

IBM

@server

iSeries

iSeries Navigator

Application Administration





@server

iSeries

iSeries Navigator

Application Administration

Contents

Part 1. Application Administration	1
Chapter 1. What's new for V5R2.	3
Chapter 2. Print this topic	5
Chapter 3. Application Administration concepts	7
Application registration	7
Register Local Settings	8
Register Central Settings	8
iSeries Navigator plug-ins and Application Administration	9
Access settings for a function	9
How access to a function is determined.	9
Administration system	10
How clients initially discover their administration system	11
Central Settings	11
How advanced settings are obtained for a user	12
Mandate and suggest values	12
Management Central and Application Administration.	13
When changes take effect	14
Application Administration as a security tool.	15
Chapter 4. Install Application Administration	17
Chapter 5. Plan your Application Administration strategy	19
Plan for Application Administration	19
Plan for the administration system and Central Settings	20
Chapter 6. Set up Application Administration	21
Set up Application Administration for Local Settings	21
Set up the administration system for Central Settings	21
Chapter 7. Manage Application Administration.	23
Register applications for Application Administration (Local Settings)	23
Register applications on the administration system (Central Settings)	23
Work with a function's access setting	24
Work with user or group access settings	25
Work with Central Settings	25
Chapter 8. Scenarios: Application Administration	29
Scenario 1: Set up Application Administration	29
Scenario 2: Set up an administration system for Central Settings	31

Part 1. Application Administration

Application Administration is an optionally-installable component of iSeries Navigator. Application Administration allows administrators to control the functions or applications available to users and groups on a specific server. This includes controlling the functions available to users that access their server through clients. If you access a server from a Windows client, the OS/400 user profile and not the Windows user determines which functions are available.

Application Administration controls access to any application that has a defined administrable function on your server. iSeries Navigator and iSeries 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 iSeries Navigator.

To use Application Administration, you must select the Application Administration component when you install iSeries Navigator. For installation instructions, see Install Application Administration.

How does Application Administration work?

Application Administration provides a convenient graphical user interface (GUI) that allows you 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 or not the user is allowed to access that function.

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 iSeries Access for Windows clients and work with advanced Application Administration settings (Central Settings). These new settings are equivalent to the Client Access Express 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 can control password, connection, service, and language settings through the advanced settings.

To learn more about Application Administration, refer to the following topics:

- Application Administration concepts

In order to fully benefit from Application Administration, you should become familiar with these concepts.

- Install Application Administration

Application Administration is an optionally-installable component of iSeries Navigator. This topic explains how to install the Application Administration component.

- Plan your Application Administration strategy

This topic provides you with information pertaining to your environment. You will answer a series of questions to help you plan your Application Administration strategy. Then, you will use your answers when configuring Application Administration.

- Configure Application Administration

In order to use Application Administration, you must configure iSeries to use Application Administration. This topic explains how to set up Application Administration according to your environment.

Manage Application Administration

As an administrator, you can perform many tasks to help you manage Application Administration. Select this topic to learn how to work with Application Administration.

Application Administration scenarios

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.

Chapter 1. What's new for V5R2

Application Administration shows exciting enhancements for V5R2. Not only can you simply allow or deny access to administrable functions (Local Settings) but also you may define an administration system that controls Central Settings.

- **Administration system**

You may configure an iSeries as an administration system. The administration system is a central system that is used to manage many of the properties used by iSeries Access for Windows clients. These properties that are managed on the administration system are called **Central Settings**.

- **Local Settings**

Prior to V5R2, each iSeries maintained its own set of Application Administration settings and these settings only controlled activity that occurred on that specific iSeries. Since each iSeries maintains its own set of settings, these settings are now referred to as **Local Settings**.



- **Central Settings**

The Central Settings allow an administrator to allow or deny a user or group access to a function or application from a central iSeries, but also they support Advanced Settings. Advanced Settings allow an administrator to customize many of the properties used by an iSeries Access for Windows client, such as defining a set of environments to be used by a client, and customizing many of the connection, service, language, and password settings used by the clients.

Central Settings allow administrators to manage most of the settings that previously could only be managed using Client Access Express Policies. Central settings can only be supported by V5R2 or later iSeries servers and V5R2 or later iSeries Access for Windows clients.

How to see what is new or changed

To help you see where technical changes have been made, this information uses:

- The  image to mark where new or changed information begins.
- The  image to mark where new or changed information ends.

To find other information about what's new or changed this release, see the Memo to Users  .

Chapter 2. Print this topic


To view or download the PDF version, select Application Administration (about 200 KB or 35 pages).

Saving PDF files

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

1. Right-click the PDF in your browser (right-click the link above).
2. Click **Save Target As...**
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

Downloading Adobe Acrobat Reader

If you need Adobe Acrobat Reader to view or print these PDFs, you can download a copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html)  .

Chapter 3. Application Administration concepts

» Before you begin working with Application Administration, you should become familiar with these concepts:

“Application registration”

Describes what applications can be administered through Application Administration.

“iSeries Navigator plug-ins and Application Administration” on page 9

Describes how plug-ins work with Application Administration.

“Access settings for a function” on page 9

Describes the different types of access settings that may be specified for a function and how Application Administration determines whether or not a user has access to a function.

“Administration system” on page 10

Describes the administration system and how Application Administration obtains the advanced settings for a user or group.

“Central Settings” on page 11

Describes how the Central Settings provide the administrator with the ability to control more complex settings that can be administered only from an administration system.

“Management Central and Application Administration” on page 13

Describes how you can use Application Administration through Management Central.

“When changes take effect” on page 14

Describes when changes take effect.

“Application Administration as a security tool” on page 15

Explains why **not** to use Application Administration as a security tool.



Application registration



Before you can administer applications, they must be registered through Application Administration. When you register an application, Application Administration creates the application’s administrable functions and default settings on the server. This allows system administrators to manage which users have access to the 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 may register an application for the Local Settings or the Central Settings. For more information, see the following topics.

“Register Local Settings” on page 8

Describes how to register applications for the Local Settings.

“Register Central Settings” on page 8

Describes how to register applications for the Central Settings.



Register Local Settings

➤ The **Applications (Local Settings)** dialog displays a list of iSeries Navigator and Client applications. The list includes applications that either have been registered on the iSeries or are installed on the client PC and are available to be registered on the iSeries. 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 server. Once you register an application, any other PC running Application Administration can administer or remove the applications administrable functions from your server.

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

Table 1. Application Administration Categories for Local Settings

Category	Description
OS/400 iSeries Navigator	Includes iSeries Navigator and any plug-ins. Example: Basic Operations.
Client Applications	Includes all other client applications that provide functions on clients that are administered through Application Administration. Example: iSeries Access for Windows.
Host Applications	Includes all applications that reside entirely on your servers and provide functions that are administered through Application Administration. Example: Backup Recovery and Media Services for iSeries.

To register an application with the Local Settings, see “Register applications for Application Administration (Local Settings)” on page 23. ⏪

Register Central Settings

➤ The **Applications (Central Settings)** dialog displays a list of client applications that support Central Settings. The two available applications are iSeries Access for Windows and Advanced Settings for iSeries Access for Windows

When the application is first registered (or added), all users and groups are allowed access to the application’s functions by default. Once you register an application, you can administer it through Application Administration. Then, all users are allowed access to the application’s functions by default. 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 iSeries Access for Windows application returns to its default settings.

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

Table 2. Application Administration applications for Central Settings

Application	Description
iSeries Access for Windows	Allows you to grant and deny access to iSeries Access for Windows administrable functions.
Advanced Settings for iSeries Access for Windows	Allows you to specify the advanced settings such as password, connection, service, environment and language.

To register an application with the Central Settings, see “Register applications on the administration system (Central Settings)” on page 23. ⏪

iSeries 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 an iSeries Navigator plug-in in two places:

- As a read-only value in the iSeries 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.

Access settings for a function

Each administrable function that your server 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.

To find more information about how Application Administration determines whether or not a user has access to a function, see "How access to a function is determined".

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 may 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 server that is used to manage many of the properties used by iSeries Access for Windows clients. A system administrator must use Application Administration to configure an iSeries server before it can act as an administration system. If you right-click a system and select Application Administration, you will see the additional choices **Local Settings** or **Central Settings** if that system is already defined as an administration system. Typically, a network will have only one iSeries server acting as an administration system. For an example network, see Figure 1. This administration system will be used by iSeries Access for Windows clients as the source of their Central Settings for Application Administration. Although a network can have multiple iSeries servers defined as an administration system, the iSeries Access for Windows clients will 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 server, 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 what environments are available to specific users and groups, and a system administrator can also control password, connection, service, and language settings.

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.

For more information, see “How clients initially discover their administration system”. <<

How clients initially discover their administration system

>> Each iSeries 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 is 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 iSeries Access for Windows->iSeries Access for Windows Properties-> Administration System. iSeries Access for Windows clients have three different ways to discover the administration system and user that will be used as the source of the client’s Central Settings:

- An administrator can specify an administration system in an iSeries Access for Windows install image. Any client that installs using this image will use the administration system defined in the image as their current administration system as long as the client does not already have 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 iSeries Access for Windows Properties.
 1. Open **iSeries 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.



Central Settings

>> Advanced settings are a part of the **Central Settings** in Application Administration and can only be administered from an administration system. They are available on iSeries systems running OS/400 V5R2 or later, and are only used by V5R2 or later iSeries Access for Windows clients. The advanced settings provide the administrator with the ability to control more complex settings than the simple access settings (allow or deny access) that are also supported in Application Administration. An administrator can use advanced settings to define a set of environments and server connections that will automatically download to an iSeries Access for Windows client. The environments and server connections can be defined as defaults (or suggested values), in which case a client can modify them, or as mandated values, in which case the client cannot modify them. In addition, advanced settings can be used to mandate or suggest clients to use specific settings for many of the password, connection, service, and language attributes used by iSeries Access for Windows clients.

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.

For more information about advanced settings, see the following topics:

- “How advanced settings are obtained for a user”
Describes how Application Administration determines a user’s password, environment, connection, service, and language settings.
- “Mandate and suggest values”
Describes how a system administrator can mandate and suggest advanced settings.



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.



Mandate and suggest 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.



Mandate

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.



Suggest

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.

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

Management Central and Application Administration

>> You can also access Application Administration through Management Central. To do so using iSeries Navigator, right-click **Management Central** and select **Application Administration**. This opens the Application Administration main dialog.

If you have Management Central installed and you have registered the functions on the Management Central system, the Application Administration dialog displays Fixes Inventory and Collection Services as read-only values when it is opened through a server.

The Application Administration dialog, when opened through a server, 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 may also define Management Central's central system to be an administration system. Defining the same server 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 server. This is the case for iSeries 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 iSeries 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 server properties. The scan frequency ranges from every client session to once every 14 days. This value is specified by the system administrator when they configure an iSeries 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 OS/400 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 iSeries 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.

Chapter 4. Install Application Administration

➤ iSeries Navigator is a component of iSeries Access for Windows that contains many subcomponents, including Application Administration. You can install Application Administration at the time you install iSeries Access for Windows. If you have already installed iSeries Access for Windows, you can choose Selective Setup from the iSeries Access for Windows folder to install additional components.

To install Application Administration, follow these steps:

Step 1: Install iSeries Access for Windows

See Getting started with iSeries Access for Windows to install iSeries Access. When you get to the Setup Wizard, go to Step 2.

Step 2: Install Application Administration

To install the Application Administration subcomponent, select the **Custom** installation option when installing iSeries Access for Windows.

1. On the **Component Selection** page of the Setup wizard, expand iSeries Navigator to see the list of subcomponents.
2. 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. <<

Chapter 5. Plan 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.

The following sets of questions will assist you in developing an Application Administration plan for your environment.

“Plan 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.

“Plan for the administration system and Central Settings” on page 20

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



Plan for Application Administration

» 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, iSeries 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.

If you have questions about how Application Administration determines whether a user is denied or allowed access to a function, see “Access settings for a function” on page 9. <<

Plan for the administration system and Central Settings

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

1. Which server, 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 server 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 server 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**. Since the Central Settings are not expected to be changed frequently, IBM recommends that the scan frequency be set to once per day, or even less frequently, in order 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 11, for more information.



Chapter 6. Set 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. See the following topics for more information:

“Set up Application Administration for Local Settings”

Describes the necessary steps to configure a function's access settings through Application Administration.

“Set up the administration system for Central Settings”

Describes how to define a system as an administration system.

To see an example of how you might use Application Administration to administer applications on your server, see Chapter 8, “Scenarios: Application Administration” on page 29. <<

Set up Application Administration for Local Settings

» These steps outline what actions you must take to actually administer functions with Application Administration. These steps should be completed based on your answers from “Plan for Application Administration” on page 19. The following steps set up the Local Settings:

1. “Register applications for Application Administration (Local Settings)” on page 23 on the servers you want to control. Complete steps 1 thru 7.
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.



Set up the administration system for Central Settings

» These steps outline the actions needed to configure an iSeries 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 Plan for the administration system and Central Settings.
5. If you select **Customize Administration of Users . . .**, complete the following 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 install 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.



Chapter 7. Manage Application Administration

» You may use a variety of tools to manage application administration. To manage application administration, you may want to become familiar with these topics:

“Register applications for Application Administration (Local Settings)”

Describes how to register applications so the administrable functions are available to Application Administration.

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

Describes how to register client applications on the administration system.

“Work with a function’s access setting” on page 24

Describes how to view or edit a function’s access setting.

“Work with user or group access settings” on page 25

Shows which functions a user or group may access and how to customize those settings.

“Work with Central Settings” on page 25

Describes how to view or edit Central Settings.



Register 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 will make the application available to all users and groups when they sign on to this specific system. Whether or not they can actually access an application’s administrable functions depends on their access setting.

You may 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 (password, environment, language, service and connection).

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

1. In iSeries Navigator, right-click the server you want to register applications on.
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.



Register 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 will make the application available to all users and groups when they sign on to this specific system. Whether or not they can actually access an application’s administrable functions depends on their access setting.

You may 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 (password, environment, language, service and connection). See “Work with Central Settings” on page 25 for a description of the functions controlled by each of these applications listed below.

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

- **iSeries Access for Windows**

This application contains the administrable functions displayed when you right-click an administration system → **Application Administration** → **Central Settings**. If you register iSeries Access for Windows, you need to complete steps 2 through 6 in “Set up Application Administration for Local Settings” on page 21.

- **Advanced Settings for iSeries Access for Windows**

This application contains the advanced settings for iSeries Access for Windows. These settings include password, environment, language, service and connection. These settings are found when you right-click an administration system → **Application Administration** → **Central Settings**. Then, click the **Advanced Settings. . .** button.

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

1. In iSeries Navigator, right-click the administration system that you want to register applications on.
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.



Work with a function’s access setting

» To view or edit the access settings for a function, complete the following 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.



Work with user or group access settings

You can use Application Administration to identify which functions a user or group may access. You can also customize access for a user or group to specific functions. To do this, follow these steps:

1. In iSeries 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 iSeries 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.

Work with Central Settings

➤ Application Administration Central Settings allow an administrator to control several iSeries Access for Windows functions that previously were managed using Client Access Express policies. To view a list of the functions and settings that you can control using Application Administration Central Settings, see the iSeries Access for Windows policy list.

Note: iSeries 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 or not a computer (PC) is allowed or denied access to a function).

The following figure shows you what to expect when you select an iSeries 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 checkboxes. The items listed are the administrable functions that are available to administer within the **Client Applications** tab.

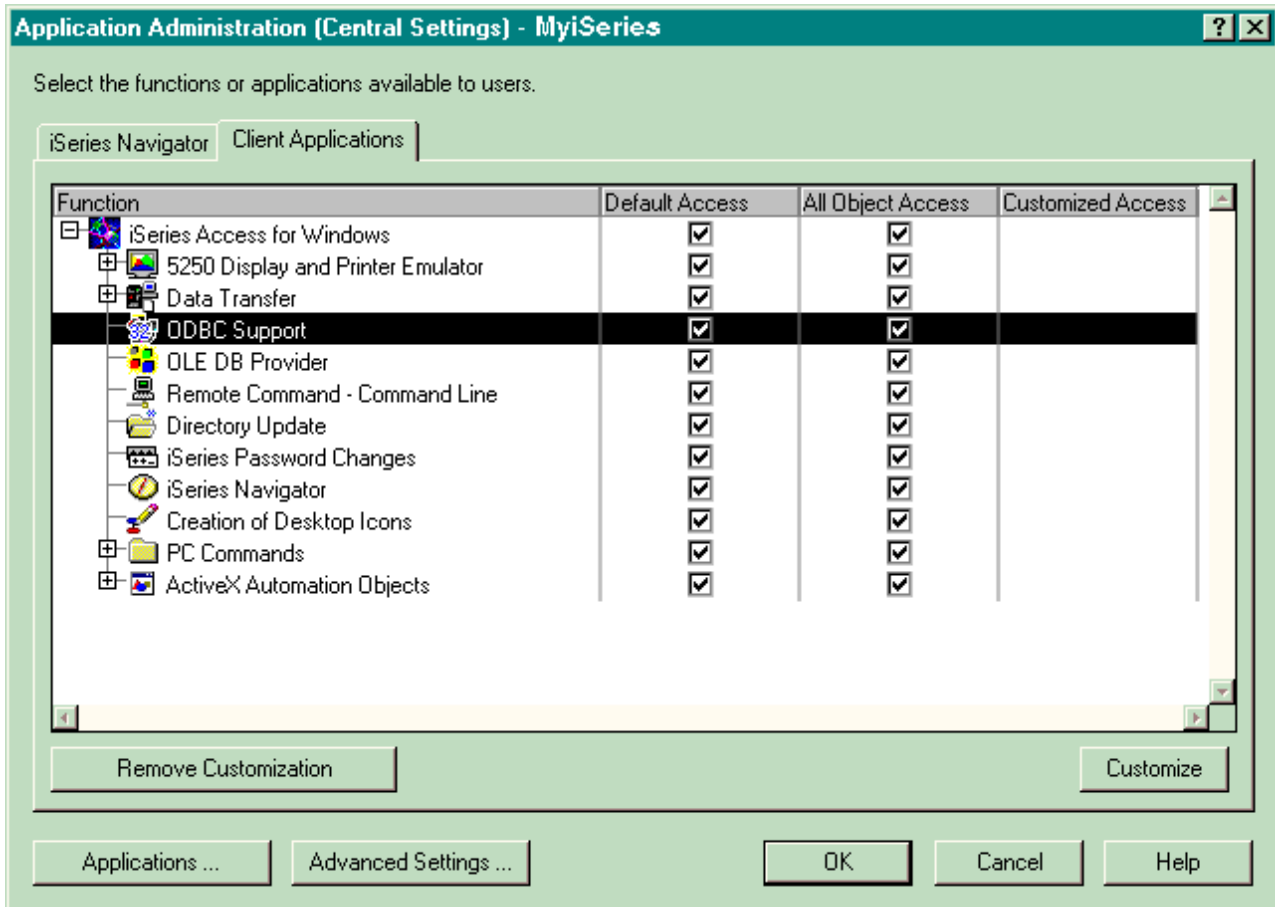


Figure 4. Application Administration Central Settings dialog listing the administrable functions.

You can administer iSeries Access for Windows functions from the Central Settings page, but in order to work with Advanced Settings for iSeries Access for Windows, you need to open the advanced settings dialog by clicking on the **Advanced Settings. . .** button. 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 iSeries Access for Windows is registered.

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

1. In iSeries 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** tab to set sign on information, performance settings and whether or not Secure Sockets layer (SSL) is used when connecting to the server. Click the padlock to change a value from mandated to suggested, or vice versa.
6. Click the **Passwords** tab to specify whether or not to warn users before their passwords expire. You may also specify whether or not to allow caching of OS/400 passwords and whether or not 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 or not to automatically start background service jobs. Click the padlock to change a value from mandated to suggested, or vice versa.
9. Click the **Environments** tab to specify what environments are available to the selected user or group. You may also customize the environment by allowing the user or group to change the environments available to them. Otherwise, the system administrator can select an environment for users or groups and not allow them to change the environment that the system administrator defines for them. Click the mandate or suggest buttons to specify whether users are allowed to change values.

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

10. Click **OK** to close the Advanced Settings dialog.
11. Click **OK** to close the Application Administration dialog.



Chapter 8. Scenarios: Application Administration

» The following scenarios show you how to use Application Administration to administer client applications.

“Scenario 1: Set up Application Administration”

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.

“Scenario 2: Set up an administration system for Central Settings” on page 31

This scenario is based on the same setup as scenario 1, but it also demonstrates how to define the system as an administration system, which contains Central Settings.



Scenario 1: Set up Application Administration

» Suppose that your company has a server (Server001) in a network that runs the following client applications:

Manufacturing application, which has a client interface with these administrable functions:

- Inventory Management
- Order Fulfillment

Finance application, which has a client interface with these administrable functions:

- Accounts Receivable
- Budgeting

Users access the server by using iSeries Access for Windows and iSeries Navigator. You must determine which applications you want to administer through Application Administration. Then you must evaluate what type of access your users require for each function.

Step 1: Plan your Application Administration strategy

Which applications to administer?

Server001 has two, and only 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 Finance users should not have access to the Manufacturing application. In addition, each group has different access settings to the various iSeries Navigator functions. Because of this, you need to register iSeries Navigator, the Manufacturing application, and the Finance application on Server001. iSeries Access for Windows and its administrable functions (iSeries Navigator) are automatically registered when you install Application Administration so you do not need to register iSeries 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 Server001 access to the following:

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.

iSeries 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 iSeries Navigator functions.

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

Step 2: Set 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.

iSeries Navigator

Basic Operations

1. From the **Application Administration** dialog, go to the **iSeries 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 **iSeries 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 **iSeries 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 iSeries Navigator functions

1. From the **Application Administration** dialog, go to the **iSeries 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. If you want to set up an administration system for Central Settings, continue to scenario 2 which explains how to use the Central Settings in your Application Administration strategy. <<

Scenario 2: Set up an administration system for Central Settings

>> In scenario 1, 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 that allow you to control sign on, connections, language, environments, service, and password information. In addition, you will also be able to control access to several additional functions of iSeries Access for Windows.

Step 1: Plan your administration system strategy

Which users do you want to administer?

Since all users have specific access settings for various functions, you need to administer all users so the access settings are enforced. Otherwise, all users would have access to all functions.

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

The only server available to the manufacturing and finance people is Server001. This server contains every user's advanced settings, so when users install, you want them to automatically

use Server001 as their administration system. Since this is the only administration system in their environment, you will specify Server001 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 iSeries 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 iSeries 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: Set 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 **Server001** 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 **Server001** 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 **Server001**.
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 were able to adapt the advanced settings to meet your company's needs. <<



Printed in U.S.A.