



System i
Connecting to System i
Application Administration

Version 6 Release 1





System i
Connecting to System i
Application Administration

Version 6 Release 1

Note

Before using this information and the product it supports, read the information in "Notices," on page 23.

This edition applies to version 6, release 1, modification 0 of IBM i5/OS (product number 5761-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

© **Copyright IBM Corporation 1998, 2008.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Application Administration	1
PDF file for Application Administration	1
Application Administration concepts	2
Application registration.	2
Application registration on Local Settings.	2
Application registration on Central Settings	3
System i Navigator plug-ins and Application Administration	3
Access settings for a function.	4
How access to a function is determined	4
Administration system	5
How clients initially discover their administration system	6
Advanced settings in Central Settings	6
How advanced settings are obtained for a user	7
Mandated and suggested values.	7
Management Central and Application Administration	7
When changes take effect	9
Application Administration as a security tool	9
Installing Application Administration.	10
Planning your Application Administration strategy	10
Planning for Application Administration	10
Planning for the administration system and Central Settings	11

Setting up Application Administration	12
Setting up Application Administration for Local Settings.	12
Setting up the administration system for Central Settings.	12
Managing Application Administration	13
Registering applications for Application Administration (Local Settings).	13
Registering applications on the administration system (Central Settings)	13
Working with a function's access setting.	14
Working with user or group access settings.	15
Working with Central Settings	15
Scenarios: Application Administration	17
Scenario: Setting up Application Administration	17
Scenario: Setting up an administration system for Central Settings	20

Appendix. Notices	23
Programming interface information	24
Trademarks	25
Terms and conditions	25

Application Administration

Application Administration is an optionally installable component of System i[®] Navigator. Administrators can use Application Administration to control the functions and applications available to users and groups on a specific system.

This includes controlling the functions available to users that access their system through clients. If you access a system from a Windows client, the operating system user profile, not the Windows user, determines which functions are available.

Application Administration controls access to any application that has a defined administrable function on your system. System i Navigator and IBM[®] i Access for Windows are examples of applications that have defined administrable functions. For example, you can grant or deny access to the printer output function in basic operations, or grant or deny access to the entire basic operations administrable function in System i Navigator.

How does Application Administration work?

Application Administration provides a convenient graphical user interface (GUI) that you can use to control the functions that are available to users and groups. When a user accesses an administrable function, the system reads the user's access setting to determine whether the user is allowed to access that function.

You can also work with many Application Administration functions through the System i Navigator Web interface. See the Web interface online help for more information. For information about the Application Administration functions that are supported on the System i Navigator Web interface, see System i Navigator URL parameters and available Web tasks.

Note: The System i Navigator Web interface of Application Administration does not include cross-system functions that Management Central handles.

What are the Central Settings?

Previously, you were able to simply deny or allow access to a function. Now you can set up an administration system to centrally manage many of the properties used by IBM i Access for Windows clients and work with advanced Application Administration settings (Central Settings). These new settings are equivalent to the IBM i Access for Windows policies.

If you have configured an administration system, you can work with the **Central Settings** on that system. An administration system is the only type of system that contains **Central Settings**. You can use the **Central Settings** on the administration system to manage which applications are available to users and groups. With the **Central Settings**, you can also customize advanced settings for users or groups. These advanced settings allow you to control what environments are available to specific users and groups. Also, the administrator, through the advanced settings, can control password, connection, service, language settings, and specify whether to automatically determine if new plug-ins are available for installation.

PDF file for Application Administration

You can view and print a PDF file of this information.


To view or download the PDF version, select Application Administration (about 200 KB).

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF link in your browser.
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

Application Administration concepts

Before you begin working with Application Administration, you should become familiar with some concepts.

Application registration

Before you can administer applications, you must register them through Application Administration.

When you register an application, Application Administration creates the application's administrable functions and default settings on the system. System administrators can use these settings to manage which users have access to a function.

An **administrable function** is any function that you can grant or deny access to by using Application Administration. Administrable functions are shown in the function column of the Application Administration dialogs. Some administrable functions include: Basic Operations, Work Management, and Configuration and Service.

You can register an application with the Local Settings or the Central Settings.

Related concepts:

“System i Navigator plug-ins and Application Administration” on page 3

If you have additional plug-ins that you want administered through Application Administration, you must register them.

Application registration on Local Settings

The Applications (Local Settings) dialog displays a list of System i Navigator and client applications.

The list includes applications that either have been registered on the IBM i operating system or are installed on the client PC and are available to be registered on the system. The dialog does not display host applications because host applications normally register their administrable function when you install them on the host system. You must install the application on your PC before you can register it on your system. After you register an application, any other PC running Application Administration can administer or remove the application's administrable functions from your system.

Application Administration organizes applications into the following categories for Local Settings:

Table 1. Application Administration categories for Local Settings

Category	Description
System i Navigator	This category includes System i Navigator and any plug-ins. Example: Basic operations.

Table 1. Application Administration categories for Local Settings (continued)

Category	Description
Client Applications	This category includes all other client applications that provide functions on clients that are administered through Application Administration. Example: IBM i Access for Windows.
Host Applications	This category includes all the applications that reside entirely on your systems and that provide functions that are administered through Application Administration. Example: Backup, Recovery, and Media Services for IBM i.

Related tasks:

“Registering applications for Application Administration (Local Settings)” on page 13

You must register an application if you want to use Application Administration to grant or deny users or groups access to specific functions.

Application registration on Central Settings

When the application is first registered (or added), all users and groups are allowed access to the application’s functions by default. You can administer a registered application through Application Administration to control which users have access to an application's functions.

Removing an application from Application Administration removes the application's administrable functions and any access settings that were added using Application Administration. When you remove Application Administration, all users again have access to the application's functions by default. Also, the Advanced Settings for the IBM i Access for Windows application returns to its default settings.

The **Applications (Central Settings)** dialog displays a list of client applications that support Central Settings.

Application Administration allows you to register the following applications on administration systems.

Table 2. Application Administration applications for Central Settings

Application	Description
IBM i Access for Windows	You can grant and deny access to IBM i Access for Windows administrable functions.
Advanced Settings for IBM i Access for Windows	You can specify advanced settings, such as password, connection, service, environment, language, and plug-ins.

Related tasks:

“Registering applications on the administration system (Central Settings)” on page 13

You must register an application if you want to use Application Administration to grant or deny users or groups access to specific functions.

System i Navigator plug-ins and Application Administration

If you have additional plug-ins that you want administered through Application Administration, you must register them.

Application Administration displays the administrable functions of a System i Navigator plug-in in the following places:

- As a read-only value in the System i Navigator hierarchy in order to specify the location of the plug-in's function within the hierarchy.

- In a first-level folder for the plug-in. You can administer the access settings for a plug-in's functions only from this folder.

When administering a plug-in, an administrator can only grant or deny access to its administrable functions. Plug-ins can only be administered through Local Settings in Application Administration. They are not supported in Central Settings.

Related concepts:

“Application registration” on page 2

Before you can administer applications, you must register them through Application Administration.

Access settings for a function

Each administrable function that your system supports has several associated access settings. The access settings determine whether a user is denied or allowed access to the function.

The access settings are:

Default Access

Determines a user's access to a function when the user and its groups are not explicitly allowed or denied access to the function.

All Object Access

Indicates whether a user or group with all object system privilege is allowed access to the function. If selected, and the user or group has all object system privilege, this setting overrides all other access settings.

Customized Access

Indicates whether users or groups are explicitly denied or allowed access to the function.

Related tasks:

“Planning for Application Administration” on page 10

These questions will help you plan which functions will be managed through Application Administration's Local Settings. In addition, you will determine what type of access users and groups will have to those functions.

How access to a function is determined

Application Administration evaluates the access settings of a function to determine whether a user is allowed or denied access to that function.

All functions have a default and an all object access setting. Functions can also have customized access settings, which allow or deny specific users and groups access to that function.

These are the steps Application Administration takes to determine whether a user can access a particular function:

1. If **All Object Access** is selected for a function, and the user has all object system privilege, the user is allowed access to the function. If not, continue to the next step.
2. If the user is either denied or allowed access by the **Customized Access** setting, then the **Customized Access** setting determines the user's access to the function. If not, then continue to the next step.
3. If the user is a member of one or more groups, then go to step 4. If not, go to step 7.
4. If **All Object Access** is selected for a function, and the group has all object system privilege, then the user can access the function. If not, then continue to the next step.
5. If the user is in a group whose **Customized Access** setting is Allowed, then the user is allowed access to the function. If not, then continue with the next group at step 4. After Application Administration processes each group, continue to step 6.
6. If the user is in a group whose **Customized Access** setting is Denied, then the user is denied access to the function. If not, then continue to the next step.

7. The **Default Access** setting determines the user's access to the function.

Administration system

The administration system is a central system that is used to manage many of the properties used by IBM i Access for Windows clients.

A system administrator must use Application Administration to configure a system before it can act as an administration system. Administration system settings are defined on the IBM i Access for Windows **Properties > Administration System** page. When you right-click a system and select Application Administration, you can see the additional choices, **Local Settings** and **Central Settings**, if that system is already defined as an administration system. Typically, a network has only one system acting as an administration system. For an example network, see Figure 1. This administration system is used by IBM i Access for Windows clients as the source of their Central Settings for Application Administration. Although a network can have multiple systems defined as an administration system, the IBM i Access for Windows clients only use a single administration system for their central settings.

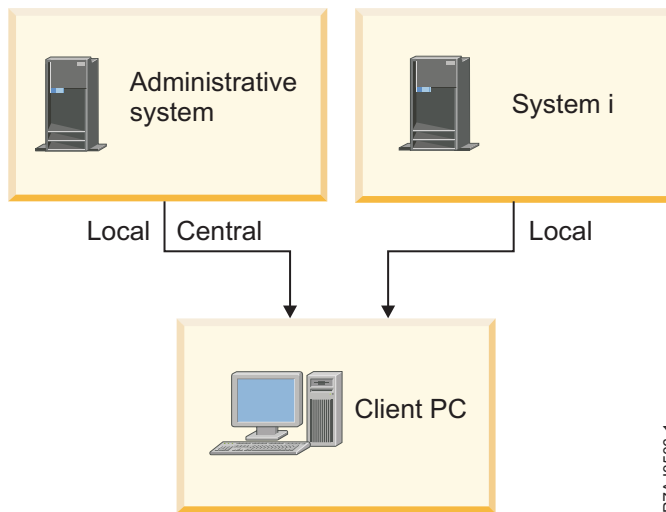


Figure 1. When a Client PC connects to a system, the Local Settings come from the system that you connect to. When you connect to an administration system, the Central Settings are sent to your Client PC from the administration system.

On the administration system, you may select the **Local Settings**. These settings allow or deny access to administrable functions. The administration system's Local Settings only apply to the administration system.

A system administrator can work with the access settings of users and groups using Application Administration on a local system, but the administration system provides additional ways to manage users and groups. An administrator can select **Central Settings** on an administration system to work with advanced settings. These advanced settings control which environments are available to specific users and groups. A system administrator can also control password, connection, service, language settings, and whether to automatically determine if new plug-ins are available for installation.

Note: You must have security administrator (*SECADM) and all object (*ALLOBJ) system privileges to work with advanced settings on an administration system. This differs from other settings in Application Administration, which only require security administrator (*SECADM) system privilege to make changes.

How clients initially discover their administration system

Each IBM i Access for Windows client uses a specific administration system and a user profile on that system to obtain their Central Settings. This administration system and user are referred to as the current administration system and user on the client.

A client's current administration system and user, if any, can be displayed by selecting **Start > Programs > IBM i Access for Windows > IBM i Access for Windows Properties > Administration System**. IBM i Access for Windows clients have three different ways to discover the administration system and the user that will be used as the source of the client's Central Settings:

- An administrator can specify an administration system in a IBM i Access for Windows installation image. The administration system that is specified in the installation image is used as the current administration system unless the client already has a current administration system.
 1. Right-click your system and select **Properties**.
 2. Click **Set Installation Image Administration System**.
 3. Specify the location of the installation image or click **Browse** to locate the installation image.
 4. Select the administration system that you want to specify as the initial administration system for all clients that install using the updated installation image.
 5. Click **OK**.
- Specify the administration system from the IBM i Access for Windows Properties page.
 1. Open **IBM i Access for Windows Properties**.
 2. Select the **Administration System** tab.
 3. If the administration system you want to connect to does not appear in the **Available administration systems and users** list, click **Add** to add an administration system and user to this list.
 4. Select an administration system from the **Available administration systems and users** list and click **Set as current**.
- If the client's current administration system has not been manually specified, the first administration system that the client connects to will be used as that client's current administration system and user.

Advanced settings in Central Settings

Advanced settings are a part of the **Central Settings** in Application Administration and can only be administered from an administration system.

The advanced settings provide the administrator with the ability to control settings more complex than the simple access settings (such as allow or deny access). An administrator can use the advanced settings to define a set of environments and system connections that automatically download to a IBM i Access for Windows client.

These environments and system connections are mandated by the administrator in the advanced settings and cannot be modified by the client. In addition, advanced settings can be used to mandate or suggest that the IBM i Access for Windows client use specific settings for the passwords, connection, service, and language attributes, and to determine automatically if new plug-ins are available for installation.

Notes:

1. Central Settings are not available on operating systems earlier than OS/400® V5R2. IBM i Access for Windows clients earlier than V5R2 cannot use Central Settings.
2. You must have security administrator (*SECADM) and all object (*ALLOBJ) system privileges to work with advanced settings on an administration system. This differs from other settings in Application Administration, which only require security administrator (*SECADM) system privilege to make changes.

How advanced settings are obtained for a user

Application Administration uses the client's current administration system and user to determine the system and user that will be used as the source of the client's Central Settings, including the advanced settings.

If the client does not have a current administration system and user, then application administration will not download any Central Settings, including the advanced settings.

For administration systems, the following steps outline how Application Administration obtains a user's advanced settings:

1. If a user has advanced settings on the administration system, Application Administration uses those settings. Otherwise, it continues to the next step.
2. If a user belongs to a group that has advanced settings on the administration system, Application Administration uses those settings. The first group found with settings is used. The groups are searched by first checking the user profile's group profile and then checking the supplemental groups. If no group settings are found, then Application Administration continues to the next step.
3. If there are default advanced settings on the administration system, Application Administration uses them. Otherwise, there are no advanced settings for the user.

Mandated and suggested values

In Application Administration, a padlock icon next to an advanced setting represents a mandated or suggested state.

An administrator can mandate or suggest the advanced settings.

Mandated state



A locked padlock represents a state of mandated. If a function has a state of mandated, the system administrator has made the value of this function mandatory and unalterable; the system administrator defined the value of this function, and the client user cannot alter or override that value.

Suggested state



An unlocked padlock represents a state of suggested. If a function has a state of suggested, the system administrator has made a suggestion as to what the value of a function should be; the system administrator defined the value of this function, but the client user can alter or override that value.

Example

The administrator indicates that a client user must use Secure Sockets Layer (SSL) when connecting to the system. If the administrator suggests that the client user connect with SSL, the client user can override the suggested value, and connect without using SSL. But, if the administrator mandates that the client user connect with SSL, all existing connections already defined on the client are changed to use SSL. New connections also use SSL, and the client user cannot override this value.

Management Central and Application Administration

You can access Application Administration through Management Central.

To do so using System i Navigator, right-click **Management Central** and select **Application Administration**. This opens the Application Administration main dialog.

The Application Administration dialog, when opened through a system selected under the My Connections container, displays Fixes Inventory and Collection Services as read-only. You must register the functions on the administration system, or they are not displayed. You can administer these functions only by accessing Application Administration through Management Central.

To see how Application Administration works in a network with Management Central, see Figure 2.



Figure 2. When a Client PC connects to a system, the Local Settings come from the system that you connect to. When you connect to an administration system, the Central Settings are sent to your Client PC from the administration system. This network does not change the function of Application Administration or Management Central.

You can define Management Central's central system to be an administration system. Defining the same system as your central system and your administration system does not alter the operation of either the central system or the administration system. For an example network, see Figure 3.



Figure 3. The administration system and the central system can be the same system. It does not change the function of Application Administration or Management Central. When a Client PC connects to a system, the Local Settings come from the system that you connect to. When you connect to an administration system, the Central Settings are sent to your Client PC from the administration system.

When changes take effect

When a change to the Local or Central Settings takes effect on the client depends on what type of change you make.

There are two main types of changes that will occur. You will be changing either the access setting of a user or group (Local Settings) or the Central Settings of the administration system.

Local Settings

Depending on the application, you may not see the changes that you make until:

- The next time the client PC signs on to the system. This is the case for System i Navigator functions.
- The next time you restart the client PC, or 24 hours after you make the change, whichever comes first. This is the case for IBM i Access for Windows functions.

Central Settings

Changes to advanced settings on the administration system depend on the scan frequency that is set on the **Administration System** page of the system properties. The scan frequency ranges from every client session to once every 14 days. System administrators specify this value when they configure a system as an administration system.

Application Administration as a security tool

Do not use Application Administration as a security tool.

Application Administration was designed for customizing the functions available on your client PC. You should not use Application Administration for administering security on your client PC for these reasons:

- Application Administration uses the Windows registry to cache restrictions on the client PC. A skilled user who is restricted from a function by Application Administration could obtain access to the function by editing the registry.
- If multiple interfaces exist to the same resource, restricting a single interface through Application Administration does not restrict the other interfaces to the same resource. For example, you can restrict a user from accessing the database function of System i Navigator through Application Administration. However, the user can still access database files by using other database interfaces, such as Open Database Connectivity (ODBC) or database control language (CL) commands.

Installing Application Administration

You can install Application Administration at the time you install IBM i Access for Windows. If you have already installed IBM i Access for Windows, you can choose Selective Setup from the IBM i Access for Windows folder to install additional components.

To install Application Administration, follow these steps:

1. Install IBM i Access for Windows. See IBM i Access for Windows: Installation and setup for more information. When you get to the Setup wizard, go to step 2.
2. Install Application Administration. To install the Application Administration subcomponent, select the **Custom** installation option when installing IBM i Access for Windows.
 - a. On the **Component Selection** page of the Setup wizard, expand System i Navigator to see the list of subcomponents.
 - b. Select Application Administration and any additional subcomponents that you want to install and continue with **Custom** installation or **Selective Setup**.

Application Administration requires no further configuration for you to start to administer applications.

Planning your Application Administration strategy

In order to optimally use all of the functions available through Application Administration, it is essential that you plan a strategy that is specific to your company.

When planning your strategy, you need to plan for the administration system that contains the Central Settings for Application Administration as well as determining how your applications will be tailored through Application Administration.

Planning for Application Administration

These questions will help you plan which functions will be managed through Application Administration's Local Settings. In addition, you will determine what type of access users and groups will have to those functions.

The first step in the planning process is to plan for Application Administration's Local Settings. The following questions will help you gather the information you need to begin to administer the Local Settings through Application Administration:

1. Which applications do you want to manage with Application Administration?

Note: You can only use Application Administration to administer applications that define administrable functions. For example, System i Navigator includes Basic Operations and Configuration and Service as administrable functions.
2. What type of access do you want users to have to the administrable functions of those applications?

- a. If you want all users to be allowed access to the function, then use the **Default Access** setting for the function. Then, by default, all users will have access to the function.
- b. If you want all users with all object system privilege to have access to the function, use the **All Object Access** setting for that function.

Note: This value allows all users with all object system privilege to have access to this function even if they are explicitly denied access to the function by using the **Customized Access** setting.

- c. Identify groups that require an access setting that differs from the **Default Access** setting. You must specify a **Customized Access** setting for each of these groups.
- d. Identify users who require an access setting that differs from the default access or customized access for the groups to which they belong. Then, you must specify a **Customized Access** setting for each of these users.
- e. Identify users not in a group who require an access setting that differs from the **Default Access** setting. You must specify a **Customized Access** setting for each of these users.

Related tasks:

“Setting up Application Administration for Local Settings” on page 12

These steps outline what actions you must take to administer functions with Application Administration. These steps should be completed based on your answers from Planning for Application Administration.

Related reference:

“Access settings for a function” on page 4

Each administrable function that your system supports has several associated access settings. The access settings determine whether a user is denied or allowed access to the function.

Planning for the administration system and Central Settings

These questions help you plan for the administration system. As a system administrator, you need to plan which systems are administration systems and which users are administered.

The administration system contains Central Settings. The Central Settings apply only to IBM i Access for Windows, so you only need to plan for the administration system if you want to administer the Central Settings supported by IBM i Access for Windows. Answer the following questions to help you gather the information you need to set up the administration system:

1. Which system, if any, do you want to be an administration system?
2. What scan frequency do you want to use? This setting can have an impact on performance if the client updates its Central Settings too often.
 - a. If you want the system to update client settings to match the settings stored on the administration system every time the client user signs on to the client, specify **Every client session**.
 - b. If you want the system to update the client settings to match the settings stored on the administration system after a specific time period, specify the **Number of days**. For example, if you want to update the client settings every day, specify 1 for **Number of days**. Because the Central Settings are not expected to be changed frequently, you might want to set the scan frequency to once per day, or even less, to avoid performance impacts on the client.
3. Which users and groups do you want to administer through Application Administration?
 - a. If you want to administer all users, select **Administer users by default**. Then, by default, all users on the system will be administered by the administration system. If you want to override the **Administer users by default** setting for specific users, continue to step b.
 - b. Select **Customize Administration of Users**.
 - c. Use the **Add** and **Remove** buttons to add or remove users and groups to the Users administered and Users not administered lists.
4. How do you want clients to discover their administration system? See “How clients initially discover their administration system” on page 6 for more information.

Setting up Application Administration

To configure Application Administration, you must configure each system's Local Settings individually. Also, you need to configure the administration system.

The system used to manage the Central Settings is the administration system.

Related reference:

“Scenarios: Application Administration” on page 17

These scenarios show how one can apply Application Administration to their company's strategy. These scenarios explain a particular company's plan and how to execute their plan through Application Administration.

Related information:

Configuring Application Administration

Setting up Application Administration for Local Settings

These steps outline what actions you must take to administer functions with Application Administration. These steps should be completed based on your answers from Planning for Application Administration.

To set up the Local Settings, follow these steps:

1. Register applications for Application Administration on the systems you want to control.
Complete steps 1 through 7 in “Registering applications for Application Administration (Local Settings)” on page 13.
2. Set the **Default Access** setting for the application's functions, if applicable.
3. Set the **All Object Access** setting for the application's functions, if applicable.
4. Use the **Customize** button to change group access settings, if applicable.
5. Use the **Customize** button to change user access settings, if applicable.
6. Click **OK** to close Application Administration.

Related tasks:

“Planning for Application Administration” on page 10

These questions will help you plan which functions will be managed through Application Administration's Local Settings. In addition, you will determine what type of access users and groups will have to those functions.

Setting up the administration system for Central Settings

These steps outline the actions needed to configure a system as an administration system.

1. Right-click the system you want to be an administration system and select **Properties**.
2. Select the **Administration System** tab.
3. Select **administration system**.
4. Complete the fields based on your answers from Planning for the administration system and Central Settings.
5. If you select **Customize Administration of Users**, follow these steps:
 - a. Select a user or group from the Users and Groups list.
 - b. Click **Set as default**, **Add** or **Remove**. You can use the add and remove actions for either the Users administered list or the Users not administered list. Otherwise, you can specify that a user or group be administered by the default setting.
 - c. Repeat the same process for any other users or groups that you want to customize.
 - d. Click **OK** to close the Customize Administration of Users dialog.
6. If you want the installation image to cause an initial administration system to be set up on the client that installs with it, complete the following steps:

- a. Click **Set Installation Image Administration System**.
 - b. Specify the location of the installation image, or click **Browse** to locate the installation image.
 - c. Select the administration system that you want to specify as the initial administration system for all clients that install using the updated installation image.
 - d. Click **OK**.
7. Click **OK** to close the **Properties** page. The system is now an administration system.

Managing Application Administration

With Application Administration, you can specify access settings for a function, user, or group. You can use Central Settings to control additional functions, such as warning users before their passwords expire and specifying which environments users or groups can access.

Registering applications for Application Administration (Local Settings)

You must register an application if you want to use Application Administration to grant or deny users or groups access to specific functions.

By registering an application on a specific system, you make the application available to all users and groups when they sign on to that system. Whether they can actually access an application's administrable functions depends on their access setting.

You might want to register applications with the Local Settings or the Central Settings. If you register an application with just the Local Settings, then you simply grant or deny access to the applications administrable functions. If you register an application with the Central Settings, not only do you grant or deny access to the administrable functions, but also you can work with the Central Settings which include the advanced settings that allow you to administer passwords, connections, services, language attributes, and to automatically determine if new plug-ins are available.

To register an application with the Local Settings, complete the following steps:

1. From System i Navigator, right-click the system on which you want to register applications.
2. Select **Application Administration**.
3. If you are on an administration system, select **Local Settings**. Otherwise, continue to the next step.
4. Click **Applications**.
5. Select the application you want to administer from the function column.
6. Click **Add** to add the application to the list of applications to administer.
7. Click **OK** to close the Applications dialog.
8. Click **OK** to close the Application Administration dialog.

Related tasks:

“Registering applications on the administration system (Central Settings)”

You must register an application if you want to use Application Administration to grant or deny users or groups access to specific functions.

Related reference:

“Application registration on Local Settings” on page 2

The Applications (Local Settings) dialog displays a list of System i Navigator and client applications.

Registering applications on the administration system (Central Settings)

You must register an application if you want to use Application Administration to grant or deny users or groups access to specific functions.

By registering an application on a specific system, you make the application available to all users and groups when they sign on to this specific system. Whether they can actually access an application's administrable functions depends on their access setting.

You might want to register applications with the Local Settings or the Central Settings. If you register an application with just the Local Settings, then you simply grant or deny access to the application's administrable functions. If you register an application with the Central Settings, not only do you grant or deny access to the administrable functions, but also you can work with the Central Settings that include the advanced settings (such as password, environment, language, service, connection, and plug-ins).

You can register the following applications for the Central Settings on an administration system:

IBM i Access for Windows

This application contains the administrable functions displayed when you right-click *an administration system* > **Application Administration** > **Central Settings**. If you register IBM i Access for Windows, you need to complete steps 2 through 6 in "Setting up Application Administration for Local Settings" on page 12.

Advanced Settings for IBM i Access for Windows

This application contains the advanced settings for IBM i Access for Windows. These settings include password, environment, language, service, connection, and whether to automatically determine if new plug-ins are available. These settings are found when you right-click *an administration system* > **Application Administration** > **Central Settings**, and then click **Advanced Settings**.

To register an application with the Central Settings on the administration system, complete the following steps:

1. From System i Navigator, right-click the administration system on which you want to register applications.
2. Select **Application Administration** > **Central Settings**.
3. Click **Applications**.
4. Select the application you want to administer from the list of applications available to administer.
5. Click **Add** to add the application to the list of applications to be administered.
6. Click **OK** to close the Applications dialog.
7. Click **OK** to close the Application Administration dialog.

Related tasks:

"Registering applications for Application Administration (Local Settings)" on page 13

You must register an application if you want to use Application Administration to grant or deny users or groups access to specific functions.

"Working with Central Settings" on page 15

Application Administration Central Settings allow an administrator to control several IBM i Access for Windows functions that previously were managed using IBM i Access for Windows policies.

Related reference:

"Application registration on Central Settings" on page 3

When the application is first registered (or added), all users and groups are allowed access to the application's functions by default. You can administer a registered application through Application Administration to control which users have access to an application's functions.

Working with a function's access setting

You can use Application Administration to view or edit the access settings for a function.

To work with a function's access setting, follow these steps:

1. Right-click the system that contains the function whose access setting you want to change.

2. Select **Application Administration**.
3. If you are on an administration system, select **Local Settings**. Otherwise, continue to the next step.
4. Select an administrable function.
5. Select **Default Access**, if applicable. By selecting this, you allow all users to access the function by default.
6. Select **All Object Access**, if applicable. By selecting this, you allow all users with all object system privilege to access the function.
7. Select **Customize**, if applicable. Use the **Add** and **Remove** buttons on the **Customize Access** dialog to add or remove users or groups in the Access allowed and Access denied lists.
8. Select **Remove Customization**, if applicable. By selecting this, you delete any customized access for the selected function.
9. Click **OK** to close the Application Administration dialog.

Working with user or group access settings

You can use Application Administration to identify which functions a user or group can access. You can also customize access to specific functions for a user or group.

To work with user or group access settings, follow these steps:

1. From System i Navigator, expand **Users and Groups**.
2. Select **All Users, Groups**, or **Users Not in a Group** to display a list of users and groups.
3. Right-click a user or group, and select **Properties**.
4. Click **Capabilities**.
5. Click the **Applications** tab.
6. Use this page to change the access setting for a user or group.
7. Click **OK** twice to close the **Properties** dialog.

If you have questions about how to proceed, the System i Navigator online help provides details about each of the fields on the dialog.

Note: In certain cases, a user may have read-only allowed access. This occurs when a function has all object access and the user has all object system privilege.

Working with Central Settings

Application Administration Central Settings allow an administrator to control several IBM i Access for Windows functions that previously were managed using IBM i Access for Windows policies.

To view a list of the functions and settings that you can control using Application Administration Central Settings, see the IBM i Access for Windows policy list.

Note: IBM i Access for Windows policies can be handled through these Central Settings. However, the following policies are not supported: installation, detailed PC5250 settings, and computer access (Application Administration does not allow you to specify whether a computer (PC) is allowed or denied access to a function).

The following figure shows you what to expect when you select *a system* > **Application Administration** > **Central Settings**. From this dialog, you can work with the Central Settings. This dialog allows you to grant or deny access to specific administrable functions by selecting the check boxes. The items listed are the administrable functions that are available to administer on the Client Applications page.

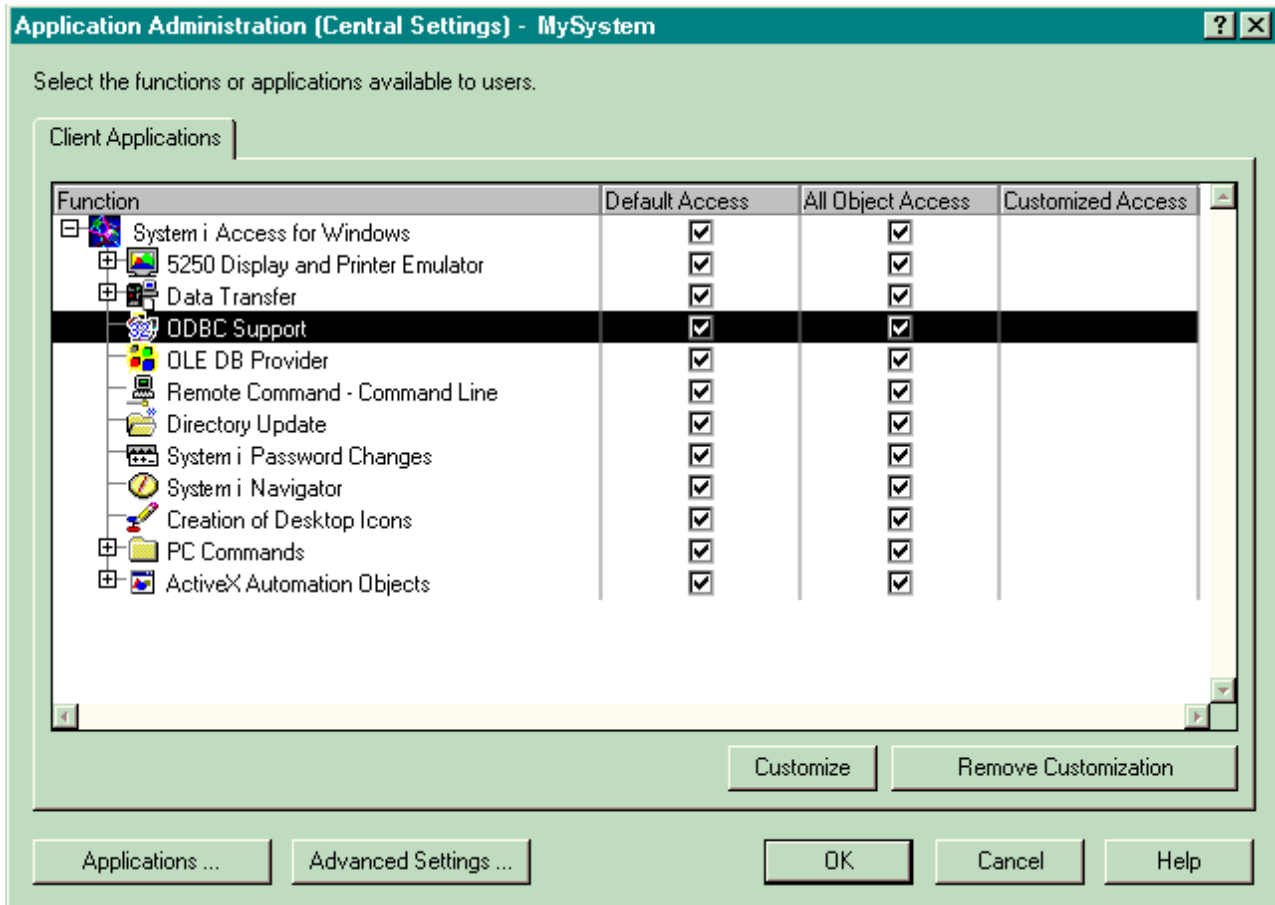


Figure 4. Application Administration Central Settings dialog listing the administrable functions.

You can administer IBM i Access for Windows functions from the Central Settings page, but to work with advanced settings for IBM i Access for Windows, you need to open the Advanced Settings dialog by clicking **Advanced Settings**. Through the administration system, a system administrator can set the advanced settings for a user or group. The administrator can either mandate or suggest these values. The advanced settings are available only if advanced settings for IBM i Access for Windows are registered.

To work with the advanced settings for a user or group, complete the following steps:

1. From System i Navigator, right-click *your administration system*.
2. Select **Application Administration > Central Settings**.
3. Click **Advanced Settings**.
4. Select the user or group you want to work with.
5. Click the **Connections** tabbed page to set sign-on information, performance settings, and whether Secure Sockets layer (SSL) is used when a user or group connects to the system. Click the padlock to change a value between mandated and suggested.
6. Click the **Passwords** tab to specify whether to warn users before their passwords expire. You may also specify whether to allow caching of passwords and whether all incoming remote commands are allowed when caching is disabled. Click the padlock to change a value from mandated to suggested, or vice versa.
7. Click the **Language** tab to specify default or user-defined values for character conversion overrides. You can also specify to enable bidirectional script transformations. Click the padlock to change a value from mandated to suggested, or vice versa.

8. Click the **Service** tab to specify whether to automatically start background service jobs. Click the padlock to change a value from mandated to suggested, or vice versa.
9. Select the **Environments** tab to specify what environments are available to the selected user or group. The environments defined by the system administrator cannot be changed by the user or group.

Note: This information differs from the IBM i Access for Windows policy.

10. Click the **Plug-ins** tabbed page. Use this page to specify whether you want to automatically determine if new plug-ins are available for installation. By default, **Automatically determine if new plug-ins are available for install** is selected. When this box is selected, the IBM i operating system scans clients for their plug-ins when they first connect to it. If the system has additional plug-ins for the client, it prompts the user to install them. This setting can be turned off by clearing the **Automatically determine if new plug-ins are available for install** box.
11. Click **OK** to close the Advanced Settings dialog.
12. Click **OK** to close the Application Administration dialog.

Related tasks:

“Registering applications on the administration system (Central Settings)” on page 13

You must register an application if you want to use Application Administration to grant or deny users or groups access to specific functions.

Scenarios: Application Administration

These scenarios show how one can apply Application Administration to their company's strategy. These scenarios explain a particular company's plan and how to execute their plan through Application Administration.

Related concepts:

“Setting up Application Administration” on page 12

To configure Application Administration, you must configure each system's Local Settings individually. Also, you need to configure the administration system.

Scenario: Setting up Application Administration

This scenario describes how to plan and configure a system to be administered through Application Administration. It demonstrates how you can control access to applications by limiting users to applications and functions that are specific to their job duties.

Suppose that your company has a system (System001) in a network that runs the following client applications:

Manufacturing application

A client interface with these administrable functions:

- Inventory Management
- Order Fulfillment

Finance application

A client interface with these administrable functions:

- Accounts Receivable
- Budgeting

Users access the system by using IBM i Access for Windows and System i Navigator. You must determine which applications you want to administer through Application Administration and evaluate what type of access users require for each function.

Step 1: Planning your Application Administration strategy

Which applications do you want to administer?

System001 has two distinct groups of users: users of the Manufacturing application, and users of the Finance application. The manufacturing users should not have access to the Finance application, and the finance users should not have access to the Manufacturing application. In addition, each group has different access settings to the various System i Navigator functions. Because of this, you need to register the Manufacturing application and the Finance application on System001. IBM i Access for Windows and its administrable functions (System i Navigator) are automatically registered when you install Application Administration, so you do not need to register System i Navigator.

What type of access do you want users to have to the administrable functions of those applications?

All users that use the Manufacturing application belong to a user group that is called MFGUSER. All manufacturing team leaders also belong to a user group that is called MFGLEAD. All users that use the Finance application belong to a user group that is called FINANCE. Now that you have determined the user groups, you can give the users of the applications on System001 access to the following applications:

Manufacturing application

Inventory Management

Only Judy, Natasha, Jose, and Alex require access to this function.

Order Fulfillment

All manufacturing team leaders require access to this function, except Alex.

Finance application

Accounts Receivable

All members of FINANCE require access to this function.

Budgeting

All members of FINANCE require access to this function.

System i Navigator

- All manufacturing users require access to basic operations.
- All finance users require access to basic operations, database, and file systems.
- All system administrators require access to all System i Navigator functions.

Note: The administrators on this system do not require access to the Manufacturing application or the Finance application. All administrators have all object system privilege.

Step 2: Setting up your Application Administration strategy

Given the information you compiled in planning your Application Administration strategy, configure the access settings for each application's administrable function as follows:

Manufacturing application

Inventory Management

1. From the **Application Administration** dialog, go to the **Client Applications** page.
2. Expand **Manufacturing application**.
3. For Inventory Management, deselect **Default Access**.
4. Click **Customize**. This opens the **Customize Access** dialog.
5. In the **Access** field, deselect **All object system privilege**.
6. Expand **All Users** in the **Users and Groups** list box.
7. Select Judy, Natasha, Jose, and Alex from the list of all users and click **Add** to add them to the **Access Allowed** list.

8. Click **OK** to save the access settings.
9. For Order Fulfillment, deselect **Default Access**.
10. Click **Customize**. This opens the **Customize Access** dialog.
11. In the **Access** field, deselect **Users with all object system privilege**.
12. Expand **All Users** in the **Users and Groups** list box.
13. Select Alex from the list of all users and click **Add** to add him to the **Access Denied** list.
14. Expand **Groups** in the **Users and Groups** list box.
15. Select MFGLEAD from the list of groups and click **Add** to add the group to the **Access Allowed** list.
16. Click **OK** to save the access settings.

Finance application

All functions

1. From the **Application Administration** dialog, go to the **Client Applications** page.
2. Expand **Finance application**.
3. For Accounts Receivable, deselect **Default Access**.
4. Click **Customize**. This opens the **Customize Access** dialog.
5. In the **Access** field, deselect **Users with all object system privilege**.
6. Expand **Groups** in the **Users and Groups** list box.
7. Select FINANCE from the list of groups and click **Add** to add the group to the **Access Allowed** list.
8. Click **OK** to save the access settings.
9. Repeat these steps for Budgeting.

System i Navigator

Basic Operations

1. From the **Application Administration** dialog, go to the **System i Navigator** page.
2. For Basic Operations, select **Default Access** and **All Object Access**.
3. Click **OK** to save the access settings.

Database

1. From the **Application Administration** dialog, go to the **System i Navigator** page.
2. For Database, deselect **Default Access**.
3. Click **Customize**. This opens the **Customize Access** dialog.
4. In the **Access** field, select **Users with all object system privilege**.
5. Expand **Groups** in the **Users and Groups** list box.
6. Select FINANCE from the list of groups and click **Add** to add the group to the **Access Allowed** list.
7. Click **OK** to save the access settings.

File Systems

1. From the **Application Administration** dialog, go to the **System i Navigator** page.
2. For File Systems, deselect **Default Access**.
3. Click **Customize**. This opens the **Customize Access** dialog.
4. In the **Access** field, select **Users with all object system privilege**.
5. Expand **Groups** in the **Users and Groups** list box.
6. Select FINANCE from the list of groups and click **Add** to add the group to the **Access Allowed** list.
7. Click **OK** to save the access settings.

All other System i Navigator functions

1. From the **Application Administration** dialog, go to the **System i Navigator** page.
2. For each function, deselect **Default Access** and select **All Object Access**.
3. Click **OK** to save the access settings.

Now, you have used the Local Settings within Application Administration to set up an environment that restricts user access to specific functions.

Related reference:

“Scenario: Setting up an administration system for Central Settings”

This scenario is based on the same setup as the scenario about setting up Application Administration, but this scenario also demonstrates how to define the system as an administration system, which contains Central Settings.

Scenario: Setting up an administration system for Central Settings

This scenario is based on the same setup as the scenario about setting up Application Administration, but this scenario also demonstrates how to define the system as an administration system, which contains Central Settings.

In the setting up Application Administration scenario, you set up Application Administration on a system to administer who has access to specific manufacture and finance applications. By defining the system as an administration system, you can administer Central Settings. These settings allow you to use the advanced settings to control sign-on, connections, language, environments, service, password information, and whether to determine automatically if new plug-ins are available. In addition, you are also able to control access to several additional functions of IBM i Access for Windows.

Step 1: Planning your administration system strategy

Which users do you want to administer?

Because all users have specific access settings for various functions, you need to administer all users to enforce the access settings. Otherwise, all users would have access to all functions.

Do you want all users who install applications by using the modified installation image to use a specified administration system?

The only system available to the manufacturing and finance people is System001. This system contains every user's advanced settings, so when users install applications, you want them to automatically use System001 as their administration system. Because this is the only administration system in their environment, specify System001 as the installation image administration system.

How often do you want to validate the client-side cache to ensure that the client's settings match the settings stored on the administration system?

The Central Settings will not change often after they are initially set up, but any changes should be distributed to all IBM i Access for Windows clients in your network within a week. Because of this, you should set the scan frequency to **Once every seven days**.

Which IBM i Access for Windows applications that are managed through Central Settings should be available to users and groups?

You want all centrally managed applications available to all users and groups except the Remote Command-Command Line administrable function.

Which advanced settings should be mandated versus suggested?

You want to make sure all users are signing on to the system using their default user ID (prompting as needed) and that a warning message is sent to them before their password expires. Therefore, sign on information and password expire warning will be mandated. This will ensure that the user does not change these two settings. All other advanced settings will be in a suggested state so the system administrator can suggest a value but the user will still be able to modify it.

Step 2: Setting up your administration system

Define the administration system.

These steps outline what actions you must take to actually administer functions on an administration system:

1. Right-click **System001** and select **Properties**.
2. Select the **Administration System** page.
3. Select **Administration System**.
4. Select **Number of days** for the scan frequency and specify 7 days.
5. Select **Administer users by default**.
6. Click **Set Installation Image Administration System**.
7. Specify the location of the installation image or click **Browse** to locate the installation image.
8. Specify **System001** for the administration system.
9. Click **OK** to close the **Set Installation Image Administration System** dialog.
10. Click **OK** to close the **Properties** dialog.

Set the Central Settings.

These steps outline what actions you must take to set the advanced settings for the administration system:

1. Right-click **System001**.
2. Select **Application Administration > Central Settings**.
3. Deselect **Remote Command-Command Line Default Access**.
4. Deselect **Remote Command-Command Line All Object Access**.
5. Click **Advanced Settings**.
6. Select the **Passwords** page.
7. Select **Warn users before server password expires**.
8. Specify 10 days so users are sent warning messages 10 days prior to expiration.
9. Click the padlock in front of this value to mandate it. (The padlock should be closed.)
10. Select the **Connections** page.
11. Select **Use default user ID, prompt as needed**.
12. Click the padlock to mandate this value. (The padlock should be closed.)
13. Leave all other advanced settings as suggested values. The padlocks for these setting should be open.
14. Click **OK** to close the **Advanced Settings** dialog.
15. Click **OK** to close the **Application Administration** dialog.

Now, you have set up an administration system that contains the Central Settings. Within the Central Settings, you are able to adapt the advanced settings to meet your company's needs.

Related reference:

“Scenario: Setting up Application Administration” on page 17

This scenario describes how to plan and configure a system to be administered through Application Administration. It demonstrates how you can control access to applications by limiting users to applications and functions that are specific to their job duties.

Appendix. 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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

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 Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

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, IBM License Agreement for Machine Code, 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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming interface information

This Application Administration publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

i5/OS
IBM
IBM (logo)
OS/400
System i

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Printed in USA