Version 9 Release 2

IBM i2 Intelligence Analysis Portfolio Product Access Management Guide

Note

Before using this information and the product it supports, read the information in “Notices” on page 27.

This edition applies to IBM® i2® Analyst's Notebook® 9.2.1 (product number 5725G07), IBM i2 Analyst's Notebook® Premium 9.2.1 (product number 5725G21), and IBM i2 iBase 8.9.13 (product number 5725G15) and to all subsequent editions and modifications until otherwise indicated in new releases.

Contents

Chapter 1. About this guide 1

Chapter 2. Contacting IBM Support 3

Chapter 3. About Product Access Management 5
Deployment scenarios 5
Single server 5
Several servers on one network 5
Several unconnected networks 5
Several connected networks 6
Permits 6
Users can borrow permits for use when not connected to the network 6
Design and deployment process 6

Chapter 4. Deploying Product Access Management on the server 7
Generate lock codes 7
Complete the permit request form and receive permits 7
Install the Sentinel RMS License Manager 7
Install permits 8
Reservation groups 9
Creating reservation groups 10

Chapter 5. Designing the deployment 11
Design the deployment 11

Chapter 6. Setting up Product Access Management on the client 13
Setting server connection options on the client 13
Installing IBM i2 applications with Product Access Management enabled 13
Setting server connection options if the Product Access Console is not installed 15

Chapter 7. Running IBM i2 applications 17
Borrowing and returning permits for offline use 17
Borrowing a permit 17
Returning a borrowed permit 18
Borrowing a permit when not connected to the network 18

Chapter 8. Accessing and interpreting the server log file 21
Sentinel RMS License Manager specification 22

Appendix A. Sentinel RMS License Manager specification 25

Notices 27

Chapter 1. About this guide

Product access management is an optional feature that enables organizations to control the number of users able to concurrently run access management enabled IBM i2 applications.

This guide describes how to set up and use Product Access Management on servers and clients. This guide assumes that the server and client are running Microsoft Windows.

Intended audience

This guide is intended for system administrators who are responsible for managing software usage within their organization.

Chapter 2. Contacting IBM Support

IBM Support provides assistance with product defects, answers FAQs, and helps users to resolve problems with the product.

About this task

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the *Software Support Handbook*.

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM Support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Online through the IBM Support Portal at https://www.ibm.com/mysupport/. You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
   - By phone. For the phone number to call in your region, see the Directory of worldwide contacts web page at https://www.ibm.com/planetwide/

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

Chapter 3. About Product Access Management

Product access management helps you to ensure that your organization remains compliant with your license agreement with IBM. You can control usage of IBM i2 applications so that the number of concurrent users stays within the number that is permitted by your license agreement. Product access management is an optional feature and IBM i2 applications can be used without it.

The applications that support Product Access Management are:

- IBM i2 Analyst's Notebook® 8.9.5, or later.
- IBM i2 Analyst's Notebook Premium 8.9.5, or later.
- IBM i2 iBase User and Designer 8.9.5, or later.

Product access management uses a server and client model to monitor application usage. Implementing product access management involves the creation, deployment, and usage of permits.

Important: The product access management feature is compatible with earlier supported versions of IBM i2 applications, but is not always compatible with later versions. If you are upgrading from an earlier version, to ensure that your licenses are handled correctly, upgrade your license manager before you upgrade your IBM i2 applications.

To upgrade the license manager, double-click `setup.exe` in the `\Product Access Management \Server` directory of the IBM i2 application downloaded distribution, and follow the steps provided.

Deployment scenarios

Product access management can be deployed in a number of different ways:

Single server

The simplest deployment scenario involves a single server. The server is connected to the same network as all users of IBM i2 applications in the organization.

This scenario has minimal complexity, but provides no alternative source of permits if the server becomes unavailable.

Several servers on one network

Several servers can be connected to a network. All users of IBM i2 applications are connected to the same network as the servers. This scenario provides alternative sources of permits and avoids creating a single point of failure. A proportion of the permits can be installed on each server.

Each client can be configured to:

- Connect to a specific server on the network
- Connect to a number of servers in a sequential manner to find an available permit
- Search the network to find any server with an available permit

By tailoring the method that is used by clients to apply for permits, network traffic can be managed.

Several unconnected networks

Your organization might have several unconnected networks. In this scenario, use one or more servers on each network to provide permits to users of that network.

To ensure that an appropriate number of permits are available, install enough permits on each server to reflect the needs of the users of each network.

Several connected networks

Your organization might have several networks that are connected by a wide area network or similar. To provide clients with a source of permits on their network, connect a server to each network and install enough permits for users of that network. To provide clients with a secondary source of permits, configure the server list on each client to include servers on other networks.

This deployment scenario provides users with a secondary source of permits if the server on their network is unavailable or all permits are in use.

Permits

A permit enables an IBM i2 application with access management to load successfully. Each server contains a number of permits that are issued to users with access on a first come first served basis. Additionally, each permit relates to a specific IBM i2 application, such as Analyst's Notebook. As a result, each available permit for an application can be used by any authorized user that requires use of that application.

Note: To run an IBM i2 application when not connected to the network, a user can borrow a permit from a server.

IBM supplies permits in a permit file. Permit files can be configured to reserve or restrict permits for use by specific users or computers.

A permit file can be installed on only the server that the permit file was generated for. If the server hardware changes, or if you want to use a different server to distribute permits from, then you must request a new permit file.

Users can borrow permits for use when not connected to the network

To run an IBM i2 application when not connected to the corporate network, a user can borrow a permit from a server. A permit can be borrowed by a user for a minimum of a day, up to a maximum of five years. The permit is copied to the client and used during startup, and the IBM i2 application does not request a permit from a server. The permit is not available to other users until it expires or is returned to the server.

For more information, see “Borrowing and returning permits for offline use” on page 17.

Design and deployment process

For information about how to design your product access management deployment and deploy it, see:

1. “Design the deployment” on page 11.
2. “Generate lock codes” on page 7.
3. “Complete the permit request form and receive permits” on page 7.
4. “Install the Sentinel RMS License Manager” on page 7.
5. “Install permits” on page 8.

Chapter 4. Deploying Product Access Management on the server

To make permits available to clients, you must generate lock codes, request permits from IBM, then install the server software and permits on the server.

Generate lock codes

A lock code is used to identify the server that is used to store permits.

About this task

In order for IBM to generate permit files, a lock code must be generated for each server. This unique code is generated based on the hardware specification of each server and is not transferable.

Note: Server details are not available to IBM, the original information is encrypted and cannot be extracted from the lock code.

Procedure

On each server that is used in the deployment:

1. Run `LockCodeGenerator.exe`. This application is found in the IBM i2 application downloaded distribution in the `\Product Access Management\Utils` directory.
2. Click **Generate Lock Code**. A lock code is displayed in the **Lock code** area.
3. To copy the lock code to the clipboard, click **Copy**.
4. Paste the lock code on a permit request form.

Complete the permit request form and receive permits

Upon receipt of a completed permit request form, IBM generates permits and sends them to you. Use one form for each server. The form is found in the IBM i2 application downloaded distribution in the `\Product Access Management\Utils` directory.

Procedure

1. Complete questions 1 - 7 on the permit request form.
2. In question 8, enter the number of users of each IBM i2 product that the permits installed on the server provide access for.
3. Send the permit request form to i2PermitRequest@uk.ibm.com.
4. IBM generates one `.lic` permit file for each server and sends the permit files to you. A permit file can contain permits for more than one IBM i2 application.

Install the Sentinel RMS License Manager

Install Sentinel RMS License Manager on each server that is used to distribute permits to clients.

Procedure

To run the Sentinel RMS License Manager installer, double-click `setup.exe` in the `\Product Access Management\Server` directory of the IBM i2 application downloaded distribution.

What to do next

When the installation of the Sentinel RMS License Manager is complete, check that a Windows service called Sentinel RMS License Manager is present on the server.

If the installer did not add a Windows Firewall exception for the Sentinel RMS License Manager, add an exception for *%ProgramFiles%*\Common Files\SafeNet Sentinel\Sentinel RMS License Manager\WinNT\lservnt.exe.

Install permits

Install permits on the server to make them available to clients.

Procedure

1. If you have not already done so, create a *%ProgramFiles%*\Common Files\SafeNet Sentinel\Administration Tools directory. Copy the contents of the \Product Access Management\Utils directory in the IBM i2 application downloaded distribution to the new directory.
2. In the Administration Tools directory, double-click WlmAdmin.exe.

   The WlmAdmin application opens.
3. In WlmAdmin, expand the server navigation tree to display the required server.
4. Right-click on the server then click **Add Feature** > **From a File** > **To Server and its File**.

   The **Open** window is displayed.
5. In the **Open** window, browse to the location of the permit file. Select the permit file, then click **Open**. The rows in the permit file are validated to ensure that they are intended for that server. If validation is successful, the permits are added to the server and a message is displayed.

   Note: In server applications such as WlmAdmin, a feature is equivalent to an IBM i2 application. For example, the IBMANB.main feature corresponds to the Analyst's Notebook application. Permits are installed on a server for a feature, and an IBM i2 application requests a permit from a server when it loads.

Results

You can use WlmAdmin to view the permits that are installed on a server.

To monitor usage of permits, see Chapter 8, “Accessing and interpreting the server log file,” on page 21.

To reserve permits on a server for use by specific users or clients, configure Reservation Groups on the server. For more information, see “Reservation groups” on page 9.

For each IBM i2 product, you receive permits for these features:

Product	Features
Analyst's Notebook	IBMANB.main (Analyst's Notebook)
Analyst's Notebook Premium	IBMANB.main (Analyst's Notebook) IBMANB.ARConnector (Analysis Repository connector for Analyst's Notebook)
iBase	IBMiBase.main (iBase)

Product	Features
iBase Designer	IBMiBase.main (iBase) IBMiBaseDesigner.main (iBase Designer)

Reservation groups

You can use reservation groups to reserve permits for particular users and client computers.

Reservation groups help to:

- Ensure that permits are available when they are required
- Balance the use of applications between individuals, teams, or departments
- Prevent unauthorized use of applications

To ensure the availability of a permit, a user or client computer can be added to a reservation group for a feature and marked as included. To prevent the use of an application, the user or client computer can be marked as excluded.

Reservation groups are applied to particular features. For IBM i2 products, the following features are used:

Product	Features
Analyst's Notebook	IBMANB.main
Analyst's Notebook Premium	IBMANB.main IBMANB.ARConnector
iBase	IBMiBase.main IBMiBaseDesigner.main

The reservation groups for each feature are held in a reservation file on the server.

When a server receives a request for a permit, it checks whether the user or client that is requesting the permit belongs to a reservation group:

- If the user or client belongs to a reservation group, and is marked as included, permits for that group are made available.
- If the user or client belongs to a reservation group, and is marked as excluded, no permits for that group are made available.
- If the user or client does not belong to a reservation group, only unreserved permits that are not in use are made available.

These restrictions apply to reservation groups:

- A server can have a maximum of 256 reservation groups.
- Each reservation group can have a maximum of 1000 members; a member is a user or client computer. Users are identified by Windows user names, and clients are identified by computer name or IP address.
- Different reservation groups for the same feature on a server cannot have common members.
- Reservation group names and member names cannot exceed 64 characters.

- The number of application permits that are reserved cannot exceed the number of permits that are installed for that application.

Note: If a reservation file is created or edited, the **Sentinel RMS License Manager** service must be restarted for the reservation groups to take effect.

Creating reservation groups

Create reservation groups to manage user access to product access management enabled applications.

Procedure

1. Copy the contents of the `\Product Access Management\Utils` directory in the IBM i2 application downloaded distribution to the *%ProgramFiles%*`\SafeNet Sentinel \Administration Tools` directory on the server.
2. In the `Administration Tools` directory, double-click `WlmAdmin.exe`. In WlmAdmin, click **Edit** > **Reservation File**.

   The WlsGrMgr application opens.
3. In WlsGrMgr, click **File** > **New**.

   Note: To edit an existing reservation list, click **File** > **Open**, browse to the location of the list, select the file, and click **Open**.
4. Click **Feature** > **Add**.

   The **Add License Reservation Wizard** opens.
5. Click **Next**. In the **Feature Name** field, enter the appropriate name. In the **Feature Version** field, enter 1 then click **Next**.
   For example, enter `IBMANB.main` in the **Feature Name** field.
6. In the **Group Name** field, enter a name for the reservation group. To select the number of permits to reserve, click the arrows in the **Tokens** field, then click **Next**.
7. Add members to the reservation group:
   a) Click **Add**, then enter the name of the member in the **Name of the Member** field.
      - For a user, enter their Windows user name.
      - For a client computer, enter the computer name or IP address.

   b) Specify whether the member is a user or a computer, click **User** or **Machine**.
   c) Specify whether the member is allowed or denied permits for the application, click **Included** or **Excluded**.
   d) Click **OK**.
8. Click **Finish**.

   The feature and reservation group are displayed in the relevant pane of the main **Wlsgrmgr** window.
9. Click **Save**.

   If a new reservation file is created, it is saved to the `My Documents\SafeNet Sentinel \Sentinel RMS Development Kit\Tools` directory with a file name of `lsreserv`.
10. To activate the reservation groups, copy the reservation file to the same directory as `lservnt.exe`, then restart the Sentinel RMS License Manager service. The default directory for `lservnt.exe` is *%ProgramFiles%*`\Common Files\SafeNet Sentinel\Sentinel RMS License Manager\WinNT`. Alternatively, if the LSRESERV environment variable defines a path and file name for the reservation file, rename the reservation file and save it in the appropriate directory.

Chapter 5. Designing the deployment

You must decide how many servers to distribute permits from and how many permits to make available from each server for each application. The number of permits that you make available to users can ensure that your organization remains compliant with your license agreement.

You can use an ordinary workstation as a permit server; dedicated server hardware is not required. For server hardware and software requirements, see “Sentinel RMS License Manager specification” on page 22. You might already have a server within your network that runs the SafeNet Sentinel RMS License Manager software.

For more information about deployment, see “Deployment scenarios” on page 5.

A permit is locked to specific server hardware. For more information about permits, see “Permits” on page 6.

Design the deployment

To ensure that users can access IBM i2 applications, design your deployment appropriately.

Procedure

1. Select which servers to distribute permits from.
2. Decide how many permits to allocate to each server for each application.

Chapter 6. Setting up Product Access Management on the client

Product access management must be enabled for each application on the client that requires monitoring. You can configure the client with a list of specific servers to request permits from. You can also enable network broadcast so that the client can search for servers.

Setting server connection options on the client

Use the **Settings** tab of the Product Access Console to configure how the client connects to servers. You can enter a list of servers that all access management enabled IBM i2 applications on the client request permits from. If a request to a server is unsuccessful, the application tries the next server in the list. You can also enable network broadcast to search for any servers that are able to supply permits, and you can modify timeout settings.

Procedure

1. From the **Start** menu, open the Product Access Console by clicking **IBM i2 Tools** > **Product Access Console**.
2. Click the **Settings** tab.
3. To modify the server list, enter a comma-separated list of server names or IP addresses in the **Server list** field.
4. Optional: To enable network broadcast, select the **Broadcasts enabled** check box.
5. To select the broadcast timeout value, click the arrows in the **Broadcast timeout (seconds)** field.

   The broadcast timeout is the maximum period (in seconds) that the client waits for a response to a search on the network for a server. Two broadcast attempts are made during this period.
6. To select the network timeout value, click the arrows in the **Network timeout (seconds)** field.

   The network timeout is the maximum period (in seconds) that the client waits for a response from a server after a request for a permit. The request might be resent a number of times during this period.

Installing IBM i2 applications with Product Access Management enabled

Installing IBM i2 applications with Product Access Management enabled allows permits to be requested from the server.

You can use **`msiexec`** to install IBM i2 applications and enable Product Access Management. Use standard **`msiexec`** command-line options to install applications in a suitable way.

```
msiexec /i "package_name.msi" I2LIC_ENABLED="#1"
```

Where *package_name* applies to the appropriate packages for the IBM i2 product:

Product	Packages
Analyst's Notebook	`IBM i2 Analyst's Notebook 9.msi`
Analyst's Notebook Premium	`IBM i2 Analyst's Notebook Premium 9.msi`
iBase	`IBM i2 iBase 9.msi`

Use the **I2LIC_ENABLED** property only with packages for Product Access Management enabled IBM i2 applications. To enable Product Access Management for the application, set the **I2LIC_ENABLED** property to "#1"; set it to "#0" to disable.

Note: If you use **msiexec** with the full user interface enabled, Product Access Management is not displayed in the feature list. Nonetheless, if you set the **I2LIC_ENABLED** property to "#1", Product Access Management is enabled.

The default feature selection of the `IBM i2 iBase 9.msi` package consists of iBase User with examples, documentation, and help. If you are using **msiexec** with the basic, reduced, or no user interface option, and want to install other features like iBase Designer, use the **ADDLOCAL** property to specify which features to install. Commands that install iBase with common features and enable access management are described in this table:

Features	Command
iBase User and iBase Designer	`msiexec /i "IBM i2 iBase 9.msi" ADDLOCAL=AdminCenter,iBaseDesigner, DesignerExamples,DesignerHelp, ThirdParty,iBaseUser,UserDocs, UserExamples,UserHelp,iBase,iBaseSSE I2LIC_ENABLED="#1"`
iBase User with GIS interfaces	`msiexec /i "IBM i2 iBase 9.msi" ADDLOCAL=iBaseExtended,GIS,GISArcGIS, GISArcView3,GISBlue8World,GISBlue8XD, GISHelp,GISMapInfo,GISMapPoint, ThirdParty,iBaseUser,UserDocs, UserExamples,UserHelp,iBase,iBaseSSE I2LIC_ENABLED="#1"`
iBase User with Plate Analysis	`msiexec /i "IBM i2 iBase 9.msi" ADDLOCAL=iBaseExtended,ANPR,ANPRDocs, ANPRHelp,ThirdParty,iBaseUser,UserDocs, UserExamples,UserHelp,iBase,iBaseSSE I2LIC_ENABLED="#1"`

You can use the following properties that are specific to product access management:

Property	Description
I2LIC_SERVERS	Sets the server list. A comma-separated list of server names that must contain no spaces. For example, `msiexec /i "IBM i2 Analyst's Notebook 9.msi" I2LIC_ENABLED="#1" I2LIC_SERVERS=server1,server2`
I2LIC_BROADCASTS_ENABLED	Enables network broadcast on the client. "#1" to enable, "#0" to disable.

Property	Description
	For example, `msiexec /i "IBM i2 Analyst's Notebook 9.msi" I2LIC_ENABLED="#1" I2LIC_BROADCASTS_ENABLED="#1"`

You can also use the Product Access Console that is installed on the client to modify the server list and enable network broadcast. If you use **msiexec** with the full user interface enabled, select **Configure Product Access Management now** on the final installation wizard stage and click **Finish**. The Product Access Console is displayed. Alternatively, click **IBM i2 Tools** > **Product Access Console**. For more information, see "Setting server connection options on the client" on page 13.

Setting server connection options if the Product Access Console is not installed

To modify the server list or enable network broadcast when the Product Access Console is not installed, you edit the registry. For example, the Product Access Console is not installed on a server operating system if the Remote Desktop or Terminal Services role is enabled.

Before you begin

Back up the registry before you modify it. Incorrect modification of the registry can make a computer unusable.

Procedure

1. To modify the server list, set the **Server Order** value of the **HKEY_LOCAL_MACHINE\SOFTWARE\i2\Licensing** key to a comma-separated list of server names or IP addresses. The list must contain no spaces.
2. To enable network broadcast, set the **Broadcasts Enabled** value of the **HKEY_LOCAL_MACHINE\SOFTWARE\i2\Licensing** key to 1. To disable, set the value to 0.

   Note: The broadcast timeout and network timeout is 1 second.

Chapter 7. Running IBM i2 applications

During startup, an access management enabled IBM i2 application requests a permit from a server. If a permit is supplied by a server, the application successfully loads. If the application cannot acquire a permit, a message is displayed and the user can click **Retry** to try again, or can close the application.

If a user knows they need to use an IBM i2 application when network access is not possible, they can borrow a permit before they disconnect. The permit is copied to the client and the application does not request a permit.

Borrowing and returning permits for offline use

Permits can be borrowed from the server to allow IBM i2 applications to be used when not connected to the network.

When a permit is borrowed, it is copied and locked to the client, and is listed as in use on the server. As a result, the IBM i2 application does not request a permit from a server during startup and the application can be used offline.

A permit can be borrowed by a user for up to five years and can be manually returned at any point during this period.

Note: If a computer that contains a borrowed permit becomes permanently unavailable (for example, if it is stolen or fails), that permit cannot be remotely returned. The permit becomes available again from the server upon expiry. To prevent these permits remaining unavailable for long periods, ask users to borrow permits for only the amount of time that they require them.

Borrowing a permit

To use an IBM i2 application when not connected to the network, borrow a permit from a server while connected to the network.

Procedure

To borrow a permit:

1. Click **IBM i2 Tools** > **Product Access Console**.

   The Product Access Console is displayed.
2. Click the **Network** tab.

   A list of available permits is displayed.
3. Select a permit from the list.

   The **Can be borrowed** column indicates whether you can borrow the permit. The **Permit** column indicates the application that the permit is for.
4. To select when the permit expires, click the arrows in the **Borrow period (days)** field.
5. Click **Borrow**.

Results

The permit is copied to the client computer. You can check the status of borrowed permits on the **Local** tab.

Returning a borrowed permit

If you have access to the network and you no longer need a borrowed permit, you can return the permit to the server.

Procedure

1. Click **IBM i2 Tools** > **Product Access Console**.
   The Product Access Console is displayed.
2. Click the **Local** tab.
3. Select a permit from the list.
4. Click **Return**.

Results

The permit is returned to the server.

Borrowing a permit when not connected to the network

With your assistance, a user can borrow a permit when they are not connected to the network. The user must be able to send and receive text and files over email or other means.

Procedure

On the client:

1. Run `WRCommute.exe`. WRCommute is found in the *%ProgramFiles%*`\Common Files\i2 Shared\Licensing` directory. The client locking code string is displayed on the **Get Locking Code** tab.

On a computer that is able to connect to the server:

2. Run `WCommute.exe`.
   WCommute is found in the IBM i2 application downloaded distribution in the `\Product Access Management\Utils` directory. On a server that is used to distribute permits, `WCommute.exe` might be present in the *%ProgramFiles%*`\Common Files\SafeNet Sentinel\Administration Tools` directory.
3. To find the server to borrow a permit from, click **Search Subnet**, or click **Single Server** and specify a server name or IP address.
4. In the navigation pane, expand the server, select the required feature, and select **Check out authorization for remote machine**.
   a) In the **Enter number of days until the commuter authorization expires** field, enter the number of days to borrow the permit for.

      Note: A permit that is remotely borrowed cannot be returned before expiry. Upon expiry, the permit automatically becomes available again from the server. Borrow the permit for only the amount of time that it is required.

   b) Click **Check Out**.
      The "**Locking code for Remote Machine**" window is displayed.
5. Click **Enter the locking code string for remote machine**, enter the client locking code string, and click **OK**.
6. Click **Save commuter authorization to file**. Browse to the directory to save the permit file to, enter a file name, click **Save**, then click **OK**.
   The permit file is saved.

On the client:

7. Run `WRCommute.exe`. On the **Install Remote Authorization Code** tab, click **Get remote authorization codes from file**. Browse to the permit file and click the permit file. Click **Open**, and click **Install**. The borrowed permit is installed on the remote user's computer.

Chapter 8. Accessing and interpreting the server log file

A server records all permit requests and returns in a log file. This file provides logging and tracing of errors and transactions. By default the log file `lservsta` is created in the `C:\Windows\system32` or `C:\Windows\SysWOW64` directory.

Each row contains the following elements:

Element	Description
Server-LFE	Customer-defined log file encryption level as specified by the license manager **`-lfe`** option
License-LFE	Vendor-defined log file encryption level. If the element is non-zero, it overrides the Server-LFE
Date	The date the entry was made, in the format: Day-of-week Month Day Time (hh:mm:ss) Year
Time-stamp	The time stamp of the entry
Feature	Name of the feature
Ver	Version of the feature
Trans	The transaction type. 0 indicates an issue, 1 indicates a denial, 2 indicates a release
Numkeys	The number of permits in use after the current issue or release. (Encrypted if encryption level is set to 3 or 4.)
Keylife	How long, in seconds, the permit was issued. Only applicable after a permit release
User	The user name that is associated with the entry
Host	The host name that is associated with the entry
LSver	The version of the Sentinel RMS Development Kit license server
Currency	The number of permits that are handled during the transaction. (Encrypted if encryption level is set to 3 or 4.)
Comment	The text that is passed in by the application that is using the permit

Use Lsusage to view the Sentinel RMS License Server log file. Lsusage is found in the IBM i2 application downloaded distribution in the `\Product Access Management\Utils` directory. To run lsusage, open a command prompt and go to the directory that contains lsusage, then run:

```
lsusage.exe -l lservsta
```

Note: If the command fails because lservsta is not found, prefix `lservsta` with the directory file path that lservsta is found in.

To create a CSV file from the log, run:

```
lsusage.exe -l lservsta -c CSV-format-filename.
```

Sentinel RMS License Manager specification

Sentinel RMS License Manager is the server software that distributes permits to clients that request them. The minimum hardware and software requirements for Sentinel RMS License Manager are:

Supported Operating Systems	All RMS platforms include support for the following versions of Microsoft Windows (32-bit and 64-bit): • Windows 7 • Windows 8.1 • Windows10 v1809 • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 It is possible to install the software on client operating systems.
Processors	x86 processors for 32-bit and x86-64 processors for 64-bit.
Hard disk space	1150 MB free hard disk space
RAM	128 MB RAM on Windows 2000, XP, and 2003. 1 GB RAM on Windows Vista and other operating systems.
Installation Path	*%Program Files*\Common Files \SafeNetSentinel\Sentinel RMS LicenseManager\WinNT
Underlying protocol	UDP (User Datagram Protocol)
Network Port (Default)	5093
Reachability of server from client	Server can receive broadcasts within a network. Server can receive directed calls from clients across networks.
Virtualization	Sentinel RMS License Manager can be run in a virtualized environment. If the virtual machine that runs Sentinel RMS License Manager is moved, the permits that are generated for use on the server remain valid. If the virtual machine is copied, aspects of the virtual machine might change and the permits might become invalid.
Event log file	By default the usage log file `lservsta` is created in the `C:\Windows\system32` directory. The log file records all permit requests and returns in

	a log file and provides logging and tracing of errors and transactions. For more information, see Chapter 8, “Accessing and interpreting the server log file,” on page 21

Appendix A. Sentinel RMS License Manager specification

Sentinel RMS License Manager is the server software that distributes permits to clients that request them. The minimum hardware and software requirements for Sentinel RMS License Manager are:

Supported Operating Systems	All RMS platforms include support for the following versions of Microsoft Windows (32-bit and 64-bit): • Windows 7 • Windows 8.1 • Windows10 v1809 • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 It is possible to install the software on client operating systems.
Processors	x86 processors for 32-bit and x86-64 processors for 64-bit.
Hard disk space	1150 MB free hard disk space
RAM	128 MB RAM on Windows 2000, XP, and 2003. 1 GB RAM on Windows Vista and other operating systems.
Installation Path	*%Program Files*\Common Files\SafeNetSentinel\Sentinel RMS LicenseManager\WinNT
Underlying protocol	UDP (User Datagram Protocol)
Network Port (Default)	5093
Reachability of server from client	Server can receive broadcasts within a network. Server can receive directed calls from clients across networks.
Virtualization	Sentinel RMS License Manager can be run in a virtualized environment. If the virtual machine that runs Sentinel RMS License Manager is moved, the permits that are generated for use on the server remain valid. If the virtual machine is copied, aspects of the virtual machine might change and the permits might become invalid.

Event log file	By default the usage log file `lservsta` is created in the `C:\Windows\system32` directory. The log file records all permit requests and returns in a log file and provides logging and tracing of errors and transactions. For more information, see Chapter 8, "Accessing and interpreting the server log file," on page 21

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM United Kingdom Limited

Hursley House

Hursley Park

Winchester, Hants, SO21 2JN

UK

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Product Number: 5725G07, 5725G15, 5725G21