

System Requirements and Impact on Resources

Note:

Impact on Resources has now been integrated into this document and dropped as a separate document.

This document lays out some important considerations you should be aware of before installation and when running Enterprise Security.

It is important to be familiar with the issues discussed below and to review them from time to time to ensure you maintain the smooth running of the product.

Contents

IBM i Platform

- Integration with Other Software
- OS/400 PTF Level
- Minimum Server Requirements
- Disk Space Required on the IBM i Server
- PC Client Requirements
- DDM Setup
- User Profiles
- Libraries
- Save File Objects
- Ports
- Performance Considerations
- Alerts
- System Audit Reports
- Application Audit File Logging and Optimize
- The Clear Log Function - Now Redundant
- Performance Benchmarks
- OS/400 System Values
- Subsystems
- Table of Jobs
- Autostart Jobs in Subsystems
- Job Queues
- Job descriptions
- Output Queues
- Operator Console Messages
- Impact on Common User Practice
- SAVSYS Backups

PC Platform

System z Platform

General Considerations

- Audit Log Files

IBM i Platform

Integration with Other Software

From v8.3, Enterprise Security includes support of the IBM Power HA high availability software, when deleting user profiles in the Enterprise Security Manager.

OS/400 PTF Level

The IBM PTF 5770DG1, which is loaded with the Group PTF, causes validation list issues when logging in to the Enforcive GUI.

The following are the PTF details:
For OS V7R4: 5770DG1 SJ04311
For OS V7R5: 5770DG1 SJ04732
For OS V7R6: 5770DG1 SJ04731

Install the following PTFs to correct the prior defective PTFs:

PTF for OS 7.6 - SJ05802, // <https://www.ibm.com/mysupport/s/fix-information?legacy=SJ05802>

PTF for OS 7.5 - SJ057799, // <https://www.ibm.com/mysupport/s/fix-information?legacy=SJ05799>

PTF for OS 7.4 SJ05800, // <https://www.ibm.com/mysupport/s/fix-information?legacy=SJ05800>

Minimum Server Requirements

1. IBM i computer running Release 7.4, or higher.
2. TCP/IP communication.
3. Active HTTP server (OS/400 or Apache)
4. Java 8 is required for sending reports by email in the Report Generator from version 8.4.02.00 and higher and in the Alert Center from version 8.4.06.00 and higher. Customers who use Enforcive Enterprise Security need to ensure that Java 8 is available on the systems where the product is installed. We recommend you do the following from the IBM i systems before installing this service pack:
 - a) Use the command DSPSFWRSC to check the installed version of Java.
 - b) If necessary, use your IBM i software media to install the appropriate version of licensed programs 5761-JV1 or 5770-JV1 and its option for Java 8.
5. A user with SECOFR authority.

Disk Space Required on the IBM i Server

The approximate disk space required on the server for the Enterprise Security program libraries is as follows:

RMTOBJ	About 270MB
RMTSMP	About 780MB
RMTFIL	About 140MB
RMTOUT	Empty
RMTLOG	Empty

The size of RMTOBJ and RMTSMP will not change during use of the product as they contain software components only.

RMTFIL will grow due to the addition of security definitions but this will remain reasonably stable once the initial setting up has been done.

RMTOUT is a temporary library that contains data extracted by the data providers en route to external servers. The files placed there should be deleted by the remote collection service initiated from the external processes. However, if these external processes are not run, the files will not be cleared and the library will expand in size.

RMTLOG is the Enterprise Security logging library and so this will grow the most due to the various audit processes that route events to the Central Audit.

The degree of logging done (and hence the rate of disk usage) can be controlled in several different ways. Each of the above applications can be set to log all access or rejections alone. Additionally, the optimize option lets you skip logging similar events. This flexibility allows you to find the balance between maximum auditing on the one hand and minimum overhead on the other. See [Application Access Control](#) for more information.

I/O-intensive activity such as batch jobs can make a significant impact on the number of events logged and so the mechanisms described above for reducing the level of logging are particularly beneficial.

Another reason for disk expansion which needs to be considered is the collection of events in the system journal and file journals.

Note: Files starting with R0 are the Report Generator viewer files by default, which can enlarge the size of the RMTFIL library. You can delete these files manually via the GUI.

The following save files can also be deleted to free up more space:

- ENFCA17 *FILE QGPL SAVF
- EXRMTCMD *FILE QGPL SAVF
- E548304 *FILE QGPL SAVF
- E548307 *FILE QGPL SAVF
- E548310 *FILE QGPL SAVF
- E548311 *FILE QGPL SAVF
- E548312 *FILE QGPL SAVF
- E548313 *FILE QGPL SAVF
- E841 *FILE QGPL SAVF
- E8410_1 *FILE QGPL SAVF
- E842 *FILE QGPL SAVF

- E843 *FILE QGPL SAVF
- E844 *FILE QGPL SAVF
- E845 *FILE QGPL SAVF

PC Client Requirements

- Disk Space: 200 MB
- Memory: 50 – 100 MB
- Windows Operating System – Windows 10 or higher.
- Read, Write and Delete permissions on the GUI installation folder.
- TCP/IP communication to the IBM i.
- Additional requirement for Enterprise Security Alert monitors and Data Key Remote Service: permission to Register/Unregister and Start/Stop the Windows service.

DDM Setup

Certain operations in Enterprise Security involve communication between two IBM i computers via DDM. These operations include remote compliance checking and replication of user profiles, passwords and definitions.

User Profiles

A number of user profiles are created in the installation process. These are summarized below.

The passwords for all the profiles below should be changed to strong passwords following installation as they possess special authorities. Some may be disabled as specified below.

These user profiles must not be deleted as long as Enterprise Security is installed on the system. They may be deleted only after a complete uninstall. They are not removed automatically in the uninstall process.

Profile	Purpose	Authority	Usage
BSAFE (pwd=*NONE)	Owner of all objects in system and default user for batch jobs	User class *SECOFR (select *USRCLS)	Must be enabled. Do not delete. BSAFE is a Group profile and users ENFORCE and ENFREP are members of the Group profile.
ENFORCE (pwd=*NONE)	Default user	User class *SECADM and special authorities of *AUDIT and *SECADM	Can be disabled if another user is created and given full access to the Enterprise Security Manager. Do not delete.
PSSAGENT	Required for CPS PSS		Can be disabled if CPS PSS is not used with IBM i computers.
PSSADMIN	Required for PSS for IBM i		Can be disabled if PSS for IBM i is not used.
PSS	Required for PSS for IBM i		Can be disabled if PSS for IBM i is not used.
ENFREP (Fixed password that cannot be changed)	Replication user	User class *SECADM	Can be disabled or the password set to *NONE if LPAR replication is not used.
PSSOWNER (pwd=*NONE)	Required for PSS for IBM i	User class *SECADM, with *ALLOBJ *SECADM *JOBCTL special authorities)	

Libraries

The following libraries are created at installation and/or upgrade time.

Library	Usage	Notes
RMTFIL	Enforcive data library	Core product
RMTSMP	Enforcive software programs	Core product
RMTOBJ	Enforcive software programs	Core product
RMTLOG	Enforcive log files	Core product
RMTOUT	Data Provider files	If Data Provider is active, the library is created. If Data Provider not used, this library can be deleted.
RMPSS	PSS addon product objects	If PSS not used, this library can be deleted.

Save File Objects

Save files (*SAVF) may exist in one or more of the core product libraries. These should not be removed. Temporary save files created in QGPL for new installations, upgrades and PTFs can be deleted after the installation has completed successfully.

Ports

Enterprise Security uses a number of different ports in the IBM i and these must be unused by other software instances and unblocked to enable the required functionality. The table below lists all ports and their purposes. If you do not require the specified functionality, then the corresponding port can be blocked or used by other applications.

Port	Purpose
21,20	LPAR Replication - FTP
25	Control Panel - Outgoing Mail Server (SMTP)
25	Alert Monitor - Mail Server Port
447	Compliance - Multi-System - DDM
447	Report Generator - Multi-System - DDM
514	Alert Center for Syslog
514	iSeries Data Provider for Syslog
1967	Enforcive GUI Client
1968	PSS Password Self Service
3060	Alert Monitor
3061	Encryption - Data Key Remote Server
4444	Enforcive GUI Client with SSL

If any of the ports listed above are required for use by other applications, please contact support.

Performance Considerations

Where activity is high and it is not necessary to log successful access attempts, set log recording to log authority violations only without logging authorized access. This can be done at the system policy or account level to ensure optimal balance between event history and performance. This is discussed further below and in the user guide.

Alerts

Alerts are a powerful means of raising the alarm following selected kinds of event. However if a large number of alerts are defined and active and their scope is not limited by object, library, function etc, this could cause a large number of alerts to be sent in a short time. This would somewhat defeat the purpose of an urgent warning for high risk events and could also create an overhead on the server, affecting performance. In version 4.1.5 and later, this may be controlled through the control panel module.

System Audit Reports

Simultaneous running of a large number of system audit or file audit reports could result in large areas of disk space being used up during the runs. No more than 3 system audit or file audit reports should be run at the same time. In version 4.1.5 and later, the temporary file size may be limited through the control panel module.

Application Audit File Logging and Optimize

There are a number of ways in which the degree of logging can be controlled. One way is to write only violations to the log. During initial product implementation we recommend writing all events. After a period of time during which authorizations are fine-tuned and product operation stabilizes, you could reduce logging by changing the default to "Violations only". Log recording can also be set per account. See **System Policy** in the product user guide.

When the System i handles a large degree of network traffic, a drop in system performance could be experienced due to intensive event logging and permissions checking. The product provides a means to minimize this performance degradation – the **optimize** option, covered in the user guide.

By default, the product is installed with optimize active for the DDM, database, data-queue and file servers. This significantly improves performance at the expense of reduced logging and the inability to take advantage of permissions checks at the function, library and object levels.

Optimizing achieves this performance improvement by skipping the permissions checks at the function, library and object levels, checking at the server level only. Additionally, it substantially reduces the amount of logging done in the Application Audit log.

More details of the optimizer and how to activate and deactivate it for different servers is covered in **System Policy** and the **Optimize** option in the product user guide.

The Clear Log Function - Now Redundant

From version 7.2, application audit events are logged in the Central Audit log file. As a result, the previous file (SRMTLGP) is discontinued. Previously, ongoing expansion of the file mandated that its size be monitored regularly. Periodically it was necessary to make use of the **Clear Log File** and **Clear Backup File** functions to reduce the size of the file. These functions no longer appear from v7.2. The Central Audit file, containing the Application Audit, is now maintained by the rollover mechanism.

Performance Benchmarks

Network access through the database server (ODBC) on OS/400 V5R3

Average access times per transaction

Full protection and logging:	0.07 sec/transaction
Protection with logging of violations only:	0.036 sec/transaction

OS/400 System Values

Upon activation of any of the Enterprise Security exit programs, the network attribute Client Request Access is changed to *REGFAC and is returned to its former value only when the last exit program has been deactivated.

When the PASS THROUGH exit program is activated, system value QRMTSIGN is changed to Remote Session = Program EXPAST, Library RMTOBJ. To retain the original value of QRMTSIGN, run the following command from the command line:

```
RMTOBJ/BSFQRMTSYS(original_value)
```

And then press F4. For example, If the original value is *FRCSIGNON , run the following command:

```
RMTOBJ/BSFQRMTSYS RMTSIGN(*FRCSIGNON)
```

When the DDM exit program is activated, the network attribute DDM Request Access is changed to EXDDM, Library RMTOBJ. It is returned to its former value when DDM is deactivated.

Subsystems

The product will run jobs in the following subsystems

```
QHTTPSVR  
QSYSWRK  
QUSRWRK
```

Table of Jobs

See [Table of Jobs](#).

Autostart Jobs in Subsystems

Certain autostart jobs may be added at installation time or when running some functions. They will appear in QUSRWRK or QSYSWRK.

In Subsystem QUSRWRK

Job Name	Job Description	Description
BSFFMTRG	RMTSMP/ BSFFMTRGJD	Read operations; write from data queue to central audit. Might alternatively be in QSYSWRK

In subsystem QSYSWRK

The following autostart jobs may be added at installation time or when running some functions.

Job Name	Job Description	Description
BDPDRV	RMTSMP/BDPDRV	Data provider start up program
BSFMCOLC	FMTFIL/BSFMCOLJD	Message queue alert collector
BSFRMON	RMTSMP/BSFRMONJD	Roll over maintenance program
BSFSQLCOM	RMTFIL/BSFSQLJD	SQL statement audit alert collector
BSFFCOL	RMTSMP/BSFFCOLJD	File audit alert collector
BSFICOL	RMTSMP/BSFISTRCOL	Application IDS collector
BSFSCOL	RMTFIL/BSFSCOLJD	System Audit IDS collector
BSFLOGC	RMTOBJ/BSFLOGJD	Recording log events for file server
BSFHCOL	RMTFIL/BSFHCOLJD	Health collector job
ENCAUDAJE	RMTSMP/ENCENCGEN	Encryption auditing job
EXACTJRDB	RMTSMP/EXACTJRJD	Writes database and file server events to central audit
EXJOBDC	RMTFIL/BSFJOBDC	OS/400 signon
EXJOBDC1	RMTFIL/BSFJOBDOF	OS/400 signoff

Job Queues

The following job queues may be created

RMTSMP/BSFICOLJQ
RMTSMP/BSFIRCVJQ
RMTSMP/BSFISNDJQ
RMTSMP/BSFMONJQ – Data Provider
RMTSMP/BSFMSNDJQ
RMTSMP/BSFSQLSNDQ
RMTSMP/BSFWSNDJQ
RMTOBJ/BSFLOGJQ
RMTFIL/BSFJOBQON (for signon control)

Job descriptions

In library RMTFIL:

ADJOB	Reports
BSFJOBDOF	Exit program use
BSFJOBDON	Exit program use
BSFSCOLJD	System audit IDS collector
DFJOB	Native user signon
NETJOB	Exit program

In library RMTSMP:

SFBCKSBSC	Restart Field Encryption jobs
BSFCNJ	Field Encryption job description
BSFFMTRGJD	Start Retrieve Data Audit
BSFISTRCOL	Application IDS alert collector
BSFSCOLJD	System audit IDS collector
BSYSALJOB	Alternative alert collector JOB
BSFREPGEN	Report generator
BDPDRV	Data Provider

Output Queues

BSPRINT in both RMTSMP and RMTFIL. Purpose - alerts

Operator Console Messages

We recommend sending only "Violations" to the operator message queue. See **System Policy** in the product user guide.

If the operator is notified of all events, then the console may become overloaded with messages from **Enterprise Security** thus having a counter-productive effect, as most events will be informative and will not require any action by the operator. If, on the other hand, the operator is notified only of unauthorized access, then he will be aware that immediate action may be required for every event posted to the console by **Enterprise Security**.

Impact on Common User Practice

During initial product implementation we recommend responding to unauthorized access requests with a "Warning" rather than with a "Reject". See **System Policy** in the product user guide.

In this way the influence of **Enterprise Security** on the organization can be evaluated without necessitating any changes in common user practice. After a period of time during which authorizations are fine-tuned and product operation stabilizes, we recommend a gradual changing of responses to "Reject". This will allow users to become gradually accustomed to the security policy you have defined, as implemented using **Enterprise Security**.

SAVSYS Backups

Versions of the product from 5.5.2 up to 7.0 required the use of the command RMTOBJ/BSFINAC before executing SAVSYS backups. From version 7.1 this is no longer required.

Users of Enterprise Security version 5.5.2 must download and install Enterprise Security PTF AP55236. If you downloaded the earlier PTF AP55232 you should replace it with AP55236. If there is a cumulative PTF released after June 2008, this may be downloaded and installed instead.

Users of Enterprise Security version 5.6 must download and install Enterprise Security PTF CUM56003 and MOD56005.

All Enterprise Security PTFs can be downloaded from Precisely Data Experience (<https://data.precisely.com/home>).

PC Platform

CPA data logging and transfer rates (batch)

Transfer via a local network to a PC running Windows server 2003 / MS SQL Server 2005 should execute at a rate of 170/Sec (170 records per second) or better, depending on the speed of your network.

Disk Space required for the Enterprise Security Manager (GUI Client)
About 50Mb

Disk Space required for the CPA
1Gb to 1.5Gb of disk space for each million events in the PC database.

System z Platform

The transfer rate of data from remote servers to the Cross-Platform Audit depends on the network bandwidth and on the performance of the participating servers. The following is a representative example:

100,000 SMF records on a Linux-based emulator running at ~15 MIPS on IBM T42 Laptop would be processed by mainframe started task in 2 minutes. In a real mainframe environment it should take even less. In benchmark tests in a typical small office network 100,000 records were imported into the CPA database (SQL Server on the network) in approximately 10 minutes.

The actual speed depends mostly on network bandwidth abilities and on the PC Server hardware. This is an offline task.

General Considerations

Audit Log Files

As with all monitoring applications, the more logging you do, the more information you have available. However, the smaller the log file and the less logged, the better the performance. There are a number of ways in which the size of the various log files can be controlled. These include the scope of events logged, the frequency of clearing the log and the general housekeeping of the database files such as reorganizing them to free up space taken by deleted records.