresponding actions:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Users</td>
<td>Displays the Load Users Selection Filter dialog box, which lets you specify criteria for selecting users.</td>
</tr>
<tr>
<td>Add New Group</td>
<td>Displays the Work with Group or Member dialog box, which lets you add a new Group.</td>
</tr>
<tr>
<td>Add New Group Member</td>
<td>Displays the Work with Group or Member dialog box, which lets you add a new Member to the selected Group.</td>
</tr>
<tr>
<td>Modify Selected Item</td>
<td>Displays the Work with Group or Member dialog box, which lets you modify a selected Group or Member.</td>
</tr>
<tr>
<td>Delete Selected Items</td>
<td>Displays a confirmation dialog box to verify whether you want to delete the selected Groups or Members.</td>
</tr>
<tr>
<td>Edit User/Server Override</td>
<td>Displays the User/Server Override dialog box, which lets you edit a User/Server Override for the selected user.</td>
</tr>
<tr>
<td>Edit User/Object Override</td>
<td>Displays the User/Object Override dialog box, which lets you edit a selected User/Object Override for the selected user.</td>
</tr>
<tr>
<td>Add New Rule Entry</td>
<td>Displays the Work with Secured Entries dialog box, which lets you add a new Secured Entry.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Reloads the Detail Pane of the Group Browser dialog box.</td>
</tr>
</tbody>
</table>

**List Pane**

Lists the type of Groups and Members displayed in the Detail Pane.

**Detail Pane**

Lists the Groups and Members contained in the Group container selected in the List Pane.
Help
Displays a window containing Help information.

Close
Closes this browser window.

Load Users
When the Load Users button is clicked on the Group Browser dialog box, the Load User Selection Filter dialog box is displayed. This dialog box lets you specify criteria for selecting users.

Help
Displays a window containing Help information.

Select
Applies the specified criteria to select users.

Cancel
Cancels the selected operation.

Object Authorities
The Object Authorities icon represents a repository of RRM Remote Object Authority records, and provides functions to manage the records.
For more information about RRM Remote Object Authorities, see “Work with RRM Object Authorities” on page 120

Right-click Options

By right-clicking Object Authorities, the following options are available:

Explore
Lists the Remote Object Authority records in the Detail Pane.

Open
Lists the Remote Object Authority records in a new window.

Create Shortcut
Creates a shortcut to the Object Authorities icon and places it on your desktop.

Authorities Browser
Displays the Authorities Browser dialog box, which lets you create, delete, and maintain Secured or What If Remote Object Authorities.

Add Segment
Displays the Maintain Remote Object Authority dialog box, which lets you add a new segment to the selected Remote Object Authority record.
Click Options

By clicking Object Authorities, all Remote Object Authority Entries are listed.

Available Options

By right-clicking a Remote Object Authority entry, the following options are available:

Explore
Displays the Remote Object Authorities of the selected record in the Detail Pane.

Open
Displays the Remote Object Authorities of the selected record in a new window.

Create Shortcut
Creates a shortcut to the selected Remote Object Authority entry and places it on your desktop.

Add a Segment
Displays the Maintain Remote Object Authority dialog box, which lets you add a new Remote Object Authority path segment based on the selected path.

Delete Segment
Displays a confirmation dialog box to verify whether you want to delete the selected segment.

Set Remote Object Authorities
Displays the Maintain Remote Object Authority dialog box, which lets you maintain the selected Remote Object Authority record.
Authorities Browser

If you right-click a Remote Object Authority entry in the Detail Pane and select Authorities Browser from the pull-down menu, the Authorities Browser dialog box is displayed. This dialog box lets you create, delete, and maintain Secured or What If Remote Object Authorities. To indicate the type of Remote Object Authority entries selected, “Secured” or “What If” is displayed in the title of the browser.
By clicking the following buttons, you can perform the corresponding actions:

<table>
<thead>
<tr>
<th>Button</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to path</td>
<td>Displays the Work with Group or Member dialog box, which lets you add a new Group.</td>
</tr>
<tr>
<td>Add New Group Member</td>
<td>Displays the Maintain Remote Object Authority dialog box, which lets you add or maintain Remote Object Authority records.</td>
</tr>
<tr>
<td>Delete Selected Items</td>
<td>Displays a confirmation dialog box to verify whether you want to delete the selected object authority.</td>
</tr>
<tr>
<td>Edit Remote Object Authority</td>
<td>Displays the Maintain Remote Object Authority dialog box, which lets you add or maintain Remote Object Authority records.</td>
</tr>
<tr>
<td>Edit User/Object Override</td>
<td>Displays the User/Object Override dialog box, which lets you edit a selected User/Object Override for the selected user.</td>
</tr>
<tr>
<td>Add New Rule Entry</td>
<td>Displays the Work with Secured Entries dialog box, which lets you add a new Secured Entry.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Reloads the Detail Pane of the Authorities Browser dialog box.</td>
</tr>
</tbody>
</table>

**Help**

Displays a window containing Help information.

**Close**

Closes this browser window.
Maintain Remote Object

If you right-click a Remote Object Authority entry in the Detail Pane and select Add a Segment or Set Remote Object Authorities from the pull-down menu, the Maintain Remote Object Authority dialog box is displayed. This dialog box lets you add or maintain Secured or What If Remote Object Authority records. To indicate the type of Remote Object Authority records selected, “Secured” or “What If” is displayed in the title of the dialog box.
The Maintain Remote Object Authority dialog box includes the following fields:

**Path**
The path and segment of the remote object authority record.

**Path**
The path of the remote object authority record.

**Segment**
The segment of the path where the remote object authority record is located. This field is displayed only if you are adding a segment.

**Add new user or group if necessary**
When selected, this option lets you dynamically create a new RRM user or user group from the value specified in the **User** field.

**Edit**
The authorities granted to this remote object.

**User profile**
The user profile of the user or group whose access will be controlled by this record.

**Read rights**
Authority to read a file (Y=yes or N=no).

**Write rights**
Authority to write a file (Y=yes or N=no).

**Execute rights**
Authority to execute a program or command (Y=yes or N=no).

**Operate rights**
Authority to create or delete a file (Y=yes or N=no).
Enabled status
Whether the decision-making process that controls remote request access to RRM is enabled or disabled for the selected entry. The following values are valid:

Enabled - The decision-making process that controls remote request access is turned on for the selected entry.

Disabled - The decision-making process that controls remote request access is turned off for the selected entry.

Authority Display Pane
Displays the Remote Object Authorities for the selected entry. If you select a listed entry, its properties are displayed in the Edit section of this dialog box.

Help
Displays a window containing Help information.

Save
Saves the remote object authority record.

Cancel
Cancels changes made during this editing session.

Calendars
The Calendars icons represents a repositories of calendar records, and provides functions to manage the records.
For more information about Calendars, see “Work with Calendars” on page 127.

Right-click Options

By right-clicking Calendars, the following options are available:

Explore
Lists all Calendars in the Detail Pane.

Open
Lists all Calendars in a new window.

Create Shortcut
Creates a shortcut to the Calendars icon and places it on your desktop.

New Calendar
Displays the Work With Calendar dialog box, which lets you create a new calendar.

Click Options

By clicking Calendars, all calendars are listed.
Available Options

By right-clicking a Calendar entry, the following options are available:

Explore
Displays the definition of the selected Calendar in the Detail Pane.

Open
Displays the definition of the selected Calendar in a new window.

Create Shortcut
Creates a shortcut to the selected Calendar and places it on your desktop.

New Calendar
Displays the Work With Calendar dialog box, which lets you create a new Calendar based on the selected Calendar.

Edit Calendar
Displays the Work With Calendar dialog box, which lets you edit the selected Calendar.

Delete Calendar
Displays a confirmation dialog box to verify whether you want to delete the selected Calendar.
Create/Edit Calendar

If you right-click a Calendar icon or Calendar entry and select Edit Calendar or New Calendar, the Work With Calendar dialog box is displayed. This dialog box lets you create or edit Secured or What If RRM Calendars. To indicate the type of Calendars selected, “Secured” or “What If” is displayed in the title of the dialog box.
The Work With Calendar dialog box includes the following fields:

**Calendar**
The name and default action of the Calendar selected from the Detail Pane.

**Name**
The name of the Calendar.

**Default Action**
The action to be taken if a matching Calendar record is not found. If no existing calendar record applies to the day and time when the transaction is received, the action specified in the **Default Action** field is taken.

**Edit**
The action to be taken during the days and times specified for the Calendar that was selected from the Detail Pane. When this dialog box is displayed by selecting **New**, default settings are displayed in this section.

**Action**
The action associated with this Calendar.
The following values are valid:

* **PASS** - The transaction succeeds.
* **FAIL** - The transaction fails.
* **OBJLIST** - An object is associated with the transaction.

**From Time**
The starting time for a specified period when the Calendar is in effect.

**To Time**
The ending time for a specified period when the Calendar is in effect.

**SUN**
Whether the Calendar is in effect Sunday.

**MON**
Whether the Calendar is in effect Monday.

**TUE**
Whether the Calendar is in effect Tuesday.
WED
Whether the Calendar is in effect Wednesday.

THU
Whether the Calendar is in effect Thursday.

FRI
Whether the Calendar is in effect Friday.

SAT
Whether the Calendar is in effect Saturday.

Clear
Clears changes to the selected Calendar that have not been saved.

Apply
Applies the specified settings.

Delete
Deletes the selected Calendar.

List Pane
Lists defined Calendars. If you select a listed Calendar, its properties are displayed in the fields above.

Help
Displays a window containing Help information.

Save
Saves the Calendar.

Cancel
Cancels the changes made during this editing session.

User/Server Overrides

The User/Server Overrides icon represents a repository of RRM User/Server Override records, and provides functions to manage the records. Typically, User/Server Overrides are used to grant or revoke user authority that exceeds all other authorities to a specified server.
For more information about User/Server Overrides, see “Work with User/Server Overrides” on page 130.

**Right-click Options**

By right-clicking **User/Server Overrides**, the following options are available:

- **Explore**
  
  Lists the User/Server Overrides in the Detail Pane.

- **Open**
  
  Lists the User/Server Overrides in a new window.

- **Create Shortcut**
  
  Creates a shortcut to the **User/Server Overrides** icon and places it on your desktop.

- **New**
  
  Displays the User/Server Override dialog box, which lets you create a new User/Server Override.

**Click Options**

By clicking **User/Server Overrides**, all User/Server Override entries are listed in the Detail Pane.
**Available Options**

By right-clicking a User/Server Override entry, the following options are available:

**Edit**
Displays the User/Server Override dialog box which lets you edit the selected User/Server Override.

**Copy**
Displays the User/Server Override dialog box, which lets you create a new User/Server Override using the values of the selected override.

**Delete**
Displays a confirmation dialog box to verify whether you want to delete the selected User/Server Overrides.

**Maintain User/Server Override**

The User/Server Override dialog box lets you edit or copy a User/Server Override. Depending on the type of override selected (Secured or What If), this dialog box lets you maintain a Secured or What If User/Server Override. To indicate the type of override selected, “Secured” or “What If” is displayed in the title of the dialog box.

If you copy a User/Server Override, the user or server of the new override must be different.
The User/Server Override dialog box includes the following fields:

**User**
Select or type the user associated with the override.

**Server**
Select or type the server to which the override applies.

**Action**
The action to be taken if the user and server match the incoming request.

**Add new user or group if necessary**
When selected, this option lets you dynamically create a new RRM user or user group from the value specified in the User field.

**Help**
Displays a window containing Help information.

**Save**
Saves the User/Server Override and displays a confirmation dialog box that indicates the operation was completed.

**Cancel**
Cancels the operation.

**User/Object Overrides**

The User/Object Overrides icon represents a repository of RRM User/Object Override records, and provides functions to manage the records.
For more information about User/Server Overrides, see “Work with User/Object Overrides” on page 133.

Right-click Options

By right-clicking User/Object Overrides, the following options are available:

Explore
Lists the User/Object Overrides in the Detail Pane.

Open
Lists the User/Object Overrides in a new window.

Create Shortcut
Creates a shortcut to the User/Object Overrides icon and places it on your desktop.

New
Displays the Maintain User/Object Override dialog box, which lets you create a new User/Object Override.

Click Options

By clicking User/Object Overrides, all overrides are listed in the Detail Pane.
Available Options

By right-clicking a User/Object Override entry, the following options are available:

Edit
Displays the User/Object Override dialog box, which lets you edit the selected User/Object Override.

Copy
Displays the User/Object Override dialog box, which lets you copy the selected User/Object Override.

Delete
Displays a confirmation dialog box to verify whether you want to delete the selected User/Object Override.

User/Object Override

The User/Object Override dialog box lets you edit or copy a User/Object Override. This dialog box lets you maintain Secured or What If User/Object Overrides. To indicate the type of override selected, “Secured” or “What If” is displayed in the title of the dialog box.
Typically, this function is used to grant or revoke user authority that exceeds all other authorities for a specified object. If you copy an override, the user or object of the new override must be different.

![User/Object Override dialog box](image)

The User/Object Override dialog box includes the following fields:

**User**
Select or type the user associated with the override.

**Object**
Select or type the object to which the override applies.

**Object browser button**
Displays the Browse Object dialog box, which lets you browse for the path of the object associated with the entry being created.

**Action**
The action to be taken if the user and object match the incoming request.

**Add new user or group if necessary**
When selected, this option lets you dynamically create a new RRM user or user group from the value specified in the **User** field.

**Help**
Displays a window containing Help information.
Save
Saves the user/object override and displays a confirmation dialog box that indicates the operation was completed.

Cancel
Cancels the edit operation.

Exit Points

The Exit Points icon represents a repository of RRM Exit Point entries, and provides functions to manage the records.

For more information about Exit Points, see “Work with Exit Points” on page 136.

Right-click Options

By right-clicking Exit Points, the following options are available:

Explore
Lists the Exit Points in the Detail Pane.

Open
Lists the Exit Points in a new window.

Create Shortcut
Creates a shortcut to the Exit Points function and places it on your desktop.
Click Options

By clicking **Exit Points**, all Exit Points are listed in the Detail Pane.

Available Options

By right-clicking an Exit Point entry, the following options are available:

**Edit Exit Points**
Displays the Edit Exit Point dialog box, which lets you edit the selected Exit Point.

**Install Exit Program**
Displays a confirmation dialog box to verify whether you want to install the Exit Program at the selected Exit Point.

**Remove Installed Exit Program**
Displays a confirmation dialog box to verify whether you want to remove the Exit Program from the selected Exit Point.

**Replace Installed Exit Program**
An RRM Exit Program is installed at sequence 1, and the custom Exit Program is retained as a customer Exit Program to be called by the RRM Exit Program. Thus, the RRM Exit Program will be called, and RRM will pass the original transaction and the RRM decision to the customer Exit Program. The customer exit program can keep or reverse the original RRM decision. RRM will then enforce the decision made by the customer Exit Program.
**Edit Exit Point**

If you right-click an Exit Point entry in the Detail Pane and select **Edit Exit Point**, the Edit Exit Point dialog box is displayed. This dialog box lets you edit Secured or What If Exit Points. To indicate the type of exit point selected, “Secured” or “What If” is displayed in the title of the dialog box.
The Edit Exit Point dialog box includes the following fields:

**Exit Point**
The name of the Exit Point. This value cannot be edited.

**Exit Format**
The format of the Exit Point. This value cannot be edited.

**Exit Program**
The NetIQ Security Solutions for iSeries Exit Program associated with this Exit Point.

**Customer Exit Program**
The customer Exit Program, if any, associated with this Exit Point.

**Library**
The library that contains the customer Exit Program associated with this Exit Point.

**Secured**
Whether the Exit Point function that restricts access to incoming requests is enabled (*YES) or disabled (*NO).

**Collected**
The collection mode of the selected exit point. The following values are valid:

- *ALL - All incoming transactions are collected.
- *NONE - No incoming transactions are collected.
- *REJECT - Rejected transactions only are collected.
- *UNSECURED - Unsecured transactions only are collected.

**Check Primary Groups**
Whether the primary group should be searched (*YES/*NO).

**Check Supplemental Groups**
Whether Supplemental Groups should be searched (*YES/*NO).

**Check RRM Groups**
Whether RRM Groups should be searched (*YES/*NO).
Allow Swap
   Whether use of a swap profile will be allowed (*YES/*NO).

Maximum Parsing Depth
   A value from 0 to 99 that indicates the maximum number of levels to search when parsing an object.

Log Incoming Transactions
   Whether What If Playback transactions should be logged (*YES/*NO). To log What If Playback transactions, you must specify *YES in this field. For more information, see “Playback What If Transaction Database” on page 157.

Log Parsed Transactions - Pass
   Whether transactions that were processed and passed should be logged (*YES/*NO).

Log Parsed Transactions - Fail
   Whether transactions that were processed and failed should be logged (*YES/*NO).

Log Parsed Object - Pass
   Whether transactions with objects that were processed and passed should be logged (*YES/*NO).

Log Parsed Object - Fail
   Whether transactions with objects that were processed and failed should be logged (*YES/*NO).

Save
   Saves the Exit Point settings.

Cancel
   Cancels the edit operation.

Help
   Displays a window containing Help information.
What If Environment

The What If icon represents the RRM What If Environment. This environment contains What If remote transaction data, and provides functions to generate and manage the data.

For more information about the What If environment, see “Work with What If Analysis” on page 148.

Right-click Options

By right-clicking What If, the following options are available:

Explore
Displays the What If environment configuration in the Detail Pane.

Open
Displays the What If environment configuration in a new window.
Create Shortcut
Creates a shortcut of the What If environment and places it on your desktop.

Copy Secured to What If
Displays a pop-up confirmation text box that instructs you to press ENTER if you want to copy Secured Entries to What If Entries.

Promote What If to Secured
Displays a pop-up confirmation text box that instructs you to press ENTER if you want to promote What If files to Secured Entries. This function replaces the current Secured Entries with What If Entries and saves the Secured Entries in a backup directory. You can restore the Secured Entries and restore the What If Entries to What If status by using the Demote What If File function.

Demote What If File
Displays a pop-up confirmation text box that instructs you to press ENTER if you want to demote the most recent What If Entries. This function reverses the effect of the promote function by restoring both the What If and Secured environments to their status before the “Promote” occurred.

Clear What If File
Displays a pop-up confirmation text box that instructs you to press ENTER if you want to remove What If Entries. This function clears the What If Entries.

Playback What If DB
Displays the What If Playback dialog box, which lets you create a database of What If transactions for use in testing or verifying the new What If configuration.

Click Options
By clicking What If, icons representing other types of What If functions are displayed. When you click one of these What If function icons, the associated entries are listed in the Detail Pane.
Playback What If Database

If you right-click the What If icon and select Playback What If DB, the What If Playback dialog box is displayed. This dialog box lets you create a database of What If transactions to test or verify the new What If configuration. After you execute What If Playback, you can review the effects of the new configuration by generating What If reports. If the results are not acceptable, you can make changes and execute What If Playback again until you achieve the desired results.
The What If Playback dialog box includes the following fields:

**Input Type**
Whether the type of input used for Playback is a journal (*JOURNAL) or a file (*FILE).

**Starting journal receiver**
The name of the first journal receiver in a series of journal receivers that stores journal entries. This field is displayed only when *JOURNAL is specified in the **Input Type** field. The following values are valid:

*CURRENT
The journal receiver that is attached when conversion of journal entries starts.

*CURCHAIN
The journal receiver chain that includes the journal receiver that is attached when conversion of journal entries starts. This receiver chain does not cross a break in the chain. If there is a break in the chain, the receiver range includes the most recent break in the chain through the receiver that is attached when conversion of journal entries starts.

**journal receiver**
The name of the journal receiver whose entries are converted for output.

**Library**
The name of the library where the starting journal receiver is located. This field is displayed only when *JOURNAL is specified in the **Input Type** field. The following values are valid:

*name* - The name of the library.

*LIBL - A list of valid libraries from which you can choose a library.

*CURLIBL - The current library.
Ending journal receiver

The name of the last journal receiver in a series of journal receivers that stores journal entries. This field is displayed only when *JOURNAL is specified in the Input Type field. The following values are valid:

*CURCHAIN

The journal receiver chain that includes the journal receiver that is attached when conversion of journal entries starts. This receiver chain does not cross a break in the chain. If there is a break in the chain, the receiver range includes the most recent break in the chain through the receiver that is attached when conversion of journal entries starts.

journal receiver

The name of the journal receiver whose entries are converted for output.

Library

The name of the library where the ending journal receiver is located. This field is displayed only when *JOURNAL is specified in the Input Type field. The following values are valid:

name - The name of the library.

*LIBL - A list of valid libraries from which you can choose a library.

*CURLIBL - The current library.

Transaction Type

The type of transaction to be processed in Playback mode. This field is displayed only when *JOURNAL is specified in the Input Type field. The following values are valid:

*ALL

All transactions are processed.

*CENTRAL

Central Server transactions are processed.

*DDM

Distributed Data Management (DDM) transactions are processed.
*DRDA
Distributed Relational Database Architecture (DRDA) transactions are processed.

*DBINIT
Database Initialization (DBINIT) transactions are processed.

*DBNDB
Database Server transactions are processed.

*DBROI
Database Server Object Information transactions are processed.

*DBSQL
Database Structured Query Language (DBSQL) transactions are processed.

*DTAQ
Original Data Queue Server transactions are processed.

*FILE
File Server transactions are processed.

*FILETFR
Original File Transfer transactions are processed.

*FTPCLT
Client File Transfer Protocol transactions are processed.

*FTPSRV
Server File Transfer Protocol transactions are processed.

*LICENSE
Original License Management transactions are processed.

*MSGSRV
Original Message Server transactions are processed.

*NETPRT
Network Printer Server transactions are processed.

*REXEC
REXEC transactions are processed.
*RMTCMD
Remote Command transactions are processed.

*RMTSQL
Remote Structured Query Language (DBSQL) transactions are processed.

*TELNET
Telnet transactions are processed.

*VRTPRT
Original Virtual Printer Server transactions are processed.

**Starting Date and Time**
The beginning date and time of the period for which you want report data. This field is displayed only when *JOURNAL is specified in the Input Type field.

**Note**
NetIQ Corporation products do not support Julian dates.

**Ending Date and Time**
The ending date and time of the period for which you want report data. This field is displayed only when *JOURNAL is specified in the Input Type field.

**File Name**
The name of the file where you want to place the data. The following values are valid:

*NONE
The reported data will not be placed in a data file.

name
The file where the data will be placed.
Library
The name of the library where the data file is located. The following values are valid:

*name - The name of the library.

*LIBL - A list of valid libraries from which you can choose a library.

*CURLIB - The current library.

Replace or Add Records
Whether you want the generated output to replace (*REPLACE) the existing report or to be appended to the end of (*ADD) the existing report. This field is displayed only when *JOURNAL is specified in the Input Type field.

Run Interactively
Whether the job should be executed interactively or in batch mode. The following values are valid:

*NO - Submits job for batch processing.

*YES - Executes job interactively.

Help
Displays a window containing Help information.

Run
Generates the What If Playback Transaction database.

Cancel
Cancels the operation.
Entries

The Entries icon in the What If environment represents a repository of RRM What If Entries, and provides functions to manage the entries.

Right-click Options

By right-clicking Entries, the following options are available:

Explore
Lists icons for the types of What If functions available in the Detail Pane.

Open
Lists icons for the types of What If functions available in a new window.

Create Shortcut
Creates a shortcut for the Entries icon in the What If environment and places it on your desktop.
New
Displays the Work With Entries dialog box, which lets you define a new What If Entry. For more information, see “Work With Entries” on page 323.

Filter
Displays the Entries Filter dialog box, which lets you specify filter criteria for selecting What If Entries.

Click Options
By clicking Entries in the What If environment, the Secured/What If Entries Filter dialog box is displayed for use in selecting What If Entries (see “Filter Entries” on page 321). After the filter is applied, What If Entries with functions that you can perform are listed.

Available Options
By right-clicking a What If entry, the following options are available:

Edit
Displays the Work With Entries dialog box, which lets you edit the selected What If Entry.

Copy
Displays the Work With Entries dialog box, which lets you copy the selected What If Entry.

Delete
Displays a confirmation dialog box to verify whether you want to delete the selected What If Entry.

Filter
Displays the Entries Filter dialog box, which lets you specify filter criteria for selecting What If entries.

RRM Groups
The RRM Groups icon in the What If environment represents a repository of What If RRM Group records, and provides functions to manage the records.
For more information about RRM Groups, see “Work with RRM Groups” on page 118.

**Right-click Options**

By right-clicking **RRM Groups** in the What If environment, the following options are available:

**Explore**

Displays the available types of What If Groups in the Detail Pane.

**Open**

Displays the available types of What If Groups in a new window.
Create Shortcut
Creating a shortcut to the RRM Groups icon in the What If environment and places it on your desktop.

Group Browser
Displays the Maintain RRM Groups And Entities dialog box, which lets you create, delete, and maintain What If RRM groups and entities.

Click Options
By clicking RRM Groups in the What If environment, icons representing the available types of What If Groups are listed. When you Click one of these Group icons (Network, User, or Operation), the associated What If entries are listed.
Network/User/Operation

The Network, User, and Operation icons in the What If environment represent repositories of each type of What If RRM Group, and they provide functions to manage the groups.
Right-click Options

By right-clicking **Network**, **User**, or **Operation** in the What If environment, the following options are available:

**Explore**
Displays the What If Entries of the selected Group type in the Detail Pane.

**Open**
Displays the What If Entries of the selected Group type in a new window.

**Create Shortcut**
Creates a shortcut to the selected What If Group icon places it on your desktop.

**Group Browser**
Displays the Maintain RRM Groups And Entities dialog box, which lets you create, delete, and maintain RRM What If groups and entities.

**New Member**
Lets you create a new What If Member in the selected group.

Click Options

By clicking **Network**, **User**, or **Operation** in the What If environment, all entries for the selected type of Group are listed.

Available Options

By right-clicking a Group entry, the following options are available:

**Explore**
Displays the contents of the selected What If Group in the Detail Pane.

**Open**
Displays the contents of the selected What If Group in a new window.

**Create Shortcut**
Creates a shortcut to the selected What If Group icon and places it on your desktop.
Edit
Displays the Work with Group/Member dialog box which lets you edit the selected What If Group or Member.

New
Displays the Work with Group/Member dialog box, which lets you create a new What If Group or Member based on the selected Group or Member. New Groups are created without the contents of the original Group.

Copy
Displays the Work with Group/Member dialog box, which lets you create a copy of a selected What If Group or Member using a different name. For Groups, the contents of the original group are also copied.

Delete
Displays a confirmation dialog box to verify whether you want to delete the selected What If Group or Member.

Group Browser
Displays the Maintain RRM Groups And Members dialog box, which lets you create, delete, and maintain RRM What If Groups and Members.

Object Authorities
The Object Authorities icon in the What If environment represents a repositories for RRM What If object authority records and provides functions to manage the records.
For more information about RRM Remote Object Authorities, see “Work with RRM Object Authorities” on page 120.

Right-click Options

When the Object Authorities icon in the What If environment is right-clicked, a pull-down menu is displayed with the following options:

Explore
Lists the What If Remote Object Authority records in the Detail Pane.

Open
Lists the What If Remote Object Authority records in a new window.

Create Shortcut
Creates a shortcut to the Object Authorities icon in the What If environment and places it on your desktop.
View
Displays the Maintain Remote Object Authority dialog box, which lets you view the paths of What If Remote Object Authority records.

Add New Segment
Displays the Maintain Remote Object Authority dialog box which lets you add a new segment to the selected What If object authority record.

**Click Options**

When the Object Authorities icon in the What If environment is clicked, all What If Remote Object Authority records are listed. By right-clicking a Remote Object Authority record and selecting an option from the pull-down menu, you can perform one of the following options:

**Explore**
Displays the What If Remote Object Authorities of the selected record in the Detail Pane.

**Open**
Displays the What If Remote Object Authorities of the selected record in a new window.

**Create Shortcut**
Creates a shortcut to the selected What If Remote Object Authority record and places it on your desktop.

**Add a Segment**
Displays the Maintain Remote Object Authority dialog box, which lets you add a new What If Remote Object Authority path segment based on the selected path.

**Delete Segment**
Displays a confirmation dialog box to verify whether you want to delete the selected path segment.

**Set Remote Object Authorities**
Displays the Maintain Remote Object Authority dialog box which lets you maintain the selected What If Remote Object Authority record.
Calendars

The Calendars icons in the What If environment represents a repositories of What If Calendar records, and provides functions to manage the records.

For more information about Calendars, see “Work with Calendars” on page 127.

Right-click Options

By right-clicking Calendars in the What If environment, the following options are available:

Explore
Lists all What If Calendars in the Detail Pane.

Open
Lists all What If Calendars in a new window.
Create Shortcut
Creates a shortcut to the Calendars icon in the What If environment and places it on your desktop.

New Calendar
Displays the Work With Calendar dialog box which lets you create a new What If Calendar based on the selected calendar.

Click Options
When the Calendars icon in the What If environment is clicked, all What If Calendars are listed. By right-clicking a What If Calendar and selecting an option from the pull-down menu, you can perform one of the following options:

Explore
Displays the definition of the selected What If Calendar in the Detail Pane.

Open
Displays the definition of the selected What If Calendar in a new window.

Create Shortcut
Creates a shortcut of the selected What If Calendar and places it on your desktop.

New Calendar
Displays the Work With Calendar dialog box which lets you create a new What If Calendar based on the selected Calendar.

Edit Calendar
Displays the Work With Calendar dialog box which lets you edit the selected What If Calendar.

Delete Calendar
Displays a confirmation dialog box to verify whether you want to delete the selected What If Calendar.
User/Server Overrides

The User/Server Overrides icon in the What If environment represents a repository of RRM What If User/Server Override records, and provides functions to manage the records.

For more information about User/Server Overrides, see “Work with User/Server Overrides” on page 130.

Right-click Options

By right-clicking User/Server Overrides in the What If environment, the following options are available:

Explore
Lists the What If User/Server Overrides in the Detail Pane.

Open
Lists the What If User/Server Overrides in a new window.
Create Shortcut
Creates a shortcut to the User/Server Overrides function in the What If environment and places it on your desktop.

New
Displays the Maintain User/Server Override dialog box which lets you create a new What If User/Server Override.

Click Options
By clicking User/Server Overrides in the What If environment, all What If User/Server Override entries are listed in the Detail Pane.

Available Options
By right-clicking a User/Server Override entry, the following options are available:

Edit
Displays the User/Server Override dialog box which lets you edit the selected What If User/Server Override.

Copy
Displays the Secured/What If User/Server Override dialog box which lets you copy the selected What If User/Server Override.

Delete
Displays a confirmation dialog box to verify whether you want to delete the selected What If User/Server Override.

User/Object Overrides
The User/Object Overrides icon in the What If environment represents a repository of RRM What If User/Object Override records, and provides functions to manage the records.
For more information about User/Server Overrides, see “Work with User/Object Overrides” on page 133.

**Right-click Options**

By right-clicking **User/Object Overrides** in the What If environment, the following options are available:

- **Explore**
  Lists the What If User/Object Overrides in the Detail Pane.

- **Open**
  Lists the What If User/Object Overrides in a new window.

- **Create Shortcut**
  Creates a shortcut to the **User/Object Overrides** icon in the What If environment and places it on your desktop.

- **New**
  Displays the Maintain User/Object Override dialog box which lets you create a new What If User/Object Override.
Click Options

By clicking User/Object Overrides in the What If environment, all What If User/Object Override entries are listed in the Detail Pane.

Available Options

By right-clicking a User/Object Override entry, the following options are available:

Edit
Displays the User/Object Override dialog box, which lets you edit the selected What If User/Object Override.

Copy
Displays the User/Object Override dialog box, which lets you copy the selected What If User/Object Override.

Delete
Displays a confirmation dialog box to verify whether you want to delete the selected User/Object Override.

Exit Points

The Exit Points icon in the What If environment represents a repository of RRM What If Exit Point entries, and provides functions to manage the entries.
For more information about Exit Points, see “Work with Exit Points” on page 136.

**Right-click Options**

By right-clicking Exit Points in the What If environment, the following options are available:

**Explore**
Lists the What If Exit Points in the Detail Pane.

**Open**
Lists the What If Exit Points in a new window.

**Create Shortcut**
Creates a shortcut to the Exit Points icon in the What If environment and places it on your desktop.
Click Options

By clicking Exit Points in the What If environment, all What If Exit Point entries are listed.

Available Options

By right-clicking an Exit Point entry, the following options are available:

Edit Exit Points
Displays the Edit Exit Point dialog box, which lets you edit the selected Exit Point.

Install Exit Program
Displays a confirmation dialog box, which lets you edit the selected What If Exit Point.

Reports

The Reports icon represents the RRM reporting component. The reporting component provides functions for selecting RRM report criteria and for displaying report output.
For more information about RRM reports, see “Work with RRM Reports” on page 165.

Right-click Options

When the Reports icon is right-clicked, a pull-down menu is displayed with the following options:

Explore
Displays the report generation and output functions in the Detail Pane.

Open
Displays the report generation and output functions in a new window.

Create Shortcut
Creates a shortcut to the Reports icon and places it on your desktop.

Click Options

When the Reports icon is clicked, the Report List and Output icons are displayed. When you click one of these icons, the associated entries are listed in the Detail Pane.
Report List

The Report List icon represents a repository of all RRM reports that can be generated.

Right-click Options

When the Report List icon is right-clicked, a pull-down menu is displayed with the following options:

Explore
Lists the types of reports available in the Detail Pane.

Open
Lists the types of reports available in a new window.

Create Shortcut
Creates a shortcut to the Report List icon and places it on your desktop.
Click Options

When the Report List icon is clicked, the following types of RRM reports are listed in the Detail Pane:

- All
- Configuration Reports
- Object Reports
- Summary/Statistics Reports
- Transaction Reports
- What If Reports

Report Type

The report type icons represent the types of reports that are available through the Operations Navigator GUI.
Right-click Options

When a report type icon is right-clicked, a pull-down menu is displayed with the following options:

Explore
Lists the available reports of this type in the Detail Pane.

Open
Lists the available reports of this type in a new window.

Create Shortcut
Creates a shortcut to the selected report type icon and places it on your desktop.

Click Options

When a report type icon is clicked, the following reports for the report type selected are listed in the Detail Pane:

All
Lists all of the following reports.

Configuration Reports

• Calendar Report
• Network Groups Report
• Operation Groups Report
• Remote Object Authority by Path
• Remote Object Authority by User
• Secured Entries Report
• User Groups Report
Object Reports

- Object Report by Date/Time
- Object Report by Function
- Object Report by Incoming Address
- Object Report by Object
- Object Report by Server
- Object Report by User

Summary/Statistics Reports

- RRM Audit Report
- Transaction Summary Report by Server
- Transaction Summary Report by User

Transaction Reports

- Data Queue Optimized Server Requests
- Data Queue Original Server Requests
- Database Server Requests
- DDM Request Access
- File Server Requests
- FTP Logon and Server Requests
- Network Print Server Entry Requests
- Network Print Server Spool file Requests
- Network Transactions by Date/Time
- Network Transactions by Function
- Network Transactions by Incoming Address
- Network Transactions by Server
• Network Transactions by User
• Original Virtual Print Server Requests
• Remt Command/Distributed Program Call Server Requests
• Remote SQL Server Requests
• Transfer Function Server Requests
• TCP Signon Server Requests

**What If Reports**

• What If Transaction by Date/Time
• What If Transaction by Function
• What If Transaction by Incoming Address
• What If Transaction by Server
• What If Transaction by User

By right-clicking a report and selecting the **Run Report** option from the pull-down menu, you can display the Request Report Dialog box, which lets you specify criteria and generate the selected report.
Run Report

If you right-click a report in the Detail Pane and select Run Report, the Request Report Dialog box is displayed. This dialog box lets you specify criteria for and generate the selected report.
The Request Report Dialog box includes the following fields. The fields displayed for each report will vary according to the report selected:

**Report Id**
The code name of the report to be generated. All valid RRM report IDs are listed in “Report IDs” on page 175. To generate an RRM report from an i5/OS command line, you must specify the correct report ID for the desired report.

**Report Description**
A description of the report to be generated.

**Job Name**
The name of this report job.

**From Time**
The beginning time of the period for which you want report data in the format *hh:mm:ss*.

**Ending Time**
The ending time of the period for which you want report data in the format *hh:mm:ss*.

**Filter Name**
The name of the user-defined filter to be used to select data to include in the report. The possible values are:

* *NONE* - The data is not filtered.

* filter name* - The name of the filter to be used.

**Starting journal receiver**
The name of the first journal receiver in a series of journal receivers that stores journal entries. The following values are valid:

* journal receiver* - The name of the journal receiver whose entries are converted for output.

* *CURRENT* - The journal receiver is used that is attached when starting to convert journal entries.
*CURCHAIN* - Uses the journal receiver chain that includes the journal receiver that is attached when starting to convert journal entries. This receiver chain will not cross a break in the chain. If there is a break in the chain, the receiver range includes the most recent break in the chain through the receiver that is attached when starting to convert journal entries.

**Library** - The name of the library where the starting journal receiver is located. The following values are valid:

`name` - The name of the library.

`*LIBL` - A list of valid libraries from which you can choose a library.

`*CURLIBL` - The current library.

**Ending journal receiver**

The name of the last journal receiver in a series of journal receivers that stores journal entries. The following values are valid:

`*CURRENT` - The journal receiver is used that is attached when starting to convert journal entries.

**journal receiver** - The name of the journal receiver whose entries are converted for output.

**Library** - The name of the library where the ending journal receiver is located. The following values are valid:

`name` - The name of the library.

`*LIBL` - A list of valid libraries from which you can choose a library.

`*CURLIB` - The current library.

**Help**

Displays a window containing Help information.

**Run**

Generates the report using the selected criteria.
Cancel

Cancels the report generation.

File to Receive Output

The name of the data file (outfile) where you want to place the report data. If a filter and an output file are specified, then the filter applies to the output file (outfile) as well as the report output. The following values are valid:

*NONE - The report data will not be placed in a data file.

outfile name - The name of the database file where the output of the command is placed.
**Library name** - The library where the file is located. The following values are valid:

name - The name of the library.

*LIBL - A list of valid libraries from which you can choose a library.

*CURLIBL - The current library.

**Replace or Add records**
Whether you will be adding data to a file or replacing the existing data. The following values are valid:

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

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

**Output queue**
The qualified name of the output queue to be used for spooled files. The following values are valid:

name - The name of the output queue to be used as the default output queue by the submitted job.

*CURRENT - The name of the current output queue.

*USRPRF - The name of the output queue defined in the user’s user profile.

*DEV - The name of the output queue defined in the printer attributes.

*JOBD - The name of the output queue defined in the job description.

**Library** - The name of the library where the output queue is located.

**Hold report on output queue**
Whether reports are to be held on the output queue (*YES/*NO). Reports that are not held are usually directed to a specified printer.
Job queue
The job queue to be used to hold submitted report jobs. The following values are valid:

*name* - If operating in batch mode, the name of the job queue to be used.

*NONE* - If operating interactively, no job queue is specified.

*Library* - The name of the library where the job queue is located.

Output
The *Output* icon represents a repository of RRM report output, and provides functions to view and delete the output.

Right-click Options
When the *Output* icon is right-clicked, a pull-down menu is displayed with the following options:

*Explore*  
Lists the generated reports in the Detail Pane.

*Open*  
Lists the generated reports in a new window.

*Create Shortcut*  
Creates a shortcut to the *Output* icon and places it on your desktop.
Click Options

When the **Output** icon is clicked, all generated RRM reports are listed in the Detail Pane. By right-clicking an output entry, you can select an option from the pull-down menu to perform one of the following options:

**View**

Displays the output for the selected report in a new window.

**Delete**

Displays a confirmation dialog box to verify whether you want to delete the selected report.

Administration

The **Administration** icon represents the RRM administration component. The administration component provides functions for managing RRM.

For more information about RRM administrative functions, see “Manage RRM” on page 200.
Right-click Options

When the Administration icon is right-clicked, a pull-down menu is displayed with the following options:

Explore
Lists the Tools and RRM Defaults icons in the Detail Pane.

Open
Displays the Tools and RRM Defaults icons in a new window.

Create Shortcut
Creates a shortcut to the Administration icon and places it on your desktop.

Click Options

When the Administration icon is clicked, the Tools and RRM Defaults icons are listed.
Tools

The *Tools* icon represents a collection of administrative functions provided to manage RRM.
Right-click Options

When the Tools icon is right-clicked, a pull-down menu is displayed with the following options:

Explore
Lists the administrative functions provided to manage RRM in the Detail Pane.

Open
Lists the administrative functions provided to manage RRM in a new window.

Create Shortcut
Creates a shortcut to the Tools icon and places it on your desktop.

Click Options

When the Tools icon is clicked, icons representing the following administrative functions are listed in the Detail Pane:

- Export Configuration
- Import Configuration
- Cycle Remote Servers
- Change FTP Attributes
- Change Telnet Attributes
- Switch Job Scheduler
- User Preferences
- Start/Stop Monitor

By right-clicking a Tools icon, you can select an option from the pull-down menu to perform one of the following options:

Run
Performs the selected administrative function.

Properties
Displays the properties for the selected administrative function.
Export Configuration

If you right-click the **Export Configuration** icon and select **Run**, the Export RRM Configuration dialog box is displayed. This dialog box lets you select the types of RRM components that you want to include in the exported configuration. By default, all types of RRM components are selected to include in the exported configuration.

![Export RRM Configuration Dialog Box]

The Export RRM Configuration dialog box includes the following fields:

**RRM Components**
- The RRM components that you select to include in the exported configuration:
  - **Exit Points**: Whether you want to include exit points in the exported configuration.
  - **Secured Rules**: Whether you want to include Secured Rules in the exported configuration.
Export Name
The name given to the exported configuration file. This name is used when an import operation is requested.

Note
When naming export files, it is recommended that you use a naming convention that produces names that are memorable and suggest export files.

Help
Displays a window containing Help information.

Export
Exports the configuration file as specified.

Cancel
Cancels the export operation.

Import Configuration
If you right-click the Import Configuration icon and select Run, the Import RRM Configuration to What If dialog box is displayed. This dialog box lets you select an exported RRM configuration file to import to one or more servers.
The Import RRM Configuration To What If dialog box (Frame 1) includes the following fields:

**Select data set to install**
Lists the RRM configuration files that you can install on one or more servers. Only RRM configuration files that have been exported are listed in this field.

**Help**
Displays a window containing Help information.

**Next**
Displays the next window in a series of windows used by this function. This button is enabled when an export file is selected.

**Cancel**
Cancels the import operation.
The Import RRM Configuration To What If dialog box (Frame 2) includes the following fields:

**Select servers to receive configuration**
Lists the available RRM servers where you can install the selected export file.

**Select All**
Selects all servers listed.

**Back**
Re-displays the previous frame of this dialog box.

**Finish**
Displays the final frame of this dialog box.

**Cancel**
Cancels the import operation.
The Import RRM Configuration To What If dialog box (Frame 3) includes the following fields:

**Server**
Lists the RRM servers that you have specified to receive the selected export file.

**Transferring File**
Selects all servers listed.

**Cancel**
Cancels the import operation.

**Cycle Remote Servers**
If you right-click the Cycle Remote Servers icon and select Run, the Cycle Remote Servers dialog box is displayed. This dialog box lets you cycle (end and restart) one or more Client Access or TCP servers.
For more information about cycling remote servers, see “Cycle Remote Servers” on page 205.

The Cycle Remote Servers dialog box includes the following fields:

**Allow Ending Subsystems**

The subsystems that you specify to be ended, if necessary. This parameter is required when a subsystem must be ended to cycle a server. This parameter also serves to remind you that a subsystem must be ended to cycle the specified server(s). The following values are valid:

- ***NONE** - No subsystems can be ended.
- **QSERVER** - The QSERVER subsystems can be ended if necessary. If the *FILE server or the *DATABASE server is selected, QSERVER must be ended.
Delay before restart
The delay period (0-3600 seconds) you specify that occurs before each selected server is cycled.

Available Servers
The names of the servers that you can select to cycle.

right arrow
After you highlight a server in the Available Servers field, use this button to move it to the Servers to Cycle field. This action selects a server to be cycled.

left arrow
After you highlight a server in the Servers to Cycle field, use this button to move it to the Available Servers field. This action de-selects a server to be cycled.

Select All
Selects all servers to be cycled by moving all servers listed in the Available Servers field to the Servers to Cycle field.

Unselect All
Unselects all servers to be cycled by moving all servers listed in the Servers to Cycle field to the Available Servers.

Servers to Cycle
The names of the servers that you have selected to cycle.

Help
Displays a window containing Help information.

Cycle
Cycles the servers listed in the Servers to Cycle field.

Cancel
Cancels the operation.

Change FTP Attributes
If you right-click the Change FTP Attributes icon and select Run, the Change FTP Attributes dialog box is displayed. This dialog box lets you change the FTP attribute to allow anonymous access.
For more information about changing FTP attributes, see “Change FTP Attribute” on page 210.

The Change FTP Attributes dialog box includes the following fields:

**Anonymous profile**

The profile name to use when a user logs on anonymously. The following values are valid:

- *NONE - Anonymous logon is not allowed.
- *usrprf - The user profile to use to log on if anonymous logon is allowed.
Default library
The initial library to be used after logon. The following values are valid:

- *USRPRF* - Uses the current library (CURLIB) specified in the user profile.
- *library name* - The name of a library that you specify.

Default directory:
The initial directory to be used after logon. The following values are valid:

- *USRPRF* - Uses the home directory (HOMEDIR) specified in the user profile.
- *directory name* - The name of an IFS directory that you specify.

Update profile last used date:
Whether you want to set the last-used date of the i5/OS user profile to today's date. The following values are valid:

- *NO* - The user profile last-used date is not changed.
- *YES* - The user profile last-used date is set to today's date.

Help
Displays a window containing Help information.

Save
Displays the settings that lets you select.

Cancel
Cancels the operation.

**Change Telnet Attributes**
If you right-click the **Change Telnet Attributes** icon and select **Run**, the Change Telnet Attributes dialog box is displayed. This dialog box lets you change the Telnet attributes to allow Autosignon access.
For more information about changing Telnet attributes, see “Change Telnet Attribute” on page 212.

The Change Telnet Attributes dialog box includes the following fields:

**AutoSignon control**

The level of authentication required for AutoSignon. The following values are valid:

- **NONE** - AutoSignon is not allowed.
- **ANY** - The password does not require validation.
- **PWDRQD** - The plain-text password must be validated.
- **ENCPWD** - The encrypted password must be validated.
Allow printer sessions
Whether printer sessions are allowed to be serviced through telnet (*YES or *NO).

Allow printer device creation
Whether new printer devices can be autocreated by the telnet server (*YES or *NO).

Allow display device naming
Whether the client can name the display device (*YES or *NO).

Help
Displays a window containing Help information.

Save
Displays the settings that lets you select.

Cancel
Cancels the operation.

Switch Job Scheduler
If you right-click the Switch Job Scheduler icon and select Run, the Switch Job Scheduler dialog box is displayed. This dialog box lets you switch from one job scheduler to another. The choices include IBM and ROBOT.
The Switch Job Scheduler dialog box includes the following fields:

**Switch job scheduler to**
The job scheduler that you want to start using. The following values are valid:

- **ROBOT** - Lets you start using the ROBOT job scheduler.
- **IBM** - Lets you start using the IBM job scheduler.

---

**Note**
If ROBOT is not installed, the Switch Job Scheduler function is disabled.

**Help**
Displays a window containing Help information.

**Save**
Displays the settings that lets you select.

**Cancel**
Cancels the operation.
User Preferences

If you right-click the User Preferences icon and select Run, the User Preferences dialog box is displayed. This dialog box lets you specify RRM user preferences.

![User Preferences Dialog Box]

The User Preferences dialog box includes the following fields:

**Maximum Displayable Object Length**
- The maximum size of an object in bytes that can be displayed.

**Logging Level**
- The level of information to be recorded during logging. The “High” setting indicates that the greatest amount of information is recorded.

---

**Note**
Logging should be performed with the assistance of a Technical Support representative.

---

**Help**
- Displays a window containing Help information.
Save
   Saves the settings that you select.

Cancel
   Cancels the operation.

**Start/Stop Monitor**

If you right-click the **Start/Stop Monitor** icon and select **Run**, the Start/Stop Collection Monitor dialog box is displayed. This dialog box lets you manage the RRM Collection Monitor.

For more information about starting or stopping the RRM Collection Monitor, see “Start/Stop RRM Collection Monitor” on page 209.
The Start/Stop Collection Monitor dialog box includes the following fields:

**RRM collection monitor:**
The action that you want the collection monitor to take. The following values are valid:

- **SWITCH** - Switches the state of the RRM Collection Monitor between running and stopped (controlled stop).
- **START** - Starts the RRM Collection Monitor.
- **STOP** - Stops the RRM Collection Monitor.

**Help**
Displays a window containing Help information.

**Execute**
Performs the action that you select.

**Cancel**
Cancels the operation.

**RRM Defaults**
The RRM Defaults icon represents a collection of administrative functions provided to manage RRM.
For more information about managing RRM default values, “Work with RRM Defaults” on page 141.

Right-click Options

When the RRM Defaults icon is right-clicked, a pull-down menu is displayed with the following options:

Explore
Displays the RRM default settings in the Detail Pane.

Open
Displays the RRM default settings in a new window.

Create Shortcut
Creates a shortcut to the RRM Defaults icon and places it on your desktop.

Edit
Displays the Work With RRM Defaults dialog box which lets you change the default settings.
Click Options

When the RRM Defaults icon is clicked, icons representing the following default values are listed in the Detail Pane:

- RRM Transaction Journal
- RRM Audit Journal
- Exit Program Library
- Alert
- Output Queue
- Output Queue Library
- Days Collected Retained

By right-clicking a default value icon and selecting the Edit option from the pull-down menu, you can display the Work With RRM Defaults dialog box to change the selected default value.
Work With RRM Defaults

If you right-click a default value icon and select **Edit**, the Work With RRM Defaults dialog box is displayed. This dialog box lets you change RRM default values.

![Work With RRM Defaults - Edit](image)

The Work With RRM Defaults dialog box includes the following fields:

**RRM Transaction Journal**

The name of the RRM transaction journal to be used. The following values are valid:

- **PentaSafe** - The PentaSafe transaction journal is used.
- **IBM** - The IBM transaction journal is used.

- **Exit Program Library**
  - **PSCOMMON**

- **Alert Action**
  - **NONE**

- **Output Queue**
  - **QPRINT**

- **Output Queue Library**
  - ***LIBL**

- **Collected Entry Retention**
  - **45**
RRM Audit Journal
The name of the RRM audit journal to be used. The following values are valid:

• *PentaSafe - The PentaSafe audit journal is used.
• *IBM - The IBM audit journal is used.
• *NONE - Audit journaling is disabled. No audit journal is used.

Note
If audit journaling is disabled, RRM will not record who has made changes to your RRM configuration.

Exit Program Library
The name of the library where the exit program resides.

Alert Action
The alert notification action to be used. The following values are valid:

• B = *Both - Use PSDetect to notify a specified person and send alert messages to a specified message queue.
• D = *PSDetect - Use PSDetect to notify a specified person.
• M = *Msgq - Send alert messages to a specified message queue.
• N = *None - No action is taken.

Output Queue
The name of the output queue.

• Output Queue Library - The name of the library where the output queue resides.

Collected Entry Retention
The number of days (0-999) that the collected entries will be kept. If you do not want to keep collected entries for any length of time, specify 0.

Help
Displays a window containing Help information.
Save
   Saves the settings that you select.

Cancel
   Cancels the operation.

**User Message Alert**

The *User Message Alert* icon represents a repository of User/Message Queue Alert entries and provides functions to manage the entries.

For more information about User/Message Alerts, see “Work With User/MsgQ Alerts” on page 143.
Right-click Options

By right-clicking User Message Alert, the following options are available:

Explore
 Lists User/Message Alerts in the Detail Pane.

Open
 Lists User/Message Alerts in a new window.

Create Shortcut
 Creates a shortcut to the User Message Alert icon and places it on your desktop.

New
 Displays the Work With User/MsgQ Alerts dialog box, which lets you define a new User/Message Alert.

Click Options

By clicking User Message Alert, all User/Message Queue Alert entries are listed.

Available Options

By right-clicking a User/Message Queue Alert entry, the following options are available:

Edit
 Displays the Maintain User/MsgQ Alerts dialog box, which lets you edit a User/Message Queue Alert.

Delete
 Displays a confirmation dialog box to verify whether you want to delete the selected User/Message Queue Alert.
**Edit User Message Alert**

If you right-click a User/Message Queue Alert entry in the Detail Pane and select **Edit**, the Work With User/MsgQ Alerts dialog box is displayed. This dialog box lets you edit a User/Message Queue Alert entry.

![Work With User/MsgQ Alerts - New dialog box]

The Work With User/MsgQ Alerts dialog box includes the following fields:

**Alert Type**
- The type of message notification to be used when alert conditions are detected. The following values are valid:
  - *MSGQ* - Causes messages to be sent to a message queue.
  - *USRPRF* - Causes messages to be sent to the message queue of a user.

**Message Queue**
- The user profile or the message queue of the user specified to receive messages.

**Message Queue Library**
- The message queue specified to receive alert messages. This field is used only when *MsgQ* is specified in the **Alert Type** field.

**Help**
- Displays a window containing Help information.
Save
Saves the changes made to the User/Message Alert record.

Cancel
Cancels the edit operation.
This appendix describes the exit points and associated exit programs of Remote Request Management (RRM).

About RRM Exit Points

RRM provides 33 exit points and their associated exit programs. These exit points are associated with the following types of exit programs:

- Original Client Access Server (all programs supported by IBM)
- Optimized Client Access Server (all programs supported by IBM)
- TCP/IP (most programs supported by IBM)
- Distributed Data Management (DDM)
- Distributed Relational Database Architecture (DRDA)

Each exit point and its associated exit program is described in “Exit Point Summary” on page 422.
Exit Point Configuration

All configuration settings for RRM exit points and their associated exit programs are stored in the Exit Point Configuration file. Changes to this file are made through the Work With Exit Points screen. The Work With Exit Points screen provides options that let you set up or maintain production or What If exit points. You can also use this screen to specify your own (customer) exit points. For more information, see “Work with Exit Points” on page 136.

Exit Point Summary

The following tables list the exit points included in RRM. The codes listed in the Journal Entry column indicate the following authorities:

R = Read
   Authority to read a file.

W = Write
   Authority to write a file.

X = Execute
   Authority to execute (run) a program.

M = Management
   Authority to create or delete objects.
### TCP/IP Exit Programs

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FTP CLIENT Request Validation—outgoing</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QTMF_CLIENT_REQ</td>
<td>VLRQ0100</td>
<td>FTPCLT</td>
<td>CN/DN/ON</td>
<td>NW0031E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session Initialization</td>
<td>X'0000'</td>
<td>INIT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create library/directory</td>
<td>X'0001'</td>
<td>MKDIR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete library/directory</td>
<td>X'0002'</td>
<td>RMDIR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set current directory</td>
<td>X'0003'</td>
<td>CD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>List file</td>
<td>X'0004'</td>
<td>LIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete file</td>
<td>X'0005'</td>
<td>DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send file</td>
<td>X'0006'</td>
<td>SEND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receive file</td>
<td>X'0007'</td>
<td>RECEIVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rename file</td>
<td>X'0008'</td>
<td>RENAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute CL command</td>
<td>X'0009'</td>
<td>COMMAND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exit Point</td>
<td>Format</td>
<td>Server</td>
<td>Journal Entry</td>
<td>Exit Program</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------</td>
<td>----------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>FTP Server Request Validation—incoming</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QTMF_SERVER_REQ</td>
<td>VLRQ0100</td>
<td>FTPSRV</td>
<td>CM/DM/OM</td>
<td>NW0031E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session Initialization</td>
<td>X'0000'</td>
<td>INIT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create library/directory</td>
<td>X'0001'</td>
<td>MKDIR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete library/directory</td>
<td>X'0002'</td>
<td>RMDIR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set current directory</td>
<td>X'0003'</td>
<td>CD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>List file</td>
<td>X'0004'</td>
<td>LIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete file</td>
<td>X'0005'</td>
<td>DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send file</td>
<td>X'0006'</td>
<td>SEND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receive file</td>
<td>X'0007'</td>
<td>RECEIVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rename file</td>
<td>X'0008'</td>
<td>RENAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute CL command</td>
<td>X'0009'</td>
<td>COMMAND</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FTP Server Logon</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QTMF_SVR_LOGON</td>
<td>TCPL0100</td>
<td>FTPSRV</td>
<td>CM/DM/OM</td>
<td>NW0032E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Server Logon</td>
<td>X'0000'</td>
<td>LOGON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exit Point</td>
<td>Format</td>
<td>Server</td>
<td>Journal Entry</td>
<td>Exit Program</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------</td>
<td>--------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>FTP Server Anonymous Logon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QTMF_SVR_LOGON</td>
<td>TCPL0200</td>
<td>FTPSRV</td>
<td>CM/DM/OM</td>
<td>NW0039E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R  W  X  M</td>
<td></td>
</tr>
<tr>
<td>Application Server Logon</td>
<td>X'0000'</td>
<td>LOGON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telnet Device Initialization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QTG_DEVINIT</td>
<td>INIT0100</td>
<td>TELNET</td>
<td>CQ/DQ/OQ</td>
<td>NW0033E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R  W  X  M</td>
<td></td>
</tr>
<tr>
<td>Application Server Logon</td>
<td>X'0000'</td>
<td>LOGON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telnet Device Termination</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QTG_DEVTERM</td>
<td>TERM0100</td>
<td>TELNET</td>
<td>CQ/DQ/OQ</td>
<td>NW0033E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R  W  X  M</td>
<td></td>
</tr>
<tr>
<td>REXEC Server Request Validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QTMX_SERVER_REQ</td>
<td>VLRQ0100</td>
<td>REXEC</td>
<td>CO/DO/OO</td>
<td>NW0032E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R  W  X  M</td>
<td></td>
</tr>
<tr>
<td>Session Initialization</td>
<td>X'0000'</td>
<td>SSNINIT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute CL command</td>
<td>X'0009'</td>
<td>COMMAND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>REXEC Server Logon</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QTMX_SVR_LOGON</td>
<td>TCPL0100</td>
<td>REXEC</td>
<td>CP/DP/OP</td>
<td>NW0032E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R  W  X  M</td>
<td></td>
</tr>
<tr>
<td>Application server logon</td>
<td>X'0000'</td>
<td>LOGON</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Trivial FTP

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trivial FTP</td>
<td>VLRQ0100</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R  W  X  M</td>
<td></td>
</tr>
<tr>
<td>Send file</td>
<td>X’0006’</td>
<td>SNDFILE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receive file</td>
<td>X’0007’</td>
<td>RCVFILE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Original Client Access

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Server</td>
<td>DTAQ0100</td>
<td>DTAQ</td>
<td>CA/DA/OA</td>
<td>NW0021E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R  W  X  M</td>
<td></td>
</tr>
<tr>
<td>Clear msg from data queue</td>
<td>CLEAR</td>
<td>- X - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create data queue</td>
<td>CREATE</td>
<td>- X - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete data queue</td>
<td>DELETE</td>
<td>- - - X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receive msg (nondestructive)</td>
<td>PEEK</td>
<td>X - - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Query data queue attributes</td>
<td>QRY ATT</td>
<td>X - - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receive msg (destructive)</td>
<td>RECEIVE</td>
<td>X - - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send msg to data queue</td>
<td>SEND</td>
<td>- X - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exit Point</td>
<td>Format</td>
<td>Server</td>
<td>Journal Entry</td>
<td>Exit Program</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------</td>
<td>---------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Remote SQL Request</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QRQ_SQL</td>
<td>RSQL0100</td>
<td>RTMSQL</td>
<td>CR/DR/OR</td>
<td>NW0037E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Connect to remote database</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create SQL package</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete current row of cursor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute SQL package</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run stored non-select stmt</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run SQL stmt w/parm marker</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare SQL package</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call iSeries program</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select DB records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select SQL package</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select DB recs w/ parm marker</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select DB records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update current row for cursor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exit Point</td>
<td>Format</td>
<td>Server</td>
<td>Journal Entry</td>
<td>Exit Program</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------</td>
<td>-----------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>File Transfer Function</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QTF_TRANSFER</td>
<td>TRAN0100</td>
<td>FILETFR</td>
<td>CT/DT/OT</td>
<td>NW0038E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Extract file path</td>
<td></td>
<td>EXTRACT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Join files</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replace file member (upload)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve file records (download)</td>
<td></td>
<td>SELECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open file</td>
<td></td>
<td>OPEN</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Message Function Server</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QMF_MESSAGE</td>
<td>MESS0100</td>
<td>MSGSRV</td>
<td>CT/DT/OT</td>
<td>NW0035E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Receive message</td>
<td></td>
<td>RECEIVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send message</td>
<td></td>
<td>SEND</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Virtual Print Server</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QVP_PRINTER</td>
<td>PRNT0100</td>
<td>VRTPRT</td>
<td>CU/DU/OU</td>
<td>NW0036E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Receive message</td>
<td></td>
<td>CHECK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send message</td>
<td></td>
<td>EXTRACT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open printer file</td>
<td></td>
<td>OPEN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### License Management

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>QIBM_QLZP_LICENSE</td>
<td>LICM0100</td>
<td>LICENSE</td>
<td>CV/DV/OV</td>
<td>NW0023E</td>
</tr>
</tbody>
</table>

#### Func Description

<table>
<thead>
<tr>
<th></th>
<th>Func #</th>
<th>Func Name</th>
<th>R</th>
<th>W</th>
<th>X</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release license</td>
<td></td>
<td>LICRLS</td>
<td>R</td>
<td>W</td>
<td>X</td>
<td>M</td>
</tr>
<tr>
<td>Request license</td>
<td></td>
<td>LICREQ</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Optimized Client Access Servers

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>QIBM_QPWFS_FILE_SERVE</td>
<td>PWFS0100</td>
<td>FILE</td>
<td>CI/DI/OI</td>
<td>NW0025E</td>
</tr>
</tbody>
</table>

#### Func Description

<table>
<thead>
<tr>
<th></th>
<th>Func #</th>
<th>Func Name</th>
<th>R</th>
<th>W</th>
<th>X</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocate conversation</td>
<td>X'0007'</td>
<td>ALLOCON</td>
<td>R</td>
<td>W</td>
<td>X</td>
<td>M</td>
</tr>
<tr>
<td>Change file attributes</td>
<td>X'0000'</td>
<td>CHGATT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create file/directory</td>
<td>X'0001'</td>
<td>CREATE</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Delete file/directory</td>
<td>X'0002'</td>
<td>DELETE</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>List file attributes</td>
<td>X'0003'</td>
<td>LISTATT</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Move file</td>
<td>X'0004'</td>
<td>MOVE</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Open file</td>
<td>X'0005'</td>
<td>OPEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Command Description

<table>
<thead>
<tr>
<th></th>
<th>Command</th>
<th>R</th>
<th>W</th>
<th>X</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>RO</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>WR</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Exit Point</td>
<td>Format</td>
<td>Server</td>
<td>Journal Entry</td>
<td>Exit Program</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------</td>
<td>--------</td>
<td>---------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>Rename file</td>
<td>RW</td>
<td></td>
<td>X X - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RWD</td>
<td></td>
<td>X X - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WRD</td>
<td>RENAME</td>
<td>X X - -</td>
<td>- - - X</td>
<td></td>
</tr>
</tbody>
</table>

**Database Server Initialization**

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>QIBM_QZDA_INIT</td>
<td>ZDAI0100</td>
<td>DBINIT</td>
<td>CD/DD/OD</td>
<td>NW0027E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Initiate DB server</td>
<td>X'0000'</td>
<td>ALLOCON</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Native Database Requests (data)**

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>QIBM_QZDA_NDB1</td>
<td>ZDAD0100</td>
<td>DBNDB</td>
<td>CE/DE/OE</td>
<td>NW0028E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Add file member</td>
<td>X'1802'</td>
<td>ADDMBR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear file member</td>
<td>X'1803'</td>
<td>CLRMBR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear save file</td>
<td>X'1808'</td>
<td>CLRSAVF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create database file</td>
<td>X'1801'</td>
<td>CRTDBF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create save file</td>
<td>X'1807'</td>
<td>CRTSAVF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create source PF</td>
<td>X'1800'</td>
<td>CRTSRCF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete database file</td>
<td>X'1809'</td>
<td>DLTF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete file member</td>
<td>X'1804'</td>
<td>DLTMBR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete file override</td>
<td>X'1806'</td>
<td>DLTOVR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Override database file</td>
<td>X'1805'</td>
<td>OVRDBF</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

QIBM_QZDA_NDB1 ZDAD0200 DBNDB CE/DE/OE NW0028E
<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Change library</td>
<td>X'180C'</td>
<td>CHGLIBL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Retrieve Object Information (package)

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>QIBM_QZDA_ROI1</td>
<td>ZDAR0100</td>
<td>DBROI</td>
<td>CF/DF/OF</td>
<td>NW0029E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Retrieve library info</td>
<td>X'1802'</td>
<td>LIBRARY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve relational DB info</td>
<td>X'1803'</td>
<td>RDB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve SQLPKG info</td>
<td>X'1808'</td>
<td>PKGINFO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve SQLPKG statement info</td>
<td>X'1801'</td>
<td>PKGSTMT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve file info</td>
<td>X'1807'</td>
<td>FILE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve member info</td>
<td>X'1800'</td>
<td>MEMBER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve record format info</td>
<td>X'1809'</td>
<td>RCDFMT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve field info</td>
<td>X'1804'</td>
<td>FIELD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve index info</td>
<td>X'1806'</td>
<td>INDEX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve column info</td>
<td>X'1805'</td>
<td>SPCLCOL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Retrieve Object Information (Keys)

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>QIBM_QZDA_ROI1</td>
<td>ZDAR0200</td>
<td>DBROI</td>
<td>CF/DF/OF</td>
<td>NW0029E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Retrieve foreign key info</td>
<td>X'1809'</td>
<td>FRGNKEY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve primary key</td>
<td>X'180A'</td>
<td>PRIMKEY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exit Point</td>
<td>Format</td>
<td>Server</td>
<td>Journal Entry</td>
<td>Exit Program</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------</td>
<td>--------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>SQL Requests (&lt;512 bytes)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QZDA_SQL1</td>
<td>ZDAQ0100</td>
<td>DBSQL</td>
<td>CG/DG/OG</td>
<td>NW0030E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Prepare SQLPKG</td>
<td>X'1800'</td>
<td>PREPARE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare and describe SQLPKG</td>
<td>X'1803'</td>
<td>PRPDESC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open/describe SQLPKG</td>
<td>X'1804'</td>
<td>OPNDESC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute SQLPKG</td>
<td>X'1805'</td>
<td>EXECUTE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute immediate</td>
<td>X'1806'</td>
<td>EXECIMM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connect remote database</td>
<td>X'1809'</td>
<td>CONNECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute immediate SQLPKG</td>
<td>X'180C'</td>
<td>FETCH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prep &amp; execute or prep &amp; open</td>
<td>X'180D'</td>
<td>PRPEXEC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open SQLPKG &amp; fetch row</td>
<td>X'180E'</td>
<td>OPNFCH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create SQLPKG</td>
<td>X'180F'</td>
<td>CRTPKG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear SQLPK</td>
<td>X'1810'</td>
<td>CLRPKG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete SQLPK</td>
<td>X'1811'</td>
<td>DLTPKG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute or Open SQLPK</td>
<td>X'1812'</td>
<td>EXECOPN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| SQL Requests (maximum 32k bytes) |         |        |               |              |
| QIBM_QZDA_SQL2             | ZDAQ0200 | DBSQL  | CG/DG/OG      | NW0030E      |
| Func Description           | Func #  | Func Name | R W X M      |
| Prepare SQLPKG             | X'1800' | PREPARE |              |
| Prepare and describe SQLPKG | X'1803' | PRPDESC |              |
| Open/describe SQLPKG       | X'1804' | OPNDESC |              |</p>
<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute SQLPKG</td>
<td>X'1805'</td>
<td>EXECUTE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute immediate SQLPKG</td>
<td>X'1806'</td>
<td>EXECIMM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connect remote database</td>
<td>X'1809'</td>
<td>CONNECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute immediate SQLPKG</td>
<td>X'1806'</td>
<td>FETCH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prep &amp; execute or prep &amp; open</td>
<td>X'180D'</td>
<td>PRPEXEC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open SQLPKG &amp; fetch row</td>
<td>X'180E'</td>
<td>OPNFCH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create SQLPKG</td>
<td>X'180F'</td>
<td>CRTPKG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear SQLPK</td>
<td>X'1810'</td>
<td>CLRPKG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete SQLPK</td>
<td>X'1811'</td>
<td>DLTPKG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute or Open SQLPK</td>
<td>X'1812'</td>
<td>EXECOPN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Data Queue Server

<table>
<thead>
<tr>
<th>QIBM_QZHQ_DATA_QUEUE</th>
<th>ZHQ0100</th>
<th>DATAQ</th>
<th>CX/DX/OX</th>
<th>NW0021E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R  W  X  M</td>
<td></td>
</tr>
<tr>
<td>Query data queue attributes</td>
<td>X'0001'</td>
<td>QRY ATT</td>
<td>X - - -</td>
<td></td>
</tr>
<tr>
<td>Receive msg (destructive)</td>
<td>X'0002'</td>
<td>RECEIVE</td>
<td>X - - -</td>
<td></td>
</tr>
<tr>
<td>Open/describe SQLPKG</td>
<td>X'0003'</td>
<td>CREATE</td>
<td>- X - -</td>
<td></td>
</tr>
<tr>
<td>Execute SQLPKG</td>
<td>X'0004'</td>
<td>DELETE</td>
<td>- - X -</td>
<td></td>
</tr>
<tr>
<td>Execute immediate SQLPKG</td>
<td>X'0005'</td>
<td>SEND</td>
<td>- X - -</td>
<td></td>
</tr>
<tr>
<td>Connect remote database</td>
<td>X'0006'</td>
<td>CLEAR</td>
<td>- X - -</td>
<td></td>
</tr>
<tr>
<td>Execute immediate SQLPKG</td>
<td>X'0007'</td>
<td>CANCEL</td>
<td>X - - -</td>
<td></td>
</tr>
<tr>
<td>Receive msg (nondestructive)</td>
<td>X'0012'</td>
<td>PEEK</td>
<td>X - - -</td>
<td></td>
</tr>
<tr>
<td>Exit Point</td>
<td>Format</td>
<td>Server</td>
<td>Journal Entry</td>
<td>Exit Program</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------</td>
<td>--------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Network Print Server Entry</td>
<td>ENTR0100</td>
<td>NETPRT</td>
<td>CY/DY/OY</td>
<td>NW0026E</td>
</tr>
<tr>
<td>QIBM_QNPS_ENTRY</td>
<td></td>
<td>NETPRT</td>
<td>CY/DY/OY</td>
<td>NW0026E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Initiate &amp; verify serve access</td>
<td>X'0802'</td>
<td>ENTRY</td>
<td>X X - -</td>
<td></td>
</tr>
<tr>
<td>Network Print Server Spooled File</td>
<td>SPLF0100</td>
<td>NETPRT</td>
<td>CY/DY/OY</td>
<td>NW0026E</td>
</tr>
<tr>
<td>QIBM_QNPS_SPLF</td>
<td></td>
<td>NETPRT</td>
<td>CY/DY/OY</td>
<td>NW0026E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Perform Spool function</td>
<td>X'010D'</td>
<td>SPLF</td>
<td>X - -</td>
<td></td>
</tr>
<tr>
<td>Remote Command/Distributed Program Call</td>
<td>CZRC0100</td>
<td>RMTCMD</td>
<td>CJ/DJ/OJ</td>
<td>NW0024E</td>
</tr>
<tr>
<td>QIBM_QZRC_RMT</td>
<td></td>
<td>RMTCMD</td>
<td>CJ/DJ/OJ</td>
<td>NW0024E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Distributed Program Call</td>
<td>X'1003'</td>
<td>PGMCALL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote command</td>
<td>X'1002'</td>
<td>RMTCMD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signon Server</td>
<td>ZSOY100</td>
<td>SIGNON</td>
<td>CB/DB/OB</td>
<td>NW0022E</td>
</tr>
<tr>
<td>QIBM_QZSO_SIGNONSERV</td>
<td></td>
<td>SIGNON</td>
<td>CB/DB/OB</td>
<td>NW0022E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Retrieve signon info</td>
<td>X'7004'</td>
<td>INFO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change password</td>
<td>X'7004'</td>
<td>CHGPWD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central Server Conversion Map</td>
<td>ZSCN100</td>
<td>CENTRAL</td>
<td>CC/DC/OS</td>
<td>NW0023E</td>
</tr>
<tr>
<td>QIBM_QZSC_NLS</td>
<td></td>
<td>CENTRAL</td>
<td>CC/DC/OS</td>
<td>NW0023E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Retrieve conversion map</td>
<td>X'1201'</td>
<td>RTVMAP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exit Point</td>
<td>Format</td>
<td>Server</td>
<td>Journal Entry</td>
<td>Exit Program</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------</td>
<td>--------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>Central Server Client Management:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QZSC_SM</td>
<td>ZSCS100</td>
<td>CENTRAL</td>
<td>CC/DC/OC</td>
<td>NW0023E</td>
</tr>
<tr>
<td>Func Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set client active (on)</td>
<td>X'1101'</td>
<td>CLACT</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Set client active (off)</td>
<td>X'1102'</td>
<td>CLINACT</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td><strong>Central Server License Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QIBM_QZSC_LM</td>
<td>ZSCS100</td>
<td>CENTRAL</td>
<td>CC/DC/OC</td>
<td>NW0023E</td>
</tr>
<tr>
<td>Func Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request license</td>
<td>X'1001'</td>
<td>LICREQ</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Release license</td>
<td>X'1002'</td>
<td>LICRLS</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Retrieve license information</td>
<td>X'1003'</td>
<td>LICINFO</td>
<td>R W X M</td>
<td></td>
</tr>
</tbody>
</table>

**Other Servers**

<table>
<thead>
<tr>
<th>Exit Point</th>
<th>Format</th>
<th>Server</th>
<th>Journal Entry</th>
<th>Exit Program</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DDM</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network attr: DDMACC</td>
<td>NA</td>
<td>DDM</td>
<td>CK/DK/OK</td>
<td>NW0034E</td>
</tr>
<tr>
<td>Func Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add member to file</td>
<td></td>
<td>ADDMBR</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Change file</td>
<td></td>
<td>CHANGE</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Exit Point</td>
<td>Format</td>
<td>Server</td>
<td>Journal Entry</td>
<td>Exit Program</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------</td>
<td>----------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Change member in file</td>
<td></td>
<td>CHGMBR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear member in file</td>
<td></td>
<td>CLEAR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute a command</td>
<td></td>
<td>COMMAND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copy file</td>
<td></td>
<td>COPY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create file</td>
<td></td>
<td>CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete file</td>
<td></td>
<td>DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extract file attributes</td>
<td></td>
<td>EXTRACT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initialize server</td>
<td></td>
<td>INIT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load</td>
<td></td>
<td>LOAD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lock</td>
<td></td>
<td>LOCK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Move</td>
<td></td>
<td>MOVE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open</td>
<td></td>
<td>OPEN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rename file</td>
<td></td>
<td>RENAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reorganize file member</td>
<td></td>
<td>RGZMBR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove file member</td>
<td></td>
<td>RMVMBR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rename file member</td>
<td></td>
<td>RNMMBR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrieve data area</td>
<td></td>
<td>RTDTARA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unload entry</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change data area</td>
<td></td>
<td>CHDTARA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear data queue</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receive data queue</td>
<td></td>
<td>RCVDTAQ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send data queue</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exit Point</td>
<td>Format</td>
<td>Server</td>
<td>Journal Entry</td>
<td>Exit Program</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------</td>
<td>--------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>DRDA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network attr: DDMACC</td>
<td>NA</td>
<td>DRDA</td>
<td>CL/DL/OL</td>
<td>NW0034E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name CONNECT</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>SQLCNN DRDA connection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ShowCase</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SC_QUERY_ROW_SEC</td>
<td>SCRS0100</td>
<td>SHWCASE</td>
<td>CW/DW/OW</td>
<td>NW0040E</td>
</tr>
<tr>
<td>Func Description</td>
<td>Func #</td>
<td>Func Name</td>
<td>R W X M</td>
<td></td>
</tr>
<tr>
<td>Alter Table</td>
<td>ALTER</td>
<td>W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Procedure</td>
<td>CALL</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment Table</td>
<td>COMMENT</td>
<td>W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Table</td>
<td>CREATE</td>
<td>W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete From Table</td>
<td>DELETE</td>
<td>W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drop Table</td>
<td>DROP</td>
<td>W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grant Authority</td>
<td>GRANT</td>
<td>W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insert into Table</td>
<td>INSERT</td>
<td>W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Label Table</td>
<td>LABEL</td>
<td>W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rename Table</td>
<td>RENAME</td>
<td>W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revoke Authority to Table</td>
<td>REVOKE</td>
<td>W</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exit Point</td>
<td>Format</td>
<td>Server</td>
<td>Journal Entry</td>
<td>Exit Program</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
<td>--------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Select from Table</td>
<td></td>
<td>SELECT</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Set Value</td>
<td></td>
<td>SET</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Update Table</td>
<td></td>
<td>UPDATE</td>
<td>W</td>
<td></td>
</tr>
</tbody>
</table>
B

Backup Files. Copies of secured entry files that are kept in case you want to restore the previous RRM configuration. When What If files are produced, the previous secured entry files become backup files. See “Secured Entry Files” and “What If Files”.

C

Calendar. The time and days of the week when a rule is in effect.

Collected Entry. A remote request files that has been collected but has not been secured by RRM. See “Secured Entry”.

D

Decision-making Algorithm. The processing component of RRM that determines whether incoming remote requests have the required authorities to access the RRM Server. See “RRM Server”.

Demote. Reverses the effect of promoting What If files to secured files by restoring the secured entry files to secured status and restoring the What If files to What If status. See “Promote” and “What If Files”.

E

Element. An RRM organizational structure such as a user, network address, or operation that can belong to groups but cannot contain groups or other elements.
Group Hierarchy. The hierarchy of groups containing other groups as members that includes the selected group.

Member. A user, address, operation, or group that belongs to an RRM group. See “Element”.

Network Address. An address within a network.

Operation. The server, function, and command reference of a remote transaction.

Primary Group. The most inclusive level of groups in a group hierarchy, which can contain other groups (supplemental groups) as members. See “Supplemental Group”.

Promote. The act of converting collected entries to secured entries, converting collected entries to What If entries, or converting What If entries to secured entries. When promoted, What If entries can be demoted from secured status back to What If status using the “demote” function. See “Demote”.

Processing Exit Program. One of two exit programs that work together to perform an RRM exit function. The other exit program is called the registered exit program. After the registered exit program identifies and calls the processing exit program, the processing exit program performs the specified exit function. See “Registered Exit Program”.

Registered Exit Program. One of two exit programs that work together to perform an RRM exit function. The second exit program is called a processing exit program. The registered exit program identifies the processing exit program associated with the exit point and determines the format of the information it receives. The registered exit program then reads an index to find the configuration of the processing exit program. See “Processing Exit Program”.

Remote Object Authority Table. The table where RRM stores remote object authority values.
Remote Request. A transaction that originates outside the RRM server. See “RRM Server”.

Report ID. The alphanumeric code (such as NW000002) that identifies each RRM report.

RRM Server. The iSeries server where RRM is installed.

Secure Mode. The exit point function that uses the Decision-making Algorithm to restrict access to incoming requests. See “Decision-making Algorithm”.

Secured Entry. An RRM record that specifies the authorities required to access the RRM server. Incoming requests are compared to secured entries to determine whether the requests have the authorities required to access the RRM server. See “Collected Entry”.

Secured Entry Files. Files that specify the authorities required to access the RRM server. Incoming requests are compared to secured entry files to determine whether the requests have the authorities required to access the RRM server. See “Backup Files” and “What If Processing”.

Supplemental Group. All levels of groups in a group hierarchy except the primary group, which contains all supplemental groups. See “Primary Group”

Swap Profile. A user profile that authorizes a user to complete a remote request when the other elements of the request do not provide enough authority.

User/Object Override. An authority (*PASS or *FAIL) specified for a user and an object that exceeds all other authorities, except a user/server override. See “User/Server Override”

User/Server Override. An authority (*PASS or *FAIL) specified for a user and a server that exceeds all other authorities.

What If Files. Secured or collected entry files that have been copied for What If processing. See “What If Processing”, “Backup Files”, and “Secured Entry Files”.

What If Playback. A function that executes a sample transaction using What If entries to produce a report that indicates the effects of those entries if implemented in a production environment. The report produced is called a What If report. See “What If Report”.

What If Playback. A function that executes a sample transaction using What If entries to produce a report that indicates the effects of those entries if implemented in a production environment. The report produced is called a What If report.
What If Processing. Processing copies of secured entry files to determine the effect of using a new RRM configuration before putting that configuration into production.

What If Report. A report based on What If settings used to test the effects of a new configuration. The report is generated by using the What If Playback function. See “What If Playback”.
Index

A
About xi
alert filters, setting up 146
alert messages 146
All RRM Reports menu 190
Allow FTP only between iSeries servers 289
authority, OS/400
  application-level 8
  object-level 6
  user-level 7

B
backup files 43

C
calendars 28
Change FTP Attribute (PSCHGFTP A) command 210
Change Telnet Attribute (PSCHGTELA) command 212
collection monitors, stop/start 209
commands
  Change FTP Attribute (PSCHGFTP A) 210
  Change Telnet Attribute (PSCHGTELA) 212
  Delete Collected Entries (PSRRMDLTC) 206
  Promote Collected Entries 114
  Restart Remote Servers (PSCYCLESVR) 205
  RRM Collection Monitor Control (PSRRMCMON) 209
  Run Report (PSRUNRPT) 167
  What If Playback 157
Configuration Reports menu 187
Configuration Wizard 214
Create Secured Entry screen 106
cycle remote servers (PSCYCLESVR) 205
D

DDMACC 202, 435, 437
Decision-making Algorithm
  examples 31
  overview 29
  processing flow 29
Delete Collected Entries command
  (PSRRMDLTC) 206

E

Enforce read-only access to files in library 295
exit point configuration 422
exit point summary 422
exit points
  configuration 422
  DDMACC 435, 437
  DRDA (DDMACC) 437
  overview 421
  QIBM_QHQ_DATAQUEUE 426
  QIBM_QLZP_LICENSE 429
  QIBM_QMF_MESSAGE 428
  QIBM_QNPS_ENTRY 434
  QIBM_QNPS_SPLF 434
  QIBM_QPWFS_FILE_SERVE 429
  QIBM_QRM_SQL 427
  QIBM_QTF_TRANSFER 428
  QIBM_QTG_DEVINIT 425
  QIBM_QTG_DEVTERM 425
  QIBM_QTMF_CLIENT 423
  QIBM_QTMF_SERVER_REQ 424
  QIBM_QTMF_SVR_LOGON 424, 425
  QIBM_QTMX_SERVER_REQ 425
  QIBM_QTMX_SVR_LOGON 425
  QIBM_QTOD_SERVER_REQ 426
  QIBM_QVP_PRINTWERS 428
  QIBM_QZDA_INIT 430
  QIBM_QZDA_NDB1 430
  QIBM_QZDA_ROI1 431
  QIBM_QZDA_SQL1 432
  QIBM_QZDA_SQL2 432
  QIBM_QZHQ_DATAQUEUE 433
  QIBM_QZRC_RMT 434
  QIBM_QZSC_LM 435
  QIBM_QZSC_NLS 434
  QIBM_QZSC_SM 435
  QIBM_QZSO_SIGNONSRV 434
  QIBM_QZDA_NDB1 430
  QIBM_QZDA_ROI1 431
  QIBM_QZDA_SQL1 432
  QIBM_QZDA_SQL2 432
  QIBM_QZHQ_DATAQUEUE 433
  QIBM_QZRC_RMT 434
  QIBM_QZSC_LM 435
  QIBM_QZSC_NLS 434
  QIBM_QZSC_SM 435
  QIBM_QZSO_SIGNONSRV 434
  SC_Query_ROW_SEC 437

exit programs
  central server client management
    (QIBM_QZSC_SM) 435
  central server conversion map
    (QIBM_QZSC_NLS) 434
  central server license management
    (QIBM_QZSC_LM) 435
  data queue server
    (QIBM_QHQ_DATAQUEUE) 433
  data queue server
    (QIBM_QZHQ_DATAQUEUE) 433
  database server initialization
    (QIBM_QZDA_INIT) 430
  DDM (DDMACC) 435
  file server
    (QIBM_QPWFS_FILE_SERVE) 429
  file transfer function
    (QIBM_QTF_TRANSFER) 428
  FTP client request validation—outgoing
    (QIBM_QTMF_CLIENT) 423
  FTP server anonymous logon
    (QIBM_QTMF_SVR_LOGON) 425
  FTP server logon
    (QIBM_QTMF_SVR_LOGON) 424
  FTP server request validation—incoming
    (QIBM_QTMF_SERVER_REQ) 424
  license management
    (QIBM_QLZP_LICENSE) 429
message function server
  (QIBM_QMF_MESSAGE) 428
native database request—
  (QIBM_QZDA_NDB1) 430
network print server entry
  (QIBM_QNPS_ENTRY) 434
network print server spooled file
  (QIBM_QNPS_SPLF) 434
remote command/distributed program
  call (QIBM_QZRC_RMT) 434
remote SQL request
  (QIBM_QRQ_SQL) 427
retrieve object information—keys
  (QIBM_QZDA_ROI1) 431
retrieve object information—package
  (QIBM_QZDA_ROI1) 431
REXEC Server logon
  (QIBM_QTMX_SVR_LOGON) 425
REXEC Server request validation
  (QIBM_QTMX_SERVER_REQ) 425
Showcase
  (SC_QUERY_ROW_SEC) 437
signon server
  (QIBM_QZSO_SIGNONSRV) 434
SQL requests— 432
SQL requests—max 32 KB
  (QIBM_QZDA_SQL2) 432
Telnet device initialization
  (QIBM_QTG_DEVINIT) 425
Telnet device termination
  (QIBM_QTG_DEVTERM) 425
trivial FTP
  (QIBM_QTOD_SERVER_REQ) 426
virtual print server
  (QIBM_QVP_PRINTWERS) 428

F
file types
  backup 43
  secured entry 43
  What If 43
Filter Definition screen 194
Filter/Threshold Definition screen 198
filters for reports 194, 198
Find and disable virus 299
FTP, change attribute 210
functions, major
  manage RRM 200
  work with calendars 127
  work with collected entries 101
  work with exit points 136
  work with RRM defaults 141
  work with RRM groups 118
  work with RRM object authorities 120
  work with RRM reports 165
  work with secured entries 53
  work with user/object overrides 133
  work with user/server overrides 130
  work with What If analysis 148

G
groups
  network 68, 71, 89
  operation 74, 77, 92, 95
  overview 26
  user 58, 62, 80
GUI, Operations Navigator
  detail pane 305
  environment pane 306
  list pane 305
  overview 304
H

Help, online 24
How to
   Allow FTP only between iSeries servers 289
   Enforce read-only access to files in library 295
   Find and disable virus 299
   Prevent addition of objects to library 293
   Restrict security officer activities 292

J

job schedulers, switch 201
journal entry codes 224

M

Main Menu 13
Maintain Calendar screen 98
Maintain Remote Object Authority screen 86, 123
Manage RRM menu 200

N

Network attr
   DDMACC (DDMACC) 437

O

Object Reports Menu 181
online Help 24
Operations Navigator plug-in
   administrative tools 396
   Calendars 340
   change FTP attributes 404
change Telnet attributes 406
Collected entries 306
Collected environment 306
cycle servers 402
default values 412
Exit Points 352
features 301
GUI 304
import configuration 399
overview 301
Remote Object Authorities 333
reports 372, 381
RRM Groups 325
Secured Entries 319
start/stop monitors 411
switch job scheduler 408
user preferences 410
User/Message Alerts 417
User/Object Overrides 348
User/Server Overrides 345
What If Calendars 374
What If Entries 365
What If environment 357
What If Exit Points 379
What If Remote Object Authorities 371
What If RRM Groups 366
What If User/Object Overrides 377
What If User/Server Overrides 376
option summary 49
options, primary
   1. Work with Secured Entries 53
   10. Work with What If Analysis 148
   2. Work with Collected Entries 101
   20. Work with RRM Reports 165
   3. Work with RRM Groups 118
   30. Manage RRM 200
   4. Maintain Remote Object Authority 86, 123
4. Work with RRM Object Authorities 120
5. Work with Calendars 127
6. Work with User/Server Overrides 130
7. Work with User/Object Overrides 133
8. Work with Exit Points 136
9. Work With RRM Defaults 141

OS/400
application-level authority 8
object-level authority 6
user-level authority 7
outfile 173, 391
output file 173, 391
overrides, user/object 133
overrides, user/server 130

P
PCSACC 202
Prevent *ALLOBJ users from accessing remote files 296
Prevent addition of objects to library 293
procedure
See how to
processing secured entries, overview 43
product flow 13
Promote Collected Entries command 114
PSCHGFTP A 210
PSCHGTELA 212
PSDetect
alert filters 146
working with 146
PSRRMCMON 209
PSRUNRPT 167
PSSecure Main Menu 13
PSWIPLAYBK 157

Q
QIBM_QHQ_DTAQ 426
QIBM_QLZP_LICENSE 429
QIBM_QMF_MESSAGE 428
QIBM_QNPS_ENTRY 434
QIBM_QNPS_SPLF 434
QIBM_QPWF _FILE SERVE 429
QIBM_QRQ_SQL 427
QIBM_QTF TRANSFER 428
QIBM_QTG_DEVINIT 425
QIBM_QTG_DEVTERM 425
QIBM_QTMF_CLIENT 423
QIBM_QTMF_SERVER_REQ 424
QIBM_QTMF_SRV_LOGON 424, 425
QIBM_QTMX_SERVER_REQ 425
QIBM_QTMX_SRV_LOGON 425
QIBM_QTOD_SERVER_REQ 426
QIBM_QVP_PRINTWERS 428
QIBM_QZDA_INIT 430
QIBM_QZDA_NDB1 430
QIBM_QZDA_ROI1 431
QIBM_QZDA_SQL1 432
QIBM_QZDA_SQL2 432
QIBM_QZHQ_DATA_QUEUE 433
QIBM_QZR C_RMT 434
QIBM_QZSC_LM 435
QIBM_QZSC_NLS 434
QIBM_QZSC_SM 435
QIBM_QZSO_SIGNONSRV 434
QPWFSERVER 202

R
recommended settings
restrict access to automatically started services 21
restrict powerful profiles with calendars 19
start collecting requests 18
start logging incoming transactions 19
remote object authority, overview 28
remote transactions, overview 5
report IDs 175
report summary 216
reports, configuration
  Remote Object Authority By User report 285, 286
reports, exit point settings
  Exit Point Settings report 274
reports, filters 194, 198
reports, master file
  Calendar report 282
  Network Group report 280
  Operation Group report 281
  Secured Entries report 272
  User Group report 278
reports, object
  Object Report by Date/Time 247
  Object Report by Function 249
  Object Report by Incoming Address 251
  Object Report by Library/Object 246
  Object Report by Server 250
  Object Report by User 248
reports, summary
  Collected Entries Report 259
  RRM Audit Report 258
  Transaction Summary by Server 253
  Transaction Summary by User 256
reports, transaction
  Data Queue Optimized Server Requests report 237
  Data Queue Original Server Requests report 236
  Database Server Requests report 232
  DDM Request Access report 228
  File Server Requests report 231
  FTP Logon and Server Requests report 222
  Network Print Server Entry Requests report 239
  Network Print Server Spool File Requests report 240
  Network Transactions by Date/Time report 241
  Network Transactions by Function report 243
  Network Transactions by Incoming Address report 245
  Network Transactions by Server report 244
  Network Transactions by User report 242
  Remote SQL Server Requests report 235
  TCP Signon Server Requests report 227
  Transfer Function Server Requests report 229
reports, What If
  What If Transaction by Date/Time 263
  What If Transaction by Function 268
  What If Transaction by Incoming Address 270
  What If Transaction by User 266
  What If Transaction Summary by Server 269
Restart Remote Servers (PSCYCLESVR) command 205
Restrict QSECOFR and all members 293
Restrict security officer activities 292
RRM
  navigation 13
  product flow 13
  screen layout 13
  security considerations 5
  usage considerations 9
RRM Collection Monitor Control
(PSRRMCMON) command 209
RRM Configuration Wizard 214
RRM exit programs, remove all 201
RRM Main Menu 13
Run Report (PSRUNRPT) command screen 167

S

SC_QUERY_ROW_SEC 437
screen layout 13
screens
All RRM Reports menu 190
Configuration Reports menu 187
Create Secured Entry 106
Filter Definition 194
Filter/Threshold Definition 198
Maintain Calendar 98
Maintain Remote Object Authority 86, 123
Manage RRM menu 200
Object Reports Menu 181
PSSecure Main Menu 13
RRM Main Menu 13
Select 66
Summary/Statistics Reports menu 183
Transaction Reports menu 177
What If Reports menu 163, 185
Work with Calendars 127
Work With Collected Entries 101
Work with Collected Objects 111
Work With Exit Points 136
Work With Exit Programs 202
Work With Filters 192
Work with Network Group Members 71, 89
Work with Remote Groups 68

Work with Operation Group Members 77
Work with Operation Groups 74, 92, 95
Work With RRM Defaults 141
Work with RRM Groups menu 118
Work With RRM Object Authority 120
Work with RRM Reports menu 165
Work With Secured Entries 53
Work With User Group Members 83
Work with User Group Members 62
Work with User Groups 58, 80
Work With User/MsgQ Alerts 143
Work With User/Object Overrides 133
Work With User/Server Overrides 130
Work with What If Analysis menu 148
Work with What If RRM Groups 151
secured entry files 43
Select Screen 66
Summary/Statistics Reports menu 183
swap profile, overview 29

T

task
See how to
Telnet, change attribute (PSCCHGTELA) 212
Transaction Reports menu 177

U

usage scenarios
Allow FTP only between iSeries servers 289
Enforce read-only access to files in library 295
Find and disable virus 299
Prevent *ALLOBJ users from accessing remote files 296
Prevent addition of objects to library 293
Restrict QSECOFR and all members 293
Restrict security officer activities 292
user interface 5
user/object override 27
user/object overrides 133
user/server override 27

W

What If entry files 43
What If Playback (PSWIPLAYBK) command 157
What If processing 45
What If Reports menu 163, 185
Work with Calendars screen 127
Work With Collected Entries screen 101
Work with Collected Objects screen 111
Work With Exit Points screen 136
Work With Exit Programs screen 202
Work With Filters screen 192
Work with Network Group Members screen 71, 89
Work with Network Groups screen 68
Work with Operation Group Members screen 77
Work with Operation Groups screen 74, 92, 95
Work With RRM Defaults screen 141
Work with RRM Groups menu 118
Work With RRM Object Authority screen 120
Work with RRM Reports menu 165
Work With Secured Entries screen 53
Work With User Group Members screen 83
Work with User Group Members screen 62
Work with User Groups screen 58, 80
Work With User/MsgQ Alerts screen 143
Work With User/Object Overrides screen 133
Work With User/Server Overrides screen 130
Work with What If Analysis menu 148
Work with What If RRM Groups menu 151