LAB: System i Access for Web

Using the Functions:

Customize

Restricting Access and General Configuration

Linda Hirsch (LLHIRSCH@us.ibm.com), IBM Rochester

System i Access for Web Development Team

IBM Rochester, MN

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

Table of Contents

Lab Objective

System i Access for Web provides support for customizing user preferences. It also provides administrators with the ability to restrict access to the various functions and subfunctions in System i Access for Web.

These restrictions are saved via policy settings for particular user and group profiles.

Customize functionality is accessed through the **Customize** tab on the System i Access for Web navigation bar. By clicking on the Customize tab, an overview of the tasks you can perform using these functions is shown in the System i Access for Web content pane.

By Default, all users of System i Access for Web are allowed to change any of their Preference settings. Those with administrator authority are allowed to restrict access to System i Access for Web functions for other user and group profiles they have access to.

In this lab you will learn how to use some of the features available in the System i Access for Web customization function. In particular, you will learn how to restrict user's access to functions such as print and database, change the data displayed by a function, control access to the file system, and configure email support.

Before starting the lab exercises, make sure you have read the **Lab Instructions** document. Information contained in that document will be used in the lab tasks contained in this document.

Good luck with the lab exercises!

Please raise your hand if you have questions!

Task 1: Change user preference to indicate which columns to display when viewing printer output queues

This task shows you how to use Customize -> Preferences functions of System i Access for Web to change the columns to display when viewing printer output queues.

Follow these steps to modify your printer viewing preferences with System i Access for Web.

1. If you currently have a browser open and it is displaying a System i Access for Web page that includes the navigation bar; you may skip to step 2, otherwise open a web browser. Open the ***System i Access for Web Main URL*** from the lab worksheet. Sign on to i5/OS using the ***User ID*** and ***Password*** values from the lab worksheet.
2. Click the **Customize** navigation tab on the left side of your browser window.
3. Click the **Preferences** link to display the preferences category panel.
4. Click the **Edit Preferences - Print** image (in the Action column) for the **Print** category.
5. Under the **Output queues** section, click the **Columns...** button for the **Output queue list columns** preference.
6. You should now see the **Columns - Output Queues** panel. Uncheck the **Action**, **Files**, and **Writer** columns. Then ensure the **Output Queue** and **Status** columns are checked.
7. Click **Save** to save the output queue columns you want displayed.
8. You should now be back at the **Edit Preferences - Print** panel again.
9. Click **Save** to save these print preferences.
10. Now, click the **Print** navigation tab on the left side of your browser window.
11. Click the **Output queues** link to display the list of printer output queues.
12. You should see the list of printer output queues with only the **Output Queue** and **Status** columns being displayed for each output queue.

Task 2: Denying access to the Printer Output Queues function

System i Access for Web allows administrators to deny access to functions of System i Access for Web. Normally, the administrator would deny access for other users and group profiles, but in this exercise, you will deny access to a function for the profile you are currently logged in as.

The following steps show you how to deny access to the Printer Output Queues function.

1. Click the **Print** navigation tab on the left side of your browser window.
2. Click the **Output queues** link to display the printer output queues.
3. Create a bookmark for this page in your browser. For example, from Microsoft Internet Explorer, use the Favorites -> Add to Favorites function. Remember the folder location of the bookmark, you'll use it in a later step.
4. Click the **Customize** navigation tab on the left side of your browser window.
5. Click the **Policies** link.
6. Ensure the i5/OS user profile you logged in as is in the **Profile** edit field, then click the **Edit Policies** button.
7. Click the **Edit Policies - Print** image (in the Action column) for the **Print** category.
8. Scroll the page and find the **Output queues** policy. For this policy, select the setting control that contains the **Allow/Deny** choices and choose **Deny**.
9. Click **Save** to save this policy setting.
10. Now use the Bookmark or Favorites function of your browser to display the bookmark to the Print -> Output Queues you created in step 3.
11. When the page comes up, hit the Reload or Refresh button from your browser. The message "**Error - You are not authorized to access this function, contact your system administrator**" should be displayed.

Task 3: Displaying the advanced Printers view

System i Access for Web allows administrators to change the view the users see when they use the Printers function of System i Access for Web. Normally, the users see the basic view of the Printers function, but in this exercise, you will change to use the advanced printers view for the profile you are currently logged in as.

The following steps show you how to get the advanced view for the Printers function.

1. Click the **Print** navigation tab on the left side of your browser window.
2. Click the **Printers** link to display the printers on the system.
3. Click the **Customize** navigation tab on the left side of your browser window.
4. Click the **Policies** link.
5. Ensure the i5/OS user profile you logged in as is in the **Profile** edit field, then click the **Edit Policies** button.

6. Click the **Edit Policies - Print** image (in the Action column) for the **Print** category.
7. Under the **Printers** section, find the **Printers list view** policy. For this policy, select the setting control that contains the **Basic/Advanced** choices and choose **Advanced**.
8. Click **Save** to save this policy setting.
9. Click the **Print** navigation tab on the left side of your browser window.
10. Click the **Printers** link to display the printers on the system.
11. When the page comes up, you should now see the advanced view for the Printers list. This view allows users more control over the resources required when using i5/OS printing.

Task 4: Displaying a single printer action option

System i Access for Web allows administrators to control the actions users can take for their printer output. Normally, the user would see multiple actions for working with their printer output. An administrator may want to hide some action options for their users. In this exercise, you will change to allow only the View PDF printer output action option for the profile you are currently logged in as.

The following steps show you how to deny access to all but the GIF printer output preview option.

1. Click the **Print** navigation tab on the left side of your browser window.
2. Click the **Printer output** link to display the list of your printer output. Note the actions available from the **Action** column. Move your mouse over the action images. Popup text will be displayed, indicating the action associated with the image.
3. Click the **Customize** navigation tab on the left side of your browser window.
4. Click the **Policies** link.
5. Ensure the i5/OS user profile you logged in as is in the **Profile** edit field, then click the **Edit Policies** button.
6. Click the **Edit Policies - Print** image (in the Action column) for the **Print** category.
7. Under the **Printer output** section, find the **View printer output** policy. For this policy, select the setting control that contains the **Allow/Deny** choices and choose **Deny**.
8. In the same section, find the **View printer output as selected format** policy. For this policy, select the setting control that contains the **Allow/Deny** choices and choose **Deny**.
9. Click **Save** to save these policy setting changes.
10. Click the **Print** navigation tab on the left side of your browser window.

11. Click the **Printer output** link to display the list of your printer output.
12. When the page comes up, you should now see only the **Work with** and **View PDF** actions available in the Action column of the Printer output list. The **View** and **View As** actions are no longer available.

Task 5: Controlling access to the file system

System i Access for Web allows access to the i5/OS Integrated File System (IFS). Administrators can control how users are able to access the IFS when using System i Access for Web. The shipped defaults for System i Access for Web allows all users to access the IFS starting at the root path. i5/OS security for the IFS is enforced by System i Access for Web. If you don't have the directories and/or files in your IFS protected by object level security, customization policies can be used to control what the users are allowed to see. In this exercise, you will change the base path for a user viewing the IFS, and not allow the profile you are currently logged in as to go to the parent directory of this base path.

The following steps show you how to set up a specific path that a user can access in the IFS.

1. Click the **Files** navigation tab on the left side of your browser window.
2. Click the **Browse files** link to display the contents of the file system. The list of contents should start at the root path in the IFS. This is indicated by a list title of **Directory Contents /,** where the slash '/' means root directory.
3. Click the **Customize** navigation tab on the left side of your browser window.
4. Click the **Policies** link.
5. Ensure the i5/OS user profile you logged in as is in the **Profile** edit field, then click the **Edit Policies** button.
6. Click the **Edit Policies - Files** image (in the Action column) for the **Files** category.
7. Under the **Browse files** section, scroll down to the **Default directory** policy. Click the **Browse…** button. Scroll down and select the radio button next to the **walab** directory path. Click the **Select** button.
8. You should be back on the **Edit Policies – Files** page. Next, find the **Display parent directory contents** policy. For this policy, select the setting control that contains the **Allow/Deny** choices and choose **Deny**.
9. Click **Save** to save these policy setting changes.
10. Click the **Files** navigation tab on the left side of your browser window.
11. Click the **Browse files** link to display the contents of the file system.
12. When the page comes up, you should now see the contents of the **walab** directory. You should not be able to navigate to this path's parent directory (which is the root directory).

Task 6: Restrict database users to only allow them to run requests they have been given

This task shows you how to restrict users of the Database functions of System i Access for Web. An administrator can set policies to allow users to run only database statements they have been given in a request. By doing this, the users can't run potentially more destructive database operations such as inserts, updates, deletes, or stored procedures.

Follow these steps to modify your database policies within System i Access for Web.

1. Click the **Database** navigation tab on the left side of your browser window. You should see links to items that provide a wide scope of database functionality.
2. Click the **Customize** navigation tab on the left side of your browser window.
3. Click the **Policies** link.
4. Ensure the i5/OS user profile you logged in as is in the **Profile** edit field, then click the **Edit Policies** button.
5. Click the **Edit Policies - Database** image (in the Action column) for the **Database** category.
6. Find the **Tables** policy. For this policy, select the setting control that contains the **Allow/Deny** choices and choose **Deny**. This prevents the user from being able to run any of the Tables functions.
7. Scroll down to the **Requests** policy section. Leave **Requests** and **Run request** policies at Allow**.** For the remaining Allow/Deny request policies in the **Request** section (14 of them), set the **Allow/Deny** settings to **Deny**.
8. Scroll down to the **Run SQL requests** policy row. For this policy, select the Allow/Deny control and choose **Deny.** This prevents the user from being able to enter and run SQL statements.
9. Scroll down to the **Copy data to table** policy row. For this policy, select the Allow/Deny control and choose **Deny.** This prevents the user from running any Copy data to table operations.
10. Scroll down to the **Import request** policy row. For this policy, select the Allow/Deny control and choose **Deny.**
11. Scroll down to the **Import query** policy row. For this policy, select the Allow/Deny control and choose **Deny.**
12. Scroll down to the **Extract i5/OS object data** policy row. For this policy, select the Allow/Deny control and choose **Deny.**
13. Click **Save** to save these policy setting changes.
14. Now, click the **Database** navigation tab on the left side of your browser window.

15. You should see only a **My requests** link. The requests listed under My requests will be the requests that were given to the user by other administrative users.

Task 7: Denying access to Messages, Files, Command, and Download functions

System i Access for Web allows administrators to deny access to functional categories of System i Access for Web. Normally, the administrator would deny access for other users and group profiles, but in this exercise, you will deny access to functional categories for the profile you are currently logged in as.

The following steps show you how to deny access to the Messages, Files, Command, and Download functional categories.

1. Click the **Customize** navigation tab on the left side of your browser window. You should see navigation tabs for many other functional categories including Messages, Files, Command, and Download.
2. Click the **Policies** link.
3. Ensure the i5/OS user profile you logged in as is in the **Profile** edit field, then click the **Edit Policies** button.
4. Click the **Change category access** link in the list of link at the bottom of the page. The Policies – Change Category Access page is displayed.
5. Find the **Command** category. For this category, select the setting control that contains the **Allow/Deny** choices and choose **Deny**. This prevents the user from being able to access any of the Command functions.
6. Find the **Download** category. For this category, select the setting control that contains the **Allow/Deny** choices and choose **Deny**. This prevents the user from being able to access any of the Download functions.
7. Find the **Files** category. For this category, select the setting control that contains the **Allow/Deny** choices and choose **Deny**. This prevents the user from being able to access any of the Files functions.
8. Find the **Messages** category. For this category, select the setting control that contains the **Allow/Deny** choices and choose **Deny**. This prevents the user from being able to access any of the Messages functions.
9. Click **Save** to save these policy setting changes.
10. You should no longer see navigation tabs for Messages, Files, Command, and Download.

Task 8: Resetting Preference and Policy settings to their default values

This task shows you how to reset policy settings to their default values. The following steps will reset the preference and policy settings you updated in tasks 1 through 7 above.

1. Click the **Customize** navigation tab on the left side of your browser window.
2. Click the **Policies** link.
3. Click the **User profiles** link.
4. Scroll down and locate your **WAxx** (where xx is your team number) profile.
5. Click the **Reset policies** image (in the Action column) for your **Waxx** profile.
6. Click the **Reset Policies** button from the **Confirm Reset Policies** page.
7. From the tasks above, verify the settings have been restored to their default values. You may have to hit the Refresh or Reload buttons on your browser to make sure the browser isn't displaying a cached page.

Congratulations!

You have completed the System i Access for Web lab!

Tradmarks and Disclaimers

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, operation 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.