Contents

NetIQ Security Solutions for iSeries 8.0 Compatibility with i5/OS V6R1

Technical Reference

December 1, 2008

NetIQ Security Solutions for iSeries 8.0 continues to help you eliminate security risks and maintain business continuity across your iSeries servers when you upgrade your operating system to i5/OS V6R1.

NetIQ has provided PTFs to ensure all the functionality you have come to expect from PSAudit, PSDetect, PSSecure, Privilege Manager, and integration with Security Manager and Secure Configuration Manager is fully operational on servers running i5/OS V6R1.

This Technical Reference provides information about i5/OS V6R1 upgrade requirements and PTFs for known compatibility issues with NetIQ Security Solutions for iSeries.

NetIQ Security Solutions for iSeries Requirements for Upgrading to i5/OS V6R1

Before upgrading your operating system, review the following pre- and post-upgrade NetIQ Security Solutions for iSeries 8.0 product requirements.

Warning
You must apply IBM PTF MF44237 *before* accessing the NetIQ Security Solutions for iSeries product. For more information, see "Post-Upgrade Requirements" on page 2.

Pre-Upgrade Requirements

Before upgrading your operating system to i5/OS V6R1, you must perform the following steps:

1. Permanently apply all currently applied NetIQ Security Solutions for iSeries PTFs by typing the following command on the iSeries command line and pressing Enter.

   ```
   APYPTF LICPGM(1PSA001) RLS(V8R0M0) SELECT(*ALL) APY(*PERM)
   DELAYED(*NO)
   ```

   Note
   It is not necessary to perform an IPL. You can run the command interactively.

2. Repeat Step **1** for licensed programs 1PSC001, 1PSD001, 1PSI001, 1PSP001 and 1PSS001.

3. ***If you are using PSSecure Profile and Password Management to monitor user profiles***, remove the Q* entry from the exclusions list and hold the PSPROFILE scheduled job. The i5/OS V6R1 upgrade can remove and replace one of the IBM "Q" profiles. To remove the entry:

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

   b. ***If the PSPROFILE job is scheduled***, put it on hold.

   c. From the NetIQ Product Access Menu, type `2` (PSSecure) and press Enter.

   d. Type `2` (Profile and Password Management) and press Enter.

   e. Type `1` (General Options Menu) and press Enter.

   f. Type `17` (User Profile Exclusions) and press Enter.

   g. Remove the entry for Q*.

Post-Upgrade Requirements

After completing the operating system upgrade, you must complete the following steps:

1. Apply IBM PTF MF44237 *before* accessing the NetIQ Security Solutions for iSeries product.

   Warning
   If you do not apply **IBM PTF MF44237** before accessing the NetIQ Security Solutions for iSeries product, your system may hang and you will be required to perform an IPL to regain control of your system. This issue occurs due to operating system changes introduced in the V6R1 release.

   Any job that attempts to access PSPasswordManager, run the STROBJCVN command on library PSSECURE, or attempts a new installation of the NetIQ Security Solutions for iSeries product with system value QFRCCVNRST set to 1 or greater *before* applying PTF MF44237 will hang. Subsystems processing these jobs cannot be ended. The only way to end the hung job is through a forced power down of the system.

   For more information about IBM PTF MF44237, see IBM APAR MA36364.

2. ***If you removed the Q* entry from the exclusion list and set the PSPROFILE job to Hold***, re-add the Q* entry to the exclusion list and release the PSPROFILE scheduled job.

Known i5/OS V6R1 Compatibility Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your security needs. We have tested all NetIQ Security Solutions for iSeries products on systems running i5/OS V6R1 and have identified the following issues:

NetIQ Corporation has resolved the following known i5/OS V6R1 compatibility issues:

PSAudit - System Auditing and Reporting (SAR)

PTF 1A03008 resolves an issue where the SQL/QRY Audit Report does not contain detail data.

To resolve an issue where the SQL/QRY Monitor ends as soon as it is started, issue the following commands from the iSeries command line:

```
RNMOBJ PSAUDIT/SAR0514F *FILE SAR0514F80

CRTDUPOBJ OBJ(QAQQDBMN) FROMLIB(QSYS) OBJTYPE(*FILE)
TOLIB(PSAUDIT) NEWOBJ(SAR0514F)

CHGOBJOWN PSAUDIT/SAR0514F *FILE NEWOWN(PSOBJOWN)

GRTOBJAUT PSAUDIT/SAR0514F *FILE REFOBJ(PSAUDIT/
SAR0514F80)
```

PSSecure - Remote Request Management

PTF 1C03087 resolves an issue where Remote Request Management (RRM) collects incorrect IP addresses causing remote transactions secured by network addresses to fail.

Secure Configuration Manager Integration

PTF 1C03085 resolves an issue where Secure Configuration Manager agent registration does not complete normally, which prevents you from running tasks, security checks, and policy templates against an iSeries server.

Known compatibility issues with i5/OS V6R1:

Operations Navigator Plug-in for RRM

You cannot install the Operations Navigator plug-in for RRM on iSeries servers running i5/OS V6R1. If you currently have the Operations Navigator plug-in for RRM installed on an iSeries server running an earlier version of the operating system, the Operations Navigator plug-in for RRM will continue to operate after you upgrade to i5/OS V6R1.

If you need further assistance with any issue, please contact NetIQ Technical Support at support@netiq.com.

Previous Operating System Version Compatibility

NetIQ Security Solutions for iSeries 8.0 continues to support the following operating system features provided in previous operating system releases.

QAUDCTL System Value Support

The Security Manager Monitor Console displays events triggered for a change to system value QAUDCTL under **All Other iSeries Alerts** instead of **QAUDCTL System Value Changed**. The PSDetect QuickStart Wizard uses a previous operating system version message ID when creating a filter to monitor for changes to QAUDCTL.

To manually change the message ID:

1. From the NetIQ Product Access Menu, type 3 (PSDetect) and press Enter.
2. Type `3` (Work with Alert Filters) and press Enter.
3. Type `5` (Work with Filters) to the left of the QHST alert filter and press Enter.
4. Type `5` (Work with Filter Details) to the left of the Monitor QAUDCTL Changes filter and press Enter.
5. Type `2` (Change) to the left of message ID CPF1806 and press Enter.
6. In the **Message ID** field, type `CPF180F` and press Enter.

Password Level Support

You can control password values and restrictions on your iSeries server by setting the password level system value QPWDLVL. The password level defines the maximum number of characters used in a password, as well as how your iSeries passwords affect communication with other systems in a network.

NetIQ Security Solutions for iSeries 8.0 components support password level 0, which uses the following standards:

- Allows a password length of 10 characters or less
- Restricts passwords from beginning with a numeric character or underscore
- Supports conversion to uppercase EBCDIC characters, including A through Z, 0 through 9, @, #, _, and $

The following sections describe how setting password levels 1, 2, and 3 affect NetIQ Security Solutions for iSeries components.

PSSecure Profile and Password Management

Profile and Password Management (PPM) helps you manage user profiles and control users' passwords on iSeries servers when QPWDLVL is set to 0 or 1. Except for specific User Profile Management (UPM) functions, PPM does not support password levels higher than 1.

Setting QPWDLVL to 2 or 3 causes the following limitations:

- Users cannot access all menu options.
- PPM does not send password expiration warning messages.
- PPM redirects users to the IBM Change Password screen when they enter an expired password.
- Users cannot synchronize profiles and passwords.

The PSPROFILE job allows you to automatically disable, delete, and archive inactive user profiles on your system. If you want to use the PSPROFILE job and other UPM functions on NetIQ Security Solutions for iSeries 8.0, apply NetIQ Security Solutions for iSeries PTF 1S03001.

PSAudit System Auditing and Reporting

System Auditing and Reporting (SAR) Profiles with Weak Passwords and 10 Point Security Check-up reports provide an analysis of the user profile passwords used in your environment. Running these reports regularly helps identify passwords that are not compliant with your company's password policy.

SAR provides the following support for operating system password levels.

QPWDLVL Setting	SAR Support
0	The Profiles with Weak Passwords and 10 Point Security Check-up reports identify weak passwords.
1	The Profiles with Weak Passwords report does not provide user profile information and the 10 Point Security Check-up report provides the password level setting instead of a pass or fail rating.

QPWDLVL Setting	SAR Support
2	You can use the Profiles with Weak Passwords and 10 Point Security Check-up reports only if your passwords meet the standard used in password level 0.
3	The Profiles with Weak Passwords report does not provide user profile information and the 10 Point Security Check-up report provides the password level setting instead of a pass or fail rating.

PSPasswordManager

PSPasswordManager checks for compliance with existing operating system password composition rules. PSPasswordManager also uses a customizable pre-defined word list beyond operating system native capabilities to enforce the use of well-constructed passwords.

PSPasswordManager provides the following support for operating system password levels.

QPWDLVL Setting	PSPasswordManager Support
0	PSPasswordManager functions without limitations.
1	PSPasswordManager does not function.
2	You can use PSPasswordManager only if your passwords meet the standard used in password level 0.
3	The PSPasswordManager component does not function.

Using NetIQ Security Solutions for iSeries 8.0 with Multiple IASPs

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

Most NetIQ Security Solutions for iSeries components reference only objects located in the Base System ASP. However, you can configure some components to reference objects located in any IASP by issuing the SETASPGRP command or specifying an IASP through the job description.

The following sections describe how multiple IASPs affect each NetIQ Security Solutions for iSeries component.

PSAudit System Auditing and Reporting

You can analyze security risks, ensure policy compliance, and secure your IASPs using Secure Configuration Manager task reports. These task reports provide the name of the IASP from which NetIQ Security Solutions for iSeries gathered QAUDJRN log data. You can also run these IASP reports through iSeries terminal emulation using the PSRUNRPT command.

For more information about IASP support, see the *NetIQ Security Solutions for iSeries Installation Guide*.

PSAudit Data Auditing and Reporting

Data Auditing and Reporting (DAR) can audit files across multiple IASPs and provide the ASP group name for a file in the heading of the File Accessed and Changed Data reports.

To use DAR to track changes made to a file that exists in libraries located in multiple IASPs, the files must have identical layouts. For example, if MYLIB/MYFILE exists in both the Base System ASP and MYASP IASP, these two files must have identical layouts. DAR can audit and run reports for both files.

Before adding a file located in an IASP to DAR or producing a DAR report, specify the appropriate IASP by either issuing the SETASPGRP command or specifying the IASP in the job description. For more information about changing a job description, see the IBM documentation.

To add a file in an IASP to DAR:

1. Specify the IASP for the current job by typing the following command and pressing Enter.

   ```
   SETASPGRP ASPGRP(IASPNAME)
   ```

   where *IASPNAME* is the name of the IASP where the file is located.

2. Access the Work with Files screen by executing the following option string starting at the NetIQ Product Access Menu:

   Opt 1 (PSAudit) > 3 (Data Auditing and Reporting)

3. Press F6 to access the **Add Files to be Journaled** window.
4. Specify the name of the file you want to monitor, and press Tab.
5. Specify the name of the library where the file is located, and press Enter.

PSSecure Remote Request Management

RRM assumes objects are located in the Base System ASP unless the remote transaction fully qualifies an object in IFS notation. If you are using RRM to secure your server at the object level, all remote transactions must provide explicit object paths.

When remote transactions fully qualify an object located in IASP, RRM correctly collects and secures the object.

The following procedure describes how to perform an FTP transfer of a fully qualified object in the example MYASP IASP.

To retrieve MYLIB/MYFILE from MYASP IASP:

1. From a PC DOS window, type the following command and press Enter.

   ```
   FTP system_ip
   ```

2. Enter your iSeries user name and press Enter.
3. Enter your iSeries password and press Enter.
4. Type the following command and press Enter.

   ```
   binary
   ```

5. Type the following command and press Enter.

   ```
   quote site namefmt 1
   ```

6. Type the following command and press Enter.

   ```
   get /MYASP/QSYS.LIB/MYLIB.LIB/MYFILE.FILE/MYFILE.MBR
   C:\MYFILE.MBR
   ```

7. Type the following command and press Enter.

   ```
   quit
   ```

8. On your iSeries server, access the Work With Collected Entries screen by executing the following option string starting at the NetIQ Product Access Menu:

   Opt 2 (PSSecure) > **3 (Remote Request Management)** > **2 (Work with Collected Entries)**

9. Type `10` (Object) in the **Op** field to the left of the FTP SEND entry and press Enter to display the object path. RRM displays the collected object path in the following format:

   ```
   /MYASP/QSYS.LIB/MYLIB.LIB/MYFILE.FILE/MYFILE.MBR
   ```

   The variables in this format are defined as follows:

   `MYASP`: Specifies the name of your IASP.

   `MYLIB.LIB`: Specifies the name of the library where the document is located on your IASP.

   `MYFILE.FILE`: Specifies the name of the file located on your IASP.

   `MYFILE.MBR`: Specifies the name of the member contained in the file located on your IASP.

PSSecure Object Authority Management

You can use Object Authority Management (OAM) with any object located in the Base System ASP or in the OAM job's IASP. To use OAM with objects in different IASPs, you must either issue the SETASPGRP command or specify the IASP in the job's description. For more information about changing a job description, see the IBM documentation.

The following procedure describes how to set authority for the example MYLIB/MYFILE based on MYTEMPLATE using the SETASPGRP command.

To set authority based upon an OAM template:

1. Specify the IASP for the current job by typing the following command and pressing Enter:

   ```
   SETASPGRP ASPGRP(IASPNAME)
   ```

   where *`IASPNAME`* is the name of the IASP where the file is located.

2. Set the authority of the file by typing the following command and pressing Enter.

   ```
   PSSECURE/STROAMAPI TEMPLATE(MYTEMPLATE) LIB(MYLIB)
   OBJ(MYFILE) TYPE(*FILE) CMPLFLG(*YES)
   ```

PSSecure Secure File Editor

You can use Secure File Editor (SFE) with any file located in the Base System ASP or in the SFE job's IASP. To use SFE with files in different IASPs, you must either issue the SETASPGRP command or specify the IASP in the job's description. For more information about changing a job description, see the IBM documentation.

The following procedure describes how to edit the example MYLIB/ MYFILE, which is located in the MYASP and MYOTHASP IASPs.

To edit a file located in a library within two IASPs:

1. Specify MYASP IASP for the current job by typing the following command and pressing Enter.

   ```
   SETASPGRP ASPGRP(MYASP)
   ```

2. Edit MYLIB/MYFILE with SFE by typing the following command and press Enter.

   ```
   DBA FILE(MYLIB/MYFILE)
   ```

3. Specify MYOTHASP IASP for the current job by typing the following command and pressing Enter.

   ```
   SETASPGRP ASPGRP(MYOTHASP)
   ```

4. Edit MYLIB/MYFILE with SFE by typing the following command and press Enter.

   ```
   DBA FILE(MYLIB/MYFILE)
   ```

PSDetect

PSDetect monitors only message queues located in the Base System ASP. PSDetect cannot monitor message queues located in an IASP.