




Highlights and fixes - service pack 8.4.00.00

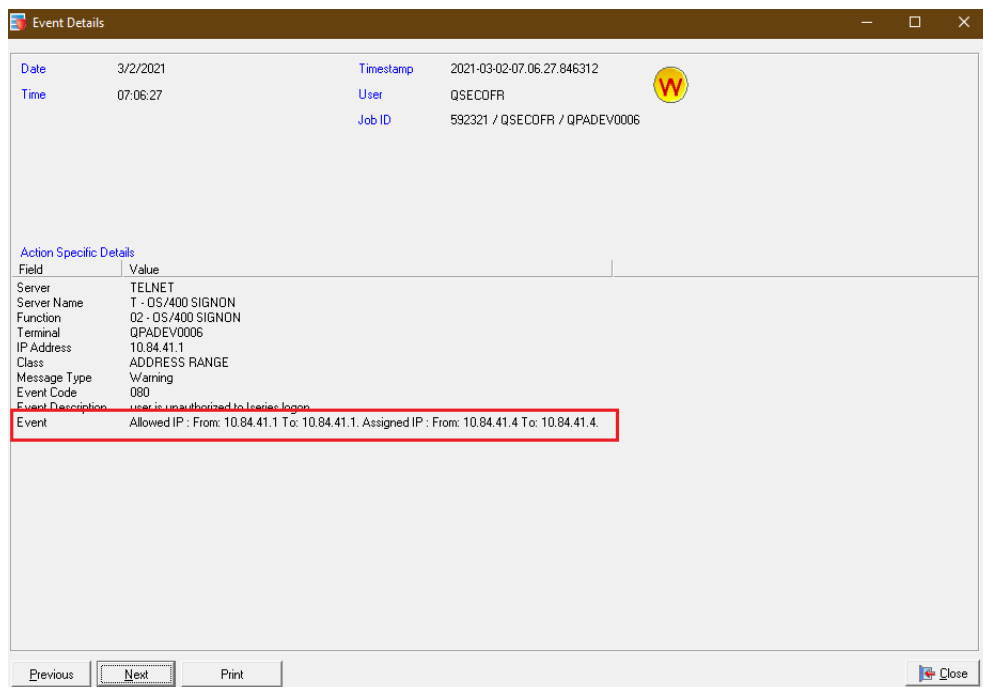
These icons indicate:

-  A change that may require action. For example, you may need to modify automation programs or exit programs or perform other actions before or after installing the product.
-  A change in behavior or a change to the user interface. You should be aware of the change, but no action may be required.
-  New function or an enhancement in the indicated software.

Features included in version 8.4.00.00

Application Access Control

SEC-8033 For Telnet, when the account type selected is IP Address Range, the Allowed IP and the Assigned IP are displayed in the Event Details.



You can generate the Application Audit Report type in Report Generator to display this information:

Serial Number:	S782DD5X
Selection Criteria:	
Report Number:	1103
Report Type:	Application Audit
Account type:	Select All
Partitions:	All Partitions
Run Type:	Current Day
From Date:	01/18/2021
From Time:	00:00:00
To Date:	01/18/2021
To Time:	07:08:58
Output Condition:	Not Specified
System:	Local System

System	Date	Time	User	IP Address	Terminal ID	Application	Function Name	Event Type	Description	Details 1
SYSI06	1/18/2021	00:20:35	JANEL	10.84.49.12	QPADEV000T	T-TELNET	02-OS400_SIGNON	S-SUCCESS	Authorized access to Os/400 Signon	
SYSI06	1/18/2021	00:20:35	QSECOFR	10.84.41.3	QPADEV000D	T-TELNET	02-OS400_SIGNON	S-SUCCESS	Authorized access to Os/400 Signon	Allowed IP : From: 10.84.41.3 To: 10.84.41.3
SYSI06	1/18/2021	00:20:54	ABY	10.84.41.3	QPADEV000G	T-TELNET	02-OS400_SIGNON	W-WARNING	user is unauthorized to Iseries logon	Allowed IP : From: 10.84.41.3 To: 10.84.41.3 Assigned IP : From: 10.84.41.11 To: 10.84.41.11
SYSI06	1/18/2021	00:28:45	ABY	10.84.41.3	QPADEV000G	T-TELNET	02-OS400_SIGNON	W-WARNING	user is unauthorized to Iseries logon	Allowed IP : From: 10.84.41.3 To: 10.84.41.3
SYSI06	1/18/2021	00:51:08	ABY	10.84.41.3	QPADEV000G	T-TELNET	02-OS400_SIGNON	W-WARNING	user is unauthorized to Iseries logon	Allowed IP : From: 10.84.41.3 To: 10.84.41.3 Assigned IP : From: 10.84.41.11 To: 10.84.41.11
SYSI06	1/18/2021	02:29:23	ENFORCE	10.84.41.3	QPADEV000D	T-TELNET	02-OS400_SIGNON	W-WARNING	user is unauthorized to Iseries logon	Allowed IP : From: 10.84.41.3 To: 10.84.41.3
SYSI06	1/18/2021	02:29:52	ABY	10.84.41.3	QPADEV000G	T-TELNET	02-OS400_SIGNON	W-WARNING	user is unauthorized to Iseries logon	Allowed IP : From: 10.84.41.3 To: 10.84.41.3 Assigned IP : From: 10.84.41.11 To: 10.84.41.11
SYSI06	1/18/2021	02:43:58	ABY	10.84.41.3	QPADEV000G	T-TELNET	02-OS400_SIGNON	W-WARNING	user is unauthorized to Iseries logon	Allowed IP : From: 10.84.41.3 To: 10.84.41.3
SYSI06	1/18/2021	03:10:08	ABY	10.84.41.3	QPADEV000G	T-TELNET	02-OS400_SIGNON	W-WARNING	user is unauthorized to Iseries logon	Allowed IP : From: 10.84.41.3 To: 10.84.41.3 Assigned IP not found.
SYSI06	1/18/2021	03:13:30	ABON	10.84.41.3	QPADEV000G	T-TELNET	02-OS400_SIGNON	S-SUCCESS	Authorized access to Os/400 Signon	Allowed IP : From: 10.84.41.3 To: 10.84.41.3 Assigned IP : From: 10.84.41.3 To: 10.84.41.3
SYSI06	1/18/2021	03:15:43	ABY	10.84.41.3	QPADEV000G	T-TELNET	02-OS400_SIGNON	S-SUCCESS	Authorized access to Os/400 Signon	Allowed IP : From: 10.84.41.3 To: 10.84.41.3

SEC-8617 In the File Protection System Policy screen, the maximum number of definitions is now 180, instead of 60.



Central Audit

SEC-8850 When a Central Audit Partition is deleted, a record of this is now written to the current Central Audit Partition.



Compliance

SEC-8526 In Compliance Administration, when adding or editing a System Value template, a GUI change input validation was added.



Control Panel

SEC-8588 The **Check the order of the values of system value QSSLCSL** setting was added to the Control Panel under Compliance.



The cipher suite values for system value QSSLCSL can be accessed in the System Value category template in Compliance Administration.

If you select **Yes** for this setting, you are able to change the order of the cipher values. When a Check Deviations job is run, a mismatch in the order of the values is treated as a deviation.

If you select **No**, the order of the cipher values is fixed. The Check Deviations job does not treat a mismatch in the order of the values as a deviation.

Encryption

SEC-8605



When encrypting IFS files, you can now prioritize jobs by setting the number of simultaneous encryption jobs.

Green Screen

SEC-8562



A new command was created to enter license keys for the following modules:

- Packet Filtering
- Compliance
- Field Masking
- Data Providers
- Encryption
- Firewall

GUI

SEC-9200

Silent installation of the Enforcive Enterprise Security GUI is now available. For details, refer to [“Silent Installation Instructions”](#) on page 40.

Report Generator

SEC-8348



The Health Monitor Report type was added to monitor the Enforcive Enterprise Security modules.

The report displays the following information checked by the Health Monitor:

- Compares the activation policy and activation status in Application Access Control
- Verifies that no exit program is missing in the registry and that the User Profile exit programs exist
- Verifies that jobs such as BSFLOGC, EXJOBDBC and EXJOBDBC1 are active
- Checks the SAUSRP file to verify that the User list is synchronized with System user profile list
- Verifies that alerts are configured to send email and email properties are defined in the Alert center

- Verifies that Report Generator is configured to send email and email properties are defined
- Checks if there are scheduler job entries for each defined policy in Compliance
- Checks if scheduler jobs exist for Inactive users in Extended Security
- Checks if the session timeout job exists in Extended Security
- Checks if all exit programs are in place and exist in the registry for Firewall Manager
- Checks if the scheduler job entry exists in Message Queue Audit
- Verifies that the Encryption module is configured as defined

The following is a sample report:

System	Module Name	Sub-Module name	Event Type	Message Text
SYSI69	Alert Center	Alert Center	Success	One of the alerts defined to send EMAIL and email properties is defined in the Control Panel
SYSI69	Application Access Control	Activation Policy	Success	FTP Server - activation status is the same as the policy
SYSI69	Application Access Control	Activation Policy	Success	FTP Client - activation status is the same as the policy
SYSI69	Application Access Control	Activation Policy	Success	TELNET - activation status is the same as the policy
SYSI69	Application Access Control	Activation Policy	Success	REXEC, RMTCMD - activation status is the same as the policy
SYSI69	Application Access Control	Activation Policy	Success	RMTSQL - activation status is the same as the policy
SYSI69	Application Access Control	Activation Policy	Success	DDM & DRDA - activation status is the same as the policy
SYSI69	Application Access Control	Activation Policy	Success	DATABASE - activation status is the same as the policy
SYSI69	Application Access Control	Activation Policy	Error	DATAQ - activation status is different than the policy
SYSI69	Application Access Control	Activation Policy	Success	Pass-Through - activation status is the same as the policy
SYSI69	Application Access Control	Activation Policy	Success	File Transfer - activation status is the same as the policy
SYSI69	Application Access Control	Activation Policy	Success	SIGNON Server - activation status is the same as the policy
SYSI69	Application Access Control	Activation Policy	Success	File Server - activation status is the same as

SEC-8991 In the IFS Authority Report type, the following new fields were added:



- CCSID of Object
- Size of Object
- Attribute change date/time
- Access date/time
- Modification date/time

System Audit

SEC-7969 The Important Information link was added to the System Audit screen to display the Action Types included in more than one Action Group.



For V7R3M0 and higher, the following Action Groups are supported by System Audit:

- NETBAS
- NETCLU

- NETCMN
- NETFAIL
- NETSCK
- NETSECURE
- NETTELSVR
- NETUDP

Fixes included in version 8.4.00.00

This list includes all relevant changes and fixes since version 8.3.09:

Alert Center

- SEC-8595 The History log alert is now fixed and takes the last QHST file into account.
- SEC-9117 For the SQL Audit alert, the alert is now correctly triggered by the number of events set in the alert definition.

Application Access Control

- SEC-8321 For the Database exit program, the permissions for an unqualified object name are now fixed.
- SEC-8542 In the Database exit program, the port number was added in the Event details for the entire SQL session.
- SEC-8764 For FTP server, the Deny All Objects status is now working properly.
- SEC-8879 For File Server, the number of adopted authority events in QAUDJRN caused by the File Server exit program was reduced.
- SEC-8948 In a swap session initiated by a SWAPON command, when the maximum time is reached and no SWPOFF command is executed, ENDJOB is now executed by the ENFORCE user to end the swap session.
- SEC-9112 For RMTCMD Program Call, when QSYS is selected in the Library list, the Object List correctly displays all the objects.
- SEC-9152 For Data Queue, Optimize now returns the correct value (Success/Warning/Reject).
- SEC-9224 When calling the API ADDMEM\$C API from the command line, an error message is now displayed if an error occurs.
- SEC-9350 For RMTCMD, when executing the commands CHGUSRPRF and CRTUSERPRF, the password is displayed as ********* in the Application Audit Event Details.

Central Audit

- SEC-8614 The QHST Log Audit Extract All job now completes successfully.

Compliance

- SEC-8411 In the System Value category, Check Deviations functions correctly.
- SEC-8979 Check Deviations now correctly handles Join Logicals and SQL Views.
- SEC-8996 In Compliance Assessment, the View Graph option works correctly when there are more than 9 templates in the Assessment Template List. The List index out of bounds error no longer occurs.

Data Providers

- SEC-8413 In the System Audit Data Provider, when running the controlled execution of data extraction jobs, the events are selected correctly according to the user IDs selected or omitted as defined on the Collection Policy tab.
- SEC-8452 In the System Audit Data Provider, the timestamp is now accurate to the millisecond.

Encryption

- SEC-8351 In the RCAC Encryption module, masking and unmasking of all registered fields in a file now works properly when using RCAC field masking.

Extended Security

- SEC-8442 In the Session timeout module, the IBM API CEERANO error message RNQ0202 is now fixed.

Firewall Manager

- SEC-8693 For incoming events, the error message MCH4405 is now fixed.

Green Screen

- SEC-8560 In the Green Screen menu, in the System Policy screen under Access Control, the updating optimize function now works correctly.

GUI

- SEC-9187 The **Object Attribute** column has been added in the Object Group Manager dialog.

LPAR Replication

- SEC-9387 Program RMTSMP/ENFREPL2CA is now working correctly.

Report Generator

- SEC-8329 The Application Audit Report type with System Group now retrieves information properly.
- SEC-8489 The QHST Log Report type now works correctly.
- SEC-8523 The File Audit Report type is now fixed when the first file in the file group in the Selection Criteria does not exist or is not journaled.
- SEC-8679 The Server Authentication Entries Report type now correctly displays the System Name instead of the Serial number.
- SEC-8740 In the System Audit (detailed) Report type, the SK action type is now fixed and the port number is correct.
- SEC-8827 In the SWAP not used in X days Report type, the **Check creation SWAP definition** parameter was added to the selection criteria.
- SEC-8988 The File Shares Report type for V7R3M0 and higher now works with the file QSYS2.Server_SHARE_INFO, and the error CPF9870 no longer occurs.
- SEC-9120 The View Data Report type now works correctly. A sample report is provided.
- SEC-9307 When the IFS Text output format is selected, and the Email check box is checked, the IFS text output file is sent by email.
- SEC-9382 In the SQL Statement Report type, when the CSV output format is selected, the entire SQL statement is displayed properly.
- SEC-9444 An error no longer occurs when creating a Report Group.

SQL Statement Audit

- SEC-9117_2 The following issues were fixed in SQL Statement Audit:
 - Executing End SQL Policy now ends the specific monitor ID
 - When adding a user to a user group defined in SQL Policy, it is no longer necessary to reactivate the policy
 - Unnecessary codes are deleted via the STRDBMON job to reduce the size of the SQAUDOUTF file
 - Fixed a bug in the extraction job which caused SQL not to work consistently on several servers
 - Added the Command row in the Event Details dialog to display the command issued on Start SQL Policy and End SQL Policy events
 - Important information about the user groups and file groups is provided in the GUI

System Audit

- SEC-8571 In the System Audit Reports, a page break was added to the spool output of the Swap Report.