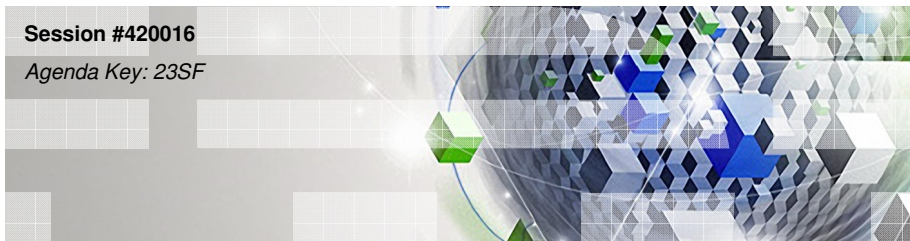


What an Administrator Needs to Know about IBM i Access for Web: Restricting Access and other Security Considerations

Speaker Name: Wayne Bowers (wbowers@us.ibm.com)

Session #420016

Agenda Key: 23SF



Power your planet.

© 2010 IBM Corporation

Agenda

- Overview
- IBM i Access for Web Runtime Considerations
 - Use of policies
 - Customizing the home page/template files
- IBM i Access for Web Environment Security Considerations
 - SSL and VPN
 - Authentication security options
 - 5250 bypass signon notes

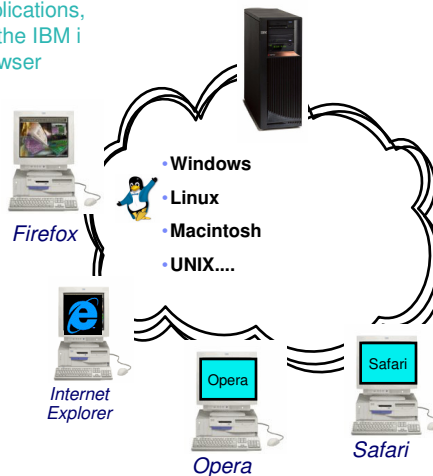
Overview



What is IBM i Access for Web?

End users can leverage business information, applications, and resources across an enterprise by extending the IBM i resources to the client desktop through a web browser

- Provides access to IBM i through a browser
 - 5250 access
 - Access to database, integrated file system, printers, output queues, jobs
 - Can run batch commands and send/receive messages
- It has the following advantages:
 - Is server based
 - Requires only a browser on the client, no configuration required at desktop, no applets installed on desktop
 - Uses industry standard protocols - HTTP, HTTPS and HTML



IBM i Access for Web Runtime Considerations



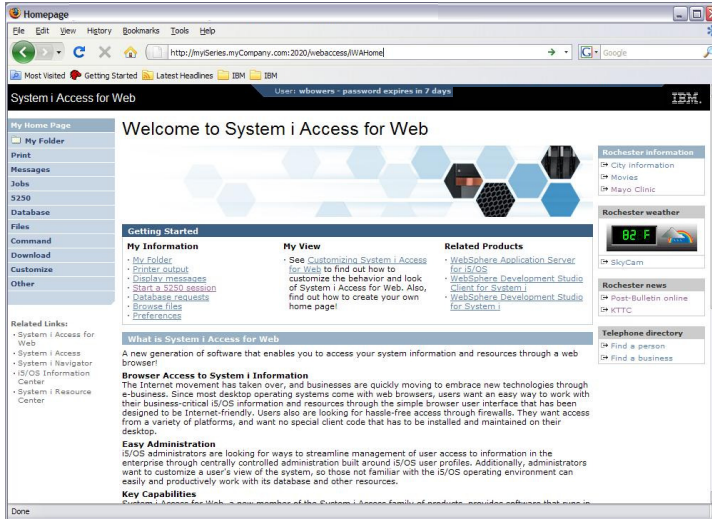
Controlling Access

3 methods to control access using IBM i Access for Web

- **Administration Policies**
 - Administrators can use the Customize function to set policies for users and groups of users.
- **User Preferences**
 - Users can set their own Preferences for things like
 - What tabs are available in the navigation bar
 - How to view output (default rows/columns per page)
 - How to filter output
- **Customize the Home page and template files**
 - Administrators can use the Customize function to replace the default IBM i Access for Web home page with their own home page.
 - Administrators can use the Customize function to replace the default template that defines the layout, look, and feel of IBM i Access for Web pages
 - Style sheets - The look of the IBM i Access for Web page content is now controlled by external style sheets.

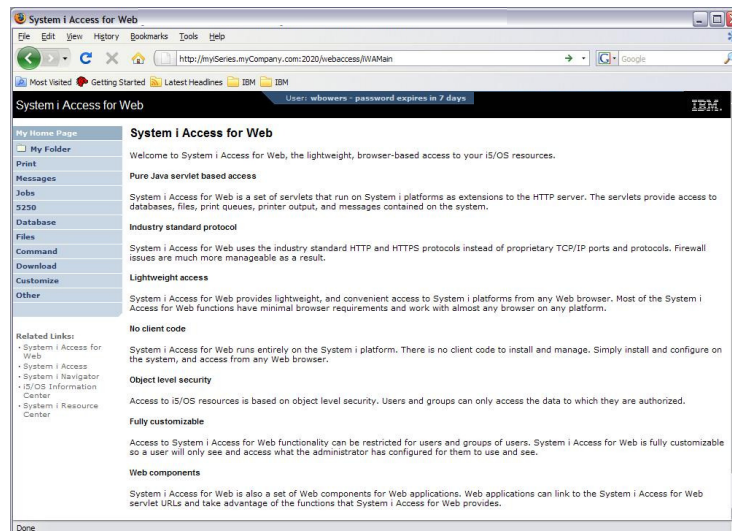
Controlling access

Home Page = <http://<myseries>:<port>/webaccess/iWAHome>



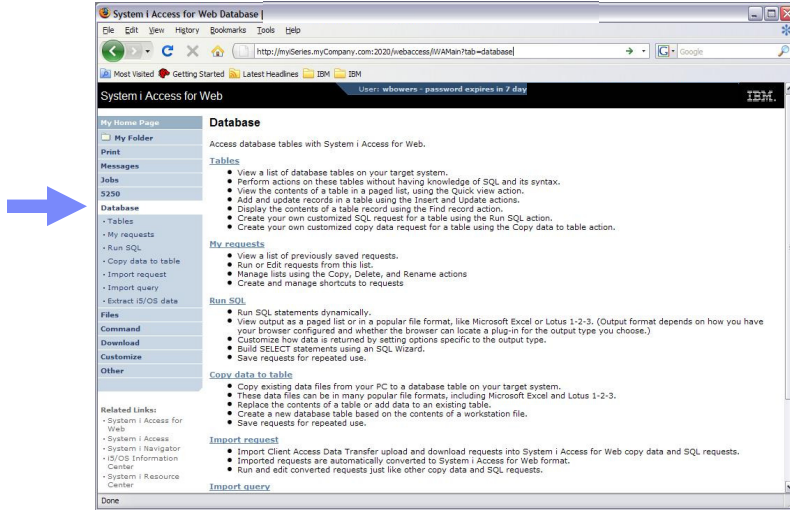
Controlling access

Main Page = <http://<myseries>:<port>/webaccess/iWAMain>



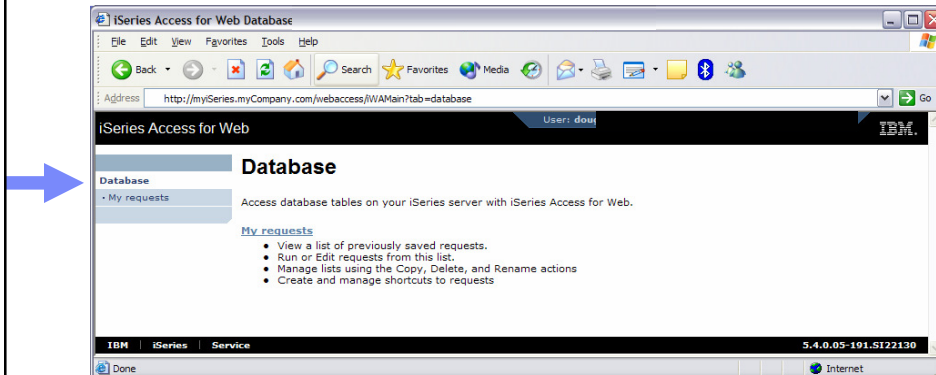
Controlling access

Product functionality



Controlling access

Sample for a user that only performs preset database queries



Controlling Access: Setting Policies



Controlling User Access

My Home Page
My Folder
Print
Messages
Jobs
5250
Database
Files
Command
Download
Customize
Other

- Customize policies for users and groups to
 - Allow/Deny functions users can access
 - Limit the information users can see
- Use group profiles to simplify policy management
 - Manage policies for group profiles
 - Add/remove users from groups
- When a function is restricted, access to the servlet is restricted
- You need *SECADM authority to customize profiles

Notes: Controlling Access - How & Whom?

- The Customize function allows administrators to set policies for users and groups of users.
- These policies control...
 - Functions a user can perform.
 - How certain information is presented to the user.
- When a function is restricted...
 - Its navigation bar content is removed.
 - Access to the servlet is restricted.
 - It takes effect immediately.
- Administrators with *SECADM special authority are automatically authorized to administer settings for users and groups of users to which they have authority.
- These administrators can then grant other user profiles permission to administer IBM i Access for Web functions.

Controlling User Access

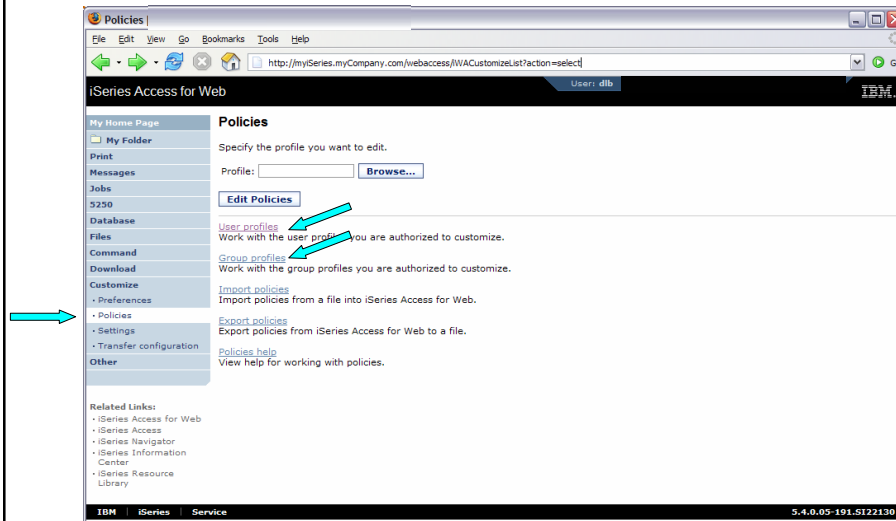
- IBM i Access for Web ships with default policy settings
- Default allows most functions to be available to all users
- Use *PUBLIC to set policies for all users
- Strategy:
 - Grant an administrator profile access to all functions
 - Deny access to all functions to *PUBLIC
 - Then allow specific users/groups access to specific functions

Action	Category	Description	Access
5250	5250	5250 user interface custom settings.	Allowed
Command	Command	Run batch command custom settings.	Allowed
Customize	Customize	Preferences and policy administration custom settings.	Allowed
Database	Database	Database tables, requests, and run SQL custom settings.	Allowed
Database connections	Database connections	Create and edit database connection definitions.	Allowed
Download packages	Download	Download packages custom settings.	Allowed
Files	Files	Integrated file system and file share custom settings.	Allowed
General	General	Page layout, language and character set custom settings.	Allowed
Jobs	Jobs	Work with jobs custom settings.	Allowed
Mail	Mail	Send mail custom settings.	Allowed
Messages	Messages	Display messages, send messages, and message queue custom settings.	Allowed
My Folder	My Folder	My Folder custom settings.	Allowed
Print	Print	Printer output, printers, printer shares and output queue custom settings.	Allowed
SameTime	SameTime	Lotus SameTime custom settings.	Allowed
Other	Other	Change password and other miscellaneous custom settings.	Allowed

Notes: Controlling Access - Strategies

- IBM i Access for Web ships with a set of default policy settings. The default policy settings allow most of the IBM i Access for Web functions to be available for all users. Without any customization, users accessing IBM i Access for Web could begin using most of the available functions.
- As an administrator of this product, you may not want your users to be able to access all of these functions. It is the responsibility of an administrator to restrict functions they do not want their users to be able to access.
- One of the quickest strategies that can be deployed to restrict a function from all users is to use the Customize Group Profiles function and customize the *PUBLIC group profile.
- This group profile is defined such that every user is a member of this group. So, for example, if you were to customize the *PUBLIC profile and set the "Browse files" and "File shares" file functions to "Deny", you would restrict file system access from this product for all users.
- If some of your users required access to this function, you could specifically customize their user profiles and set this function back to "Allow". In this way, only users that have been specifically allowed access will be able to use that function, all others would not have access.
- It should be noted that the *PUBLIC group profile includes the administrator user ID that is used to customize other group and user profiles. If you were to deny functions for *PUBLIC, this would affect the administrator user profile. As you customize IBM i Access for Web for *PUBLIC, you may want to consider specifically allowing your administrator user profile to have access so that it is not locked out of IBM i Access for Web functions.

Controlling Access - Setting policies (continued)



Controlling Access - Setting policies (continued)

Actions:
 Edit policies
 View all policies
 View group members
 Copy policies
 Reset policies

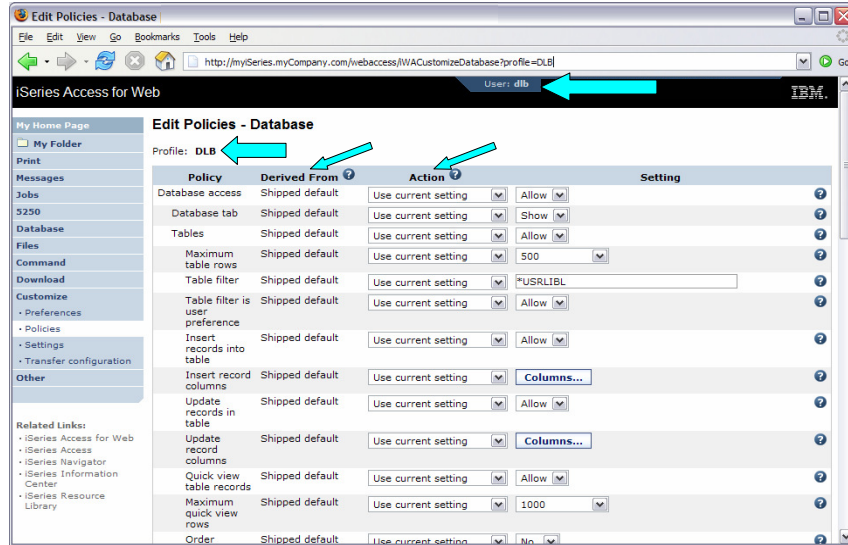
Controlling Access - Setting policies

Administrator actions on user & group profiles

Action	Description
Edit	This action is always available. Use this option to create or modify policy settings for the specified user or group profile.
View all policies	Select this action to view all of the policy settings currently being used for the profile.
View group membership	Select this action to display the Group Membership page that lists the group and supplemental group profiles (by name) the user profile has been assigned membership.
View group members	Select this action to display the Group Membership page that lists the user profiles (by name) that are currently members of the group profile.
Copy	This action is only available when the user or group profile currently has specific policy settings. It allows you to copy all of the policy settings from this profile to one or more other profiles.
Reset	This action is only available when the user or group profile currently has policy settings. It allows you to remove all of the policy settings specific to this profile.

Related Links:
 iSeries Access for Web
 iSeries Access
 iSeries Navigator
 iSeries Information Center
 iSeries Resource Library
 iSeries Help

Controlling Access - Setting policies (continued)



Controlling Access - Setting policies (continued)

Administrator Action on each policy setting

Action	Description
Use current setting	This is the default action that is pre-selected. If the setting is not modified, no action is performed. If the setting is modified, it will be added to the user or group profile record in the System i Access for Web policies file.
Apply setting to profile	Select this action to add the current setting to the user or group profile record in the IBM i Access for Web policies file. The setting will be written to the user or group profile record, even if it was not modified. You would use this action to ensure the user or group profile gets this setting. This is because a different policy setting may be used based on the user profile being a member of one or more IBM i group profiles.
Reset to default	Select this action to remove the setting from the user or group profile record in the IBM i Access for Web policies file. This option is only available if the user or group profile record currently contains a specific setting for this policy.

Controlling Access - Setting policies (continued)

The "Derived From" column (displayed when editing policy and preference settings) indicates where the policy setting that will be used for this user profile was found.

Action	Description
Profile setting	Indicates the setting is currently specific to the profile being customized. The setting had previously been applied to this profile.
Group - (groupName)	Indicates the setting is not specific to the profile being customized, but is being derived from the specified IBM i group profile and the user is a member of this group.
*PUBLIC setting	Indicates the setting is not specific to the profile being customized. No setting was found in any IBM i group profile memberships. The setting is being derived from the *PUBLIC group settings. This is a special group profile available to IBM i Access for Web administrators. All user profiles are automatically members of this special group profile. Administrators can modify this group profile to easily apply settings to all IBM i Access for Web users.
Shipped default	Indicates the setting is not specific to the profile being customized, no setting was found in any IBM i group profile memberships, or the special *PUBLIC group profile. The setting is being derived from a shipped default value.
Parent policy	Indicates the function is a sub-function of a higher level category, and its policy setting is being controlled by a top level policy setting. For example, Tables is a sub-function of Database. If Database is restricted, Tables will be restricted as well and would show its being controlled by a parent policy.

Policies Example: Simple Database User

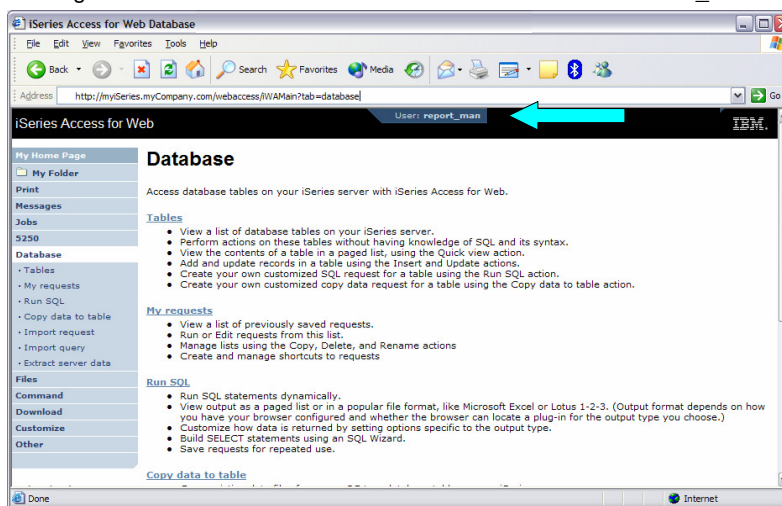


Example: Simple Database User

- The following screen shots step through setting the policies so a specific user only has the ability to run preconfigured database queries to generate reports.
- This example shows
 - the “Before” picture of what DB functions a user can perform with no customization of System i Access for Web
 - the specific database policies to set to restrict our user named REPORT_MAN
 - what general policies need to be set to restrict use of non-DB related functions by REPORT_MAN
 - The “After” picture of what REPORT_MAN can do
- When the policy is set, it takes effect immediately.

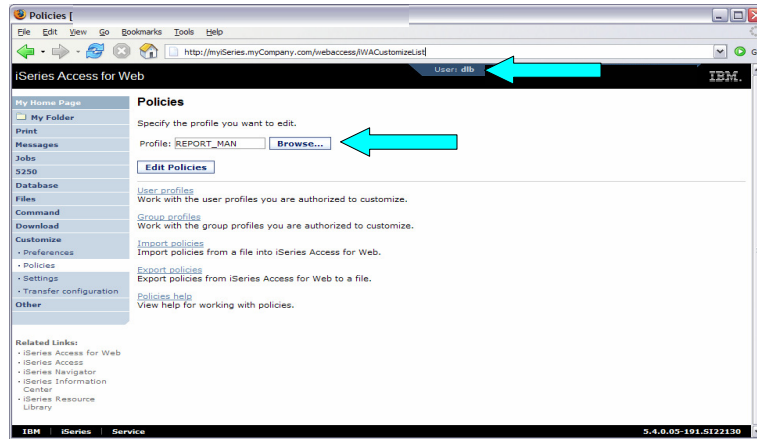
Example: Simple Database User - Before

Accessing the Database tab of IBM i Access for Web as user REPORT_MAN



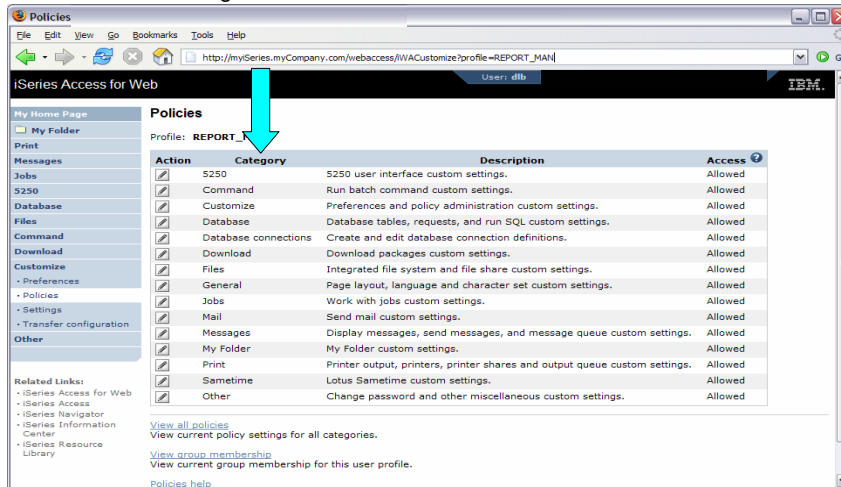
Example: Simple Database User - Policies

- Policies - the starting point for customization of a specific user or group.
- This is a new browser session, where we signed on as an administrator.



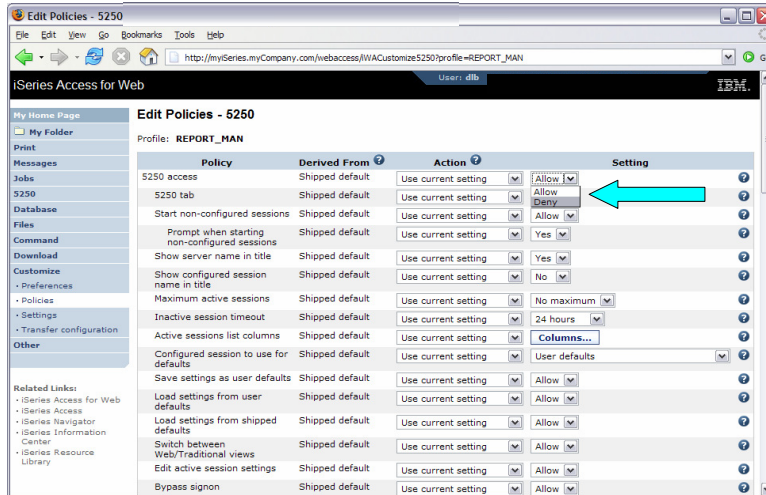
Example: Simple Database User - Categories

- Determine which categories need to be restricted/modified.



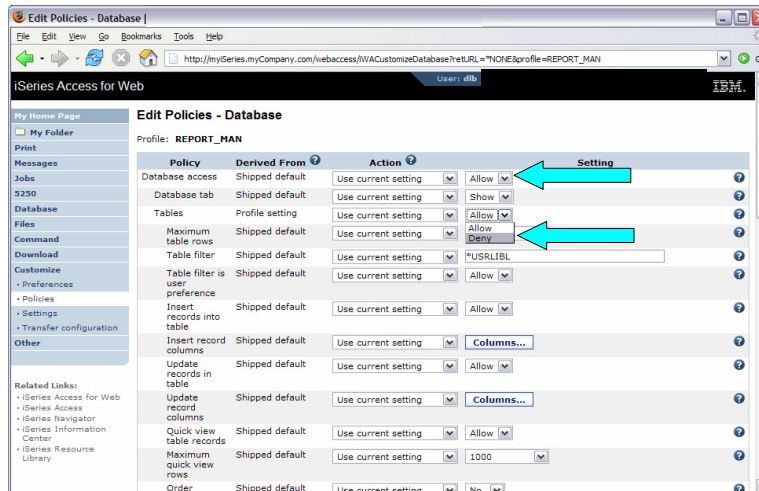
Example: Simple Database User – Other

- Turn off the other non-Database functions. Set top level to Deny.
- Repeat for each category, other than Database



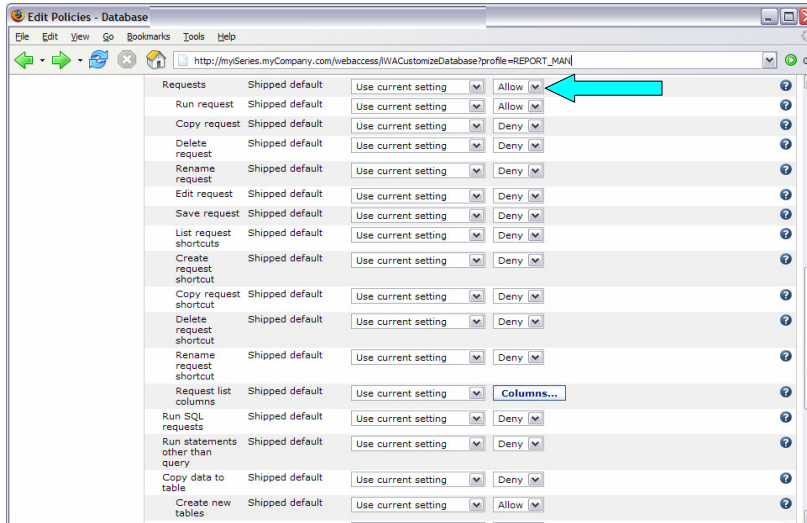
Example: Simple Database User

- Allow access to Database function.
- Set Tables policy to Deny.



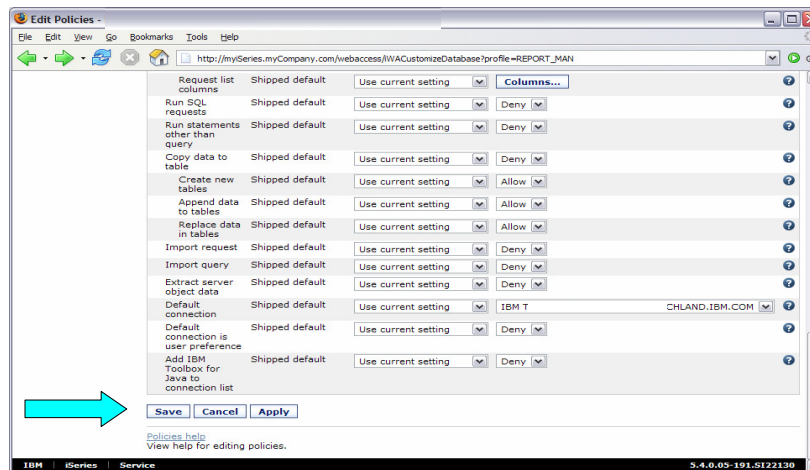
Example: Simple Database User

- Only allow the user the ability to run a saved DB request (Run request)



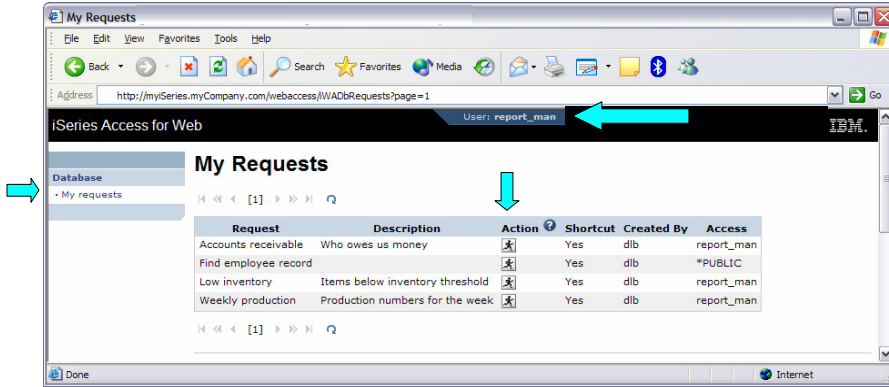
Example: Simple Database User

- Turn off the ability to perform the remaining database functions
- Save the changes



Example: Simple Database User - Completion

- The user can now only run the DB queries they have been given.



Policies Example: 5250 Access

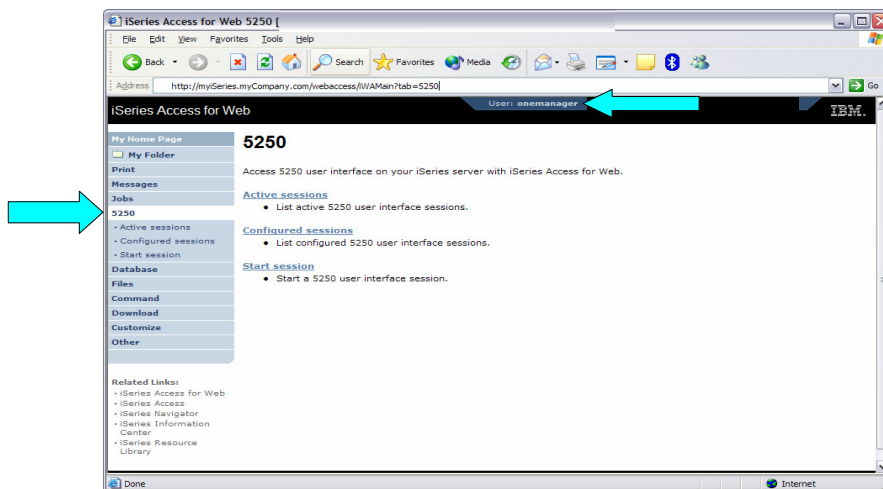


Example: 5250 Access

- The following screen shots step through setting up the items necessary to allow a group of users to use a single pre-configured 5250 session.
- In this example, ONEMANAGER is one of the user profiles in the MANAGERS group.
- This example shows
 - Creating a 5250 session and 5250 session shortcut to be used by the management team
 - Making the 5250 session shortcut the session used by the MANAGERS group profile.
 - Restricting access to other functions in System i Access for Web.
- When the policy is set, it takes effect immediately.

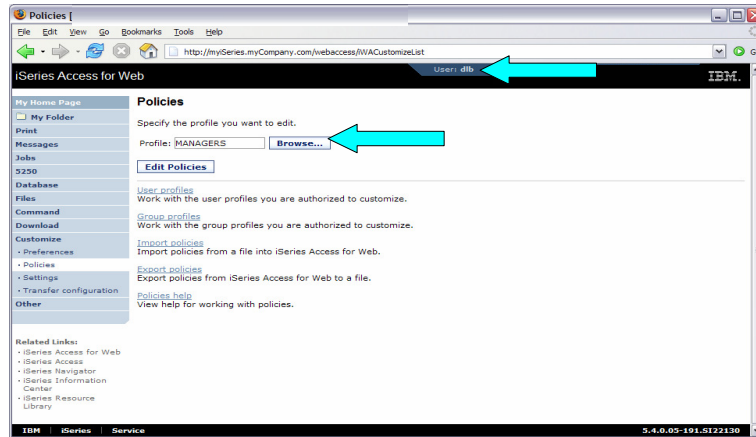
Example: 5250 Access - Before

- Access the 5250 tab IBM i Access for Web Main page as user ONEMANAGER.



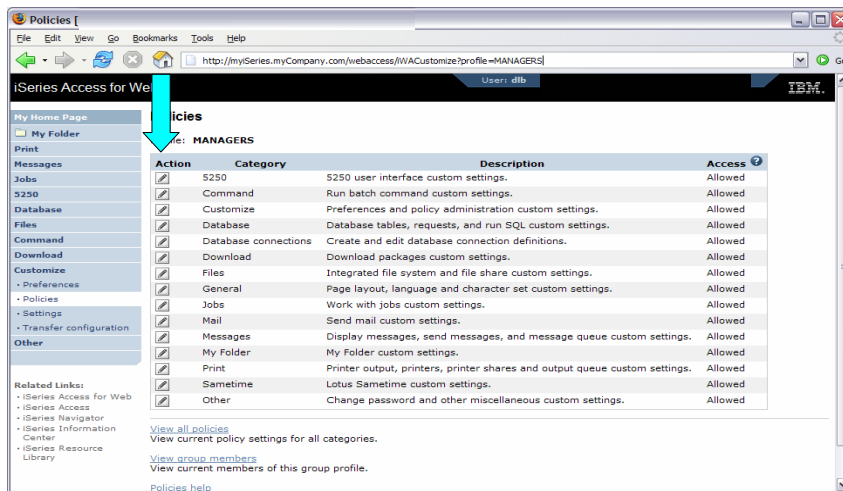
Example: 5250 Access - Policies

- Policies - the starting point for customization of a specific user or group.
- This is a new browser session, where we signed on as an administrator.



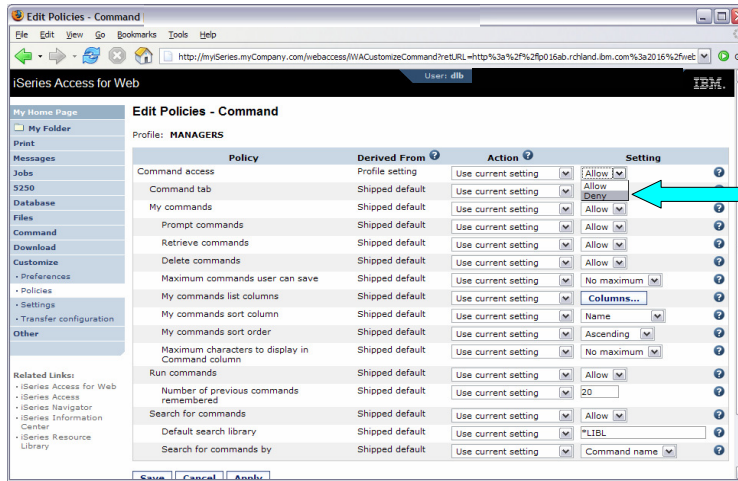
Example: 5250 Access - Categories

- Determine which categories need to be restricted/modified.



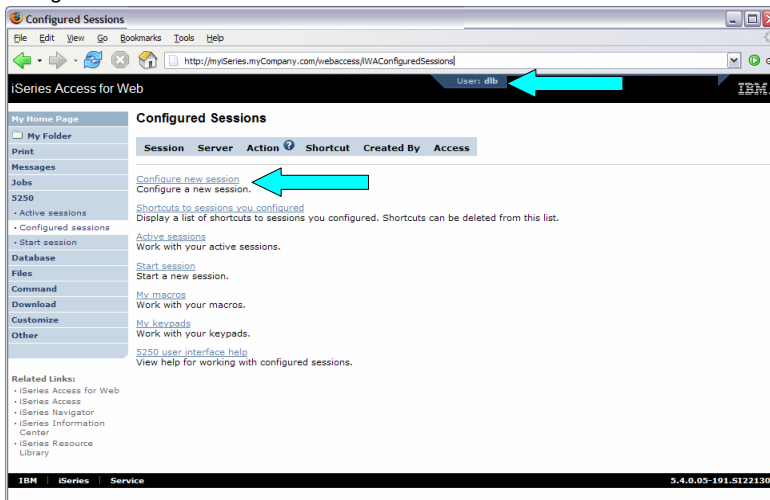
Example: 5250 Access – Other

- Turn off the other non-5250 functions. Set top level to Deny.
- Repeat for each category that should be restricted for the MANAGERS group.



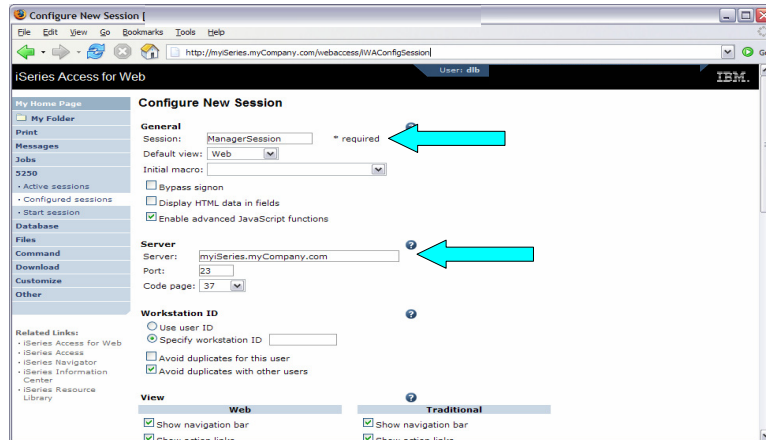
Example: 5250 Access – Functional Setup

- The administrator goes to the Configured Sessions link on the 5250 tab. Select the "Configure new session" link.



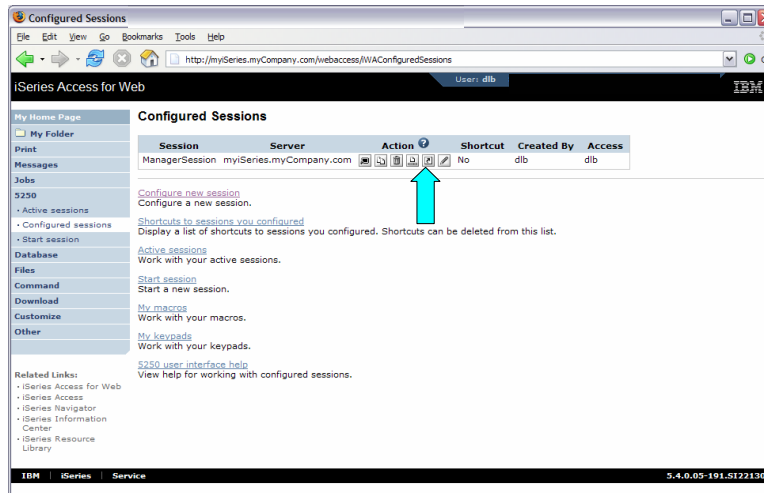
Example: 5250 Access – Functional Setup

- The administrator configures the 5250 session settings to be used by the managers.
- Settings include the server to connect to, color schemes, and many other options.



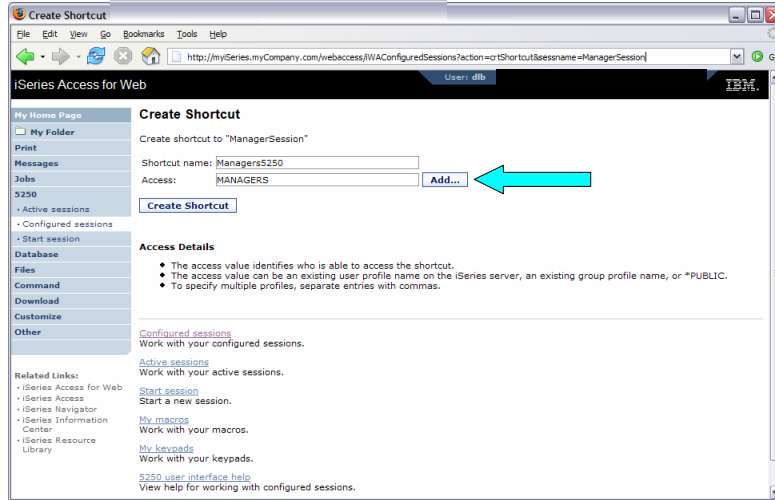
Example: 5250 Access – Functional Setup

- The saved session is only available to the administrator that is currently signed on.
- The session must be shared to the managers. Use the "Create Shortcut" action.



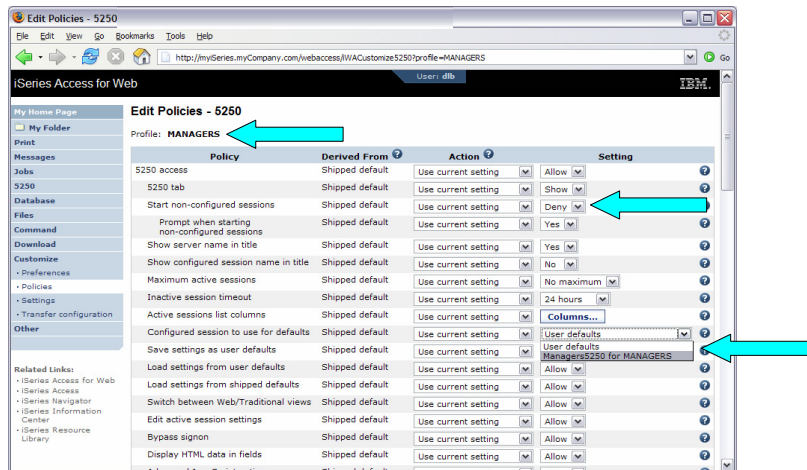
Example: 5250 Access – Functional Setup

- Name the shortcut whatever you wish.
- Session can be shared with MANAGERS group, *PUBLIC, or individual profiles.



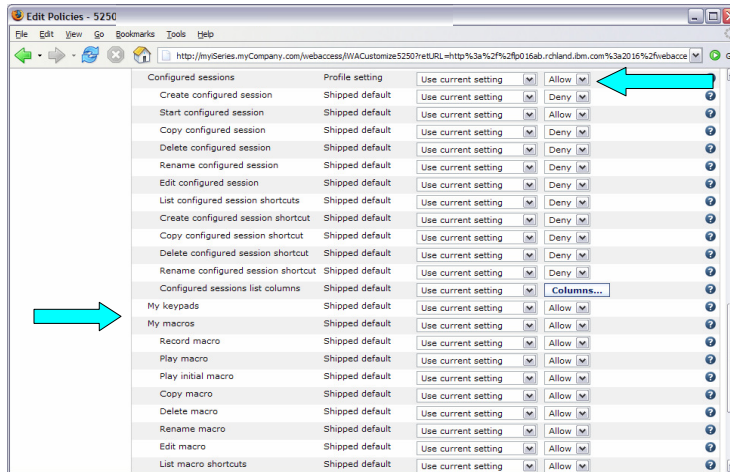
Example: 5250 Access – Back to Customize

- Go back to 5250 in Customize – Policies for the MANAGERS group profile.
- Select the shortcut to use as the default session settings for the MANAGERS.
- Select settings to lock MANAGERS out of starting/configuring new sessions.



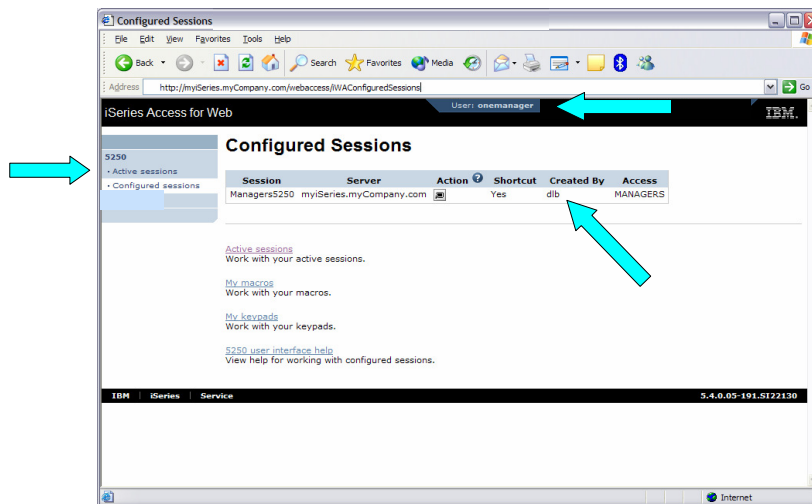
Example: 5250 Access – More 5250 Settings

- Set all 5250 policies to Deny, except Configured Sessions and Start Configured Sessions.
- You may also want to allow them to access My Keypads and My Macros.



Example: 5250 Access – After

- The managers can now only start a pre-configured 5250 session, or reconnect to an active session.



User Preferences



User Preferences

- The Preferences function allows users to customize IBM i Access for Web settings to meet their needs.
- By default, all users are allowed to modify their preferences.
- Preferences are a subset of the complete list of available policy settings.
- Users can set the following types of preferences
 - Column inclusion and ordering for functions that display output in columns.
 - Number of rows per page to display on output.
 - Show or hide navigation bar tabs.
 - Preferred language and character set.
 - Database table filters and default database connection.
 - Number of commands to save in the run command history.

User Preferences (continued)

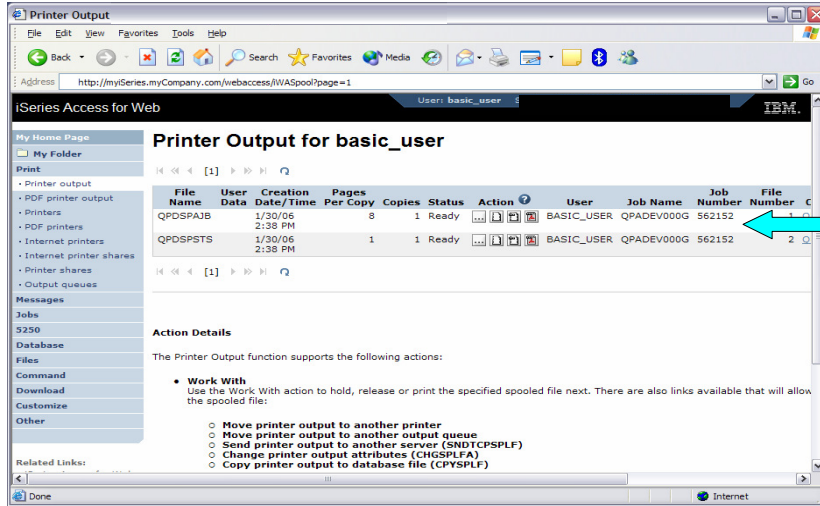
- Restricting access to Preferences
 - Administrators can deny specific users or groups from accessing their preferences.
 - This is controlled by the "Edit preferences" policy.
 - This policy is useful in organizations where administrators want to set up all customization options for users and ensure users are not able to modify any preference settings.

Example: User Preferences, Printer output

- The following screen shots step through setting a user preference for Printer output.
- This example shows
 - the default printer output page for user BASIC_USER.
 - what settings the user can modify to change the printer output page output.
 - the printer output page after user BASIC_USER modifies the preferences.
- When the preference is set, it takes effect immediately.

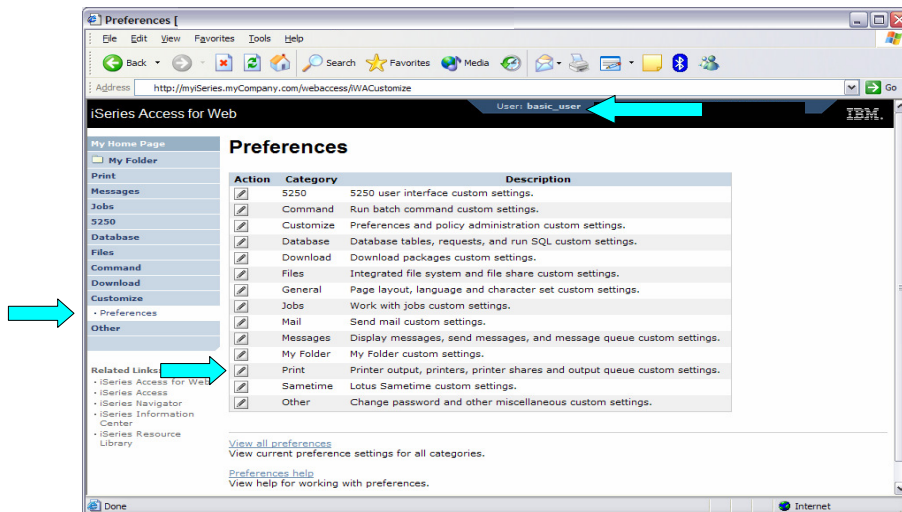
Example: User Preferences, Printer output (continued)

- The printer output display defaults with many columns of information.



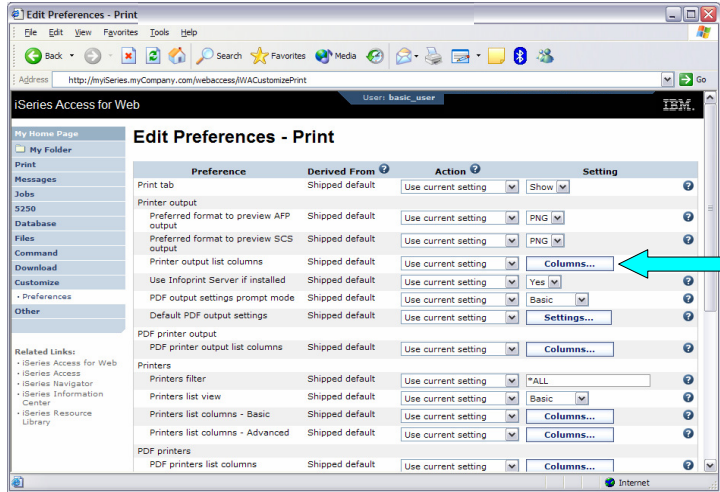
Example: User Preferences, Printer output (continued)

- Click on the Customize tab to work with Preferences.



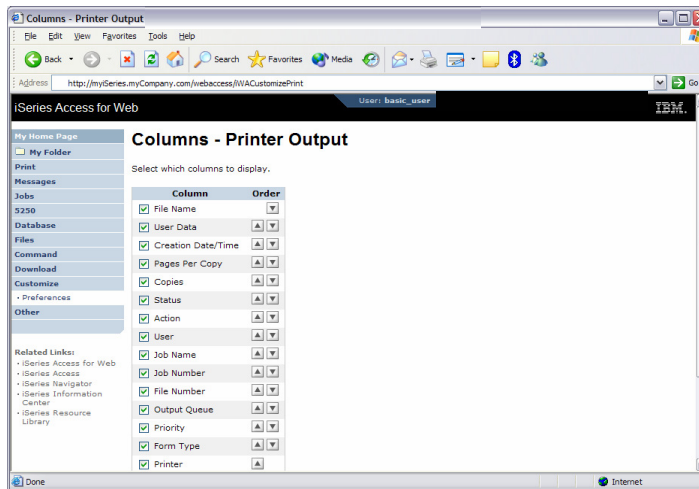
Example: User Preferences, Printer output (continued)

- Click on the Print category.
- Click on the Columns button for the "Printer output list columns" Preference.



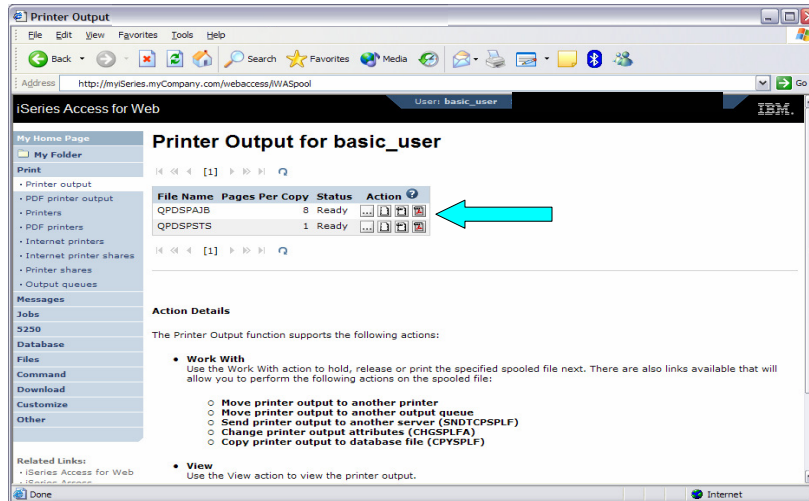
Example: User Preferences, Printer output (continued)

- The Columns displayed can be toggled off/on by checking the box.
- Click OK and Save buttons to immediately save the changes.



Example: User Preferences, Printer output (continued)

- The printer output display now only has a few columns.



Example: User Preferences, Printer output (continued)

Tips

- This example showed that a user can modify their printer output view. An administrator can:
 - Restrict the user's access to the Preferences interface.
 - Perform the same changes by setting policies for the user, or a group of users.
- The Preferences interface that the user has access to is only a subset of all the policy settings an administrator can access for the same function.

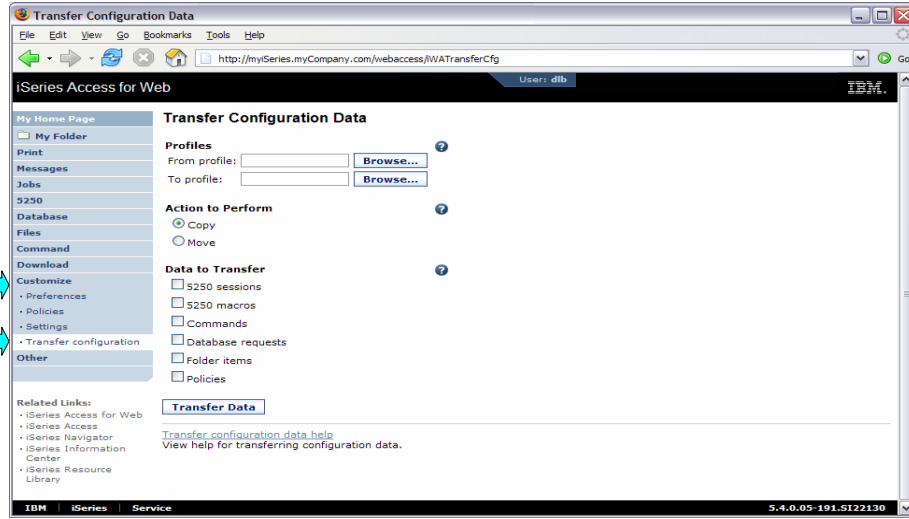
Policy Tools for Administrators



Policies and Tools

- Import/Export policy settings - export policies [to a different system](#)
 - Pick a user or group for export
- Transfer configuration data from one user to another [on the same system](#)
 - Move and copy operations supported for:
 - 5250 sessions and macros
 - Saved commands
 - Database requests
 - My Folder items
 - Policies

Transfer Configuration Data



Page Customization



Home Page Customization

- A default home page is displayed when the iWAHome servlet is invoked.
 - <http://<mySystem.myCompany.com>/webaccess/iWAHome>
 - It's a starting point to highlight functions.
 - It's an example of how to build your own home page or pages that access IBM i Access for Web functionality.
- The Customize function allows you to replace the default home page.
- Default home page replacement can be done for all users (*PUBLIC), or can be changed for only certain users and/or groups of users.
- Great article - example
 - "Build a quick and easy Web site with System i Access for Web" - Janet Weber
 - http://www.ibm.com/servers/eserver/iseries/access/pdf/build_website_article.pdf
 - Updated Oct 2006 in [System i News](#) - "Tailor System i Access for Web"

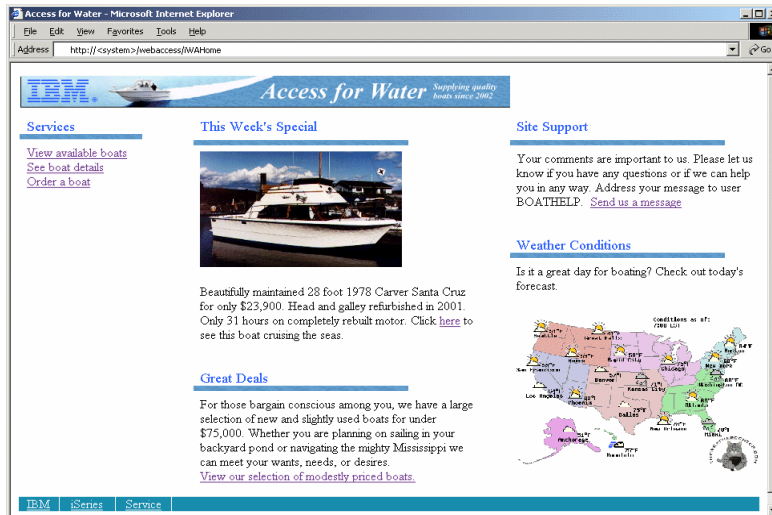
Home Page default – iWAHome servlet <http://<system>/webaccess/iWAHome>

- Change colors and banner on home page

The screenshot displays the default iSeries Access for Web home page. It features a navigation menu on the left with options like 'My Home Page', 'Messages', 'Tasks', '3270', 'Database', 'Files', 'Command', 'Download', 'Customize', and 'Other'. The main content area is titled 'Welcome to iSeries Access for Web' and includes sections for 'Getting Started', 'My View', 'Easy Administration', 'Key Capabilities', and 'Related Products'. A banner for 'Spring 2006 Conference & Expo COMMON' is visible at the bottom of the main content area. The page footer contains the text 'Power your planet.' and '© 2010 IBM Corporation'.

Home Page customization – iWAHome (another example)

- Custom home page - <http://iseriesd.dfw.ibm.com/webaccess/iWAHome>



Template file customization

- IBM i Access for Web has a default look for its functional pages.
 - This look is controlled by a template file and cascading style sheet.
- The template file has sections to specify
 - Header/footer areas of functional pages.
 - Where IBM i Access for Web content is placed in the page.
- The Customize function allows you to replace the default template file.
- Default template file replacement can be done for all users (*PUBLIC), or can be changed only for certain users and/or groups of users.



Template Customization Example

- Custom template – change banner

The screenshot shows a web browser window titled "Quick View of BOATS.BOATS [SeriesD.DFW.IBM.COM] - Microsoft Internet Explorer". The page features a custom banner with the text "Access for Water" and "Supplying quality boats since 2002". Below the banner is a "Current Orders" section with a table listing various boat models and their specifications.

BTYPE	BNAME	BFEET	BYEAR	BCOST	BNT01	BNT02
C	Poole Boat Co Aluminum	80	1979	1000000	-Located in S. Diego, CA	-Twin Detroit diesels.
P	Carver Santa Cruz	28	1978	23900	-Constructed of fiberglass.	-Single Chevy 350 gas engine, 250 hp. Fresh water cooled.
P	Mako Sportfisher	19	1989	13000	-Located in Anacortes, WA.	-Great fishing boat
P	Monk Bridgedeck Cruiser	36	1956	19900	-Built of mahogany, oak, and cedar.	-The 130 hp power plant is a single, Chrysler cyl. diesel
P	Monk Flybridge/Sedan	34	1985	55000	-Double planked cedar on oak frames.	-The 165 hp power plant is a 1985 V6 Detroit diesel
P	Monterey Marine Custom	80	1996	2975000	-Located in Stuart, FL	-Monthly payment.
S	Bill Garden Schooner	36	1953	27500	-The hull is 1/8" carvel cedar planked atop 1 1/4" x 1 1/2" oak frames	and the deck is cedar planked with tar seal



Edit Policies: specify home page and template files

The screenshot shows a web browser window titled "Edit Policies - General [SeriesD.DFW.IBM.COM] - Mozilla Firefox". The page displays a configuration table for "Edit Policies - General" with columns for Policy, Derived From, Action, and Setting.

Policy	Derived From	Action	Setting
Home page HTML file	Shipped default	Use current setting	/QIBM/ProdData/Access/Web2/html/homepage.h
Template HTML file	Shipped default	Use current setting	/QIBM/ProdData/Access/Web2/html/webaccess.h
Main page HTML file	Shipped default	Use current setting	/QIBM/ProdData/Access/Web2/html/overview.htm
Home page	Shipped default	Use current setting	Allow
Template	Shipped default	Use current setting	Allow
Navigation	Shipped default	Use current setting	Allow
Related links	Shipped default	Use current setting	Allow

Special tags

- Within the home page and template .html files, special tags are used.
 - When these tags are encountered by the IBM i Access for Web code, they are replaced with the appropriate content.
- **Special tags...**

<ul style="list-style-type: none"> - %%CONTENT%% - %%include section=file%% - %%MENU%% - %%STYLESHEET%% - %%STYLESHEET_CLASSIC_COLORS%% - %%TITLE%% - %%SYSTEM%% - %%USER%% - %%VERSION%% 	<p>Replaced with...</p> <ul style="list-style-type: none"> functional content for the page, separates the header/footer HTML section/fragment to include navigation bar default style sheet prior to V5R4 title of the page name of IBM i being accessed IBM i user profile used to access the server version of System i Access for Web
--	--
- For detailed information on these special tags
 - V6R1 System i Access for Web Info Center
 - Connecting to IBM i->System i Access->System i Access for Web->System i Access for Web in a web application sever environment->Customizing System i Access for Web->Default page content->Home page

iWAHome - structure

<http://<system>/webaccess/iWAHome>

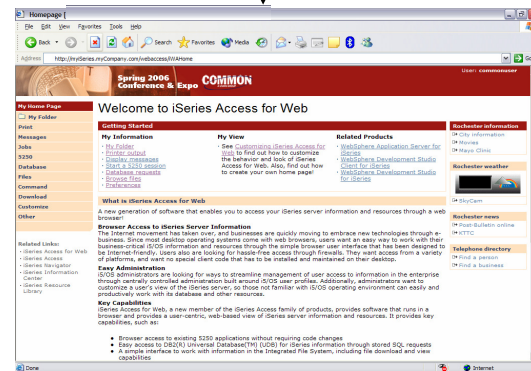
Homepage file
common_homepage.html

Defines content, layout, images, links to be displayed when the iWAHome servlet is invoked in the browser.

Image files
images/s06common.gif
images/iwa_navCorner.gif

Cascading Style Sheet file
common_styles.css

Defines the colors, fonts, font sizes for the various elements in the .html files.



IBM Power Systems

iWA servlet Template - structure

<http://<system>/webaccess/iWASpool>

Homepage file
common_homepage.html

Defines content, layout, images, links to be displayed when the iWAHome servlet is invoked in the browser.

Template file
common_template.html

Defines the header, content, footer on all other servlet pages.

Image files
images/s06common.gif
images/iwa_navCorner.gif

Cascading Style Sheet file
common_styles.css

Defines the colors, fonts, font sizes for the various elements in the .html files.

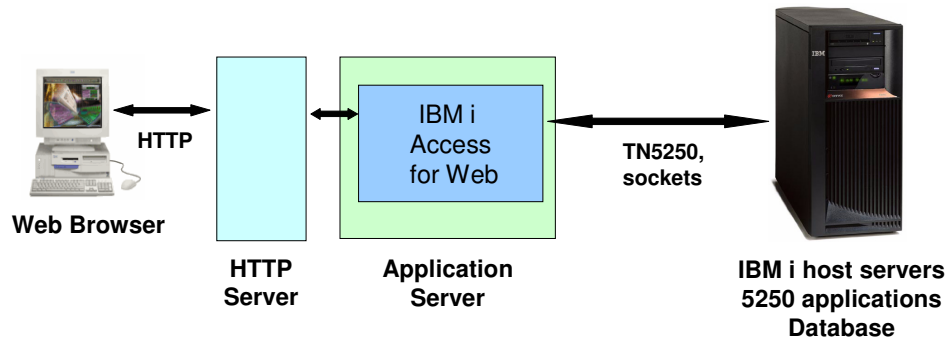
67 **Power your planet.** © 2010 IBM Corporation

IBM Power Systems

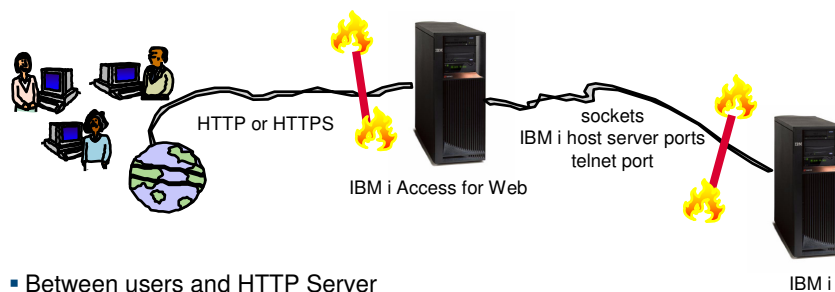
Environment Security Considerations

68 **Power your planet.** © 2010 IBM Corporation

IBM i Access for Web Environment



IBM i Access for Web Environment (continued)



- Between users and HTTP Server
 - Secure Socket Layer (SSL)
 - Virtual Private Networking (VPN)
 - Firewalls
- Between IBM i Access for Web and IBM i
 - VPN
 - Firewalls

Secure Sockets Layer

- Used for data confidentiality between Web browser and HTTP server
 - Digital certificates used to determine trust relationships
 - Point to Point encryption for all data (PC App to Server App)
 - Part of the standard HTTPS protocol
- See Info Center for specific details on Configuration and Setup.
 - See the “Configure WebSphere Security” topic
- Levels of SSL
 - TLSv1, SSLv3 recommended, use 128-bit or higher
 - SSLv2 should not be used anymore. Disable in clients and server (APAR SE25734)

Virtual Private Networking

- Used for data confidentiality between Web browser and HTTP server
 - Digital certificates and User authorization used establish tunnel
 - End to End encryption for all data (PC to Server tunnel)
 - Allows any protocol, including standard HTTP
- See Info Center for specific details on Configuration and Setup.
 - See the “Virtual Private Networking” topic

Security Options



Security Options: Authorization and Authentication

- How does the user authenticate to IBM i Access for Web?
- How does IBM i Access for Web authenticate with IBM i?
- IBM i Access for Web in a WebSphere Single Signon (SSO) environment
- Special considerations for 5250

Authorization

- Authorization is verifying that authenticated users have permission to access requested resources
- IBM i Access for Web uses the IBM i user profile and object level security to authorize access to IBM i resources
- IBM i Access for Web provides application level control of access to functions through policies
 - Policies can be administered at the IBM i user and group profile levels

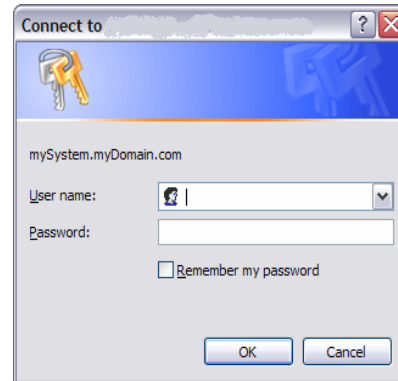
Policies		Profile: JHANSEN		
Action	Category	Description	Access	
<input checked="" type="checkbox"/>	\$250	\$250 user interface custom settings.	Allowed	
<input checked="" type="checkbox"/>	Command	Run batch command custom settings.	Allowed	
<input checked="" type="checkbox"/>	Customize	Preferences and policy administration custom settings.	Allowed	
<input checked="" type="checkbox"/>	Database	Database tables, requests, and run SQL custom settings.	Allowed	
<input checked="" type="checkbox"/>	Database connections	Create and edit database connection definitions.	Allowed	
<input checked="" type="checkbox"/>	Download	Download packages custom settings.	Allowed	
<input checked="" type="checkbox"/>	Files	Integrated file system and file share custom settings.	Allowed	
<input checked="" type="checkbox"/>	General	Page layout, language and character set custom settings.	Allowed	
<input checked="" type="checkbox"/>	Jobs	Work with jobs custom settings.	Allowed	
<input checked="" type="checkbox"/>	Mail	Send mail custom settings.	Allowed	
<input checked="" type="checkbox"/>	Messages	Display messages, send messages, and message queue custom settings.	Allowed	

Authentication

- Authentication is verifying the identity of the user
- IBM i Access for Web supports two types of authentication
 - Application
 - IBM i Access for Web handles the authentication
 - Application Server
 - WebSphere Application Server handles the authentication
- Specified by the AUTHTYPE parameter on the CFGACCWEB2 command
 - Application: AUTHTYPE(*APP)
 - Application Server: AUTHTYPE(*APPSVR)

Application Authentication

- IBM i Access for Web handles authentication
- IBM i user profile and password
 - Hostname specified by the TGTSVR parameter on the CFGACCWEB2 command
- Method: HTTP basic authentication
 - RFC2617
 - User profile and password are encoded (not encrypted) in the HTTP headers and should be protected

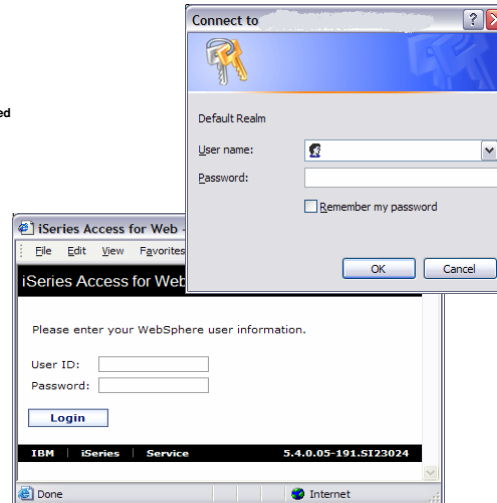


Application Server Authentication

- WebSphere handles authentication
- WebSphere credentials
 - Typically a user ID and password
 - Can be Windows domain login information (new in V6R1)
 - Kerberos-based
 - Requires WebSphere Application Server V6.1 or later
 - Authenticated with the active WebSphere user registry
- Specified by the AUTHTYPE parameter on the CFGACCWEB2 command
 - Application Server Authentication: AUTHTYPE(*APPSVR)
- WebSphere provides different methods of gathering credentials
 - Applications can choose which methods to support

Application Server Authentication (continued)

- **IBM i Access for Web supports two methods of gathering credentials**
 - HTTP basic authentication
 - User ID and password are encoded (not encrypted) in the HTTP headers and should be protected
 - Form-based authentication
 - User ID and password are clear text and should be protected
 - Kerberos-based authentication (VBR1)
 - Windows domain login information sent via Simple and Protected GSS-API Negotiation Mechanism (SPNEGO)
 - No additional prompt for user credentials
- **Specified by the AUTHMETHOD parameter on the CFGACCWEB2 command**
 - HTTP basic authentication: AUTHMETHOD(*BASIC)
 - Form-based authentication: AUTHMETHOD(*FORM)
 - Kerberos-based authentication: AUTHMETHOD(*KERBEROS)

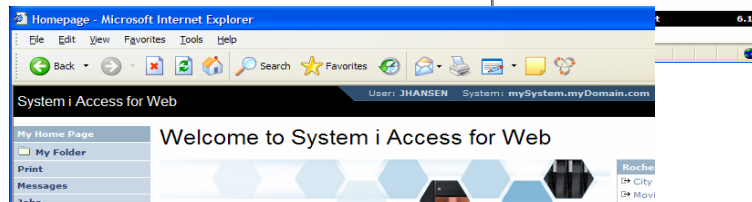
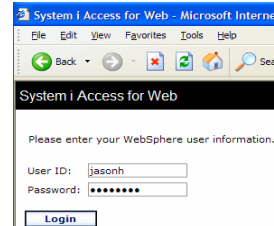


Application Server Authentication Authorization

- **HTTP basic authentication and form-based authentication**
 - IBM i Access for Web uses Enterprise Identity Mapping (EIM) to map the authenticated WebSphere user identity to an IBM i user profile
 - IBM i Access for Web identifies the user by the mapped IBM i user profile
 - IBM i user profile is used to authorize access to IBM i resources using object level security
- **Kerberos-based authentication**
 - IBM i Access for Web uses Kerberos-based credentials to authenticate with IBM i
 - IBM i uses Network Authentication Service (NAS) and EIM to map the Kerberos-based identity to an IBM i user profile
 - IBM i Access for Web identifies the user by the mapped IBM i user profile
 - IBM i user profile is used to authorize access to IBM i resources using object level security

Application Server Authentication Configure IBM i Access for Web

- Configure IBM i Access for Web
 - CFGACCWEB2 AUTHTYPE(*APPSVR) AUTHMETHOD(*FORM) ...
 - CFGACCWEB2 AUTHTYPE(*APPSVR) AUTHMETHOD(*KERBEROS) ...



5250 Sessions

- 5250 sessions can be started to any system running IBM i
- Must provide user profile and password on IBM i Sign On screen

Start Session

Server: []
 Port: 23
 Code page: 37

Workstation ID
 Use user ID
 Specify workstation ID []
 Avoid duplicates for this user
 Avoid duplicates with other users

General
 Initial macro: []
 Bypass signon
 Display HTML data in fields

Start Session

Sign On

System
 Subsystem QINTER
 Display QPADEV0006

User:
 Password
 Program/procedure
 Menu
 Current library

RELEASE: V05R03M00
 DRIVER: 2600722
 USE OF THIS SYSTEM IS FOR IBM MANAGEMENT APPROVED PURPOSES ONLY.
 USE IS SUBJECT TO AUDIT AT ANY TIME BY IBM MANAGEMENT.

5250 Session Bypass Signon

- QRMTSIGN system value must be *VERIFY
- Select bypass signon when starting or configuring a session

Configure New Session

General

Session: * required

Default view:

Initial macro:

Bypass signon

Display HTML data in fields

Enable advanced JavaScript functions

System

System:

Port:

Start Session

System

System:

Port:

Code page:

Workstation ID

Use user ID

Specify workstation ID

Avoid duplicates for this user

Avoid duplicates with other users

General

Initial macro:

Bypass signon

Display HTML data in fields

- IBM i Access for Web must be configured for application authentication or application server authentication with Kerberos for bypass signon to be available
 - CFGACCWEB2 AUTHTYPE(*APP) ...
 - CFGACCWEB2 AUTHTYPE(*APPSVR) AUTHMETHOD(*KERBEROS) ... (V6R1 Access for Web and WAS 6.1 or later)

5250 Sessions in Portlets

- Bypass signon
 - QRMTSIGN system value must be *VERIFY
 - Settings to enable bypass signon and specify the credential to use

iSeries 5250 Session

Start Session

Server

Server:

Port:

Code page:

Display HTML data in fields

Workstation ID

Use user ID

Specify workstation ID

Avoid duplicates for this user

Avoid duplicates with other users

Bypass signon

Enable bypass signon

Use credential specific to this portlet window

User:

Password:

Confirm password:

Use credential set with iSeries Credentials portlet

Credential:

Use system shared credential set by administrator

Credential:



Try out Access for Web for yourself!

Start your browser and connect to the following web site:

<http://iseriesd.dfw.ibm.com/webaccess/iWAHome> (case sensitive)

<p>User ID = WACUST Password = demo2pwd</p>	<p>This shows the basic look of System i Access for Web as we ship it. You can try various functions -- including working with printer output, creating database requests, etc. Click on the 5250 tab, sign onto the IBM i, then start an RPG application called BOATS and run it.</p>
<p>User ID = BOATADMIN Password = demo2pwd</p>	<p>This is an example of how a customer might design a web page for their use. You will see that an end user could start the same BOATS application by clicking on the 5250 session, or they could have used HATS to run the application. You will also see other links that would let a user work with spoolfile information, work with IFS, run database requests, etc..</p>

Send email to: LLHIRSCH@us.ibm.com to reset the user profiles on iseriesd.dfw.ibm.com if either one gets disabled.



Special notices

This document was developed for IBM offerings in the United States as of the date of publication. IBM may not make these offerings available in other countries, and the information is subject to change without notice. Consult your local IBM business contact for information on the IBM offerings available in your area.

Information in this document concerning non-IBM products was obtained from the suppliers of these products or other public sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information contained in this document has not been submitted to any formal IBM test and is provided "AS IS" with no warranties or guarantees either expressed or implied.

All examples cited or described in this document are presented as illustrations of the manner in which some IBM products can be used and the results that may be achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions.

IBM Global Financing offerings are provided through IBM Credit Corporation in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government clients. Rates are based on a client's credit rating, financing terms, offering type, equipment type and options, and may vary by country. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice.

IBM is not responsible for printing errors in this document that result in pricing or information inaccuracies.

All prices shown are IBM's United States suggested list prices and are subject to change without notice; reseller prices may vary.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

Any performance data contained in this document was determined in a controlled environment. Actual results may vary significantly and are dependent on many factors including system hardware configuration and software design and configuration. Some measurements quoted in this document may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Some measurements quoted in this document may have been estimated through extrapolation. Users of this document should verify the applicable data for their specific environment.

Revised September 26, 2006



Special notices (cont.)

IBM, the IBM logo, ibm.com AIX, AIX (logo), AIX 6 (logo), AS/400, Active Memory, BladeCenter, Blue Gene, CacheFlow, ClusterProven, DB2, ESCON, i5/OS, i5/OS (logo), IBM Business Partner (logo), IntelliStation, LoadLeveler, Lotus, Lotus Notes, Notes, Operating System/400, OS/400, PartnerLink, PartnerWorld, PowerPC, pSeries, Rational, RISC System/6000, RS/6000, THINK, Tivoli, Tivoli (logo), Tivoli Management Environment, WebSphere, xSeries, z/OS, zSeries, AIX 5L, Chiphopper, Chipkill, Cloudscape, DB2 Universal Database, DS4000, DS6000, DS8000, EnergyScale, Enterprise Workload Manager, General Purpose File System, GPFS, HACMP, HACMP/6000, HASM, IBM Systems Director Active Energy Manager, iSeries, Micro-Partitioning, POWER, PowerExecutive, PowerVM, PowerVM (logo), PowerHA, Power Architecture, Power Everywhere, Power Family, POWER Hypervisor, Power Systems, Power Systems (logo), Power Systems Software, Power Systems Software (logo), POWER2, POWER3, POWER4, POWER4+, POWER5, POWER5+, POWER6, POWER7, pureScale, System i, System p, System p5, System Storage, System z, Tivoli Enterprise, TME 10, TurboCore, Workload Partitions Manager and X-Architecture are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

The Power Architecture and Power.org wordmarks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

UNIX is a registered trademark of The Open Group in the United States, other countries or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries or both.

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

Intel, Itanium, Pentium are registered trademarks and Xeon is a trademark of Intel Corporation or its subsidiaries in the United States, other countries or both.

AMD Opteron is a trademark of Advanced Micro Devices, Inc.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

TPC-C and TPC-H are trademarks of the Transaction Performance Processing Council (TPPC).

SPECint, SPECfp, SPECjbb, SPECweb, SPECjAppServer, SPEC OMP, SPECviewperf, SPECcapc, SPECchpc, SPECjvm, SPECmail, SPECimap and SPECcsfs are trademarks of the Standard Performance Evaluation Corp (SPEC).

NetBench is a registered trademark of Ziff Davis Media in the United States, other countries or both.

Altivec is a trademark of Freescale Semiconductor, Inc.

Cell Broadband Engine is a trademark of Sony Computer Entertainment Inc.

InfiniBand, InfiniBand Trade Association and the InfiniBand design marks are trademarks and/or service marks of the InfiniBand Trade Association.

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

Revised February 9, 2010