WebReport/i

Report Intranet Feature

Version 14

As of June 2022

Kisco Systems LLC
54 Danbury Road, #439
Ridgefield, CT 06877

Phone:	**(518) 897-5002**
E-mail:	**Sales@Kisco.com**
WWW:	**http://www.kisco.com**
Customer Support:	**http://www.kisco.com/webreport/support**

Table Of Contents

Introduction

This documentation covers the WebReport/i Report Intranet Feature. This documentation is intended to provide you with information on how to configure the Apache HTTP server on your System i server to run the Report Intranet Feature in WebReport/i and instructions on using this browser based feature.

Overview

The Report Intranet Feature in WebReport/i is a feature that allows you to deploy reports from your IBM i System through an Intranet website. This requires that your IBM i use the Apache HTTP web server active and configured.

The browser based Intranet allows you to deploy report distribution through a browser. You control which reports are deployed this way through options selected during conversion in WebReport/i.

All of the reports deployed through this new feature must be processed through the WREPORT command or processed through Automatic Routing through what is known in WebReport/i as an HTML routing. These reports are converted into any one of the many formats available in WebReport/i and are stored in the IFS on your System i. Several new options have been added to the WREPORT/HTML Routing process that identify the report as going to the Intranet, control where the reports are stored and classify the report so that you can control which users can view the report. When a report is added to the Intranet, it must be coded as to the class of report so that the distribution controls can be enforced.

Each user who is going to view reports must log in to the Intranet using a valid IBM i user profile and password. They must also be registered to WebReport/i along with classification codes that describe which reports they are allowed to work with. This can be done either at the user profile level or at the group level. A classification of *ALL at the user or group level will give the user access to all reports in the Intranet.

Adding Reports To The Intranet

Reports are added to the WebReport/i Report Intranet using the WREPORT command, option #2 on the MASTER menu. They can also be added from the "Work with WebReport/i Spool Files" function, option #4 on the MASTER menu, or by Automatic HTML routing.

When processing any of these options, you will now find a new option for the type of document. By coding the type with the special value of '*INTR', the report being processed will be stored in the Report Intranet on your system. **Note that this can only be done AFTER the Report Intranet option has been installed and configured.**

When storing a report in the Report Intranet, three new fields must be entered as follows:

Intranet folder name	This is a working folder that must be entered. You can choose any value you want, but a value must be entered. If the folder does not exist already, one will be automatically created. **Do not precede the value entered with a slash character ('/')**
Intranet file name	Enter the name of the file to be stored in the Report Intranet. Make sure that the suffix characters assigned to the file name conform with the format of the document. For example, if this is a *PDF conversion, then the Intranet file name should end with the characters ".pdf".
Intranet class	Each report stored in the Report Intranet must be coded with a class code. This code is assign by you and can be up to 5 characters long, all upper case. The coding structure is wide open, so some consideration should be given to this. The class code will be used to control which users are allowed to view the reports that are stored in the Report Intranet. For example, if a report is a system status report, you might code it with a class code of 'SYSTS'. If it is an Inventory report, then you might use a class code of 'INV'. Then, when you configure user access to the Report Intranet, you can indicate which class of reports each user will be allowed to view.

When reports are added to the Report Intranet, they are actually stored in the Integrated File System on your System i. You will find them in the following IFS path:

/www/webreport/htdocs/*folder*/*

The *folder* should be replaced with the "Intranet folder name" used above.

When a report is added to the Report Intranet, it is also posted to the index listing for the contents of the Report Intranet. If a match is found in this index listing, the previous entry will be automatically replaced.

Adding Documents To The Intranet

The WebReport/i Report Intranet feature lets you store converted spool files in the IFS and provide access to them via a web browser. A command included with the software lets you post your own files or documents to the Intranet for sharing with end users. This opens up the Intranet feature to uses beyond just working with spool files converted by WebReport/I.

The new command is "Add Report To Intranet" (ADDINTRPT). Using this command, you can let the WebReport/i Intranet feature know about additional files that you want to make available to your Intranet users. The command lets you select the folder within the Intranet where you want the files placed, specify the file name and code the file for the access class that you want to limit access to.

Before using the ADDINTRPT command, you must first place your file in the correct IFS location for your Intranet path. The files available to the Intranet are all stored in the following path:

/www/webreport/htdocs/

Within this path, you must also create the folder you want to use. For example, if you want to create a folder for Prices, then you would create a new folder under the htdocs path named "prices".

Once the new folder is added, then the reports you add will be in the path:

/www/webreport/htdocs/prices/

To then make these files available to your Report Intranet users, all you need to do is run the ADDINTRPT command. There are 5 parameters as follows:

TITLE	Enter a simple description for the file being stored.
FORMAT	Enter the code that describes the type of file being added to the Intranet. You must use one of the following codes: *HTML *TXT *PDF *XLS *RTF *TIF *CSV *XLX
FLR	Enter the name of the folder you are using. Do not start this folder name with a slash character (/).
IFS	Enter the name of the file you have placed. Note that these filename may not contain embedded blank characters in the name. Any blank characters found will cause the command to stop with an error.
INTRCLASS	Enter the access class code that you want to use. See the documentation for the Intranet feature for a full description on how class codes are used.

Maintaining Reports In The Intranet

The index of reports is manually maintained at this point by using option #3 on the MASTER menu which is “Review HTML Index” (WRKWEBIDX). To remove a report from the Report Intranet, just locate it using this option and delete it with option 4.

With Release 13, WebReport/i allows for an Intranet user to delete reports that are displayed in their authorized set of reports.

For an Intranet user to be able to delete reports from their browser display session, they must first be authorized to perform report deletes. This is done from the User Access feature (F9) in the Review HTML Index feature, option #3 on the MASTER menu.

Users must be enrolled in the User Access feature before they can access reports through the Intranet. When users are set up, you will now find a new field; "User allowed to delete reports?". This field will default to no access (value N). If you want an Intranet user to be able to delete reports, change this value to Y.

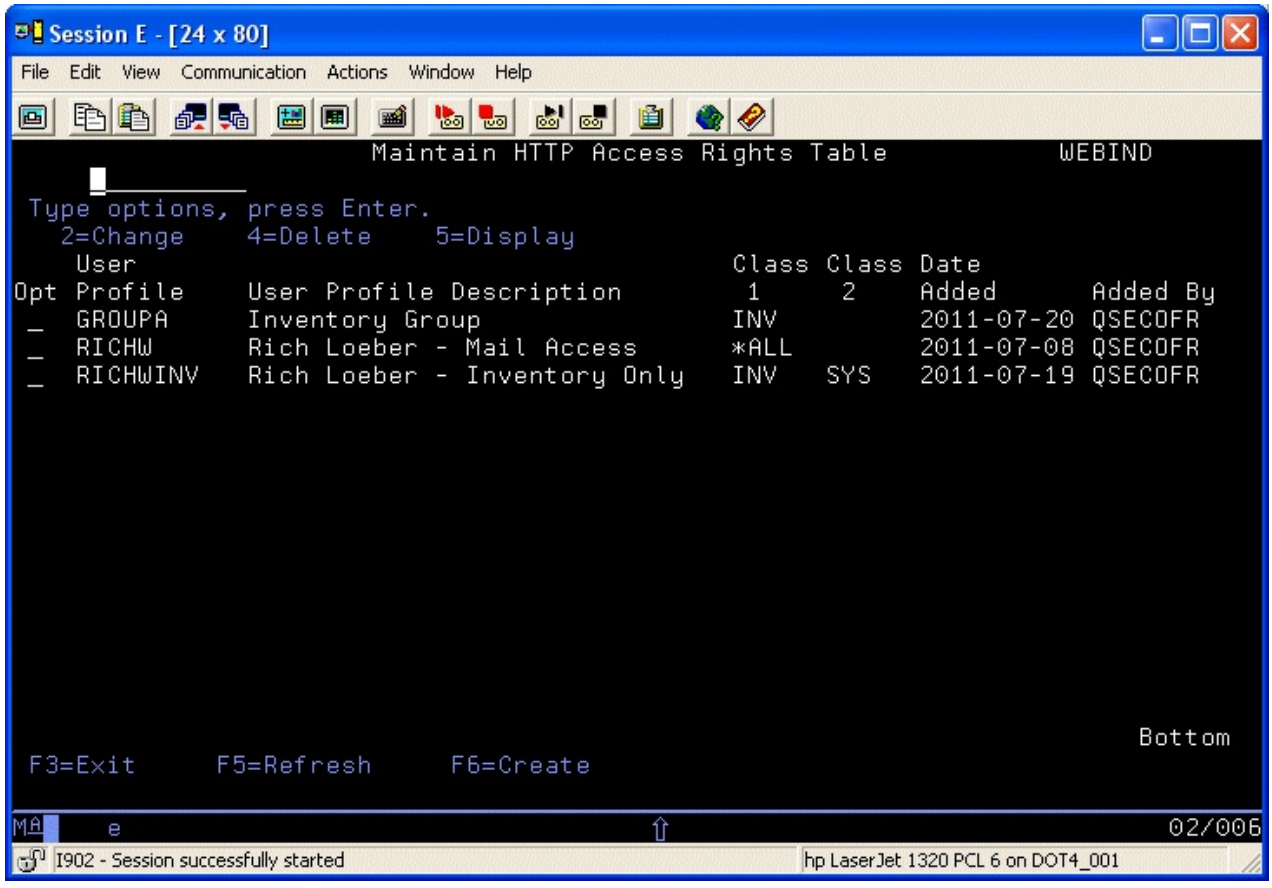
The Intranet report list has also now been changed with a new "Delete" column on the right side of the display panel. When a user is authorized to process report deletes, a blue box icon will display under the "Delete" column heading. To delete a report, click on this icon. A confirmation panel will be shown and you can either confirm the delete or cancel it at that point.

Configuring Users For Intranet Access

For a user to access reports using the browser based Report Intranet Feature in WebReport/i, they must have a valid IBM i user profile and password. If a user is already set up with a profile and password, no additional profile needs to be created. If a user is not currently a user on your system, a new profile will need to be issued. For those users that you do not want to have actual logon access for terminal sessions, make sure that the new profile is set up with the INLMNU(*SIGNOFF) setting so that terminal signon is disabled. Also, make sure that these users have very limited security with no special authorities. This will limit your security exposure.

Once a user profile has been created, you then need to use a new feature in WebReport/i to define which reports the user is allowed to view from the Report Intranet. To access this new feature, run option #3 on the MASTER menu, Review HTML Index (WRKWEBIDX). This option was previously used to track reports that were converted into PC formats and stored in various locations on the system. A new feature now lets you specify that the report being converted should be sent to the Report Intranet.

After starting option #3 on the MASTER menu you will now see a new F9 function key available that will take you to the "Maintain HTTP Access Rights Table" feature. When you select this option, the following screen will be displayed:

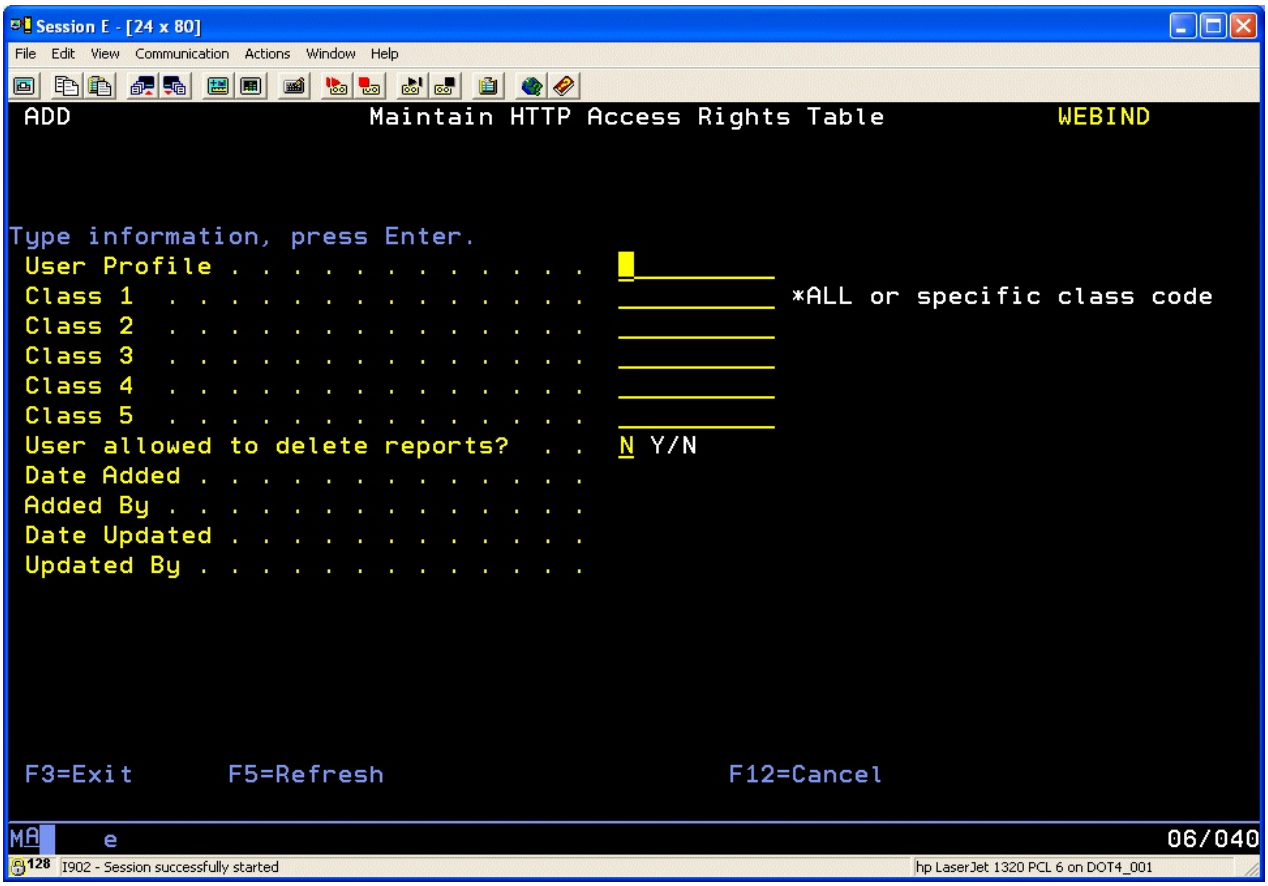


Initially, this will be displayed with no records listed.

Users can be registered to use the Report Intranet either by their individual user profile or by the

group profile that is associated with their user profile. Using the group profile will simplify setup. If your installation uses groups, then I would suggest you explore this capability.

To add a profile to this list, use the F6 key:



Enter the user profile, either for the individual user or the group that you are registering, then enter up to five class codes for the user to be authorized to see when logged into the Report Intranet. If you want to authorize the profile for all reports, then enter the special value of *ALL in the first class code and leave the rest of them blank.

If you want the user to be able to use the delete function from their browser to remove reports from the system, change the "User allowed to delete reports?" setting to **Y**.

When you enter the record, the date added and added by fields will be completed automatically. If you have occasion to change the registration the date updated and updated by fields will also be updated automatically.

Using The Report Intranet

To use the Report Intranet in WebReport/i, you must first configure the Apache HTTP server on your system and start the server instance for WebReport/i. Please refer to the separate configuration section of this documentation for instructions on how to set this up. You must also have placed reports into the Report Intranet and configured user access as shown in the previous sections of this documentation.

To get started, just type in the following URL on your browser:

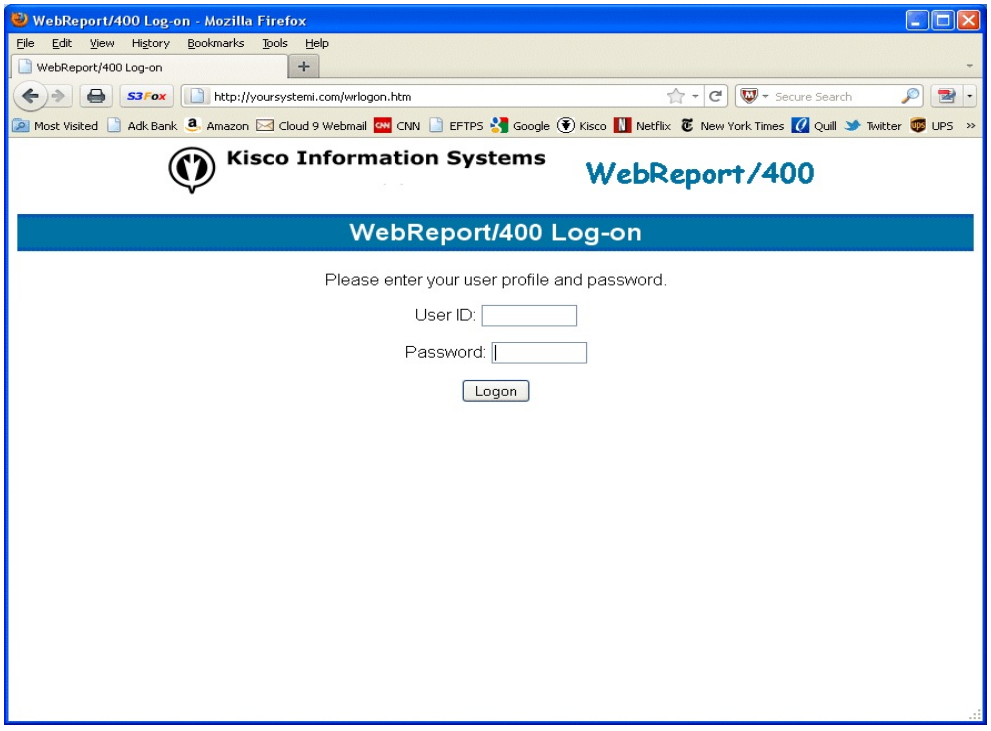
http://yoursystemi.com/wrlogon.htm

If you have secure HTTPS configuration completed, replace the "http" with "https".

Replace the "yoursystemi.com" with a reference to your System i TCP/IP address. You can use either a named address or a numerical address, such as "10.1.1.12".

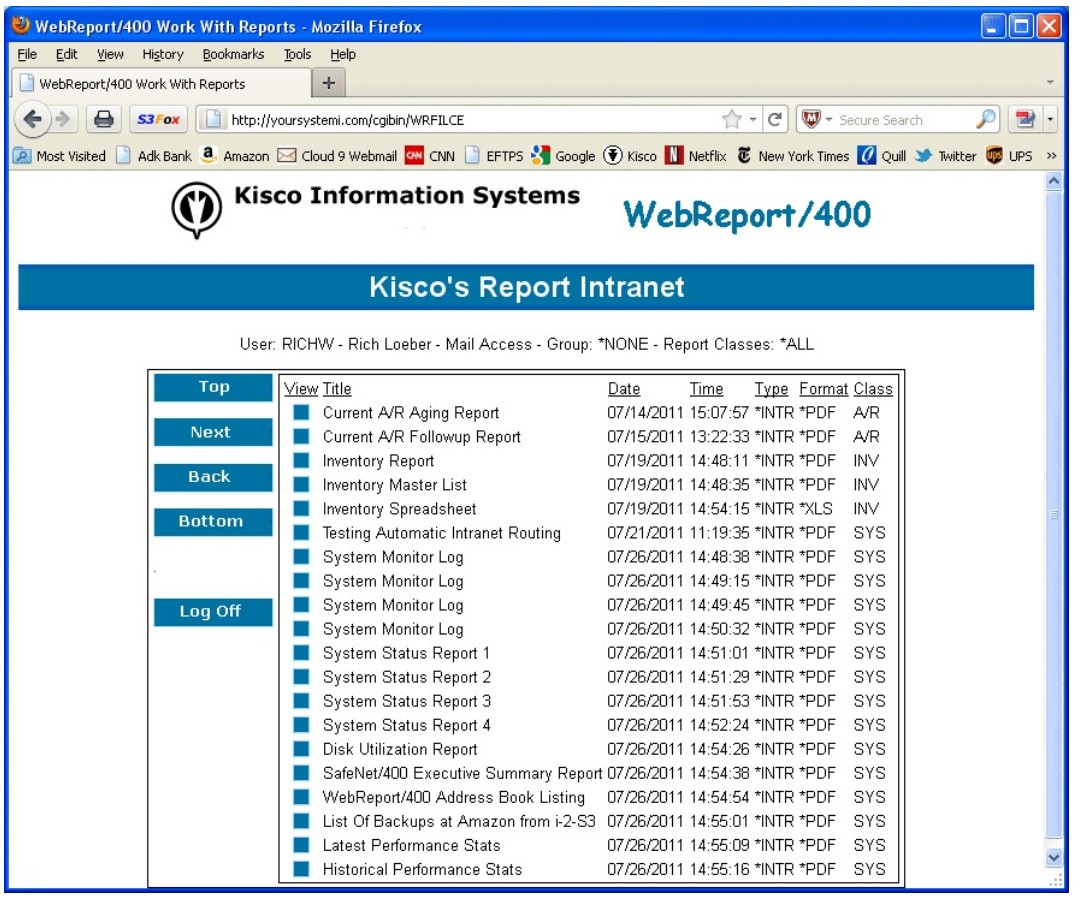
Important note: The initial recommendation from Kisco Systems is to implement the Intranet using the HTTP connection. This connection is not secure and it is recommended that you take precautions as your user profile and password will be passed as open text through your network. See the documentation for setup considerations for an HTTPS secure connection.

When you enter the above URL, the following will be displayed by your browser:



Log on to your system using a user profile that is authorized to use the WebReport/i Report Intranet. When the logon is completed, the following starting point display will come up in your browser:

WebReport/i will validate the user profile and password used. If the user is not authorized to use the Report Intranet or the password is not valid, the logon request will be rejected. If the logon is successful, then the following will be displayed on your browser:



When the list if first shown, it is presented in date and time sequence. If you want to change the list to be shown in Report Title sequence, just click on the Title in the column heading. Similarly, if you are looking at multiple Classes of reports, you can change the sequence to show by Class and Report Title by clicking on the Class in the column heading. Clicking again on the Date heading will return the display to date and time sequence.

To view any report listed, just click on the small blue button to the left. The large blue buttons on the left panel can be used for navigation purposes.

Note that the user profile logged on is shown along with the system level description of that profile. If there is a group profile associated with the user, it will also be displayed along with the class code (or codes) that the user is authorized to view.

In this case, the profile has no group associated with it and is authorized to look at all reports in the Report Intranet.

It will be helpful for you and your users to get into the practice of using the Log Off option when done using the Report Intranet as that takes the software through a cleanup process that will remove some temporary objects from your system.

If the user has been authorized to delete reports, each report listed will have an additional column on the right hand side of the display with a delete option available. Clicking on that option will cause the report to be removed from the Intranet following a confirmation process.

Apache HTTP Server Configuration

For the Report Intranet in WebReport/i to work, you will have to configure and activate a server instance for the Apache HTTP server on your System i.

The following checklist will have to be done to complete the configuration. The details will follow for each step.

Step 1: Start the Apache Administrative server tool on your IBM i.
Step 2: Create a new HTTP server instance named WEBREPORT
Step 3: Edit the configuration file for the new server instance
Step 4: Locate and open the WEBREPORT.txt file supplied by Kisco
Step 5: Cut/Paste the WEBREPORT.txt file contents into the configuration file and apply it
Step 6: Install the server instance files supplied by Kisco
Step 7: Start the new WEBREPORT server instance
Step 8: Finalize object installation setup
Step 9: Authorize system profiles in security setup
Step 10: Customize settings for your requirements

Step 1: Start the Apache Administrative server tool on your System i.

To configure an Apache server instance, you must first start the Administration server instance for Apache. You can do this from a command line on your System i with the following command:

STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)

The server may take a while to initialize, so wait a few minutes before starting up the configuration wizard in your browser. When you are ready, point your browser to the following web address:

http://yoursystemi.com:2001/

The system will prompt you for a user profile and password. Once that has been supplied, a page of iSeries Tasks will be displayed. Select the "IBM Web Administration for iSeries" option. This will take you to the Web Administration wizard that comes with your OS.

Step 2: Create a new HTTP server instance named WEBREPORT

After you sign on and get to the Web Administration page, navigate to the "Manage" tab and then the "HTTP Servers" tab below that. Under the "Common Tasks and Wizards", select "Create HTTP Server". For server name, you MUST specify the value "WEBREPORT". The server description of "Kisco WebReport/i Server" can also be used. Click on Next for all of the following displays taking all of the default options presented until you reach the "Create HTTP Server" panel with a "Finish" button at the bottom. Press the Finish button to complete creating the new server instance.

Step 3: Edit the configuration file for the new server instance

The above process will leave you with the new WEBREPORT server instance already selected. Scroll down on the left hand list of tasks to the "Tools" section and select the item marked "Edit Configuration File". This will open an edit window with what appears to be a text file displayed by the Web Administration wizard. Leave this open in your browser and move on to the next step.

Step 4: Locate and open the WEBREPORT.txt file supplied by Kisco

In the program materials sent to you from Kisco, you will find a text file named WEBREPORT.txt. Locate this file and open it with NotePad or WordPad on your desktop PC. At this point, you will have the Configuration File for the new server instance open in your browser and the WEBREPORT.txt file open on your desktop.

Step 5: Cut/Paste the WEBREPORT.txt file contents into the configuration file and apply it

Using standard cut and paste methods, copy ALL of the text in the WEBREPORT.txt file over so that it replaces ALL of the text in the Configuration File for the new server instance. When you are done, double check to make sure that all of the Configuration File characters have now been replaced.

Step 6: Install the server instance files supplied by Kisco

Once you have verified that the cut and paste was successful, press the Apply button below the Configuration File in your browser. (You can also close the WEBREPORT.txt file, you will not need it again. Make sure you do not make any changes to this file. If your NotePad or WordPad program asks if you want to save the file, reply "No".)

Step 7: Start the new WEBREPORT server instance

Start the newly created server instance. You can do this from the Web Administration page or from your command line. If you do this from the command line, issue the following:

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(WEBREPORT)
```

The server instance will now be active. Go to your browser and enter the following URL:

```
http://yoursystemi.com
```

IBM's standard test page should now be shown. This will indicate that the server is active, but you are not yet ready to use the Report Intranet Feature features of WebReport/i yet.

Step 8: Finalize object installation setup

At this point, additional objects need to be installed in the IFS plus the required service programs used by your installed version of the OS needs to be set up for use by WebReport/i. You can do all this from your command line by running the following command from the command line:

CALL PGM(WEBREPORT/WWWINSTAL)

This process will restore objects to the IFS for use by the newly configured server instance. It will then set those objects with the correct access authority and finally, it will set up the server service programs needed by the HTTP server on your system.

Step 9: Authorize system profiles in security setup

Before you can use the Intranet feature from a browser, you will need to add two system user profiles in the list of Security Profiles. Using option #15 on the INSTALL menu, add the following two profiles to the list as Administrators for all functions (Authorization Code 1):

QTMHHTP1
QTMHHTTP

These profiles must be set up regardless of whether you have Application Security active or not in the general application settings in option #9 (WEBSET) from the INSTALL menu.

Step 10: Customize settings for your requirements

There are two customized settings that you should set at this point using the WEBSET command in WebReport/i. This can be done from the command or by using option #9 on the INSTALL menu. The two settings that control the Report Intranet Feature are:

Intranet Lines Roll Factor

This controls the number of detail lines that are shown on each web page. The setting defaults to 20 lines, but you can set it to as high or low a number as you like.

Intranet Title

This text will appear as a heading line on your Report Intranet display in your web browser. Note that if you want to use a quote character, it must be entered as two single quotes. The default value as shipped is “Kisco‘‘s Report Intranet”.

At this point, the Report Intranet Feature in WebReport/i is available for use on your system.

If you want to configure your own server instance or use a different instance that is already active on your system, you can do so provided that the following are taken into account:

- Add WEBREPORT as a directory entry
- ADD a URL mapping entry to map “/cgibin/” to WEBREPORT

- Authorize user access to WEBREPORT
- Permit CGI programs to be run from WEBREPORT

If you have other HTTP server instances already running, you may want to configure the WebReport/i instance so that it works from a different port number. If that is the case, then the access URL that you use to start the Report Intranet Feature in WebReport/i will appear as follows:

http://yoursystemi.com/wrlogon.htm

Security Considerations

For instructions on how to configure the Apache server for a secure HTTPS connection, please review the following section of this documentation.

If you decide to implement the Apache server without HTTPS security, then the logon process used will pass a valid user profile and password through your network in open clear text. As a result, Kisco specifically recommends that you only use this feature in a secure network environment where all activity takes place behind a firewall or a strong network router using internal IP addresses only.

As a second level of security, we also recommend that you set up a special user profile for use with Report Intranet access. You should use this profile only for the purpose of logging in to Intranet through your browser. When you set the profile up, limit its function in the event that the profile and password are compromised. We recommend that you include the following additional specification when the profile is created:

INLMNU(*SIGNOFF)	This will force a logoff if someone tries to log on through a normal terminal session using this profile.

Also, if you have exit point control software in place, you should set this profile up to deny all network access to your system. This will prevent the profile from being used by FTP, ODBC, iNavigator, etc. If you do not have exit point control software in place, we suggest you take a look at our SafeNet/i software for your system to guard against this threat.

Configuring Apache for HTTPS Secure Use

WebReport/i supports use of this Report Intranet tool over a secure HTTPS browser connection. We recommend that when you first set up and configure the Report Intranet on your system, that you use the previous non-secure configuration to get started. This will simplify the setup routine. The following documentation assumes that you already have a working configuration using plain HTTP browser connections to your IBM i server.

HTTPS Configuration Overview

The following sequence of events must be completed to convert your working HTTP server instance (named WEBREPORT) from a plain HTTP server configuration to a secure HTTPS server configuration.

1. Start the *ADMIN server instance on your IBM i and log in.
2. Update your current HTTP server instance configuration to support HTTPS.
3. Enable SSL for the server instance and register the WEBREPORT application.
4. Connect to the Digital Certificate Manager application on your browser.
5. Create a new digital certificate in the *SYSTEM certificate store.
6. Validate the newly created certificate.
7. Assign the new certificate to the WEBREPORT application.
8. Start the updated WEBREPORT server instance.
9. Verify that the configuration is working correctly.

Step 1 - Start the *ADMIN server instance on your System i and log in.

From the command line on your system, enter the following command:

STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)

This will start the web server administration tool on your system. This startup process can take a minute or two to complete. After waiting, go to your web browser and enter the following address in the address box of your browser:

http://yoursystemi.com:2001

You will be prompted for a logon process. **You must sign on as a security officer** with full authority to your system, such as QSECOFR. When the logon is complete, the IBM i5/OS Tasks menu should be displayed. On some releases of the IBM i/OS, you may have to select a link to the "i5/OS Tasks" page following a successful logon process.

Step 2 - Update your current HTTP server instance configuration to support HTTPS.

From the i5/OS Tasks menu, select the "IBM Web Administration for i5/OS" link. This will start the Apache web administration tool. Select the "Manage" tab and then, when it is displayed, select the "HTTP Servers" tab. In the "Server:" selection box, locate and select the WEBREPORT server. **If it is not there, then you need to configure it and test it in a non-secure environment before continuing with this procedure.** This is covered earlier in this documentation. When you have selected the WEBREPORT server, verify that it is showing with a status of "Stopped". If active, then you will need to stop it now before continuing.

Before continuing, you will need the text file named WEBREPORT_HTTPS.txt that was shipped with your software. If you received your software on CD, you will find this file on the CD. If you got your software by download, this file is available on the download page for WebReport/i at www.kisco.com. When you have located this file, open it in a text editor such as NotePad or WordPad.

In your current browser session, scroll down the lefthand panel until you find the link that shows as "Edit Configuration File" under the "Tools" section at the bottom of the panel. Select this link and your current configuration file will be displayed. If you have customized this at all from the configuration file shipped from Kisco Systems, we recommend that you cut and paste the current configuration statements into a separate text file and save it for possible future use. Once this has been done, you should remove all of the current statements in the configuration file. Then, cut and paste the statements from the WEBREPORT_HTTPS.txt file into the configuration file. When this is done, press the "Apply" button at the bottom of the panel.

Step 3 - Enable SSL for the server instance and register the WEBREPORT application

Select the "Security" link from the lefthand panel. In the tab labeled "SSL with Certificate Authentication", select the SSL box and choose the "Enabled" setting. Then, in the box immediately next to the "SSL certificate application name:", key in the value "WEBREPORT". We recommend that you do this in all capital letters. Press the "Apply" button to record these changes.

Your server instance is now converted to work with HTTPS. Continue with the next steps.

Step 4 - Connect to the Digital Certificate Manager application on your browser.

In your browser, re-enter the base address for the i5/OS Tasks:

http://yoursystemi.com:2001

This will bring you back to the main menu. Select the link for the "Digital Certificate Manager".

Note: The following process will self-issue a digital certificate for use with your HTTPS server instance. When used from your browser, this will give you a warning because your server is not a registered certificate issuer, but the process will work correctly as long as you bypass the warning. On some browsers, such as Firefox, you will be allowed to accept the certificate the first time you use it and it will not be questioned again. Other browsers, like some versions of Internet Explorer, will question your use every time. Regardless, you will know where the certificate came from and you will be able to trust it by virtue of that knowledge.

Step 5 - Create a new digital certificate in the *SYSTEM certificate store.

Select the button in the top left corner of your browser that reads “Select a Certificate Store”. On the next panel, select the *SYSTEM store and press the “Continue” button. (If the *SYSTEM store does not exist, you will need to first create it using the “Create New Certificate Store” link.) Your system will prompt you for the password for the *SYSTEM certificate store. If you don’t know the password, you can use the reset function to assign a new password. When you are finished, the *SYSTEM certificate store will be open and available.

Now, select the “Create Certificate” link from the left-hand panel. On the next panel, select the option for “Server or client certificate” and press the “Continue” button. Next, select the option for “Local Certificate Authority” and press “Continue” again. Now the certificate form is displayed. Fill out the required fields as follows:

Certificate label	Enter the value “WEBREPORT”.
Common name	Enter a unique name. Kisco recommends that you use the system name for your system (or partition) as shown from the DSPNETA command display.
Organization name	Enter the name of your company or organization.
State or province	Enter the name of the state or province where you are located.
Country or region	Enter an abbreviation for your country.

Select the “Continue” button at the bottom of the page and your certificate will be created.

Step 6 - Validate the newly created certificate.

In the left hand panel, select the “Manage certificates” link. Next, select the “Validate certificate” link. Choose the “Server or client” option and press the “Continue” button. Select the WEBREPORT that you just created, then press the “Validate” button at the bottom of the page. If everything with the certificate is OK, a message will be displayed confirming that the certificate is valid.

Step 7 - Assign the new certificate to the WEBREPORT application.

In the left hand panel, select the “Assign certificate” link. Select the WEBREPORT certificate, then press the “Assign to Applications” button. Locate the WEBREPORT application in the list displayed and place a check mark next to it. Press the “Continue” button. A message will be displayed confirming that the certificate is now assigned to the application.

Step 8 - Start the updated WEBREPORT server instance.

On a terminal session command line, enter the following command:

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(WEBREPORT)
```

This will start the server instance that has been converted for use with HTTPS security. If the

server instance fails to start, make sure there is not another server instance active using the secure port number 443. Only one application at a time can be active using this port. If you need more than one active, you will have to change the server instance to use a different port number.

Step 9 - Verify that the configuration is working correctly.

Once the server instance has been started, enter the following web address into your browser's address box:

https://yoursystemi.com

A test page from the WEBREPORT server instance should be displayed. As stated earlier, a warning message about the certificate in use may be issued by your browser. Please note the comments associated with Step 4 above about this issue.