



Database Activity Monitoring User Guide

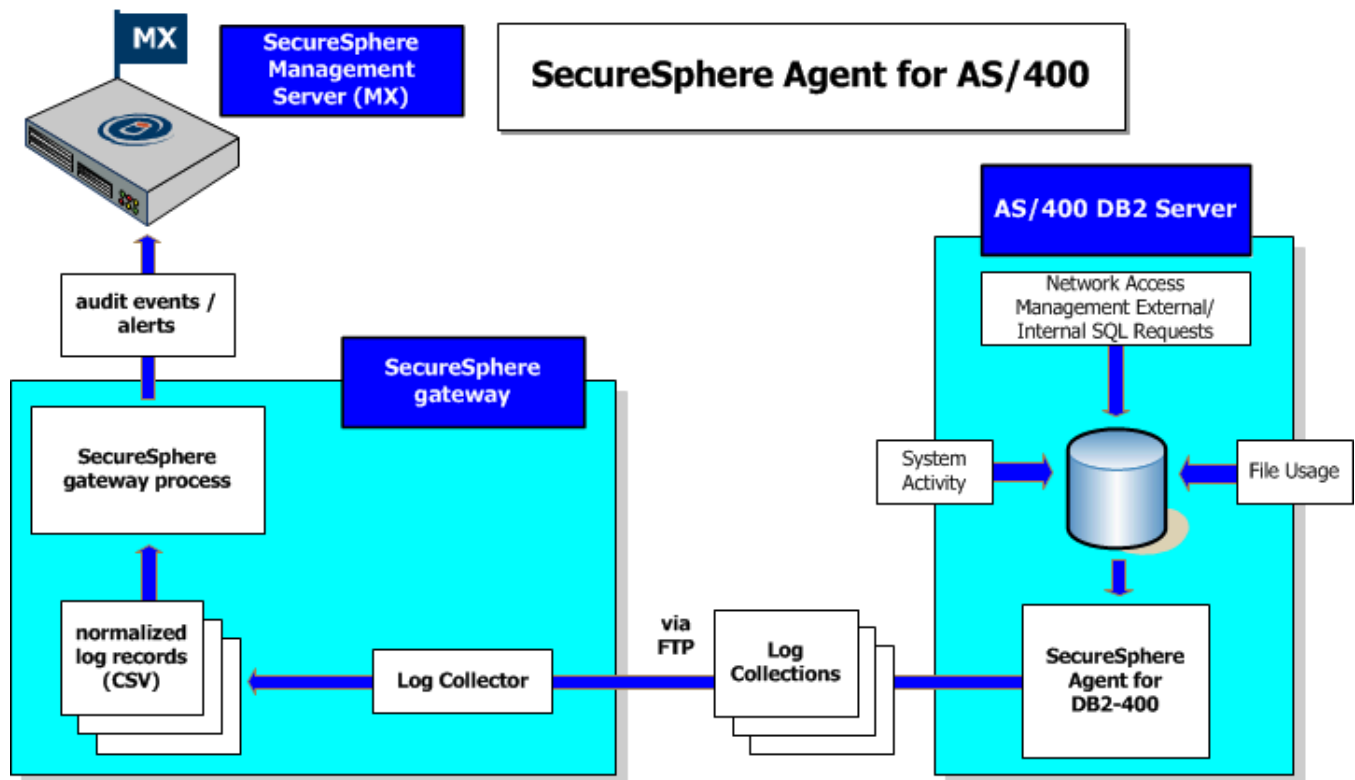
Contents

Working with DB2 on AS/400	3
SecureSphere Agent for AS/400 Configuration Tasks	3
Release Content v2.16	4
System Requirements for Installing AS/400 Agent	5
SecureSphere Agent for AS/400 Installation and Configuration	5
SecureSphere Agent for AS/400 First Time Login	13
Requesting a License for SecureSphere Agent for AS/400	15
Installing a new License for SecureSphere Agent for AS/400	15
Upgrading the SecureSphere DB2 AS400 Native Side	16
Configuring a DB2 for an AS/400 Log Collector Instance	22
Configuring the Firewall for FTPS Support for AS/400	23
Setting DB Statistics (SQL Response Size)	24
SecureSphere Agent for AS/400 Failed Login Support	27
Maintenance Options	28
Uninstalling SecureSphere Agent for AS/400	29

Working with DB2 on AS/400

SecureSphere monitors DB2 AS/400 database activity, network and system log using Log Collector by acquiring the log records and generating reports and alerts based on those log records.

The log records are extracted from the DB2 Server by SecureSphere agent for AS/400 and written to a location from which SecureSphere retrieves them, converts them to CSV format and pushes the CSV data to the SecureSphere gateway.



The SecureSphere gateway processes the DB2 log records in the same way it processes database activity which it monitors directly, with this exception: because SecureSphere sees only the logs for the database events rather than the events themselves, the following SecureSphere functionality is not available:

- Matching the traffic to the service is based on the log collector instance and not on the IP address and port number in the logs
- Network policies: firewall, network protocol validation, stream signatures
- DB protocol validation policies
- Server group level policies
- Network settings (for example, connection timeout)
- Event blocking
- Audit Responses

SecureSphere Agent for AS/400 Configuration Tasks

The following table presents SecureSphere Agent for AS/400 Configuration Tasks.

AS/400 Task Overview

	Task Overview	For more information, see...
1.	Install and configure the Agent.	SecureSphere Agent for AS/400 Installation and Configuration
2.	In SecureSphere, create and configure the Log Collector instance for the DB2 service.	Configuring a DB2 for an AS/400 Log Collector Instance
3.	Request a license.	Requesting a License for SecureSphere Agent for AS/400
4.	Install a new license.	Installing a new License for SecureSphere Agent for AS/400

Release Content v2.16

The latest agent version is 2.16. The new content added to this version is:

- **DBOPEN New options Preselect which origins and types of IO to control**
 - Customer may select to control ODBC+STRSQL, Skip NativeIO, or restrict the types of IO more selectively.
 - The selection is done extremely fast, and can reduce the number of transactions to analyze.
- **Product Performance improvement**
 - The number of files used was reduced results with less file opens.
 - The file opens of files is differently handled to reduce file opens.
 - Algorithms used to analyze transactions were improved.
- **New functionalities added to the product:**
 - Work with Collected Data shows the amount of disk space used by the different parts of the product
 - Automatic control of the number of Journal Receivers for QAUDJRN based on the number of days that the system should stay online.
- **New options added to the product menus:**
 - Work with FTP Active Jobs
 - Check FTPS (SSL) Availability
- **Improved Logging:**
 - More ways to display the log Skip non-relevant access types for optimized performance.
- **Known issues and enhancements:**

- All known issues were resolved.
- All enhancements since the previous release are included.
- **Business intelligence enablement:**
 - Visualizer - the business intelligence component – supports all the collected information.
 - Visualizer is not included in the Agent license, but the professional support team may decide to use it themselves to answer questions and user requests.
- **Operating system support**
 - Razlee Agent 02.16 supports the IBM iSeries 7.5 operating system.
- **Bug Fixes**

Useful Links:

- **Installation files on Imperva FTP:** https://ftp-us.imperva.com/Downloads/Imperva_Agents/AS400
- **Release Notes:** [DAM Release Notes](#)
- **DAM User Guide:** [Working with DB2 on AS/400](#)

System Requirements for Installing AS/400 Agent

The following are the requirements for installing the AS/400 Agent.

Component	Disk Requirements
File usage (AP- Journal)	70MB
Network access management (Firewall)	140MB
System activity (Audit)	300MB
SecureSphere Agent	2MB

For information about supported versions, see the Database Security Coverage tool at <https://www.imperva.com/data-security-coverage-tool/>.

SecureSphere Agent for AS/400 Installation and Configuration



Note: When working with the FTP service on the AS/400 machine, the service must be in the active mode. Before changing the FTP mode, make sure that any other FTP client software in use is changed to the active mode as well. To change the FTP service mode to active, use the following command:

```
CRTDTAARAA DTAARA (QUSRSYS/QTMFTPPASV) TYPE (*LGL) AUT*USE
```

Before installing the agent for the first time, review [System Requirements for Installing AS/400 Agent](#).

To install the SecureSphere Agent for AS/400 for the first time:

1. Make sure you have downloaded the A2P files and PTF folder from the Downloads section of the [Imperva Customer Portal](#) at the following path: /Downloads/SecureSphere_Agents/AS400.
2. Login to AS/400 server with a powerful user profile, preferably QSECOFR or a user with *ALLOBJ, *AUDIT, *SECADM, *JOBCTL and *SAVSYS authorities, Limit capabilities = *NO.
3. In the command line, enter:

```
CRTLIB LIB(ISECAGENT) TYPE(*TEST) TEXT('SecureSphere Agent: Temporary Library').
```

The following message appears:

```
Library ISECAGENT created
```

4. Create the following save files in library ISECAGENT by typing:
 1. CRTSAVF FILE(ISECAGENT/SMZ8)

The following message appears:

```
File SMZ8 created in library ISECAGENT
```

2. CRTSAVF FILE(ISECAGENT/SMZJ)

The following message appears:

```
File SMZJ created in library ISECAGENT
```

3. CRTSAVF FILE(ISECAGENT/SMZ4)

The following message appears:

```
File SMZ4 created in library ISECAGENT
```

4. CRTSAVF FILE(ISECAGENT/SMZS)

The following message appears:

```
File SMZS created in library ISECAGENT
```

5. To make sure all the new files were created, type
STRPDM

, select **Work with Objects** and filter according to the relevant library (ISECAGENT). If part of the files do not appear, you need to create them again and understand the problem (permissions issue, system is overloaded, etc.).

Work with Objects Using PDM					RAZLEE3
Library		ISECAGENT		Position to	
				Position to type	
Type options, press Enter.					
2=Change		3=Copy		4=Delete	
8=Display description		9=Save		5=Display	
				10=Restore	
				7=Rename	
				11=Move ...	
Opt	Object	Type	Attribute	Text	
█	SMZJ	*FILE	SAVF		
—	SMZS	*FILE	SAVF		
—	SMZ4	*FILE	SAVF		
—	SMZ8	*FILE	SAVF		
Bottom					
Parameters or command					
==>					
F3=Exit		F4=Prompt		F5=Refresh	
F9=Retrieve		F10=Command entry		F6=Create	
				F23=More options	
				F24=More keys	

At this point: The files should be empty: **size = 0**.

- Use FTP in BIN mode to copy the corresponding installation media into the previously created save files:

FTP

(type IP Address or System Name)

user (use the same user name as in point No. 1)

password (type the password)

BIN

PUT GSrelVos.A2P isecagent/smz8

PUT AUrelVos.A2P isecagent/smz4

PUT JRrelVos.A2P isecagent/smzJ

PUT SAreIVos.A2P isecagent/smzS

rel = component release version, os = operating system version

QUIT

```

C:\>ftp 1.1.1.101
Connected to 1.1.1.101.
220-QTCP at 1.1.1.101.
220 Connection will close if idle more than 5 minutes.
User (1.1.1.101:(none)): qsecofr
331 Enter password.
Password:
230 QSECOFR logged on.
ftp> bin
200 Representation type is binary IMAGE.
ftp> put GS150U61.A2P isecagent/snz8
200 PORT subcommand request successful.
150 Sending file to member SMZ8 in file SMZ8 in library ISECAGENT.
226 File transfer completed successfully.
ftp: 32117184 bytes sent in 4.13Seconds 7785.98Kbytes/sec.
ftp> put AU110U61.A2P isecagent/snz4
200 PORT subcommand request successful.
150 Sending file to member SMZ4 in file SMZ4 in library ISECAGENT.
226 File transfer completed successfully.
ftp: 35811072 bytes sent in 4.56Seconds 7849.86Kbytes/sec.
ftp> put JR070U61.A2P isecagent/snzj
200 PORT subcommand request successful.
150 Sending file to member SMZJ in file SMZJ in library ISECAGENT.
226 File transfer completed successfully.
ftp: 19472112 bytes sent in 2.44Seconds 7986.92Kbytes/sec.
ftp> put SA010U61.A2P isecagent/snzS
200 PORT subcommand request successful.
150 Sending file to member SMZS in file SMZS in library ISECAGENT.
226 File transfer completed successfully.
ftp: 1654752 bytes sent in 0.22Seconds 7555.95Kbytes/sec.
ftp> quit
221 QUIT subcommand received.

C:\>

```

7. In the command line, type:

```
ADDLIB LIB (ISECAGENT)
```

. The following message appears:

```
Library ISECAGENT added to library list
```

8. To make sure the library was added to the library list, type

```
DSPLIBL
```

. The ISECAGENT item appears in the list.

9. Restore the installation program from the SecureSphere Agent save file into the installation library:

```
RSTOBJ OBJ (INSTISA) SAVLIB (SMZS) DEV (*SAVF) OBJTYPE (*PGM) SAVF (SMZS) MBROP
T (*ALL) ALWOBJDIF (*ALL) RSTLIB (ISECAGENT)
```

The following message appears:

```
1 objects restored from SMZS to ISECAGENT
```

10. Make sure the new file was added to the ISECAGENT library, as explained in step 3.

Work with Objects Using PDM

RAZLEE3

Library ISECAGENT

Position to

Position to type

Type options, press Enter.

2=Change

3=Copy

4>Delete

5=Display

7=Rename

8=Display description

9=Save

10=Restore

11=Move ...

Opt	Object	Type	Size	Text
█	INSTISA	*PGM	69632	Install ISA Product
—	SMZJ	*FILE	24576	
—	SMZS	*FILE	1867776	
—	SMZ4	*FILE	129753088	
—	SMZ8	*FILE	24576	

Bottom

Parameters or command

===>

F3=Exit

F4=Prompt

F5=Refresh


F6=Create

F9=Retrieve

F10=Command entry

F23=More options


F24=More keys



Note: Make sure that previous SMZ* libraries do not exist:

- STRPDM
- Opt.1
- SMZ*
- If the SMZ* libraries do exist contact IMPERVA or see the upgrade section in this user guide before you running step 10

11. Run the program: **CALL PGM(INSTISA)**



Note: The following examples are for a Firewall, but are relevant for all the components.

12. If there was a problem restoring the media, such as a damaged file, authorization problem or the save file is empty, the following error message appears:

SMZ8-Firewall: Missing installation media. R-Retry, C-Cancel, S-Skip

1. Select one of the following actions:

R-Retry: tries to perform the same operation again

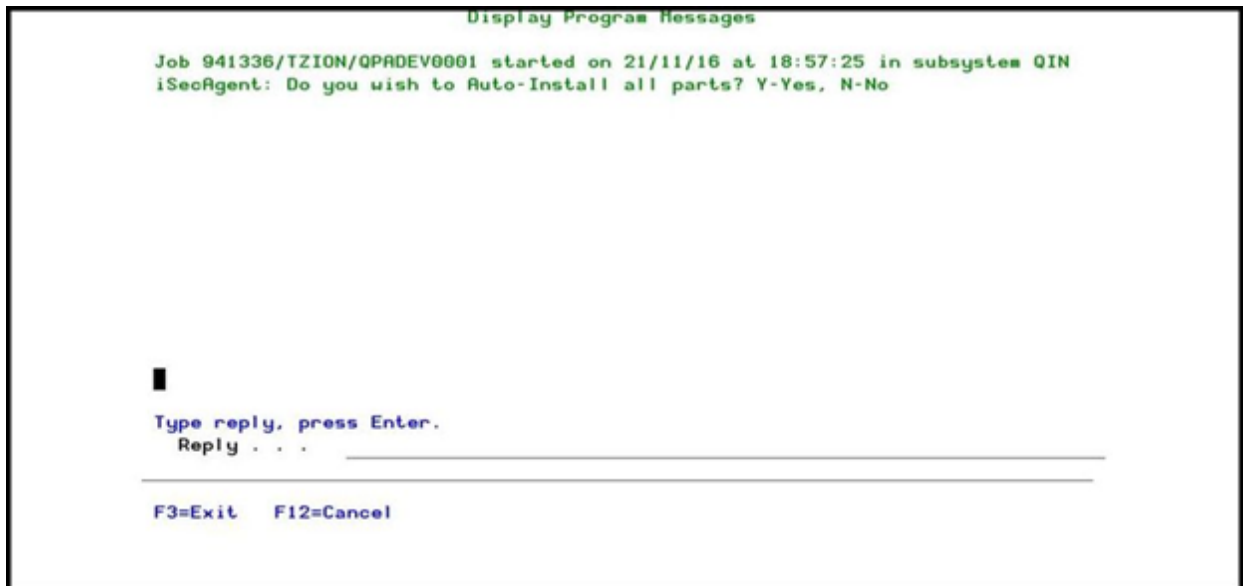
C-Cancel: aborts the installation process and displays the following error message:

'Error occurred while installing an essential part of the SecureSphere Agent. Check detailed messages (DSPJOBLOG + F10 on the screen or print

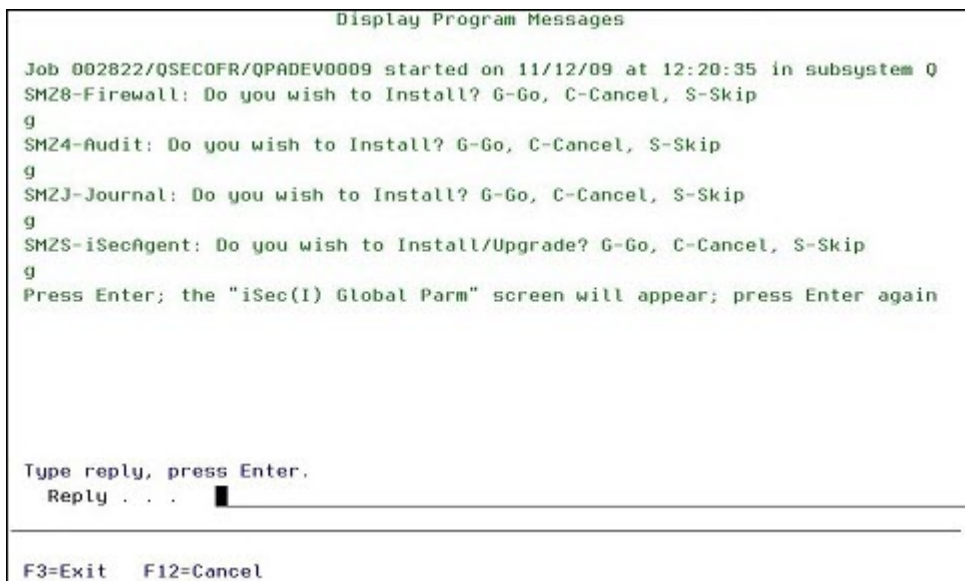
```
via DSPJOBLOG OUTPUT(*PRINT) '
```

S-Skip: bypasses the installation or upgrade of the current product component and continues with the next component or step of the installation procedure

13. During first time installation, the following message appears:
Do you wish to Auto-Install all parts? Y-Yes, N-No



14. Select **Y**.
15. If **N** was selected, module-by-module installation proceeds.



SMZ8-Firewall: Do you wish to Install? G-Go, C-Cancel, S-Skip

1. Select one of the following actions:

G-Go: proceeds with the installation/release upgrade of the component in question

C-Cancel: aborts the installation process and displays the following error message:

```
'Error occurred while installing an essential part of the SecureSphere
Agent. Check detailed messages (DSPJOBLOG + F10 on the screen or print
via DSPJOBLOG OUTPUT(*PRINT) '
```

S-Skip: bypasses the installation or upgrade of the current component and continues with the next component or step of the installation procedure

16. During first time installation, each component's configuration screen appears in sequence. Press **Enter** at the prompt to install that component and move on to the next component.

```
Firewall
```

```
===
```

```
'Press Enter; the "iSec(I) Global Parm screen will appear; press Enter again'
```

```
Audit
```

```
==
```

```
'Press Enter; the "iSecBas System Conf screen will appear; press Enter again'
```

```
Journal
```

```
==
```

```
'Press Enter; the "Configuration" screen will appear, press Enter again.'
```

17. If the installation of all the components ends normally, the following message appears:

```
*** Installation of iSecAgent has ended successfully *** Press Enter ***
```

18. In the command line, type:

```
CLRLIB LIB(ISECAGENT)
```

The following message appears:

```
Library ISECAGENT cleared.
```

To make sure the library was cleared, see step 3.


Specify Objects to Work With

Type choices, press Enter.

Library	<u>I</u> SECAGENT	*CURLIB, name
Object:		
Name	<u>*ALL</u>	*ALL, name, *generic*
Type	<u>*ALL</u>	*ALL, *type
Attribute	<u>*ALL</u>	*ALL, attribute, *generic*, *BLANK

F3=Exit F5=Refresh F12=Cancel


19. Unzip the PTF file under the Network Access Management component folder and execute the file.



Notes:

- PTF installation can only be performed from a Windows based operating system machine.
- Make sure you have an FTP connection between the machine from where you are running the PTF and the AS/400.
- When executing the PTF file, you may type "i" to start the installation immediately or wait a few seconds for the installation to start automatically.
- During installation you are asked to provide the AS400 machine IP, user and password. Imperva recommends using **QSECOFR** for the user.

20. Unzip the PTF files under the System Activity component folder and execute the files in the order they are named.



Notes:

- PTF installation can only be performed from a Windows based operating system machine.
- Make sure you have an FTP connection between the machine from where you are running the PTF and the AS/400.
- When executing the PTF file, you may type "i" to start the installation immediately or wait a few seconds for the installation to start automatically.
- During installation you are asked to provide the AS400 machine IP, user and password. Imperva recommends using **QSECOFR** for the user.

Notes:

- If there are problems during installation, see your local system administrator.
- Should this installation procedure end abnormally, run it again while using S=Skip to skip the parts that were already properly installed. In this case, you will have to finish the installation by running option 81 in each module and pressing **Enter** for each (To ensure default controlling parameters exists).
- First time installations can be done independently. If the system already contains a previous SecureSphere or iSecurity installation perform an upgrade procedure, see [Upgrading the SecureSphere DB2 AS400 Native Side](#), or contact Imperva Technical Support before installing SecureSphere Agent for AS/400.

SecureSphere Agent for AS/400 First Time Login

To login for the first time:

1. Login with user:
ISECAGENT
and password:
AGENT
. A request to change the default password appears.

```

                                     Sign-on Information
                                     System:  S658B35C
Password has expired. Password must be changed to continue sign-on
request.

Press Enter to change your password.

F3-Exit sign-on request
(C) COPYRIGHT IBM CORP. 1980, 2005.

```

2. Press **Enter** to change the default password. See the Note below.

Change Password

User profile : ISECAGENT

Password last changed : 11/12/09

Type choices, press Enter.

Current password

New password

New password (to verify)

F3-Exit

F12-Cancel

3. To start SecureSphere Agent for AS/400, type STRISA in the command line. The main menu appears.

SAIMPMMN

SecureSphere Agent for DB2/400

iSecurity/Agent
System: RLDEMO

Network Access Management

1. Activation

2. Display Settings

3. User Activity Statistics

5. Display Activity Log

6. DBOPEN/SQL Exit Point Setting

7. DB Statistics Settings

Advanced Options

21. Blocking (Firewall)

22. Auditing Studio

23. Application Security

24. GDPR/PCI Encryption

File Usage

32. Journal Read Operation

33. Work With Reports

35. Display Application Journal

System Activity

51. Activation

52. OS/400 Audit Features

55. Display Log

General

81. System Configuration

82. Maintenance

90. Signoff

99. About

Selection or command

(c) www.razlee.com

Note:

Make sure your password has the following characteristics:

- It must have no fewer than 10 characters and no more than 14 characters.
- It must have at least one number, one capital letter, and one special character from:

- * + = # % ^ : / ~ . , [] _
- It cannot have more than two characters repeated in succession.

Requesting a License for SecureSphere Agent for AS/400

To access this information, select option **81. System Configuration** from the main menu. The following window appears.

```

SAPARMR      SecureSphere Agent System Configuration      14/11/16 16:28:50      SS20
Select one of the following:

                                General
                                91. Language Support
                                99. Copyright Notice

Selection ==> █

Release ID . . . . . 02.04 16-03-30 440E466 520 7459 1
Authorization code . . . . . ██████████ 1 S520

F3=Exit  F22=Enter Authorization Code
  
```

The license is provided by Imperva. To receive the license, you need to provide Imperva with the following information or send the Opt. 81 screenshot:

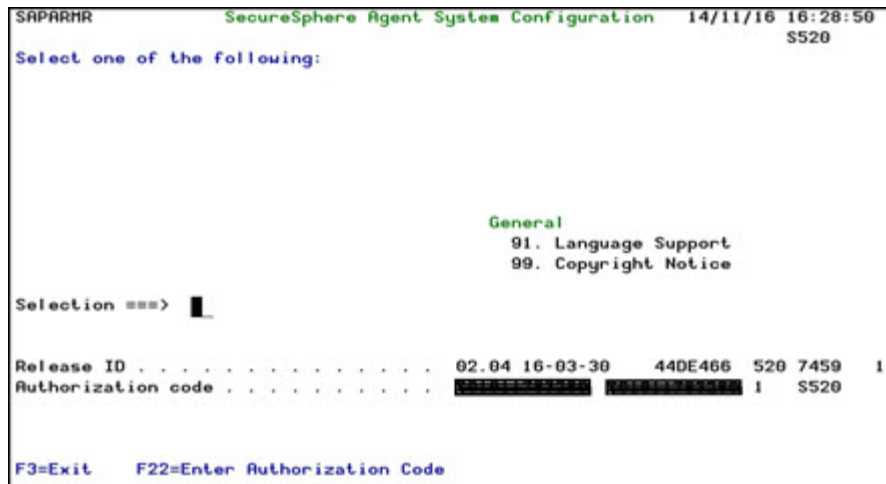
- **Product:** Name of the Product, e.g. SecureSphere Agent System Configurator
- **Model number:** The model number, e.g. 520
- **Processor feature:** The number representing the Processor feature, e.g. 7459
- **Your current LPAR:** The current LPAR you are working on, e.g. 1

Installing a new License for SecureSphere Agent for AS/400

To enter the license key:

1. Select option **81. System Configuration**

from the main menu. The following window appears:



2. Press **F22** to enter the license key.
3. On the screen above, enter the authorization code you were provided, as follows:
 1. First enter the 12 digit code in the left field.
 2. Enter the LPAR numbers in the right field beginning in the left most position.
4. After entering the authorization code, press **Enter** twice to confirm and return to the main menu.
5. To make sure the authorization code is correct, select option **55. Display Log**

and ensure you do not receive an error message.

Upgrading the SecureSphere DB2 AS400 Native Side

To upgrade an existing installation of Raz-Lee's technology, prior to SecureSphere Agent for AS/400 installation:

1. Make sure you have downloaded the A2P files and PTF folder from the Imperva FTP site.
2. Login to AS/400 server with a powerful user profile, preferably QSECOFR or a user with User Class *SECOFR or with *AUDIT, *SECADM, *JOBCTL and *SAVSYS authorities.
3. Deactivating Network Access Management:
 1. From the main menu, select option **1. Activation -> 21.Suspend Activity (before upgrade)** from the **Exit Points Settings** menu.
 2. Select option **1. Work with Servers from the Exit Points Settings** menu.
 3. Make sure all servers' Secure status is set to **No** and press **Enter** to confirm. Press **F3** to return to the main menu.
4. Deactivating System Activity
 1. To deactivate System Activity, select **51. Activation > 5. Work With Active Jobs** from the main screen to check if the subsystem ZAUDIT is active.
 2. If active, press **F3** and then de-activate product by selecting **2. De-activate Real- Time Detection** from the **Activation** screen.
5. In the command line, type:

```
CRTLIB LIB(ISECAGENT) TYPE(*TEST) TEXT('SecureSphere Agent: Temporary Library')
```

If the library already exists, the following message appears:

Library ISECAGENT already exists.

Go to the next step (5) (which is in the gateway/GUI).

6. If there is a running Agent and you wish to upgrade, then perform the following:
 1. In **Setup > Sites**, select the relevant service.
 2. Uncheck **Enable** in the **Log Collector** settings.
 3. Click **Save** and wait until the configuration is applied. This may take as long as a minute or so.
7. Create the following save files in the ISECAGENT library by typing the following commands:
 1. CRTSAVF FILE (ISECAGENT/SMZ8)

If the following message appears:

```
File SMZ8 in library ISECAGENT already exists.
,type:
```

```
CLRSAVF FILE (ISECAGENT/SMZ8) .
```

The following message appears:

```
Save file SMZ8 in library ISECAGENT cleared.
```

2. CRTSAVF FILE (ISECAGENT/SMZJ)

If the following message appears:

```
File SMZJ in library ISECAGENT already exists.
,type
```

```
CLRSAVF FILE (ISECAGENT/SMZJ)
```

The following message appears:

```
Save file SMZJ in library ISECAGENT cleared.
```

3. CRTSAVF FILE (ISECAGENT/SMZ4)

If the following message appears:

```
File SMZ4 in library ISECAGENT already exists.
,type
```

```
CLRSAVF FILE (ISECAGENT/SMZ4)
```

The following message appears:

```
Save file SMZ4 in library ISECAGENT cleared.
```

4. CRTSAVF FILE (ISECAGENT/SMZS)

If the following message appears:

```
File SMZS in library ISECAGENT already exists.
,type
```

```
CLRSVAF FILE (ISECAGENT/SMZS)
```

The following message appears:

Save file SMZS in library ISECAGENT cleared."

8. Use FTP in BIN mode to copy the corresponding installation media into the previously created save files:

FTP

(type IP Address or System Name)

user

(use the same user name as in point No. 1)

password (type the password)

BIN

```
PUT GSrelVos.A2P isecagent/smz8
```

```
PUT AUrelVos.A2P isecagent/smz4
```

```
PUT JRrelVos.A2P isecagent/smzJ
```

```
PUT SAreIVos.A2P isecagent/smzS
```

rel = component release version, os = operating system version

```
C:\>ftp 1.1.1.101
Connected to 1.1.1.101.
220-QTICP at 1.1.1.101.
220 Connection will close if idle more than 5 minutes.
User (1.1.1.101:(none)): qsecofr
331 Enter password.
Password:
230 QSECOPR logged on.
ftp> bin
200 Representation type is binary IMAGE.
ftp> put GS150U61.A2P isecagent/smz8
200 PORT subcommand request successful.
150 Sending file to member SMZ8 in file SMZ8 in library ISECAGENT.
226 File transfer completed successfully.
ftp: 32117184 bytes sent in 4.13Seconds 7785.98Kbytes/sec.
ftp> put AU110U61.A2P isecagent/smz4
200 PORT subcommand request successful.
150 Sending file to member SMZ4 in file SMZ4 in library ISECAGENT.
226 File transfer completed successfully.
ftp: 35811072 bytes sent in 4.56Seconds 7849.86Kbytes/sec.
ftp> put JR070U61.A2P isecagent/smzj
200 PORT subcommand request successful.
150 Sending file to member SMZJ in file SMZJ in library ISECAGENT.
226 File transfer completed successfully.
ftp: 19472112 bytes sent in 2.44Seconds 7986.92Kbytes/sec.
ftp> put SA010U61.A2P isecagent/smzS
200 PORT subcommand request successful.
150 Sending file to member SMZS in file SMZS in library ISECAGENT.
226 File transfer completed successfully.
ftp: 1654752 bytes sent in 0.22Seconds 7555.95Kbytes/sec.
ftp> quit
221 QUIT subcommand received.
C:\>
```

9. In the command line, type:
ADDLIB LIB (ISECAGENT)

. The following message appears:

```
Library ISECAGENT added to library list
```

10. Restore the installation program from the SecureSphere Agent save file into the installation library. Type:

```
RSTOBJ OBJ(INSTISA) SAVLIB(SMZS) DEV(*SAVF) OBJTYPE(*PGM) SAVF(SMZS) MBROPT(*ALL) ALWOBJDIF(*ALL) RSTLIB(ISECAGENT)
```

The following message appears:

```
1 objects restored from SMZS to ISECAGENT
```

11. Check for object locks on each specific module program library. Type:

```
WRKOBJLCK SMZx *LIB
```

The following message appears:

```
There are no locks for the specified object
```

Check for object locks on each specific module data library. Type:

```
WRKOBJLCK SMZTMPA*LIB
```

```
WRKOBJLCK SMZ4DTA*LIB
```

```
WRKOBJLCK SMZJDTA*LIB
```

```
WRKOBJLCK SMZSDTA*LIB
```

The following message appears:

```
There are no locks for the specified object
```

```
OR: SMZ4/CHKSECLCK PART(SMZx) TYPE(*ALL )
```

The following message appears:

```
No locks found for files of type *ALL of iSecurity library SMZx8.
```

Where:

x= 8, 4, J, S

SMZ8= Network Access Management

SMZ= File Usage

SMZJ= System Activity

SMZS= SecureSphere Agent for AS/400

12. Run the program. Type:

```
CALL PGM(INSTISA)
```



Note: The following examples are for Firewall but are relevant for all the components.

13. If there was a problem restoring the media, such as a damaged file, authorization problem or the save file is empty, the following error message appears:

```
SMZ8-Firewall: Missing installation media. R-Retry, C-Cancel, S-Skip
```

1. Select one of the following actions:

R-Retry: tries to perform the same operation again

C-Cancel: aborts the installation process and displays the following error message:

```
'Error occurred while installing an essential part of the SecureSphere
Agent. Check detailed messages (DSPJOBLOG + F10 on the screen or print
via DSPJOBLOG OUTPUT(*PRINT) '
```

S-Skip: bypasses the installation or upgrade of the current product component and continues with the next component or step of the installation procedure.

The program checks if the product components were already installed;

14. If the component version being installed is equal or higher than the existing component version in the disk, the following message appears:

```
SMZ8-Firewall: Do you wish to Upgrade? G-Go, C-Cancel, S-Skip
```

1. Select one of the following actions:

G-Go: continues with the release upgrade of the component

C-Cancel: aborts the installation process and displays the error message:

```
'Error occurred while installing an essential part of the SecureSphere
Agent. Check detailed messages (DSPJOBLOG + F10 on the screen or print
via DSPJOBLOG OUTPUT(*PRINT) '
```

S-Skip: bypasses the installation or upgrade of the current product component and continues with the next component or step of the installation procedure

15. If the component version being installed is lower than the existing component version in the disk, the following message appears:

```
SMZ8-Firewall: Downgrading NN.N YY-MM-DD to NN.N YY-MM-DD
```

```
G-Go, S-Skip
```

Select one of the following actions:

G-Go: start the downgrading process

S-Skip: bypass the downgrading or upgrade of the current product component and will continue with the next component or step of the installation procedure.

16. The component SecureSphere Agent must always be upgraded. When the following message will be prompted:

SMZS-SecureSphere Agent: Do you wish to Upgrade? G-Go, C-Cancel, S-Skip

Select G to start the upgrade process

17. If the installation of all the components ends normally, the following message appears:

```
*** Installation of SecureSphere Agent installed successfully *** Press Enter
***
```

18. In the command line, type:

```
CLRLIB LIB(ISECAGENT)
```

The following message appears:

```
Library ISECAGENT cleared
.
```



Note: During the upgrade procedure, program libraries SMZx are created again on every installation. These libraries are created on the system ASP. Data Libraries SMZxDTA SMTTMPx are NOT created again and existing definitions are preserved.


19. Unzip the PTF file under the Network Access Management component folder and execute the file.



Notes:


- PTF installation can only be performed from a Windows based operating system machine.
- Make sure you have an FTP connection between the machine from where you are running the PTF and the AS/400.
- When executing the PTF file, you may type "i" to start the installation immediately or wait a few seconds for the installation to start automatically.
- During installation you are asked to provide the AS400 machine IP, user and password. Imperva recommends using **QSECOFR** for the user.

20. Unzip the PTF files under the System Activity component folder and execute the files in the order they are named.


	<p>Notes:</p> <ul style="list-style-type: none"> PTF installation can only be performed from a Windows based operating system machine. Make sure you have an FTP connection between the machine from where you are running the PTF and the AS/400. When executing the PTF file, you may type "i" to start the installation immediately or wait a few seconds for the installation to start automatically. During installation you are asked to provide the AS400 machine IP, user and password. Imperva recommends using QSECOFR for the user.
---	--

Configuring a DB2 for an AS/400 Log Collector Instance

To use a SecureSphere Log Collector, you must configure a DB2 for an AS/400 Log Collector instance.

	<p>Note: If there is a running Agent and you wish to add an in-product Application Journal, then perform the following:</p> <ol style="list-style-type: none"> In Setup > Sites, select the relevant service. Uncheck Enable in the Log Collector settings. Click Save and wait until the configuration is applied. This may take as long as a minute or so. Check Enable. Click Save.
---	--

To configure a DB2 for an AS/400 Log Collector instance:

- In the **Main** workspace, select **Setup > Sites**.
- In the **Sites Tree**, navigate to the server group.
- Select the DB2 service you want to monitor.
- In the **Definitions** tab, under **Log Collectors**, click .
- Enter a **Name**.
- In **Type**, select **DB2 over AS/400**.
- Select a **Gateway** on which the collector instance will run.

Specify a gateway, not a gateway group.

- In **Host**, specify the IP address of the AS/400 DB2 server to monitor.
- Click **Save**.
- Click the plus sign next to **Name** to display the other parameters:
 - Executable (read-only)**
 - Protocol** – Select either **FTP** or **FTPS**. Configuring FTPS ensures the collected logs from the AS/400 DB2 are encrypted using SSL for enhanced security.

In order to support FTPS, you must configure the AS400 machine as an SSL FTP server. For more information, refer to the IBM Support website.

If you configure FTPS support, you must also configure the firewall to support the communication based on the operation mode (Active or Passive mode). For more information, see [Configuring the Firewall for FTPS Support for AS/400](#).

- **Location** – Remote directory that is used for collector logs and files.
 - **User, Password and Verify Password** – Enter the **User** and **Password** required in order to open an FTP connection to **Host** to transfer the audit records to the SecureSphere gateway.
 - **Delete Processed Log** – Select in order to delete logs (on **Host**) after they have been processed by SecureSphere.
 - **Connection Interval (minutes)** – Specify how frequently the collector instance should retrieve logs from **Host**.
 - **Additional Configuration** – To change the default configuration, consult with Technical Support.
11. Select **Enabled** to activate this collector instance.
 12. Click **Save**.

Configuring the Firewall for FTPS Support for AS/400

If you select FTPS as the protocol, you must configure the firewall to support the communication, as follows:

To support Active mode FTP, open the following communication channels:

- FTP server port 21 from anywhere (Client initiates connection)
- FTP server port 21 to ports > (larger than, high port range) 1023 (Server responds to client's control port)
- FTP server port 20 to ports > (larger than, high port range) 1023 (Server initiates data connection to client's data port)
- FTP server port 20 from ports > (larger than, high port range) 1023 (Client sends ACKs to server's data port)

To support Passive mode FTP, open the following communication channels:

- FTP server port 21 from anywhere (Client initiates connection)
- FTP server port 21 to ports > (larger than, high port range) 1023 (Server responds to client's control port)
- FTP server ports > (larger than, high port range) 1023 from anywhere (Client initiates data connection to random port specified by server)
- FTP server ports > (larger than, high port range) 1023 to remote ports > 1023 (Server sends ACKs (and data) to client's data port)

By default, the configuration is for Active mode. You can switch to passive mode at any time.

To configure Passive mode FTP protocol for FTPS support for AS/400:

1. In the **Main** workspace, select **Setup > Sites**.
2. In the navigation tree on the left, select the Server Group to which the log collector is assigned.
3. Select the Service to which the log collector is assigned.
4. Verify that the **Definitions** tab is selected and expand **Log Collectors**.
5. Select the **Log Collector**.
6. Update **Additional Configuration** by adding

is-passive-connect="true"
to the
settings
tab, for example:


Before:

```
<as400> <remote-time-cmd string="CALL SMZS/SATIMER ##OUTLIBRARY##" remote-file-name="SATIMEF" local-file-name="timestamp"/> <settings delete-local-files="true" max-timeframe-in-hours="24" file-size-in-seconds="3600" is-library-file-format="true"/><timestamp-file> <fields> <field name="date" start-offset="23" length="6"/> <field name="time" start-offset="29" length="6"/> <field name="ccsid" start-offset="105" length="5"/> ...
```

After:

```
<as400> <remote-time-cmd string="CALL SMZS/SATIMER ##OUTLIBRARY##" remote-file-name="SATIMEF" local-file-name="timestamp"/> <settings  
is-passive-connect="true"  
  delete-local-files="true" max-timeframe-in-hours="24" file-size-in-seconds="3600" is-library-file-format="true"/><timestamp-file> <fields> <field name="date" start-offset="23" length="6"/> <field name="time" start-offset="29" length="6"/> <field name="ccsid" start-offset="105" length="5"/> ...
```

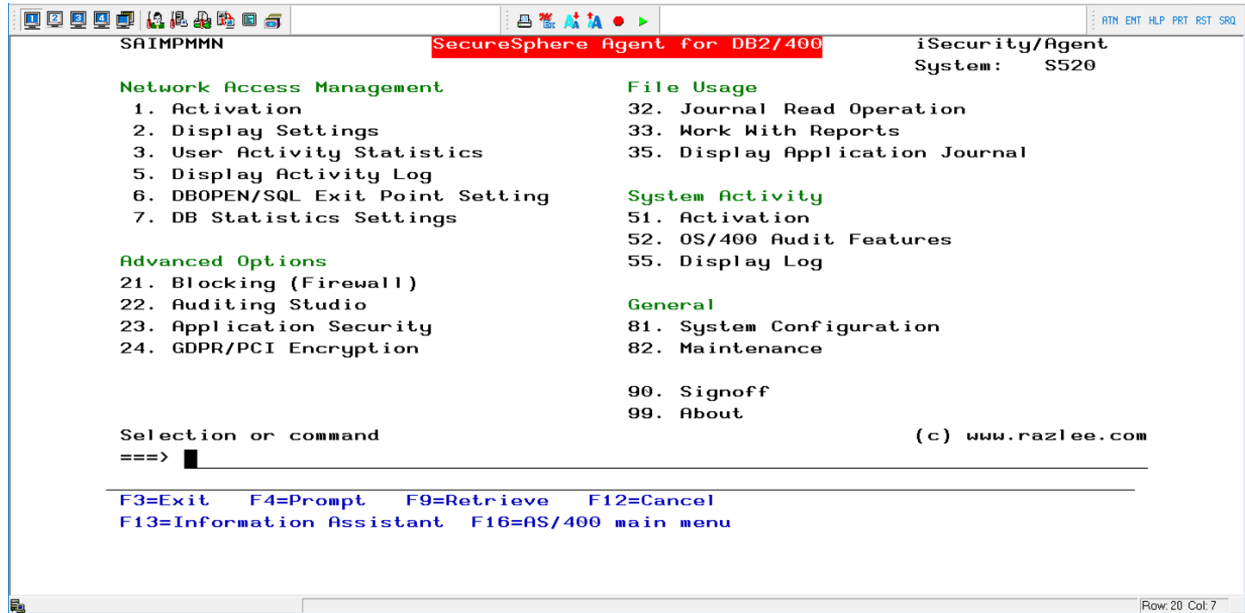
7. Click **Save**.

	<p>Note: To configure Active mode when Passive mode has been set, repeat the procedure above but in Step 6, remove the text string is-passive-connect="true".</p>
---	---

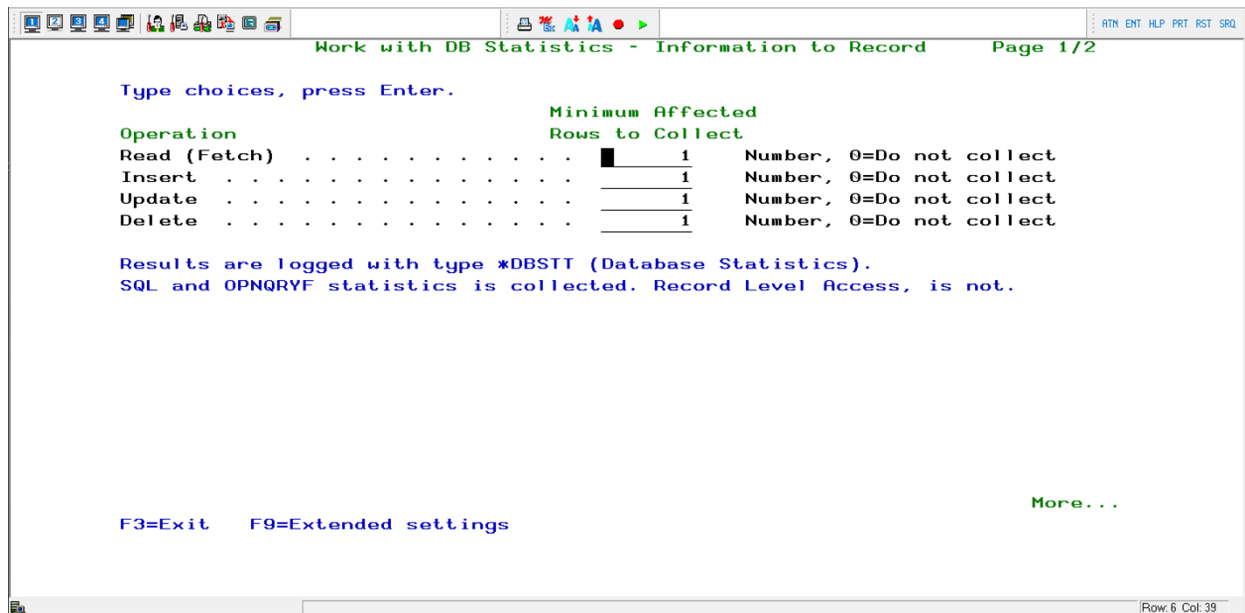
Setting DB Statistics (SQL Response Size)

To activate DB Statistics: STRISA > 7. DB Statistics Settings

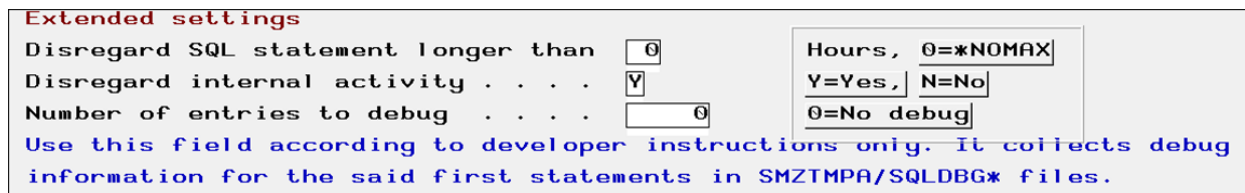
1. In the SecureSphere Agent for DB2/400 window, under **Network access Management**, select **Activation** to activate Agent Network Access Management component.
2. Under **Network access Management**, select **DB statistics Settings**.



3. Update the following fields: minimum value = 1.



4. Press **F9** > **Optional parameter**.



5. Press **F6** > **Sequence #** > **Active = Y**.

Work with DB Statistics - Data to Control Page 2/2

Type choices, press Enter.
1=Select 4=Delete

Subset . . .

Opt	Seq	Active	Description
<input checked="" type="checkbox"/>	1	Y	/* No filter defined. All files are included */

Bottom

At least one control entry must be Active for DB statistics to start.

F3=Exit F6=Add New F10=Inc/Exclude F12=Previous

[Row: 7 Col: 3]

6. Define the filter or keep it as it is.

Filter DB Statistics (FTRDBSTT)

Type choices, press Enter.

Filter by database file:

File	<input checked="" type="checkbox"/> *NONE	Name, generic*, *NONE, *ALL
Library	_____	Name, generic*
Filter Operator	_____	*EQ, *NE
+ for more values		

Filter by user profile:

User	_____	Name, generic*, *NONE...
Filter Operator	*EQ	*EQ, *NE
+ for more values		

Filter by job name:

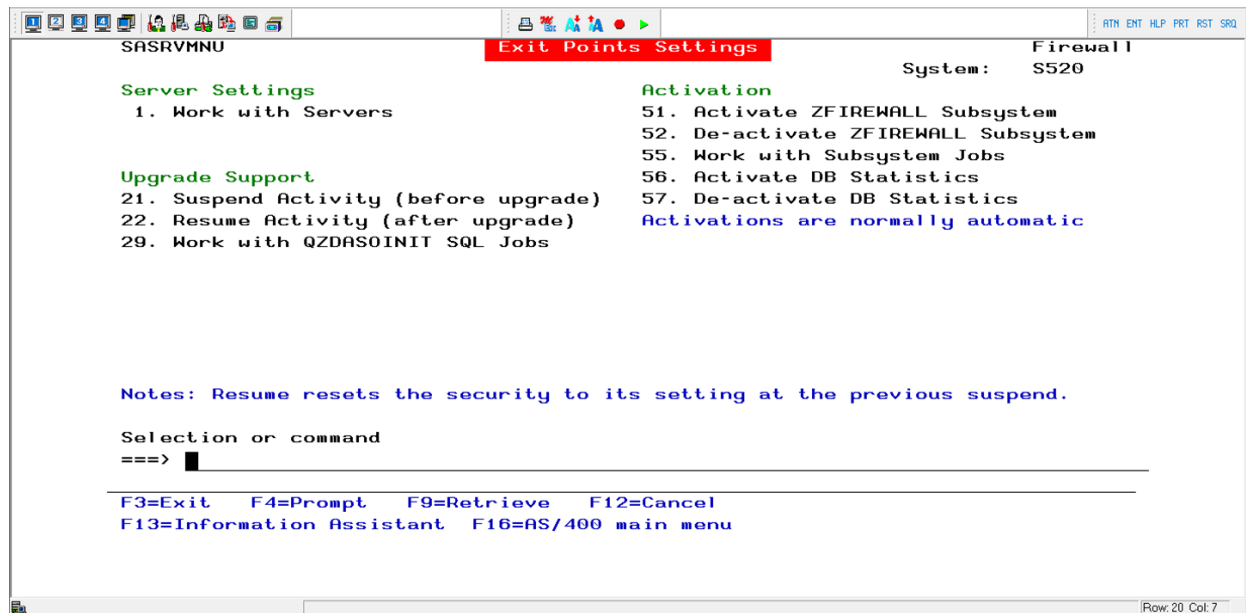
Name	* _____	Name, generic*, *, *ALL
User	_____	Name, generic*, *ALL
Number	_____	000000-999999, *ALL
Filter operator	*EQ	*EQ, *NE

Bottom

F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

[Row: 5 Col: 35]

7. Press **Enter**.
8. Press **Enter**.
9. Press **F3**.
10. Select **Activation**.
11. Select **Activate DB Statistics**.



12. Select **Work with Subsystem Jobs** and check that **Agent Network Access Management** component and **DB statistics** are active.

GS#DBMON	SECURITY1P	STAPEL	AKTIV		PGM - GSDBMNM
GS#FIRELOG	SECURITY1P	AUTO	AKTIV		PGM - GSLOGFWR
GS#FIREWAL	SECURITY1P	AUTO	AKTIV		PGM - GSSIGNON

SecureSphere Agent for AS/400 Failed Login Support

As of AS400 AGENT-SA02.13 (FIREWALL-GS18.26, AUDIT-AU14.16, JOURNAL-JR09.10), the agent's Audit module (14.16) supports Failed Login events. This means that the Audit log file supports two new entry-types, Authority failure (AF) and Invalid password (PW). Once an event with type AF or PW arrives, a Failed Login event is created in the gateway.

The specific use-case supported are:

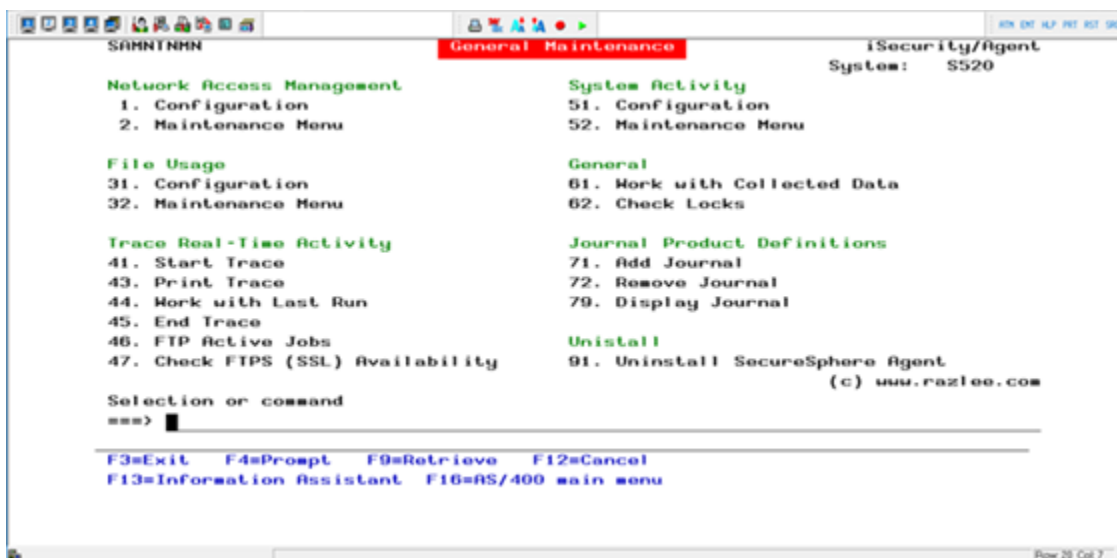
AF	S	Attempt made to sign on without entering a user ID or a password.
AF	T	Not authorized to TCP/IP port
PW	P	An incorrect password was entered.
PW	Q	Attempted sign on (user authentication) failed because the user profile was disabled.

PW	R	Attempted sign on (user authentication) failed because the password expired.
PW	U	User name is not valid.
PW	S	SQL decrypted a password that was not valid

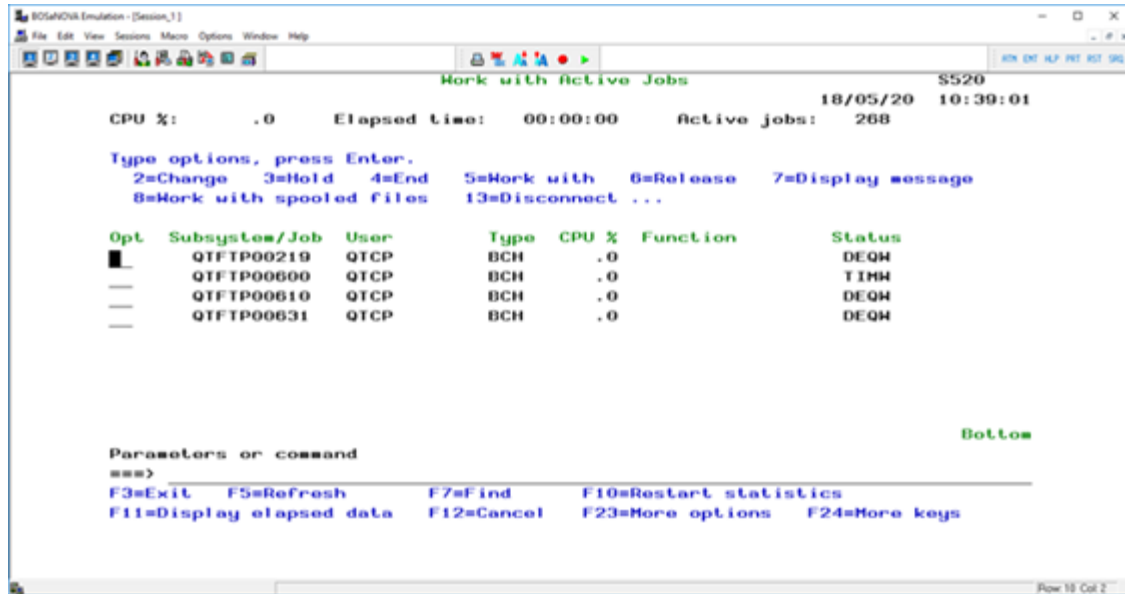
Maintenance Options

The following Maintenance options are available:

In the General Maintenance screen:



- FTP Active Jobs - When the Imperva gateway is connected with only one ISECAGENT, the FTP user job should be active.



- Check FTPS (SSL) Availability - Check FTPS (SSL) Availability on the AS400



Uninstalling SecureSphere Agent for AS/400

To uninstall the SecureSphere Agent for AS/400:

1. Disable the gateway connected to the agent you want to uninstall.
2. Login to the agent as user **QSECOFR**.
3. Type **STRISA** and press **Enter**.
4. Under **System Activity**, go to **Activation(51) -> Deactivate(2)**.
5. Under **Network Access Management**, go to **Activation(1) > Work with servers (1)**.
6. Type **1** in all of the options.

7. In the **Secure** line under **Original**, Type **2**.
8. Go to **Deactivate (52)**.
9. In the SecureSphere Agent for DB2/400 menu (STRISA), go to **Maintenance (82) > (91)** and follow the instructions for uninstalling.
10. Repeat step 9 for Application Journal (STRJR).
11. Repeat step 9 for Audit (STRAUD).
12. Repeat step 9 for Firewall (STRFW).