

Session:



# Safely Unleashing iSeries Navigator

*IBM @server iSeries*

**Laural Schneckloth**

laurals@us.ibm.com  
IBM Rochester

8 Copyright IBM Corporation, 2002. All Rights Reserved.  
This publication may refer to products that are not currently available in your country. IBM makes no commitment to make available any products referred to herein.

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

## Overview

IBM @server iSeries

### ● Controlling the Client

- Install/Update
- Microsoft Policies
- Application Administration
- Passwords

***If you can't do the function on a green-screen command line, then you can't do it through Operations Navigator!***

### ● Controlling the Connection

- Secured Sockets Layer (SSL)

### ● Controlling the iSeries

- Security Wizard
- Security Policies (system values)
- Audit Policies
- Resource Security

### ● Where to get more information



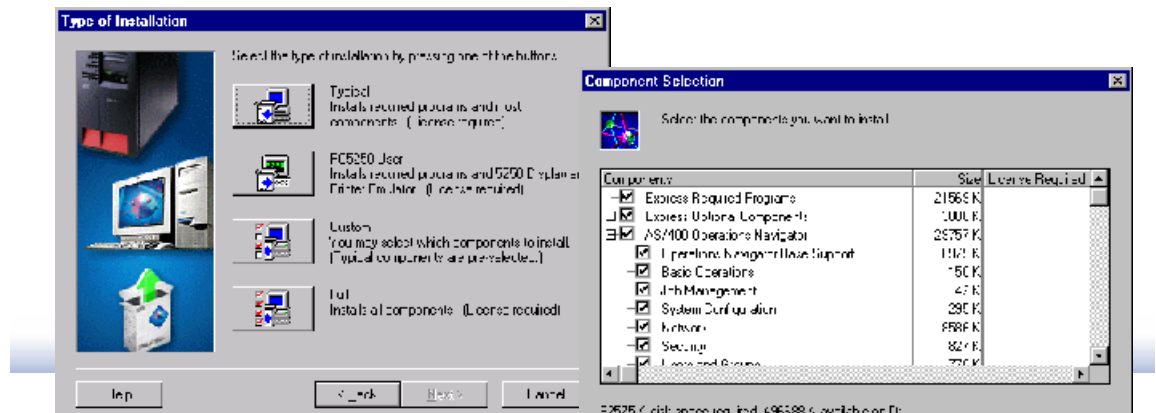
**IBM @server. For the next generation of e-business.**

# Install and Update

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

## Controlling Install

- **Limit access to functions by limiting what is installed** IBM @server iSeries
- **If users can access the "full" install image, they can install undesired components.**
  - Users can run Selective Setup
- **For multi-user PCs it may be desirable to allow some users to use a given function, but not to allow others to do so.**
  - This is especially true in a Windows Terminal Server scenario.
- **Control access to file share QIBM**
  - NetServer ships with QIBM as a file share that everyone can use
  - You can control access to the file share





## Client Access Policies

IBM  server iSeries

- **Microsoft System Policies can restrict installation/removal of iSeries Access for Windows components and subcomponents**

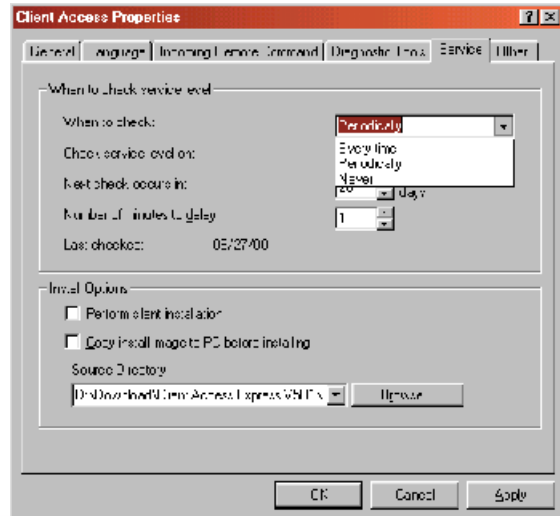
- **Policies can also be used to control which install related functions can be run.**

- **Install**

- Can restrict Setup, Selective Setup, upgrades, etc.
- Can restrict individual install options
- Can restrict iSeries Navigator and iSeries Navigator subcomponents.
- Can restrict iSeries Navigator plug-ins.

- **Service**

- Can mandate location of selective setup and install service pack
- Can prevent SP installs and SP level checking
  - ▶ Not recommended!
- Can mandate service pack level checking values in the iSeries Access Properties panels.



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

## Policy Files

IBM  server iSeries

- **Created by the administrator**

- **Stored on a file server accessible to the clients to be administered such as:**

- NetServer
  - ▶ Instructions for creating a share for policy downloading are in the Setup guide.
- NT IPCS
  - ▶ Comes with a 'Netlogon' share already configured. PC's will download policies automatically from this share.
- NT Server
  - ▶ Also comes with a 'Netlogon' share.

- **Can be applied to users or computers in a network**

- **Are binary files which can only be manipulated using the System Policy Editor from Microsoft**

- Note: The binary formats differ between Windows 95/98 and Windows NT/2000

- **Policy templates determine what the administrator sees when editing a policy file**

- **How policies work:**

- Client PCs download a policy file from a file server at Windows login time
- Policies from downloaded file are set in the PC registry
- PC program examines and uses these registry values if present

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

## Policy Templates

IBM @server iSeries

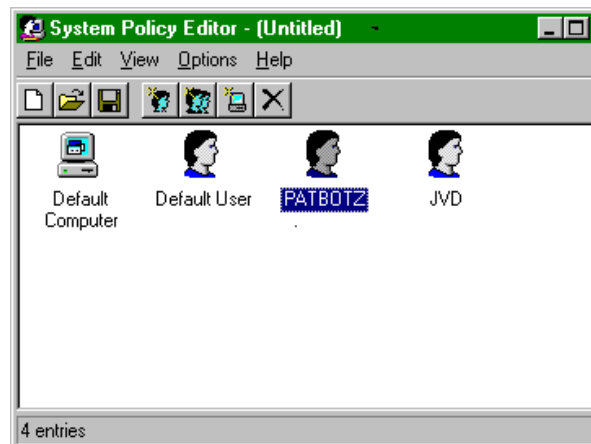
- **The policy editor uses policy templates to present the administrator with a GUI interface for editing policy files.**
  - Templates are shipped by Microsoft with Windows 95, 98, and NT/2000 for controlling many PC operating system functions.
  - Office 97 also ships policy templates.
  - Policy templates for iSeries Access for Windows can be created by running cwbadgen.exe

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

## System Policy Editor

IBM @server iSeries

- **System Policy Editor**
  - Provided by Microsoft for manipulating policy files
- **Available from many sources:**
  - Windows 98 install CD
  - Windows NT Server install CD
  - Microsoft Web Site
    - ▶ Zero Administration for Windows Kit (ZAK)
    - ▶ <http://www.microsoft.com/management>
  - Office 97 Resource Kit or later
  - Or, search for "Policy Editor" or poledit.exe

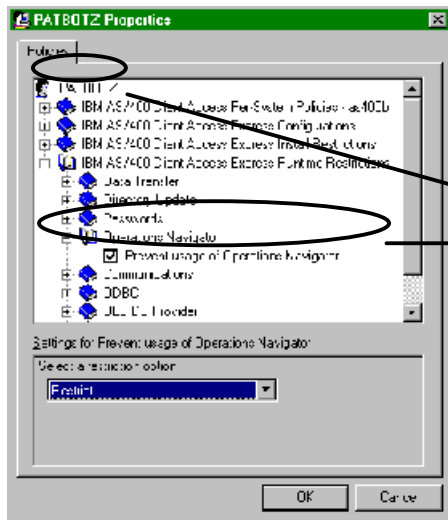


IBM @server. For the next generation of e-business.

# System Policy Editor

IBM  server iSeries

Double clicking on one of the user icons reveals the iSeries Access for Windows policies...



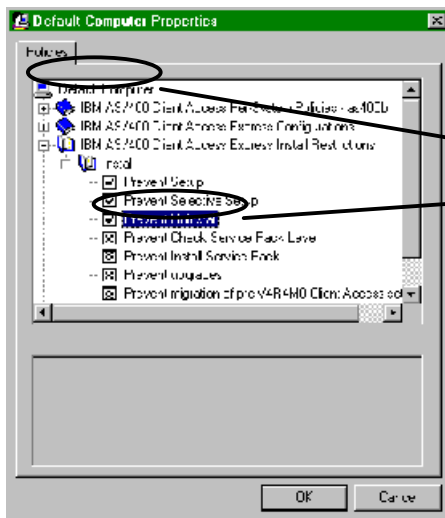
Policy for specific user PATBOTZ is not to allow him to use iSeries Navigator...

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

# System Policy Editor

IBM  server iSeries

Double clicking on the default computer icon reveals the Client Access policies...



Policy for default computer is to not allow iSeries Access for Windows to be uninstalled...

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

## Examples of iSeries Access for Windows Policies

IBM @server iSeries

- **Install**
  - Restrict Setup, Selective Setup, upgrades, etc..
  - Restrict individual install options
  - Restrict iSeries Navigator and iSeries Navigator sub-components
  - Restrict iSeries Navigator plug-ins
- **Passwords**
  - Prevent changing of OS/400 passwords
  - Prevent caching of OS/400 passwords (95/98 only)
  - Set password expiration warning values
- **Data Transfer**
  - Prevent uploads or downloads
  - Prevent a user from creating a new file but allow the user to append data to an existing file.
  - Restrict a user to running only configured requests. The user would be permitted to click on a desktop icon to initiate a preconfigured transfer request, but would not be able to change the request or to create a new one.
  - More effectively 'control' which can be used, such as the ability to run batch uploads/downloads, GUI uploads/downloads, autostart uploads/downloads, use Excel add-ins, etc..
  - Restrict which iSeries a request may be run against.
  - Prevent RTOPCBs or RFROMPCBs
- **PC5250**
  - Limit the number of PC5250 sessions a user can have active to a given iSeries.
- **Middleware**
  - Restrict iSeries ODBC driver or OLE DB usage on a per-iSeries basis.
  - Control use of Remote Command functions
- **Connections**
  - Preconfigure iSeries system connectivity; then when a user starts a Client Access function only the preconfigured system would be available for use
- **SSL**
  - Define policies by connection environment. For example, when a user is connecting from the 'home' environment, SSL is required, however when using an 'office' environment SSL is not needed.
- **Directory Update**
  - Prevent usage of update
- **Service**
  - Mandate service pack level checking values which show up in the Client Access Properties panels.
  - Mandate location of where selective setup and install service pack come from.
  - Prevent SP installs and SP level checking
    - ♦ Not recommended!
- **iSeries Navigator**
- **and much more...**

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

## Application Administration

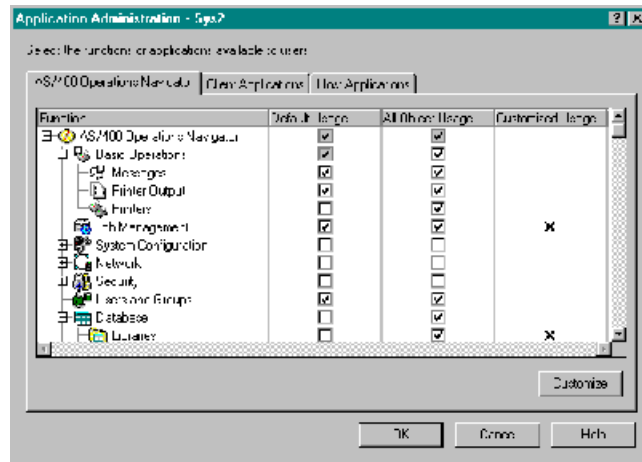
IBM @server. For the next generation of e-business.

## Application Administration

IBM  server iSeries

### ● What does it do?

- Provides ability to control access to two types of functions:
  - Specific application interface functions (iSeries Navigator Components)
    - ▶ Simple allowed or not allowed settings.
    - ▶ Similar to limited capability for PC5250 interfaces
    - ▶ for iSeries Access for Windows functions, restrictions can optionally be stored on a central iSeries.
  - Advanced features - used by iSeries Access for Windows for complex access settings.
    - ▶ Similar to using Windows Policies.
    - ▶ Stored on a central iSeries.



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

## Application Administration

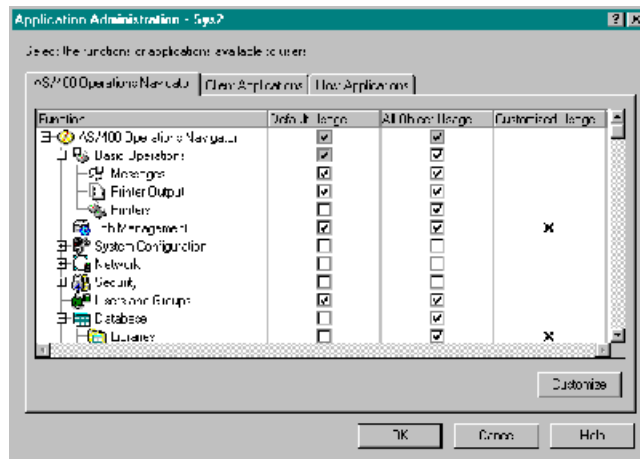
IBM  server iSeries

### ● When do you use Local App. Admin. settings?

- To control what functions users see in iSeries Navigator or iSeries Access for Windows on a per iSeries basis.
- When you want access restrictions tied to the iSeries user profile - not the PC used.

### ● When do you use Central App. Admin. Settings

- To control what functions users can access in iSeries Access for Windows regardless of the iSeries being accessed
- When you want to use Advanced App. Admin. settings to control iSeries Access configurations.



### ● When do you use Advanced App. Admin. Settings?

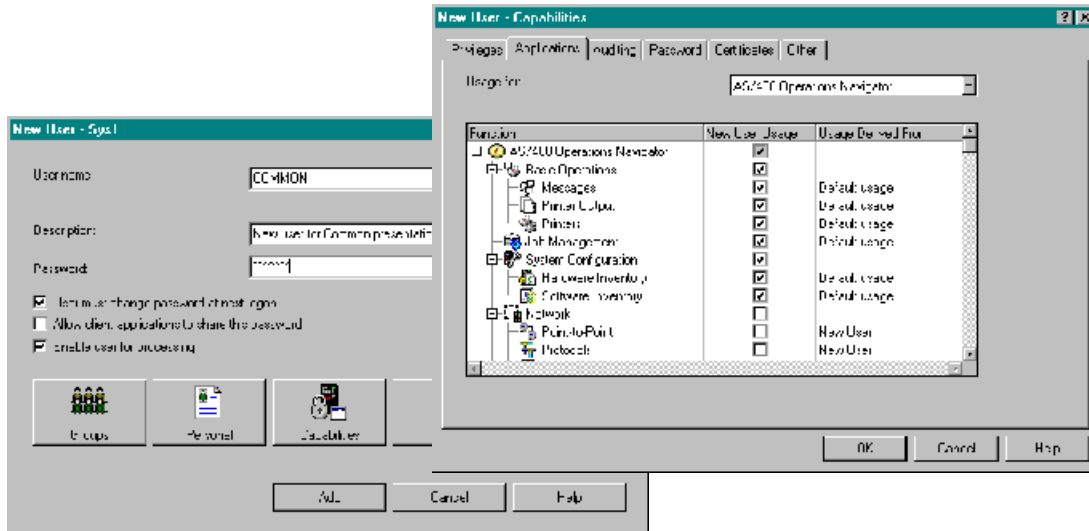
- When you want to control complex features of iSeries Access for Windows.
  - ▶ Require SSL connections
  - ▶ Restrict which systems show up in iSeries Navigator, etc..



## Application Administration - Local Settings

IBM  server iSeries

- Set up individual users with more or less iSeries Navigator access
- Go to User properties--Capabilities, and use the Applications tab to give or take away access to iSeries Navigator functions



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

## Notes: Application Administration

IBM  server iSeries

**Default Access.** The Application Administration menu option available on each iSeries system allows you to set up the default access scheme for iSeries 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 all but those users with \*ALLOBJ (all object) privilege.

**Individual Access.** An individual user can then be given more or less access. View the individual's user properties under "Users and Groups," push the "Capabilities" push button (this was called "Security" in previous releases), and click on the "Applications" tab in the Capabilities dialog. This dialog shows you if the user currently has access to each subcomponent of iSeries Navigator, and from where the usage is derived--the default access scheme, \*ALLOBJ privilege, membership in a group that has explicit access, or explicit user access.

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

## Notes: Central Settings - Policy Support

IBM  server iSeries

### ● *Application Administration Central Settings - Why do we have these?*

iSeries Access for Windows has used "Windows' Policies" for several releases to allow administrators to configure client PCs from a central server:

- *Administrators can restrict users from specific iSeries Access functions. For example, an administrator can prevent a user from using iSeries Access's Data Transfer functions.*
- *Administrators can configure several iSeries Access attributes. For example, an Administrator can define the signon attributes used by an iSeries Access user.*

iSeries Access for Windows still supports its "Windows' Policies" in V5R2, but this support has always been very difficult and complex for administrators to configure and manage and is seldom used by our customers. For that reason, Application Administration was enhanced in V5R2 to provide support for most of the function supported by "iSeries Access for Windows" Policies templates. This new support is referred to as "Central Settings" in Application Administration.

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

## Notes: Application Administration

IBM  server iSeries

### *New Application Administration Concepts for V5R2*

In order to support the functionality previously only available via "iSeries Access for Windows" Policies templates, Application Administration introduced several new concepts in V5R2:

**Administration System:** The "Administration System" is any V5R2 or later iSeries that has been configured to serve "Central Settings" to client PCs. By default, all iSeries are configured to not be an "Administration System".

**Local Settings:** Local settings can reside on any iSeries and were the only type of administrative settings supported by Application Administration prior to V5R2. They are called "local settings" because each iSeries maintains its own set of Application Administration settings. When an iSeries Access for Windows client accesses multiple iSeries servers, it will use a different set of local settings for each server.

**Central Settings:** Central settings are new in V5R2 and can only be supported by V5R2 or later iSeries servers that are configured as an "Administration System". Only V5R2 or later iSeries Access for Windows clients will retrieve central settings from an "Administration System". The central settings affect iSeries Access for Windows properties that apply to all iSeries servers that the client may access. The main difference between "Central Settings" and "Local Settings" is that the central settings are retrieved from a single central server, while local settings are retrieved from each iSeries being accessed by the PC.

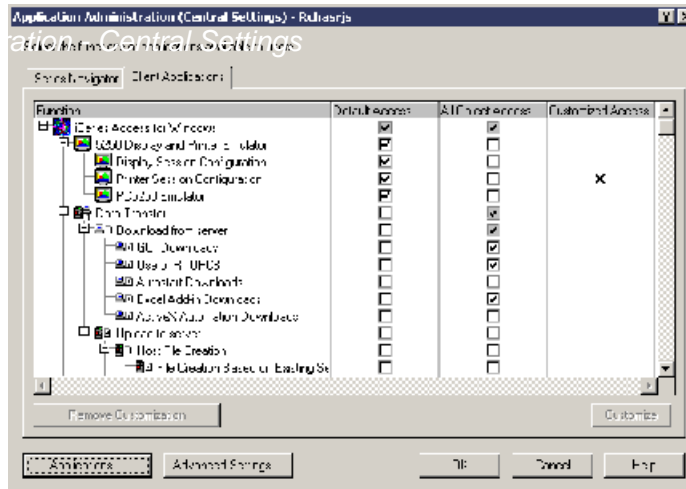
IBM  server. For the next generation of e-business.

## Application Administration - Central Settings

IBM  server iSeries

### Central Settings:

- Affect iSeries Access for Windows properties that apply to all iSeries servers that the client may access.
- Central settings are new in V5R2 and can only be supported by V5R2 or later iSeries servers that are configured as an "Administration System".
- Only V5R2 or later iSeries Access for Windows clients will retrieve central settings from an "Administration System"



More Details: [www.ibm.com/eserver/iseries/navigator/presentations.html](http://www.ibm.com/eserver/iseries/navigator/presentations.html)  
Look for "V5R2 App Admin Enhancements"

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

## Application Administration - Advanced Central Settings

Controlling Configuration Values with Advanced Central Settings

IBM  server iSeries

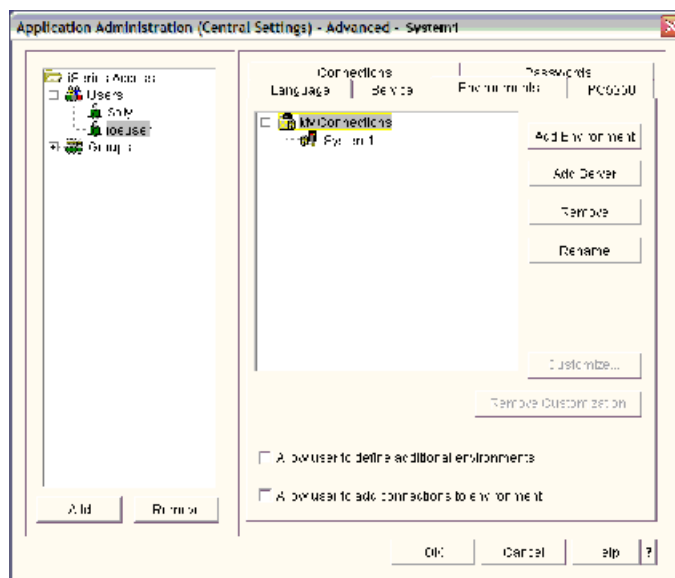
### ● Controlling System Access:

- ▶ Pre-define Environments and connections for the user.
- ▶ Can restrict users from adding or removing connections or environments - this limits what iSeries systems they can access with iSeries Navigator and Client Access Express.

### ● Controlling Other Settings:

- ▶ Require SSL connections
- ▶ Set sign-on preferences
- ▶ Set language preferences

- All advanced settings can be "suggested" - will be used by default, but can be changed by the user, or they can be "mandated" - cannot be changed by the user.



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

## Notes: Application Administration - Central Settings

IBM  server iSeries

To take advantage of the "Central Settings" support in iSeries Navigator, you will have to execute the following steps:

1. Configure an iSeries to be an "Administration System". This system will be where the "Central Settings" will be managed.
2. Register the Central Settings that you wish to manage from the "Administration System"
3. Determine the properties you wish to manage through "Central Settings" and modify them as you see fit.
4. Choose the mechanism that client PCs will use to 'discover' their "Administration System".

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

## Notes: Application Administration - Central Settings

IBM  server iSeries

### *Administration System Discovery*

Once an administrator has configured an iSeries to be an administration system, and registered and modified the central settings, the client PC (any PC with V5R2 or later 'iSeries Access for Windows' installed) must still 'discover' the administration system and use it to download its settings. The administration system that a client PC user uses as the source of its central settings is called the 'Current Administration System' of the PC user.

This client 'discovery' of its current administration system can be done in one of three ways:

- By installing from an 'iSeries Access for Windows' image that has an initial current administration system defined.
- By signing on with iSeries Navigator to an Administration system that can administer the current user (as long as the current pc user does not already have a current administration system defined).
- Manual selection of the current administration system by the client pc user.

From the client PC user's perspective, the central settings are downloaded from the user's 'current administration system using the current administration user. These values can be viewed from the "Administration System" page in "iSeries Access for Windows Properties". You can get to this page by:

- Select 'Start'
- Select "Programs-> IBM iSeries Access for Windows -> iSeries Access for Windows Properties" to launch iSeries Access properties panels.
- Select the "Administration System" page.

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

## Notes: Application Administration - Central Settings

### Administration System Discovery - Set in Install Image

IBM  server iSeries

The install mechanism allows an administrator to define the administration system (but not user) in an iSeries Access for Windows install image.

If a client PC installs using this image, the client PC will begin to use the administration system as its current administration system. The first time the client PC attempts to download the central settings from this system, the client PC user will have to specify a user, which will then be used as the current administration user.

The install image can be modified from iSeries Navigator by displaying the "Administration System" properties panel for an iSeries properties:

- From iSeries Navigator, select an iSeries and right click. Select "Properties".
- Select the "Administration System" page after the properties sheet is displayed. This will bring up the panel shown on the next page.

To alter the install image, select the "Set Installation Image Administration System" button. (Note: this button can be used to alter install images on iSeries that are NOT configured as administration systems).

**For full details on Central Settings:**  
**[www.ibm.com/eserver/series/navigator/presentations.html](http://www.ibm.com/eserver/series/navigator/presentations.html)**  
**Look for "V5R2 App Admin Enhancements"**

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

## How Application Administration works

IBM  server iSeries

- Application Administration settings are stored on the iSeries and associated with the user profile.
- PC software calls AppAdmin APIs to determine if it can perform a particular function or not.
- AppAdmin API downloads the AppAdmin data from the iSeries as needed.
- The data is cached on the PC, and updated when the AppAdmin data on the iSeries changes.
- Application Administration is built into Operations Navigator / iSeries Access.

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

## Comparing Policies and Application Administration

IBM @server iSeries

### Policy Administration

- Based on Microsoft System Policy support
- Uses Microsoft System Policy Editor and Client Access Policy templates
- Can restrict access to specific functions on a per-iSeries basis or globally
- PC driven -- not dependent on specific OS/400 release
- Can set policies on a specific PC as well as users
- Can be used to 'configure' as well as restrict functions

### The Microsoft Way...

- Preferred method for those familiar or already using Microsoft System Policies

### Applications Administration

- Based on iSeries user profiles
- Easy-to-use iSeries Navigator GUI
- User profile can roam with user (from any PC)
- A user can have different profiles for different iSeries
- Can restrict usage of particular iSeries Navigator functions
- Can also restrict iSeries Access for Windows functions like PC5250, Data Transfer, and remote command
- Can configure Policy-like restrictions for iSeries Access for Windows.
- APIs available for use by other plug-ins

### The iSeries Way...

- Preferred method for those who want to control access via iSeries user profiles

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

## Overview

IBM @server iSeries

### ● Controlling the Client

- Install/Update
- Microsoft Policies
- Application Administration
- Passwords

### ● Controlling the Connection

- Secured Sockets Layer (SSL)

### ● Controlling the iSeries

- Security Wizard
- Security Policies (system values)
- Audit Policies
- Resource Security

### ● Where to get more information

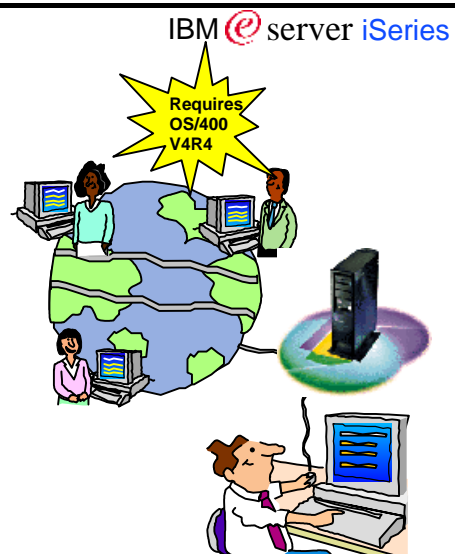


IBM @server. For the next generation of e-business.

This page is intentionally not blank.

## Secure Sockets Layer (SSL)

- **Secure communications sessions between PC and iSeries**
  - Session encrypted
  - Not subject to eavesdropping
- **Can choose which iSeries Access for Windows applications are encrypted**
  - PC5250
  - Data Transfer
  - iSeries Navigator
  - Others
- **Can assure connection is to iSeries system you expect**
  - Diminishes spoofing possibilities
- **Requires installation and configuration of both the client and server**
  - Software
  - Digital Certificates



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

## Notes: SSL

IBM  server iSeries

Originally created by Netscape, the Secure Sockets Layer (SSL) is the industry standard for session encryption between clients and servers. Data exchanged between the clients and the servers is encrypted and, therefore, not subject to eavesdropping. SSL uses asymmetric, or public key, encryption to encrypt the session between a server and client (user). The client and server negotiate this session key during an exchange of digital certificates. The key expires automatically after 24 hours, and a different key is created for each client and server connection. Consequently, even if unauthorized users intercept and decrypt a session key (which is unlikely), they cannot use it to eavesdrop on later sessions.

Additionally, the iSeries Access for Windows client uses the OS/400 Server Authentication support so users can be assured that the system they are connecting to is the iSeries system they intended to connect to. This capability diminishes the possibility of spoofing in an Internet environment.

**Q. What are the security distinctions between a client using a Secure Sockets Layer (SSL) connection and a client using a Virtual Private Network (VPN) connection, such as Layer 2 Tunneling Protocol (L2TP)? Are these connections mutually exclusive? When should you use one instead of the other?**

A. SSL connections and L2TP connections are not mutually exclusive; for example, you could have an SSL connection inside an L2TP tunnel. However, you would normally use one or the other as performance would likely be impacted by their simultaneous use.

- SSL is an application level of security; and thus requires your networking application (such as iSeries Access) to support SSL. iSeries Access for Windows fully supports SSL. If you have some data that needs to be encrypted and other data that does not, the Express client makes it easy to set up only some of its applications (for example, PC5250 and Data Transfer) to use SSL. Because SSL is usually easier and quicker to configure than L2TP, it is probably a simpler alternative if your users connect to the Internet only periodically. The iSeries Access for Windows client includes full SSL support when connecting to iSeries systems at OS/400 V4R4 or later.
- You should use VPN, which is based on industry standards such as L2TP, when you want to create a continuous, long-term connection between a client and a server. Because VPN offers many security features (such as data encapsulation, encryption, and authentication), it is a good choice for connection between servers or for virtual LANs between two networks. You can also use L2TP connection to create a secure VPN between a dial-in client and your home system via a local Internet Service Provider (ISP) instead of dialing long distance or using dedicated lines. OS/400 V4R4 supports L2TP for remote VPN connections.

**Q. Does iSeries Access for Windows support VPN (L2TP) connections?**

A. VPN connections are handled by the underlying operating systems and are actually transparent to iSeries Access, which simply uses TCP/IP to make connections.

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

## Setting Up Secure Sockets Layer (SSL)

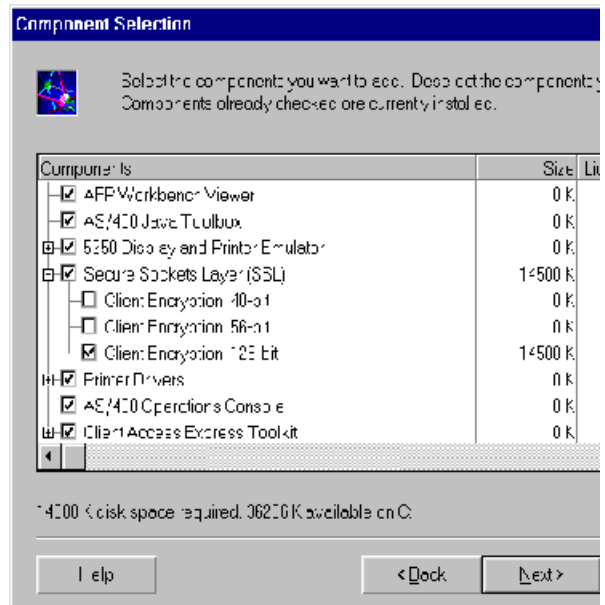
IBM  server iSeries

### ● On iSeries

- Install Cryptographic Access Provider LPP (5722-ACx)
  - ▶ AC2 = 56-bit (not in V5R2)
  - ▶ AC3 = 128-bit
- Install Client Encryption LPP (5722-CEx)
  - ▶ CE 2,3
- Authorize users to SSLxxx directory

### ● On PC

- Install client encryption (5722-CEx)
  - ▶ CE2 = 56-bit (not in V5R2)
  - ▶ CE3 = 128-bit



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

## Notes: SSL Pre-reqs

IBM  server iSeries

To use the iSeries Access SSL capability, the following licensed program products (LPPs) and options must be installed on the iSeries:

- 5722-SS1 Option 34 - Digital Certificate Manager (DCM). You need DCM to create your digital authority and to maintain your digital certificates.
  - 57229-TC1 - TCP/IP Connectivity Utilities for AS/400
  - 5722-DG1 - IBM HTTP Server for AS/400. This product is required to access DCM browser-based interface.
  - 5722-ACx - Cryptographic Access Provider. The value x determines the maximum key length permitted by cryptographic algorithms. These cryptographic products create certificate keys.
    - 5722-AC2 - 56-bit key length (not supported with V5R2 iSeries Access for Windows), 5722-AC3 - 128-bit key length
  - You now need the client counterpart for encryption. You need to install one or more the following no-charge LPPs on an AS/400. These LPPs are best installed on the same iSeries as you are using to install the Express client code (i.e., the iSeries system identified as containing the source directories for iSeries Access 'Check Service Level' to look for updates).
  - 5722-CEx - Client Encryption. The value x determines the maximum key length permitted by cryptographic algorithms. This client code can then be downloaded to user PCs running the iSeries Access for Windows client. You can install the 2 Client Encryption products on one iSeries, but you can only install one product on a PC.
    - 5722-CE2 - Client Encryption (56-bit) - not for V5R2, 5769-CE3 - Client Encryption (128-bit)
- Because of export regulations for products containing encryption technology, the 5722-CEx products are installed on the iSeries with authority set to 'PUBLIC EXCLUDE'. So before users can install any of these products on their PC, they need to be granted authority to 1 or more of the above Client Encryption products.
- For example to grant user CAROLE authority to use the 128-bit client encryption, the iSeries administrator would need to run the following command: CHGAUT OBJ('QIBM/ProdData/CA400/Express/SSL/SSL128') USER(CAROLE) DTAAUT(\*RX)
  - If you wanted to grant all users authority to install the 128-bit encryption support on their PCs, you could run the following iSeries command: CHGAUT OBJ('QIBM/ProdData/CA400/Express/SSL/SSL128') USER(\*PUBLIC) DTAAUT(\*RX)
- Now Express users can click on the 'Selective Setup' icon in the iSeries Access for Windows folder and select one of the above Client Encryption products to be installed. (Note: if you are allowing the iSeries Access 'Check Service Level' function to be used, iSeries Access will periodically download any updates that get applied to the Client Encryption products on the iSeries.) A new icon IBM Key Management is added to the iSeries Access client folder, and a new Secure Sockets tab is added to the iSeries Access for Windows Properties panel.

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

## SSL - Steps to Configuring

IBM  server iSeries

- Choose one of these techniques



### 1. Using a local Certificate Authority (CA)

- Create a local CA on your iSeries
- Create a system certificate
- Install server certificates
- Assign certificates to applications (iSeries Access Servers)
- Install the Local CA certificates
  - ▶ On your PC
  - ▶ In iSeries Access

### 2. Using a well-known Certificate Authority (CA)

- Obtain digital certificate
- Assign certificate to applications (iSeries Access Servers)
- Configure the iSeries Access functions to use SSL

For full details on configuring SSL for iSeries Access for Windows:  
<http://www-1.ibm.com/servers/eserver/iseseries/access/presentations.html>  
 Search for "Configuring the iSeries Access Servers to Use SSL"

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

## Notes: Digital Certificates

IBM  server iSeries

You need to decide what type of digital certificates you are going to use. You could choose to have an Internet Certificate Authority (CA) to issue certificates, or create your own CA and issue private certificates for your Intranet, or use a combination of Internet CAs and your own CA. Detailed information about SSL, digital certificates and network security can be obtained at these web sites:

- AS/400 Information Center web site: <http://www.as400.ibm.com/infocenter/>, select Internet and Secure Networks.
- IBM Vault Registry Software Web site: [www.internet.ibm.com/commercepoint/registry/](http://www.internet.ibm.com/commercepoint/registry/) provides more information about security and trust on the Internet.
- Internet Engineering Task Force: <http://www.ietf.org/> provides information on updates to the standards for certificates.
- VeriSign Information Desk: [http://digitalid.verisign.com/info\\_ctr.htm](http://digitalid.verisign.com/info_ctr.htm) provides more information about using digital certificates on the Internet.

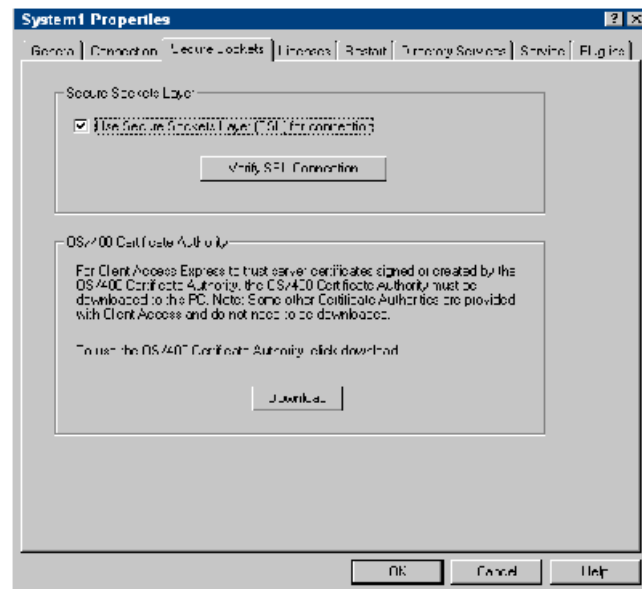
IBM  server. For the next generation of e-business.

## Configure Secured Sockets Layer (SSL)

IBM  server iSeries

### • Security Properties

- First, obtain a certificate and perform additional steps for recognizing a local CA, if appropriate
- Next, set the "Use SSL" checkbox in the system "Properties" dialog in iSeries Navigator to use SSL for connections between this client and the iSeries for iSeries Navigator functions.
- That's it!!!



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

## Overview

### ● Controlling the Client

- Install/Update
- Microsoft Policies
- Application Administration
- Passwords

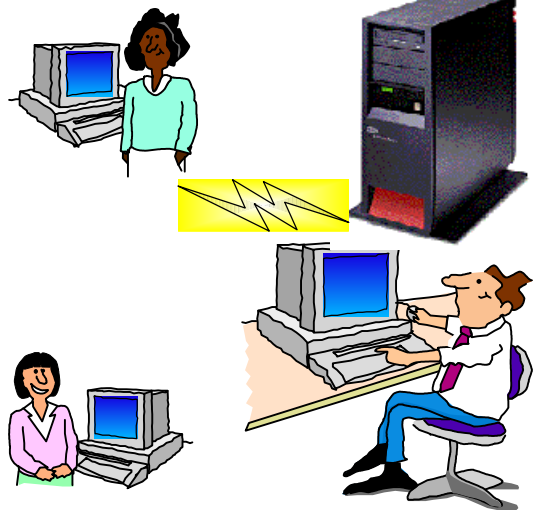
### ● Controlling the Connection

- Secured Sockets Layer (SSL)

### ● Controlling the iSeries

- Security Wizard
- Security Policies (system values)
- Audit Policies
- Resource Security

### ● Where to get more information



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

## Isn't that enough?

IBM @server iSeries

Isn't controlling iSeries Navigator and the connection enough?

- NO!
- You are not protected from
  - Programs using ODBC (e.g. Microsoft Excel, Lotus 123)
  - FTP
  - Other client server applications

Only complete solution is using iSeries object level security.

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

This page is intentionally not blank.

## Security Wizard

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

## Security Wizard

- **Configure security using the Security Wizard**
- **Advises on security system values based on how you use your system**

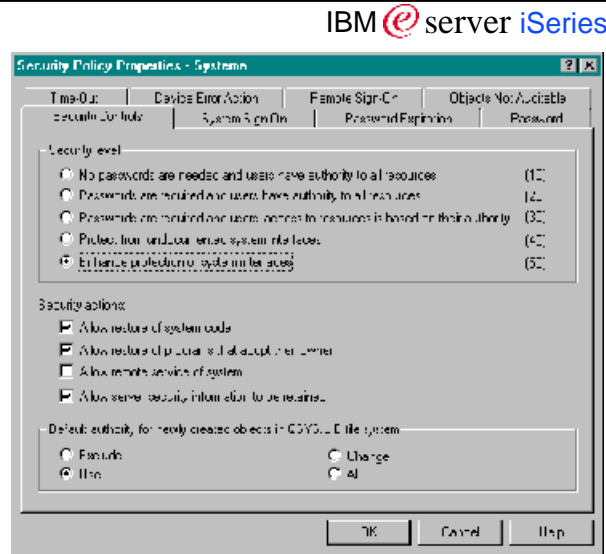
The screenshot displays three overlapping windows from the AS/400 Security Wizard. The top window is a question dialog: "Is your AS/400 directly connected to the Internet or a network that is connected to the Internet?" with radio buttons for "Yes" and "No". Below it is a "Welcome to the AS/400 Security Wizard" window with a "Next" button. The bottom window shows the "AS/400 Operator's Navigator" interface with a tree view of system components. The "Security" component is selected, and a context menu is open with "Configure" highlighted. The IBM @server logo is visible at the bottom of the interface.

## Security and Auditing Policies (System Values)

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

## Security Policy Properties

- **Access security policy settings via properties**
- **Administer security system policy on a single iSeries**
  - ▶ Security related system values and network attributes
  - ▶ Copying to another iSeries not supported
  - ▶ \*ALLOBJ and \*SECADM special authorities required for most settings



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

## Notes: Security Policies

IBM e server iSeries

The Security Controls window shows the system values that control the level of security on the AS/400. It consists of the following system values:

QSECURITY - the values listed correspond to security levels 10 - 50  
 QALWOBJRST  
 Allow restore of system code - \*ALWSYSSTT  
 Allow restore of programs that adopt authority - \*ALWPGMADP  
 QRMTSRVATR - allow remote service of system  
 QRETSVRSEC - allow server security information to be retained  
 QCRTAUT - default authority for newly created objects

The following system values are administered on the other properties pages:

Device Error Action - QDEVRCYACN - no special authority required to change this sysval  
 Password Expiration - QPWDEXPITV  
 Password Rules - QPWDMINLEN, QPWDMAXLEN, QPWDRQDDGT, QPWDLMTCHR, QPWDLMTREP, QPWDLMTAJC, QPWDRQDDIF, QPWDPOSDIF, QPWDVLDPGM  
 System sign-on rules - QMAXSIGN, QMAXSGNACN, QDPSGNIINF, QLMTSECOFR, QLMTDEVSSN, QAUTCFG, QAUTOVRT  
 Time-out - QINACTIV, QINACTMSGQ, QDSCJOBIV  
 Remote sign-on control - QRMTSIGN  
 Objects Not Auditable - QALWUSRDMN  
 Functions not supported:  
 Setting security policy for Application Access, such as Client Access/400, DDM, FTP, etc.  
 Copy Security Policy from one AS/400 to another

A check is done before displaying the first properties page. If the user is not authorized to change a value, that value is grayed out. Anyone that has at least \*USE authority to the DSPSYSVAL command can display these settings.

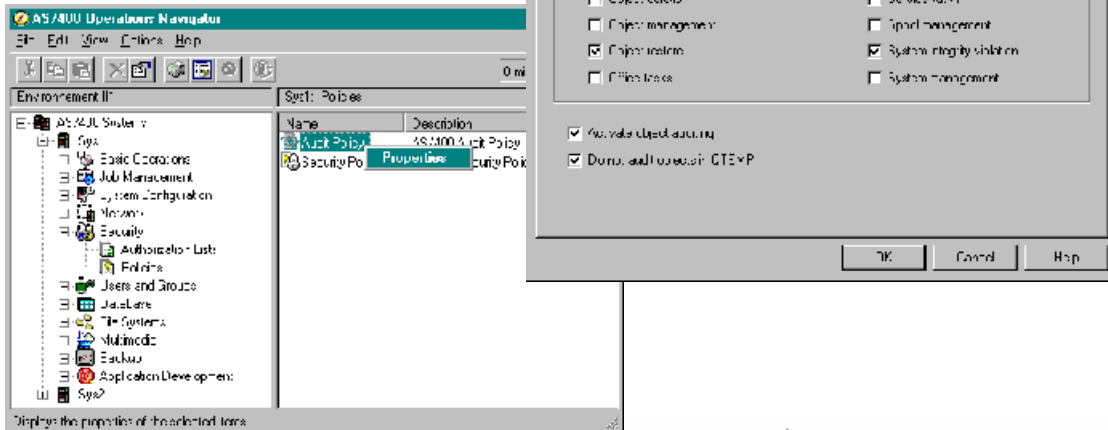
IBM e server. For the next generation of e-business.

## Audit Policy

- **Administer iSeries auditing functions**

- ▶ Specific users
- ▶ System values

- **Special authority \*AUDIT needed**



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

## Notes: Auditing Policies

IBM @server iSeries

The Properties page for System Auditing reflects the following system values:

QAUDCTL \*AUDLVL - Activate action auditing  
 QAUDLVL - List of actions to audit  
 QAUDCTL \*OBJAUD - Activate object auditing  
 QAUDCTL \*NOQTEMP - Do not audit objects in QTEMP

The New Objects tab allows to set the default auditing for newly created objects. This properties page represents the system value QCRTOBJAUD.

Special authority \*AUDIT is required to change these system values.

Functions not supported:

- Auditing a specific object
- Setting Audit values for objects
- View Audit Log/Generate reports from Audit Log (use Display Journal command to analyze information in QSYS/QAUDJRN)
- Copying Audit Controls between iSeries
- Setting Audit values for users (auditing based on AS/400 user profile values is supported)

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

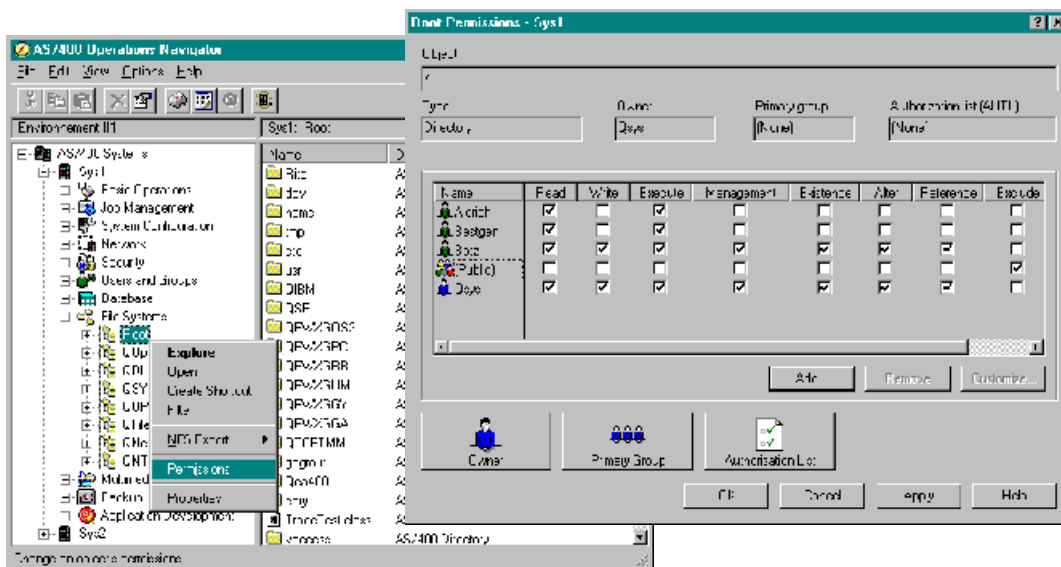
# Resource Security

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

## Permissions

IBM @server iSeries

- Set up resource security



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

## Notes: Resource Security

IBM  server iSeries

In order to change resource security, you need either special authorities, such as \*ALLOBJ, object management rights to an object, or be the owner of the object. Here are some examples:

To retrieve security information about an object, you need \*OBJMGT authority to the object.

To change the list of authorized users, you need \*OBJMGT plus any authorities being given or taken away. In addition you need \*OBJOPR if it is a \*FILE object.

To give \*OBJMGT authority to another user, you need to be the owner of the object or have special authority \*ALLOBJ.

To change the owner of a QSYS.LIB object, you need \*OBJEXIST plus \*OBJOPR if it is a \*FILE, \*LIB or \*SBSD object. To change the owner of a program, service program or SQL package that adopts its owner's authority, you need \*ALLOBJ and \*SECADM special authorities. To change the owner of a QDLS object, you need to be the owner or have \*ALLOBJ.

To change the primary group, you need \*OBJEXIST, if it is a QSYS.LIB object plus \*OBJOPR if it is a \*FILE, \*LIB or \*SBSD object. For the QDLS file system, you need either \*ALLOBJ or ownership. In addition, you need \*DLT authority to the current primary group and \*ADD to the new primary group.

The following authority checks are done before the window is displayed:

Check if the user is the owner of the object. If yes, they can change the list of authorized users. If not:

Check if the user has \*ALLOBJ authority. If yes, they can make any changes to the list. If not:

Determine what authorities the user has to the object. \*OBJMGT is the minimum authority required. Any authorities the user doesn't have to the object are shaded.

If a user does not have the required authorizations to change the owner or the primary group, these buttons are shaded.

If a user is not authorized to change the authorization list, the button is shaded.

If a user does not have \*READ authority to a library, the 'New Objects' button is shaded.

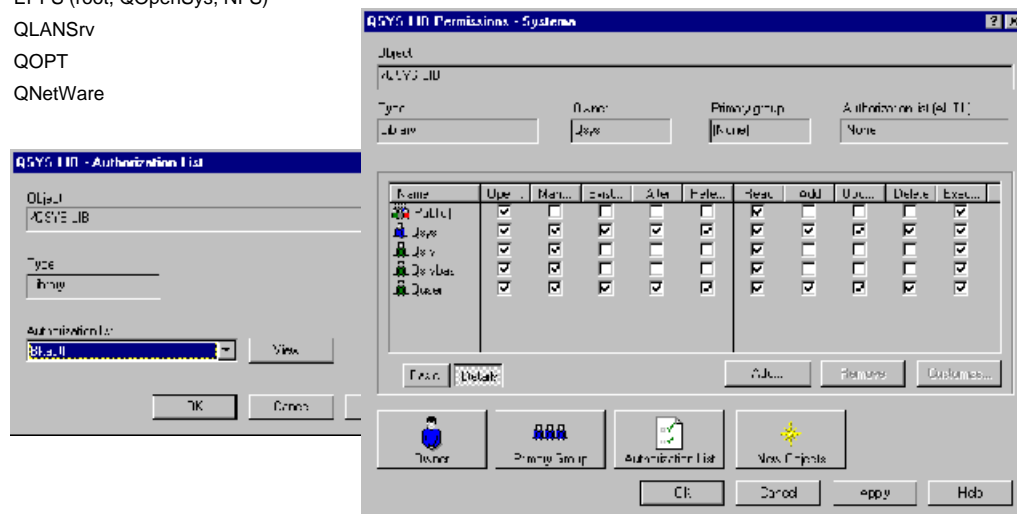
IBM  server. For the next generation of e-business.

## Resource Security

IBM  server iSeries

- **Resource Security is supported for the following file systems:**

- ▶ QSYS.LIB
- ▶ QDLS
- ▶ EPFS (root, QOpenSys, NFS)
- ▶ QLANSrv
- ▶ QOPT
- ▶ QNetWare



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

## Notes: Resource Security

IBM  server iSeries

The following functions are supported for the various File Systems:

| File System  | Change Authority | Change Auth. List | Change Owner | Change Primary Group |
|--------------|------------------|-------------------|--------------|----------------------|
| EPFS         | Yes              | Yes               | Yes          | Yes                  |
| QSYS         | Yes*             | Yes*              | Yes**        | Yes**                |
| QDLS         | Yes              | Yes               | Yes          | Yes                  |
| QLANSrv      | Yes              | No                | No           | No                   |
| QOPT         | No               | Yes***            | No           | No                   |
| QNetWare**** | Yes              | No                | Yes          | No                   |

\* Valid for all external object types except \*EXITRG and \*MEM

\*\* Valid for all external object types except \*EXITRG, \*MEM, and \*JOBSCD

\*\*\* Can change the authorization list only for the volume (first level directory after /QOPT)

\*\*\*\* QNetWare can be dynamically mounted on a directory. Therefore, we wouldn't know based on the path name that we were in the QNetWare file system. In this case, the options available would be the same as the options available to the file system that the mounted on directory is in, such as EPFS.

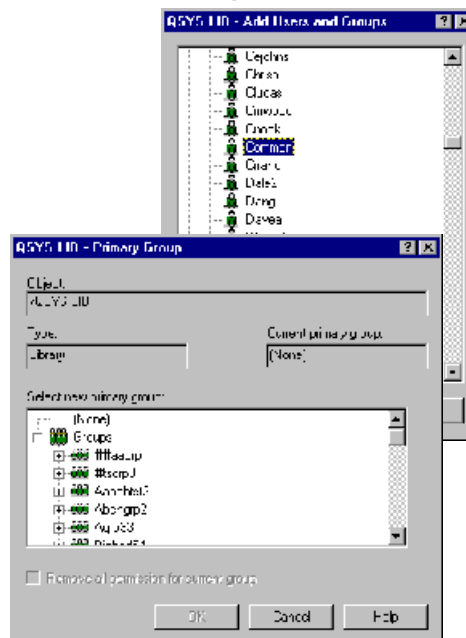
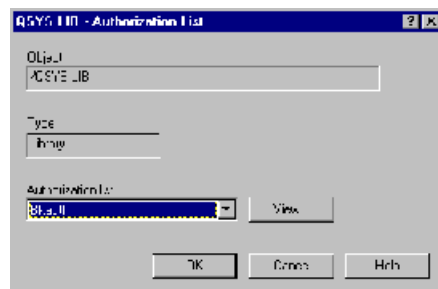
IBM  server. For the next generation of e-business.

## Resource Security - Change Access

IBM  server iSeries

- **Change resource security information, including:**

- ▶ Private authorities
- ▶ Public authority
- ▶ Owner
- ▶ Primary group
- ▶ Create and maintain Authorization lists
- ▶ Default public authority for newly created objects
- ▶ Sensitivity level for QDLS objects



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

## Notes: Change Access

IBM  server iSeries

It is very easy to change individual access rights, the authorization list, the owner, the primary group, the default public authority for newly created objects, or the sensitivity level of an object. All of these tasks can be done via the Permissions panel. Here you can select these functions via a button. If you want to add a user to the list of authorized users and groups, you simply click on the 'Add' button. Then you can display the lists of 'All Users', 'Groups', or 'Users Not in a Group'. Choose the desired user(s) from the list. In the same way you can select a new owner, an authorization list, and a primary group.

Adding a new user/group or changing a user's/group's authority is the same as command GRTOBJAUT.  
Removing an authorized user/group is the same as command RVKOBJAUT. Changing the owner of an object is the same as command CHGOBJOWN.

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

## Resource Security - Required Authority

IBM  server iSeries

- **Special authorities or object authorities required, for example:**

- ▶ \*OBJOPR for \*FILE objects
- ▶ \*OBJMGT
- ▶ \*ALLOBJ or Owner
- ▶ etc...

- **Authority checks are done before windows are displayed**

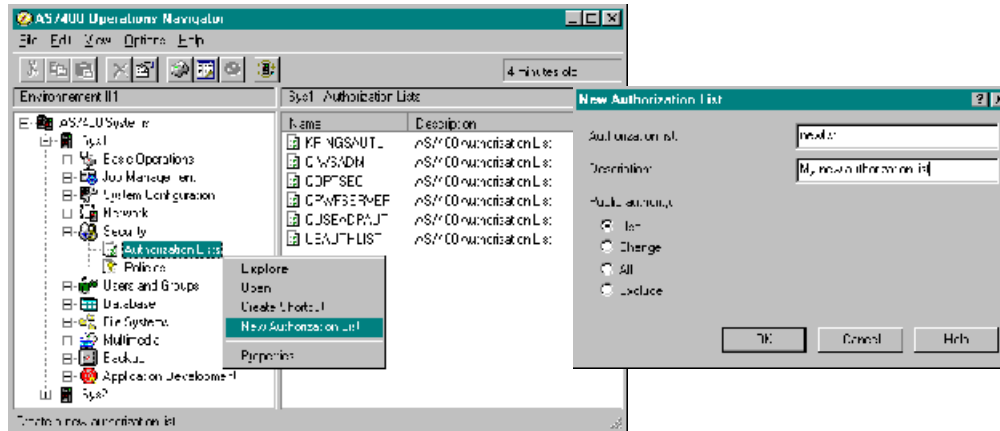


IBM  server. For the next generation of e-business.

## Authorization Lists

IBM  server iSeries

- Create and Delete
- Add, Remove or Change Users
- Change Owner and Primary group
- Display objects secured by AUTL



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

## Notes: Authorization Lists

IBM  server iSeries

A new authorization list can be created using the 'New' option from the context menu of the Authorization List folder. You can then specify a Name, Description, and the Public Authority to the authorization list. This function uses the Create Authorization List (CRTAUTL) command on the iSeries. It is also possible to delete an authorization list via the 'Delete' option of an authorization list. This is based on the Delete Authorization List (DLTAUTL) command.

The following actions can be performed on an authorization list from the Properties pages:

- Add users or groups (Add Authorization List Entry - ADDAUTLE)
- Remove users or groups (Remove Authorization List Entry - RMVAUTLE)
- Change users or groups (Change Authorization List Entry - CHGAUTLE)
- Change owner
- Change primary group

In order to perform any of the above actions, a user needs Authorization List Management Rights as well as the granted or revoked authorities.

Furthermore, a list of objects secured by the authorization list can be displayed.

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

## Overview

### ● Controlling the Client

- Install/Update
- Microsoft Policies
- Application Administration
- Passwords

### ● Controlling the Connection

- Secured Sockets Layer (SSL)

### ● Controlling the iSeries

- Security Wizard
- Security Policies (system values)
- Audit Policies
- Resource Security

### ● Where to get more information



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

## Where to Get More Information

IBM @server iSeries

- For the latest iSeries Operations Navigator information, visit:

[ibm.com/eserver/series/navigator](http://ibm.com/eserver/series/navigator)

- Includes information such as:

- ▶ Articles
- ▶ Presentations
- ▶ Demos
- ▶ Redbooks
- ▶ FAQs
- ▶ Information APARs
- ▶ And more!

- iSeries Information Center

- ▶ [ibm.com/eServer/iSeries/InfoCenter](http://ibm.com/eServer/iSeries/InfoCenter)

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

## Summary

IBM  server iSeries

### ● Controlling the Client

- Install/Update
- Microsoft Policies
- Application Administration
- Passwords

***If you can't do the function on a command line from the green-screen then you can't do it through Operations Navigator!***

### ● Controlling the Connection

- Secured Sockets Layer (SSL)

### ● Controlling the iSeries

- Security Wizard
- Security Policies (system values)
- Audit Policies
- Resource Security

### ● Where to get more information



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

## Trademarks and Disclaimers

IBM  server iSeries

© IBM Corporation 1994-2002. All rights reserved.

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 (logo) business | OS/400     |
| IBM               |            |

Lotus, Freelance Graphics, and Word Pro are registered trademarks of Lotus Development Corporation and/or IBM Corporation. Domino is a trademark of Lotus Development Corporation and/or IBM Corporation.

C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.  
 Java and all Java-based trademarks are 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.  
 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.

This document was created with Win2PDF available at <http://www.daneprairie.com>.  
The unregistered version of Win2PDF is for evaluation or non-commercial use only.