

Welcome to the Waitless World

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

Wayne Bowers  
wbowers@us.ibm.com

Session ID: 420016  
Agenda Key: 37CV - Rosedown Third Floor

© 2015 IBM Corporation

Welcome to the Waitless World

## Let's Get Mobile - IBM i Mobile Access



<b>Monday</b>		
3:30pm	Grand Salon B 9&12 First Floor	Let's Get Mobile – A Hands On Introduction to IBM i Mobile Access
<b>Tuesday</b>		
3:30pm	Rosedown Third Floor	Let's Get Mobile – 5250, Database, Print, and More on the Go
5:00pm	Rosedown Third Floor	Let's Get Mobile – What an Administrator Needs to Know about IBM i Mobile Access
<b>Wednesday</b>		
2:00pm	Magnolia Third Floor	OPEN LAB: Test Drive IBM i Mobile Access

© 2015 IBM Corporation


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

## Overview





PowerSystems  **Overview** Welcome to the Waitless World 

- 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



5


© 2015 IBM Corporation

PowerSystems  **Overview** Welcome to the Waitless World 


- 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
    - GA Level PTF SI56123 for 5770XH2 released in May 2015
    - Latest Function is available in current Access for Web Service Pack PTF SI60257 released in March 2016

6

© 2015 IBM Corporation



## Overview


Welcome to the Waitless World 


- 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)
      - » ENDTCPSPVR SERVER(\*IAS) INSTANCE(ADMIN5)
    - ADMIN5 runs on port 2011

© 2015 IBM Corporation

7



## Overview

Welcome to the Waitless World 


  

- 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 Application Server instances or other Web Application Server types like WebSphere Application Server, though additional customization is required

© 2015 IBM Corporation

8





# Overview


Welcome to the Waitless World 


- 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>

© 2015 IBM Corporation

9



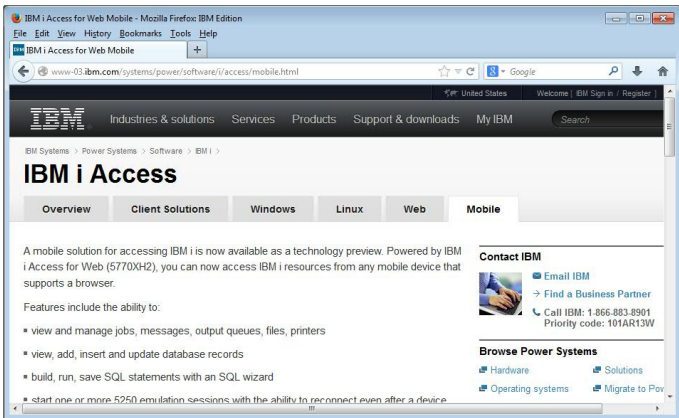
# Overview

Welcome to the Waitless World 

More Information:  
<http://www.ibm.com/systems/power/software/i/access/mobile.html>

Latest Information available at this location



© 2015 IBM Corporation

10

## 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

PowerSystems  **Controlling Access** Welcome to the Waitless World 

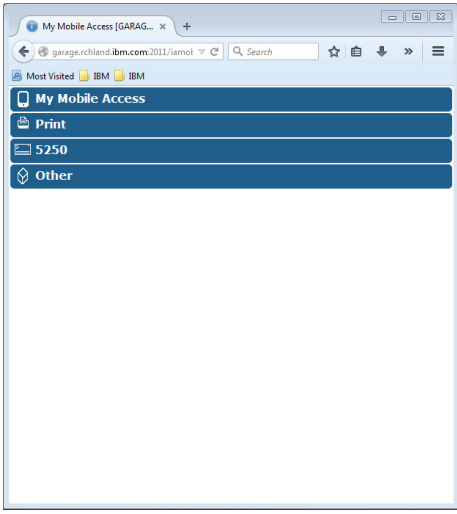
*Main Page = <http://<powerisys>:2001/iamobile>*





© 2015 IBM Corporation 13

PowerSystems  **Controlling Access** Welcome to the Waitless World 

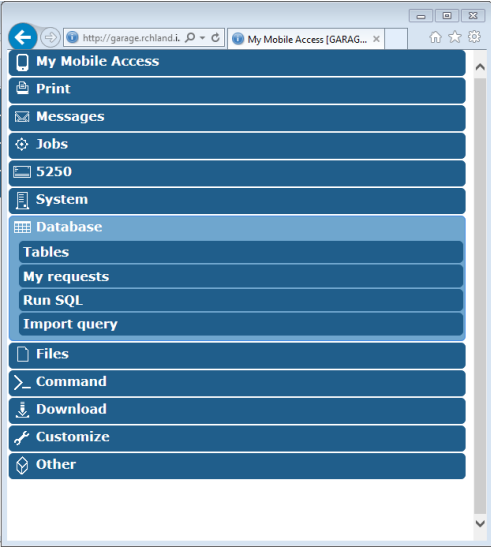
*Main Page = <http://<powerisys>:2001/iamobile>*



© 2015 IBM Corporation 14



PowerSystems  **Controlling Access** Welcome to the Waitless World 

Product functionality

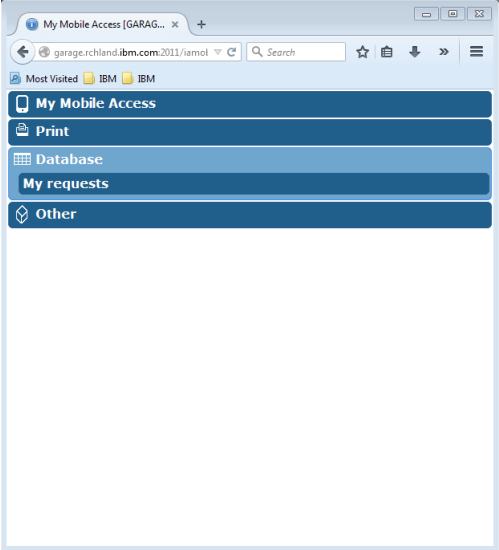


→

© 2015 IBM Corporation 15

PowerSystems  **Controlling Access** Welcome to the Waitless World 

Sample for a user that only performs preset database queries



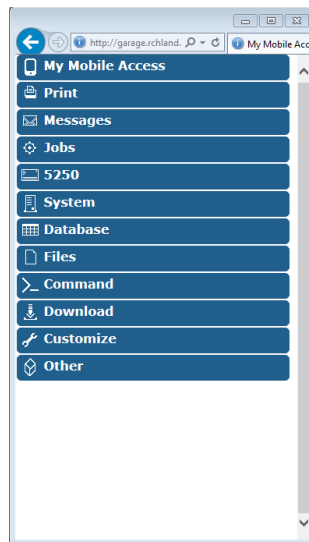
→

© 2015 IBM Corporation 16

## Controlling Access: Setting Policies



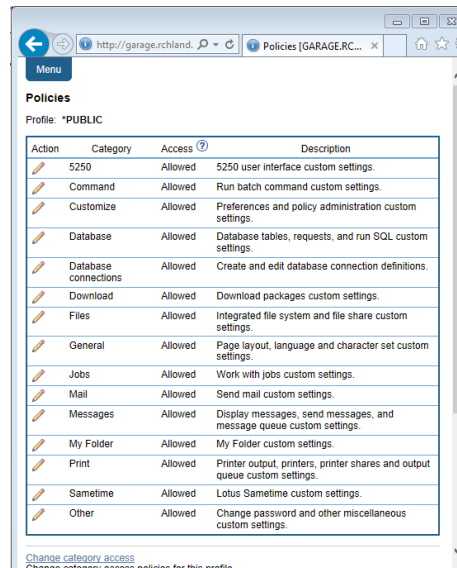
## Controlling User Access



- 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


- 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.

- 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




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


Welcome to the Waitless World


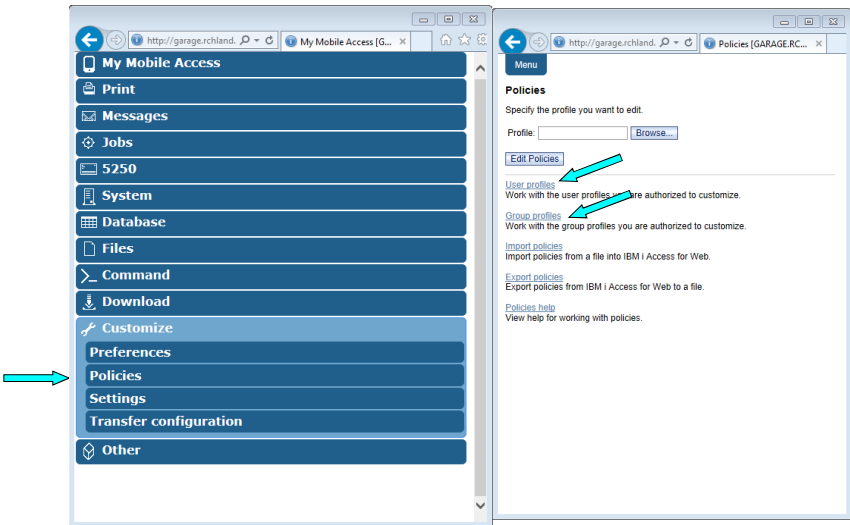
- IBM i Mobile Access ships with a set of default policy settings. The default policy settings allow most of the IBM i Mobile Access functions to be available for all users. Without any customization, users accessing IBM i Mobile Access could begin using most of the available functions.
- As an administrator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

© 2015 IBM Corporation
21



## Setting Policies

Welcome to the Waitless World




© 2015 IBM Corporation
22

## Setting Policies (continued)

Welcome to the Waitless World

© 2015 IBM Corporation

23

## Setting Policies (continued)

Welcome to the Waitless World

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.

© 2015 IBM Corporation

24



## Setting Policies (continued)

Welcome to the Waitless World

© 2015 IBM Corporation

25

## Setting Policies (continued)

Welcome to the Waitless World

### 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.

© 2015 IBM Corporation

26

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.

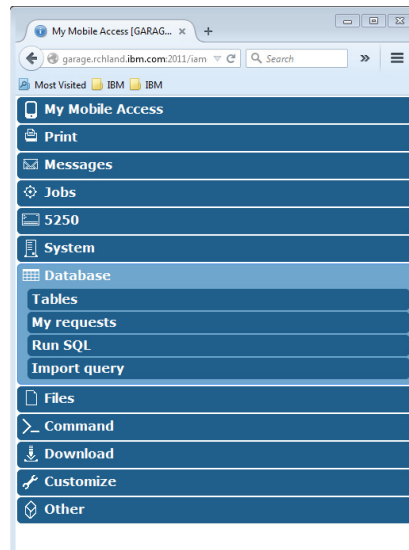
Action	Description
Profile setting	Indicates the setting is currently specific to the profile being customized. The setting had previously been applied to this profile.
Group – (groupName)	Indicates the setting is not specific to the profile being customized, but is being derived from the specified IBM 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: 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.

Accessing the Database tab of IBM i Mobile Access as user REPORT\_MAN



## Database User - Policies

Welcome to the Waitless World

- 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.

31 © 2015 IBM Corporation

## Database User - Categories

Welcome to the Waitless World

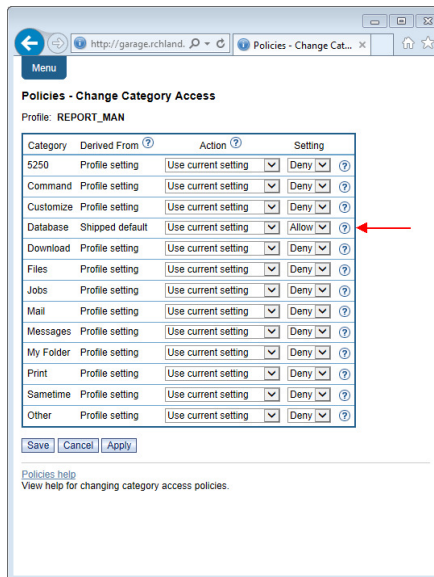
- Change Category Access

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

32 © 2015 IBM Corporation

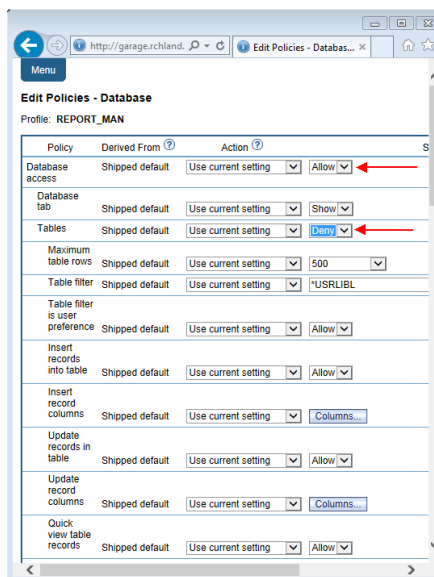
## Database User - Categories


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




## Database User – Database Policies

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

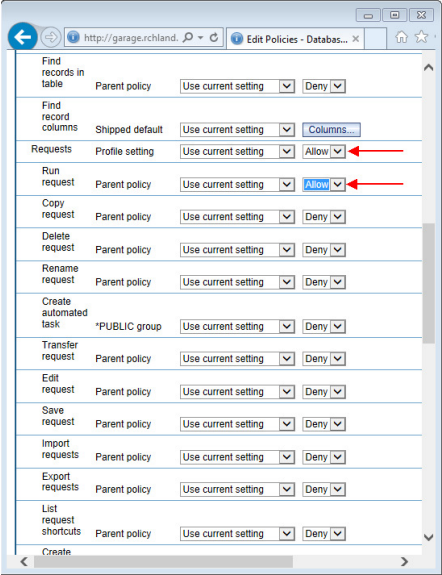





## Database User – Database Policies

Welcome to the Waitless World 


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



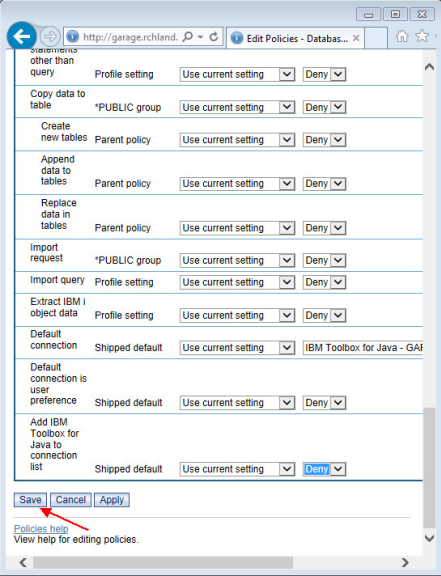
35 © 2015 IBM Corporation





## Database User – Database Policies

Welcome to the Waitless World 

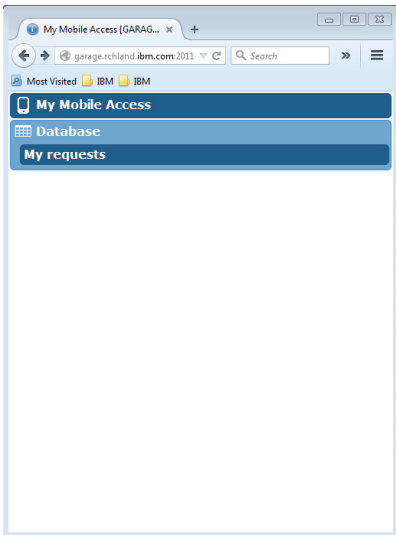
- Turn off the ability to perform the remaining database functions
- Save the changes



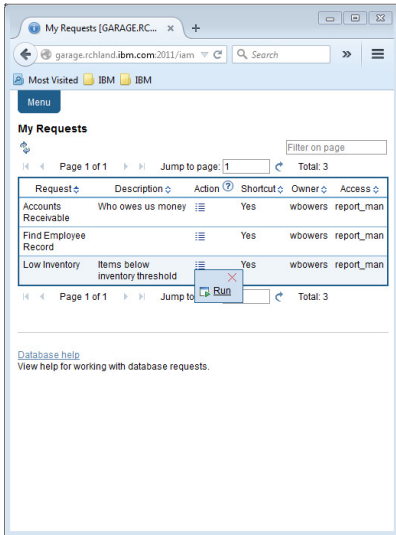
36 © 2015 IBM Corporation

PowerSystems  **Database User – Results** Welcome to the Waitless World 

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



My Mobile Access [GARAG... x +]  
 garage.richland.ibm.com:2011  
 Search  
 Most Visited IBM IBM  
 My Mobile Access  
 Database  
 My requests



My Requests [GARAG... x +]  
 garage.richland.ibm.com:2011/iam  
 Search  
 Most Visited IBM IBM  
 Menu  
 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: Run Total: 3

[Database help](#)  
View help for working with database requests.

37 © 2015 IBM Corporation

PowerSystems  Welcome to the Waitless World 

## Policies Example: 5250 Access

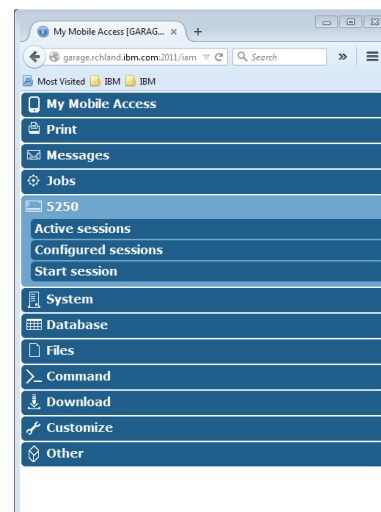


for Business


38 © 2015 IBM Corporation

- 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.


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








## 5250 Access - Policies


Welcome to the Waitless World 


- 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.



41  
© 2015 IBM Corporation

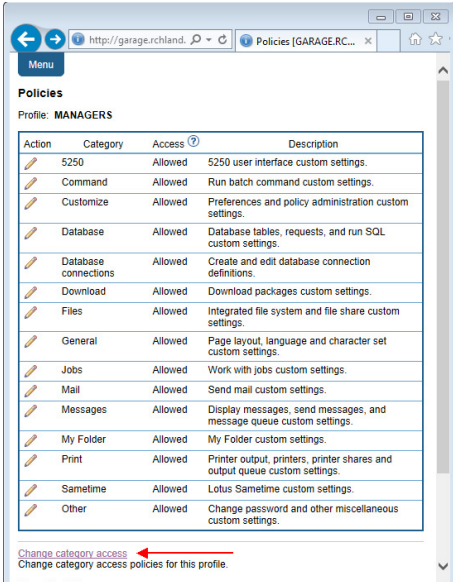


## 5250 Access - Categories

Welcome to the Waitless World 

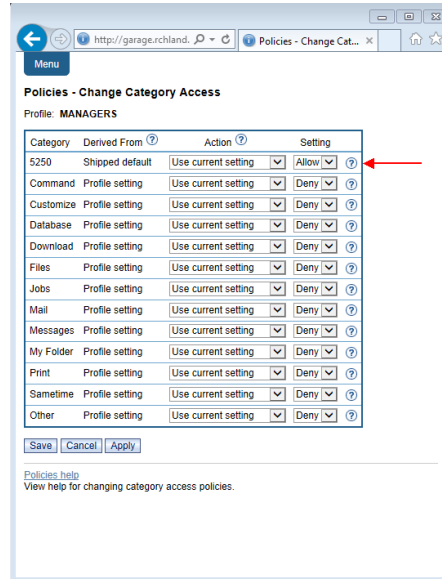
- Change Category Access



42  
© 2015 IBM Corporation

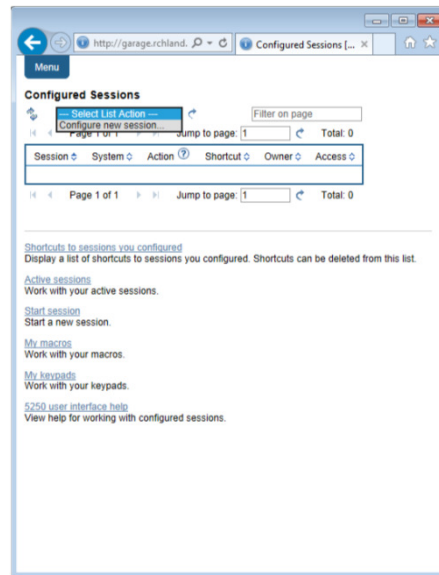
# 5250 Access - Categories


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




# 5250 Access – Functional Setup

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



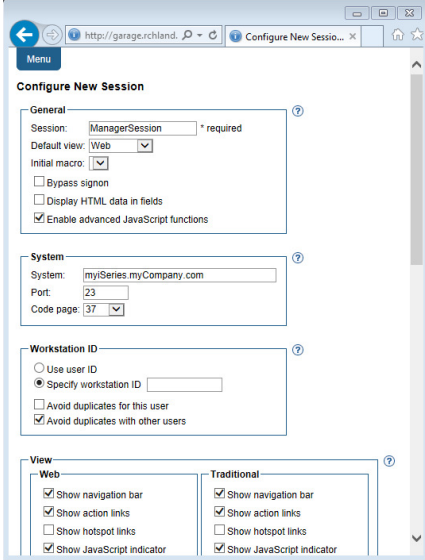


## 5250 Access – Functional Setup


Welcome to the Waitless World 


- 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.



45 © 2015 IBM Corporation

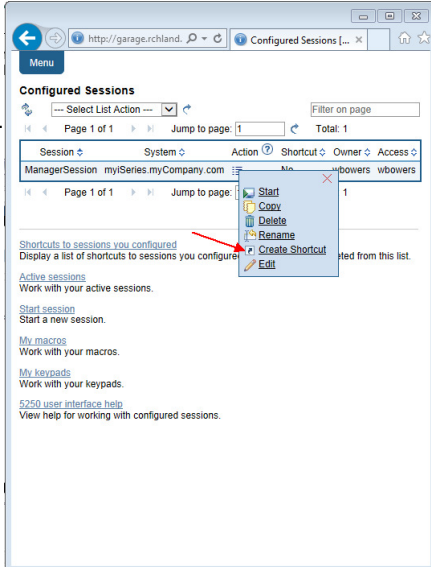


## 5250 Access – Functional Setup


Welcome to the Waitless World 

- 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.




46 © 2015 IBM Corporation



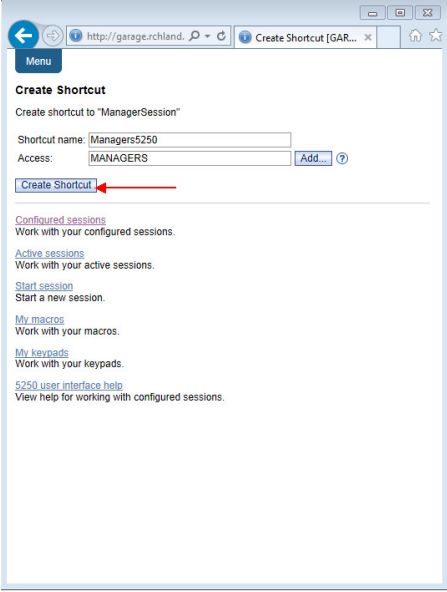
## 5250 Access – Functional Setup

Welcome to the Waitless World




  

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




47

© 2015 IBM Corporation



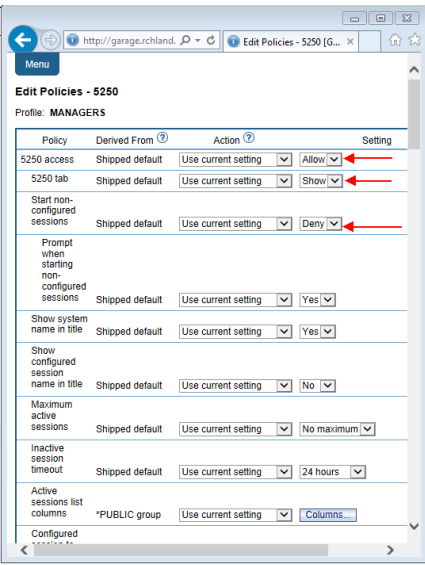
## 5250 Access – Customize Policies

Welcome to the Waitless World




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




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...

48

© 2015 IBM Corporation

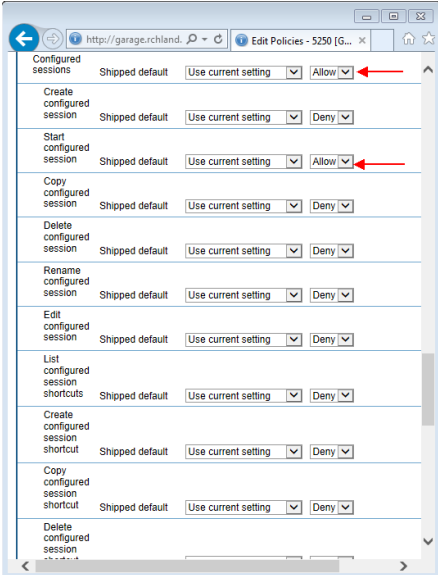


## 5250 Access – More 5250 Settings


Welcome to the Waitless World 


- 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.



49
© 2015 IBM Corporation

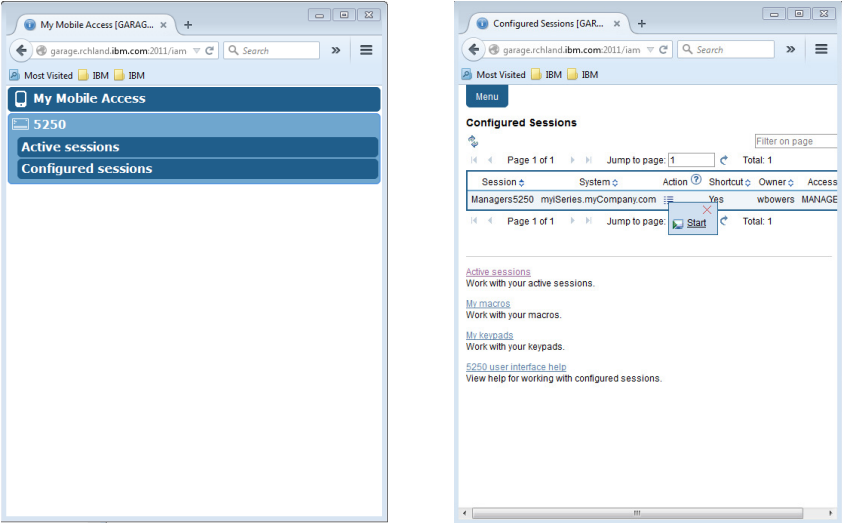


## Example: 5250 Access – Results

Welcome to the Waitless World 

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





50
© 2015 IBM Corporation

## 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.

Power Systems  **User Preferences** Welcome to the Waitless World 



- 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.

© 2015 IBM Corporation 53

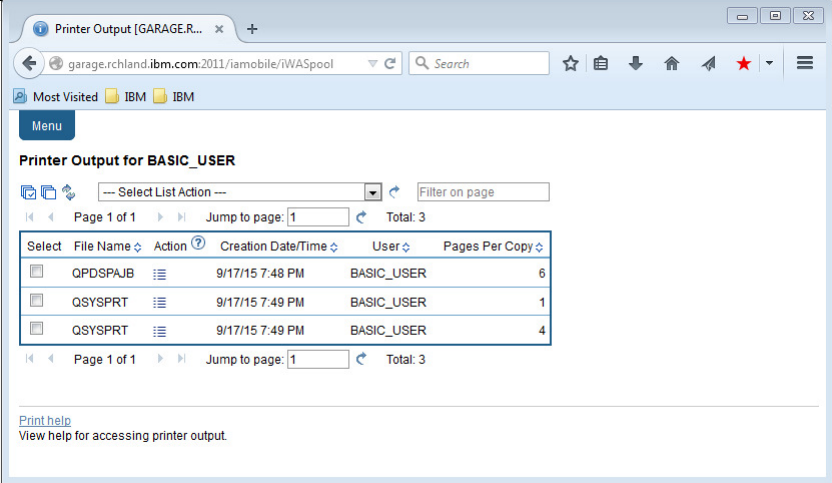
Power Systems  **Example: User Preferences** Welcome to the Waitless World   
**Printer Output**

- 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.

© 2015 IBM Corporation 54



PowerSystems  **Printer Output - Default** Welcome to the Waitless World 

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

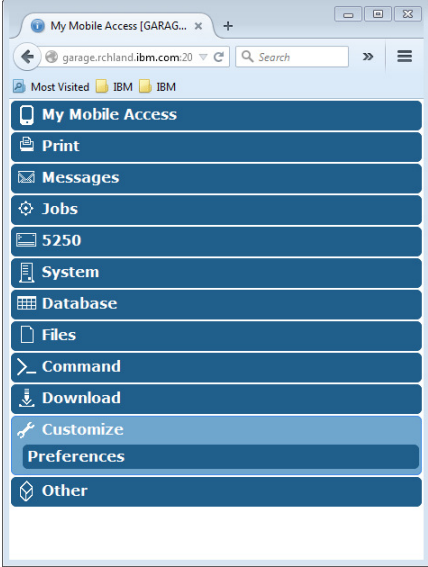


Select	File Name	Action	Creation Date/Time	User	Pages Per Copy
<input type="checkbox"/>	QPDSPAJB		9/17/15 7:48 PM	BASIC_USER	6
<input type="checkbox"/>	QSYSPRT		9/17/15 7:49 PM	BASIC_USER	1
<input type="checkbox"/>	QSYSPRT		9/17/15 7:49 PM	BASIC_USER	4

55 © 2015 IBM Corporation


PowerSystems  **User Preferences – Printer Output** Welcome to the Waitless World 

- Click on the Customize tab to work with Preferences.




56 © 2015 IBM Corporation



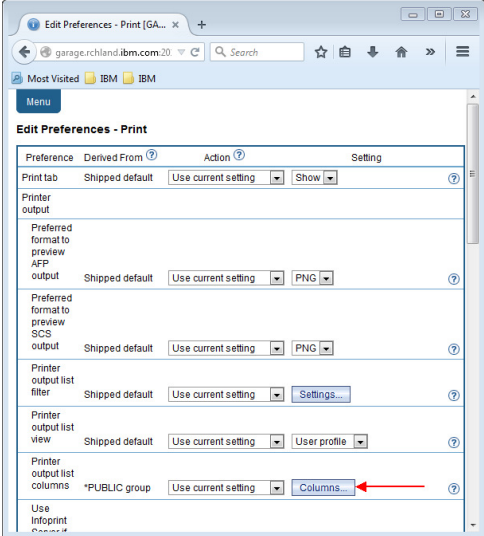


## User Preferences – Printer Output

Welcome to the Waitless World 


  

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




57

© 2015 IBM Corporation

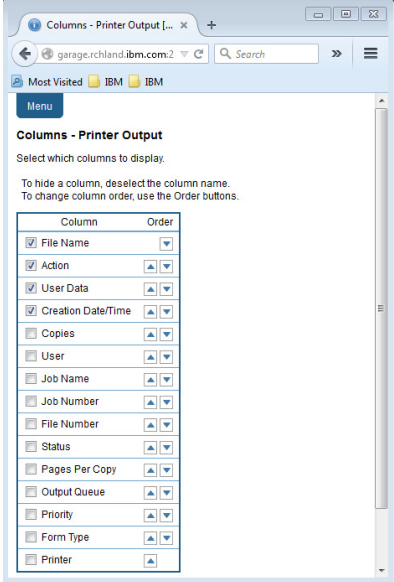


## User Preferences – Printer Output

Welcome to the Waitless World 



  

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

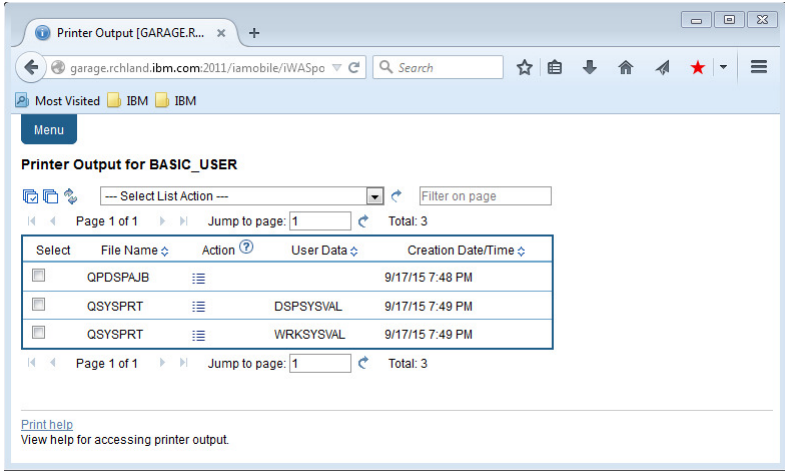


58

© 2015 IBM Corporation



PowerSystems  **User Preferences – Printer Output** Welcome to the Waitless World 

- The printer output display now has custom columns.



Select	File Name	Action	User Data	Creation Date/Time
<input type="checkbox"/>	QPDSPAJB			9/17/15 7:48 PM
<input type="checkbox"/>	QSYSPRT		DSPSYSVAL	9/17/15 7:49 PM
<input type="checkbox"/>	QSYSPRT		WRKSYSVAL	9/17/15 7:49 PM

59 © 2015 IBM Corporation

PowerSystems  **User Preferences – Printer Output** Welcome to the Waitless World 

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.

60 © 2015 IBM Corporation

## Administrative Tools



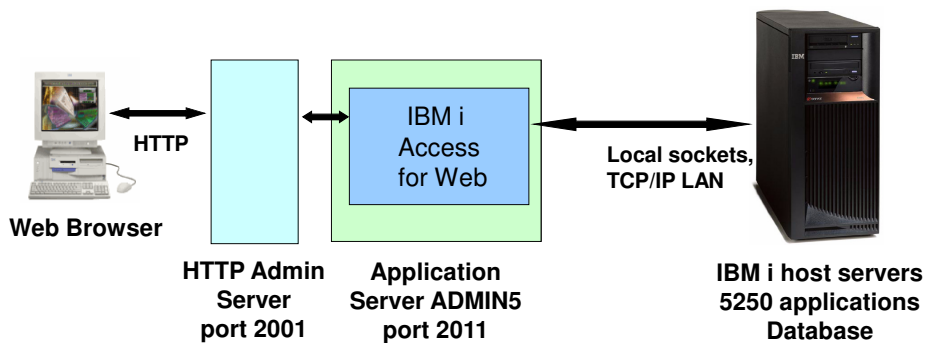
## Policies and Tools

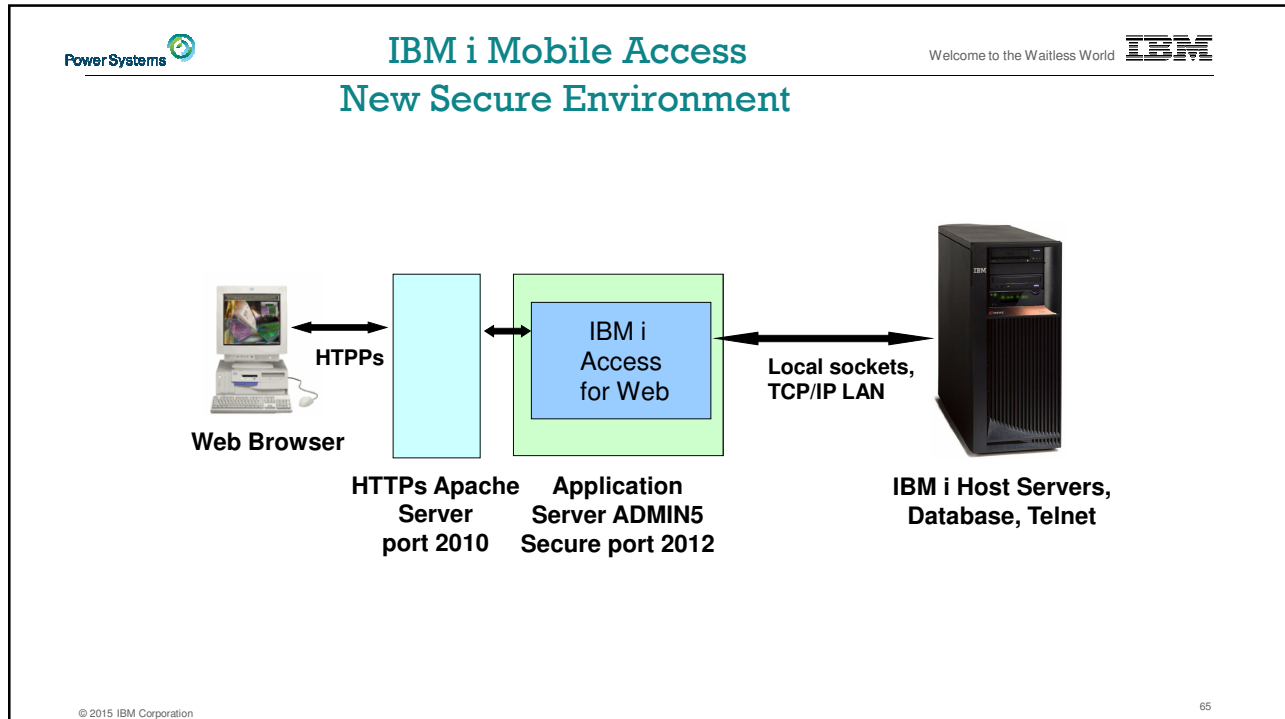
- Import/Export policy settings - export policies to a different system
  - Pick a user or group for export
- Transfer configuration data from one user to another on the same system
  - Move and copy operations supported for:
    - 5250 sessions and macros
    - Saved commands
    - Database requests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



# Environment Security



# IBM i Mobile Access Default Environment





PowerSystems  **Mobile Access Secure Deployment** Welcome to the Waitless World 

- The IBM i HTTP Admin Apache Server on port 2001 has been able to be secured with SSL on port 2010 for some time
  - IBM i DCF Knowledgebase Document:
    - <http://www.ibm.com/support/docview.wss?uid=nas8N1013544>
- The HTTP Admin5 Integrated Application Server job that IBM i Mobile Access is deployed to previously only ran on non-SSL port 2011.
- Recent HTTP Group PTF updates allow Admin5 to be secured with SSL on port 2012
  - r7.1 SF99368 Level 38
  - r7.2 SF99713 Level 13
  - r7.3 SF99722 Level 1

© 2015 IBM Corporation 66

PowerSystems **Mobile Access Secure Deployment** Welcome to the Waitless World **IBM**

RCHESP1 - IBM Navigator for i x HTTP Server Administration on... x +

rchesp1.rchland.ibm.com:2001/HTTPAdmin

IBM Web Administration for i

Setup **Manage** Advanced | Related Links

All Servers | HTTP Servers **Application Servers** Installations

Running Server: Admin5 - V8.5 (int app svr)

Admin5

### Manage Integrated Web Application Server - V8.5 (int app svr)

Server: Admin5

No description for server Admin5

The IBM integrated Web application server for i provides a secure and easy to configure environment for hosting servlet based Web applications while requiring minimal system resources such as memory. Easy to use interfaces for managing the server, installing and managing the applications, as well as managing other resources such as virtual hosts and database connections are provided.

For more information, please visit: <http://www.ibm.com/systems/i/software/ias/>

© 2015 IBM Corporation 67

PowerSystems **Mobile Access Secure Deployment** Welcome to the Waitless World **IBM**

RCHESP1 - IBM Navigator for i x HTTP Server Administration on... x +

rchesp1.rchland.ibm.com:2001/HTTPAdmin

IBM Web Administration for i

Setup **Manage** Advanced | Related Links

All Servers | HTTP Servers **Application Servers** Installations

Running Server: Admin5 - V8.5 (int app svr)

Admin5 > Configure SSL

### Configure SSL

Welcome - Step 1 of 9

Welcome to the Configure Secure Sockets Layer (SSL) wizard. This wizard assists you in configuring SSL for application server Admin5.

- Secure Sockets Layer (SSL)**  
SSL is an industry standard that provides secure communications. SSL is two protocols: a record protocol and a handshake protocol. The record protocol controls the flow of the data between two endpoints of an SSL session. The handshake protocol uses a digital certificate to authenticate one or both endpoints of the SSL session and to establish a unique symmetric key used to generate keys to encrypt and decrypt data for that SSL session.
- Digital certificate**  
A digital certificate is an electronic credential used to establish proof of identity in an electronic transaction. It is comprised of a public key and some identifying information that a trusted Certificate Authority (CA) has digitally signed. Each public key has an associated private key. The private key is not stored with or as part of the certificate. In this wizard, the server (the endpoint which is being authenticated) must prove that it has access to the private key associated with the public key contained within the digital certificate.
- Keystore**  
A keystore is a storage facility for cryptographic keys and certificates. Entries in a keystore can be a key entry or a trusted certificate entry. Key entries hold very sensitive cryptographic key information, which is stored in a protected format to prevent unauthorized access. Typically, a key stored in this type of entry is a secret key, or a private key accompanied by the certificate chain for the corresponding public key. Trusted certificate entries contain a single public key certificate belonging to another party. It is called a trusted certificate because the keystore owner trusts that the public key in the certificate indeed belongs to the identity identified by the subject (owner) of the certificate. The issuer of the certificate vouches for this, by signing the certificate.

Back **Next** Cancel

© 2015 IBM Corporation 68

PowerSystems **Mobile Access Secure Deployment** Welcome to the Waitless World **IBM**

© 2015 IBM Corporation 69

PowerSystems **Mobile Access Secure Deployment** Welcome to the Waitless World **IBM**

© 2015 IBM Corporation 70

PowerSystems **Mobile Access Secure Deployment** Welcome to the Waitless World **IBM**

Admin5 > Configure SSL

Specify keystore password - Step 4 of 9

Keystore is stored in a protected format to prevent unauthorized access. Specify the password to load and store the keystore. The password is also used to protect the key entry in the keystore. Keep this password in a safe place for future access to it.

Specify the password for the keystore

Password: ●●●●●●

Back Next Cancel

© 2015 IBM Corporation 71

PowerSystems **Mobile Access Secure Deployment** Welcome to the Waitless World **IBM**

Admin5 > Configure SSL

Specify Digital Certificate - Step 6 of 9

To configure SSL, your server must have a digital certificate. The server presents the certificate to prove its identity to the client or user that requests access to the resources the server controls. Specify a digital certificate for the server.

Specify digital certificate for server

Issue a new-self signed certificate

Select existing certificate from the keystore

Digital certificate: RCHESP1\_3\_8\_16

Note: Digital certificate marked with (\*) is expired.

Back Next Cancel

© 2015 IBM Corporation 72





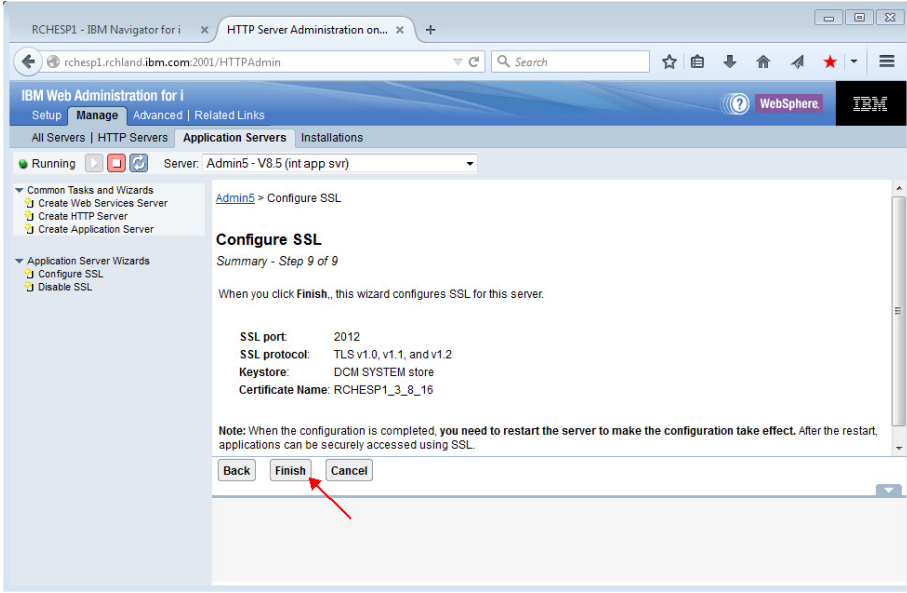
PowerSystems **Mobile Access Secure Deployment** Welcome to the Waitless World **IBM**

© 2015 IBM Corporation 73

PowerSystems **Mobile Access Secure Deployment** Welcome to the Waitless World **IBM**



© 2015 IBM Corporation 74

PowerSystems  **Mobile Access Secure Deployment** Welcome to the Waitless World 



IBM Web Administration for i  
Setup **Manage** Advanced | Related Links

All Servers | HTTP Servers | **Application Servers** | Installations

Running   Server: Admin5 - V8.5 (int app svr)

Admin5 > Configure SSL

**Configure SSL**  
Summary - Step 9 of 9



When you click **Finish**, this wizard configures SSL for this server.

SSL port: 2012  
SSL protocol: TLS v1.0, v1.1, and v1.2  
Keystore: DCM SYSTEM store  
Certificate Name: RCHESP1\_3\_8\_16

Note: When the configuration is completed, you need to restart the server to make the configuration take effect. After the restart, applications can be securely accessed using SSL.



Back **Finish** Cancel

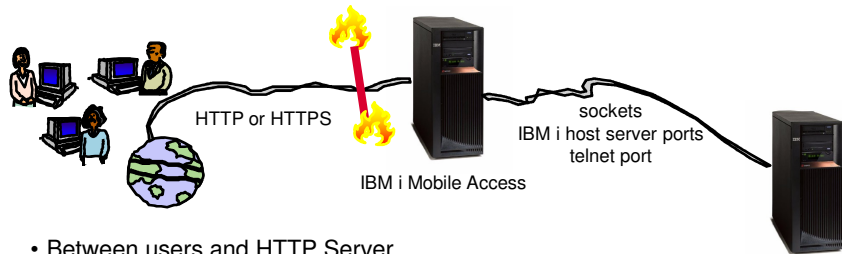
© 2015 IBM Corporation 75

PowerSystems  **Mobile Access Secure Deployment** Welcome to the Waitless World 

- The default IBM i Mobile Access URL:
  - <http://system:2001/iamobile>
- Redirects to:
  - <http://system:2011/iamobile/iWAHome>
- The secure IBM i Mobile Access URL is:
  - <https://system:2010/iamobile>
- Redirects to:
  - <https://system:2012/iamobile/iWAHome>

© 2015 IBM Corporation 76



PowerSystems  **IBM i Mobile Access Environment** Welcome to the Waitless World 



The diagram illustrates the IBM i Mobile Access Environment. On the left, three users are shown with laptops, connected to a globe representing the internet. A line labeled 'HTTP or HTTPS' connects them to a server labeled 'IBM i Mobile Access'. This server is depicted with a flame icon, suggesting security or encryption. A second line connects this server to another server labeled 'IBM i'. This connection is labeled 'sockets', 'IBM i host server ports', and 'telnet port'.

- 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

© 2015 IBM Corporation 77

PowerSystems  **5250 SSL Telnet** Welcome to the Waitless World 

- 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 DCF Knowledgebase Document N1020432 “IBM i Access for Web r7.2 5250 SSL Enablement”
  - <http://www-01.ibm.com/support/docview.wss?uid=nas8N1020432>

© 2015 IBM Corporation 78

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

## Questions?





Welcome to the Waitless World 

## 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 inquiries, 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

© 2015 IBM Corporation

81



Welcome to the Waitless World 

## 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.

SPECint, SPECintp, SPECintp, SPECweb, SPECjAppServer, SPEC OMP, SPECviewperf, SPECcapc, SPECchpc, SPECjvm, SPECmap, SPECimap and SPECcs 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.

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

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

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

Revised December 2, 2010

© 2015 IBM Corporation

82