NetIQ Security Solutions for IBM i 8.1 - Compatibility with IBM i 7.2

Technical Reference

SEPTEMBER 2015

NetIQ Security Solutions for IBM i 8.1 continues to help you eliminate security risks and maintain business continuity across your IBM i servers when you upgrade your operating system to IBM i 7.2.

NetIQ has provided PTFs to ensure all the functionality you have come to expect from PSAudit, PSDetect, and PSSecure is fully operational on servers running IBM i 7.2.

This Technical Reference provides information about IBM i 7.2 upgrade requirements and PTFs available to address known compatibility issues with NetIQ Security Solutions for IBM i.

Legal Notice

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.

Planning Your IBM i 7.2 Upgrade

This section addresses issues to consider and provides steps to follow before upgrading your operating system to IBM i 7.2 on systems running NetIQ Security Solutions for IBM i 8.1.

Upgrade Checklist

Review the following checklist items before upgrading to IBM i 7.2.

NetIQ Sentinel Agent Manager (SAM) Processing Issues

If you use NetIQ Sentinel Agent Manager (SAM) for IBM i to collect IBM i logs, consider upgrading to IBM i 7.2 when you have no batch processes scheduled. The upgrade process can generate a large volume of journal entries in the QAUDJRN, depending on the journal settings. Processing these journal entries will require additional time and can severely affect jobs in SAM and the PSAudit System Auditing and Reporting (SAR) function.

Permanently Apply PTFs

Before upgrading your operating system to IBM i 7.2, you must permanently apply all currently applied NetIQ Security Solutions for IBM i PTFs.

TO PERMANENTLY APPLY PTFS:

1. Type the following command on the IBM i command line.

   ```
   APYPTF LICPGM(1PSA001) RLS(V8R1M0) SELECT(*ALL) APY(*PERM)
   DELAYED(*NO)
   ```

   Note You can run the command interactively. It is not necessary to perform an IPL after applying the NetIQ PTFs.
2. Press **Enter**.
3. Repeat Steps **1** and **2** for licensed programs 1PSC001, 1PSD001, 1PSI001, and 1PSS001.

Checklist Items

□ 1. ***If you use NetIQ Sentinel Agent Manager to audit IBM i log data,*** determine the best time to perform the upgrade. For more information, see “NetIQ Sentinel Agent Manager (SAM) Processing Issues” above.

□ 2. Review the known issues described in “Known IBM i 7.2 Compatibility Issues” below.

□ 3. Permanently apply all currently applied NetIQ Security Solutions for IBM i PTFs for all licensed programs: 1PSA001, 1PSC001, 1PSD001, 1PSI001, and 1PSS001. For instructions, see “Permanently Apply PTFs” above.

□ 4. ***If you are using PSSecure Profile and Password Management to monitor inactive user profiles,*** remove the Q* exclusion from the User Profile Management feature and hold the PSPROFILE scheduled job. For more details and instructions, see “Remove the Q* Exclusion” below.

□ 5. ***After upgrading to IBM i 7.2,*** re-add the Q* exclusion to the User Profile Management feature and start the PSPROFILE scheduled job. For instructions, see “Re-Add the Q* Exclusion” below.

Remove the Q* Exclusion

The upgrade to IBM i 7.2 can remove and replace one of the IBM “Q” profiles. If you are using PSSecure Profile and Password Management (PPM) to monitor inactive user profiles, you must remove the Q* exclusion from the PPM User Profile Management function. You must also hold the PSPROFILE scheduled job.

TO REMOVE THE Q* EXCLUSION FROM PPM:

1. On the command line, type `WRKJOBSCDE`, and then press **Enter**.
2. **If the PSPROFILE job is scheduled,** put it on hold.
3. From the NetIQ Product Access Menu, type 2 (PSSecure), and then press **Enter**.
4. Type 2 (Profile and Password Management), and then press **Enter**.
5. Type 1 (General Options Menu), and then press **Enter**.
6. Type 17 (User Profile Exclusions), and then press **Enter**.
7. Remove the entry for Q*.

Re-Add the Q* Exclusion

After you upgrade to IBM i 7.2, you must re-add the Q* exclusion to the PPM User Profile Management function and release the PSPROFILE scheduled job. For more information, see “Remove the Q* Exclusion” above.

Known IBM i 7.2 Compatibility Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your security needs. We have tested all NetIQ Security Solutions for IBM i products on systems running IBM i 7.2. This section describes known issues found during compatibility testing and any available PTFs for remediation.

Licensing

Purchase and Demo Screen Returns Incorrect OS Version

PTF 1C04064 resolves an issue where the wrong operating system version is displayed on the Purchase and Demo Screen.

TO ACCESS THE PURCHASE AND DEMO SCREEN FROM THE IBM I COMMAND LINE:

1. Type `PSMENU`, and then press **Enter**.
2. Type `80` (Enter access codes), and then press **Enter**.

PSAudit - System Auditing and Reporting (SAR)

SQL/QRY Monitor Stops Collecting Data

PTF 1A04014 resolves an issue where data is fully or partially missing from the SQL/QRY Audit Report after an OS upgrade or after a Technology Refresh (TR) is applied.

Object Authority by Object Report Ends Abnormally

PTF 1A04013 resolves an issue where the Object Authority by Object report fails when run for a large number of objects. The following message is shown in the job log: “Job message queue for &3/&2/&1 cannot be extended. Job ended.”

Object Authority by User Report Ends Abnormally

PTF 1A04013 resolves an issue where the Object Authority by User report fails when run for a large number of objects. The following message is shown in the job log: “Job message queue for &3/&2/&1 cannot be extended. Job ended.”

PSAudit - Data Auditing and Reporting (DAR)

View Data Failure

PTF 1A04012 resolves an issue where the View Data (Option 5) option fails.

PSSecure - Object Authority Management (OAM)

Generate Authority File Failure

PTF 1A04013 resolves an issue where the job submitted through Option 20 (Generate Authority File) of the OAM main menu fails when run for a large number of objects. The following message is shown in the job log: “Job message queue for &3/&2/&1 cannot be extended. Job ended.”

Non-Comp Report/Force Compliance (STROAMAPI) Failure

PTF 1S04007 resolves an issue where the STROAMAPI command fails when run for a large number of objects. The following message is shown in the job log: “Job message queue for &3/&2/&1 cannot be extended. Job ended.”

The STROAMAPI command can be accessed through the command line or through the Non-Comp Report/Force Compliance option (Option 10) of the OAM main menu.

PSSecure - Profile and Password Management (PPM)

Cannot Support New User Profile Parameters

IBM i 7.2 introduced the new user profile parameter: “Maximum allowed storage large” (MAXSTGLRG). Change and create user profile functions within the following NetIQ product components do not support this new parameter:

- PSSecure Profile and Password Management (PPM)
- Secure Configuration Manager (SCM) - Profiles object
- Sentinel Agent Manager for IBM i

Note that these NetIQ product components also do not support the following user profile parameters:

- Character identifier control (CHRIDCTL)
- Locale job attributes (SETOBJATR)
- Locale (LOCALE)
- EIM association (EIMASSOC)
- User expiration date (USREXPDATE)
- User expiration interval (USREXPITV)
- Block password change (PWDCHGBLK)
- Local password management (LCLPWDMGT)

Cannot Support New Permissible Values for Limited Device Sessions

PTF 1S04008 adds support for new permissible values (1-9) for the Limited Device Sessions (LMTDEVSSN) user profile parameter in the Profile Templates feature.

PSDetect - QuickStart Configuration Wizard

Email Support Configuration Failure

PTF 1C04063 resolves an issue where the PSDetect QuickStart Configuration Wizard fails when attempting to configure email support.

QAUDCTL Incorrect Alert Filter Creation

PTF 1C04063 resolves an issue where an incorrect message ID is added when creating an alert filter to monitor for changes to QAUDCTL. The correct message ID, CPF180F, is now used.

SM/IM Alerts Created with Incorrect User Name

PTF 1C04063 resolves an issue where SM/IM alerts are created with the wrong user name parameter.

Operations Navigator Plug-in for RRM

No Longer Supported

You cannot install the Operations Navigator Plug-in for Remote Request Management (RRM) on any systems running an IBM i 6.1, 7.1, or 7.2 Navigator client.

Previous Operating System Version Compatibility

NetIQ Security Solutions for IBM i 8.1 continues to support the following IBM 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 8.1 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. PSPROFILE job and other UPM functions will work at password level 2 and 3.

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 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.

Using NetIQ Security Solutions for iSeries 8.1 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.
   ```
   SETASPGRP ASPGRP(IASPNAME)
   ```
   where `IASPNAME` is the name of the IASP where the file is located.
2. Press **Enter**.
3. 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)**
4. Press **F6** to access the **Add Files to be Journaled** window.
5. Specify the name of the file you want to monitor, and then press **Tab**.
6. Specify the name of the library where the file is located, and then 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 `FTP system_ip`, and then press **Enter**.
2. Enter your iSeries user name and press **Enter**.
3. Enter your iSeries password, and then press **Enter**.
4. Type binary, and then press **Enter**.
5. Type `quote site namefmt 1`, and then press **Enter**.
6. Type the following command:
   ```
   get /MYASP/QSYS.LIB/MYLIB.LIB/MYFILE.FILE/MYFILE.MBR C:\MYFILE.MBR
   ```
7. Press **Enter**.

8. Type `quit`, and then press **Enter**.
9. 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)**
10. Type `10` (Object) in the **Op** field to the left of the FTP SEND entry, and then 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`
where

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. To specify the IASP for the current job, type the following command, and then press **Enter**:
   ```
   SETASPGRP ASPGRP(IASPNAME)
   ```
   where IASPNAME is the name of the IASP where the file is located.
2. To set the authority of the file, type the following command, and then press **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. To specify MYASP IASP for the current job, type the following command, and then press **Enter**:
   ```
   SETASPGRP ASPGRP(MYASP)
   ```

2. To edit MYLIB/MYFILE with SFE, type the following command, and then press **Enter**:
   ```
   DBA FILE(MYLIB/MYFILE)
   ```
3. To specify MYOTHASP IASP for the current job, type the following command, and then press **Enter**:
   ```
   SETASPGRP ASPGRP(MYOTHASP)
   ```
4. To edit MYLIB/MYFILE with SFE, type the following command, and then 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.