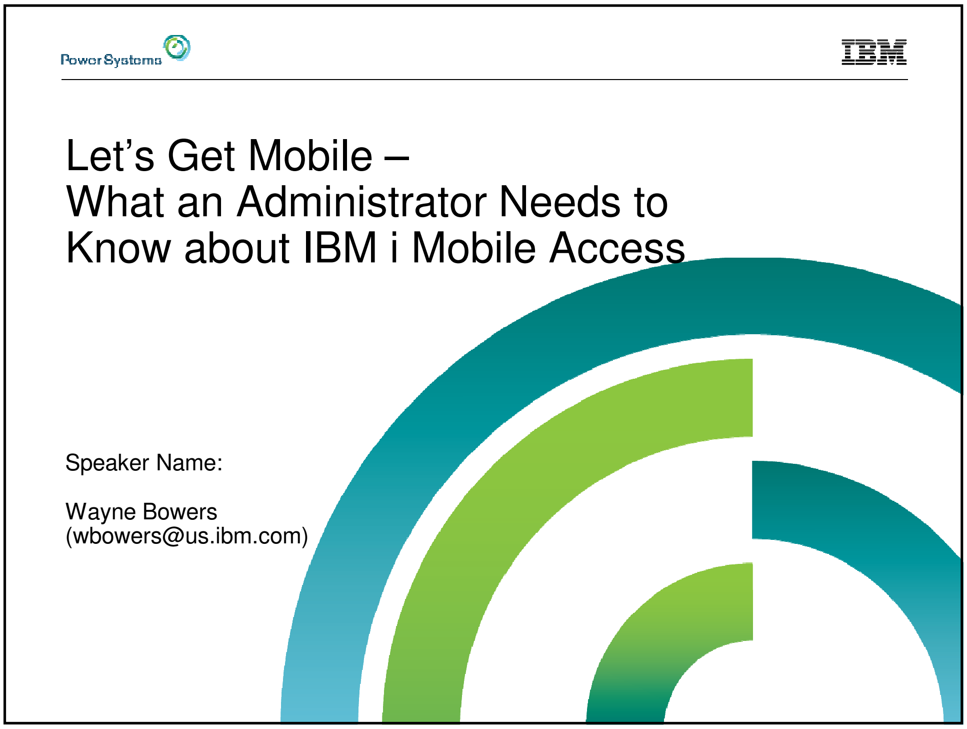
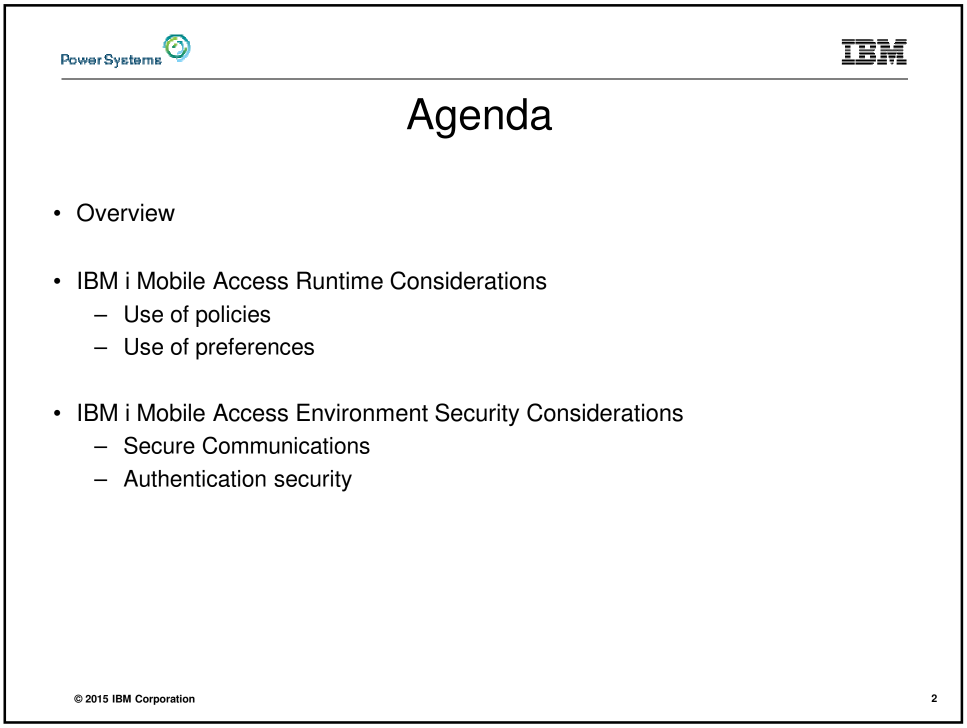


Let's Get Mobile – What an Administrator Needs to Know about IBM i Mobile Access

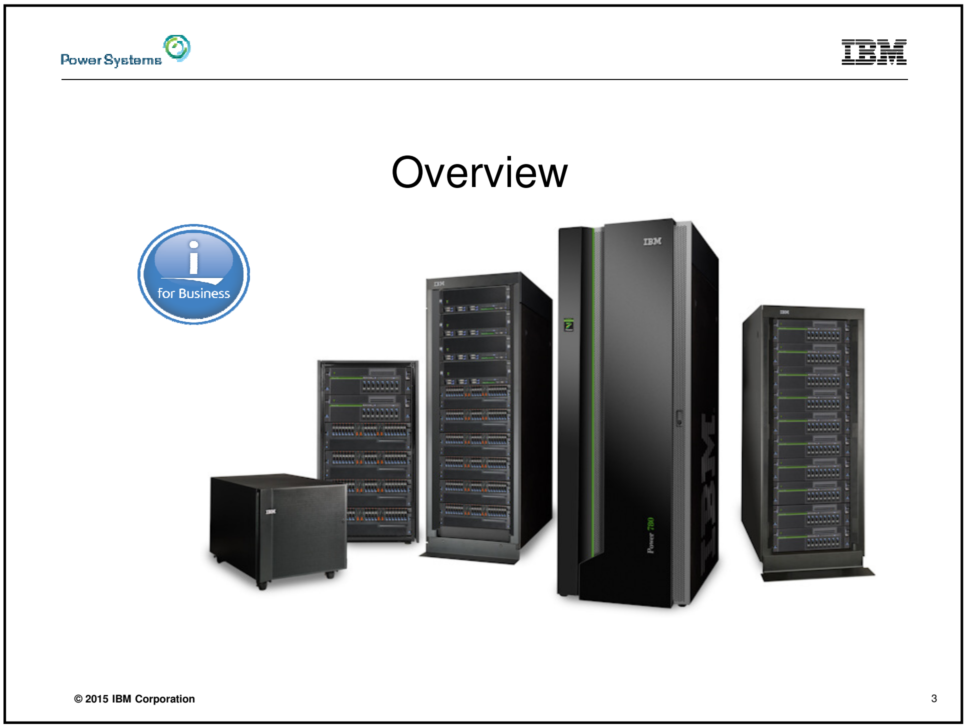
Speaker Name:

Wayne Bowers
(wbowers@us.ibm.com)

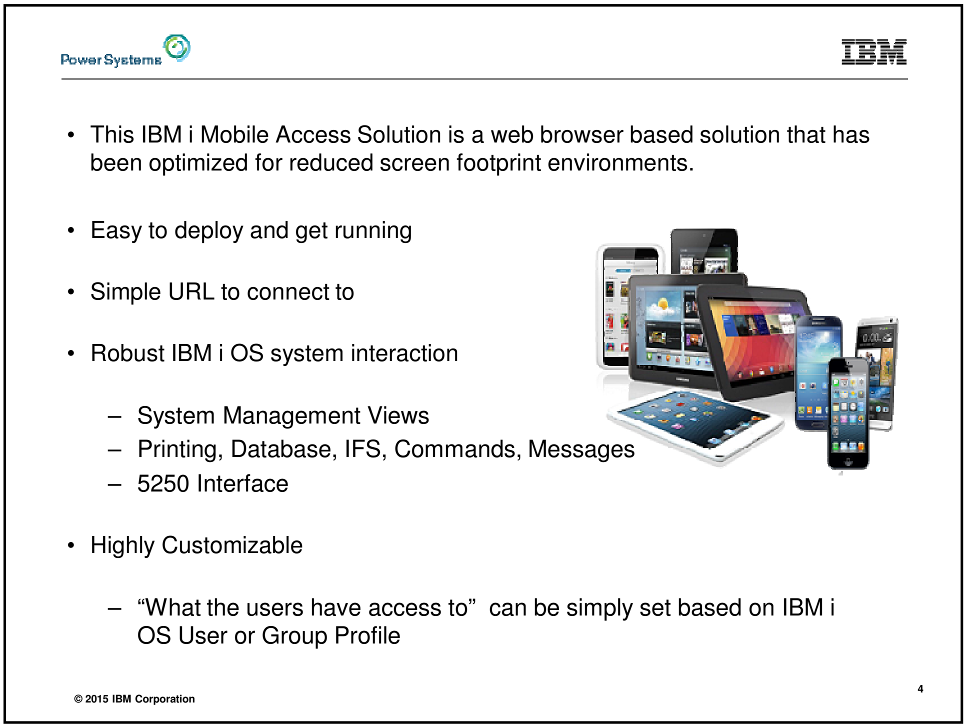


Agenda

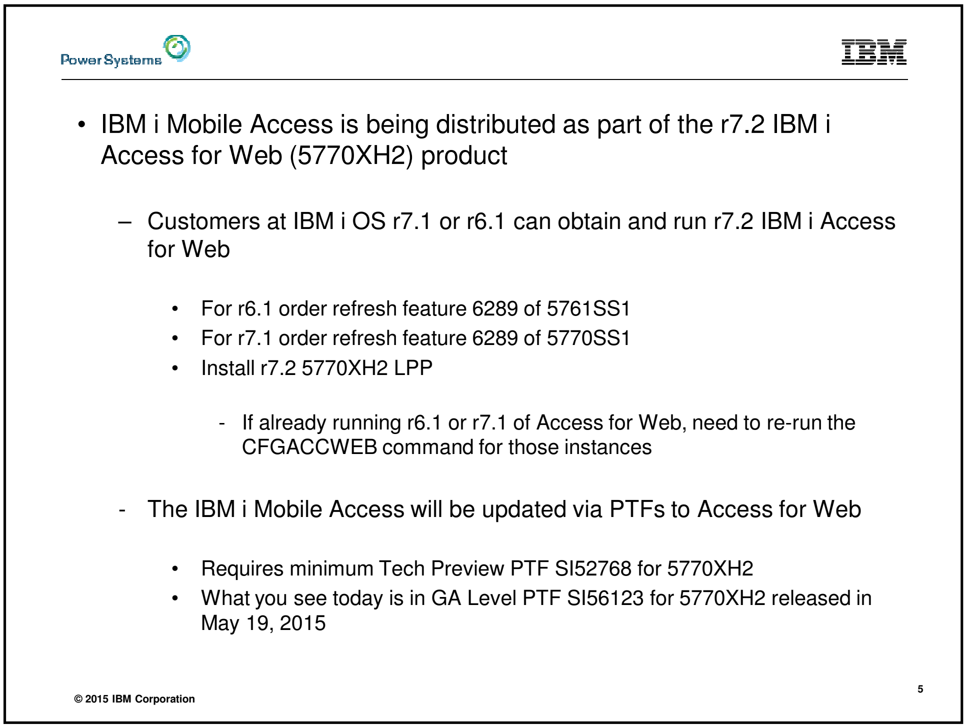
- Overview
- IBM i Mobile Access Runtime Considerations
  - Use of policies
  - Use of preferences
- IBM i Mobile Access Environment Security Considerations
  - Secure Communications
  - Authentication security



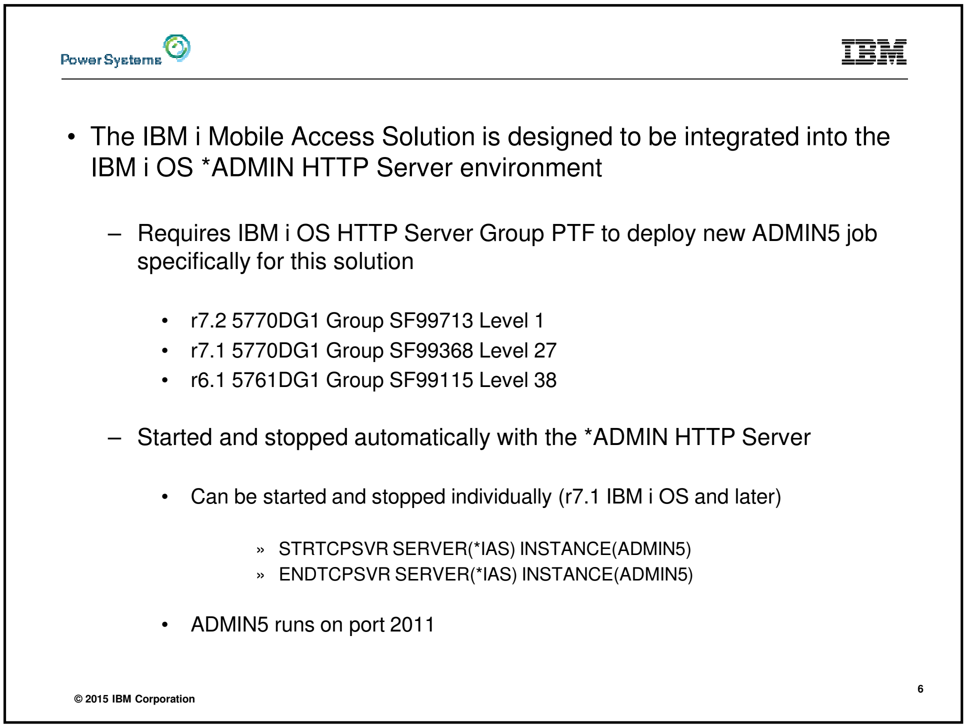
Overview



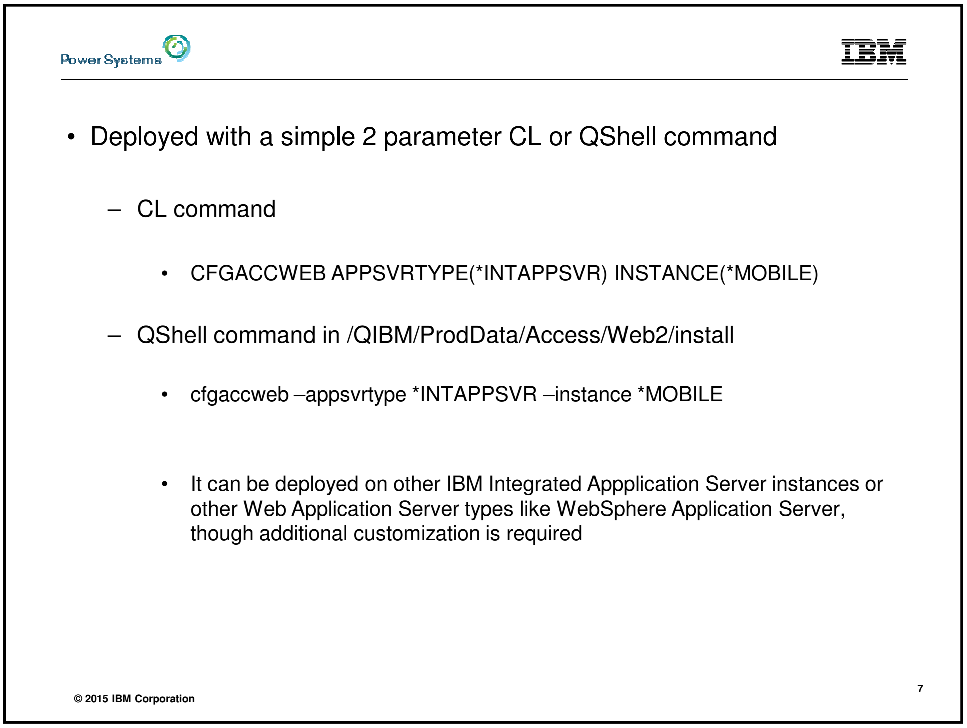
- This IBM i Mobile Access Solution is a web browser based solution that has been optimized for reduced screen footprint environments.
- Easy to deploy and get running
- Simple URL to connect to
- Robust IBM i OS system interaction
  - System Management Views
  - Printing, Database, IFS, Commands, Messages
  - 5250 Interface
- Highly Customizable
  - "What the users have access to" can be simply set based on IBM i OS User or Group Profile



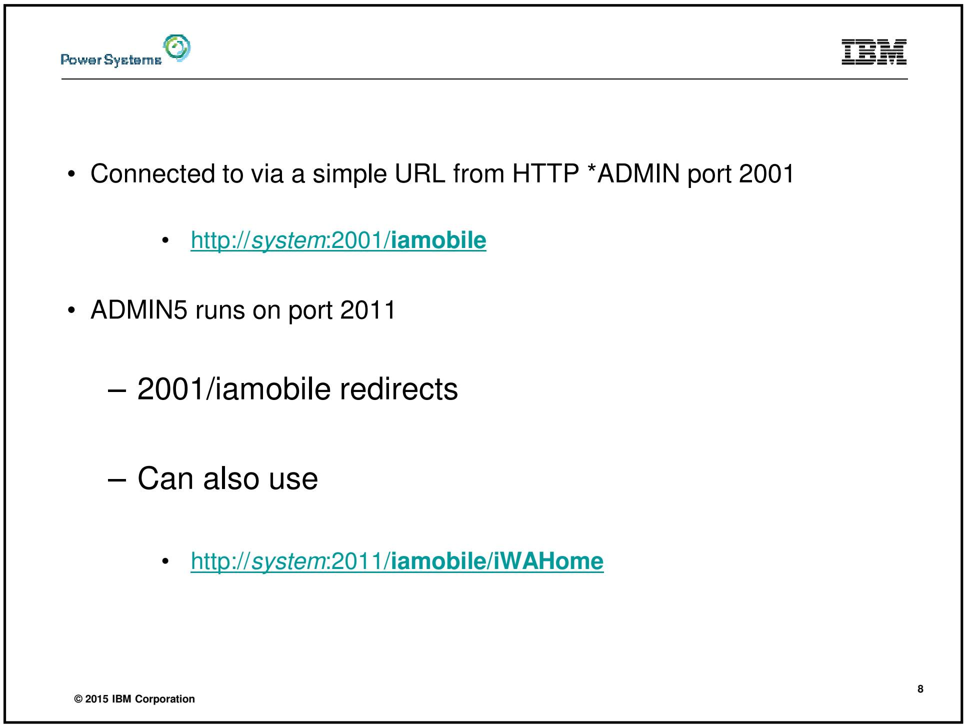
- IBM i Mobile Access is being distributed as part of the r7.2 IBM i Access for Web (5770XH2) product
  - Customers at IBM i OS r7.1 or r6.1 can obtain and run r7.2 IBM i Access for Web
    - For r6.1 order refresh feature 6289 of 5761SS1
    - For r7.1 order refresh feature 6289 of 5770SS1
    - Install r7.2 5770XH2 LPP
      - If already running r6.1 or r7.1 of Access for Web, need to re-run the CFGACCWEB command for those instances
  - The IBM i Mobile Access will be updated via PTFs to Access for Web
    - Requires minimum Tech Preview PTF SI52768 for 5770XH2
    - What you see today is in GA Level PTF SI56123 for 5770XH2 released in May 19, 2015



- The IBM i Mobile Access Solution is designed to be integrated into the IBM i OS *ADMIN HTTP Server environment
  - Requires IBM i OS HTTP Server Group PTF to deploy new ADMIN5 job specifically for this solution
    - r7.2 5770DG1 Group SF99713 Level 1
    - r7.1 5770DG1 Group SF99368 Level 27
    - r6.1 5761DG1 Group SF99115 Level 38
  - Started and stopped automatically with the *ADMIN HTTP Server
    - Can be started and stopped individually (r7.1 IBM i OS and later)
      - » STRTCPSVR SERVER(*IAS) INSTANCE(ADMIN5)
      - » ENDTCPSVR SERVER(*IAS) INSTANCE(ADMIN5)
    - ADMIN5 runs on port 2011



- Deployed with a simple 2 parameter CL or QShell command
  - CL command
    - CFGACCWEB APPSVRTYPE(*INTAPPSVR) INSTANCE(*MOBILE)
  - QShell command in /QIBM/ProdData/Access/Web2/install
    - cfgaccweb –appsvrtype *INTAPPSVR –instance *MOBILE
    - It can be deployed on other IBM Integrated Appplication Server instances or other Web Application Server types like WebSphere Application Server, though additional customization is required

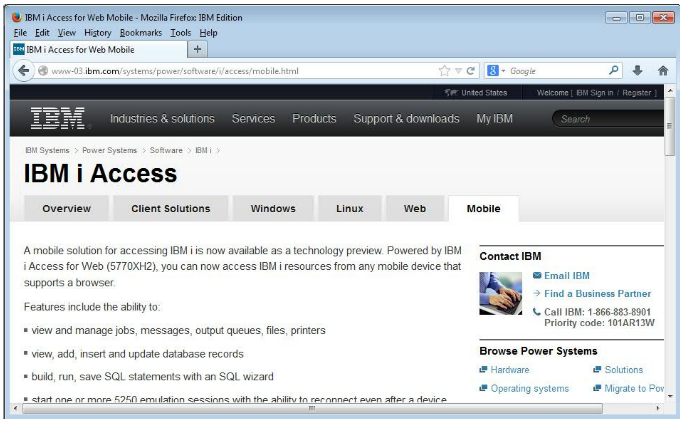


- Connected to via a simple URL from HTTP *ADMIN port 2001
    - http://*system*:2001/**iamobile**
- ADMIN5 runs on port 2011
  - 2001/iamobile redirects
  - Can also use
    - http://*system*:2011/**iamobile/iWAHome**

More Information:

http://www.ibm.com/systems/power/software/i/access/mobile.html

Latest Information available at this location


IBM i Access for Web Mobile - Mozilla Firefox: IBM Edition
File Edit View History Bookmarks Tools Help
IBM i Access for Web Mobile
www-03.ibm.com/systems/power/software/i/access/mobile.html
Google
United States
Welcome [IBM Sign in / Register]
Industries & solutions
Services
Products
Support & downloads
My IBM
Search
IBM Systems > Power Systems > Software > IBM i >
Overview
Client Solutions
Windows
Linux
Web
Mobile

IBM i Access

A mobile solution for accessing IBM i is now available as a technology preview. Powered by IBM i Access for Web (5770XH2), you can now access IBM i resources from any mobile device that supports a browser.

Features include the ability to:

- view and manage jobs, messages, output queues, files, printers
- view, add, insert and update database records
- build, run, save SQL statements with an SQL wizard
- start one or more 5250 emulation sessions with the ability to reconnect even after a device

Contact IBM

Email IBM

Find a Business Partner

Call IBM: 1-866-883-8901
Priority code: 101AR13W

Browse Power Systems

Hardware

Solutions

Operating systems

Migrate to Pov

Runtime Considerations

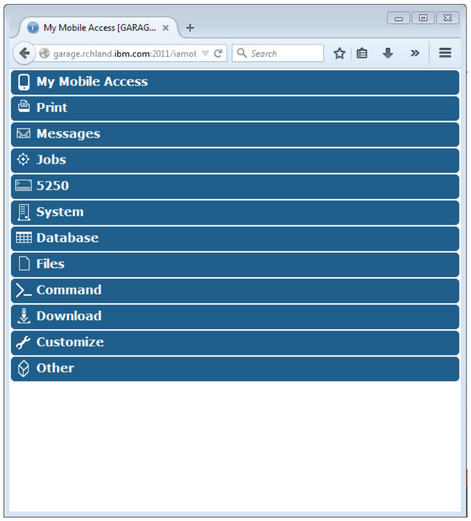
Controlling Access

Methods to control access using IBM i Mobile Access

- 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

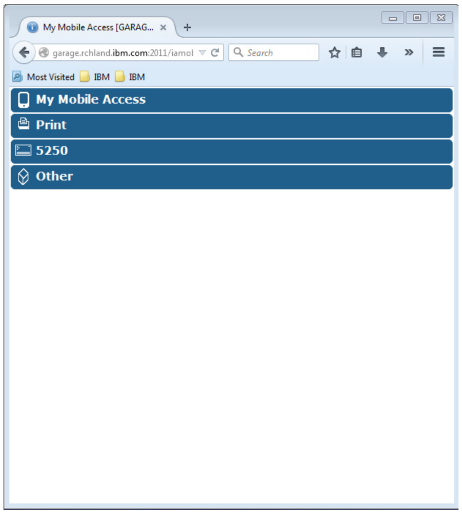
Controlling Access

Main Page = http://<myiseries>:2001/iamobile



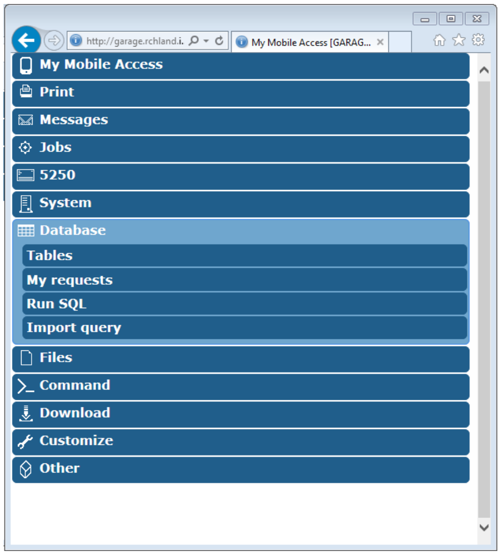
Controlling Access

Main Page = http://<myiseries>:2001/iamobile



Controlling Access

Product functionality

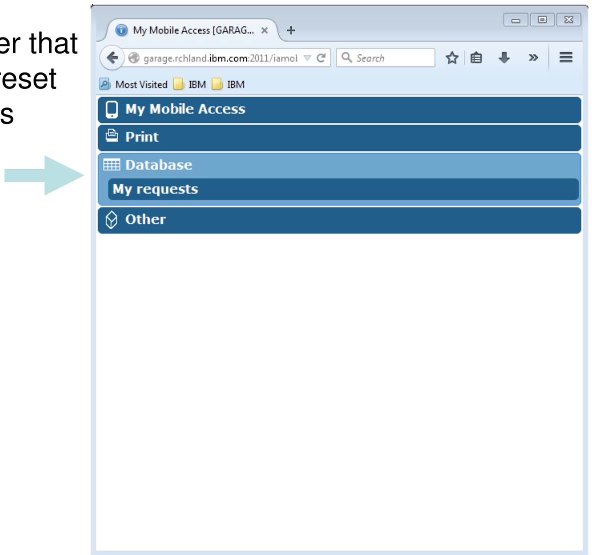


Power Systems

IBM

Controlling Access

Sample for a user that only performs preset database queries



- My Mobile Access
- Print
- Database
  - My requests
- Other

© 2015 IBM Corporation

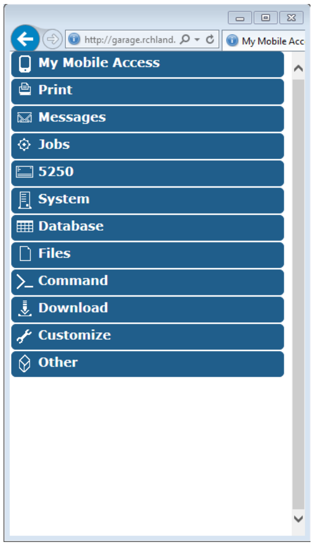
Power Systems

IBM

Controlling Access: Setting Policies

© 2015 IBM Corporation

Controlling User Access



•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

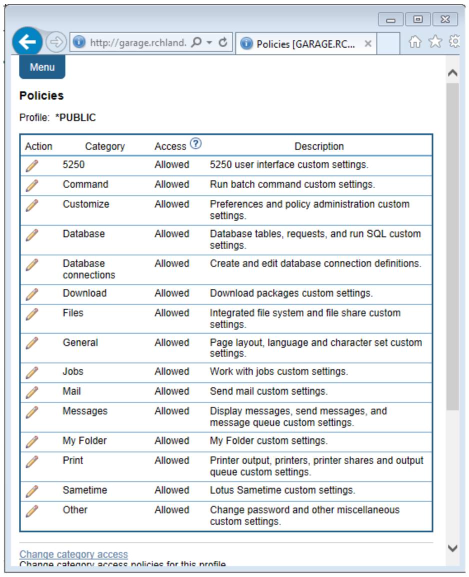
•You need *SECADM authority to customize profiles

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 Mobile Access functions.

Controlling User Access

- IBM i Mobile Access 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



Policies

Profile: *PUBLIC

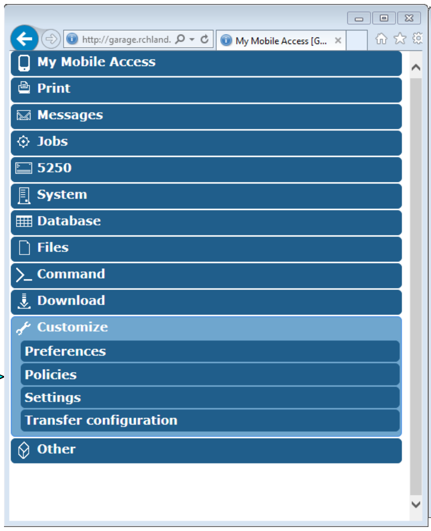
Action	Category	Access ?	Description
✎	5250	Allowed	5250 user interface custom settings.
✎	Command	Allowed	Run batch command custom settings.
✎	Customize	Allowed	Preferences and policy administration custom settings.
✎	Database	Allowed	Database tables, requests, and run SQL custom settings.
✎	Database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

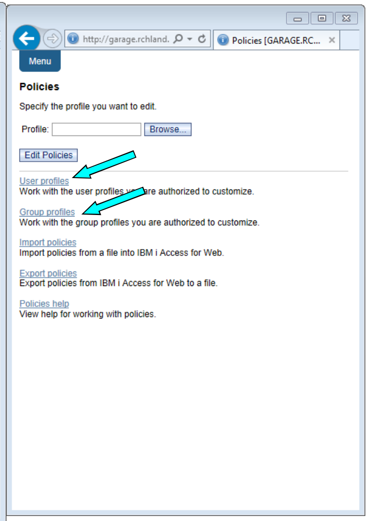
Change category access
Change category access policies for this profile

Controlling Access - Strategies

- IBM i Mobile Access ships with a set of default policy settings. The default policy settings allow most of the IBM i Mobile Access functions to be available for all users. Without any customization, users accessing IBM i Mobile Access 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 Mobile Access functions.

Setting Policies





Policies

Specify the profile you want to edit.

Profile: ▭ Browse...

Edit Policies

User profiles
Work with the user profiles you are authorized to customize.

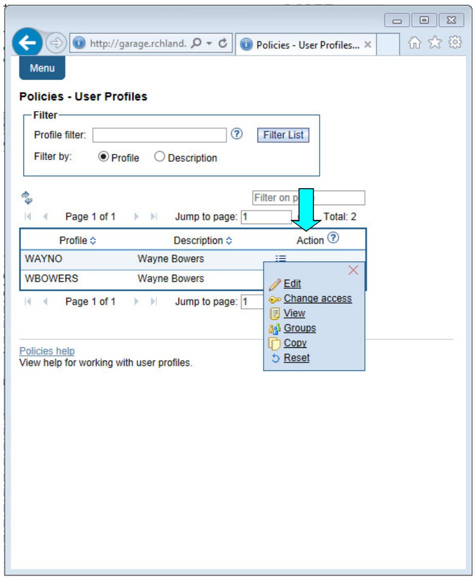
Group profiles
Work with the group profiles you are authorized to customize.

Import policies
Import policies from a file into IBM i Access for Web.

Export policies
Export policies from IBM i Access for Web to a file.

Policies help
View help for working with policies.

Setting policies (continued)



Policies - User Profiles

Filter

Profile filter: ▭ ? Filter List

Filter by: ● Profile ○ Description

Filter on p

Page 1 of 1 Jump to page: 1 Total: 2

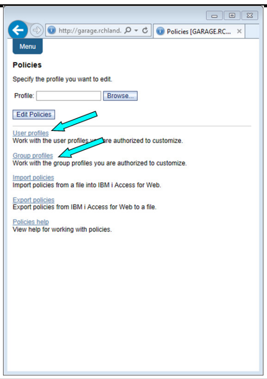
Profile	Description	Action
WAYNO	Wayne Bowers	☰
WBOWERS	Wayne Bowers	

Page 1 of 1 Jump to page: 1

Policies help
View help for working with user profiles.

Setting policies (continued)

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.



Policies

Specify the profile you want to edit.

Profile: Browse...

Edit Policies

User profiles
Work with the user profiles you are authorized to customize.

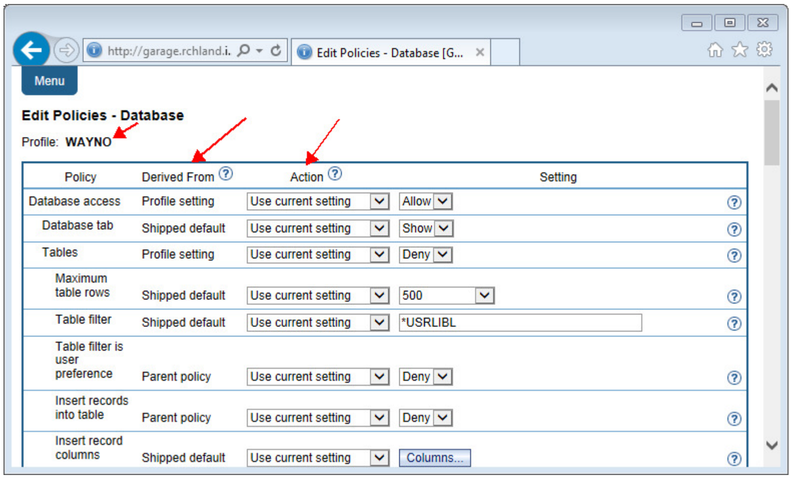
Group profiles
Work with the group profiles you are authorized to customize.

Import policies
Import policies from a file into IBM i Access for Web.

Export policies
Export policies from IBM i Access for Web to a file.

Policies help
View help for working with policies.

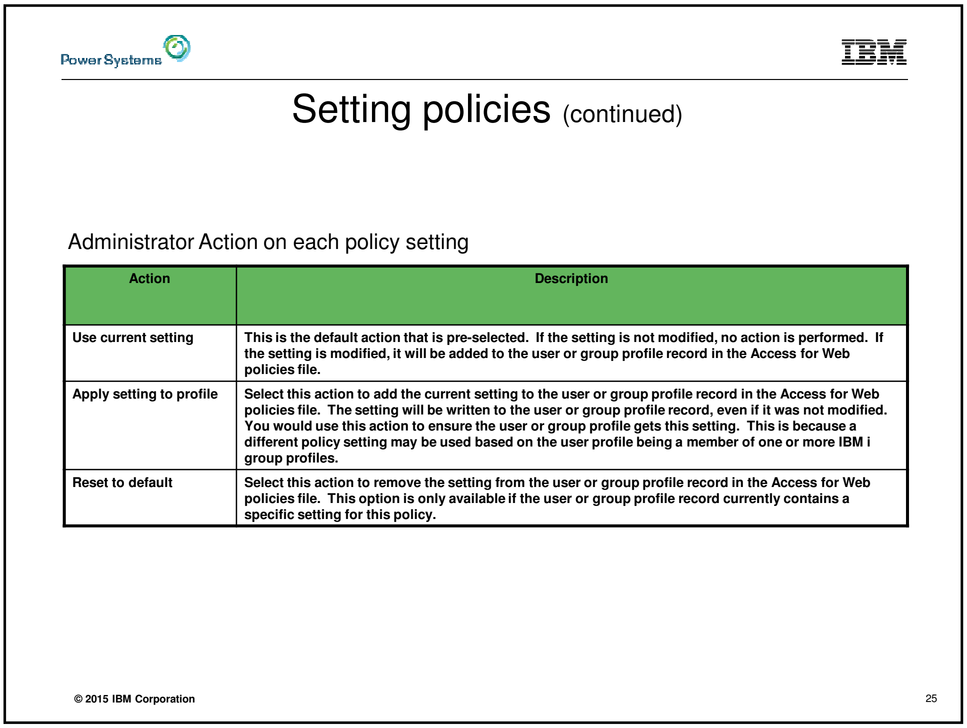
Setting policies (continued)



Edit Policies - Database

Profile: **WAYNO**

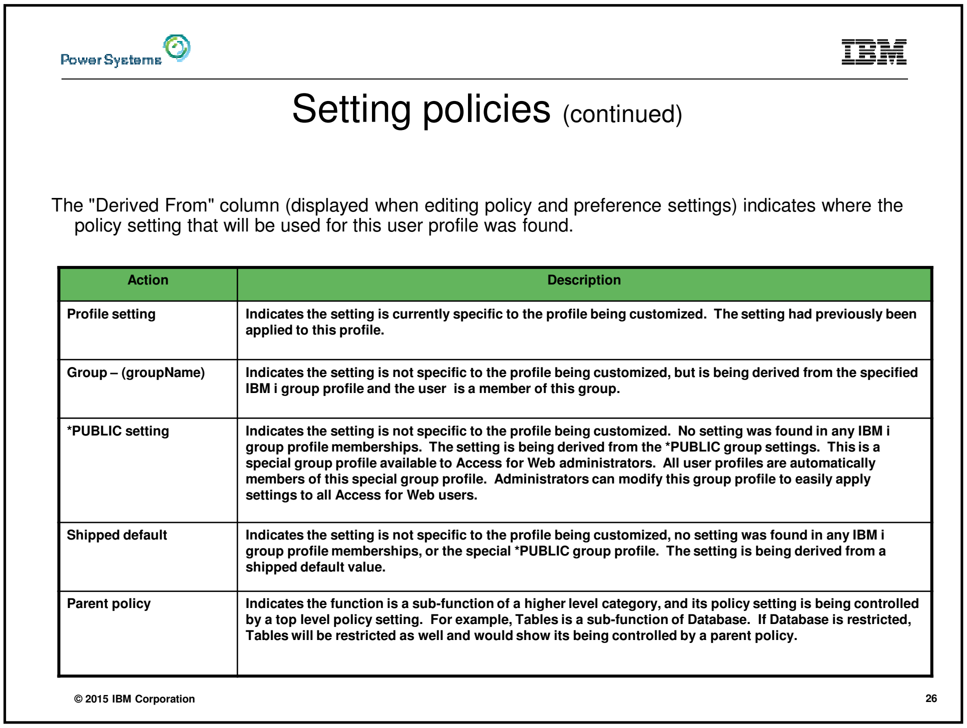
Policy	Derived From	Action	Setting
Database access	Profile setting	Use current setting	Allow
Database tab	Shipped default	Use current setting	Show
Tables	Profile setting	Use current setting	Deny
Maximum table rows	Shipped default	Use current setting	500
Table filter	Shipped default	Use current setting	*USRLIBL
Table filter is user preference	Parent policy	Use current setting	Deny
Insert records into table	Parent policy	Use current setting	Deny
Insert record columns	Shipped default	Use current setting	Columns...



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 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 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 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.



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 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 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.

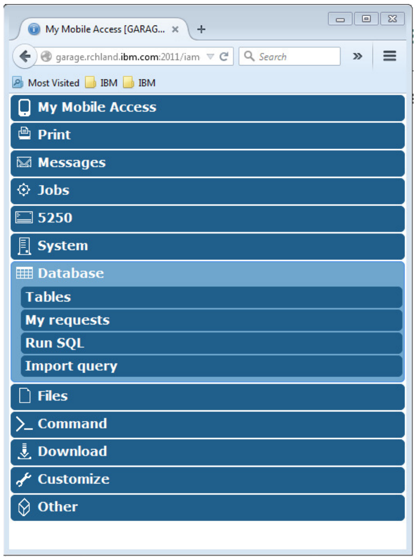
Policies Example:
Simple Database User

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 IBM i Mobile Access
  - 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.

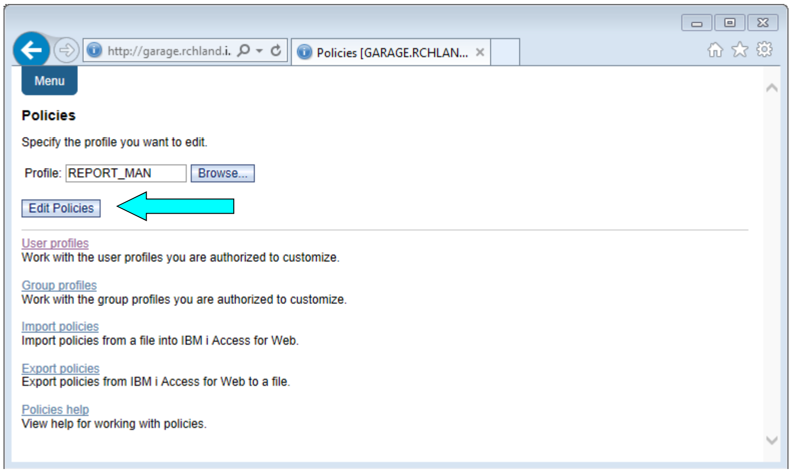
Simple Database User - Before

Accessing the Database tab of IBM i Mobile Access as user REPORT_MAN



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.



Policies

Specify the profile you want to edit.

Profile: REPORT_MAN Browse...

Edit Policies

User profiles
Work with the user profiles you are authorized to customize.

Group profiles
Work with the group profiles you are authorized to customize.

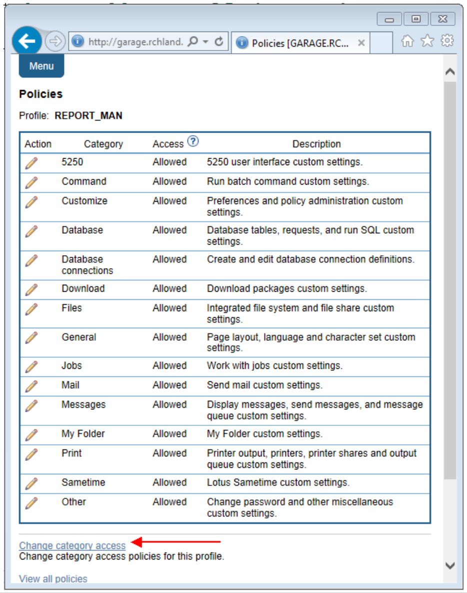
Import policies
Import policies from a file into IBM i Access for Web.

Export policies
Export policies from IBM i Access for Web to a file.

Policies help
View help for working with policies.

Simple Database User - Categories

- Change Category Access



Policies

Profile: **REPORT_MAN**

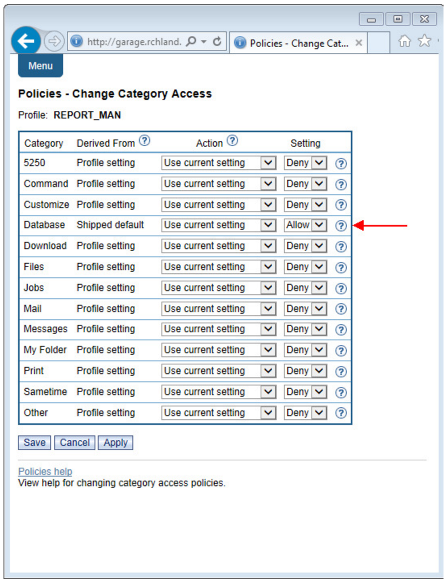
Action	Category	Access	Description
✎	5250	Allowed	5250 user interface custom settings.
✎	Command	Allowed	Run batch command custom settings.
✎	Customize	Allowed	Preferences and policy administration custom settings.
✎	Database	Allowed	Database tables, requests, and run SQL custom settings.
✎	Database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

Change category access
Change category access policies for this profile.

View all policies

Simple Database User - Categories

- Turn off all non-Database functions by Applying setting of Deny to Profile
- Leave Database to Allow



Policies - Change Category Access

Profile: **REPORT_MAN**

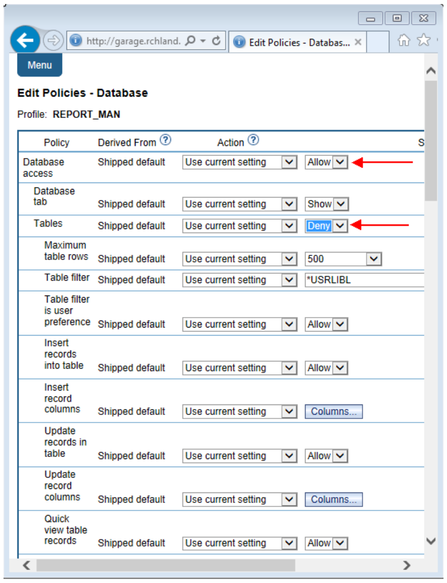
Category	Derived From	Action	Setting
5250	Profile setting	Use current setting	Deny
Command	Profile setting	Use current setting	Deny
Customize	Profile setting	Use current setting	Deny
Database	Shipped default	Use current setting	Allow
Download	Profile setting	Use current setting	Deny
Files	Profile setting	Use current setting	Deny
Jobs	Profile setting	Use current setting	Deny
Mail	Profile setting	Use current setting	Deny
Messages	Profile setting	Use current setting	Deny
My Folder	Profile setting	Use current setting	Deny
Print	Profile setting	Use current setting	Deny
Sametime	Profile setting	Use current setting	Deny
Other	Profile setting	Use current setting	Deny

Save Cancel Apply

Policies help
View help for changing category access policies.

Simple Database User Database Policies

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



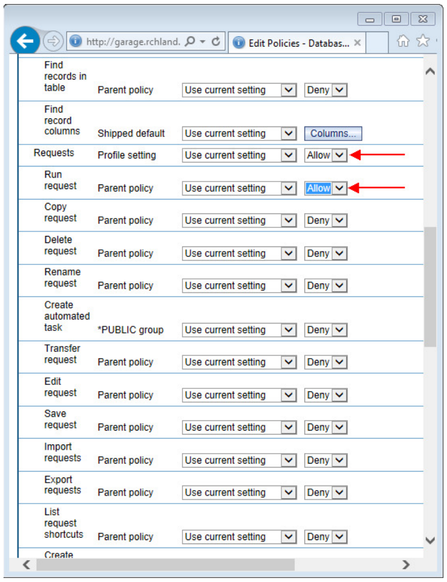
Edit Policies - Database

Profile: **REPORT_MAN**

Policy	Derived From	Action		S
Database access	Shipped default	Use current setting	Allow	
Database tab	Shipped default	Use current setting	Show	
Tables	Shipped default	Use current setting	Deny	
Maximum table rows	Shipped default	Use current setting	500	
Table filter	Shipped default	Use current setting	*USRLIBL	
Table filter is user preference	Shipped default	Use current setting	Allow	
Insert records into table	Shipped default	Use current setting	Allow	
Insert record columns	Shipped default	Use current setting	Columns...	
Update records in table	Shipped default	Use current setting	Allow	
Update record columns	Shipped default	Use current setting	Columns...	
Quick view table records	Shipped default	Use current setting	Allow	

Simple Database User Database Policies

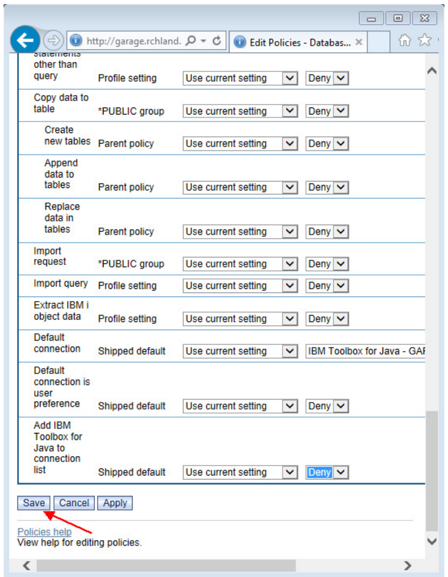
- Only allow the user the ability to run a saved DB request (Run request)



Find records in table	Parent policy	Use current setting	Deny
Find record columns	Shipped default	Use current setting	Columns...
Requests	Profile setting	Use current setting	Allow
Run request	Parent policy	Use current setting	Allow
Copy request	Parent policy	Use current setting	Deny
Delete request	Parent policy	Use current setting	Deny
Rename request	Parent policy	Use current setting	Deny
Create automated task	*PUBLIC group	Use current setting	Deny
Transfer request	Parent policy	Use current setting	Deny
Edit request	Parent policy	Use current setting	Deny
Save request	Parent policy	Use current setting	Deny
Import requests	Parent policy	Use current setting	Deny
Export requests	Parent policy	Use current setting	Deny
List request shortcuts	Parent policy	Use current setting	Deny
Create			

Simple Database User Database Policies

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

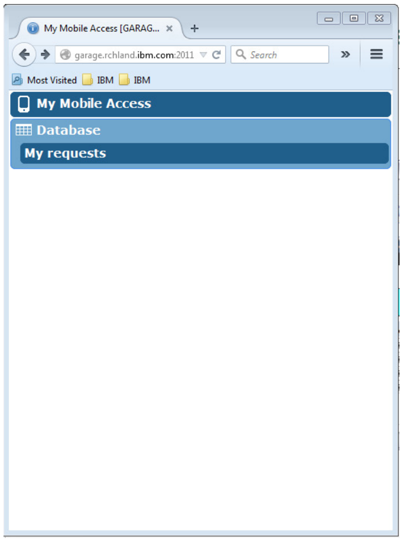


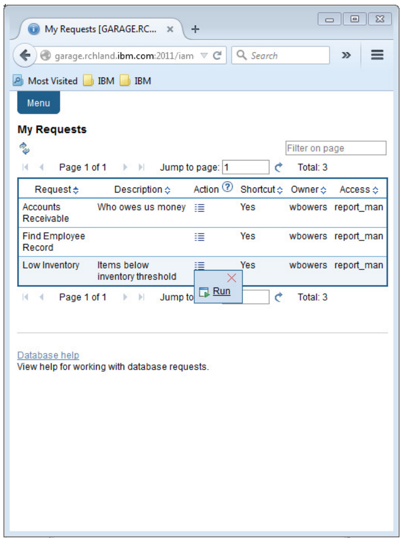
statements other than query	Profile setting	Use current setting	Deny
Copy data to table	*PUBLIC group	Use current setting	Deny
Create new tables	Parent policy	Use current setting	Deny
Append data to tables	Parent policy	Use current setting	Deny
Replace data in tables	Parent policy	Use current setting	Deny
Import request	*PUBLIC group	Use current setting	Deny
Import query	Profile setting	Use current setting	Deny
Extract IBM i object data	Profile setting	Use current setting	Deny
Default connection	Shipped default	Use current setting	IBM Toolbox for Java - GAI
Default connection is user preference	Shipped default	Use current setting	Deny
Add IBM Toolbox for Java to connection list	Shipped default	Use current setting	Deny

Policies help
View help for editing policies.

Simple Database User - Results

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





My Requests

Filter on page

Page 1 of 1 Jump to page: 1 Total: 3

Request	Description	Action	Shortcut	Owner	Access
Accounts Receivable	Who owes us money	☰	Yes	wbowers	report_man
Find Employee Record		☰	Yes	wbowers	report_man
Low Inventory	Items below inventory threshold	☰	Yes	wbowers	report_man

Page 1 of 1 Jump to Total: 3

Database help
View help for working with database requests.

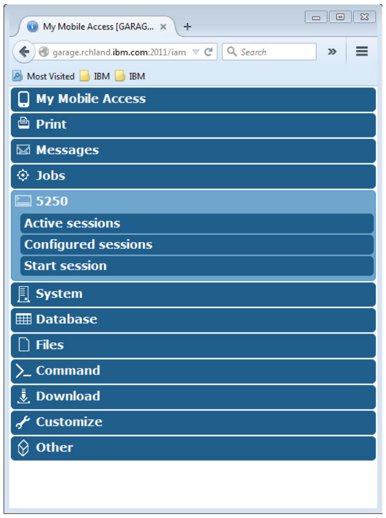
Policies Example: 5250 Access

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.

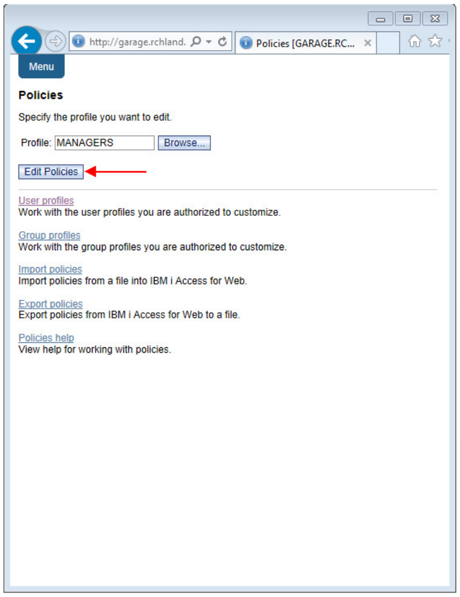
5250 Access - Before

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



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.



Policies

Specify the profile you want to edit.

Profile: MANAGERS Browse...

Edit Policies

User profiles
Work with the user profiles you are authorized to customize.

Group profiles
Work with the group profiles you are authorized to customize.

Import policies
Import policies from a file into IBM i Access for Web.

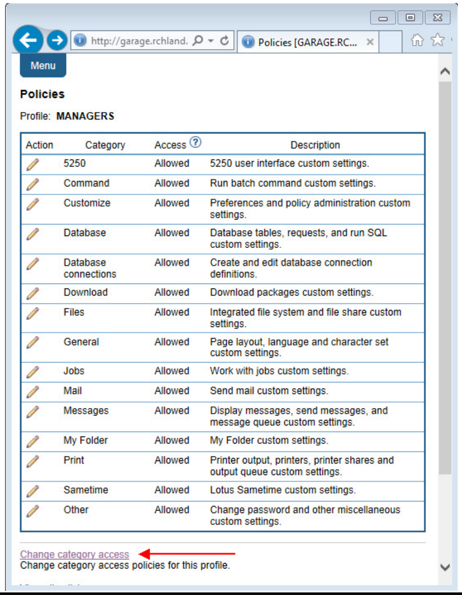
Export policies
Export policies from IBM i Access for Web to a file.

Policies help
View help for working with policies.

Power Systems

5250 Access - Categories

- Change Category Access



Policies

Profile: **MANAGERS**

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

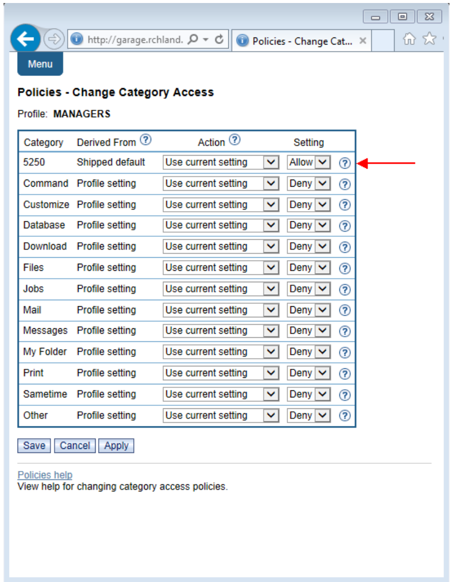
Change category access

Change category access policies for this profile.

Power Systems

5250 Access - Categories

- Turn off all non-5250 functions by Applying setting of Deny to Profile
- Leave 5250 to Allow



Policies - Change Category Access

Profile: **MANAGERS**

Category	Derived From	Action	Setting
5250	Shipped default	Use current setting	Allow
Command	Profile setting	Use current setting	Deny
Customize	Profile setting	Use current setting	Deny
Database	Profile setting	Use current setting	Deny
Download	Profile setting	Use current setting	Deny
Files	Profile setting	Use current setting	Deny
Jobs	Profile setting	Use current setting	Deny
Mail	Profile setting	Use current setting	Deny
Messages	Profile setting	Use current setting	Deny
My Folder	Profile setting	Use current setting	Deny
Print	Profile setting	Use current setting	Deny
Sametime	Profile setting	Use current setting	Deny
Other	Profile setting	Use current setting	Deny

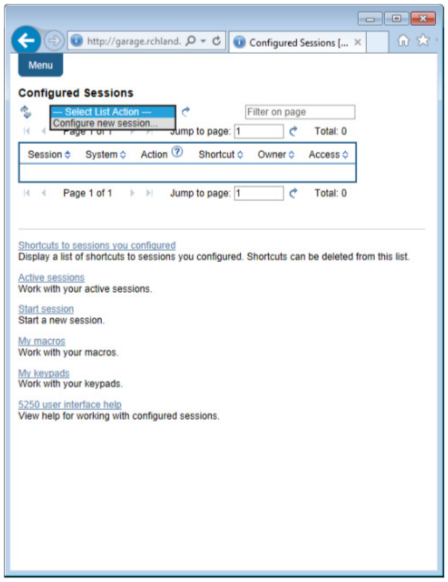
Save Cancel Apply

Policies help

View help for changing category access policies.

5250 Access – Functional Setup

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



Configured Sessions

Shortcuts to sessions you configured
Display a list of shortcuts to sessions you configured. Shortcuts can be deleted from this list.

Active sessions
Work with your active sessions.

Start session
Start a new session.

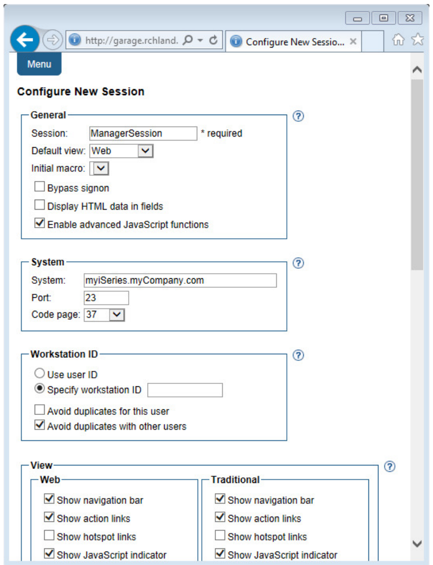
My macros
Work with your macros.

My keypads
Work with your keypads.

5250 user interface help
View help for working with configured sessions.

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.



Configure New Session

General

Session: ManagerSession * required
Default view: Web
Initial macro:
□ Bypass signon
□ Display HTML data in fields
☑ Enable advanced JavaScript functions

System

System: myiSeries.myCompany.com
Port: 23
Code page: 37

Workstation ID

○ Use user ID
● Specify workstation ID
□ Avoid duplicates for this user
☑ Avoid duplicates with other users

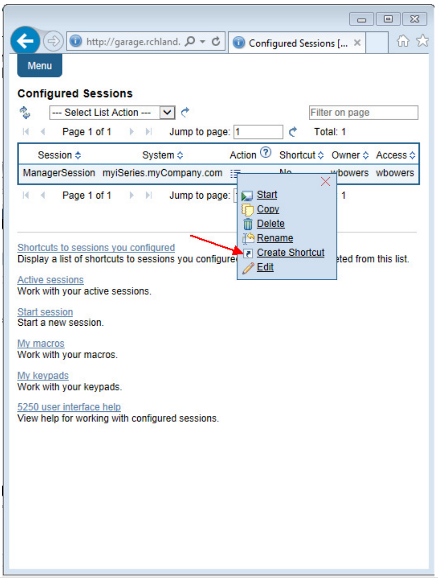
View

Web
☑ Show navigation bar
☑ Show action links
□ Show hotspot links
☑ Show JavaScript indicator

Traditional
☑ Show navigation bar
☑ Show action links
□ Show hotspot links
☑ Show JavaScript indicator

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.



Configured Sessions

Page 1 of 1   Jump to page: 1   Total: 1

Session	System	Action	Shortcut	Owner	Access
ManagerSession	myiSeries.myCompany.com	☰	No	wbowers	wbowers

Page 1 of 1   Jump to page:

Shortcuts to sessions you configured
Display a list of shortcuts to sessions you configure[...]ted from this list.

Active sessions
Work with your active sessions.

Start session
Start a new session.

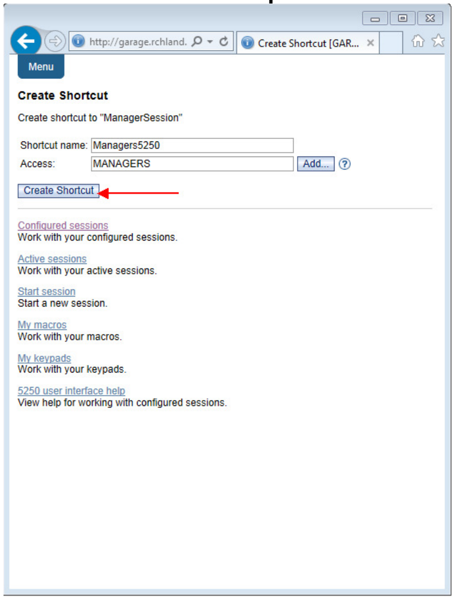
My macros
Work with your macros.

My keypads
Work with your keypads.

5250 user interface help
View help for working with configured sessions.

5250 Access – Functional Setup

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



Create Shortcut

Create shortcut to "ManagerSession"

Shortcut name: Managers5250

Access: MANAGERS

Configured sessions
Work with your configured sessions.

Active sessions
Work with your active sessions.

Start session
Start a new session.

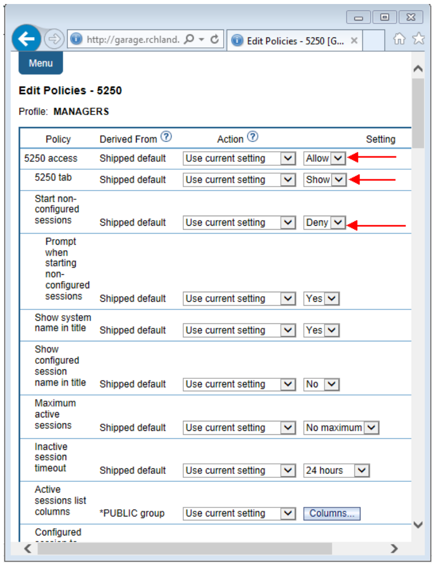
My macros
Work with your macros.

My keypads
Work with your keypads.

5250 user interface help
View help for working with configured sessions.

5250 Access – Customize Policies

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



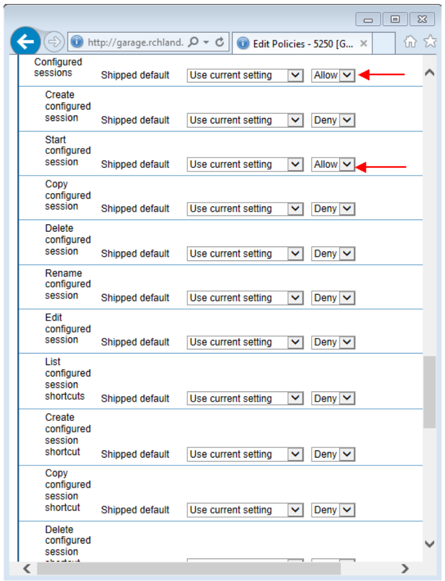
Edit Policies - 5250

Profile: MANAGERS

Policy	Derived From	Action	Setting
5250 access	Shipped default	Use current setting	Allow
5250 tab	Shipped default	Use current setting	Show
Start non-configured sessions	Shipped default	Use current setting	Deny
Prompt when starting non-configured sessions	Shipped default	Use current setting	Yes
Show system name in title	Shipped default	Use current setting	Yes
Show configured session name in title	Shipped default	Use current setting	No
Maximum active sessions	Shipped default	Use current setting	No maximum
Inactive session timeout	Shipped default	Use current setting	24 hours
Active sessions list columns	*PUBLIC group	Use current setting	Columns...
Configured			

5250 Access – More 5250 Settings

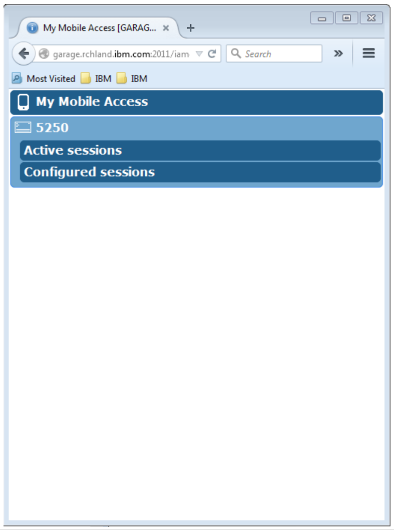
- Set all 5250 policies to Deny, except Configured Sessions and Start Configured Sessions.
- You may also want to allow them to access My Keypads and My Macros.

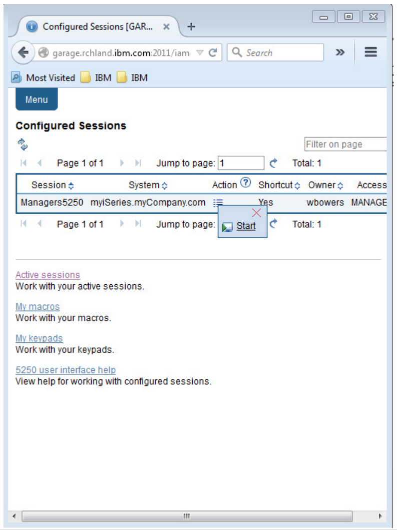


Configured sessions	Shipped default	Use current setting	Allow
Create configured session	Shipped default	Use current setting	Deny
Start configured session	Shipped default	Use current setting	Allow
Copy configured session	Shipped default	Use current setting	Deny
Delete configured session	Shipped default	Use current setting	Deny
Rename configured session	Shipped default	Use current setting	Deny
Edit configured session	Shipped default	Use current setting	Deny
List configured session shortcuts	Shipped default	Use current setting	Deny
Create configured session shortcut	Shipped default	Use current setting	Deny
Copy configured session shortcut	Shipped default	Use current setting	Deny
Delete configured session			

Example: 5250 Access – Results

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





Configured Sessions

Page 1 of 1 Jump to page: 1 Total: 1

Session	System	Action	Shortcut	Owner	Access
Managers5250	myiSeries.myCompany.com	☰	Yes	wbowers	MANAGE

Page 1 of 1 Jump to page: Total: 1

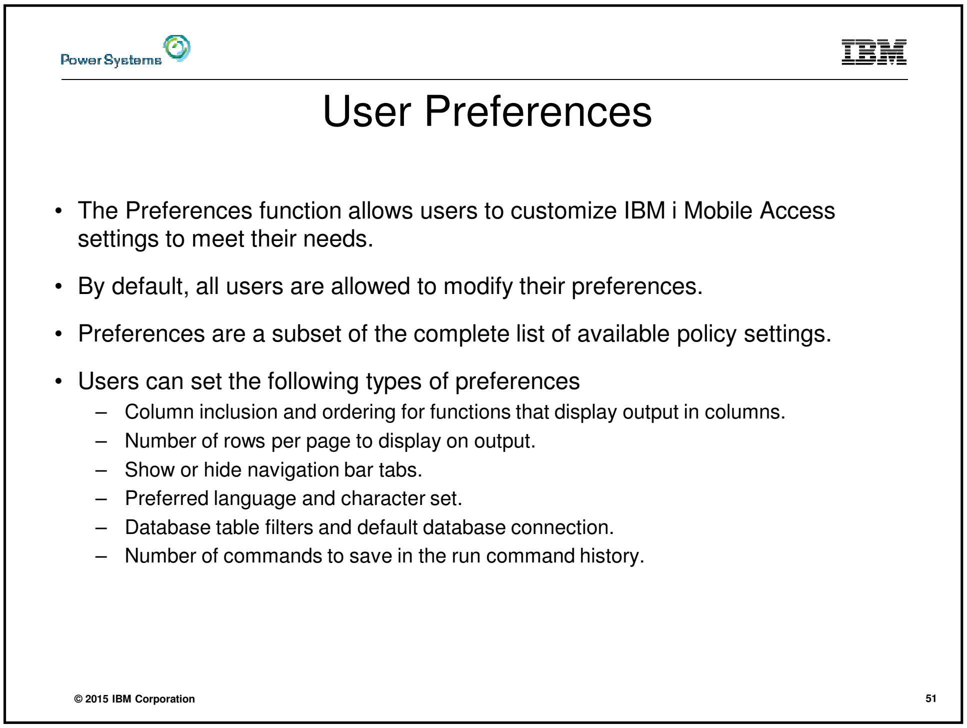
Active sessions
Work with your active sessions.

My macros
Work with your macros.

My keypads
Work with your keypads.

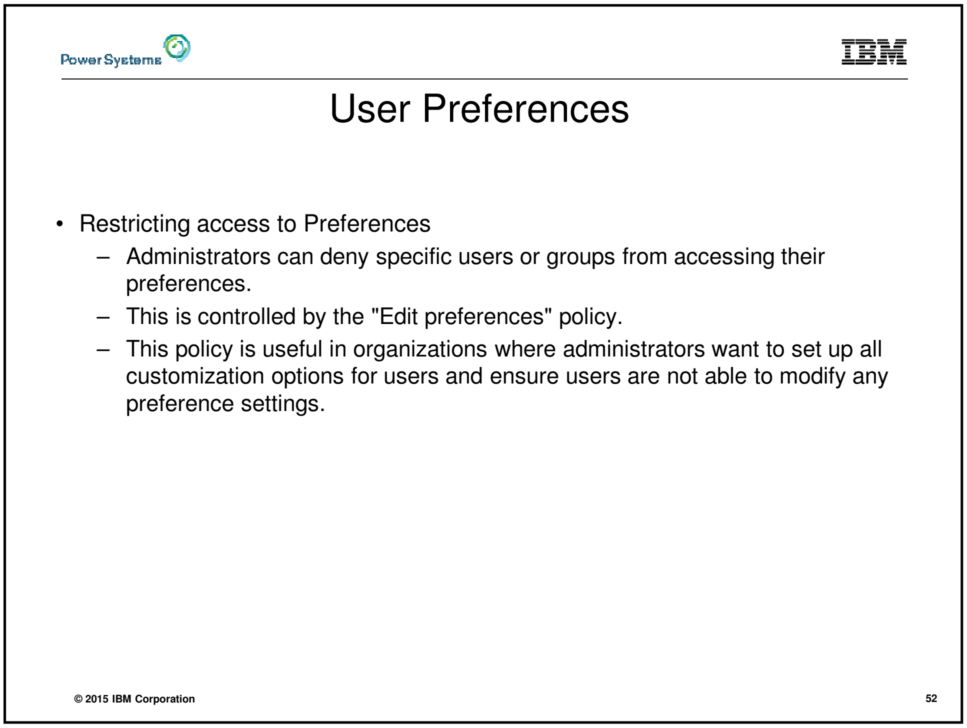
5250 user interface help
View help for working with configured sessions.

User Preferences



User Preferences

- The Preferences function allows users to customize IBM i Mobile Access 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

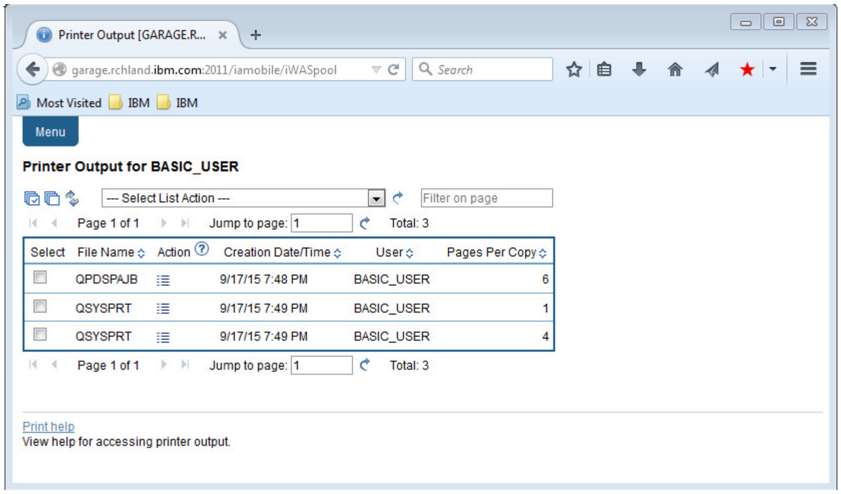
- Restricting access to Preferences
  - Administrators can deny specific users or groups from accessing their preferences.
  - This is controlled by the "Edit preferences" policy.
  - This policy is useful in organizations where administrators want to set up all customization options for users and ensure 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.

Printer Output - Default

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



Printer Output [GARAGE.R...
garage.rchland.ibm.com:2011/iamobile/iWASpool
Search
Most Visited
IBM
IBM
Menu

Printer Output for BASIC_USER

--- Select List Action ---

Filter on page

Page 1 of 1 Jump to page: 1 Total: 3

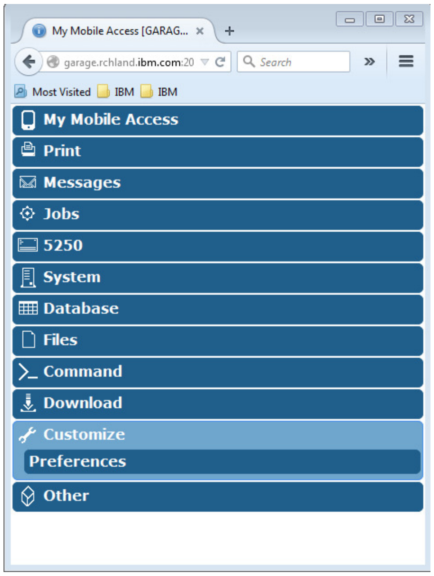
Select	File Name	Action	Creation Date/Time	User	Pages Per Copy
□	QPDSPAJB	☰	9/17/15 7:48 PM	BASIC_USER	6
□	QSYSPRT	☰	9/17/15 7:49 PM	BASIC_USER	1
□	QSYSPRT	☰	9/17/15 7:49 PM	BASIC_USER	4

Page 1 of 1 Jump to page: 1 Total: 3

Print help
View help for accessing printer output.

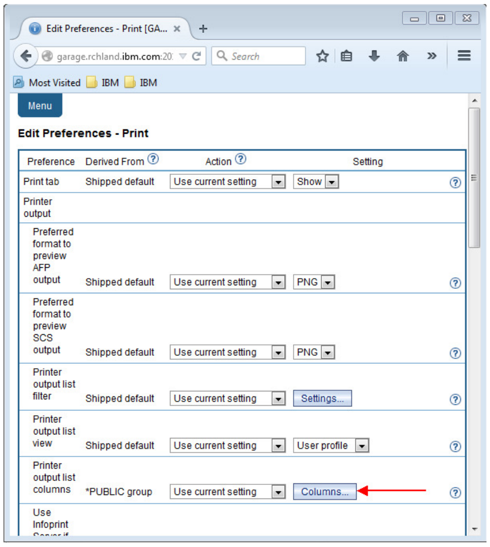
User Preferences, Printer Output

- Click on the Customize tab to work with Preferences.



User Preferences, Printer Output

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

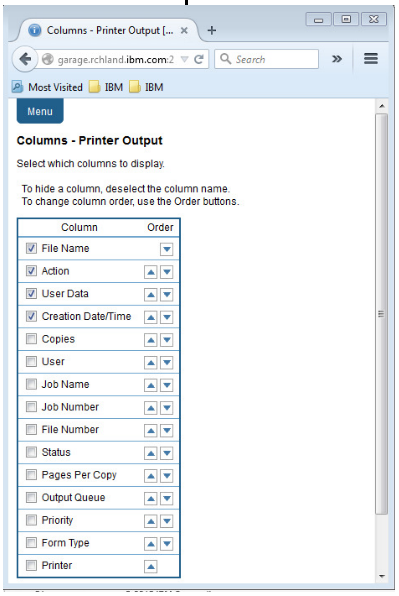


Edit Preferences - Print

Preference	Derived From ?	Action ?	Setting	
Print tab	Shipped default	Use current setting	Show	?
Printer output				
Preferred format to preview AFP output	Shipped default	Use current setting	PNG	?
Preferred format to preview SCS output	Shipped default	Use current setting	PNG	?
Printer output list filter	Shipped default	Use current setting	Settings...	?
Printer output list view	Shipped default	Use current setting	User profile	?
Printer output list columns	*PUBLIC group	Use current setting	Columns...	?
Use Infoprint				

User Preferences, Printer Output

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



Columns - Printer Output

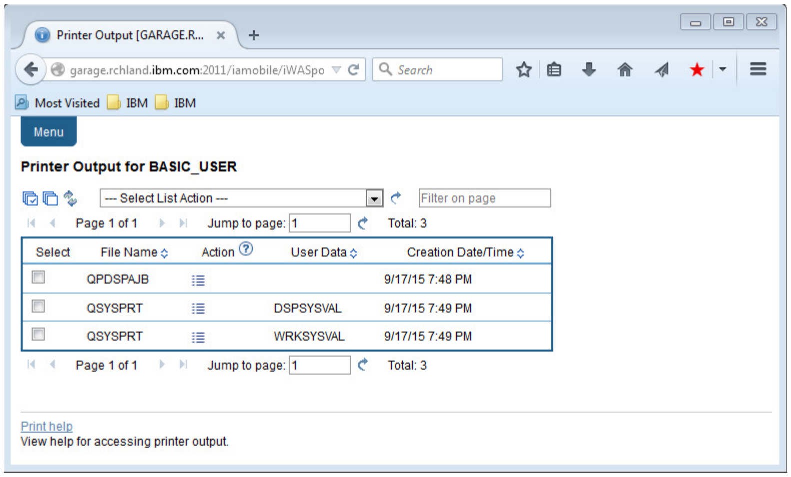
Select which columns to display.

To hide a column, deselect the column name.
To change column order, use the Order buttons.

Column	Order
☑ File Name	▼
☑ Action	▲ ▼
☑ User Data	▲ ▼
☑ Creation Date/Time	▲ ▼
□ Copies	▲ ▼
□ User	▲ ▼
□ Job Name	▲ ▼
□ Job Number	▲ ▼
□ File Number	▲ ▼
□ Status	▲ ▼
□ Pages Per Copy	▲ ▼
□ Output Queue	▲ ▼
□ Priority	▲ ▼
□ Form Type	▲ ▼
□ Printer	▲

User Preferences, Printer Output

- The printer output display now has custom columns.



Printer Output [GARAGE.R...
garage.rchland.ibm.com:2011/iamobile/iWASpo
Search
Most Visited
IBM
IBM
Menu

Printer Output for BASIC_USER

--- Select List Action ---   Filter on page

Page 1 of 1   Jump to page: 1   Total: 3

Select	File Name	Action	User Data	Creation Date/Time
□	QPDSPAJB	☰		9/17/15 7:48 PM
□	QSYSPRT	☰	DSPSYSVAL	9/17/15 7:49 PM
□	QSYSPRT	☰	WRKSYSVAL	9/17/15 7:49 PM

Page 1 of 1   Jump to page: 1   Total: 3

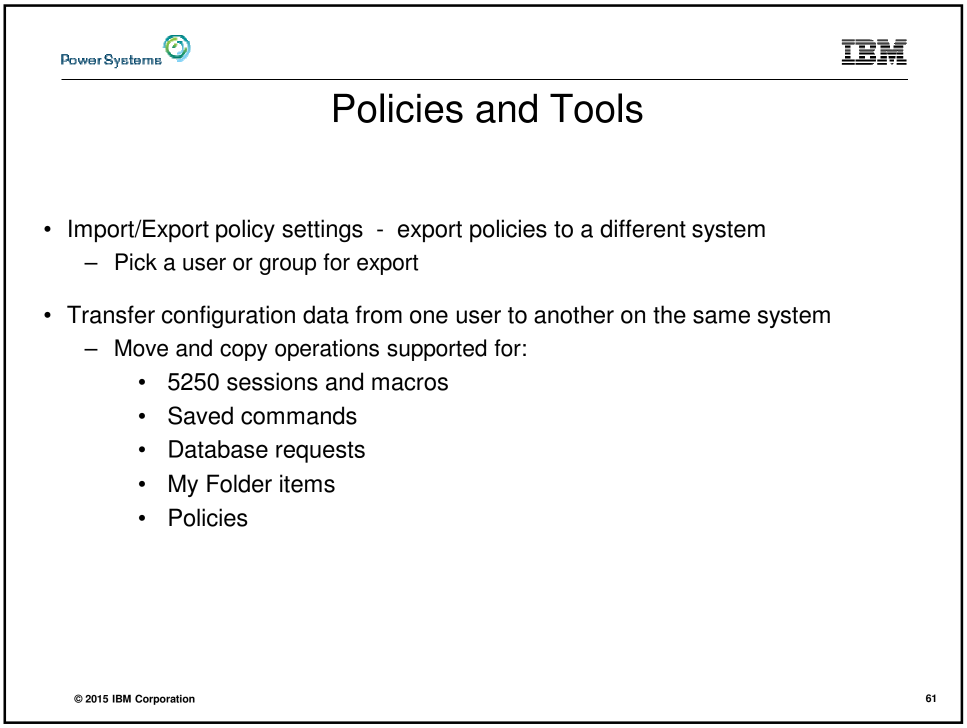
Print help
View help for accessing printer output.

User Preferences - Printer Output

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

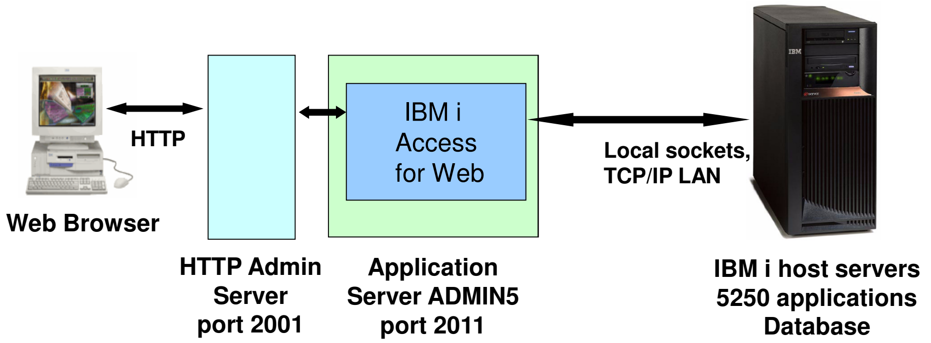


Policies and Tools

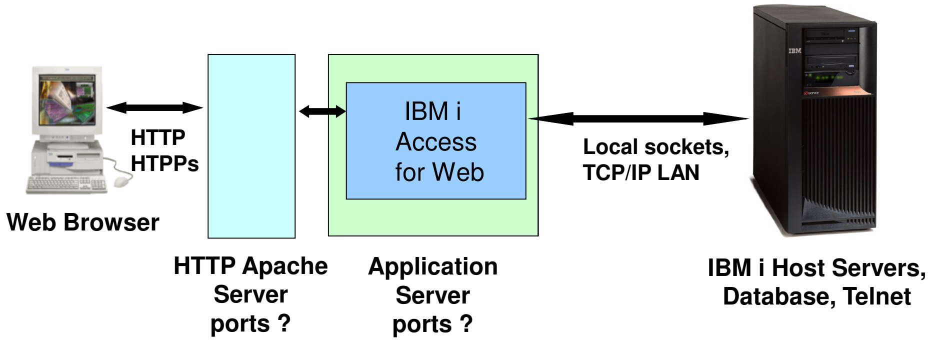
- Import/Export policy settings - export policies to a different system
  - Pick a user or group for export
- Transfer configuration data from one user to another on the same system
  - Move and copy operations supported for:
    - 5250 sessions and macros
    - Saved commands
    - Database requests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

Environment Security

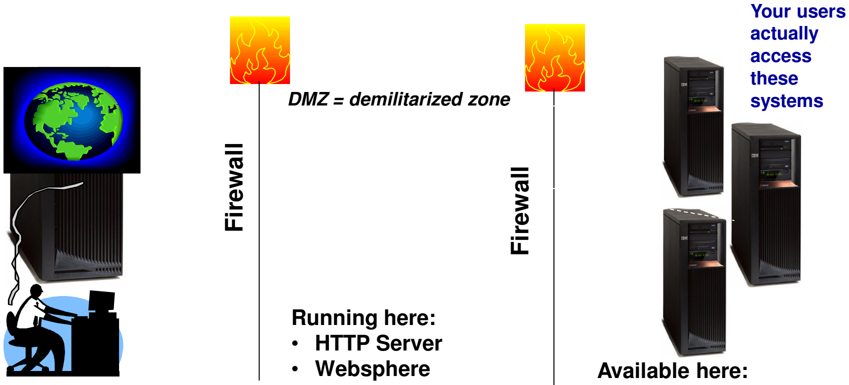
IBM i Mobile Access Default Environment


HTTP
Web Browser
IBM i Access for Web
Local sockets, TCP/IP LAN
HTTP Admin Server port 2001
Application Server ADMIN5 port 2011
IBM i host servers 5250 applications Database

IBM i Access for Web Environment


HTTP
HTPPs
Web Browser
IBM i Access for Web
Local sockets, TCP/IP LAN
HTTP Apache Server ports ?
Application Server ports ?
IBM i Host Servers, Database, Telnet

Access for Web Environment



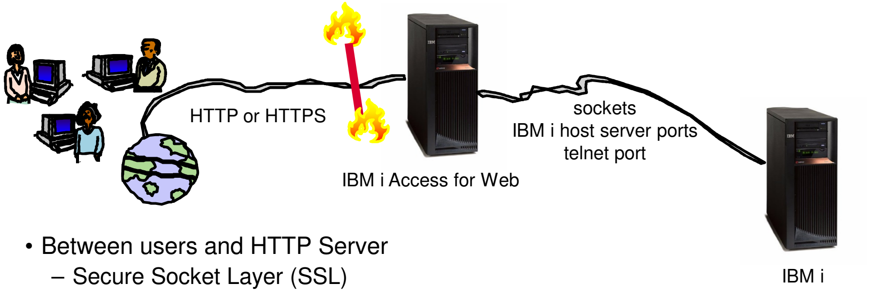
Running here:

- HTTP Server
- Websphere Application Server or Integrated Web Application Server
- IBM i Access for Web
  - ➢ "Target Server" parameter

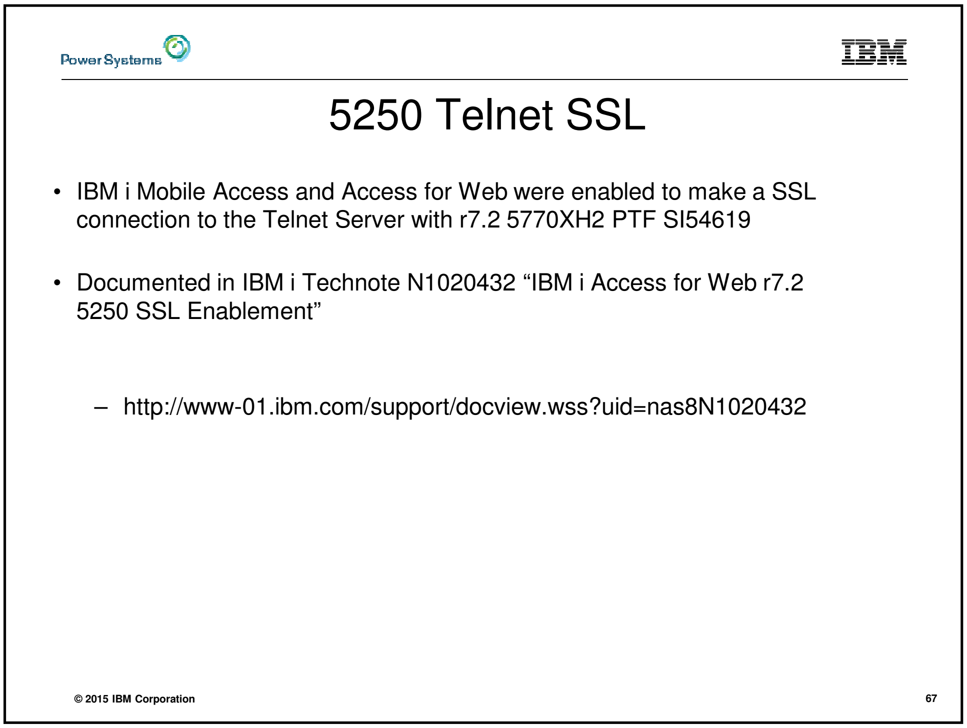
Available here:

- Access for Web 57xx-XH2 LPP
- IBM i Access Family 57xx-XW1 available licenses
- IBM i Host Servers and Telnet Server

Access for Web Environment



- Between users and HTTP Server
  - – Secure Socket Layer (SSL)
  - – Virtual Private Networking (VPN)
  - – Firewalls
- Between IBM i Access for Web and IBM i on the same System
  - – TCP/IP sockets over loopback to Host Server or Telnet
  - – Telnet SSL available on same or different system



5250 Telnet SSL

- IBM i Mobile Access and Access for Web were enabled to make a SSL connection to the Telnet Server with r7.2 5770XH2 PTF SI54619

- Documented in IBM i Technote N1020432 “IBM i Access for Web r7.2 5250 SSL Enablement”

  – http://www-01.ibm.com/support/docview.wss?uid=nas8N1020432

Authentication Options

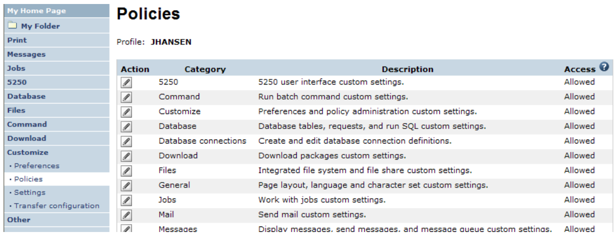
Authorization and Authentication

- How does the user authenticate to IBM i Mobile Access or 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**

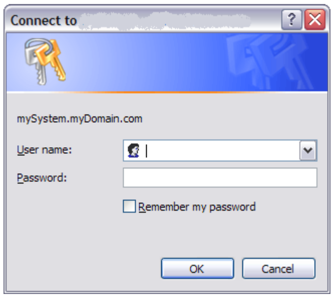
Action	Category	Description	Access
✎	5250	5250 user interface custom settings.	Allowed
✎	Command	Run batch command custom settings.	Allowed
✎	Customize	Preferences and policy administration custom settings.	Allowed
✎	Database	Database tables, requests, and run SQL custom settings.	Allowed
✎	Database connections	Create and edit database connection definitions.	Allowed
✎	Download	Download packages custom settings.	Allowed
✎	Files	Integrated file system and file share custom settings.	Allowed
✎	General	Page layout, language and character set custom settings.	Allowed
✎	Jobs	Work with jobs custom settings.	Allowed
✎	Mail	Send mail custom settings.	Allowed
✎	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 (Default)
    - IBM i Access for Web handles the authentication
    - Only option on Integrated Application Server
  - 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



Connect to [redacted]

mySystem.myDomain.com

User name:

Password:

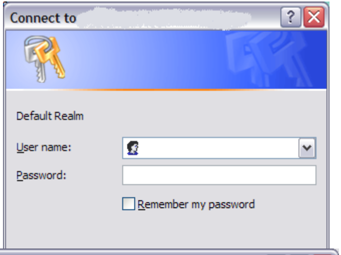
□ Remember my password

Application Server Authentication

- WebSphere handles authentication
- WebSphere credentials
  - Typically a user ID and password
  - Can be Windows domain login information
    - 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

- 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** (V6R1)
    - **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)

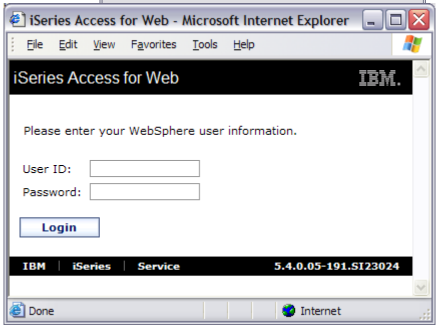


Default Realm

User name:

Password:

□ Remember my password


iSeries Access for Web - Microsoft Internet Explorer
File Edit View Favorites Tools Help
iSeries Access for Web
IBM.

Please enter your WebSphere user information.

User ID:

Password:

Login

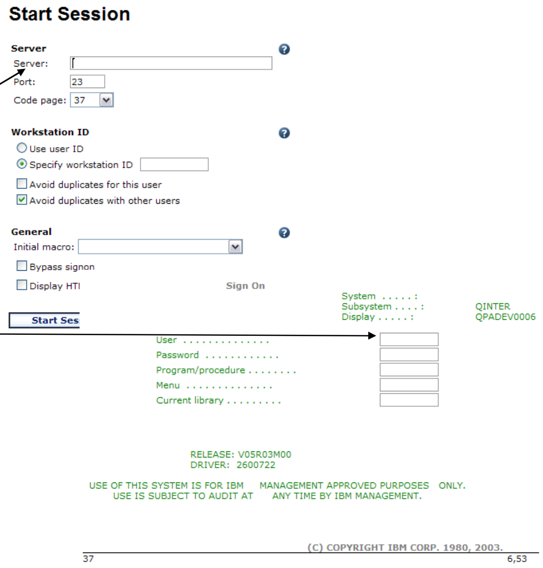
IBM | iSeries | Service 5.4.0.05-191.SI23024
Done
Internet

Application Server Authentication

- 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 authentiation
  - 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

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

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

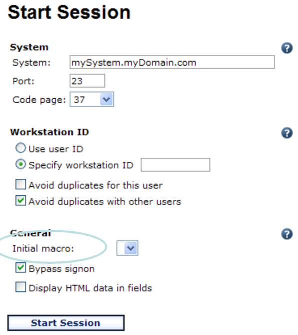
□ Display HTI

Start Ses

```
                              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.

                                        (C) COPYRIGHT IBM CORP. 1980, 2003.
37                                                                   6,53
```

5250 Bypass Signon

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



Start Session

System

System: mySystem.myDomain.com

Port: 23

Code page: 37

Workstation ID

○ Use user ID

● Specify workstation ID

□ Avoid duplicates for this user

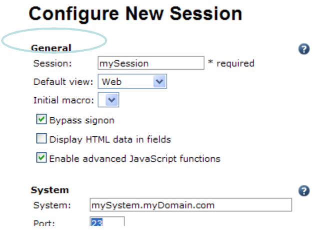
☑ Avoid duplicates with other users

General

Initial macro:

☑ Bypass signon

□ Display HTML data in fields



Configure New Session

General

Session: mySession * required

Default view: Web

Initial macro:

☑ Bypass signon

□ Display HTML data in fields

☑ Enable advanced JavaScript functions

System

System: mySystem.myDomain.com

Port: 23

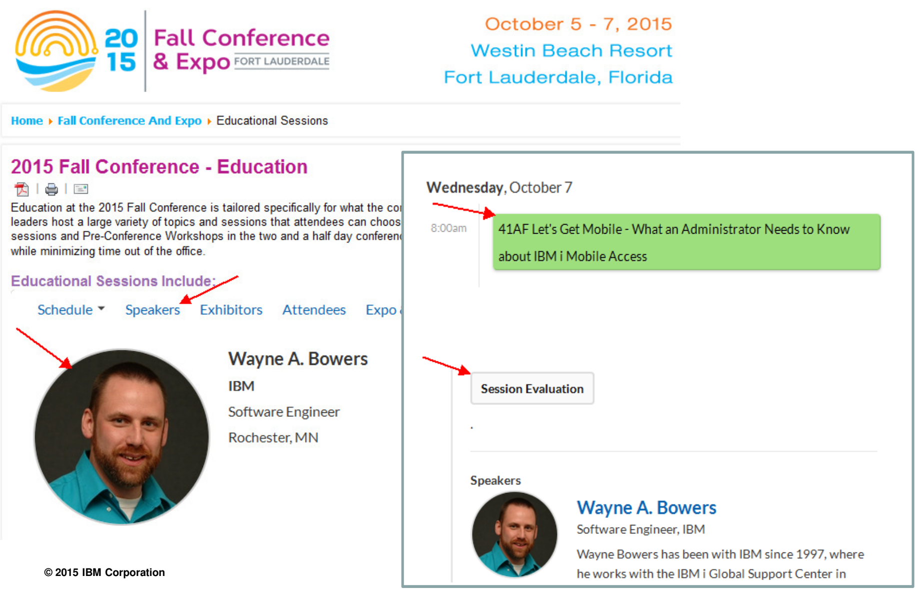
- **IBM i Access for Web must be configured for application authentication or application server authentication with Kerberos for bypass signon to be available**
  - CFGACCWEB2 AUTHTYPE(*APP) …
  - CFGACCWEB2 AUTHTYPE(*APPSVR) AUTHMETHOD(*KERBEROS) … (V6R1 Access for Web and WAS 6.1 or later)

Summary

- Overview
- IBM i Mobile Access Runtime Considerations
  - Use of policies
  - Use of preferences
- IBM i Mobile Access Environment Security Considerations
  - Secure Communications
  - Authentication security

Questions ?

Session Evaluation



2015 Fall Conference & Expo FORT LAUDERDALE

October 5 - 7, 2015
Westin Beach Resort
Fort Lauderdale, Florida

Home ▸ Fall Conference And Expo ▸ Educational Sessions

2015 Fall Conference - Education

Education at the 2015 Fall Conference is tailored specifically for what the co
leaders host a large variety of topics and sessions that attendees can choos
sessions and Pre-Conference Workshops in the two and a half day conferen
while minimizing time out of the office.

Educational Sessions Include:

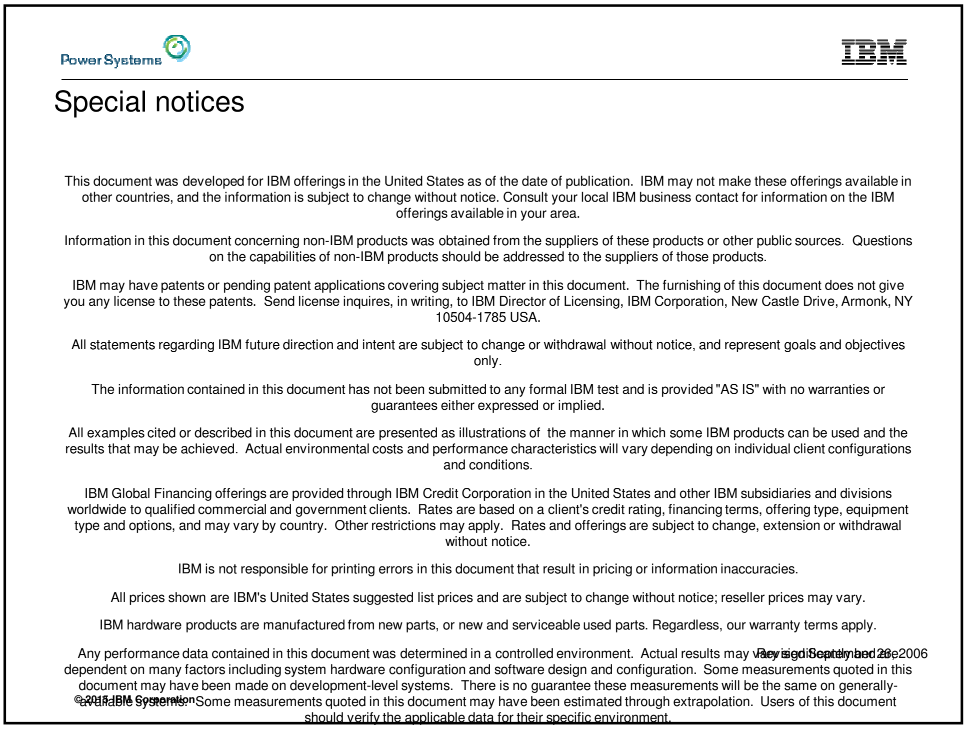
Wayne A. Bowers
IBM
Software Engineer
Rochester, MN

Wednesday, October 7

8:00am 41AF Let's Get Mobile - What an Administrator Needs to Know about IBM i Mobile Access

Speakers

Wayne A. Bowers
Software Engineer, IBM
Wayne Bowers has been with IBM since 1997, where he works with the IBM i Global Support Center in



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 5L, AIX 6 (logo), AS/400, BladeCenter, Blue Gene, 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, Active Memory, Balanced Warehouse, CacheFlow, Cool Blue, IBM Systems Director VMControl, pureScale, TurboCore, Chiphopper, Cloudscape, DB2 Universal Database, DS4000, DS6000, DS8000, EnergyScale, Enterprise Workload Manager, General Parallel 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, POWER6+, POWER7, System i, System p, System p5, System Storage, System z, TME 10, 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 full list of U.S. trademarks owned by IBM may be found at: http://www.**ibm.com**/legal/copytrade.shtml.

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

AltiVec is a trademark of Freescale Semiconductor, Inc.

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

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

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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.

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

Revised December 2, 2010

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

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.

Notes on performance estimates

- rPerf for AIX
- rPerf (Relative Performance) is an estimate of commercial processing performance relative to other IBM UNIX systems. It is derived from an IBM analytical model which uses characteristics from IBM internal workloads, TPC and SPEC benchmarks. The rPerf model is not intended to represent any specific public benchmark results and should not be reasonably used in that way. The model simulates some of the system operations such as CPU, cache and memory. However, the model does not simulate disk or network I/O operations.
- rPerf estimates are calculated based on systems with the latest levels of AIX and other pertinent software at the time of system announcement. Actual performance will vary based on application and configuration specifics. The IBM eServer pSeries 640 is the baseline reference system and has a value of 1.0. Although rPerf may be used to approximate relative IBM UNIX commercial processing performance, actual system performance may vary and is dependent upon many factors including system hardware configuration and software design and configuration. Note that the rPerf methodology used for the POWER6 systems is identical to that used for the POWER5 systems. Variations in incremental system performance may be observed in commercial workloads due to changes in the underlying system architecture.
- All performance estimates are provided "AS IS" and no warranties or guarantees are expressed or implied by IBM. Buyers should consult other sources of information, including system benchmarks, and application sizing guides to evaluate the performance of a system they are considering buying. For additional information about rPerf, contact your local IBM office or IBM authorized reseller.
- ==
- CPW for IBM i
- Commercial Processing Workload (CPW) is a relative measure of performance of processors running the IBM i operating system. Performance in customer environments may vary. The value is based on maximum configurations. More performance information is available in the Performance Capabilities Reference at: www.ibm.com/systems/i/solutions/perfmgmt/resource.html

Revised April 2, 2007