

# **LAB: Administrator's First Steps to Customize System i Access for Web**

**Linda Hirsch** [lhirsch@us.ibm.com](mailto:lhirsch@us.ibm.com)

**<http://www.ibm.com/systems/i/software/access/web>**

© IBM Corporation 2007

## Table of Contents

Preface.....	3
Introduction.....	3
Lab objective.....	3
About this lab.....	4
Setting System i Access for Web policies .....	4
Lab exercises.....	6
Removing unwanted tabs from the navigation bar .....	6
5250.....	11
Print.....	16
Files.....	19
Integrating with e-mail.....	24
Checkpoint #1 .....	26
New group of users .....	27
Database.....	30
My Folder.....	35
Checkpoint #2 .....	38
Transfer customization/configuration settings to a new user .....	39
Summary .....	43
Reference information .....	44
Trademarks and Disclaimers.....	45

# Preface

## ***Introduction***

System i Access for Web enables users to connect to i5/OS and leverage business information, applications, and resources through point-and-click, easy-to-use interfaces. Users can upload workstation data to DB2 for i5/OS, query and download database information, work with their printer output, run business applications, and much more! Some reasons why System i Access for Web is ideal for desktop users:

- Can be used from any desktop that has a browser.
- Nothing to install, configure, or maintain at the workstation desktop.
- Since it uses industry-standard protocols (HTTP, HTTPS and HTML), it is an ideal solution for remote users who need Internet access through a firewall as well as internal users.
- A friendly interface that is tightly integrated with the desktop browser makes it easy to navigate through screens. Its simple-to-use GUI enables users unfamiliar with i5/OS to easily navigate their way to work with applications, find their printer output, run database requests, etc.

It provides a full range of capabilities similar to its native Windows counterpart, iSeries Access for Windows, so users can start 5250 sessions, have access to printers and printer output, the database, and the integrated file system. Users can access easy-to-use GUIs to run batch commands, send and receive messages, work with printer output without ever starting a 5250 session.

## ***Lab objective***

The objectives of this lab are to...

- Provide an example of how you can make System i Access for Web available to users of your system.
- Teach you how System i Access for Web can be managed and controlled through i5/OS group and user profile profiles.
- Teach you how to use System i Access for Web policies to control how users access i5/OS resources.
- Provide you with exercises, information, and hands on experience so that you can take this lab home and implement it within your environment.

## **About this lab**

This lab will show you how you might initially make System i Access for Web available to your users. The lab will walk through the steps you can perform as an administrator before turning System i Access for Web ‘loose’ in your network.

In this lab, we are initially going to let a set of remote users use a small portion of System i Access for Web. The lab instructors have setup the following user environment...

- WAXxADM/WAXxPWD    An i5/OS administrator user profile used to perform configuration
- SALESxx/WAXxPWD    An i5/OS group user profile
- SALESxxA/WAXxPWD    An i5/OS user profile that is a member of the SALESxx group profile
- SALESxxB/WAXxPWD    An i5/OS user profile that is a member of the SALESxx group profile
- SALESxxC/WAXxPWD    An i5/OS user profile that is a member of the SALESxx group profile

where “xx” is a number assigned to you by the lab instructor

You will use the WAXxADM user profile to configure and manage how the individual remote users use System i Access for Web. You will use WAXxADM to set policies for the SALESxx group profile. The advantage of setting policies on a group user profile is all members of the group inherit the same policies so the policies need only be set and managed for a single user.

In your home environment, you might create a similar environment where you would have an i5/OS group profile called SALES, and then add remote sales users to this group. System i Access for Web functions could then be managed for the remote sales users through the SALES group.

Before we begin the exercises, it may be helpful to explain how System i Access for Web enforces policies and how i5/OS user and group profiles get authorities.

## **Setting System i Access for Web policies**

The first area of System i Access for Web that you need to become familiar with is the Customize → Policies function. This function gives an administrator access to the policies that control what features of System i Access for Web users will be able to use.

In order to use the Policies function and work with i5/OS profiles, the administrator i5/OS user profile must have \*SECADM special authority. An administrator does have the option of delegating this capability to a non-\*SECADM user by setting a System i Access for Web policy.

To give another user the ability to access the Policies function, there are two requirements...

- The System i Access for Web ‘Grant administrator privileges’ policy must be set for the delegated user.

- The delegated user profile does not require the \*SECADM special authority, but it must have \*CHANGE object authority for the user and group profiles for which it will set policies.

In this lab, you will be using user profile WAXXADM which has \*SECADM special authority.

System i Access for Web enforces policy settings for a user in the following order:

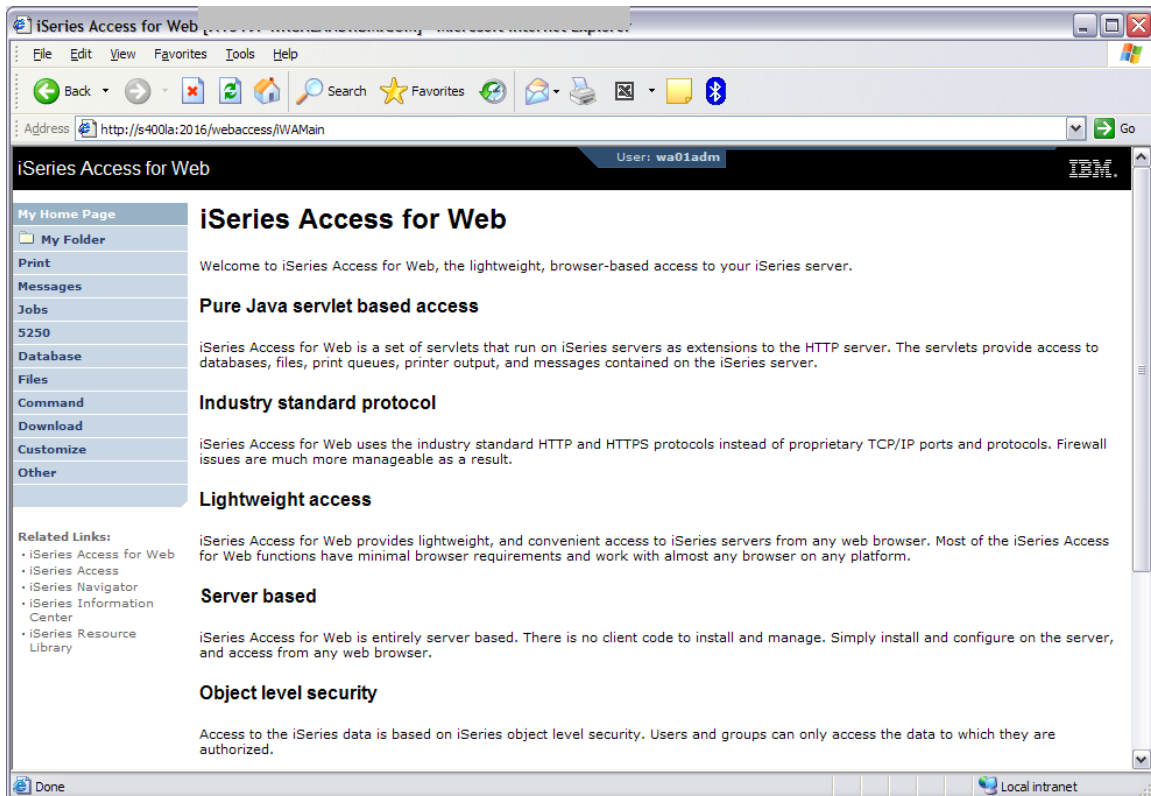
1. If a policy has been specifically set at the user profile level, it takes priority over all other settings.
2. If no policy has been set at the user profile level, then group profile memberships are checked. If the policy has been set for any of the user's group profiles, it is enforced.
3. If no policy has been set at the user or the group profile level, then a special group called \*PUBLIC is checked. All System i Access for Web users are automatically members of the \*PUBLIC group profile, and cannot be removed from this group.
4. If a policy setting has not been set, then the shipped default policy setting for the \*PUBLIC group profile is enforced.

Consequently, you may want to set as many policies at the \*PUBLIC level as possible, then you only need to do it once for all users. Then you can go to the i5/OS group user profile level to allow or remove certain items. Finally you can make changes at the user profile level for things that are unique to an individual user. This lab will cover examples of items that could be set at these various levels.

## Lab exercises

### ***Removing unwanted tabs from the navigation bar***

When System i Access for Web is initially deployed to the web environment, all functions are available to all users as shown in the screen shot below. The navigation bar on the left side of the window provides access to functions such as Print, Messages, Jobs, 5250, Database, etc.



The system/web administrator must disable (policy restrict) the functions that users should not be able to use.

In this lab we will initially have our SALESxx group access only three (3) of the many functions that are available. The users that are in the SALESxx group will have access to the following functions:

- 5250 – users need access to i5/OS applications, such as an RPG program for placing orders or updating existing orders, etc.
- Print – users will want to check their printer output (i5/OS SPOOLFILE) to determine the status of orders. They may want to view an invoice or email it to their customer.

- Files – there is common data stored in the integrated file system (IFS) on i5/OS that users need to access. We also want to give each individual user profile a private directory in the IFS where they can store their own information.

Follow these steps to remove all the tabs in the navigation bar that we do not want users to access:

1. Open a browser using the website address provide by the lab instructor.

It is recommended that you use the Microsoft Internet Explorer web browser. In later steps you will be opening another web browser using a different user ID.

Some browsers share user ID information between multiple sessions, thus you won't be prompted for a user ID/password. Microsoft Internet Explorer does not share this session information and will prompt you so that you can logon using a different user ID.

2. When prompted, login using the user name **WAXxADM** and password **WAXxPWD**...where "xx" is the number assigned to you by the lab instructor.

The WAXxADM user profile has \*SECADM special authority.

3. Note that in the top right corner of the web page **User: WAXxADM** is shown to be logged on and **System: <name of system provided by the lab instructors>** is the i5/OS system connected.
4. Click the **Customize** tab in the navigation bar on the left side of the web page.
5. Click the **Policies** link.
6. In the Profile field, type **SALESxx**...where "xx" is the numeric value assigned to you by the lab instructor.
7. Click the **Edit Policies** button.
8. The web page will be refreshed listing the categories of System i Access for Web functions. The remaining steps will walk you through editing policies for the functions that we are not going to allow users to access.
9. The 5250 category will be customized in a later step.
10. Click the action icon for the Command category.
11. The web page will be refreshed listing all the policies associated with the Command function.

You will notice that the policies are listed in a hierarchy. This means that setting a top level policy will affect all of those policies that are indented below it.

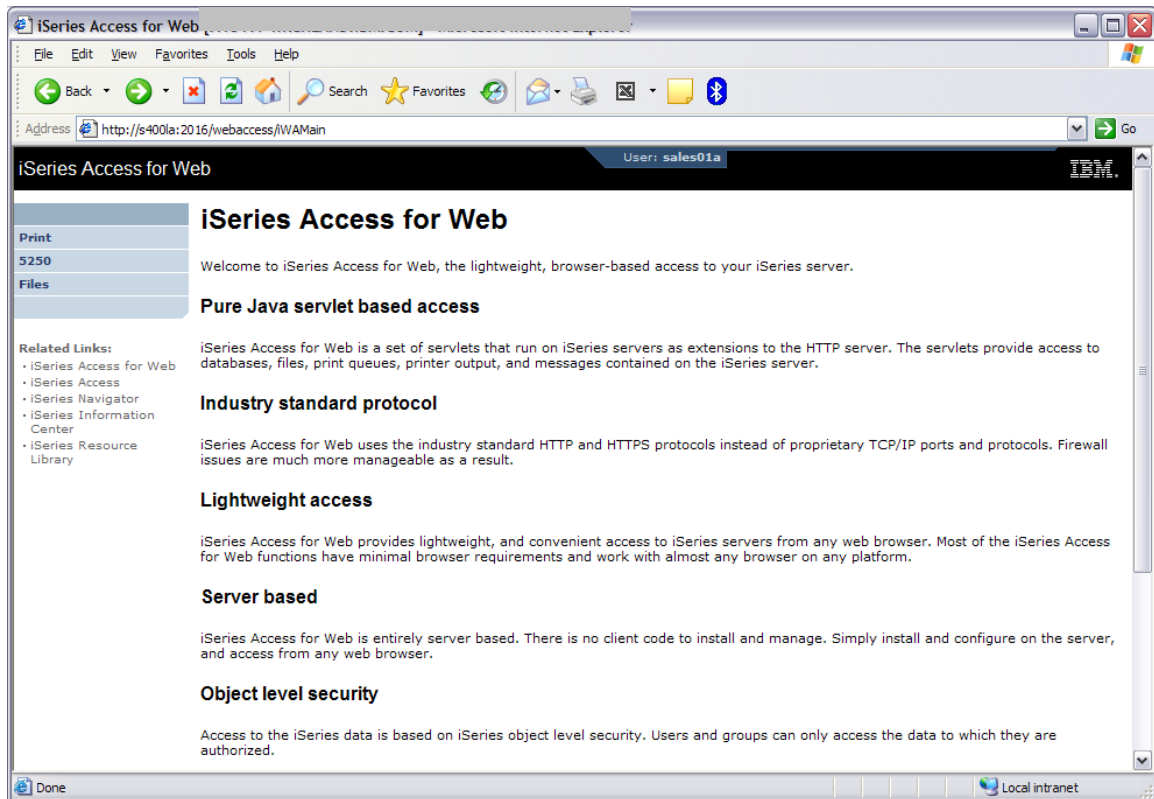
The top level policy is 'Command access'. The Setting defaults to Allow. Change the Setting to **Deny**.

Because this is the top level policy, setting it to Deny will also set all those policies below it in the hierarchy to Deny so only the top level policy needs to be set.

12. Click the **Save** button at the bottom of the web page.
13. Click the action icon for the Customize category.
14. The top level policy is 'Customize access'. Change the Setting to **Deny**.
15. Click the **Save** button at the bottom of the web page.
16. Click the action icon for the Database category.
17. The top level policy is 'Database access'. Change the Setting to **Deny**.
18. Click the **Save** button at the bottom of the web page.
19. Skip the Database connection category.
20. Click the action icon for the Download category.
21. The top level policy is 'Download access'. Change the Setting to **Deny**.
22. Click the **Save** button at the bottom of the web page.
23. Skip the Files category. This category will be modified in a later step.
24. Click the action icon for the General category.
25. Locate the 'Home page' policy. Change the Setting to **Deny**.
26. Click the **Save** button at the bottom of the web page.
27. Click the action icon for the Jobs category.
28. The top level policy is 'Jobs access'. Change the Setting to **Deny**.
29. Click the **Save** button at the bottom of the web page.
30. Skip the Mail category. This category will be modified in a later step.
31. Click the action icon for the Messages category.
32. The top level policy is 'Messages access'. Change the Setting to **Deny**.
33. Click the **Save** button at the bottom of the web page.
34. Click the action icon for the My Folder category.
35. The top level policy is 'My Folder access'. Change the Setting to **Deny**.
36. Click the **Save** button at the bottom of the web page.



37. Skip the Print category. This category will be modified in a later step.
38. Click the action icon for the Sametime category.
39. The top level policy is 'Sametime access'. Change the Setting to **Deny**.
40. Click the **Save** button at the bottom of the web page.
  
41. Click the action icon for the Other category.
42. The top level policy is 'Other access'. Change the Setting to **Deny**.
43. Click the **Save** button at the bottom of the web page.
  
44. Now let's see the result of setting these policies to restrict access to System i Access for Web functions.  
  
Open a new browser using the website address provided by the lab instructor.
45. When prompted, login using the user name **SALESxxA** and password **WAxxPWD**...where "xx" is the number assigned to you by the lab instructor.
46. Note that in the top right corner of the web page **User: SALESxxA** is shown to be logged on and **System: <name of system provided by the lab instructors>** is the i5/OS system connected.
47. In the previous steps, you set policies for the user group profile SALESxx. You just logged in as user SALESxxA who is a member of the SALESxx group profile.  
  
All user profiles that are members of the SALESxx group will use the policies that were set. The SALESxxA web page will look similar to this



Only the functions we want this group of users to have access to are available.

48. Click each of the tabs in the navigation area on the left side of the web page to see what functions are available. You will see that each have many capabilities. The lab exercise that follow will show you how to customize each of these functions.

## 5250

In the browser session where you are signed on as SALESxxA, you will see that there are three links under the 5250 tab:

- Active Sessions  
The Active sessions list displays the active 5250 sessions for the current user. This is an easy way for an end user to see what sessions are open, quickly reconnect to those sessions, or end them.
- Configured sessions  
The Configured sessions link enables users to connect to i5/OS systems using previously configured sessions. As an administrator, you can configure sessions for users so that you control the i5/OS systems your users are connecting. You can also...
  - set up Bypass signon so the user does not have to reenter a user ID and password on the i5/OS sign on screen
  - identify what their screen view will be (web view or traditional green on black screen view)
  - specify a macro to play immediately after the session is started (perhaps to start a specific application and put them on first screen of the application)
  - set the option to enable advanced JavaScript functions so the user can use page up, page down, and function keys
  - enable HTML data defined using the DDS HTML keyword to be displayed
- Start session  
The Start session link allows an end user to start their own session connections to any i5/OS system in the network and identify any of the options listed above for Configured Sessions.

In this exercise, we will remove the Start Session link, and only allow users to start 5250 sessions that were previously configured for them. We will also set additional restrictions in the 5250 category.

1. Switch to the browser window where WAXXADM is logged in.
2. First we are going to configure two 5250 sessions for use by the users in the SALESxx group.

Click the **5250** tab in the navigation bar on the left side of the web page.

- Click **Configured sessions**.

- Click **Configure new session**.
- In the Session field, type **East Coast i5/OS system**.
- Check the box for **Bypass signon**.
- In the Server field, type the name for Server #1 using the information provided by the lab instructor.

The other session settings allow you to further customize how the 5250 session will be presented to the users of the SALESxx group.

- Scroll down to the bottom of the web page and click the **Save** button.
- Create another session. Click **Configure new session**.
- In the Session field, type **West Coast i5/OS system**.
- Check the box for **Bypass signon**.
- In the Server field, type the name for Server #2 using the information provided by the lab instructor.
- Scroll down to the bottom of the web page and click the **Save** button.
- Now that the sessions have been created and are owned by the WAXXADM user, the sessions can be made available to end users.

In the list of Configured sessions, click the Action column icon to **Create shortcut** for the **East Coast i5/OS system** session.

- Remove “Shortcut to” in the Shortcut name field.
- In the Access field, type **SALESxx** where “xx” is the number assigned to you by the lab instructor.
- Click the **Create Shortcut** button.
- In the list of Configured sessions, click the Action column icon to **Create shortcut** for the **West Coast i5/OS system** session.
- Remove “Shortcut to” in the Shortcut name field.
- In the Access field, type **SALESxx** where “xx” is the number assigned to you by the lab instructor.

- Click the **Create Shortcut** button.

Creating these shortcuts for the SALESxx group gives all members of the SALESxx group access to the shortcuts.

3. Click the **Customize** tab in the navigation bar on the left side of the web page.
4. Click the **Policies** link.
5. In the Profile field, type **SALESxx...** where “xx” is the numeric value assigned to you by the lab instructor.
6. Click the **Edit Policies** button.
7. The web page will be refreshed listing the categories of System i Access for Web functions.
8. Click the action icon for the 5250 category.
9. To remove the Start session link from the 5250 tab, set the ‘Start non-configured sessions’ policy (3<sup>rd</sup> policy from the top) to **Deny**.
10. Set the ‘Configured session to user for defaults’ policy (10<sup>th</sup> policy from the top) to **East Coast i5/OS system...**

This will default a 5250 session to this configured session.

11. To prevent end users from changing their active session settings (i.e. screen view, colors, etc), set the ‘Edit active session settings’ policy (15<sup>th</sup> policy from the top) to **Deny**.
12. About half way down the list of policies is a subgroup called ‘Configured sessions’ containing several sub-policies. This subgroup policy will be left set to the default value of “Allow”, but the following sub-policies will be set to **Deny**.
  - Create configured session
  - Copy configured session
  - Delete configured session
  - Rename configured session
  - Edit configured session
  - Create configured session shortcut
  - Copy configured session shortcut
  - Delete configured session shortcut
  - Rename configured session shortcut

This group of policy settings will allow the users in the SALESxx group to use the 5250 sessions configured by WAXxADM but will not allow them to create their own sessions or modify those given to them.

13. At the bottom of the list of policies is a subgroup called 'My macros' containing several sub-policies. The subgroup policy will be left set to the default value of "Allow", but the following sub-policies will be set to Deny.

- Record macro
- Copy macro
- Delete macro
- Rename macro
- Edit macro
- Create macro shortcut
- Copy macro shortcut
- Delete macro shortcut
- Rename macro shortcut

This group of policy settings will allow the users in the SALESxx group to use any macros configured by WAXxADM but will not allow them to create their own macros or modify those given to them.

14. Click the **Save** button at the bottom of the web page.
15. To see the changes that were made above, switch to the browser window where SALESxxA is logged in.
16. Click the **5250** tab.

The Start session link was removed.

17. Click the **Configured sessions** link.

The list of configured sessions available to user SALESxxA are those that WAXxADM is providing to the SALESxx group profile.

The only action allowed on the two configured sessions is to Start them.

Configured Session

File Edit View Favorites Tools Help

Address http://s-400la:2016/webaccess/iWAConfiguredSessions User: sales01a

## iSeries Access for Web

### Configured Sessions

Session	Server	Action	Shortcut	Created By	Access
East Coast i5/OS system	S400LA		Yes	wa01adm	SALES01
West Coast i5/OS system	S400LA2		Yes	wa01adm	SALES01

**Print**

**S250**

- Active sessions
- Configured sessions

**Files**

**Related Links:**

- [iSeries Access for Web](#)
- [iSeries Access](#)
- [iSeries Navigator](#)
- [iSeries Information Center](#)
- [iSeries Resource Library](#)

[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.

[My macros](#)  
Work with your macros.

[My keypads](#)  
Work with your keypads.

[S250 user interface help](#)  
View help for working with configured sessions.

IBM | iSeries | Service 5.4.0.05-191.S125551

Done Local intranet

## **Print**

The print function offers many different capabilities for working with printer output, printers, and printer shares. In the browser session where you are signed on as SALESxxA, you can see them under the Print tab.

In this exercise, we will give the users in the SALESxx group access only to the Printer output capability. This will enable them to connect to the i5/OS system and work with their print output.

1. Switch to the browser window where WAXxADM is logged in.
2. Click the **Customize** tab in the navigation bar on the left side of the web page.
3. Click the **Policies** link.
4. In the Profile field, type **SALESxx...** where “xx” is the numeric value assigned to you by the lab instructor.
5. Click the **Edit Policies** button.
6. The web page will be refreshed listing the categories of System i Access for Web functions.
7. Click the action icon for the Print category.
8. Near the top of the list of policies is a subgroup called ‘Printer output’ containing several sub-policies. The subgroup policy will be left at “Allow”, but the sub-policies need to be reviewed, and changed to **Deny** if you do not want users to have the capability each policy represents. Below is some information to help you determine what should be set to Deny. For this lab we recommend leaving the Printer output sub-policies set to Allow. As you roll out System i Access for Web in your business, you should review what functions you want to allow your users to access.
  - System i Access for Web has a built-in PDF conversion program that converts the SCS or AFP printer output to a PDF document. This enables the printer output to be viewed in the browser and then printed on any printer the user can access, or it can be attached to an email. This is a very useful function that you’ll likely want your user to have.
  - The ‘Work with’ actions for printer output allow the user to hold, release or print the specified spooled file next. There are also links available that enable users to Move printer output to another printer, Move printer output to another output queue, Send printer output to another server (SNDTCPSPLF), Change



printer output attributes (CHGSPLFA), and Copy printer output to database file (CPYSPLF).

- One policy you definitely should modify is the 'Printer output list columns'. When you view printer output there are 15 different columns of information shown about each print job, and to see all this information you must move the slide bar over in the browser. You should reduce these columns to the ones that are pertinent to your users, and that fit on the screen. You can also modify the order in which these columns are displayed.
9. There are several other subgroup policies at the same level as 'Printer output'. These policies should be set to **Deny** so that they do not appear on the Print tab. The names of these policy subgroups are
- PDF printer output
  - Printers
  - PDF printers
  - Internet printers
  - Internet printer shares
  - Printer shares
  - Output queues
10. Click the **Save** button at the bottom of the web page.
11. To see the changes that were made above, switch to the browser window where SALESxxA is logged in.
12. Click the **Print** tab.
- Only Printer output is now available.
13. Click the **Printer output** link. Spooled files should be listed similar to the screen below.

Printer Output |

File Edit View Favorites Tools Help

Address http://s400la:2016/webaccess/IWASpool User: SALES01A

iSeries Access for Web IBM

## Printer Output for SALES01A

Print

- Printer output
- 5250
- Files

Related Links:

- iSeries Access for Web
- iSeries Access
- iSeries Navigator
- iSeries Information Center
- iSeries Resource Library

File Name	User Data	Creation Date/Time	Pages Per Copy	Copies	Status	Action	User	Job Name	Job Number	File Number	Output Queue
QPNPSPRTF	Demo readm	4/6/07 11:48 AM	1	1	Ready	[...]	SALES01A	QPRJOB	446125	7	WEBLIB/WEBQU
QPDSPAJB		4/6/07 11:48 AM	12	1	Ready	[...]	SALES01A	QPRJOB	446125	8	QGPL/QPRINT

Action Details

The Printer Output function supports the following actions:

- Work With**  
 Use the Work With action to hold, release or print the specified spooled file next. There are also links available that will allow you to perform the following actions on the spooled file:
  - Move printer output to another printer
  - Move printer output to another output queue
  - Send printer output to another server (SNDTCPSPLF)
  - Change printer output attributes (CHGSPPLFA)
  - Copy printer output to database file (CPYSPLF)

Local intranet

## **Files**

The Files function lets users access the i5/OS integrated file system (IFS) as a file server. Workstation files and documents can be...

- viewed
- uploaded and downloaded
- emailed directly from the IFS
- accessed using a variety of other functions such as use of the built-in zip and unzip capability of System i Access for Web.

The Files function is a very convenient way for users to work with workstation information as the users do not need to know the directory path to work with their documents. And because the files are stored on the i5/OS system, normal i5/OS system backup procedures are saving user data.

In the browser session where you are signed on as SALESxxA, you will see that there are three links under the Files tab:

- Browse files  
The Browse file link allows the user to browse, navigate, and access directories/files in the i5/OS integrated file system (IFS).
- Browse file share  
The Browse file share link allows the user to browse, navigate, and access a specific i5/OS NetServer file share.
- File shares  
The File shares link lists the i5/OS NetServer file shares available to the user.

In this exercise, we want to setup Files access where selecting the Browse files link will take the user directly to their own private directory. The private directory will contain the users private/personal files and a link to a shared directory.

This exercise will have you...

- Remove the file share links from the Files tab for all users in the SALESxx group.
- Set each user in the SALESxx group to use their own unique/private directory in the IFS.
- Provide each individual user with access to a shared directory so that all users of the SALESxx group can access/share common data.

### Remove the file shares links from the Files tab

1. Switch to the browser window where WAXxADM is logged in.

2. Click the **Customize** tab in the navigation bar on the left side of the web page.
3. Click the **Policies** link.
4. In the Profile field, type **SALESxx...** where “xx” is the numeric value assigned to you by the lab instructor.
5. Click the **Edit Policies** button.
6. The web page will be refreshed listing the categories of System i Access for Web functions.
7. Click the action icon for the Files category.
8. In the middle of the list of policies is a subgroup called ‘Browse file share’ containing many sub-policies. Set this subgroup policy to **Deny**.
9. Near the bottom of the list of policies, you should see a sub-policy named ‘File shares list’. This policy controls whether the File shares function is available in the Files tab. This policy is under the hierarchy of the ‘Browse file share’ subgroup so we don’t need to specifically set it to Deny.
10. Click the **Save** button at the bottom of the web page.
11. To see the changes that were made above, switch to the browser window where SALESxxA is logged in.
12. Click the **Files** tab.

Only the Browse files link is available.

Set each user in the SALESxx group to use their own unique/private directory

The default view for the Browse Files link is to show every directory in the IFS “root” (/) directory. We want each member in our SALESxx group to see only two directories in the IFS...

- A unique directory for each user where they can store their private information.
- A common directory for the SALESxx group where information is stored for use by all of the members of the group.

Typically when an i5/OS system administrator creates a user profile, a user home directory would also be created. Creating individual home directories for each user under the /home directory is preferable. The ‘/home’ directory is a subdirectory under

the “root” (/) directory. The i5/OS system default expects the name of the home directory of a user to be the same name as the user profile. For this lab, the lab instructors have already created the following IFS directories for you and copied sample data to the directories...

- /home/SALESxxA
- /home/SALESxxB
- /home/SALESxxC

On your i5/OS system in your business, you can create directories in the IFS using the i5/OS command MKDIR command. You can use this command to create directories for your users. An example of using the command is...

```
MKDIR DIR('/home/SALESxxA') DTAAUT(*EXCLUDE) OBJAUT(*NONE)
or use iSeries Navigator.
```

The steps below will have you modify the policies that set the default directory to access when the Browse files link is selected.

1. Switch to the browser window where WAXXADM is logged in.
2. Click the **Customize** tab in the navigation bar on the left side of the web page.
3. Click the **Policies** link.
4. In the Profile field, type **SALESxxA**...where “xx” is the numeric value assigned to you by the lab instructor.

All previous access to policies had you access the group user profile policies. Now you are accessing policies for a specific member of the group profile. We want to set user level policies for this specific user, not group level policies.

5. Click the **Edit Policies** button.
6. The web page will be refreshed listing the categories of System i Access for Web functions.
7. Click the action icon for the Files category.

If you scroll down the list of displayed policies, you will see the effect of setting the ‘Browse file share’ policy at the group profile level in the earlier steps. For example, the ‘Browse file share’ policy shows that it’s setting has been derived from the Group – SALESxx level and is set to Deny.

8. Near the top of the list of policies is a subgroup called ‘Browse files’ (6<sup>th</sup> policy).

Locate the policy 'Default directory' in the subgroup (3<sup>rd</sup> policy in the subgroup).

9. Type **/home/SALESxxA** in the Setting field where "xx" is the number assigned to you by the lab instructor.
10. We will leave SALESxxA user with full authority to copy, delete, zip/unzip, etc., information in this single directory.

Click the **Save** button at the bottom of the web page.

11. To see the changes that were made above, switch to the browser window where SALESxxA is logged in.
12. Click the **Files** tab.
13. Click **Browse files**.

The web page will be refreshed listing at the top 'Directory Contents /home/SALESXXA'

14. You would then repeat the above steps for each user in the SALESxx group so that each user's default Browse files access is in the /home/SALESxxX directory. For this lab it is not necessary to repeat the steps for other members of the SALESxx group.

#### Provide access to shared directory

All members of the SALESxx group likely have a need to access and share common information. The steps below will have you add to the /home/SALESxxA user's directory a symbolic link to a directory containing common information.

This symbolic link will appear as a directory named SALESINFO within the path /home/SALESxxA. From this link, each member of the SALESxx group can access and share the files in SALESINFO.

1. Switch to the browser window where WAXxADM is logged in.
2. Click the **Command** tab in the navigation bar on the left side of the web page.
3. Click the **Run command** link.
4. In the Command field, type the following command where "xx" is the number assigned to you by the lab instructor

**ADDLNK OBJ('/SALESINFO') NEWLNK('/home/SALESxxA/SALESINFO')**

5. Click the **Run Command** button.
6. To see the changes that were made above, switch to the browser window where SALESxxA is logged in.
7. Click the **Files** tab.
8. Click **Browse files**.

The web page will be refreshed showing the SALESINFO directory in the list.

9. You would then repeat the above steps for each user in the SALESxx group so that each user has access to the SALESINFO directory. When the command is run once, you can click the Retrieve action icon to get the command back into your prompt. Then simply change the user directory name and run again.

Now when a member of the SALESxx group uses the Files → Browse Files option they will be placed in their home directory and also have access to the SALESINFO directory.

The screenshot shows a web browser window titled "Browse Files /home/SALES01A". The address bar shows the URL: http://s4001a:2016/webaccess/WAFileList?filePath=%2Fhome%2FSALES01A. The page content includes a sidebar with "Print 5250" and "Files" (Browse files). The main area is titled "Directory Contents /home/SALES01A" and shows a summary: "Found 1 directories. Found 6 files with a total size of 102,700 bytes." Below this is a table of files and directories.

Name	Size (bytes)	Type	Modified	Action
SALESINFO		Directory	4/5/07 11:50:43 AM	[Icons]
My 2004 Sales.jpeg	18915	File	4/5/07 11:35:01 AM	[Icons]
My 2005 Sales.xls	13824	File	4/5/07 11:35:01 AM	[Icons]
My 2005 Sales.jpeg	19927	File	4/5/07 11:35:01 AM	[Icons]
My 2005 Sales.xls	14848	File	4/5/07 11:35:01 AM	[Icons]
My 2006 Sales.jpeg	20338	File	4/5/07 11:35:01 AM	[Icons]
My 2006 Sales.xls	14848	File	4/5/07 11:35:01 AM	[Icons]

Below the table is a section titled "Copy Files to Server" with the text: "Specify the file to copy to directory /home/SALES01A on X1519P4.RCHLAND.IBM.COM. Data is copied in binary format." There is a "File:" input field, a "Browse..." button, and a checkbox for "Replace file".

## ***Integrating with e-mail***

System i Access for Web can integrate with an end user's e-mail. You can use the e-mail integration from several places within System i Access for Web, including Database, Print, Files, and Commands. You can also send e-mail notifications when items are saved to a user's personal folder or when a user's personal folder has reached a size threshold.

To use the e-mail integration, an e-mail address and an SMTP mail server (mail server that receives and routes e-mail) must be specified within System i Access for Web policy settings. The lab instructor has already preconfigured the e-mail address/SMTP mail server policy settings for the SALESxx/SALESxxA group/user profiles for the lab environment.

For this lab, the SMTP mail server policy was set for the group profile SALESxx. By setting the SMTP mail server for the group, all members of the group will inherit the setting. The e-mail address policy has been set on each individual user (SALESxxA, SALESxxB, SALESxxC) because it is specific to a user profile.

Use the steps below to see what policies have been set so that you can perform a similar configuration in your environment at home.

1. Switch to the browser window where WAXxADM is logged in.
2. Click the **Customize** tab in the navigation bar on the left side of the web page.
3. Click the **Policies** link.
4. In the Profile field, type **SALESxx...** where "xx" is the numeric value assigned to you by the lab instructor.
5. Click the **Edit Policies** button.
6. The web page will be refreshed listing the categories of System i Access for Web functions.
7. Click the action icon for the Mail category.

The 'Send mail' policy is set to **Allow**. This policy controls access to the Mail as Attachment function. When set to Allow, users are allowed to send items such as PDF output, SQL results, and integrated file system files as e-mail attachments. The Mail as Attachment option is not available until an SMTP mail server name and e-mail address are configured for the user.

The 'SMTP mail server' policy is currently set to the name of the i5/OS system being used for this lab. A typical environment would have this server name configured at



the \*PUBLIC group setting level. For this lab, we have set it at the SALESxx group profile level.

For the lab environment, we are using the SMTP mail server on our i5/OS lab system. This policy can be set to any SMTP mail server in your network; it does not have to be an SMTP mail server on your i5/OS system.

8. Click the **Cancel** button.
9. Click the **Policies** link under the Customize tab.
10. In the Profile field, type **SALESxxA** ... where “xx” is the numeric value assigned to you by the lab instructor.
11. Click the **Edit Policies** button.
12. The web page will be refreshed listing the categories of System i Access for Web functions.
13. Click the action icon for the Mail category.

The ‘Send mail’ policy is derived (inherited) from the SALESxx group profile and is set to **Allow**.

The ‘SMTP mail server’ policy is derived (inherited) from the SALESxx group profile and is set to the name of the i5/OS system being used for this lab.

For this lab, the lab instructors have set the ‘E-mail address’ policy to **SALESxxA@TECCONF1** (or the name of our i5/OS lab system). This policy specifies the e-mail address to use in the From field on the e-mail attachment settings page when using the mail as attachment function. The mail as attachment function is not available until this e-mail address and the SMTP mail server policies have been set. This can be any valid e-mail address, it does not have to be an i5/OS email address.

14. Click the **Cancel** button.

As mentioned earlier, you can set similar policy settings in your environment to enable the System i Access for Web e-mail integration.

## **Checkpoint #1**

System i Access for Web is ready for use by the SALESxx group.

The features of System i Access for Web have been pared down to only those needed by the SALESxx group. The members of the SALESxx group can...

- Connect 5250 sessions using session configurations given to them by the system administrator.
- View printer output.
- Access files in a private directory in the integrated file system, and share files with others members of the SALESxx group from a common directory.

The remaining exercises will build upon the configuration settings performed so far. The following exercises are going to have you...

- Setup access for a new group of users...Help desk users. This new group of users will start with the same access to i5/OS resources as the SALESxx group.

We will copy the policies that were set for the SALESxx group to the HELPxx group. Shortcuts to the 5250 sessions owned by WAXXADM will also be setup for the members of the HELPxx group.

- Give members of the HELPxx group access to the Database function of System i Access for Web. The members will be able to run database requests given to them by WAXXADM.
- Give members of the HELPxx group access to the My Folder function. The members will be able to store results from using System i Access for Web functions to their personal folder.

## ***New group of users***

In this exercise, we are going to work with another i5/OS group profile. This new group profile contains members of the Help Desk organization. We would like to give the Help Desk users the same capabilities we gave the SALESxx group, and then add a couple of additional features.

To do this we could...

- Walk through the steps for the earlier exercises but perform them for the Help Desk users. That would be a lot of work and errors could be made during the manual steps.
- Just add the individual Help Desk user profiles to the SALESxx group. This would work but it would not allow us to add additional features because adding additional features would also add those features to the SALESxxX users.
- We could use the Copy function of Customization to copy the policy settings from the SALESxx group to our Help Desk group. This is the easiest way to get the Help Desk user configuration started and the one we will use in the steps below.

The lab instructors have setup the following user environment...

- HELPxX/WAxXPWD      An i5/OS group user profile
- HELPxXA/WAxXPWD    An i5/OS user profile that is a member of the HELPxX group profile

where “xx” is a number assigned to you by the lab instructor

Use the steps below to copy the policies set for the SALESxx group to the HELPxX group, and give the members of the HELPxX group access to the 5250 sessions owned by WAxXADM.

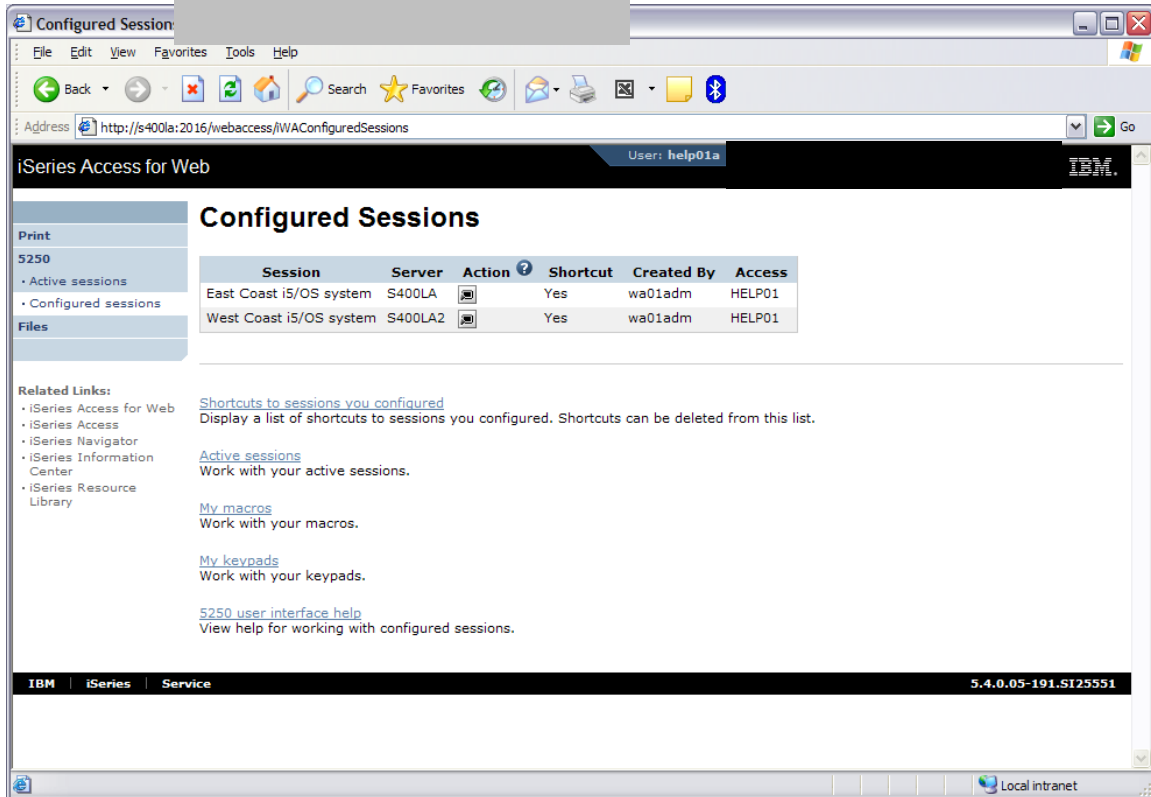
1. Switch to the browser window where WAxXADM is logged in.
2. Click the **Customize** tab in the navigation bar on the left side of the web page.
3. Click the **Policies** link.
4. In the Profile field, type **SALESxx** ...where “xx” is the numeric value assigned to you by the lab instructor.
5. Click the **Edit Policies** button.
6. The web page will be refreshed listing the categories of System i Access for Web functions. Below the list of categories are several links that help you manage the

policies for this user.

- View all policies
- View group members
- Copy policies
- Reset policies
- Policies help

7. Click the **Copy policies** link.
8. In the To profiles field, type **HELPxx** ...where “xx” is the numeric value assigned to you by the lab instructor.
9. Check the box for **Overwrite existing policies**.
10. Click the **Copy Policies** button. Policies have now been set for the HELPxx group. All members of the HELPxx group will use these policies when they login to System i Access for Web.
11. Click the **5250** tab in the navigation bar on the left side of the web page. WAXxADM owns the listed 5250 sessions. An earlier exercise had you create shortcuts to these 5250 sessions for the members of the SALESxx group. We need to create shortcuts to these 5250 sessions for the members of the HELPxx group.
12. Click the **Configured sessions** link.
13. In the list of Configured sessions, click the Action column icon to **Create shortcut** for the **East Coast i5/OS system** session.
14. Remove “Shortcut to” in the Shortcut name field.
15. In the Access field, type **HELPxx** where “xx” is the number assigned to you by the lab instructor.
16. Click the **Create Shortcut** button.
17. In the list of Configured sessions, click the Action column icon to **Create shortcut** for the **West Coast i5/OS system** session.
18. Remove “Shortcut to” in the Shortcut name field.
19. In the Access field, type **HELPxx** where “xx” is the number assigned to you by the lab instructor.
20. Click the **Create Shortcut** button.

21. To see the changes that were made, open a new browser window and login as user **HELPxxA** ...where “xx” is the numeric value assigned to you by the lab instructor.
22. Click the **5250** tab.
23. Click the **Configured sessions** link.
24. The webpage should look similar to the screen shown below.



It should be noted that we only copied polices from the SALESxx group to the HELPxx group. Earlier exercises had you set Files policies specifically for the SALESxxA user (Browse files access to the /home/SALESxxA directory). Those policies were not copied. To limit the HELPxxA users' Browse files access, you could copy policies from user SALESxxA to user HELPxxA...but you would still need to modify HELPxxA's individual user level policy settings for Files and Mail.

The effect of not setting the Browse files policy is that when HELPxxA clicks the Browse files link, they will be given access to the root directory of the integrated file system.

## **Database**

In this exercise, we are going to give the HELPxx group access to the DB2 for i5/OS database.

The System i Access for Web Database function provides an enormous amount of capability, for example:

- The *Tables* function enables users to view a list of database tables on the i5/OS system and perform actions on those tables without having knowledge of SQL and its syntax.
- The *My requests* function enables users to view, list, and run saved requests.
- The *Run SQL* function enables users to run SQL statements dynamically and save those statements to requests for repeated use.
- The *Copy data to table* function enables users to copy data files from your workstation to a database on the i5/OS system.
- The *Import request* function enables users to import Client Access Data Transfer upload/download requests into System i Access for Web.
- The *Import query* function enables users to import queries generated by Query for i5/OS and DB2 UDB for System i Query Manager.
- The *Extract server data* function enables users to extract object information (such as directory entries, messages, software fixes, software products, user profiles, etc.) into a database table.

We do not want members of the HELPxx group to be able to access all of the capabilities listed above. The HELPxx group is going to be limited to only being able to run database requests that the administrator creates and gives to them.

The steps below will first create a sample database request. Then Database policies will be set so that members of the HELPxx group can only access these database requests from the Database tab.

### Create a sample database request

The steps below will walk through creating a database request. Once created and owned by WAXxADM, a shortcut to it is created for use by members of the group profile HELPxx.

1. Switch to the browser window where WAXxADM is logged in.

2. Click the **Database** tab in the navigation bar on the left side of the web page.
3. Click the **Run SQL** link.
4. In the SQL Statement field, type the statement listed below. This statement will select all records from a database table named QCUSTCDT in library QIWS.

**SELECT \* FROM QIWS.QCUSTCDT**

5. In the SQL Output → Type dropdown box, select  
**Portable Document Format (.pdf)**
6. Click the **Save Request** button.
7. In the Request name field, type **Data for HELPxx users – PDF format**
8. Click the **Save Request** button.
9. Click the **My requests** link to see the list of saved requests.

When the request is run, the database will be queried, the results written to a PDF document, and the PDF document is displayed in the browser window.

Click the **Run** action icon to see the data.

When done, click the **Back** button of the browser to return to the System i Access for Web page.

10. Now we want to give the members of the HELPxx group access to this database request.

Click the **Create shortcut** action icon for the ‘Data for HELPxx users – PDF format’ request.

11. Remove “Shortcut to” in the Shortcut name field.
12. In the Access field, type **HELPxx** where “xx” is the number assigned to you by the lab instructor.
13. Click the **Create Shortcut** button.

The database requests are now available to the members of the HELPxx group, but now we need to give the members access to the Database functions.

### Set policies for accessing the Database function

The steps below will walk through setting the policies to allow and limit database access for members of the HELPxx group. All the links on the Database tab will be removed except for 'My requests'. The action allowed on listed database requests will be limited to the 'Run' action.

1. Switch to the browser window where WAXxADM is logged in.
2. Click the **Customize** tab in the navigation bar on the left side of the web page.
3. Click the **Policies** link.
4. In the Profile field, type **HELPxx** ...where "xx" is the numeric value assigned to you by the lab instructor.
5. Click the **Edit Policies** button.
6. The web page will be refreshed listing the categories of System i Access for Web functions.
7. Click the action icon for the Database category.

You will see that all of the database policies have been set to Deny. These policies were copied from the SALESxx group where Database was not made available to members of the SALESxx group.

8. The top level policy is 'Database access'. Change the Setting to **Allow**.
9. Click the **Apply** button at the bottom of the web page. This will reset all of the database policies to Allow for the HELPxx group.
10. Locate the subgroup policy called 'Tables'. Change the Setting to **Deny** so that the *Tables* link will be removed from the Database tab.
11. Locate the subgroup called 'Requests'. This subgroup policy will be left set to Allow so that the Database tab has the My requests link. The following list of sub-policies under 'Requests' will be set to **Deny**.
  - Copy request
  - Delete request
  - Rename request
  - Edit request
  - Save request
  - Create request shortcut
  - Copy request shortcut
  - Delete request shortcut



- Rename request shortcut
12. Locate the subgroup policy called ‘Run SQL requests’. Change the Setting to **Deny** so that the *Run SQL* link will be removed from the Database tab.
  13. Locate the subgroup policy called ‘Copy data to table’. Change the Setting to **Deny** so that the *Copy data to table* link will be removed from the Database tab.
  14. Locate the subgroup policy called ‘Import request’. Change the Setting to **Deny** so that the *Import request* link will be removed from the Database tab.
  15. Locate the subgroup policy called ‘Import query’. Change the Setting to **Deny** so that the *Import query* link will be removed from the Database tab.
  16. Locate the subgroup policy called ‘Extract server object data’. Change the Setting to **Deny** so that the *Extract server data* link will be removed from the Database tab.
  17. Click the **Save** button at the bottom of the web page.
  18. To see the changes that were made, switch to the browser window where HELPxxA is logged in ...where “xx” is the numeric value assigned to you by the lab instructor.
  19. Refresh the browser.
  20. Click the **Database** tab.
  21. Click the **My requests** link.
  22. The webpage should look similar to the screen shown below.

Now when any member of the HELPxX group selects the Database tab, they will only see the My requests link. When this link is selected, they will only see database requests that have been given to them. The only action users can perform on the listed database requests is Run.

My Requests [ ]

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Bluetooth

Address http://s400la:2016/webaccess/iWADBRequests?page=1 User: help01a

iSeries Access for Web IBM

## My Requests

Print  
5250  
Database  
• My requests  
Files

Request	Description	Action	Shortcut	Created By	Access
	Data for HELPxx users - PDF format		Yes	wa01adm	help01

Related Links:

- iSeries Access for Web
- iSeries Access
- iSeries Navigator
- iSeries Information Center
- iSeries Resource Library

[Shortcuts to requests you created](#)  
Displays a list of shortcuts to requests you created. Shortcuts can be deleted from this list.

### Shortcuts

- A database request can only be accessed by the user profile used to create it.
- A shortcut is a way to share a request with other users and groups.
- Changes to the original request are automatically picked up by the shortcut.
- The access value identifies who is able to access the shortcut.

### Action Details

My Requests supports the following actions for requests and shortcuts:

- **Run**  
Use the Run action to run a saved SQL or copy data to table request. When a shortcut is run, the original request is run.

[Top of page](#)

IBM iSeries Service 5.4.0.05-191.S125551 Local intranet

## **My Folder**

When using System i Access for Web functions, the results of those functions can be stored to a personal folder in the i5/OS integrated file system. By default, every user of System i Access for Web is assigned a personal folder.

Multiple functions of System i Access for Web provide the option to store operation results to a personal folder. For example, a printer output file can be converted into a PDF document and then saved to the owner's personal folder or another's personal folder.

Using the My Folder function, the contents of the personal folder can be viewed, opened, e-mailed, copied to the i5/OS integrated file system, or copied to another user's personal folder.

Members of the SALESxx group were denied access to My Folder. When those policy settings were copied to the HELPxx group, members of the HELPxx group were also denied access to My Folder. This exercise is going to allow members of the HELPxx group access to the My Folder function.

1. Switch to the browser window where WAXXADM is logged in.
2. Click the **Customize** tab in the navigation bar on the left side of the web page.
3. Click the **Policies** link.
4. In the Profile field, type **HELPxx** ...where "xx" is the numeric value assigned to you by the lab instructor.
5. Click the **Edit Policies** button.
6. The web page will be refreshed listing the categories of System i Access for Web functions.
7. Click the action icon for the My Folder category.

You will see that all of the My Folder policies have been set to Deny. These policies were copied from the SALESxx group where My Folder was not made available to members of the SALESxx group.

8. The top level policy is 'My Folder access'. Change the Setting to **Allow**.
9. Click the **Apply** button at the bottom of the web page. This will reset all of the My Folder policies to Allow for the HELPxx group.

10. We will leave most of the policy settings set to default values.

We will change the 'Maximum folder size' policy setting. The default is 'No maximum'. Leaving the setting to 'No maximum' would allow the user to use as much system storage as they wanted. This may not be desirable in your environment.

Set the Setting to **100 MB**.

11. Click the **Save** button at the bottom of the web page.

12. To see how objects can be placed into the personal folder, switch to the browser window where HELPxxA is logged in ...where "xx" is the numeric value assigned to you by the lab instructor.

13. Click the **Print** tab in the navigation bar on the left side of the web page.

14. Click the **Printer output** link.

15. Click the **View PDF** action icon for a spool file listed.

16. In the Destination drop down box, select **Personal folder**.

17. Click the **Settings** button.

If desired, you could enter a different description of the item that will be placed in the personal folder.

The 'Folder owner' field is defaulted to HELPxxA. If you wanted to send this item to a different user's personal folder, you would enter their i5/OS user ID in this field.

Leave the fields set to the default values. Click the **OK** button.

18. Click the **Run** button.

The printer output will be converted to a PDF document and the document will be placed in the personal folder.

19. Click the **My Folder** tab in the navigation bar on the left side of the web page. The webpage should look similar to the screen shown below.

Click the **Open** action icon to view the PDF document.

Click the Back button of the browser to return to the System i Access for Web webpage.

My Folder

File Edit View Favorites Tools Help

Address http://s400la:2016/webaccess/RWAMyFolder User: help01a

iSeries Access for Web IBM

## My Folder

My Folder

Print 0.02% of 100 MB used






\$250

Database

Files

Related Links:

- iSeries Access for Web
- iSeries Access
- iSeries Navigator
- iSeries Information Center
- iSeries Resource Library

Item	Status	From	Date/Time	Size	Action
<input type="checkbox"/> Printer output in PDF	Unopened	help01a	4/5/07 10:21 PM	16279	    

[Delete Selected Items](#)

Mark all opened  
Change the status of all items in this folder to opened.

Mark all unopened  
Change the status of all items in this folder to unopened.

Delete all opened items  
Delete all of the opened items from this folder.

Delete all items  
Delete all of the items from this folder.

Local intranet

## ***Checkpoint #2***

System i Access for Web is ready for use by the HELPxx group.

The features of System i Access for Web for this group were based on the settings provided to the SALESxx group. The HELPxx group settings were further enhanced to include access to the Database and My Folder functions.

The remaining exercise addresses how to transfer customization and configuration settings from an existing user to a new user.

## ***Transfer customization/configuration settings to a new user***

If a new employee were to join the Sales team, what would be the process for giving them access to System i Access for Web like the other people on the Sales team?

The information below discusses the steps to add a new user and transfer System i Access for Web configuration information from one user profile to another.

For this discussion, assume the new employee is given the user ID **SALESxxZ** ... where “xx” is the numeric value assigned to you by the lab instructor.

1. Since the i5/OS system administrator had previously created the SALESxx group, the administrator now uses the System i Navigator *Users and Groups* → *All Users* function to add **SALESxxZ** to the SALESxx group.
2. Since many System i Access for Web policies have been set for the SALESxx group, **SALESxxZ** automatically has all the same capabilities and look in System i Access for Web as the other members of the SALESxx group.

It was not necessary for the System i Access for Web administrator to copy any policies to the new member.

With the addition of user **SALESxxZ** to the Sales team, user **SALESxxA** is being promoted to a new position and is leaving the Sales team. User **SALESxxZ** will be taking over user **SALESxxA**'s job responsibilities. How can configuration items owned by **SALESxxA** be transferred to **SALESxxZ** ?

1. In the 5250 exercise, the WAXxADM administrator created shortcuts to 5250 sessions for user SALESxxA. These shortcut settings were stored as user configuration data specific to user SALESxxA. They are not part of any group level policy settings.
2. The Transfer Configuration Data function enables administrators to transfer System i Access for Web configuration items between i5/OS user profiles. This transfer applies to configuration items stored/set at the user level. It does not transfer information stored/set at the group or higher levels.

The Transfer function supports transferring configuration items at the category level from a source user profile to a target user profile. Configuration items that can be transferred include:

- 5250 sessions -- configured 5250 sessions and shortcuts currently defined for the source profile are transferred to the target profile's Configured Sessions list.

- 5250 macros -- recorded 5250 macros and macro shortcuts currently defined for the source profile are transferred to the target profile's My Macros list.
  - Commands -- saved commands currently defined for the source profile are transferred to the target profile's My Commands list.
  - Database requests -- saved database requests and request shortcuts currently defined for the source profile are transferred to the target profile's My Requests list.
  - Folder items -- currently in the My folder list for the source profile are transferred to the target profile's My Folder list.
  - Policies set for the source profile are set for the target profile. All settings currently set for the target profile are removed prior to transferring settings. That is, settings from the source profile are not merged with current target profile settings. Note: Group policy and preference settings for the source profile are not transferred.
3. Switch to the browser window where WAXxADM is logged in.
  4. Click the **Customize** tab in the navigation bar on the left side of the web page.
  5. Click the **Transfer configuration** link.
  6. In the From profile field, type **SALESxxA** ...where “xx” is the numeric value assigned to you by the lab instructor.
  7. In the To profile field, type **SALESxxZ** ...where “xx” is the numeric value assigned to you by the lab instructor.
  8. The Copy action to perform will copy the configuration items to the new user. The Move action to perform will move the configuration items to the new user.  
  
Select the **Move** option just to make sure everything is transferred.
  9. Select all the options listed in the Data to Transfer option.  
  
When the Transfer Configuration Data runs, it will tell us if some of the categories did not have anything to transfer.
  10. Click the **Transfer Data** button.

The web page will be updated with the results of the Transfer. It is likely that you received some errors and warnings for the transfer operation. In the middle of the



web page is a summary of the **Transfer results** where it lists how many errors and warnings occurred, and the total items transferred during the transfer operation. Let's look into the details of what occurred during the transfer.

The errors likely indicate that some items could not be transferred because the SALESxxZ user is not allowed to use some functions. The ability to run Commands would be an example.

The warnings likely indicate that the SALESxxA user did not have any configuration data to transfer to SALESxxZ user.

One item was moved from SALESxxA to SALESxxZ. Click the **View all results** link in the middle of the web page. The list of items will be refreshed indicating that SALESxxA policies were transferred successfully. These were policies set specifically for user SALESxxA (not group level policies).

Because these user level policies were transferred, let's look at what those policies are set to...they may need to be modified.

11. Click the **Customize** tab in the navigation bar on the left side of the web page.
12. Click the **Policies** link.
13. In the Profile field, type **SALESxxZ** ...where "xx" is the numeric value assigned to you by the lab instructor.
14. Click the **Edit Policies** button.
15. The web page will be refreshed listing the categories of System i Access for Web functions. Below the list of categories are several links.

Click the **View all policies** link.

16. The displayed web page lists all of the policy settings for user SALESxxZ and what level the policies are set (derived from). For more information regarding the levels at which policies are set, click the Help link (? icon) in the header of the 'Derived From' column.
17. We want to see what user level policies were transferred by the Transfer configuration function. We want to review these policy settings because we may need to modify them to make them unique to user SALESxxZ.

At the top of the webpage is an option on how to sort the list. Click the Sort by: **Derived From** link.

18. The list will be refreshed showing category→policy items that have a ‘Derived From’ column value of ‘Profile setting’ at the top of the list.

19. You will see the ‘Files→Default directory’ policy...

- The policy has a Derived from value of ‘Profile setting’ which means this policy was set at a user level (not a group, \*PUBLIC, or default setting level).
- The current setting is ‘/home/SALES01A’

Since this list of policies is for user SALESxxZ, this user level policy should be updated to have a value of ‘/home/SALES01Z’.

20. You will see that the ‘Mail→E-mail address’ policy...

- The policy has a Derived from value of ‘Profile setting’ which means this policy was set at a user level (not a group, \*PUBLIC, or default setting level).
- The current setting is ‘SALESxxA@S400LA’

Since this list of policies is for user SALESxxZ, this user level policy should be updated to have a value of ‘SALESxxZ@S400LA’.

21. We are not going to update these policies as part of this lab. We wanted to show you how to check the policies that were transferred and how to see what policies may need additional modification.

## **Summary**

Since System i Access for Web integrates nicely with the i5/OS user and group profile concepts, administration for web browser users is greatly simplified.

We have shown in this lab that we can use the Customize Policy tools to fully control the functions each user has access to, and how we can reuse policies that are set up.

All this adds up to easier administration of i5/OS web browser users.

## Reference information

The i5/OS and System i Information Center documentation can be used to learn more about System i Access for Web. You can access the Information Center at:

- <http://publib.boulder.ibm.com/infocenter/iseres/v5r4/index.jsp?topic=/rzamm/rzammaccessweb.htm>

## Trademarks and Disclaimers

© IBM Corporation 1994-2007. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at <http://www.ibm.com/legal/copytrade.shtml>.

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. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others.

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

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

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

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

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

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

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

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