About Product Access Management

Product access management helps you to ensure that your organization remains compliant with your license agreement with i2®.

You can control usage of 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 i2® applications can be used without it. The applications that support Product Access Management are:

- i2® Analyst's Notebook 9.2.0, or later.
- i2® Analyst's Notebook Premium 9.2.0, or later.
- i2® iBase User and Designer 8.9.13, or later.

Note: Previous versions of i2® Analyst's Notebook Premium must be uninstalled before you attempt to install a later version. i2® Analyst's Notebook and i2® iBase can be upgraded from the current versions.

Product access management uses a server and client model to monitor application usage. This guide assumes that the server and client are running Microsoft™ Windows™. Implementing product access management involves the creation, deployment, and usage of permits.

Important: If you are upgrading from IBM products with product access management licenses to i2 Group products, you need to request new licenses, see Requesting permits on page 4. You must return any 'borrowed' IBM permits to the server before beginning the upgrade.

The product access management feature is compatible with earlier supported versions of 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 i2® applications.

To upgrade the license manager, double-click `setup.exe` in the `\Product Access Management \Server` directory of the 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 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 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

Permits enable i2® applications 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 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.

i2 Group 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.

Note: PAM enabled i2 Group products require i2 Group PAM licenses, and IBM products require IBM PAM licenses. You cannot use an i2 Group PAM license with an IBM product, and vice versa. If you are upgrading your IBM products to i2 Group products, you must request new PAM licenses by completing a permit request form. To find out more, see Requesting permits on page 4.

To run an i2® application when not connected to the network, a user can borrow a permit from a server. For more information about borrowing permits, see Permits for offline use on page 9.

Design and deployment process

There are a number of processes involved in the design and deployment of product access management.

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

1. Designing the deployment on page 3.
2. Generate lock codes on page 3.
3. Requesting permits on page 4.

4. Install the Sentinel RMS License Manager on page 4.
5. Install permits on page 4.

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 11. 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 1.

A permit is locked to specific server hardware. For more information about permits, see Permits on page 2.

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

Deploying Product Access Management

To make permits available to clients, you must generate lock codes, request permits from i2, 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.

In order for 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 i2, the original information is encrypted and cannot be extracted from the lock code.

On each server that is used in the deployment:

1. Run `LockCodeGenerator.exe`. This application is found in the 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.

Requesting permits

Permits are obtained by completing a permit request form that is sent to i2 Group.

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

1. Complete questions 1 - 7 on the permit request form.
2. In question 8, enter the number of users of each i2®Group product that the permits installed on the server provide access for. If you are requesting licenses for earlier versions of the product, use the form supplied in that distribution.
3. Send the permit request form to `i2PermitRequest@i2group.com`.
4. i2 Group 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 i2® application.

Install the Sentinel RMS License Manager

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

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

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.

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 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 i2® application. For example, the i2.ANB.main feature corresponds to the Analyst's Notebook application. Permits are installed on a server for a feature, and an i2® application requests a permit from a server when it loads.

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

To monitor usage of permits, see Accessing the server log file on page 11.

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 5.

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 i2® products, the following features are used:

i2 Product	Features
Analyst's Notebook	i2.ANB.main
Analyst's Notebook Premium	i2.ANB.main
	i2.ANB.Premium
iBase	i2.iBase.main
	i2.iBaseDesigner.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.

1. Copy the contents of the `\Product Access Management\Utils` directory in the 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 `i2.ANB.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.

Setting up clients

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

Set your server connection options to enable successful connection for each client.

On each client, use the **Settings** tab of the Product Access Console to configure how to connect to servers. You can enter a list of servers that all access management enabled 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.

1. From the **Start** menu, open the Product Access Console by clicking **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 i2® applications

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

You can use `msiexec` to install 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 i2® product:

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

Use the I2LIC_ENABLED property only with packages for Product Access Management enabled 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 `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 "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 "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 "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 "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 "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 **i2 Tools** > **Product Access Console**. For more information, see Setting server connection options on page 7.

Setting server connection options without the Product Access Console

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.

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

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.

Running i2® applications

During startup, an access management enabled 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 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.

Permits for offline use

Permits can be borrowed from the server to allow 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 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 i2® application when not connected to the network, borrow a permit from a server while connected to the network.

To borrow a permit:

1. Click **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**.

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

Borrowing a permit offline

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.

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 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.

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.

1. Click **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**.

The permit is returned to the server.

Accessing 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.

Use Lsusage to view the Sentinel RMS License Server log file. Lsusage is found in the 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 Accessing the server log file on page 11