IBM @ server *iSeries*

iSeries Operations Navigator: User and Security Administration

Greg Hintermeister

IBM Rochester, MN USA

IBM @server. For the next generation of e-business.

Contents

IBM @ server *iSeries*

- Operations Navigator
  - Basics / Installation
- Overview of User and Group Management
  - What's new this release
  - Working with Users and Groups directly on individual systems vs. on one or more systems through Management Central
- Managing Users and Groups on Individual Systems
- Managing Users and Groups Across Multiple Systems
  - New User / New Group
  - Edit Users / Edit Groups
  - Send User(s) or Group(s) to other systems
  - Delete User(s) or Group(s)
  - Users and Groups Inventory
- Managing Resource Security
  - Work with object permissions
  - Manage authorization lists
- Application Administration
  - Restrict access to Operations Navigator, iSeries applications, and client applications

IBM @server. For the next generation of e-business.

Contents (continued...)

- Managing System Values
  - Updating single systems
  - Compare and Update across multiple systems
- Security Wizard
  - Understand and change your iSeries security related settings
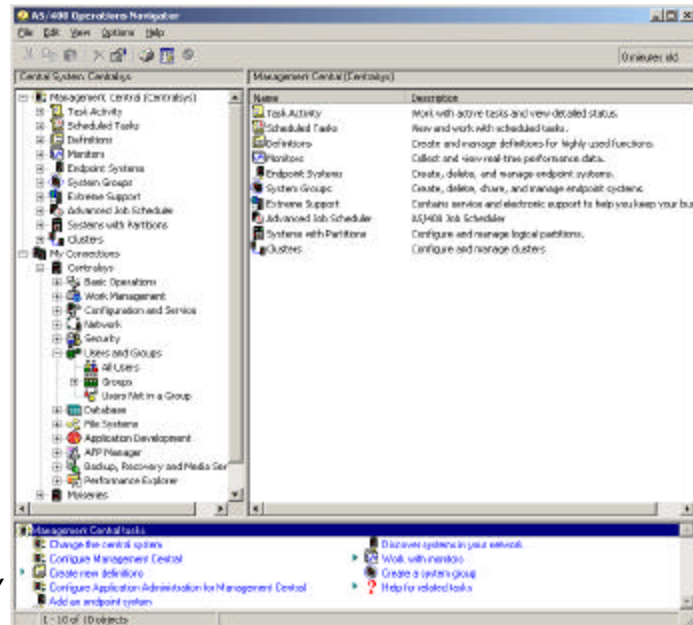- Reference Materials

IBM @server. For the next generation of e-business.

Operations Navigator: Our Goals

IBM @server iSeries

- **Modernize the user interface**
- **Leverage the latest user interface technology**
- **Easy administration of systems in a network**

Visit the Operations Navigator web site!

www.ibm.com/eserver/iseries/oper_nav

IBM @server. For the next generation of e-business.

Operations Navigator Adds Ease of Use

IBM @server iSeries

- **Leverage your user's Windows skills**
  - Explore view, properties sheets, context menus, drag and drop

- **Reduce need to learn command interface**
  - Easier to understand terminology / concepts
  - Graphics - not just icons
  - Wizards
  - High degree of function integration, not standalone utilities
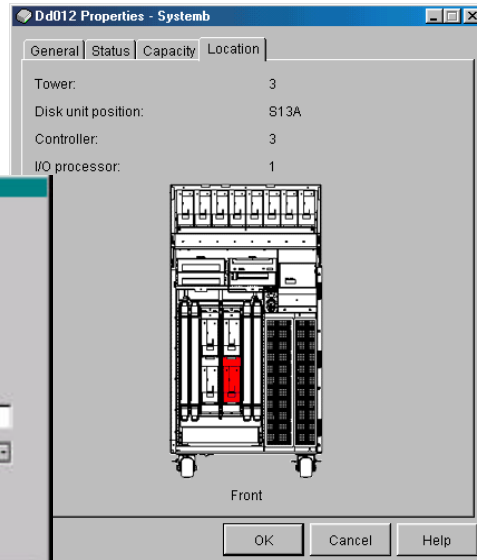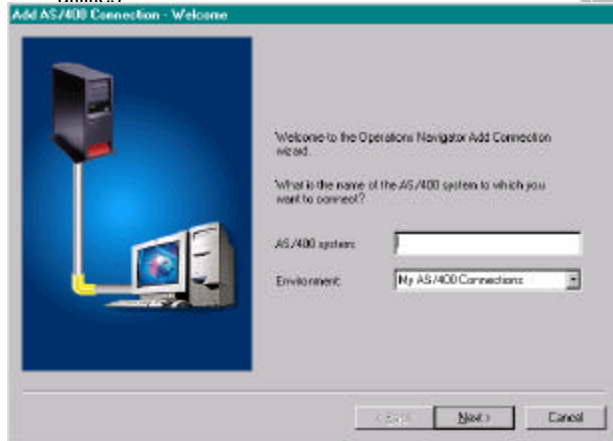
Operations Navigator Makes Users Productive

IBM @server iSeries

- **Lists of objects give rich information**
- **Customized views (Include, Columns, Sort)**
- **Desktop shortcuts to frequently used functions**
- **AutoRefresh, list print, find in list, drag and drop capability**
- **Management Central--manage multiple systems as easy as one**

Management Central: Basic Concepts

IBM @server iSeries

- Operations Navigator includes **Management Central**
- Management Central is a technology we use to:
  - Do things to multiple systems with one request
    - Apply fixes, run commands, distribute software, monitor system activity, manage users and groups, update systems values, etc...
  - Manage long running tasks
  - Schedule tasks
- **MC Pervasive** provides some of these tasks through wireless devices or the browser

IBM @server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

Notes: Management Central Basic Concepts

IBM @server iSeries

- **You can have one or more central systems in your AS/400 network; from within Operations Navigator you select one of these to be your Management Central, central system. You may select a different central system at any time.**

- **AS/400s connected to the central system can be managed; these are referred to as Endpoints**
  - The central server gets a request from the Operations Navigator PC and fans it out to the targeted systems
  - Status and any results flow back from the endpoints to the central server
  - The Operations Navigator PC gets status and results from the central server
  - Tasks can be long-running or scheduled, PC is not required to wait for tasks to complete

- **Endpoints can be collected into System Groups for convenience**
  - Can operate against a group with one request

- **Functions available**
  - Real-time performance monitors (available in V4R3)
  - Remote Operations
  - Inventory Collection
  - Manage Software Fixes
  - Package and Object Distribution
  - Performance Collection Services
  - Job Scheduler GUI (integrated with the above)
  - Manage Users and Groups
  - Manage System Values
  - Run Commands
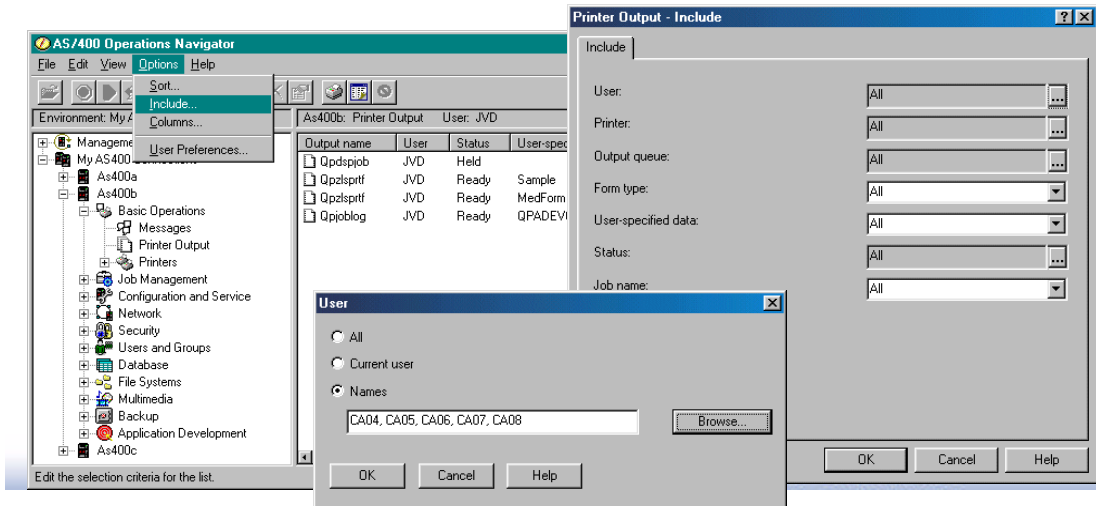
IBM @server. For the next generation of e-business.

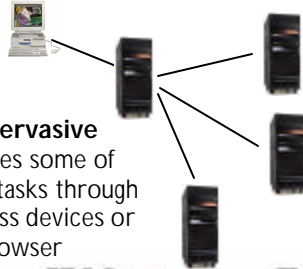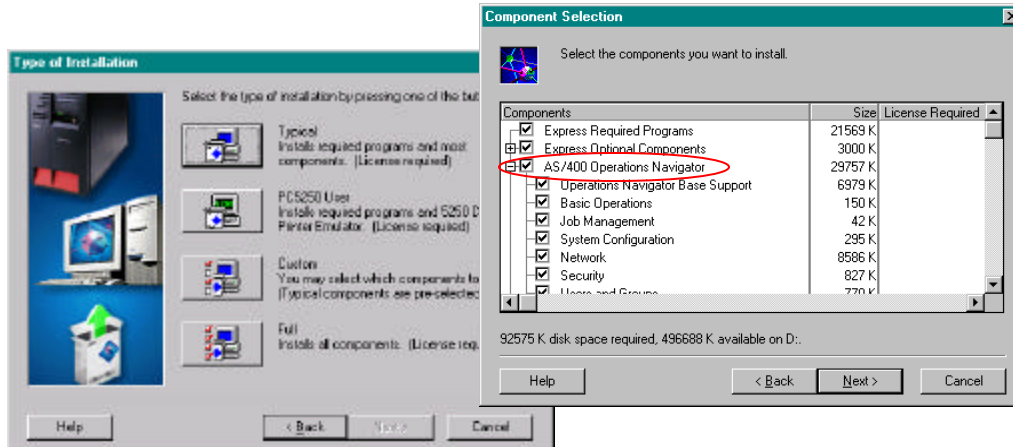IBM Confidential Until Announced 8 2001 IBM Corporation

Operations Navigator Packaging

IBM @ server iSeries

- Operations Navigator is packaged with Client Access Express
  - An optional component of Client Access Express, installed with Express
- However, it's considered to be part of OS/400
- Does not require a Client Access license
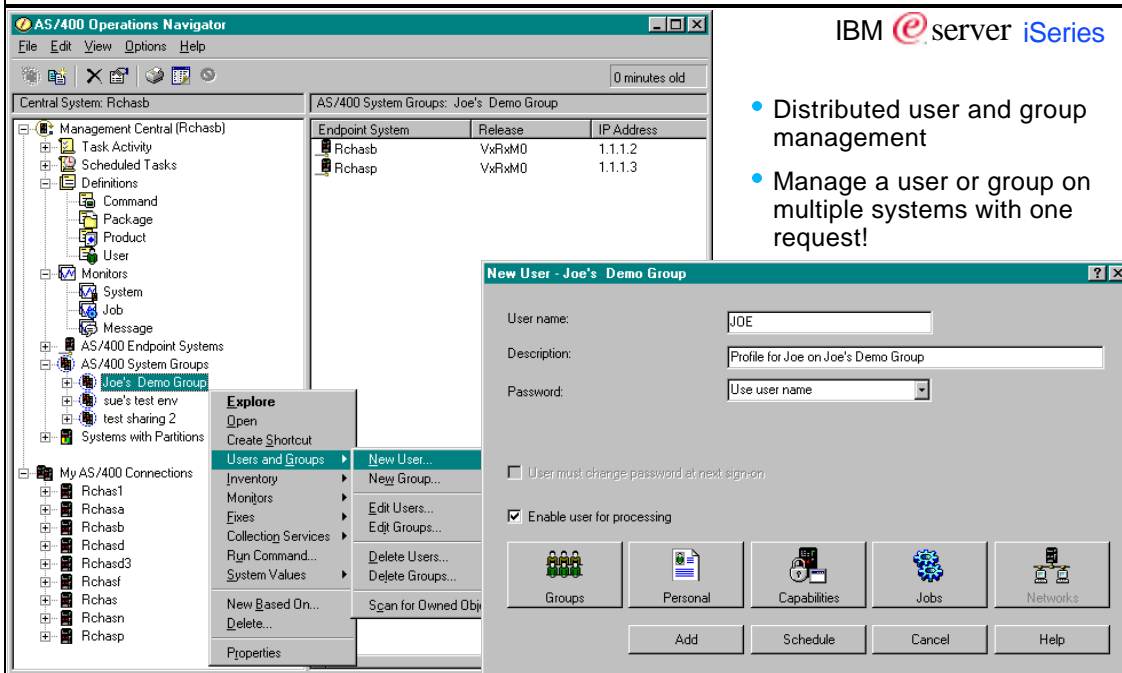

IBM @server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

New User and Group Management functions

IBM @ server iSeries

- Distributed user and group management
- Manage a user or group on multiple systems with one request!

IBM @server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

Managing Users and Groups

IBM @server iSeries

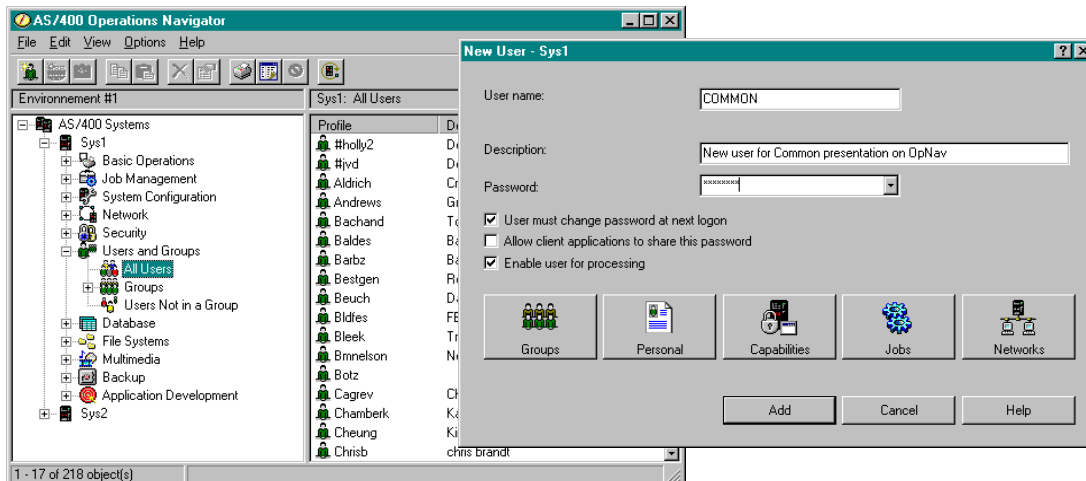- Working with Users and Groups on individual systems vs. through Management Central
  - Management Central User and Group administration availabe in V5R1
  - Individual system User and Group management available in all supported versions
  - Most of the same functions can be done through both interfaces, but are accomplished by different "services".
    - User and Group management actions on Individual systems happen directly on that system immediate on pressing the OK button.
    - Through Management Central, the actions are submitted in a task on the central system. The task will run either immediately or at a scheduled day/time; and will perform the action on the remote system. Progress and results of the actions are maintained on the central system.
  - Functions available only through the individual system:
    - Changing or setting some properties under "capabilities" such as Application Administration and Certificates
    - Server Authentication entries under "Networks"

IBM @server. For the next generation of e-business.

Managing Users and Groups: Individual System

IBM @server iSeries

- **Users and Groups Functions**
  - Create, Change, Delete, Copy Users
  - Create, Change, Delete, Copy Groups
  - Add Users to Groups

- **User includes:**
  - All user profile information
  - System distribution directory entry
  - Domino enrollment (if Domino GUI plug-in installed

IBM @server. For the next generation of e-business.

Managing Users and Groups

IBM @server *iSeries*

Managing Users and Groups Across Multiple Systems
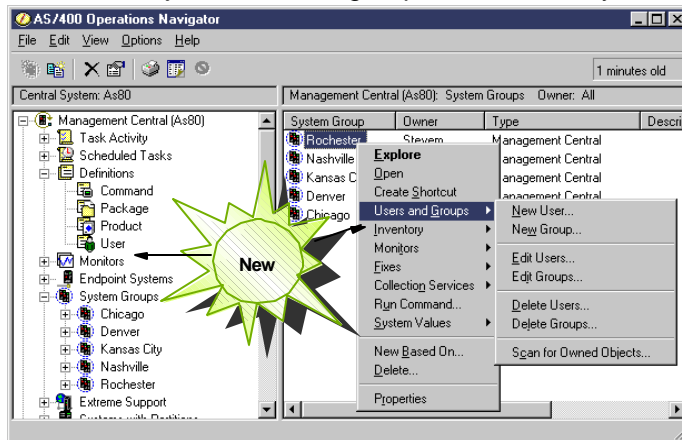
IBM @server. For the next generation of e-business.

Users and Groups

IBM @server *iSeries*

Manage Users and Groups Across Multiple Systems with Management Central!

- Create a user definition, then create similar users based on that definition
- Create, edit, and delete users or groups, and even schedule those actions
- Scan for owned objects to find out what objects a user or group owns across systems
- Collect and search inventory of users and groups
  - For example, see all users who have Security Officer privileges on one or more systems
  - Export inventory to PC file
- Send users or groups from one system to multiple systems
  - Names, passwords, authorities, and other profile properties get copied

IBM @server. For the next generation of e-business.

Notes: Users and Groups

IBM ℮ server iSeries

You can now manage your users and groups across multiple systems using Management Central. You can do tasks such as:

- Create a user definition and then create multiple users across multiple systems based on the definition. Create user definitions for the types of users on your system. Then, when a request comes in for a new user, all special authorities, attributes, and other information common to that type of user will already be there.   You can even specify a command to be run after a user is created from a user definition!

- Create, edit, and delete users and groups across multiple endpoint systems or system groups--and even schedule these actions. For example, use the Edit Users function to change the properties for one or more users on the selected endpoint systems or system groups. This is useful if, for example, you need to change the authority level for several users on multiple systems, or if a user who has access to multiple systems changes their name, you can easily edit that information and apply the change to all systems.

- Scan for owned objects to find out what objects a user or group owns across multiple endpoint systems or system groups, and even scan owned objects for multiple users simultaneously.

- Collect an inventory of the users and groups on one or more endpoint systems, and then view, search, or export that inventory to a PC file. Extensive advanced search capabilities are provided for easy searching. For example, you can search that inventory to see who has Security Officer priviliges, as well as query other profile properties. Also, columns are sortable, so when you view user or group inventory, you can click on the column headings in the right pane of Operations Navigator to organize the information how you want it.

- Send users and groups from one system to multiple endpoint systems or system groups. Unlike the Copy action, the Send function copies as many user properties as possible to the target system(s), including the user name and password, security settings, authorities, and mail options.

Note: All OS/400 special authorities and other authorities that are needed when working with users and groups through a 5250 emulation screen are honored when managing users and groups with Management Central. This includes security administration (*SECADM) privileges and authority to the profiles with which you're working.

IBM ℮ server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

New User / New Group - Overview

IBM ℮ server iSeries

New User:
- Create a user on multiple AS/400 systems
  - ► profile name / password / description
  - ► add the user to groups
  - ► personal information: name, location, mail
  - ► capabilities: privileges, auditing, password, unique identifier
  - ► job information: general, session startup, display session, output, international settings

- Create a user from a 'User Definition'
  - ► user definition is a template for a specific 'type' of user
  - ► can run a command after a user is successfully created

New Group:
- Create a user group on multiple AS/400 systems
  - ► profile name / description
  - ► put users into the group
  - ► set up group privileges
  - ► set the unique identifier

IBM ℮ server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

Create a New User

IBM @server iSeries

AS/400 Operations Navigator

File Edit View Options Help

24 minutes old

Central System: System2   System Groups: Rochester

Management Central (System2)
- Task Activity
- Scheduled Tasks
- Definitions
- Monitors
- Endpoint Systems
- System Groups
  - Roche...
  - UALab
- Extreme Su
- Systems wi
- Clusters
- My Connection
  - System1
  - System2
  - System3
  - System4

Endpoint System   Release
System1   v5r1m0
System2   v5r1m0
System3   v5r1m0

Explore
Open
Create Shortcut
Users and Groups ▶   New User...
Inventory ▶   New Group...
Monitors ▶
Fixes ▶   Edit Users...
Collection Services ▶ Edit Groups...
Run Command...
System Values ▶   Delete Users...
                     Delete Groups...
New Based On...
Delete...   Scan for Owned Ob
Properties

Creates a new user on

New User - Rochester

User name: NEWUSER1

Description: New user profile for demo

Password: *******

☑ User must change password at next sign-on

☑ Enable user for processing

Groups   Personal   Capabilities   Jobs   Networks

Add   Schedule   Cancel   Help

IBM @server. For the next generation of e-business.

Notes: Create a New User

IBM @server iSeries

A new AS/400 user can be created on one or more AS/400 systems.   To create a New User:

1) Right click on a system group
    Select New User from the Users and Groups sub-menu

2) Fill in the user name and optionally the description and password fields.   Make sure the "User must change password at next signon" and "Enable user for processing" fields are set properly.   Note: the user name can be a maximum of 10 characters.

3) Click on the "Groups" button and set up the user's list of groups. (optional)

4) Click on the "Personal" button and fill in the user's name, location and mail information. (optional). This information results in a System Distribution Directory (SDD) entry being added for this user. (ADDDIRE command)

5) Click on the "Capabilities" button and fill in the following: (all optional)
    user's privileges   (privilege class, system privileges - special authorities)
    auditing   information   (object auditing, which actions to audit)
    password expiration information
    unique identifier settings

6) Click on the "Jobs" button and fill in the following: (all optional)
    user's general job information   (current library, job description, etc.),
    session startup information   (initial program, etc.),
    display session information   (attention program, assistance level, user options, etc.),
    output information   (print device, output queue, message queue, etc.)
    international information   (language, country, locale, etc.)

7) Click on Schedule. Once you schedule the task, it will be listed in the Scheduled Tasks->Users and Groups container.   Clicking Add instead of Schedule starts the Create User task immediately.   If you run the task immediately, the task status will be shown in the Task Activity->Users and Groups container of Management Central.

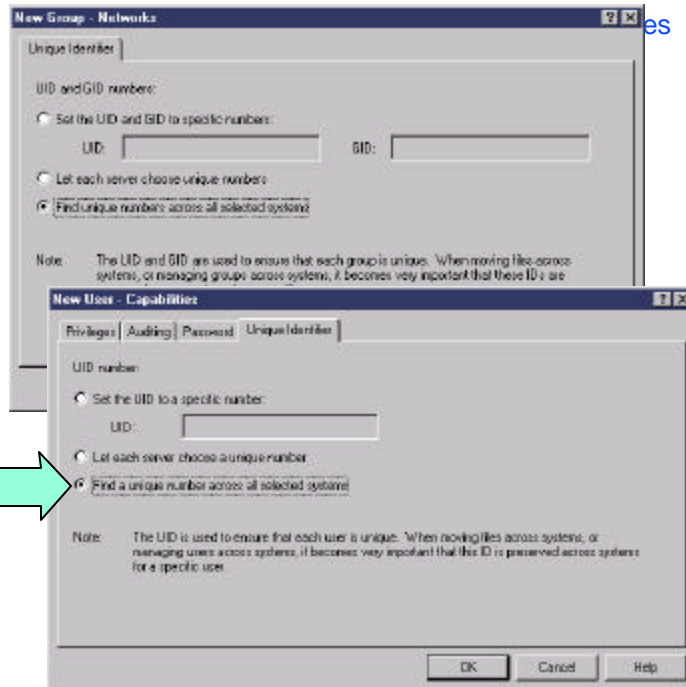IBM @server. For the next generation of e-business.

User Definition

IBM @ server iSeries

- A template for users with similar attributes
- Create one for each department in your company
  - Security and permissions likely the same for each user in department
  - Change ID, password, & personal information per user
- Specify a command or program in definition
  - Runs after users based on definition have been successfully created
  - Automatically substitute new profile name in command string
- Sharing options
- Create users based on that definition
  - On a single system or
  - Across multiple systems

New

- When creating users, set user properties
  - On a new user-by-new user basis or
  - Use settings defined in the user definition

IBM @server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

Notes: User Definition

IBM @ server iSeries

A user definition allows you an easier way to create a new user on multiple endpoint systems or system groups. Create user definitions for the various types of users on your system. Then, when a request comes in for a new user, all special authorities, auditing, session startup, and other information common to that type of user will already be there. You only need to specify the name for the user, a brief description to help you identify this user in a list of users, and a new password for the user. All other properties of the new user are based on the properties stored in the user definition, unless you choose to change them. You may also select the groups the user should belong to and provide personal information about the user at the time the user is created.

You can create the new user immediately or you can schedule a later time when you want the user to be created. For example, you can create a user definition named Accounting Users, which specifies all the special authorities and other properties that the users in your accounting department need. Then, at any time, you can create one or more new users based on that definition on any endpoint system or system group.

In the user definition, you can specify a command or program to run on the target system immediately after a user is created successfully on the system. The command or program is run when a user is created from the definition. This can be any command that can be used in the OS/400 batch environment. You cannot run an interactive command. You can use the replacement variable &USER any place in the command where you want the command to substitute the name of the user that is being created. For example, you could specify the command CRTLIB &USER to create a library with the user name as the name of the library. This will create a library each time the definition is used to create a user.

When creating a new user from a definition, you can change properties of the new user, and this does not affect the properties defined in the user definition. Or you can simply use the definition properties for each new user you create, and then just specify a name and password for the user.

The process of creating a user definition and a new user based on a definition is shown in the following pages.

IBM @server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

Create a New Group

Notes: Create a New Group

A new group (of users) can be created on one or more systems.   To create a new group:

**1) Right click on a system group
     Select New Group from the Users and Groups sub-menu**

2) Fill in the group name (required) and optionally the description field.

3) Select the users who should be members of the group and add them to the "Selected users" list by clicking on the "Add->" button. (Optional)

4) Optionally, left click on the "Capabilities" button and set the group's privileges (privilege class, system privileges).

5) Optionally, left click on the "Networks" button and set the unique identifier setting.

6) Click on Schedule. Once you schedule the task, the task will be listed in the Scheduled Tasks->Users and Groups container.   Clicking Add instead of Schedule starts the Create Group task immediately.   If you run the task immediately, the task status will be shown in the Task Activity->Users and Groups container of Management Central.

Synchronizing Unique Identifiers Across Systems

Environments where UID / GID must be the same on multiple systems for a specific user or group

Example environments:
- ▸ AS/400 Clusters
- ▸ Independent Auxiliary Storage Pool (IASP)
- ▸ Shared IFS files

Notes: Synchronizing Unique Identifiers

IBM @ server iSeries

In some environments such as clustered systems, shared IFS files, etc., some applications depend upon the user or group profile name and unique identifiers to be consistent across multiple systems. These applications identify a particular user or group across systems as a combination of matching profile name, UID and GID values. If any of those three fields do not match, then the application assumes it is a different user or group. Therefore, in these environments it is critical to have UID and GID values synchronized when appropriate.

For a user, the following fields must be synchronized for these environments:
  user name
  UID value
  GID value must be set to 0 (zero)

For a group, the following fields must be synchronized for these environments:
  group name
  UID value
  GID value

Management Central offers an option for automatically synchronizing the UID and GID values for user and group profiles across AS/400 systems. The option to "Find a unique number across all selected systems" is available on the Unique Identifiers panel whenever you create a new user or group, and also when you edit users or groups.

The Users and Groups inventory must be up-to-date in order for this option to work properly. Management Central will use the information in the Users and Groups inventory to automatically select a UID and GID value which are not in use by any other user or group profiles on any of the selected systems. It will then assign that UID / GID number to the user or group when it creates the user or group.

The Edit Users and Edit Groups function works in a similar manner when the "Find a unique number across all selected systems" option is set.

Edit Users - Edit Some Settings

IBM @server iSeries

IBM @server. For the next generation of e-business.

Notes: Edit Users - Edit Some Settings

IBM @server iSeries

You can now edit one or more users or groups on an endpoint system or on all the systems in a system group using Management Central. Changing user and group settings across multiple systems can save significant time for a system administrator. For example, you could quickly and easily change the authority level for several users or groups across multiple systems. You can specify this editing task and then schedule it to run at a convenient time.

To change settings for users:

1) Right click on a system groug and select Edit Users from the Users and Groups sub-menu

2) Click on the Browse button to get a list of users to select from. Or if you prefer, you may type in the user names you want to edit, separating each name with either a comma or a space. Note: System-defined users cannot be edited; these users typically start with a Q, like QSECOFR.

3) If you have clicked on the Browse button, you will get a window containing a list of users on the selected systems. You can select the users you wish to edit, then click on the OK button. Once you have selected which users you want to edit on the selected systems, you will need to select which settings you want to edit for those users and make the desired settings updates:

4) Select the category of settings you wish to edit first by selecting from the "Category" pulldown. The window will now display a list of settings for the category you have selected.

5) Select one or more settings you wish to edit for that category, and select the Properties button to change the settings.

6) You now see the panel for the category you have selected to edit.   Notice that only the settings you selected to edit from that category are enabled to be changed. Update the settings to the desired values. Click on the OK button. This will take you back to the Edit Users dialog and show the results of your changes to those settings.

You can edit as many settings in as many categories as you wish.   Each time you Click on the OK button it will take you back to the Edit Users dialog and show the results of your changes to the settings in the current category you have selected.

IBM @server. For the next generation of e-business.

Send - Overview

IBM @server iSeries

One 'source' system, multiple 'target' systems

Can send multiple users or groups together

Sends as many properties as possible (unlike Copy)

- ► user or group profile
- ► passwords (including NT and LAN server passwords)
- ► security settings
- ► private authorities
- ► mail options
- ► can specify UID / GID values to be synchronized

New

Send task can be scheduled

Users and Groups inventory is automatically updated

IBM @server. For the next generation of e-business.

Send Users

IBM @server iSeries

IBM @server. For the next generation of e-business.

25

Notes: Send Users

IBM @ server iSeries

When you send one or more users to one or multiple target systems, as many user properties as possible are copied to the new systems, including the user name, passwords (including NT and LAN server passwords if the user has them), security settings, private authorities, and mail options that are not copied when you select to Copy a user to another system (see Copy Note below). An entry in the system distribution directory (SDD) is added (ADDDIRE) or changed (CHGDIRE) for each user that is sent. The SDD fields that are sent are the fields you see in the panels in the 'Personal' section on a New User or Edit Users. Several of the system-defined users cannot be sent; these users typically start with a Q, like QSECOFR.

Copy Note: The Copy function is not available within Management Central. It is available in Operations Navigator when you expand a system under My Connections, expand Users and Groups, select either "All Users", "Groups", or "Users Not in a Group", then select one or more users or groups in the right pane, right click to get the context menu, and the Copy function is one of the available functions.

Send Note: You will need Security Administration and Save/Restore system privileges (that is, *SECADM and *SAVSYS special authorities) on the source and target systems. If you choose to synchronize the unique identifiers, you will need All Object access as well as Security Administration and Save/Restore system privileges on the target systems (that is, *ALLOBJ, *SECADM and *SAVSYS special authorities).

IBM @server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

Delete Users and Groups - Overview

IBM @ server iSeries

Delete multiple users / groups on multiple systems
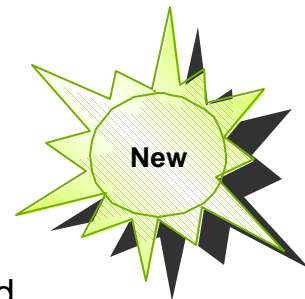
Delete task can be scheduled

Actions for owned objects:
- ► do not delete if owns objects
- ► delete owned objects
- ► transfer ownership of objects

How to find out what objects are owned?

Scan for Owned Objects!
- ► lists owned objects on multiple systems
- ► specifies maximum number to view
- ► standalone function or use in the context of 'Delete'

New

Users and Groups inventory is automatically updated

IBM @server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

Notes: Delete Users

You can now delete one or more users or groups on an endpoint system or on all the systems in a system group using Management Central. This function can save significant time for a system administrator. You can set up a delete task and then schedule it to run at a convenient time.

To delete users:

1) Right click on a system group
     Select Delete Users from the Users and Groups sub-menu

2) Click on the Browse button to get a list of users to select from. Or if you prefer, you may type in the user names you want to delete, separating each name with either a comma or a space. Note: System-defined users cannot be deleted; these users typically start with a Q, like QSECOFR.

3) If you have clicked on the Browse button, you will get a window containing a list of users on the selected systems. You can select the users you wish to delete, then click on the OK button. The 'Users to Delete' field is now filled in.

Now you need to decide what to do with the objects owned by the users. If you need to see a list of the objects, you can use the "Scan for Owned Objects" function. Select the action to take if the user owns objects. If you want to transfer owned objects to another user, you can use the Browse function to get a list of users to select from.

4) Click on Schedule.
     Clicking OK instead of Schedule starts the Delete Users task immediately.

Note: if the user does not exist on an endpoint system, the delete operation will fail due to "user not found".

IBM **e** server. For the next generation of e-business.

IBM Confidential Until Announced **8** 2001 IBM Corporation

Notes: Delete Groups

1) Right click on a system group
     Select Delete Groups from the Users and Groups sub-menu
     You need to select the groups to delete just like you selected the users to delete (previous pages).

2) Action to take if group is primary group of objects:
    ► Do not delete group - specifies not to delete any group that is the primary group of any object on any system from which it is being deleted.
    ► Remove primary group from objects - specifies to remove this group as the primary group for any objects on any system from which the group is being deleted.
    ► Change primary group - specifies to delete all the specified groups and to specify a different group as the primary group for any objects that had this group as the primary group. When you select this option, you must specify the name of another group to be the primary group. You may click Browse to select from a list of valid group names in the central system inventory for all selected systems. If you specify a group that does not exist on the endpoint system or system group, the delete operation will fail.

3) Action to take if group owns objects:
    ► Do not delete group - specifies not to delete any groups that own objects on the system from which they are being deleted. However, if the group's message queue is the only object owned by the group, both the group and the message queue will be deleted.
    ► Delete objects that group owns - specifies to delete all the specified groups and the objects that they own on the system from which they are being deleted.
    ► Transfer objects to another user - specifies to delete all the specified groups and to transfer ownership of any objects (including any message queues) that they own on the system from which they are being deleted. When you select this option, you must specify the name of a user to transfer ownership to. Ownership of the objects is transferred regardless of the new owner's current authority to the objects. You may click Browse to select from a list of valid user names in the central system inventory for all selected systems.

4) Click on Schedule.
     Clicking OK instead of Schedule starts the Delete Groups task immediately.

IBM **e** server. For the next generation of e-business.

IBM Confidential Until Announced **8** 2001 IBM Corporation

Search for Users

IBM **e** server iSeries

IBM e server. For the next generation of e-business.

IBM Confidential Until Announced **8** 2001 IBM Corporation

Notes: Search for Users

IBM **e** server iSeries

Searching on users and groups provides you with a lot of flexibility to query the user and group inventory for the information you want. The Basic search is for quick searches to find a particular user or group. The Advanced search page gives you the flexibility to search on additional profile properties.

The advanced search is for more detailed searching, and to search on fields that aren't simple text fields.   For example, you can find all profiles not signed on in a month, find all profiles that have been disabled, find all profiles that are using more than 30 MB of storage, find all security officers, and so on.   Note: keywords used on the green screen (such as *SYSOPR for user class - that is, privilege class) can not be used in the search panels.

The following items can be searched with the advanced search for Users and Groups inventory:

Enabled	No Password	Unique identifier (UID)	Department
Previous sign-on date	Created Date	Unique identifier (GID)	Location
Sign-on attempts not valid	Last changed Date	Company	Office
Date password expires	Privilege class	Telephone number	Building
System privileges (special authorities)	Limit capabilities	Fax number	Mailing address
Accounting code	Storage used	Job title	

From the Search Results window, you can perform many of the actions that you can perform on a user or group elsewhere within Management Central. For example, you can delete a user or group, edit the profile (e.g., remove its Security Officer authority), view its properties, or scan for objects owned by a user or group. Also from the results window, you can export the search results into a spreadsheet, text file, or HTML (web) page.

IBM e server. For the next generation of e-business.

IBM Confidential Until Announced **8** 2001 IBM Corporation

Managing iSeries Resource (Object) Security

IBM *e* server iSeries

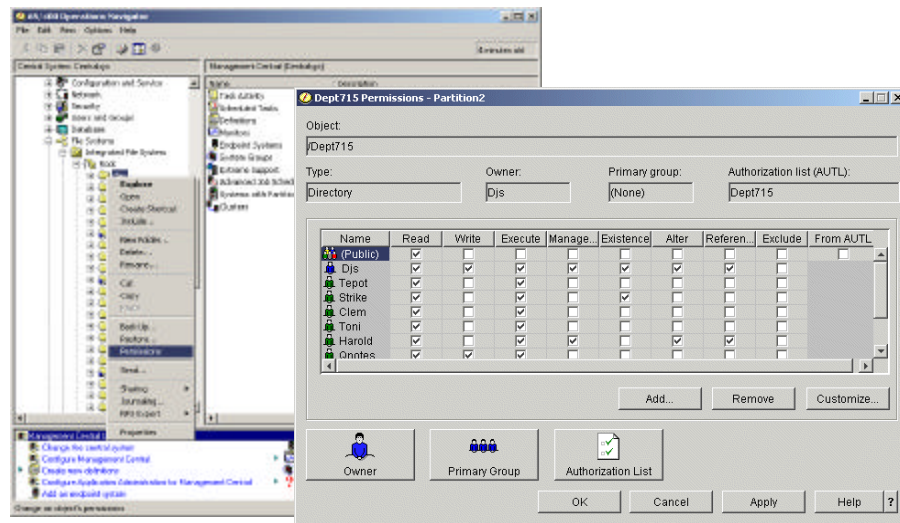*Work with Permissions for certain object types*
Manage Authorization Lists

IBM *e*server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

Permissions

IBM *e* server iSeries

- **Set up resource security**
- **Permissions menu choice available on objects such as directories, files, and printers**
- **Permissions for most OS/400 objects can also be accessed through the File Systems container (QSYS.LIB file system)**

IBM *e*server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

Authorization Lists

- **Create/Delete Authorization lists**
- **View the properties of an Authorization List**
- **Change the permissions for Users and Groups in Authorization lists**
- **Add/Remove Users and Groups to Authorization Lists**
- View the objects secured by an Authorization List

IBM @server iSeries
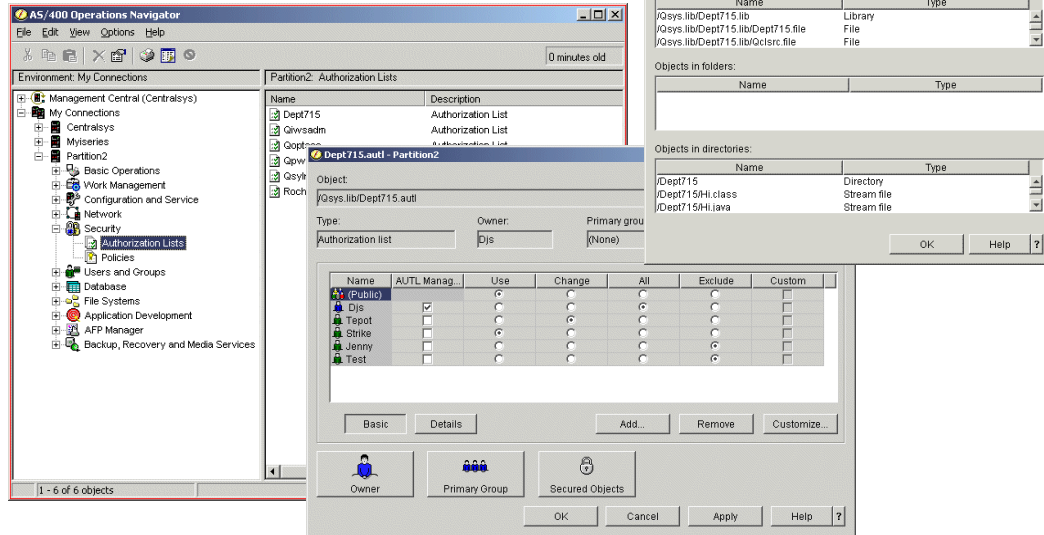
IBM @server. For the next generation of e-business.

Application Administration

- Manage access to functions on a "per iSeries user" basis
- Administer OpNav, other Client, and Host applications
- Separate settings and access schemes for each iSeries in your network
- Ability to even restrict users with All Object privilege
- You can copy access settings from function to function for ease of administration

IBM @server iSeries
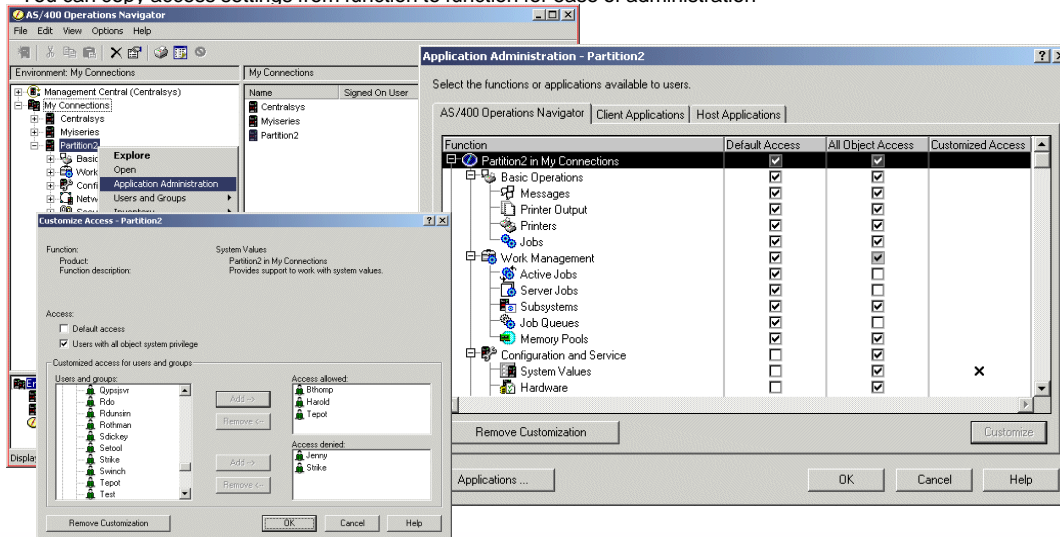
IBM @server. For the next generation of e-business.

Application Administration: Registering Applications

- Add and remove applications to be administered through Application Administration
- No changes can be made to the "shipped value" for access settings until the application has been registered to Application Administration
- If an application is shown in both lists on this dialog, it indicates the application has been registered on the iSeries, but there are some administrable functions for this application that are defined on this client, but are not registered on the iSeries. You can select the application and press "Add" to register the additional functions.
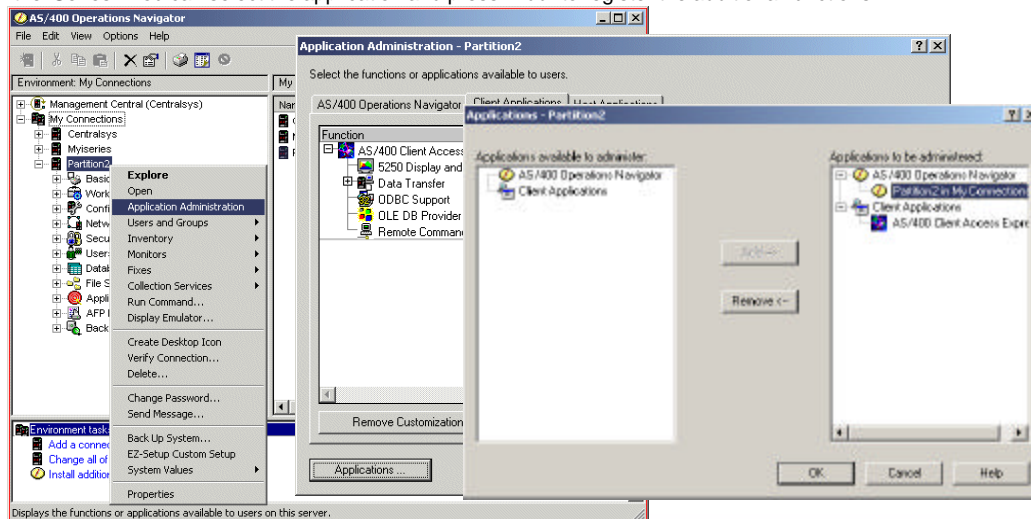
IBM @server iSeries

IBM @server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

Notes: Application Administration

IBM @server iSeries

To Access Application Administration:
For an individual iSeries...
- Right Click on "Management Central (SystemX)" in Operations Navigator
- Select Application Administration from the context menu
This will allow you to view and modify access settings for administrable functions in Operations Navigator, other Client Applications, and Host applications. Selecting the "Applications" button from this dialog allows you to work with Operations Navigator, other Client, and Host applications that can be restricted with Application Administration

For Administering functions specific to Management Central on your current Central System...
- Right Click on "Management Central (SystemX)" in Operations Navigator
- Select Application Administration from the context menu
This will allow you to view and modify access settings only for administrable functions associated with Management Central on the current Central System. Selecting the "Applications" button from this dialog, only allows you to work with Management Central applications that can be restricted with Application Administration.

Registering Applications to be administered: Application Administration cannot be used to restrict access to an application's functions until the application has been registered on the iSeries. To register Applications, select the "Applications" button from the Application Administration dialog. Then select the applications you want to administer and click the "Add" button.

Default Access: The Application Administration dialog allows you to set up the default access scheme for Operations Navigator and any other host or client applications which make use of Application Administration. You can explicitly give or take away access to the default user; you can also take away access to those users with *ALLOBJ (all object) privilege.

Individual Access: An individual user or group can then be given more or less access. This can be done by using the "Customize" button from the Application Administration dialog and selecting users and groups that should be specifically allowed or denied access to a function. To easily view and manage all of the access settings for an individual user or group, select the user's properties under "Users and Groups," push the "Capabilities" push button, and click on the "Applications" tab in the Capabilities dialog. This dialog also shows where the users access for each function comes from --the default access scheme, *ALLOBJ privilege, membership in a group that has explicit access, or explicit user access.

Note: You must have Security Administrator authority on the iSeries in order to change access settings in Application Administration, or to access the "Applications" dialog.
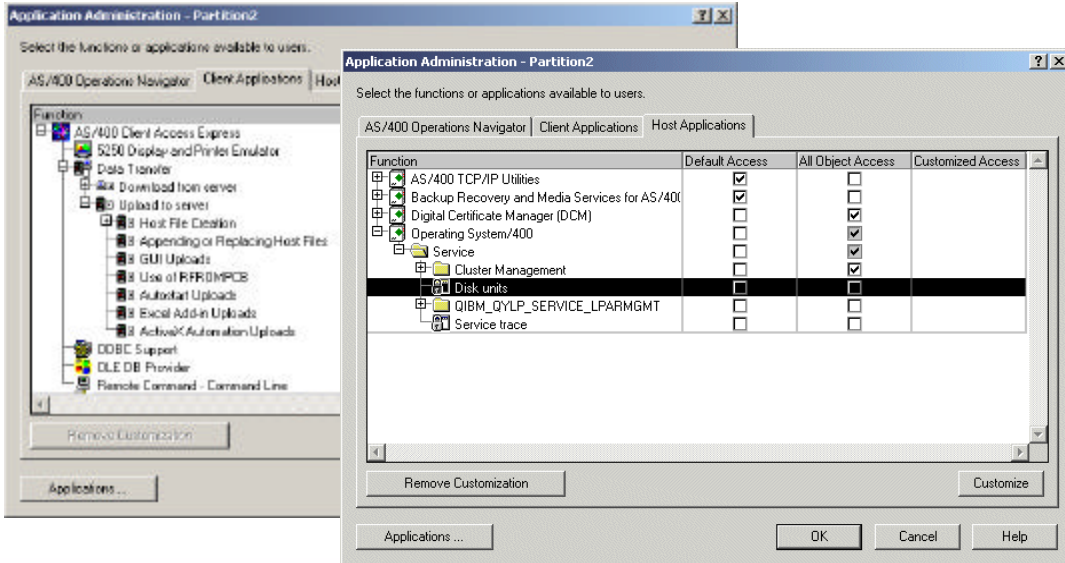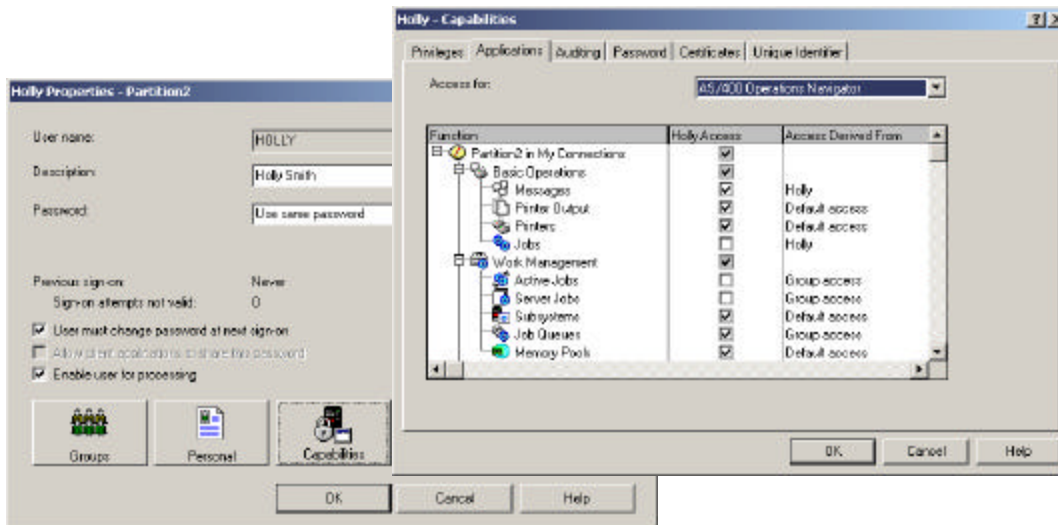
IBM @server. For the next generation of e-business.

IBM Confidential Until Announced 8 2001 IBM Corporation

Application Administration - By System

- **Control access to server and client applications that want to make use of Application Administration**

- **Disk management is not available by default**

IBM @server iSeries

Application Administration - By User

- Individual users and groups can be given more or less access
  - Use user or group properties, Capabilities button, Applications tab

- All Application Administration information is stored on the server and roams with users when they use Operations Navigator on a different PC

IBM @server iSeries

Notes: Application Administration

How Does Application Administration Work?
- Application Administration settings are stored on the AS/400 and associated with the user profile.
- Software calls AppAdmin APIs to determine if it can perform a particular function or not.
- For Operations Navigator and Client Applications, AppAdmin API downloads the AppAdmin data from the AS/400 as needed.
- The data is cached on the PC, and updated when the AppAdmin data on the AS/400 changes.
- No special PC configuration is required. Application Administration is built into Client Access.

Notes: Application Administration

Using Application Administration

This chart shows whether, for a particular user, access to a function is allowed or denied. It shows the interaction between the customized application administration settings, whether the user has All Object privilege, group membership, etc. "AOA selected" means that users with All Object privilege are allowed to access the function according to the default access scheme for the system. "User defined in CA" means that the user's application settings have been changed to either explicitly allow or deny
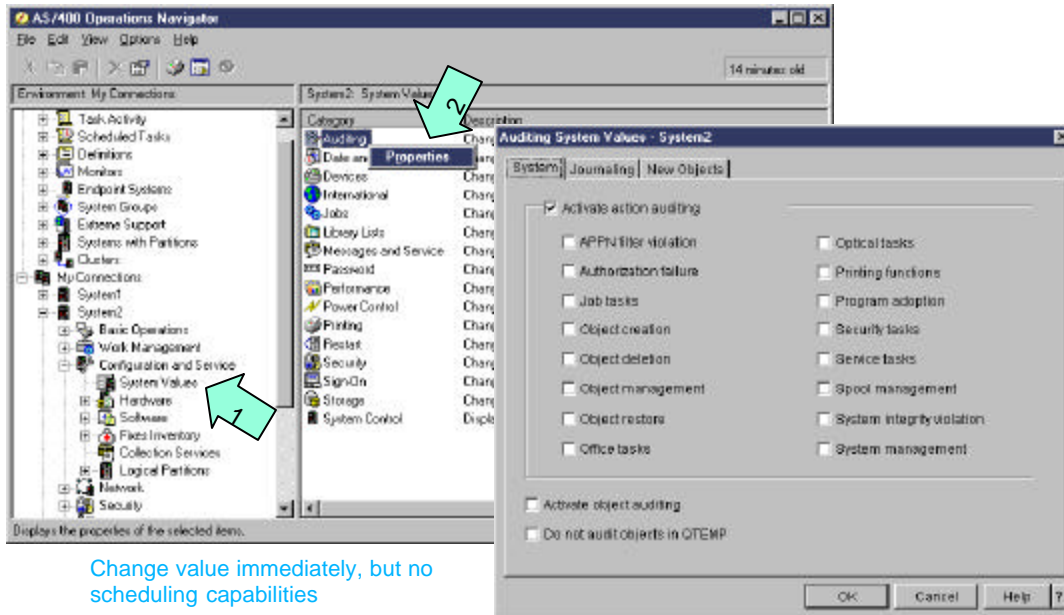
access.
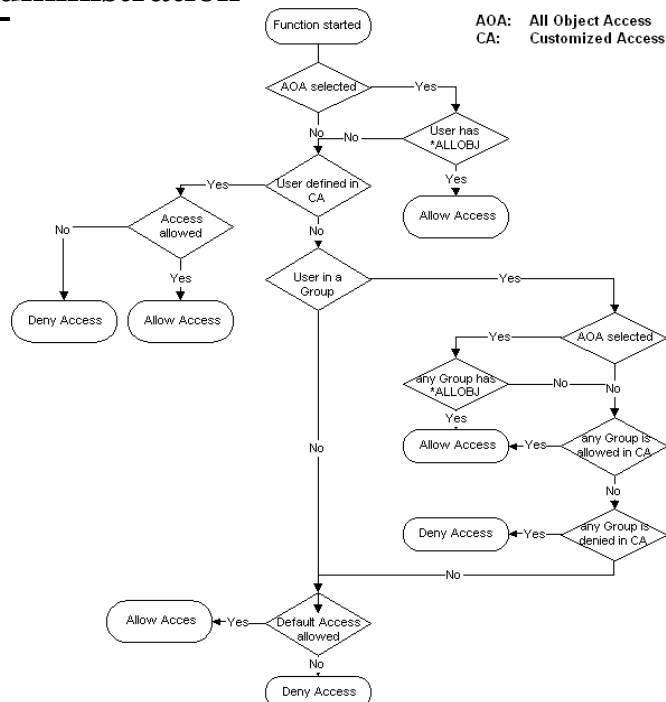
Managing System Values

Managing System Values
➡ *Updating single systems*
➡ *Compare and Update across multiple systems*

IBM @server. For the next generation of e-business.

Change System Values on a Single System

IBM @server iSeries

Change value immediately, but no
scheduling capabilities

IBM @server. For the next generation of e-business.

Notes: Change System Values on a Single System

IBM *e* server iSeries

Purpose: change system values on a single system.
Authorities Required: In order to change a system value on a system, the same authority is required as if you were changing the system value on a 5250 emulation session (green screen).

1) Expand My Connections, then expand the system you want to change system values on. Expand Configuration and Service Click on a System Values.

The right pane is populated with a list of the system value categories. System values are grouped into one of the following categories: Auditing, Date and Time, Devices, International, Jobs, Library Lists, Messages and Service, Password, Performance, Power Control, Printing, Restart, Security, Sign-on, Storage, System Control.

2) Right click on the category you want to change and select Properties.

A property sheet window is displayed which may contain one or more pages depending on the category selected. Each page contains one or more system values that may be changed. Make the changes you want, then click OK for the changes to be made immediately. Note: clicking the Help button allows you to view which system value(s) on the server (eg, QAUDLVL) map to the attributes displayed on the GUI.

When do changes to a System Value take effect?
When the new setting for a system value takes effect depends on which system value it is. Not all system value changes are used by the system immediately when a system value is changed. For some values such as Start-up Program (QSTRUPPGM), changes take effect at the next restart of the iSeries. To find out when a specific system value change takes effect, see the help for that particular system value.

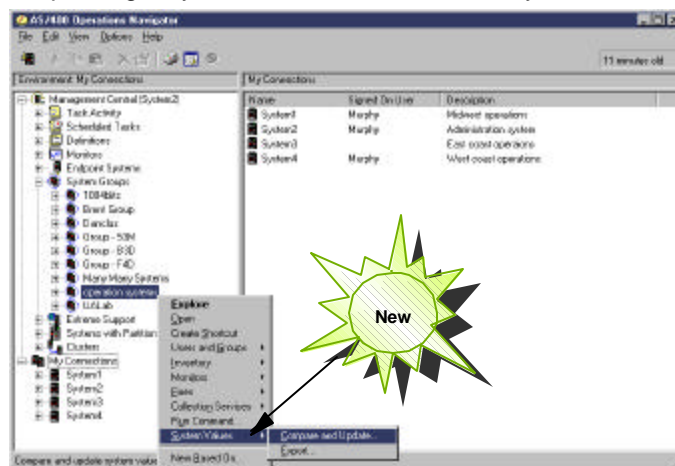IBM *e* server. For the next generation of e-business.

Changing System Values Across Multiple Systems

IBM *e* server iSeries

*Manage System Values across Multiple Systems
with Management Central!*

- Collect inventory for system values
- Compare system values on multiple target systems to those on a model system
  - Export inventory to PC file
- Update system values on target systems based on those of a model system
  - Also schedule the updates
- Change system values on a single system

IBM *e* server. For the next generation of e-business.

Notes: Changing System Values Across Multiple Systems

You can now manage system values across multiple systems using Management Central. You can do tasks such as:

- Collect an inventory of system values on one or more endpoint systems.
- Compare collected system values inventory on one or more endpoint systems to a model system. The model system values are live; the endpoint systems are from the inventory database. View all the system values or only those that are different from the model system. Also export the inventory to a PC file.
- Update selected system values on multiple endpoint systems or system groups--and even schedule these actions. This is useful if your endpoint systems need to be configured the same.

Note: All OS/400 special authorities and other authorities that are needed when updating system values through a 5250 emulation screen are honored when updating system values with Management Central.

IBM @server. For the next generation of e-business.

Compare and Update System Values

IBM @server. For the next generation of e-business.

Notes: Compare and Update System Values

IBM @server iSeries

Purpose: Compare system values on multiple endpoints to those on a model system, and optionally update the endpoints to match the selected system values on the model system.

Authorities Required: In order to update a system value on a target endpoint system, the same authority is required as if you were changing the system value on a 5250 emulation session (green screen). Also, a matching profile with password on the endpoint systems you will update system values on.

Compare and Update:

• One 'model' system, multiple 'target' systems
• Model system data is real time, target system data obtained from central system database
• Can customize view
  ▸ show only differences
  ▸ summary of system values selected for update
• Update task can be scheduled
• Export target system data to a PC file

The first time Compare and Update is launched, the model system defaults to the Management Central central system. It is remembered the next time the window is launched. The system values are divided into a number of categories. The initial category is always Auditing. The system values associated with the current category are displayed in the Model System Settings table. The target systems are listed below in the Target Systems table, however, initially there is no data in the adjoining column.

The Target Systems table will be updated showing the selected system value in the heading of the second column and the current value (as obtained from the system values inventory database) for each target system.

Note: If system values inventory collection has not been done for a target system, "Value not collected" will be specified in the second column of the target system table for that target system.

IBM @server. For the next generation of e-business.

IBM Confidential Until Announced **8** 2001 IBM Corporation

Security Wizard

IBM @server iSeries

• **Configure security using the Security Wizard**

• **Advises on security system values based on how you use your system**

IBM @server. For the next generation of e-business.

IBM Confidential Until Announced **8** 2001 IBM Corporation

Security Wizard

- **Provides detailed report of recommended changes**
- **If requested, will make the recommended changes, with any modifications you select.**
- **Allows rollback of changes previously made through the wizard**

IBM @server iSeries

Security Wizard - Partition2

The Security Wizard generates two reports that explain the security recommendations.

Specify the directory where you want the reports

Administrator Information Report

C:\Documents and Settings\djs\My Documents   Browse ...

Summary of Recommendations

| Security Auditing Policy | Security Level | Security Journal Reports | Password Level |
| Security Controls | Password Rules | Security Reports | |

To accept a recommended setting for a security control, leave its checkbox checked.
To keep the current setting for a security control, click its checkbox to remove the check.

Security Control	Current Setting	Recommended Setting
☑ Allow object restore	Restore all objects	Restore programs with secu
☑ Remote power on an...	No	No
☑ Max sign on action	Disable device and profile	Disable device and profile
☑ Disconnect job interval	120	240
☑ Use adopted authority	None	QUSEADPAUT
☑ Retain server security	Yes	Yes
☑ DDM request access	Check object authorizations	Check object authorization
☑ Max not valid sign on	5	3
☑ Inactive message qu...	Disconnect job	Disconnect job
☑ Inactive job time out	120	15
☑ Sign on info	Display	Display
☑ Shared memory control	Allow usage of shared memory	Allow usage of shared mem
☑ Remote sign on	Require sign on	Require sign on
☑ Remote service attrib...	Off	Off
☑ Verify object on restore	Do not verify signature on restore	Verify: Restore unsigned ob
☑ Job action	File for user	File for user
☑ Limit security officer	No	Yes

OK   Cancel

Administrator Report

System value name: QMAXSIGN
Current setting: 5
Recommended setting: 3

System value name: QMAXSIGNACN
Current setting: 2
Recommended setting: 3

Following are operational considerations for the QMAXSIGN and QMAXSIGNACN system values.
The system will allow 3 consecutive attempts for a user to sign on correctly (correct user ID and password combination).
When a user exceeds the unsuccessful sign-on attempts (3), the system will do the following:
Set the status of the user's profile to 'DISABLED'. To make a user's profile available for sign on again, use the following command: CHGUSRPRF USRPRF(profile-name) STATUS(*ENABLED)
Vary off the device where the user attempted to sign on. To make a workstation available for sign on again, use the Work with Configuration Status (WRKCFGSTS) command to vary on the device.

OK

IBM @server. For the next generation of e-business.

Reference Information

IBM @server iSeries

- Operations Navigator: www.ibm.com/eserver/iseries/oper_nav/
- Management Central: www.ibm.com/eserver/iseries/sftsol/mgmtcentral.htm
- Client Access Express: www.ibm.com/eserver/iseries/clientaccess
- AS/400 Home Page: www.ibm.com/eserver/iseries
- AS/400 Publications: publib.boulder.ibm.com/pubs/html/as400/infocenter.htm
- Redbooks: www.redbooks.ibm.com
  - Managing AS/400 V4R4 with Operations Navigator, SG24-5646-00
  - Management Central: A Smart Way to Manage AS/400 Systems, SG24-5407-00
  - AS/400 Client Access Express for Windows: Implementing V4R4M0, SG24-5191-00
- Technical Studio for AS/400: Operations Navigator Workshop
  - Technical Studio contains technical information on topics such as Client Access, Operations Navigator, Web Builder's Workshop, Domino for AS/400 and more. The information for Operations navigator can be accessed at: www.iSeries.ibm.com/tstudio/opsnav/guiframe.htm
- Tivoli Home Page: www.tivoli.com
- Systems Management Partner Program: www.ibm.com/eserver/iseries/smpg
- Advanced Job Scheduler: www.ibm.com/eserver/iseries/jscheduler

IBM @server. For the next generation of e-business.

Trademarks and Disclaimers

IBM @server iSeries

8 Copyright International Business Machines Corporation 2001
References in this document to IBM products or services do not imply that IBM intends to make them available in every country.
The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AS/400	IBM Logo
AS/400e	iSeries
e-business logo	OS/400
IBM	

Lotus, Freelance, and Word Pro are trademarks of Lotus Development Corporation in the United States, other countries, or both.
Tivoli and NetView are trademarks of Tivoli Systems Inc. in the United States, other countries, or both.
C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
PC Direct is a trademark of Ziff Communications Company in the United States, other countries, or both and is used by IBM Corporation under license.
ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.
UNIX is a registered trademark of The Open Group in the United States and other countries.
SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.
Other company, product and service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information in this presentation concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of the specific Statement of Direction.

Some information in this presentation addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.

IBM @server. For the next generation of e-business.

IBM Confidential Until Announced **8** 2001 IBM Corporation