NetIQ Security Solutions for iSeries 8.0 Compatibility with i5/OS V5R4

Technical Reference

May 1, 2006

Contents

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 V5R4.

NetIQ is currently working on PTFs to ensure all the functionality you have come to expect from PSAudit, PSDetect, PSPasswordManager, and PSSecure is fully operational on servers running i5/OS V5R4.

This Technical Reference provides information about known compatibility issues, password levels, and procedures for using NetIQ Security Solutions for iSeries 8.0 components with Independent Auxiliary Storage Pools (IASPs).

Note
Before upgrading your operating system to i5/OS V5R4, you must permanently apply all currently applied NetIQ Security Solutions for iSeries PTFs by issuing the APYPTF command.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, Provider-1, SiteManager-1, and VPN-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveReporting, ADcheck, AppAnalyzer, AppManager, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Knowing is Everything, Knowledge Scripts, Mission Critical Software for E-Business, MP3check, NetConnect, NetIQ, the NetIQ logo, NetIQ Change Administrator, NetIQ Change Guardian, NetIQ Compliance Suite, NetIQ Group Policy Administrator, NetIQ Group Policy Guardian, NetIQ Group Policy Suite, the NetIQ Partner Network design, NetIQ Patch Manager, NetIQ Risk and Compliance Center, NetIQ Security Administration Suite, NetIQ Security Analyzer, NetIQ Security Manager, NetIQ Vulnerability Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Server Consolidator, VigilEnt, Vivinet, Work Smarter, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Known V5R4 Compatibility Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your security needs. The following V5R4 compatibility issues are currently being researched. If you need further assistance with any issue, please contact Technical Support (support@netiq.com).

PSAudit – System Auditing and Reporting (SAR)

V5R4 operating system changes affect the following SAR features:

- The SQL/QRY Monitor ends as soon as it is started or the SQL/QRY Audit Report does not show data.
- Loading the File, Object, and Library Database fails. When the File, Object, and Library Database load fails, data is not available for those reports that depend on this database as an information provider. The reports dependent on this database have the field “Last database load” in the submittal window for the report. This report information is not available when you run Vulnerability Manager reports.
- Adding libraries to the Inclusion/Exclusion List for the File, Object, and Library Database fails.

PSSecure – Inactive Session Monitor

Inactive Session Monitor does not time out sessions exceeding the maximum allowed period of inactivity.

PSDetect

The V5R4 release changed the message ID used to monitor changes to QAUDCTL. PSDetect QuickStart Wizard uses the pervious 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**.

Security Manager Integration

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**.

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.

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.
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 predefined word lists 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 Vulnerability Manager 5.5 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

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 IASO 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.