Information Builders

WebFOCUS

Setting Up Your Environment

WebFOCUS Business User Edition

April 22, 2016

Contents

Chapter 1

Setting Up Your Environment

Configure and customize your environment, create users and groups, and manage your resources using the available functionalities.

In this chapter:

Using the Administration Console

The Administration Console contains the settings that configure the WebFOCUS Client, customize internal or external authentication settings, connect you to ReportCaster, and support diagnostic research.

Opening the Administration Console

Because the Administration Console contains settings that can alter the operation of your entire WebFOCUS installation, it is available only to those users with the privileges to update or reconfigure system settings. In the Business User Edition, the Administration Console is available only to the Manager User.

Before you can open the Administration Console, you must sign in with a User ID that has the privilege to do so. Once you have signed in with the appropriate privileges, the Administration Console is visible and available for review and updates. You can then open the Administration Console from the Menu bar, or from a link on the Getting Started page.

You can also open the Administration Console directly from the address bar of your browser window by entering the URL of the Administration Console and then signing in with a User ID that has the appropriate privileges.

Procedure: How to Sign In to the Administration Console From the Start Menu

1. If WebFOCUS Business User Edition has been installed on a Windows machine, click the *Start* button, and then click the *Information Builders* folder.
2. Click the *WebFOCUS Business User Edition 82* folder, and then click *Run WebFOCUS Business User Edition*.
3. In the Sign In page, type the *ID* and *Password* of a User that has privileges to open the Administration Console, and then click *Sign In*.
4. To open the Administration Console from the Menu bar, click *Administration*, and then click *Administration Console*.
5. To open the Administration Console from the Quick Links Page, in the Manage section, click *Configure System*.

Procedure: How to Sign in to the Administration Console From a Browser Window

1. Go to the URL:

   `http(s)://machine:port/context/admin`

where:

`machine`

Is the network id of your computer.

`port`

Is the number of the port that connects your computer to the server hosting WebFOCUS BUE.

`context`

Is the local address for WebFOCUS BUE. For example, *ibi_apps*.

2. On the Sign In page, type the *ID* and *Password* of a User that has privileges to open the Administration Console, and click *Sign In*.

   The Administration Console opens automatically.

   To display the Administration Console using a different language, you can use the Dynamic Language Switch on the Configuration menu.

Using the Administration Console Menu Bar

The Administration Console menu bar appears above the Administration Console tab display. Its commands and features are available to all of the Administration Console tabs.

Using the Licenses Menu

The Licenses Menu links you to information about your current product license, an audit of User and Group licenses and roles, and to information about licenses for all third-party software products included in the installation. Using Licenses menu commands you can:

- View the current license number, product edition, license key expiration date, and the number of licensed users. You can also add new license numbers.
- Access license information for all third-party software packaged with WebFOCUS BUE.

Reviewing Client License Information

The WebFOCUS Client command opens the License Information dialog box. This dialog box identifies the current license key and the individual product components made available by that key. You can also use it to replace the current license key with a new license key when your current license expires or changes.

	Available Functionality
License Information	The License Information section provides the following information: ❑ **Product Edition.** The name of the current product edition. ❑ **License Key.** The license key currently in use. ❑ **License Key Expiration Date.** The date the license key will expire. ❑ **User Licenses.** The total number of available user licenses and the number of licenses used for each user category. For example: ❑ **Product Components.** The product components your license entitles you to use. If the check box to the right of an entry is visible and selected, you are entitled to use that product component.
	❑ **New License Key.** Opens the Update License dialog box, where you can add a new license key and site code.

Reference: **Managing Client Licenses**

Access to WebFOCUS features and the number of licensed users is based on your license key and site code.

When the number of users exceeds the number of licensed users, the User Licenses Used count displays, in red, a message that the user license count has been exceeded, which is written to the event.log trace file. Users that are authorized to access the Administration Console will receive a message upon signing in.

User licenses are maintained or enforced when the following product components are licensed:

- **WebFOCUS Portal.** The number of Licensed Portal Users.
- **Portal Users (PR).** The number of users with Portal Privileges.

- **InfoAssist+ Users.** The number of users with portal privileges and InfoAssist+ privileges.

Procedure: **How to Configure License Codes**

Access to the WebFOCUS features and the number of Managed Reporting users is based on your license key and site code. You can change these values from the License Management page.

1. In the Administration Console menu bar, click *Licenses*, and then click *WebFOCUS Client*.

   The License Management window opens, displaying features available under the current license.

2. Click *New License Key*.
3. Type your new license key and site code.
4. Click *Validate*.

   The License Management page displays the current license key, the new license key, and the features that the new license key provides.

5. Click *Save* to implement the new license.

You must reload your web application in order for your changes to take effect. In addition, users must sign out and sign back in to obtain access to any new features.

Reviewing User Audit Information

The User Audit command evaluates the repository license usage for Total Users, Portal Users, and InfoAssist+ Users. The command produces a License Analysis report that identifies the total number of licenses by license type, the number of licenses in use by license type, and analyzes license assignments by Group and by User.

You can run the User Audit utility (license_audit.bat) from your local WebFOCUS installation directory, which is available in the following location:

```
drive:\ibi\WebFOCUS_BUE82\WebFOCUS\utilities\mr
```

When you run this program, it generates the License Analysis report and transfers it to the auditUserCounts.htm file, in the same directory.

The License Analysis report contains the following information:

License Analysis	
License Key	Displays your current license key.

License Analysis	
User License	Displays the user license types that are authorized under your current license key. This can include the following: ❑ TotalUsers ❑ PortalUsers ❑ InfoAssistUsers
Code	Displays the code for each user license, such as TU for Total Users.
Maximum	Displays the maximum number of user licenses that are available with your license key.
In Use	Displays the number of user licenses that are currently in use.
Available	Displays the number of user licenses that are available for each license.
Analysis of Groups	
Group Path	Displays the Groups stored in the repository. The following groups are created by the WebFOCUS Repository Creation utility, by default: ❑ /EVERYONE ❑ /Getting_Started ❑ /Managers ❑ /Retail Samples
License Type(s)	Displays the license types for each Group, such as TU.
Role	Displays the role of each Group, such as SystemFullControl.
On Resource	Displays the resource to which the Role is applied for the Group.
Former Type(s)	Displays the former types of licenses for each Group.

License Analysis	
Groups Summary	Displays counts for the following: ❑ Number of groups ❑ Number of groups with license types ❑ Number of groups with no license types ❑ Number of groups with changed user types ❑ Number of groups with cleared user types ❑ Number of groups with unchanged types
Analysis of Users	
User Name	Displays the users stored in the repository. The following users are created by the WebFOCUS Repository Creation utility, by default: ❑ manager
License Type(s)	Displays the license types assigned to each user.
# Group w/Licenses	Displays the number of groups with licenses of which the user is a member.
Former Type(s)	Displays the license types that have been changed or cleared for each user.
User Summary	Displays counts for the following: ❑ Number of users ❑ Number of users with license types ❑ Number of users with no license types ❑ Number of users with changed user types ❑ Number of users with cleared user types ❑ Number of users with unchanged types

Procedure: **How to Run the User Audit for the WebFOCUS Client from the Administration Console**

1. From the Administration Console menu bar, click *Licenses*, and then click *User Audit*.

   The License Analysis report opens in a separate browser window.

Reviewing Third Party Licenses

The Third Party command opens the 3rd Party Information page that displays the following information for each third-party software application used to support different features in WebFOCUS BUE:

- Description
- Version
- File(s)
- License
- Third-Party Links

The WebFOCUS BUE product uses various third-party software applications that support a variety of features.

Clearing the Cache

The Clear Cache command refreshes the state of the WebFOCUS application by applying saved changes that are not applied dynamically. Even though some changes are dynamic or only require the administrative user to clear the cache to take effect, others require an administrative user to recycle the web application.

Closing the Administration Console

The Close command closes the Administration Console. After the console closes, you remain signed in to your work session.

Opening Administration Console Help

When you click the Help icon, the online Help file opens to a topic that describes the tab, setting, or feature currently on display.

Configuring Security

In the Administration Console Security Tab, you can adapt the default security settings to your local environment.

Security can either be configured internally in the WebFOCUS BUE repository, or externally in a Microsoft Active Directory or an LDAP directory that is not part of WebFOCUS BUE. To accommodate this, you can use either the Internal page or the External page on the Security tab in the Administration Console.

Internal authentication and authorization is enabled by default.

Using Internal Security

Internal authentication and authorization is enabled by default. Optionally, you can use the settings in the Internal page to configure password policies.

Maximum Sign-In Attempts (IBI_Max_Bad_Attempts)

Specifies the number of unsuccessful sign-in attempts allowed before the account status is changed to locked. The default value is 0, which allows unlimited attempts.

Lockout Duration (Minutes) (IBI_Account_Lockout_Duration)

Specifies the number of minutes before the status of an account changes from locked to active. The default value is 0 (off).

Lockout Duration Reset (Minutes) (IBI_Account_Lockout_Duration_Reset)

Specifies the number of minutes that must elapse after the number of failed sign-in attempts specified by the Maximum Sign-in Attempts setting before the allowed sign-in attempt counter is reset to 0. The available range is from 1 to 99,999 minutes. The default value is 0 (off).

Enforce Password Complexity (IBI_Password_Complexity)

Specifies password requirements. The default value is False (check box clear).

If set to True (check box selected), passwords must:

- Not contain the user account name or parts of the full name of the user that exceed two consecutive characters.
- Be at least six characters long or at least the number of characters specified in Minimum Password Length, whichever is greater.
- Contain characters from three of the following four categories:
  - Uppercase English characters (A through Z).
  - Lowercase English characters (a through z).
  - Base 10 digits (0 through 9).
  - Non-alphabetic characters (for example, !, $, #, %).

- Complexity requirements are enforced when passwords are changed or created.

Minimum Password Length (IBI_Password_Minimum_Length)

Defines the required minimum length of a password. The default value is 0 characters.

Password Reuse (IBI_Password_Reuse)

Specifies the number of recent passwords that cannot be reused. The default value is 0 changes. If Password Reuse is set to 25, for example, WebFOCUS BUE will track the 25 most recent password changes.

Days Until Password Expires (IBI_Password_Expire)

Specifies the number of days that a password will remain active. The default value is 0, which prevents passwords from expiring. Once the password has expired, the user must take the action specified by the IBI_Password_Expire_Action setting.

Days Until Password Expiration Warning (IBI_Password_Expire_Warning)

Specifies the number of days prior to expiration that a warning will be displayed to the user. The default value is 0, which provides no warning. The value should be less than or equal to the IBI_Password_Expire setting.

Password Expiration Result (IBI_Password_Expire_Action)

Specifies the action required when a password expires. You can choose one of the following options:

- *To force Users with Expired passwords to change their passwords before signing in.* (MUSTCHANGE) This is the default value.
- *Change the status of users with expired passwords to inactive. Such users cannot sign in until a Manager resets the password in the Security Center.* (DISABLE-USER)

Using External Security

Use the External page if you have elected to configure security in a Microsoft Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) directory that is not part of WebFOCUS BUE.

Enable External Security

When you select this check box, internal security settings are overridden. WebFOCUS BUE directs all authentication activities and approvals to the external system you identify on this page.

External Security Type (IBI_Authentication_Type)

The drop-down list box for this field contains the following values:

- **Reporting Server.** Authenticates users against an AD or LDAP directory.
- **Legacy LDAP.** This value is not used with the Business User Edition.
- **Custom Java Plug-In.** This value is not used with the Business User Edition.

Understanding Custom Settings

To add custom settings using the Administration Console, select *Configuration*, select *Custom Settings*, and then enter the code changes in the text box. To encrypt the file containing the customizations, select the *Encrypt* check box.

Understanding Redirection Settings

You can view or edit redirection settings for the WebFOCUS Client though the Redirection Settings area of the Administration Console. However, you should not alter Redirection Settings without consulting Customer Support Services.

Redirection allows users to save report output in a temporary directory when a request is executed. Then an HTTP call is made from the browser to retrieve the temporary stored output for display in the browser.

If redirection is turned off, the report output displays in the browser immediately after the request is executed.

To change redirection settings in the Administration Console, click the *Configuration* tab and then *Redirection Settings*. The Redirection Settings panel opens, as shown in the following image.

Redirection Settings

WebFOCUS Extension	Content Type	Format	Redirect	Server Extension	Save Report	Client Extension	IBFS Format
.acx	text/plain	ascii	no	ACCESS	no	.acx	ascii
.bmp	image/bmp	binary	no	BMP	no	.bmp	binary
.cfg	text/cfg	ascii	no	N/A	no	.cfg	ascii
.class	java/*	binary	no	N/A	no	.class	ascii
.css	text/css	binary	no	CSS	no	.css	ascii
.csv	application/csv	ascii	yes	N/A	no	.csv	ascii
.dif	application/x-dif	ascii	yes	N/A	no	.dif	ascii
.doc	application/msword	ascii	yes	DOC	no	.doc	ascii
.docx	application/vnd.openxml	binary	no	DOCX	no	.docx	binary
.e97	application/vnd.ms-excel	ascii	no	N/A	no	.e97	ascii
.err	text/plain	ascii	no	ERRORS	no	.err	ascii
.fex	text/plain	ascii	no	FOCEXEC	no	.fex	ascii
.foc	application/foc	binary	no	FOCUS	no	.foc	binary
.for	text/plain	ascii	no	N/A	no	.for	ascii
.ftm	application/x-ftm	ascii	no	FOCTEMP	no	.ftm	ascii
.gfa	application/gfa	binary	no	N/A	no	.gfa	binary
.gif	image/gif	binary	no	GIF	no	.gif	binary
.hex	text/plain	ascii	no	N/A	no	.hex	ascii

Procedure: How to Change Redirection Settings

It is recommended that you do not change these settings unless instructed to do so by Customer Support Services.

1. In the Administration Console on the Configuration tab, click *Redirection Settings*.
2. In the Redirect column, select *yes* on a row to redirect the output to a temporary directory for the specified extension.
3. In the Save Report column, select *yes* to prompt users in the browser to open or save report output. When Save Report is set to *yes*, the report output retains the Save As name, if specified in the request.

For example, specifying ON TABLE PCHOLD AS MYREPORT FORMAT PDF in a request and setting Save Report to *yes* for the .pdf extension enables a user to open or save the output as MYREPORT.pdf. The Save As name specified is returned to the browser in uppercase. If Save Report is set to *yes* and no Save As name is specified in the request, a random file name is generated.

Important: You must do the following to use the Save Report functionality for GRAPH requests (specified with a PNG, SVG, GIF, JPEG, or JPG format in the procedure):

- Set Save Report to *yes* for the .htm Extension.

  Running a server-side GRAPH request creates an HTM file that contains a link to the actual graph output, which is stored as a temporary image file with a .jpeg, .jpg, .gif, .svg, or .png extension.

- When you execute a GRAPH request, if you select the *Save* option when prompted to open or save the output, the output is saved to an HTM file using only a reference to the graph image, which will eventually expire and be deleted from the server (according to the temporary file expiration settings in the Client Configuration).

- To preserve the output of the GRAPH request, open the saved HTM file, right-click the graph image, and select *Save Picture As* to save it to disk permanently. You can then substitute an absolute reference to the saved image file in the returned HTM output file.

4. If you want to encrypt the redirection settings, select the Encrypt check box at the bottom of the screen.
5. Click *Save* to save your changes in the Redirection Settings panel.

Changing Application Settings

The Application Settings enables Managers to update configuration settings that are required by various components of the WebFOCUS BUE web application. You can view or edit the application settings through the Administration Console.

Initially, WebFOCUS BUE reads the configuration file to locate parameters and their values. If a parameter does not exist in the file, the BUE will then obtain the parameter and its value from the web.xml file of the web application currently deployed by the BUE.

Reference: Understanding Change Management Settings

The Change Management Settings determine which files are exported during the change management process, the format of the exported file, and whether some legacy functionality is preserved.

File Types Included in Export Package (IBI_CM_EXPORT_WFRS_FILE_EXTENSIONS)

Determines, by file extension, which files from the WebFOCUS Reporting Server or the web will be included in exports created by the change management feature. The values included by default are acx, bmp, css, fex, gif, htm, html, ico, jpeg, jpg, mas, png, sty, and svg.

Retain Handles (IBI_CM_RETAIN_HANDLES)

This option is not relevant to the BUE.

Zip Change Management Package (IBI_CM_ZIP)

When selected (True), the export package is compressed and delivered in a zip file.

Name format of Zip export files (IBI_CM_ZIP_FILE_FORMAT)

Select an option from the drop-down menu to specify the name format of the zip file.

Verify Signature on Import (IBI_CM_ZIP_VERIFY_SIGNATURE)

When selected (True), the export package is flagged for signature verification, which ensures both that the code has not been tampered with and that the signature was produced with the expected key.

Reference: Understanding Deferred Reporting Settings

Deferred Reporting Settings determine how deferred reports are processed.

Prompt for Custom Deferred Report Description (IBI_DEFERRED_CUSTOM_DESCRIPTION)

When this check box is selected, the default setting, users are prompted to optionally customize the description for the deferred report, which defaults to the title of the report being run deferred. This occurs whenever the description defined in the parameter (IBIMR_defer_description) has not been submitted with the run deferred report request.

When this check box is clear, the title of the report being submitted to run deferred is assigned to the deferred report description automatically, and no prompt appears.

Display Deferred Request Submitted Notification (IBI_DEFERRED_NOTIFY_SUBMITTED)

When this check box is selected, the default setting, the Deferred Request Submitted window displays to confirm a successful deferred request. The user clicks *OK* to close the window.

When this check box is clear, the Deferred Request Submitted window does not display.

Display Deferred Ticket Delete Confirmation (IBI_DEFERRED_TICKET_DELETE_CONFIRM)

Activates an automated message that prompts the user to confirm the deletion of a deferred report. When this check box is selected, which is the default, a message prompts the user to confirm the deletion, so a deletion requires two clicks. When this check box is clear, the user is not prompted to confirm the deletion, so a deletion requires only one click. Making a large number of deletions is faster when suppressing the confirmation message.

Reference: Understanding Parameter Prompting Settings

The Parameter Prompting Settings determine parameter prompting behavior in the WebFOCUS BUE Client.

Managed Reporting (IBIMR_PROMPTING)

Enables or disables parameter prompting for all Managed Reporting requests. Possible values are:

- **Off.** Turns off parameter prompting at the site level.
- **Run with Default Values. (XMLRUN)** Prompts for amper variables created with the -DEFAULT command and any other amper variable that does not have a value. This is the default value.
- **Always Prompt. (XMLPROMPT)** Prompts for amper variables created with the -DEFAULT command when there is another amper variable that does not have a value assigned.

Managed Reporting when Prompt Parameters Property Unset (IBIMR_PROMPTINGUNSET)

Enables or disables parameter prompting for Managed Reporting procedures (FEXes) when IBIMR_prompting is set to XMLPROMPT or XMLRUN, and the Prompt for Parameters setting is unchecked in the FEX Properties dialog box. Possible values are:

- **OFF.** Turns off parameter prompting.
- **Run with Default Values. (XMLRUN)** Prompts for amper variables created with the -DEFAULT command and any other amper variable that does not have a value. This is the default value.
- **Always Prompt. (XMLPROMPT)** Prompts for amper variables created with the -DEFAULT command when there is another amper variable that does not have a value assigned.

Self Service (IBI_WFDESCRIBE_DEFAULT)

Enables or disables amper auto prompting for self-service reporting. Possible values are:

- **OFF.** Turns off auto prompting. This is the default value.

- **Run with Default Values. (XMLRUN)** Prompts for amper variables created with the -DEFAULT command and for any other amper variable that does not have a value.
- **Always Prompt. (XMLPROMPT)** Only prompts for amper variables created with the -DEFAULT command when there is another amper variable that does not have a value assigned and, therefore, will be prompted for.
- **Display XML (Debug with syntax error checking). (XML)** The XML document describing the amper variables is displayed in the browser. This setting is used internally, and is recommended for debugging and syntax error checking purposes only.
- **Display XML (Debug). (XMLCHECK)** The XML document describing the amper variables is displayed in the browser. This setting is used internally, and is recommended for debugging purposes only.

Note: Managed Reporting uses a separate variable setting, which is IBIMR_prompting.

Default Template (IBI_WF_DESCRIBE_HTML)

The HTML template that defines the auto prompt layout.

Null Behavior (IBIF_DESCRIBE_NULL)

Specifies the value (_FOC_NULL or FOC_NONE) that the client assigns (in a -SET command) to the amper variable when the dynamic multi-select list *No Selection* value is selected. The default value is _FOC_NULL.

Changing Client Settings

The client configuration settings are grouped into categories under the Configuration menu in the WebFOCUS console. The term *Initial Value* next to a setting means that the value shown initially is the installation default value and that it can be overridden by setting the variable explicitly in the URL request.

InfoAssist+ Properties

Settings in the InfoAssist+ Properties page of the Administration Console determine the display and use of the InfoAssist+ tool that opens when Advanced Users, Developers, or Managers create or update content.

To enable or disable reporting options for the InfoAssist+ tool, click *Utilities*, scroll down to the bottom of the Configuration tab menu, and then click *InfoAssist+ Properties*.

Reference: Understanding InfoAssist+ Home Tab Properties

The InfoAssist+ Home tab enables you to control the most commonly used properties and options from the Format, Design, Filter, and Report groups. These properties are:

Use Live Preview Mode

Determines whether InfoAssist+ opens in the Live Preview mode or the Query Design View by default. When *Yes* is selected, InfoAssist+ opens in the Live Preview mode as the default. When *Yes* is not selected, InfoAssist+ starts with the Query Design View. If *Allow User Override* is checked for this option, users can change the setting specified by the Manager.

Record Limit

Enables the Record Limit menu of the Home tab. If *Show* is not selected, the Record Limit menu is removed from the InfoAssist+ interface.

Themes

Provides InfoAssist+ users with various color-coded StyleSheet themes that can be used to style reports and charts. Users can select standard InfoAssist+ themes, or select customized cascading style sheet themes created by your organization.

Page Heading

Enables the Head/Foot menu of the Home tab. InfoAssist+ users can use the Head/Foot menu to add a heading or footing to each page of the report output.

Report Heading

Enables the Head/Foot menu of the Home tab. InfoAssist+ users can use the Head/Foot menu to add a heading or footing to the first page of the report output.

Reference: Understanding InfoAssist+ Format Tab Properties

In InfoAssist+, the Format tab provides different options for selecting output formats and other reporting features, depending on whether the user is creating a report query or a chart query. For reports, the Format tab provides access to the Output Types, App Ribbon, Destination, Navigation, and Features groups. You can show or hide the following properties available in the InfoAssist+ Format tab:

Active Report Format

Enables the use of the HTML active report format. An HTML active report is a self-contained report that is designed for offline analysis. It contains all of the data and JavaScript within the HTML output file and it includes analysis options, such as filtering, sorting, and charting.

Select the check box to ensure that this option appears in the drop-down lists for the Report Output Format, Chart Output Format, and Document Output Format properties under the Tool Options Dialog Defaults section.

Additional HTML Formats for Chart

Enables the use of the PNG, JPEG, GIF, and SVG output formats. The default value is PNG. PNG is not available as a format for chart output.

Additional PDF Formats for Chart

Enables the use of the PDF/SVG and PDF/GIF output formats. The default value is PDF/SVG.

Excel 2000 Format

Enables the use of the Excel 2000 spreadsheet output format. The Excel 2000 format supports most StyleSheet attributes, allowing for full report formatting. The computer on which the report displays must have Microsoft Excel 2000 installed.

When this check box is selected, this output format option is available to select in the Output Format drop-down menus in the Tool Options Dialog Defaults section.

This check box is selected, by default.

Excel 2000 Formula

Enables the use of the Excel 2000 formulas when the *Excel 2000 Format* option is selected.

This check box is selected, by default.

XLSX (Excel 2007) Format

Enables the use of the XLSX (Excel 2007) spreadsheet output format. The computer on which the report displays must have Microsoft Excel 2007 installed.

When this check box is selected, this output format option is available to select in the Output Format drop-down menus in the Tool Options Dialog Defaults section.

This check box is selected, by default.

XLSX (Excel 2007) Formula

Enables the use of the XLSX (Excel 2007) formulas when the *Excel 2007 Format* check box is selected.

This check box is selected, by default.

Excel Pivot

Enables the use of the Excel 2000 PivotTable output format. PivotTable is an Excel tool for analyzing complex data, much like OLAP.

This check box is clear, by default.

HTML Format

Enables the use of the HTML page report format.

Select the check box to ensure that this option appears in the drop-down lists for the Report Output Format, Chart Output Format, and Document Output Format properties under the Tool Options Dialog Defaults section.

InfoMini Run Immediate

If *Enable* is selected, reports run immediately when InfoMini first launches. This setting is enabled by default.

Other Chart Types

Allows the creation of more complex graph output types, such as Spectral Maps, Gauge Charts, and Pareto Charts.

Pages on Demand

Enables the display of report output one page at a time. InfoAssist+ users can use the navigation menu at the bottom of the output screen to view each page. This option is activated only when HTML or active report output format is selected.

PDF Format

Enables the use of the PDF report format.

Select the check box to ensure that this option appears in the drop-down lists for the Report Output Format, Chart Output Format, and Document Output Format properties under the Tool Options Dialog Defaults section.

PowerPoint 2000 Format

Enables the use of the PowerPoint® 2000 document output format. The computer on which the report appears must have Microsoft PowerPoint 2000 or higher installed.

Select the check box to ensure that this option appears in the drop-down lists for the Report Output Format, Chart Output Format, and Document Output Format properties under the Tool Options Dialog Defaults section.

PowerPoint 2007 Format

Enables the use of the PowerPoint® 2007 document output format. The computer on which the report appears must have Microsoft PowerPoint 2007 or higher installed.

Select the check box to ensure that this option appears in the drop-down lists for the Report Output Format, Chart Output Format, and Document Output Format properties under the Tool Options Dialog Defaults section.

Stack Measures

Displays all numeric measure field names in the first column of the report output, with the corresponding numeric data values displayed across time in a column for each selected time period. The Stack Measures feature is activated only when HTML, Excel, or PowerPoint output format is selected. If *Allow User Override* is checked for this option, users can change the setting specified by the Manager.

User Selection

Allows users to change the output type of their reports at run time.

Reference: Understanding InfoAssist+ View Tab Properties

Enables InfoAssist+ users to customize the view of different report components in the InfoAssist+ tool, such as the design mode, output location, and data view. You can configure the following properties in the InfoAssist+ View tab:

Display View Tab

Enables the View tab and all of its menu options. If this is not selected, the View tab is removed from the InfoAssist+ interface.

Data Panel

Allows the user to customize Data Panel settings. Values are *Logical* (default), *List*, and *Structured*.

Query Panel

Allows the user to customize the view of the query components, such as Filters, Column and Row labels, and Measures when building a report. Values are *Tree* (default), *Area 2x2* (2 columns by 2 rows), *Area 1x4* (1 column by 4 rows). If *Allow User Override* is checked for this option, users can change the setting specified by the Manager.

Reference: Understanding InfoAssist+ Tool Options Dialog Defaults Properties

Enables Managers to specify default tool settings. If *Allow User Override* is checked for an option, users can change the setting specified by the Manager. However, the Manager cannot specify a default value that has already been disabled in one of the other groups. For example, if you have disabled the active report format in the Format Tab section, you will see an error message if you attempt to set that format as a default Compose Output Format in the Dialog Defaults section.

Report Output Format

Sets the default format for reports. Valid values are *HTML*, *active report*, *PDF*, *EXL07*, *EXL2K*, *PowerPoint 2000*, *PowerPoint 2007* , and *Visual Discovery AE* . To ensure that these options are available, a Manager must select the check box for each under the Format Tab section. The default value is *HTML*.

Chart Output Format

Sets the default format for charts. Valid values are *HTML*, *HTML5*, *active report*, *PDF*, *EXL2K*, *PowerPoint 2000*, and *PowerPoint 2007*. To ensure that these options are available, a Manager must select the check box for each under the Format Tab section. The default value is *HTML*.

Document Output Format

Sets the default format for reports that are generated using the Document Composer tool. Valid values are *HTML*, *active report*, *PDF*, *EXL2K*, *PowerPoint 2000*, and *PowerPoint 2007*. To ensure that these options are available, a Manager must select the check box for each under the Format Tab section. The default value is *Active Report*.

Page Orientation

Sets the default page orientation for reports and charts. Valid values are *Portrait* and *Landscape*. The default value is *Portrait*.

Page Size

Sets the default page size for reports and charts. Valid values are *A3*, *A4*, *A5*, *Letter*, *Tabloid*, *Legal*, *PPT-SLIDE*, and *Large Size*. The default value is *Letter*.

Data Preview Method

Sets the default action for whether reports are previewed using sample data or actual data from the data source. Valid values are Sample and Live. The default value is Live.

Record Limit

Sets the default maximum number of rows retrieved from the data source when Interactive Design view is selected. This feature is useful in reducing response time if users are working with a large amount of data. It is applicable only when developing the report. The record limit setting will not affect the report output at run time. Valid values are 0 to 10,000 rows. The default value is 500 rows.

Output Target

Sets the default location for reports and charts. Valid values are *Single tab*, *New tab*, *Single window*, and *New window*. The default value is *Single tab*.

InfoAssist+/Portal StyleSheet

Sets the style sheet to be used for InfoAssist+ and the Portal. Click *Change Stylesheet* to open the Browse predefined template files window.

Visualization StyleSheet

Sets the style sheet to be used when creating visualizations. Click *Change Stylesheet* to open the Browse predefined template files window.

Encode HTML

Encodes script tags within data, so that the tags are replaced and not executable in a browser. The default value is Yes. This includes the ON TABLE SET HTMLENCODE ON command in the procedure.

Enable Pages On Demand

Allows InfoAssist+ users to view report output one page at a time. The user can use the navigation menu at the bottom of the output screen to view each page. This option is activated only when HTML or active report output format is selected.

Rows retrieved from cache

Establishes how many rows of cached data stored in a binary file are returned to the output window at one time. The default value is 100 rows.

Reference: Understanding InfoAssist+ File Options

Determines which of the following file types can be selected by InfoAssist+ users when creating and saving HOLD files:

Binary

Stores report or chart data as binary numbers in numeric fields. Binary files use the extension (*.ftm).

FOCUS

Stores report or chart data as text in a segment structure that conforms to FOCUS database requirements. FOCUS files use the extension (*.foc).

Comma Delimited with Titles

Stores report or chart data as text in sequence by field. Alphanumeric fields are enclosed in quotation marks. Fields are separated by commas and are preceded by Field Names. Comma Delimited with Titles files use the extension (*.csv) (Comma Separated Values).

Plain Text

Stores report or chart data as text in sequence by field without delimiters or field names. Plain Text files use the extension (*.ftm).

Tab Delimited

Stores report or chart data as text in sequence by field. Fields are separated by tab characters. Tab Delimited files use the extension (*.tab).

Tab Delimited with Titles

Stores report or chart data as text in sequence by field. Fields are separated by tab characters, and are preceded with field names. Tab Delimited with Titles files use the extension (*.tab).

Database Table

Stores report or chart data as text in a field structure that conforms to a Structured Query Language (SQL) Database format. Database Table files use the extension (*.sql).

Database Table output is only available when working against an SQL database.

Hyperstage

Stores report or chart data as text in a field structure that conforms to the Hyperstage database table format. Hyperstage files use the extension (*.bht).

Hyperstage output is only available when the reporting server has a Hyperstage adapter configuration.

SQL script

Stores report or chart data as text in a sequential field structure that can be imported into a database table that conforms to the Structured Query Language (SQL) Database format. SQL Script files use the extension (*.sql).

SQL Script output is only available when working against an SQL database.

XML

Stores report or chart data as text in a field structure that conforms to the rules of the Extensible Markup Language. Fields are separated by tags that identify content. XML files use the extension (*.xml).

Reference: Understanding InfoAssist+ Miscellaneous Options

Use two-part file name

If selected, this option requires the use of two-part file names, which specify the path to the Master File location. If not selected, a one-part file name must be used instead. The default value is selected.

Expand Data Source Tree

Determines whether the initial view of the data source tree is expanded or collapsed. If selected, the tree is expanded. If not selected, the tree is collapsed. The default value is selected.

Join Tool

Displays the Join menu option on the InfoAssist+ Data tab. If not selected, the Join menu option is removed from the Data tab. The default value is selected.

Layout Tab

Enables the Layout tab in the InfoAssist+ control panel. If not selected, the Layout tab is removed from the InfoAssist+ control panel. The default value is selected.

Series Tab

Enables the Series tab in the InfoAssist+ control panel. The Series tab displays only when working with chart queries. It provides access to charting properties and options in the Properties, Line, and Pie menus. If not selected, the Series tab is removed from the InfoAssist+ control panel. The default value is selected.

Reporting Server Configuration Settings

Reporting Server configuration settings are available on the Configuration tab of the Administration Console. To view them you must expand the Reporting Server folder and the Server Connections folder, and click the Reporting Server icon.

Reference: Reporting Server Node Properties

The Reporting Server Node properties from the Basic pane are explained below.

Basic

Node Name

The logical name of the node. The name cannot be the same as any other node name. It must begin with a letter and cannot be more than eight characters. The Client will use this name when it accesses this server.

Node Description

Optional. The description of the node that appears in the Configuration pane. If this is omitted, the node name will be used.

Host

The Host name or IP address of the Server.

TCP/IP Port

The Port number for the TCP listener. The default port is 8120.

HTTP(S) Port

The Port number for the HTTP listener. This is typically one port after the TCP/IP port.

The default HTTP port is 8121.

Security

The security options for the reporting server connection.

- **Prompt for Credentials.** This option is not relevant for the BUE.
- **HTTP Basic.** This option is not relevant to the BUE.
- **Kerberos.** This option is not relevant for the BUE.
- **SAP Ticket.** This option is not relevant to the BUE.
- **Service Account.** This option is not relevant to the BUE.
- **Trusted.** Allows you to connect to the Reporting Server with only a user ID. This option is useful when no password is available for the user. Controls should be placed on the Server to ensure that connections from unauthorized clients are rejected. For example, you can employ the Reporting Server RESTRICT_TO_IP setting or configure a network firewall so that only a particular client can connect to the Server.

> **Note:** When configuring the Client to make trusted connections to the Reporting Server, you must also enable the Reporting Server to accept trusted connections.

Advanced

The Reporting Server Node properties from the Advanced pane are explained below.

Service Name

Description for the Reporting Server node. This description displays to end users.

Use HTTPS

Enables encrypted communication between the Client and the Reporting Server HTTP listener. The default value is off.

This option must be selected if the Reporting Server HTTP listener is configured to use SSL. If you are using a self-signed certificate to enable HTTPS communication with a Reporting Server, the certificate must be configured in the Java environment where the Client is installed. This enables HTTPS communication between the Reporting Server and the Administration Console.

Compression

Enables data compression. By default, data compression is disabled.

Encryption

Sets data encryption ability and the cryptography symmetric method used.

Select one of the following options from the drop-down list:

- **0.** Off. This is the default value.
- **AES.** Advanced Encryption Standard. The AES selections are in the format

  CIPHER(*x*)(-*MODE*)

  where:

  CIPHER

  Is AES128, AES192, AES256.

  x

  Is optional and defines an RSA key length of 1024 bits. When this is not specified, the RSA key is 512 bits.

  CBC

  Is optional and defines the use of Cipher Block Chaining (CBC) mode. When the mode is not specified, Electronic Code Book (ECB) is used.

For example, AES256x-CBC is the AES256 cipher with a 1024-bit RSA key in CBC mode. AES128 is the AES128 cipher with a 512-bit RSA key in ECB mode.

Connect Limit

Specifies the number of seconds that the Client will hold the pending connection. Other possible values are 0 (no wait) and -1 (infinite wait). The default value is -1.

Maximum Wait

Specifies the time, in seconds, that the Client will wait before timeout. You can optionally specify different return times for the first row and other rows. A single number indicates the return time is valid for any row. If two numbers are separated by a comma, the first number specifies the return time for the first row and the second number specifies the return time for the subsequent rows. The default value is -1, which indicates an infinite wait time.

Security Object

For any security option, a Manager can specify one or more HTTP header names and/or cookie names as follows:

- **Cookie.** Specify each HTTP cookie name separated by a comma (,). For example:

  `cookie_name1, cookie_name2`

- **Header.** Specify each HTTP header name separated by a comma (,). For example:

  `header_name1, header_name2`

Note:

- HTTP cookie and header names must not contain commas (,) or colons (:). These are reserved delimiters.
- REMOTE_USER is a special type of HTTP header variable whose contents will not be sent to the Reporting Server. Therefore, it is not a valid HTTP header value. Instead, specify the WF_REMOTE_USER variable.

Reference: Reporting Server Node Security Options

The security options from the Client Configuration pane are explained below.

Prompt for Credentials

WebFOCUS makes an explicit connection to the Reporting Server with the user ID and password specified in the Web Security tab. This is the default value.

HTTP Basic

WebFOCUS extracts the user ID and password from the authorization header. These credentials are then used to make an explicit connection to the Reporting Server. You should only select this option when your web tier is performing Basic Authentication.

> **Note:** You can verify that the authorization header is available in by selecting *HTTP Request Info* in the *Diagnostics* tab.

Kerberos

WebFOCUS passes a Kerberos ticket for the user to the Reporting Server. This option enables an end-to-end single sign on solution from the desktop to WebFOCUS, from WebFOCUS to the Reporting Server, and from the Reporting Server to supported relational DBMS systems. To use Kerberos authentication, the Reporting Server must run in security OPSYS mode.

SAP Ticket

WebFOCUS passes the user MYSAPSSO cookie, which is created on SAP Enterprise Portal, to the Reporting Server. The Reporting Server then validates the cookie using the SAP security API. This option enables single sign on from WebFOCUS to a Reporting Server configured with the Data Adapter for SAP for environments using Open Portal Services in SAP Enterprise Portal.

Service Account

Allows you to specify a user ID and password to be used for all connections to the Reporting Server.

The service account credentials are encrypted and stored in the SECURITY keyword of the odin.cfg file. When defined, the service account overrides any other credentials that may be presented to WebFOCUS for this Reporting Server node, and all users connect to the Reporting Server using the same credentials. This approach does not make it possible to identify which user is running a given request on the Reporting Server in Managed Reporting deployments, and therefore is not recommended for them.

Trusted

Allows you to connect to the Reporting Server with only a user ID. This option is useful when no password is available for the user. Controls should be placed on the Server to ensure that connections from unauthorized clients are rejected. For example, you can employ the Reporting Server RESTRICT_TO_IP setting or configure a network firewall so that only a particular client can connect to the Server.

Note: When configuring the WebFOCUS Client to make trusted connections to the Reporting Server, you must also enable the Reporting Server to accept trusted connections.

Using the ReportCaster Console

Describes configuration options for authorized users using the ReportCaster Console.

The ReportCaster Console is the interface that provides access to the tools that administer the Distribution Server and manage schedule job logs, blackout dates, and execution Ids.

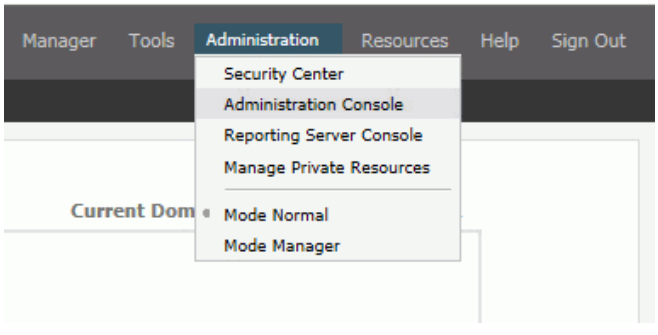
Note: Throughout this section, the ReportCaster Console will be referred to as the Console.

Using the ReportCaster Console

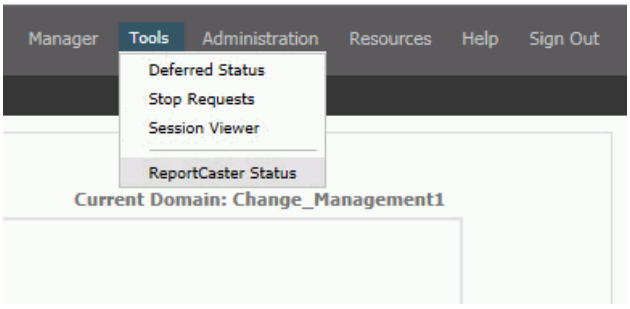
The following tools are accessible from the Console.

- Server Status
- Job Status
- Job Logs
- Blackout Periods
- Global Updates
- Purge Logs

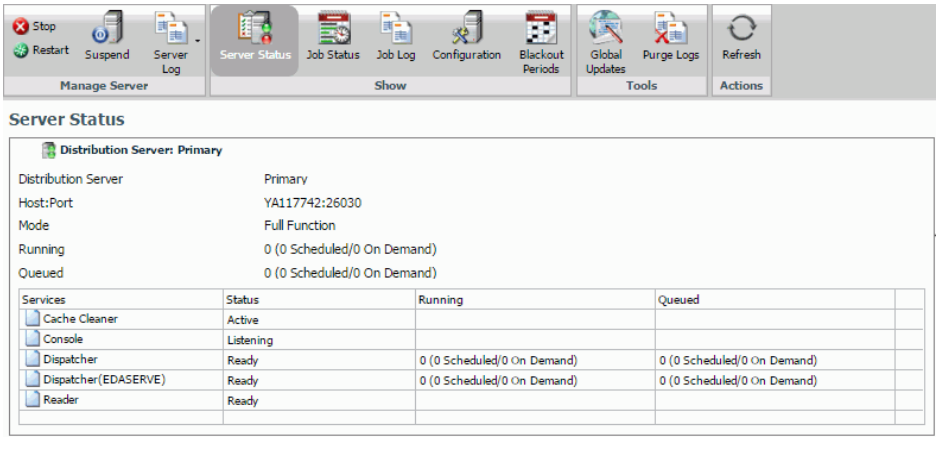
In WebFOCUS Business User Edition configurations licensed for ReportCaster, authorized users can access the ReportCaster Console through the Administration Console, from the Administration option on the menu bar, as shown in the following image.



Depending upon your privileges, these options are also available from the ReportCaster Status option on the Tools menu, as shown in the following image.

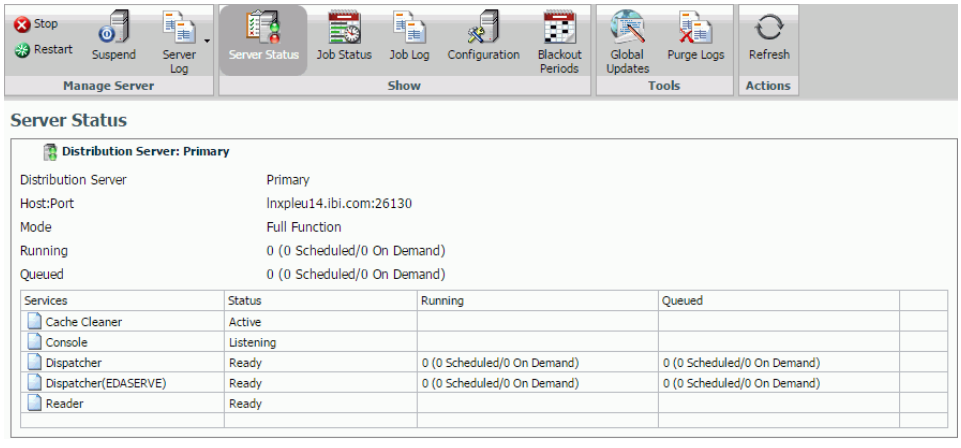


The Console intuitive ribbon displays in a new browser window, as shown in the following image. The ribbon displays a tab for each tool the user is authorized to access.



Server Status

The Server Status tool allows Managers to select a Distribution Server to restart, suspend, or stop. The tool also enables Managers to view traces or refresh data, as shown in the following image.



Viewing the Distribution Server Status

The Server Status tool, accessed by selecting the Server Status tab in the Console, enables you to view the status of the Distribution Server. The Server Status tool also provides details about the Distribution Server, such as the host name and port number, the status, and the number of jobs that are running and in the queue. The Distribution Server information includes:

- **Distribution Server.** The name used to identify the server in the Console. Primary is the name given to the server listed in the ReportCaster Configuration tool setting (*Primary Distribution Server*).

  Note: When the Distribution Server attempts to make an SMTP connection to an Email server, the connection will timeout after five minutes.

- **Host** and **Port.** The host name and port number where the Distribution Server is installed.
- **Mode.** The state and function of the Distribution Server. Options include:
  - **Full Function.** Indicates that the Distribution Server is up and functioning. When you configure ReportCaster with a secondary Distribution Server, this indicates that the server is acting as the primary Distribution Server.
  - **Down.** Indicates that the Distribution Server is stopped.

- **Running.** The number of scheduled and on demand jobs that are currently running.
- **Queued.** The number of scheduled and on demand jobs that are in the Distribution Server queue.
- **Services.** The services currently running on the Distribution Server. Options include:
  - **Cache Cleaner.** The Distribution Server uses this service to refresh the IBFS Cache. The frequency at which the cache is refreshed is controlled by the setting IBI_Repository_Sync_Interval in the Administration Console.
  - **Console.** The Distribution Server uses this service to listen for communication from the ReportCaster application or API.
  - **Dispatcher.** The Distribution Server uses this service to execute scheduled jobs.

    Note: Depending on your server configuration, you may have one or more additional Dispatchers listed in the Server Status Dialog box.
  - **Reader.** The Distribution Server uses this service to poll the Repository.
- **Status.** The status of each service currently running on the Distribution Server. Options include:
  - **Ready.** The service is available.
  - **Standing By.** The service is standing by.
  - **Suspend.** The service is suspended.
  - **Listening.** The Console service is actively listening.
  - **Polling.** The Reader service is active.
  - **Monitoring.** The Repository Monitor is active.
  - **Waiting.** Displayed when a job in the running queue is waiting for a connection to the reporting server. Occurs when a multi-task schedule is started because a connection is available to the reporting server in the first task but then waits because a connection is not available to the reporting server in the second task.

From the Server Status interface, you can perform the following tasks:

- **Refresh.** Retrieves the most current information and refreshes the Distribution Server status with this information.
- **Restart.** Recycles the Distribution Server and the Application Server.

- **Suspend.** This option is always available. Suspends the Distribution Server services, but the server remains running. When you suspend a server, the Suspend button label will change to Resume.
- **Stop.** Brings the Distribution Server completely down.

> **Note:** When you stop the Distribution Server using this option, you must restart it from the machine where it resides. You cannot restart the Distribution Server remotely.

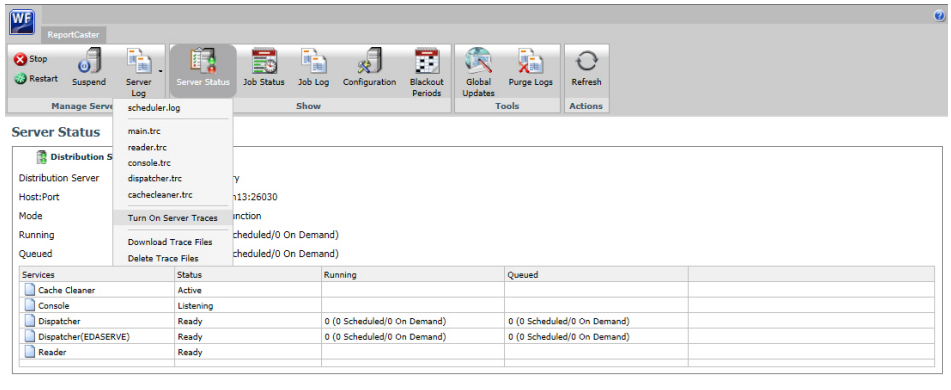
- **View Trace.** Allows you to view trace information for the scheduler.log, main.trc, reader.trc, console.trc, and dispatcher.trc files. You can also turn the Distribution Server traces on or off. For more information, see *How to Turn Distribution Server Traces On or Off* on page 41.

> **Note:** Distribution Server traces are tracked separately from Job traces using this functionality. You do not need to turn on job traces to see distribution server traces.

- **Help.** Opens the Console Server Status online documentation.

Procedure: How to Turn Distribution Server Traces On or Off

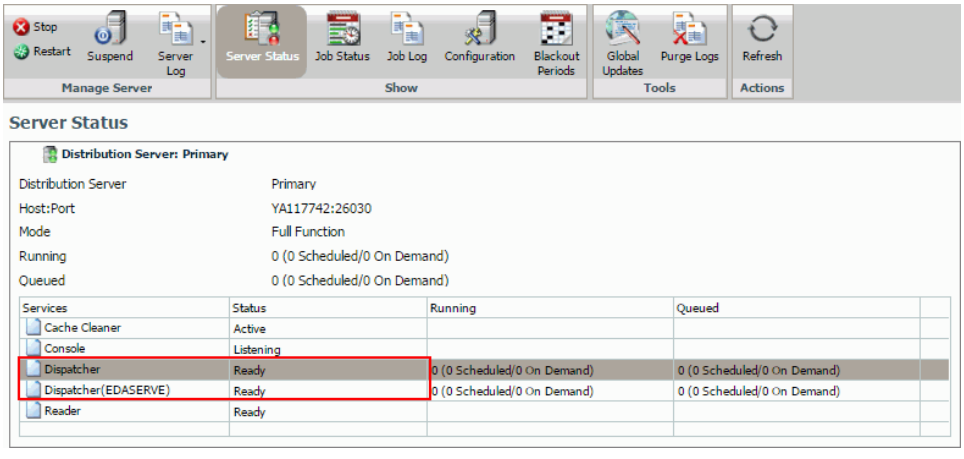
1. From the ReportCaster Console, select *Server Status*.
2. From the Distribution Server list, select a server.
3. On the toolbar, click the down arrow on the Server Log button.
4. Click *Turn On Server Traces* to turn the Distribution Server traces on, as shown in the following image.



To disable the Distribution Server traces, follow steps 1 and 2, and then hover over Turn On Server Traces and click *Turn Off Server Traces*.

Separate Job Queues for Each Data Server

The Distribution Server has separate job queues for each Reporting Server, as well as an additional queue for tasks that do not require a Reporting Server, as shown in the following image. Therefore, there will always be at least one job thread available for each Reporting Server, in addition to at least one thread for non-server based jobs. No one Reporting Server can have all of the available job threads consumed by jobs associated with that server.



Viewing, Stopping, Suspending, and Restarting the Distribution Server

The Server Status interface enables you to stop and restart the Distribution Server, as follows:

- To stop the Distribution Server, click the *Stop* button. A window opens, asking you to confirm that you want to stop the server. Click *Yes*.

  Note: When you stop the Distribution Server using this option, the Server Status Restart option cannot be used to restart the Distribution Server. To start the Distribution Server, log on to the machine on which the Distribution Server is installed.

- To suspend the Distribution Server, click the *Suspend* button. A window opens, asking you to confirm that you want to suspend the server. Click *Yes*.

- To restart the Distribution Server, click the *Restart* button. A window opens, asking you to confirm that you want to restart the server. Click *Yes*.

  When you restart the server, the Distribution Server and the ReportCaster Application are restarted.

- To obtain the most current information about the Distribution Server, click *Refresh*.

Procedure: How to Restart a Server

1. Select a server that is running.
2. From the toolbar, click *Restart* to restart the server.

   A window opens, asking you to confirm that you want to restart the server.
3. Click *Yes*.

Procedure: How to Suspend and Resume a Server

1. Select the server in Full Function mode.
2. On the toolbar, click *Suspend*.

   A window opens, asking you to confirm that you want to suspend the server.
3. Click *Yes*.

   The reader service is suspended and the toolbar button changes to *Resume*.

   To resume polling the repository for schedules, click *Resume*. Click *Yes* to confirm.

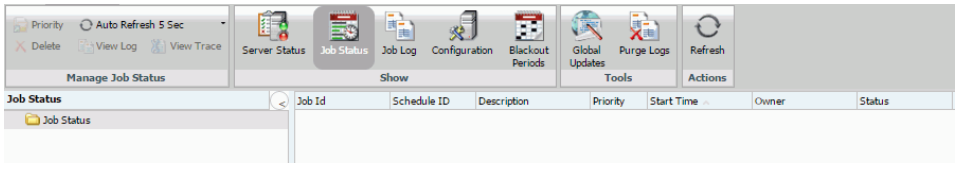
Procedure: How to Stop a Server

1. Select a running server and click *Stop*.

   A window opens, asking you to confirm that you want to stop the server.
2. Click *Yes*.

Job Status

Another resource for tracking schedules is the schedule job status. The schedule status provides a list of scheduled jobs that are in the Distribution Server queue. Status information includes the Schedule ID, the time it started running, and the status of the job.



The schedule information includes:

- **Job Id.** The ID assigned to the job.
- **Schedule ID.** A unique ReportCaster generated key assigned to the job when it was scheduled.

- **Description.** The description provided when the schedule was created.
- **Priority.** The priority level of the schedule. 1 is the highest and 4 is the lowest priority.
- **Start Time.** The time that the schedule run began.
- **Owner.** The name of the user who owns the schedule.
- **Status.** The status of the scheduled job. It contains one of the following values:
  - **Running.** The scheduled job is currently running.
  - **Queue.** The scheduled job is waiting for a thread to become available to run the request.
  - **Server Name.** The Reporting Server to which the job has been submitted.

Job Log

The Job Log tab enables you to view the logs of executed jobs belonging to you or to users whose job logs you are authorized to see. You can view log and trace information, open job logs, delete job logs, refresh job logs, or access related help for job logs on the Job Log tab. You can also view log and trace information for the daily and on-demand Log Purge jobs. The Log Purge log can be accessed from the system folder. The logs for other jobs can be accessed under the folder of the user to whom the job belongs.

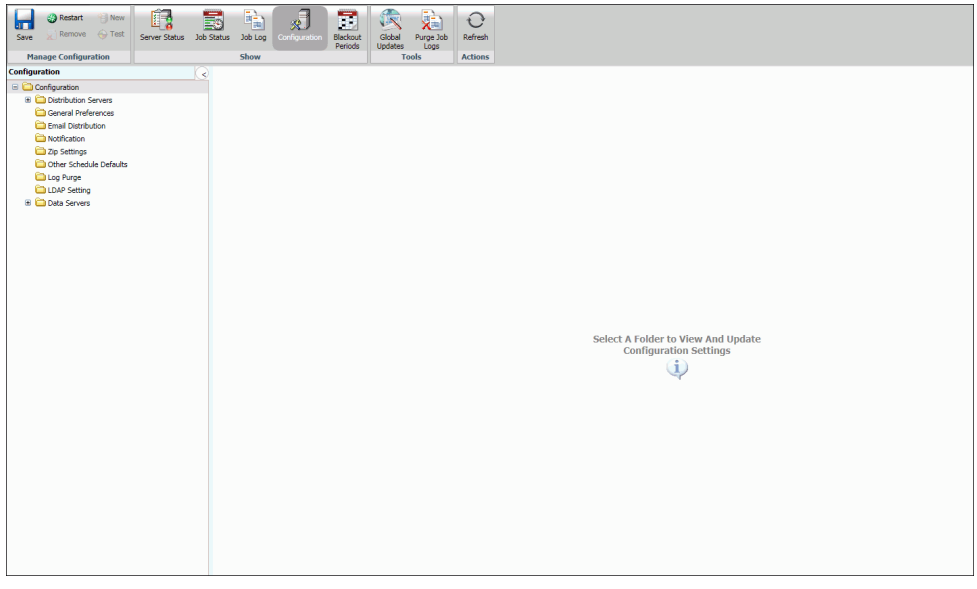
Note: The Job Log tab supports the functionality of a multiple selection, whereby you can open or delete multiple files simultaneously.

The job logs information includes:

- **Job Id.** The ID assigned to the job.
- **Start Time.** The time that the schedule was run.
- **Job Duration(seconds).** The amount of time needed to complete a job.
- **Job Status.** The status of the job when it completed processing.
  - **Success.** No errors occurred during the scheduled job processing.
  - **Error.** One or more errors occurred during the scheduled job processing. No report was generated or distributed.
  - **Warning.** One or more warnings occurred during the scheduled job processing. A report was generated and distributed.

ReportCaster Configuration

The Configuration tool enables Managers to view and manage the configuration of the Distribution Server, Servlet (deployed in WebFOCUS Business User Edition web application) interfaces and tools. Options that Managers can modify include Distribution Servers, Repository Settings, General Preferences, Email Distribution, Notification, and other options, as shown in the following image.



Configuration Icons

In the Configuration tab on the ReportCaster Console ribbon, a series of icons enable you to perform the following tasks.

> **Note:** When you select *Configuration* in the ReportCaster Console ribbon, the Manage Configuration group displays on the left-hand side. Clicking *Server Status*, *Job Status*, *Job Log*, or *Blackout Periods* will change the name and functionality of this group, depending where you are in the interface. These options all appear in the Show group of the ribbon.

- **Manage Configuration group**
  - **Save.** Saves any changes made to the configuration. You will receive a message asking you to confirm the save. You must save the changes to the configuration settings as part of the process to implement the change. For details, see *Changing Configuration Settings* on page 47

- **New.** Creates a new Reporting Server. This option is only active when working in the Data Servers folder.
- **Remove.** Deletes a Reporting Server from the ReportCaster configuration. You will receive a message asking you to confirm the deletion. This option is only active when working in the Data Servers folder.
- **Test.** Tests the connection to the selected server or repository. This option is only active when working in the Data Servers, Repository Settings, and LDAP Settings folders. You may be prompted for a user ID and password to connect to a specified server. You will receive a message describing whether the test succeeded or failed.
- **Restart.** Restarts the Distribution Server and ReportCaster to implement changes to the server configuration. You can also select *Restart* from the Action menu. For more information, see *Changing Configuration Settings* on page 47.

- **Tools group**
  - **Global Updates.** Authorized users can make global updates in the Global Updates interface for the Mail Server, Printer, Email Address, Email from, and Data Server values stored in schedules and distribution lists.
  - **Purge Logs.** Provides on-demand capability for purging logs. You can also specify a number of days (past) for which to purge logs. For example, if you want to purge logs for the past month, you would use the default number of days, which is 30. You can also specify an option for traces: Default Traces, No Traces, or Trace On. For more information, see *How to Purge Logs on Demand* on page 110.
- **Actions group**
  - **Refresh.** Refreshes the settings to reflect the last saved configuration settings.
- **Help.** Opens the online Help file. This option is only available when accessing the configuration tool through the ReportCaster web application. It is not available when accessing the tool from the Windows Programs menu or by running editit.bat or the UNIX editit script file from the /utilities directory within the ReportCaster Distribution Server installation.

Configuration Tab Folders

The Configuration tab provides access to configuration settings through the following folders:

- **Distribution Servers.** Defines and configures the Distribution Server.

- **General Preferences.** Specifies which Address Book access types, distribution formats, and methods will be available to a user creating a schedule. In this folder, you can also specify whether schedule group blackout dates can be defined, and if ReportCaster scheduling options will include the ability to distribute a PDF file directly to a printer. For details on these settings, see *General Preferences* on page 53.
- **Email Distribution.** Configures email settings, such as the default email host, number of attempts to distribute to an email host, and security information. For details on these settings, see *Email Distribution* on page 58.
- **Notification.** Configures notification settings, such as the notification email host and default notification type. For details on these settings, see *Notification* on page 63.
- **Zip Settings.** Provides settings to configure how Zip files will be created and named. For details on these settings, see *Zip Settings* on page 67.
- **Other Schedule Defaults.** Defines the default end date and time of a ReportCaster schedule. For details on these settings, see *Other Schedule Defaults* on page 69.
- **Log Purge.** Allows you to specify the time and period that log files will be automatically purged. For details on these settings, see *Log Purge* on page 70.
- **LDAP Setting.** Allows you to configure ReportCaster self-service users to be authenticated and authorized against an LDAP data source rather than the WebFOCUS Business User Edition Repository. You can also configure ReportCaster to retrieve email address information from an LDAP data source. For details on these settings, see *LDAP Setting* on page 71.
- **Data Servers.** Allows you to configure multiple Reporting Servers, including cluster servers. For details on these settings, see *Data Servers Settings* on page 73.

Changing Configuration Settings

To implement changes to the ReportCaster server configuration settings, you must save the changes, and then restart the Distribution Server and the ReportCaster web application. Use the following steps to save any configuration changes.

1. After you make changes to any of the configuration settings within a Configuration folder, click the *Save* icon in the Manage Configuration group toolbar.

   A window opens, asking you to confirm the save.

2. Click *OK*.

   A window opens, explaining that you must restart the Distribution Server and the ReportCaster Web Application in order for the changes that you saved to take effect.

3. Click *OK*.

4. Click the *Restart* icon in the Manage Configuration toolbar.

   A window opens, asking you to confirm that you want to stop all running jobs and restart.

5. Click *Yes*.

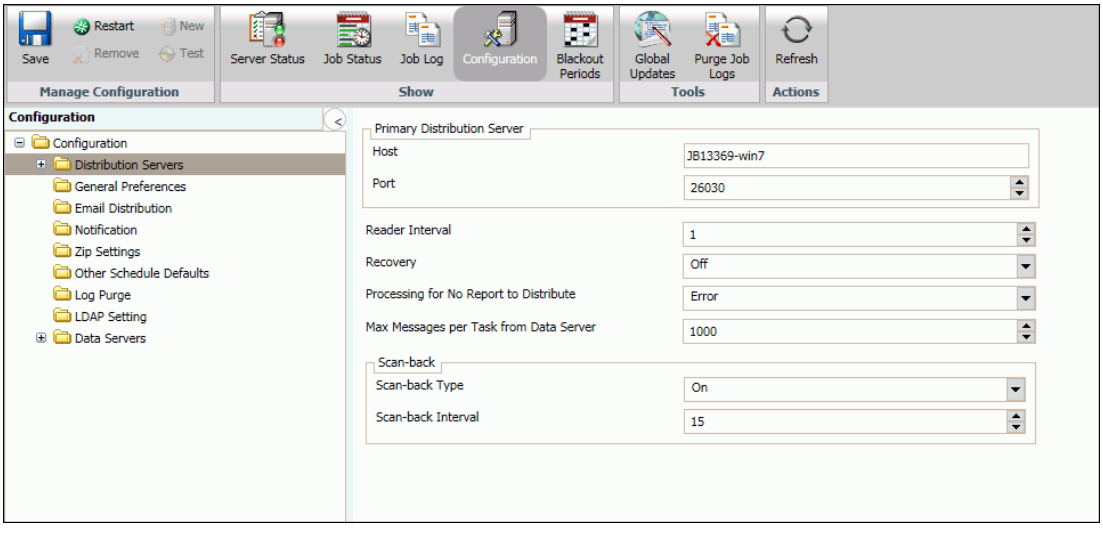
6. Notify all users that are currently logged that they must restart their sessions to obtain the new configuration information. This is required because user sessions have information cached pertaining to the ReportCaster configuration. The user interfaces must be restarted to obtain any updated configuration information.

Changing Default User IDs

Several of the Configuration tab folders provide the option to change the default user ID and/or password. To change a default user ID settings, click the icon that appears to the right of the setting field. This opens the User dialog box, where you can type a new user ID and password. When your changes are complete, click *OK* to exit the User dialog box. Remember to save your changes and restart the Distribution Server to implement any changes.

Distribution Server Settings

The Distribution Servers folder, shown in the following image, contains the settings that define and configure the Distribution Server. The Server Status option, located on the ribbon, provides the ability to restart the Distribution Server, suspend distribution, stop distribution, switch servers, and refresh data. For more information, see *Server Status* on page 39.



The Distribution Servers folder contains the following configuration settings.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Primary Distribution Server section		
Host	Required.	Host name of the primary Distribution Server.
Port	Required.	Port number of the primary Distribution Server.
Reader Interval	Required. Default value is 1 minute.	Polling interval (in minutes) for the ReportCaster Distribution Server to check for scheduled jobs. An acceptable value is any positive integer from 1 to 999999. Negative numbers and zero are not allowed. **Note:** This setting is also available in the Administration Console.
Recovery	Default value is OFF.	**On.** During startup, the ReportCaster Distribution Server recovers scheduled jobs that were processed but not completed. **Off (Default).** During startup, the ReportCaster Distribution Server does not recover any scheduled jobs. **Note:** This setting is also available in the Administration Console.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Processing for No Report to Distribute	Required. Default value is Error.	Specifies whether the *No Report to Distribute* message from the WebFOCUS Reporting Server is categorized as an error or a warning. This is a global setting, relevant to all schedules. Possible values are: ❑ **Error.** The *No Report to Distribute* message is categorized as an error and the message is written to the ReportCaster log report in red. When the schedule has the Notification option set to Error, the Notification is sent. ❑ **Warning.** The *No Report to Distribute* message is categorized as a warning and the message is written to the log report (in orange) as an informational message. When the schedule has the Notification option set to Warning, no error notification is sent. These settings also apply to burst reports when there is a *No Report to Distribute* message for an individual burst value.
Max Messages per Task from Data Server	Required. Default value is 1000	Controls the number of messages for each task from the Data Server written to the ReportCaster log file.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Scan-back section		

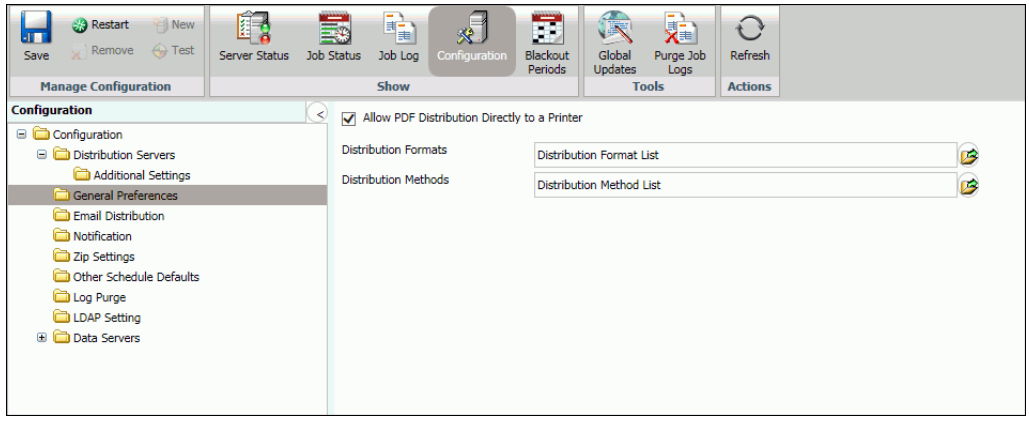
Setting	Optional or Required/Default Value	Descriptions and Possible Values
Scan-back Type	Required. Default value is On.	Possible values are: ❑ On ❑ Off ❑ Reset Next Run Time
Scan-back Interval	Default value is 15, 24 hour periods.	If the Distribution Server is unavailable for a period of time, this is the number of 24 hour periods (beginning with the Distribution Server restart time) that you want the Distribution Server to scan for jobs not yet run and run them. **Note:** This setting is also available in the Administration Console.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Additional Settings folder		
SSL Certificate section		
The Console Requires Secure SSL Connection	Optional	Select this check box to encrypt the communication between the ReportCaster application and the ReportCaster Distribution Server. After enabling secure communication and saving the changes, you must manually restart the ReportCaster application and the ReportCaster Distribution Server.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
SSL Certificate	Required if The Console Requires Secure SSL Connection check box is selected.	A default SSL Certificate is supplied by the installation procedure. You can optionally replace the default certificate with your own certificate to activate secure communication.
Schedule Job Traces	Default value is Off.	
Hold Repository Connection	By default, this option is selected.	**Selected.** The database connection is kept open throughout the execution of the schedule, including obtaining Address Book information and writing information to the log files. **Not selected.** The database connection is dropped before executing the schedule. A new connection is made after the schedule is executed to obtain Address Book information and write information to the log files.

General Preferences

The General Preferences folder in the Configuration tab, as shown in the following image, contains settings that determine which distribution formats and methods will be available to a user.



The General Preferences folder contains the following configuration settings.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Allow PDF Distribution Directly to a Printer	Required. By default, this option is selected.	When selected, PDF is a selectable format for the Printer distribution method. This enables a PDF file to be distributed directly to a printer. The printer must have the appropriate driver to print PDF files.
Distribution Formats	Optional. All formats are enabled, by default.	Specifies what report and graph formats are available to users.
Distribution Methods	Optional. All distribution methods are enabled, by default.	Specifies what distribution methods are available to users.

Specifying Schedule Format Settings

The Distribution Formats setting in the General Preferences folder enables users to specify what report and graph formats are available to users and groups.

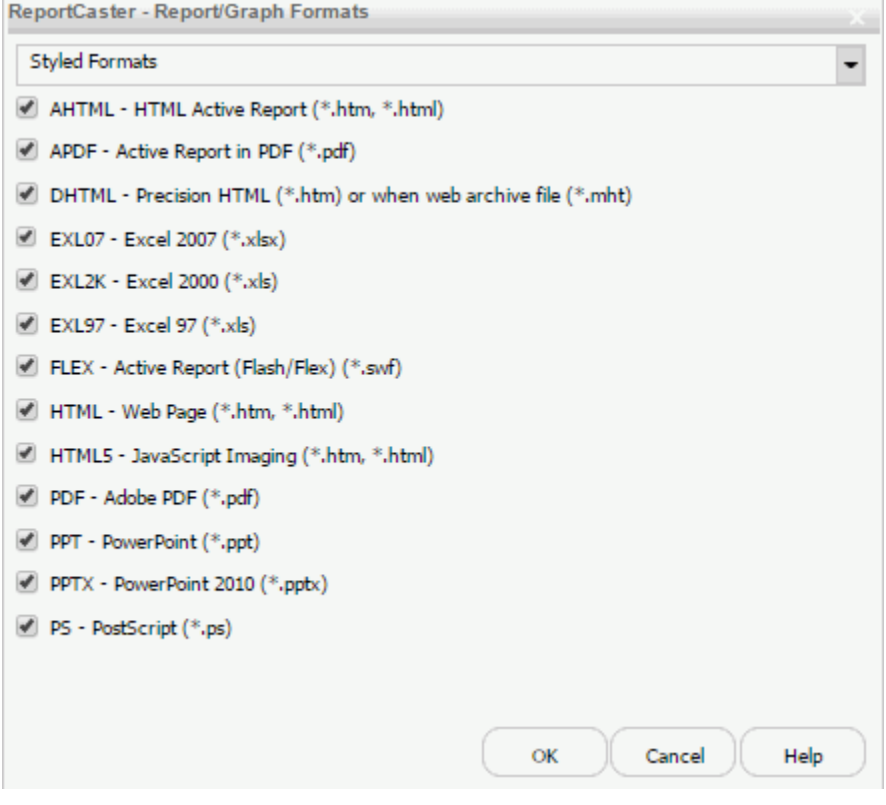
This setting only applies to WebFOCUS (Repository) procedures. By default, all report and graph formats are enabled (selected). A minimum of one report or graph format must be selected.

Note: If a Format is cleared after a schedule using that Format has been created, the schedule will fail when it is run. A message in the log will indicate how to fix the problem.

Procedure: How to Specify Schedule Format Settings

1. In the General Preferences folder, click the icon to the right of the *Distribution Formats* field.

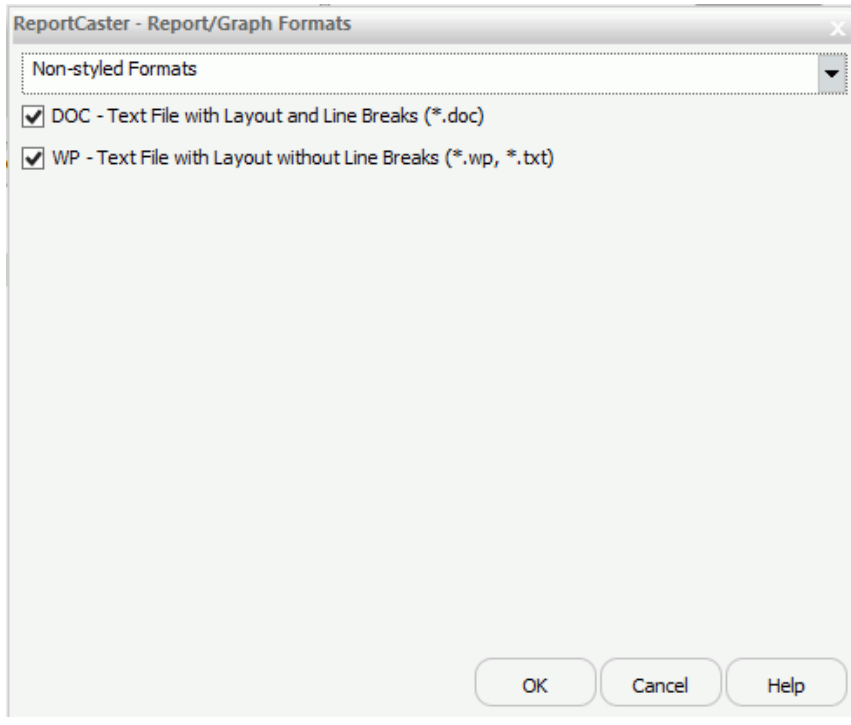
   The ReportCaster - Report/Graph Formats dialog box opens, as shown in the following image.



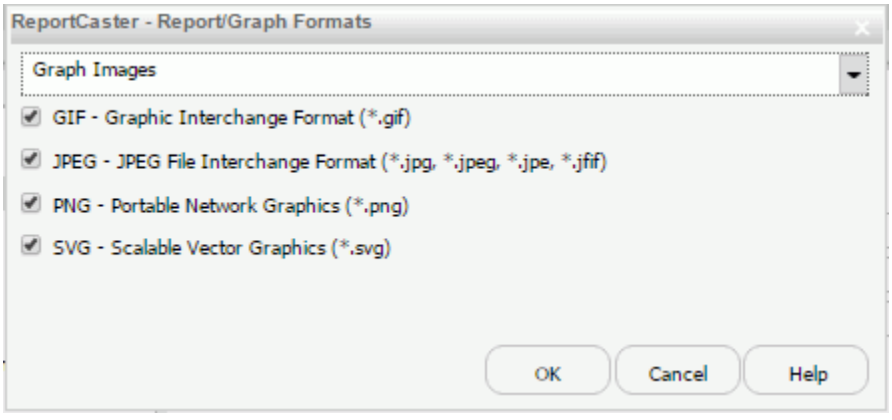
2. Using the Styled Formats drop-down list, you can select *Specialized Formats*, *Non-styled Formats*, or *Graph Images*. Optionally, you can keep the default, *Styled Formats*.

   By default, *Styled Formats* are displayed with each format type selected.

3. To enable or disable styled formats, select or clear the check box for one of the listed formats.
4. To enable or disable Non-styled Formats, which do not support styling using WebFOCUS StyleSheet commands, select *Non-styled Formats* from the drop-down list. By default, the Non-styled Formats are displayed with each format type enabled, as shown in the following image.



5. To enable or disable graph images, which are created by a WebFOCUS BUE graph request, select *Graph Images* from the drop-down list. By default, the graph image formats are displayed with each format type enabled, as shown in the following image.



6. When your selections are complete in the Report/Graph Formats dialog box, click *OK*.

   The changes are saved and the Report/Graph Formats dialog box closes.

7. To implement the configuration changes, restart the Distribution Server and WebFOCUS BUE web application.

Specifying Schedule Distribution Method Settings

The Distribution Methods setting, in the General Preferences folder, enables authorized users to specify the distribution methods that are available to users and groups. If a method is cleared after a schedule using that method has been created, and *Only run schedules for selected Distribution Method* is selected, the schedule processing will not run the scheduled tasks. A message in the log will indicate that the distribution method is not configured for use. In addition, a schedule that has multiple distributions will not run if one of the distribution methods is cleared in the Distribution Methods drop-down menu, in the General Preferences folder, of the Configuration tab.

By default, all distribution methods are enabled (selected).

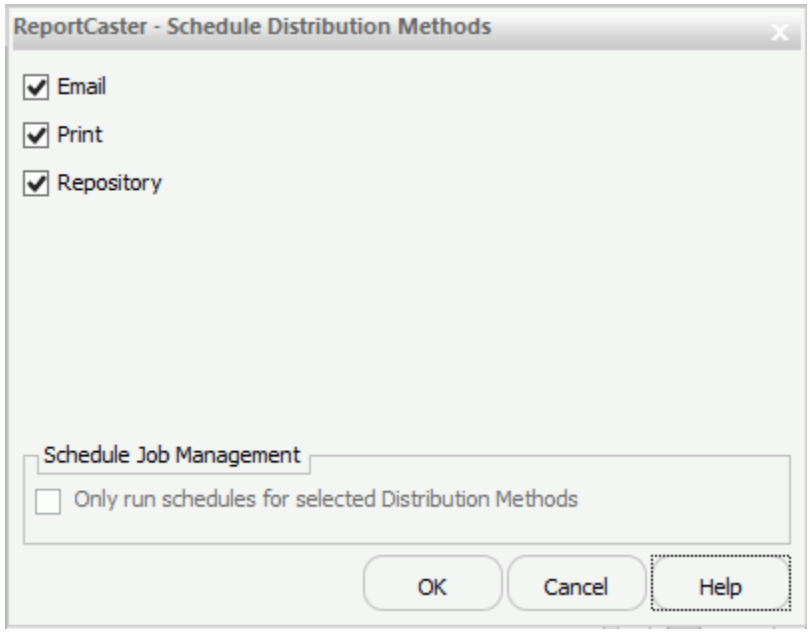
Note: A minimum of one distribution method must be selected.

The Repository option only appears if these products are enabled. Repository is an optional product component that is installed with the WebFOCUS BUE Client.

Procedure: How to Specify Schedule Distribution Method Settings

1. In the General Preferences folder, click the icon to the right of the *Distribution Methods* field.

   The ReportCaster - Schedule Distribution Methods dialog box opens, as shown in the following image.



2. To enable or disable specific distribution methods, select or clear the check box for one of the listed options.

   Note: At least one schedule distribution method must be selected.

3. Optionally, select the *Only run schedules for selected Distribution Methods* check box to limit the schedules running to those that have at least one of the Distribution Methods selected.

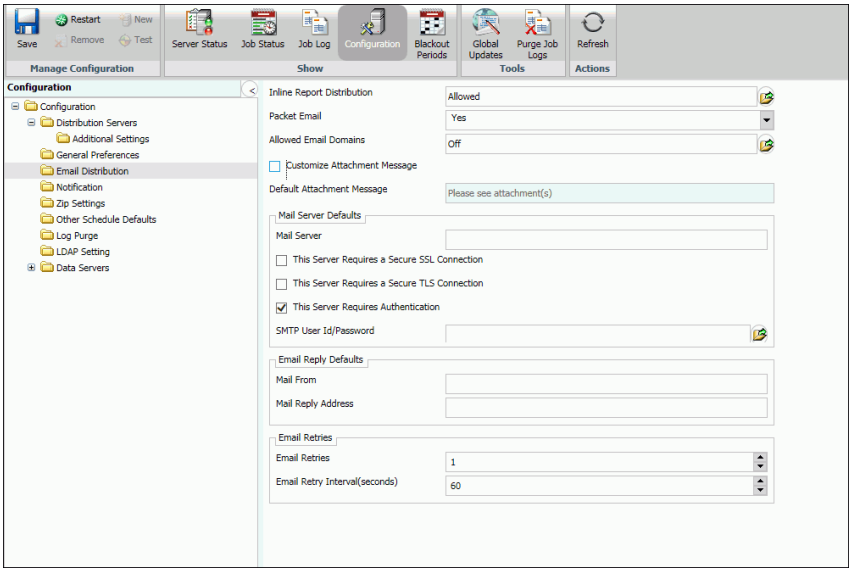
4. When your selections are complete in the Schedule Distribution Methods dialog box, click *OK*.

   The changes are saved and the Schedule Distribution Methods dialog box closes.

5. To implement the configuration changes, restart the Distribution Server and WebFOCUS BUE web application.

Email Distribution

The Email Distribution folder in the Configuration tab contains default email settings, email retry options, and email security. The Email Distribution window is shown in the following image.



The Email Distribution and Notification folder contains the following configuration settings.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Inline Report Distribution	Required. The default value is Allowed.	Specifies whether the Schedule tool will enable the email distribution option to send a report in the body of the email (inline). **Note:** If this option is cleared after a schedule using this option has been created, the schedule will fail when it is run. A message in the log will indicate how to fix the problem.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Packet Email	Required. The default value is Yes.	Controls how task output and burst content are distributed through email. Valid values are: ❑ **No.** Each burst value or task output is distributed in a separate email. ❑ **Yes.** People receiving burst values or output from tasks will receive a single email with multiple attachments. ❑ **Burst.** Each burst value in a distribution list will generate a separate email for a given email address. There may be one or more attachments in the email, depending on the number of tasks in the schedule.
Allowed Email Domains	The default value is Off.	Contains the email domains that are authorized in a distribution. **Note:** Files containing email addresses intended for distribution are also verified for valid domains at schedule execution time. If it contains a restricted address, then no delivery is made to that address and an error message is written to the log file.
Customize Attachment Message	Optional	Provides the ability to specify a custom message.
Default Attachment Message	Required.	Defines the default message used in your Email Distribution. The message that you define here displays in the Basic Scheduling Tool.

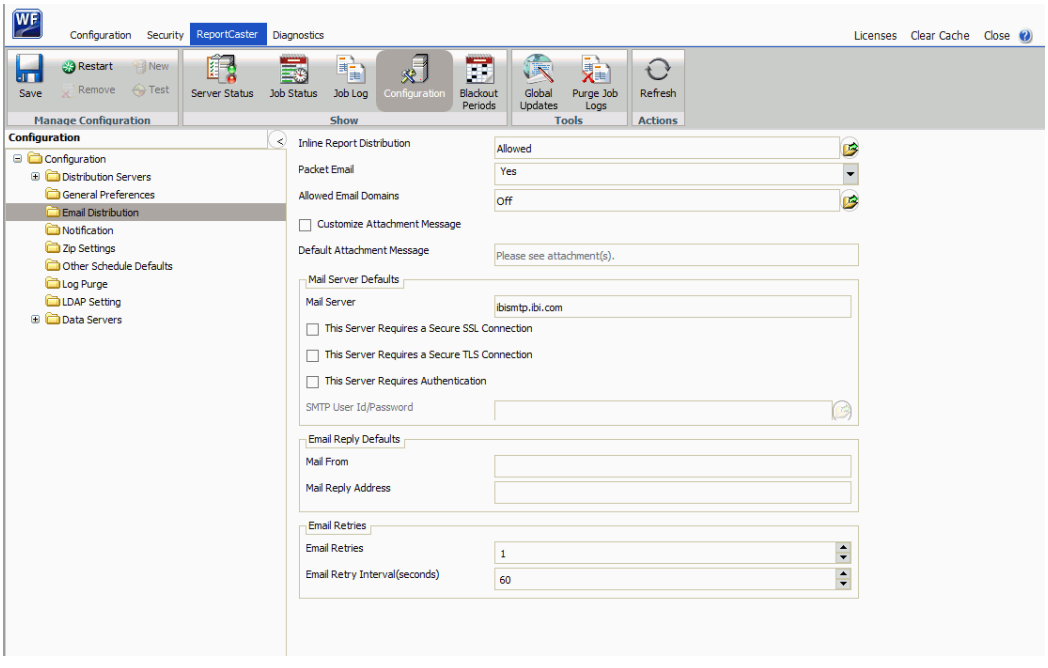
Setting	Optional or Required/Default Value	Descriptions and Possible Values
Mail Server Defaults section		
Mail Server	Required.	Name of the default mail server used to distribute an email schedule. You can also specify a port for Mail Host using *hostname*:*port*. If you do not specify a port or the port you specify is not present, the default port is used.
This Server Requires a Secure SSL Connection	Optional.	Select this check box if the specified mail server uses SSL.
This Server Requires a Secure TLS Connection	Optional.	Select this check box if the specified mail server uses TLS.
This Server Requires Authentication	Optional.	Select this check box if the specified mail server requires authentication with a user ID and password.
SMTP User Id/Password	Required if the mailhost is using SMTP Authorization. No default value.	User ID and password used to connect to the mailhost.
Email Reply Defaults section		
Mail From	Optional.	Default value for the email From field. This can be any value.
Mail Reply Address	Optional.	Default email reply address when creating an email schedule.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Email Retries section		
Email Retries	The default value is 1.	Number of times the Distribution server will try to connect to the email server to deliver report output. If the Distribution server is unable to connect to the email server on the first try, it will attempt to connect again after the specified Email Retry Interval has passed. A message for each attempt is written to the log file. Valid values are 0 through 9.
Email Retry Interval(seconds)	The default value is 60 seconds.	Amount of time that the Distribution server will wait between retries. Valid values are 1 through 999.

Procedure: **How to Configure Email Distribution**

1. From the ReportCaster Tools menu, click *ReportCaster Status*.
2. Click the *Configuration* button, as shown in the following image.

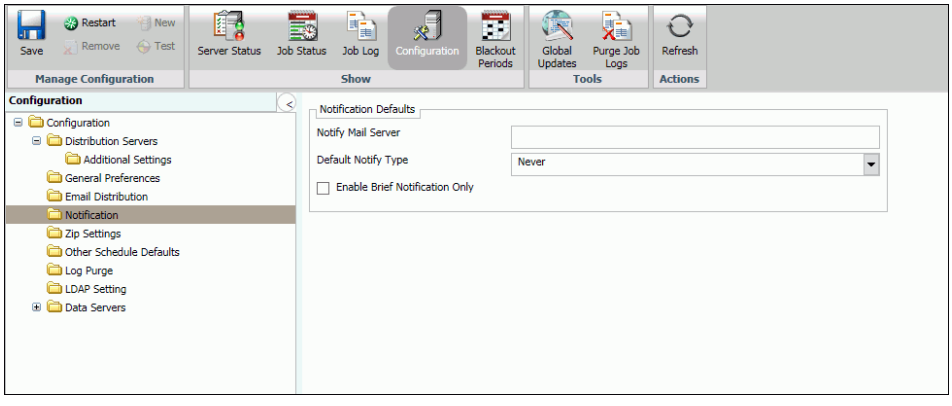
Note: Authorized users can also access the ReportCaster Configuration tool from the Administration Console.



3. In the left pane, select the *Email Distribution* folder.
4. Populate the email distribution fields. You can:
   - Make changes to the current email settings. For more information, refer to the preceding table.
   - Supply any default values that you would like to be available at schedule creation time.
5. If your mail server(s) require authentication or SSL or TLS, check the appropriate boxes and enter the required credentials. For more information, see the *Installation* topic in the Information Center.
6. Click *Save.*

Notification

The Notification folder in the Configuration tab contains default notification settings. The Notification window is shown in the following image.



The Notification folder contains the following configuration settings.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Notification Defaults section		

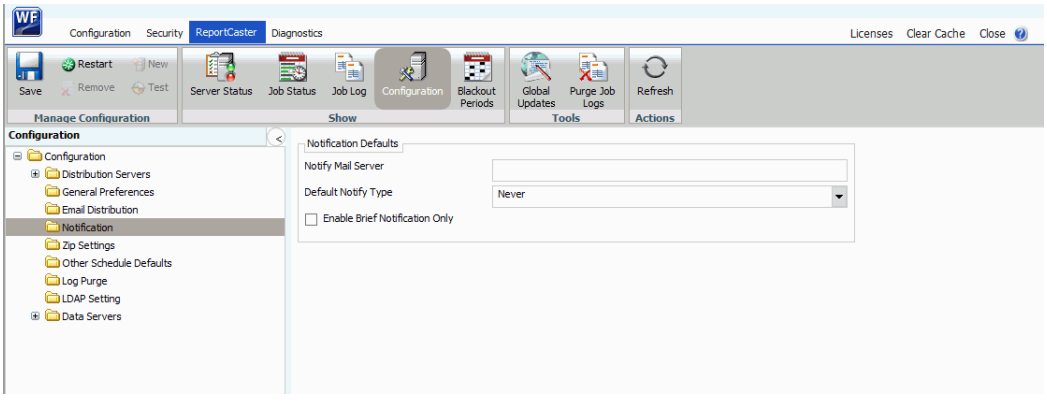
Setting	Optional or Required/Default Value	Descriptions and Possible Values
Notify Mail Server	Optional.	Name of the mail server that distributes the notification email. If blank, ReportCaster uses the Mailhost setting as the notification mail server. **Tip:** Information Builders recommends using different mail servers for notification and email distribution. This way, if there is a problem with your Mailhost, notification will still be sent. Having separate mail servers ensures that you will be informed when the default mail server falters. You can also specify a port for the Notify Mailhost using *hostname*:*port*. If you do not specify a port or the port you specify is not present, the default port is used.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Default Notify Type	The default value is Never.	Specifies whether to send notification of the schedule status to a specified email address. Possible values are: ❑ **Never.** This is the default value. ReportCaster does not send notification of the schedule status under any circumstance. ❑ **On Error.** The specified users are notified when errors are encountered while running the schedule. Information Builders recommends using the On Error notification option. ❑ **Always.** The specified user is always notified when the schedule runs. **Note:** This setting is also available in the Administration Console.
Enable Brief Notification Only	Optional.	Controls whether Full Notification is available as a scheduling option. When this check box is selected, you can only select the Brief Notification option when you schedule a report. Full Notification is not available. **Note:** Messages are displayed in the log when Full Notification is disabled. If a schedule is created before Full Notification is disabled, when the schedule executes, a Brief Notification will be sent, and a warning will be displayed in the schedule log.

Procedure: How to Configure Notification

1. From the ReportCaster Tools menu, click *ReportCaster Status*.
2. Click the *Configuration* button, as shown in the following image.

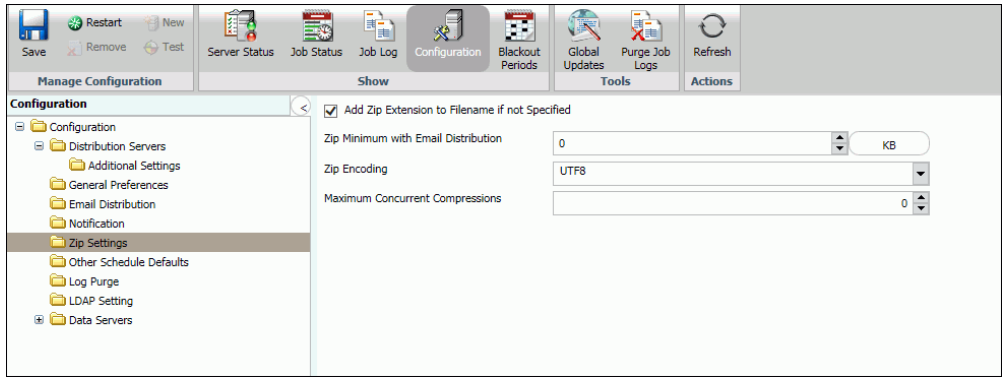
> **Note:** Authorized users can also access the ReportCaster Configuration tool from the Administration Console.



3. In the left pane, select the *Notification* folder.
4. Populate the notification fields. You can:
   - Make changes to the current notification settings. For more information, refer to the preceding table.
   - Supply any default values that you would like to be available at schedule creation time.
5. Click *Save*.

Zip Settings

The Zip Settings folder in the Configuration tab, as shown in the following image, contains settings for adding an extension to a distributed Zip file, the Zip encryption to use for distribution.



The Zip Settings folder contains the following configuration settings.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Add Zip Extension to Filename if Not Specified	Required. By default, this option is selected.	Controls whether or not the .zip file extension will be automatically appended to the Zip file name entered by the user in a schedule distributed by email or FTP. Select this option if you want to automatically append .zip to the entered file name. Do not select this option if you want to use the file name as entered by the user and not have .zip automatically appended to the file name.
Zip Minimum with Email Distribution	Required. The default size is in KB and set to 0.	Select either MB or KB and customize the size of your file using the up and down arrows.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Zip Encoding	Optional.	Specifies an encoding other than the default encoding of the ReportCaster Distribution Server platform. The encoding specified must match the encoding used by WinZip or any other Zip utility installed on the Distribution Server. **Note:** This setting is also available in the Administration Console.
Maximum Concurrent Compressions	Optional The default value is zero (0).	The total number of compression operations that the Distribution Server will perform simultaneously. If many running jobs include a compression operation (for example, zipping the output before sending), the compression operations could consume all of the available resources on the Distribution Server. You can lower this number to prevent this from occurring.

Procedure: **How to Configure Zip Settings**

1. From the ReportCaster Tools menu, click *ReportCaster Status*.
2. Click the *Configuration* button.

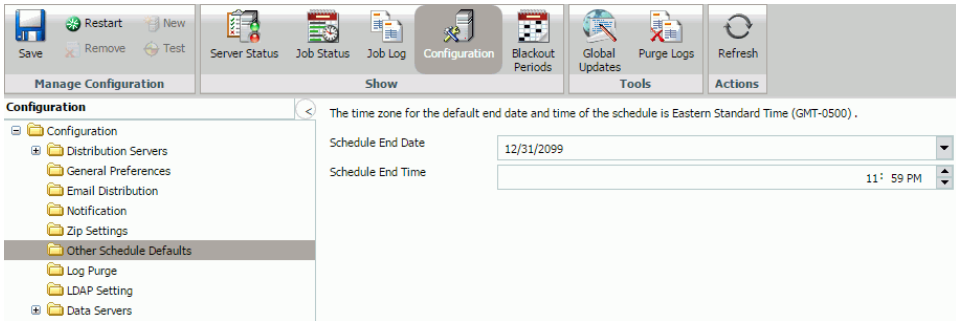
   Note: Authorized users can also access the ReportCaster Configuration tool from the Administration Console.

3. In the left pane, select the *Zip Settings* folder.
4. Populate the Zip Settings fields using the information provided in the preceding tables.
5. If you want to produce zipped output that is encrypted and password protected, you can use the Zip Encryption Password Plug-in. To use your own program to supply the password, select *Custom* from the drop-down list and enter the name of the program in the Zip Encryption Password Plug-in Name field. To use the default, select *Default*.
6. Click *Save*.

Other Schedule Defaults

The Other Schedule Defaults folder in the Configuration tab, as shown in the following image, contains settings for Schedule End Date and Schedule End Time.

Note: Depending on your time zone, the default Schedule End Date may be set to Jan 1, 2100.

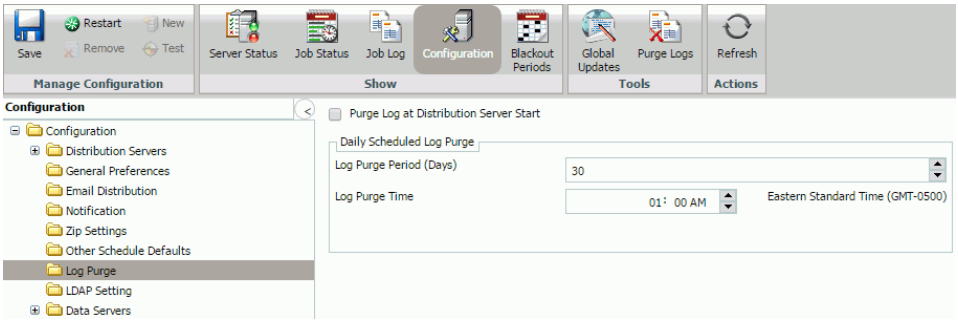


The following table lists and describes the configuration settings available in the Other Schedule Defaults folder.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Schedule End Date	Required.	Clicking the drop-down menu displays a calendar where you can select the schedule end date.
Schedule End Time	Required.	Manually, you can enter an end time for the schedule. Alternatively, use the arrows to assign a schedule end time.

Log Purge

The Log Purge folder in the Configuration tab, as shown in the following image, contains settings for purging log files, log purge periods, and log purge times.



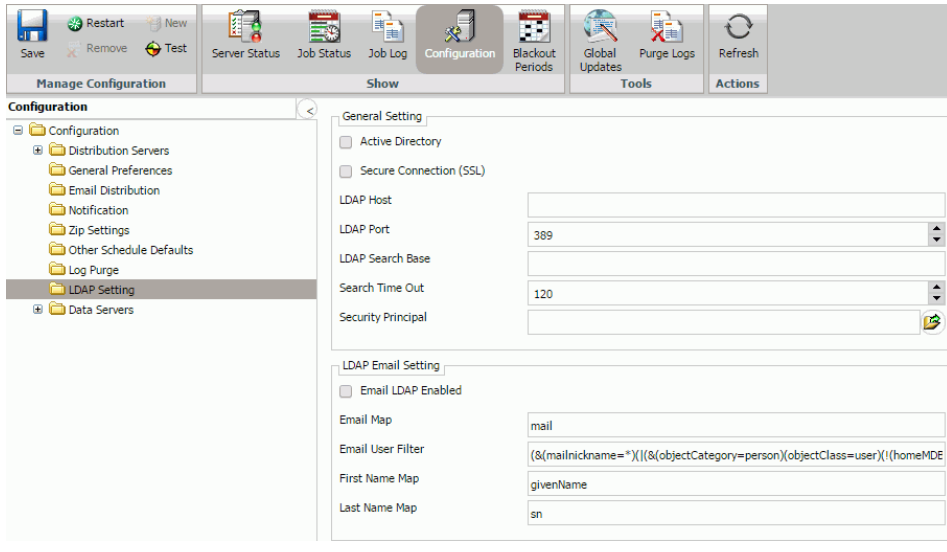
The Log Purge folder contains the following configuration settings.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Purge Log at Distribution Server Start	Optional. By default, the check box is unchecked.	When selected, log reports are automatically purged each time the Distribution Server starts. This is in addition to the scheduled log purging that is set using the Log Purge Period and Log Purge Time options.
Daily Scheduled Log Purge section		
Log Purge Period (Days)	Optional.	Automatically purges individual log reports when they are older than a set number of days. **Note:** This setting is also available in the Administration Console.
Log Purge Time	Optional.	Time at which log purging occurs. **Note:** This setting is also available in the Administration Console.

LDAP Setting

ReportCaster can be configured to retrieve email address information from an LDAP data source. The leading mail server software vendors use LDAP for storage of email information. This includes Active Directory on Windows platforms.

The LDAP Setting folder in the Configuration tab, as shown in the following image, contains settings to define LDAP server connection and security, as well as LDAP email settings.



The LDAP Settings folder contains the following configuration settings.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
General Setting section		
Active Directory	By default, this option is not selected.	Select if you are using the Active Directory technology for LDAP. Do not select if you are using any other technology for LDAP.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Secure Connection (SSL)	By default, this option is not selected.	Indicates whether or not SSL (Secure Sockets Layer) is used to communicate with the LDAP server.
LDAP Host	There is no default value.	Host name or IP address of your LDAP directory server.
LDAP Port	Default value is 389.	Port on which the directory server listens.
LDAP Search Base	There is no default value.	Filter for LDAP searches. Only the subtree below the search base is available for LDAP queries. For example, dc=ibi, dc=com.
Search Time Out	Default value is 120.	Time, in seconds, that ReportCaster can search an LDAP data source before timing out.
Security Principal	No default value.	Service account of the user performing authentication. The user must have sufficient access rights to locate user entries in the directory. Select the icon to the right of this option to open the User dialog box, where you can type a user name and password.
LDAP Email Setting section		
Email LDAP Enabled	By default, this option is not selected.	Indicates whether ReportCaster is enabled to retrieve email address information from an LDAP data source.
Email Map	Default value is mail.	Attribute type for email entries.

Setting	Optional or Required/Default Value	Descriptions and Possible Values

Email User Filter	Default value provided is dependent on the LDAP Type selected.	Filter for email entries to be retrieved. For example:
		`(& (mailnickname=*)`
		`(|(&(objectCategory=person)`
		`(objectClass=user)(!(homeMDB=*))`
		`(!(msExchHomeServerName=*)))`
		`(&(objectCategory=person)`
		`(objectClass=user)(|(homeMDB=*)`
		`(msExchHomeServerName=*)))`
		`(&(objectCategory=person)`
		`(objectClass=contact))`
		`(objectCategory=group)`
		`(objectCategory=publicFolder)))`

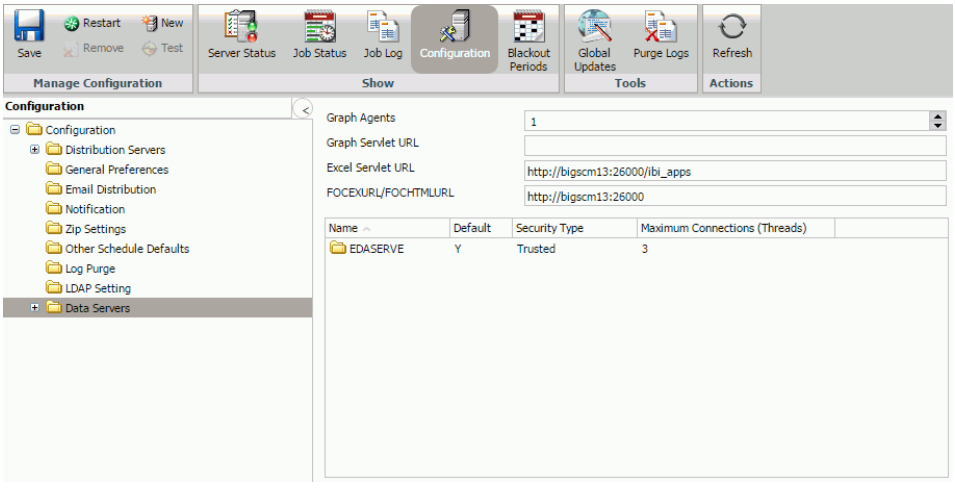
First Name Map	Default value is givenName.	Attribute for first name entries.
Last Name Map	Default value is sn.	Attribute for last name entries.

Data Servers Settings

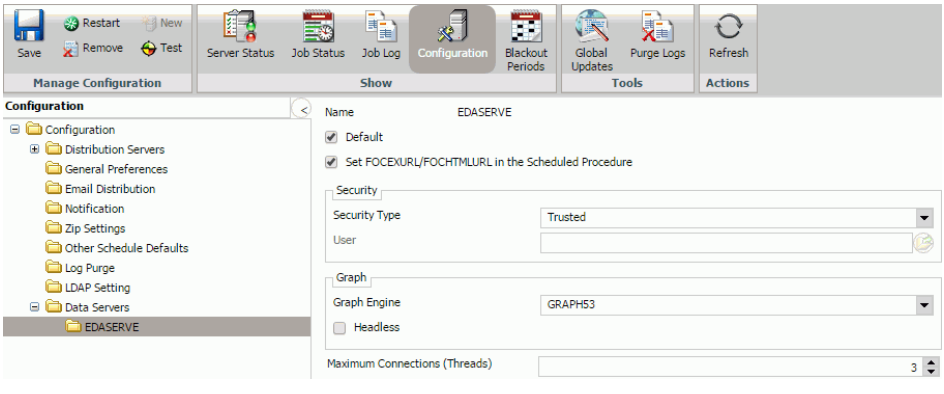
The Data Servers folder in the Configuration tab contains settings to configure the Reporting Servers associated with ReportCaster. Using the configuration settings in this folder, you can also configure multiple Reporting Servers with ReportCaster.

Note: Data Server connection information is stored in the WebFOCUS BUE Client, and not in ReportCaster. ReportCaster runs scheduled procedures through the WebFOCUS BUE Client which is installed with the Distribution Server. When a ReportCaster job is executed by the WebFOCUS BUE Client, the alternate deferred server is used if an alternate deferred server is defined.

The following image shows the display in the right panel when the Data Servers folder is selected. Initially, the default data server appears in this panel with information, such as the data server name, URL (used to connect to the Reporting Server), the type of server, whether or not it is the default server, and what security type it is using. When you add a data server that ReportCaster can access, it will appear in this list.



The following image shows the configuration settings when you select a specific data server under the Data Servers folder (in this example, EDASERVE).



The Data Servers folder contains the following configuration settings.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Settings for the Data Servers folder:		
Graph Agents	The default value is 1.	Optimizes the processing of graphs. Due to performance considerations, Information Builders generally recommends configuring this setting to 1 Graph Agent for each concurrent graph report. However, your own internal testing should determine the Graph Agent value that best suits the business needs of your organization.
Graph Servlet URL	Optional. There is no default.	Overrides the default graph server setting and configures graph image files to be created on the Application Server. Type the following value `http://hostname/context_root/IBIGraphServlet` where: *`hostname`* Is the host name of the Application Server where the WebFOCUS BUE Client is installed. *`context_root`* Is the site-customized context root for the WebFOCUS BUE web application deployed on your Application Server. ibi_apps is the default value. This setting is available for WebFOCUS BUE Server and WebFOCUS BUE procedures. This setting should not be used when web server security is enabled. This includes Basic authentication, IWA, SSL, and third-party security products (such as SiteMinder). In these cases, the web server security settings can prevent WebFOCUS BUE from creating the graph.

Setting	Optional or Required/Default Value	Descriptions and Possible Values

Excel Servlet URL	Default value is
	`http://localhost:8080/ibi_apps`
		Specifies the application server to be used to zip the file components that comprise an EXCEL® 2007 file (.xlsx) as follows:
		`&URL_PROTOCOL://servername/alias/IBIEXCELSERVURL`
		where:
		`URL_Protocol`
		Is HTTP.
		`servername`
		Is the name of the application server where the WebFOCUS BUE Client is installed.
		`alias`
		Is the context root of the WebFOCUS BUE application. The default is ibi_apps.
		This setting is available for WebFOCUS BUE Server and WebFOCUS BUE procedures. This setting should not be used when web server security is enabled. This includes Basic authentication, IWA, SSL, and third-party security products (such as SiteMinder). In these cases, the web server security settings can prevent WebFOCUS BUE from creating the Excel 2007/2010 file.

FOCEXURL/FOCHTMLURL	Default value is `http://localhost:8080`	Specifies the host name and port of the FOCEXURL/FOCHTMLURL.
Settings for an individual Data Server:		
Name	Required.	Name of the selected Data Server. **Note:** Data Server names are case-sensitive. Data Servers are defined in the WebFOCUS BUE Client as uppercase so you should also define Data Servers as uppercase in ReportCaster.
Default	Required.	This option is selected by default.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Set FOCEXURL/ FOCHTMLURL in the scheduled procedure	Required.	This setting is selected, by default. If this setting is not selected, the Distribution Server will not set the value of FOCEXURL or FOCHTMLURL for a scheduled procedure. Therefore, when cleared, if FOCEXURL or FOCHTMLURL is already set in the edasprof.prf file, this setting remains in effect, unless it is overridden in the scheduled procedure.
Security section		
Security Type	By default, this option is set to User.	**Static.** A valid Execution Id and password is supplied in the User setting. When creating a schedule, you cannot specify an Execution Id and password. **User.** A valid Execution Id and password must be specified when creating a schedule. **Shared.** When creating a schedule, the user ID and password is internally assigned as the Execution Id and password. **Note:** Since the actual password is not stored in the WebFOCUS BUE repository, the Shared configuration can only be used when a password is not required to connect to the Reporting Server. **Trusted.** The Execution Id is the schedule owner and no password is sent to the WebFOCUS BUE Reporting Server when schedules run. **Note:** The Reporting Server must be a configured to accept a Trusted connection when the Trusted option is selected.
Graph section		
Graph Engine	Required. The value is GRAPH53.	Controls which graph engine to use for server-side graphics. By default, this specifies the GRAPH53 setting.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Headless	By default, this option is not selected.	Determines whether a graphics card exists on the WebFOCUS BUE Reporting Server. When not selected (the default), a graphics card exists on the server. When selected, no graphics card exists on the server.
Maximum Connection/Threads	Required. The default connection is 3.	Maximum number of connections available to the Reporting Server. You can specify a maximum of 20 connections. This setting works in conjunction with the optional Weight setting, enabling you to prioritize the alternate servers in a cluster queue.

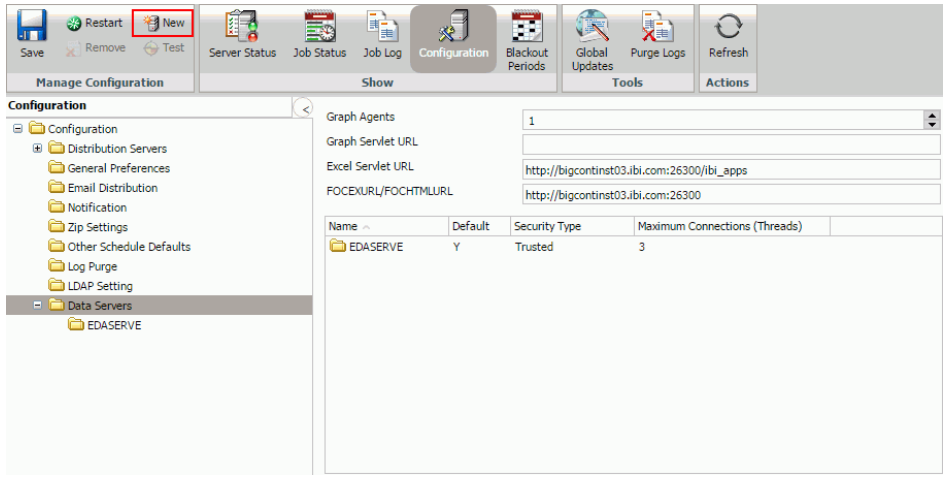
Configuring Reporting Servers With ReportCaster

You can configure multiple Reporting Servers with ReportCaster through the Data Server folder in the ReportCaster Configuration tab. Although the installation program automatically populates values for the default EDASERVE server, all additional Reporting Servers must be added to the configuration manually.

Note: If the default Reporting Server is changed on the Client, then the change will not be effective until the period specified by the IBFS Cache Cleaner service or until the Distribution Server is restarted. If the Distribution Server is installed on another machine with a separate copy of the Client, then a change to the default Reporting Server will not be effective until the same change is made on the Client installed on the same machine as the Distribution Server.

Procedure: How to Add a Reporting Server

1. In the left panel of the Configuration tab, select the *Data Servers* folder, then select *New* in the toolbar, as shown in the following image.

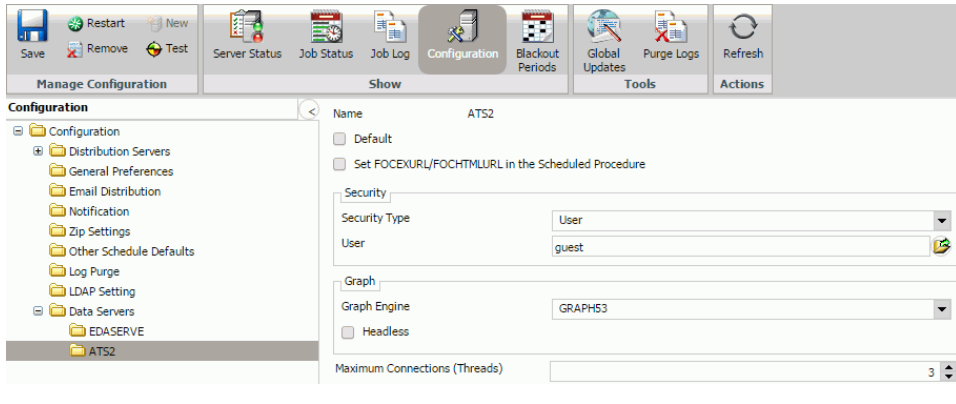


Note: The default Data Server names are SERVER, SERVER 2, SERVER 3, and so on.

2. From the Available Data Servers dialog box, select one or more Data Servers, and click *OK*. You can optionally select the Select All check box.

3. Double-click the new server node in either the Data Servers folder in the left panel or the server list in the right panel.

   The right panel displays the default properties for the selected server, as shown in the following image.



4. Provide values for the appropriate settings.

   In the Name field, verify the name of the server you want to add to the ReportCaster configuration is the same as the NODE setting for that server specified in the WebFOCUS BUE Client Server Connections configuration. You can review the WebFOCUS BUE Client Server Connections by accessing the Administration Console and selecting Reporting Servers within the Configuration tab.

   Optionally, provide values for the Security Type and Maximum Connections settings or leave the default values in place.

   You can also optionally set the Data Server being added to be the default Data Server when new schedules are created, specify not to have the FOCEXURL and FOCHTMLURL settings automatically added when scheduled jobs run, and specify that the Data Server does not have a graphics card, is Headless.

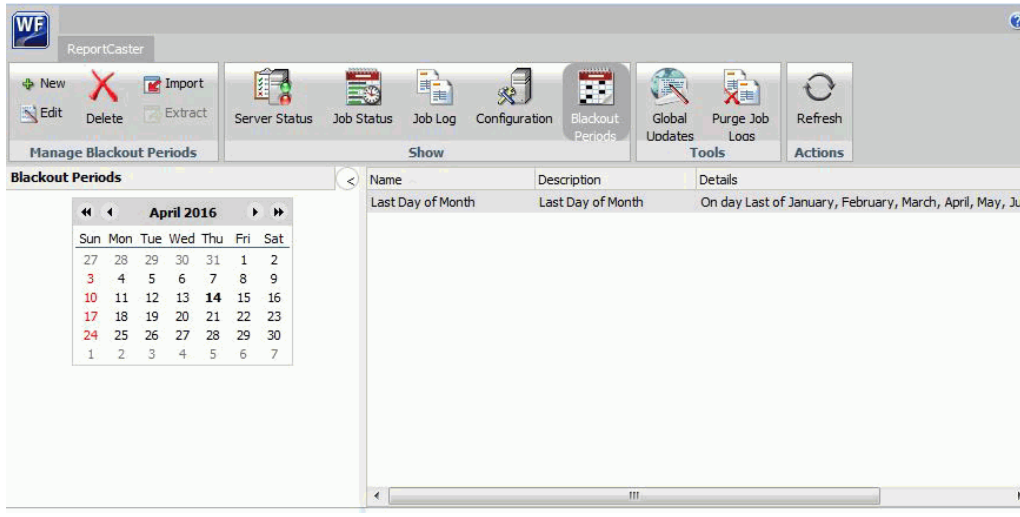
5. To implement the changes in ReportCaster, in the Configuration tab toolbar, select *Save*, then *Restart*.

Caution: Information Builders recommends that you avoid changing the name of a Reporting Server, since all existing jobs on that server will no longer run.

Using Blackout Periods

Blackout Periods are those dates and times on which schedules will not run and cannot be set to run. A user authorized to access the Blackout Periods tool can view, define, update, import, export, and delete blackout periods.

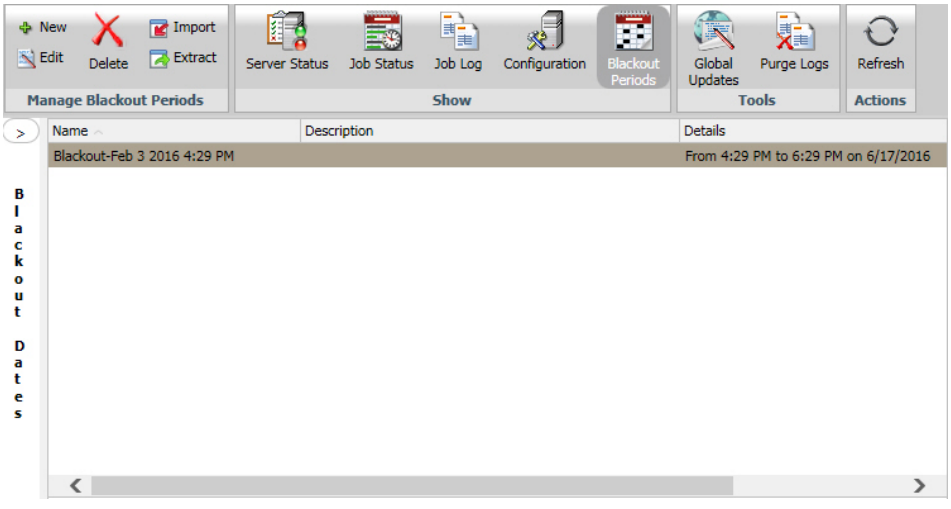
To view schedule blackout periods, select *Blackout Periods* from the Show group in the Console. The Blackout Periods interface, which is shown in the following image, provides a calendar in the left panel and the right panel lists the blackout dates you are authorized to manage.



Users authorized to manage blackout periods can add new blackout periods, delete blackout periods, replace the description of existing blackout periods, and extract existing blackout period information to a file for future use. In the ReportCaster Blackout Periods interface, these tasks can be completed using the following features:

- The Blackout Date and Time dialog box, accessed from the New and Edit buttons in the Manage Blackout Periods group.
- The Import Dates dialog box, accessed from the Manage Blackout Periods group.
- The Extract Blackout Dates dialog box, accessed from the Manage Blackout Periods group.

You can change the month or year using the arrows at the top of the calendar. Dates only appear as available or unavailable. You can show or hide the left panel by clicking the arrow in the top-right corner of the left panel. The following image shows the display with the left panel hidden.



Reference: Blackout Period Configurations

Every type of Blackout Period profile shares the same basic settings: Group Assignment, Name, Description, Details, and Blackout Time. Within that basic configuration, there are four types of Blackout Periods that accommodate differing scheduling requirements. These include:

- **Weekly Blackout Periods.** Recur on a specified day or days of the week.
- **Monthly Blackout Periods.** Recur on a specified monthly date or dates.
- **Single Day Blackout Periods.** Occur only once on a specified date.
- **Every Day Blackout Periods.** Recur at a specified time every day.

This variety of profiles enables you to build blackout periods into your reporting schedule that accommodate those regularly recurring and special one-day events that would cause you to suspend reporting.

Reference: Basic Blackout Period Settings

The Blackout Date and Time dialog box contains settings that define the timing and frequency of a scheduled Blackout Period. There are four variations of this dialog box to accommodate the Weekly, Monthly, Single Day, and Every Day frequency options.

The following table describes settings in the Global Blackout Date and Times profile.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Group	Displays the name (Global).	Displays the name (Global).
Name	Optional. By default displays the name: Blackout-[Current Date] [Current Time] For example: Blackout-Jun 26 2015 10:27 AM	A descriptive name for the Blackout Date and Time profile. You can modify the default name by clicking within the Name field.
Description	Optional.	A detailed description of the Blackout Date and Time profile.
Details Label	Assigned to the profile after creation.	A summary of the detailed times and frequency of the Blackout Period. This is a narrative description of the selections you make in the Weeks, Days, Months, and Blackout Time fields. ReportCaster creates this description automatically when you save the profile, and updates it when you save changes to it. You cannot create, edit, or delete it directly.

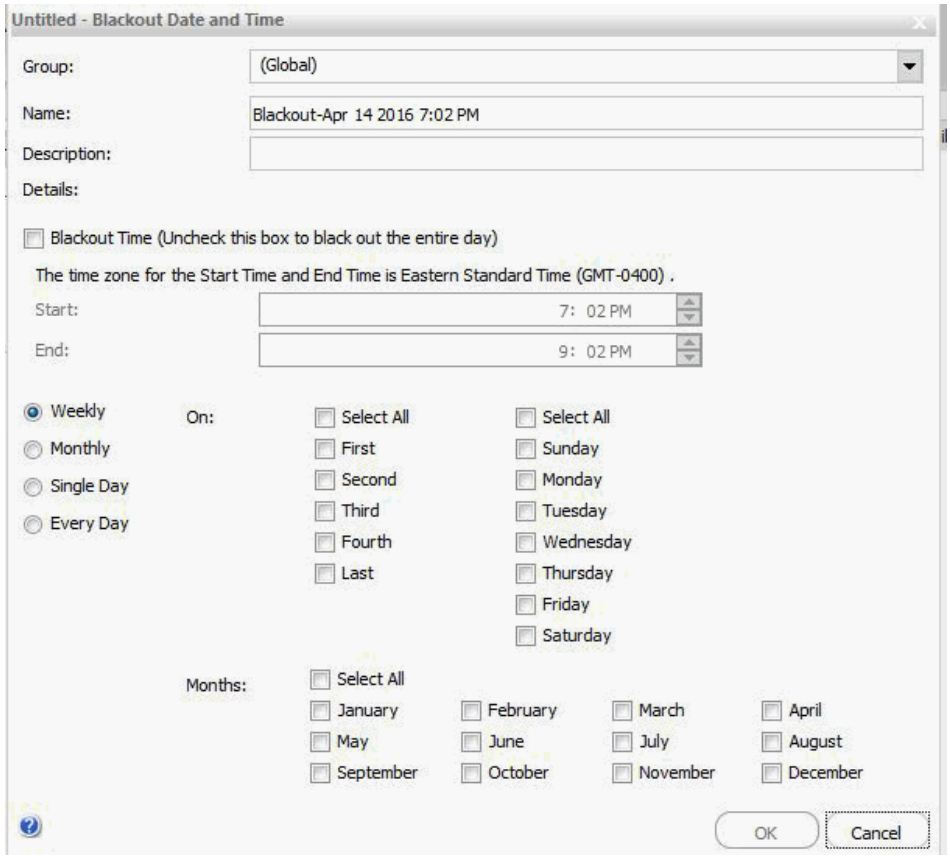
Setting	Optional or Required/Default Value	Descriptions and Possible Values
Blackout Time check box	By default this check box is cleared.	**Selected.** The Blackout Period covers the hours specified in the Start (Time) and End (Time) fields. **Not Selected.** The Blackout Period covers the entire day. **Note:** If you change a profile from Single Date to any other frequency setting, you must clear this check box if the blackout period is to cover the entire day.
Start (Time)	Optional. By default, displays the current hour and minute.	The Hour and Minute in which a Blackout Period is to begin. This value is relevant only if the Blackout Time check box is selected.
End (Time)	Optional. By default, displays the time two hours *after* the current hour and minute.	The Hour and Minute in which a Blackout Period is to end. This value is relevant only if the Blackout Time check box is selected.
Frequency	Required. By default, the Weekly option is selected.	**Weekly.** Blackout periods that recur on a specified day of the week. **Monthly.** Blackout periods that recur on a specified monthly date. **Single Day.** Blackout periods that occur once on a specified date. **Every Day.** Blackout periods that recur at a specified time every day.

Procedure: How to Configure a Blackout Period

To configure a blackout period:

1. From the Manage Blackout Periods group on the ribbon, click *New*.

   The Blackout Date and Time dialog box opens, as shown in the following image.



2. Accept the default Name assigned to the Blackout Period profile or enter a new value for Name.
3. Type a description for the Blackout Period profile in the Description field.
4. If this blackout period must cover the entire day, leave the Blackout Time check box cleared and skip to step 7.
5. If this blackout period must be limited to a range of hours within a day, select the Blackout Time check box and configure the start and end time for the Blackout Period.

For more information, see *How to Configure a Start Time and End Time for a Blackout Period* on page 94.

6. Click the appropriate frequency option:
   - **Weekly.** Establish the frequency for the blackout period. For configuration information, see *Configuring Weekly Blackout Periods* on page 86.
   - **Monthly.** Establish the frequency for the blackout period. For configuration information, see *Configuring Monthly Blackout Periods* on page 89.
   - **Single Day.** Select the date for the blackout period. For configuration information, see *Configuring Single Day Blackout Periods* on page 92.
   - **Every Day.** Establish the hours for the daily blackout period. For configuration information, see *Configuring Every Day Blackout Periods* on page 93.
7. Review your configuration.
   - If your configuration of dates and hours is unacceptable, the OK button will not respond when you attempt to click OK. Adjust your configuration and refresh the profile by clearing and reselecting the recurring check boxes.
   - If your configuration is acceptable, the OK button will be available, and the Details label will include a description summarizing your selections.
8. When your configuration is complete, click *OK*.

   An entry for the Blackout Profile appears in the right pane of the Blackout Dates window and the Blackout Date Calendar in the left pane highlights the new blackout dates.

Configuring Weekly Blackout Periods

The Weekly Blackout Period configuration bases its recurrence on a specified day of the week. It suits events that recur as part of a weekly schedule, regardless of the date on which that day falls.

Even though the name implies that this Blackout Period occurs only once a week, Blackout Periods using the weekly configuration can occur more or less frequently.

The tools in this configuration enable you to specify:

- The day, or days, of the week on which the blackout period will occur.
- The week, or weeks, of the month in which the blackout period will occur.
- The month, or months, of the year in which the blackout period will occur.

Instead of requiring you to enforce blackout periods on the same day each and every week, this flexible configuration enables you to schedule Blackout Periods that occur more than once a week. It also enables you to configure Blackout Periods that skip one or more weeks in a month or skip one or more months in a year.

Weekly Blackout Period Settings

If you select the Weekly option, the Blackout Date and Time dialog box displays a unique set of options that enables you to schedule Blackout Periods for specified days of the week.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
On Week of the Month Check Boxes (Left Column)	Required (At least one selection from this column.)	The week of the month check boxes list ordinal weeks of the month. When you select one, you define the week of the month in which this blackout period is to occur. That is, the first week of the month, the second week, and so on. You can select one or more individual weeks. The Select All check box automatically selects every week of the month, establishing a blackout period that takes place every week in a month.
On Days of the Week check boxes (Right Column)	Required (At least one selection from this column).	The day of the week check boxes list the days of the week. When you select one, you define the day of the week in which this blackout period will occur. That is, on Monday, Tuesday, and so on. You can select one or more individual days. The Select All check box automatically selects every day of the week, establishing a blackout period that takes place every day of your selected weeks in the month.

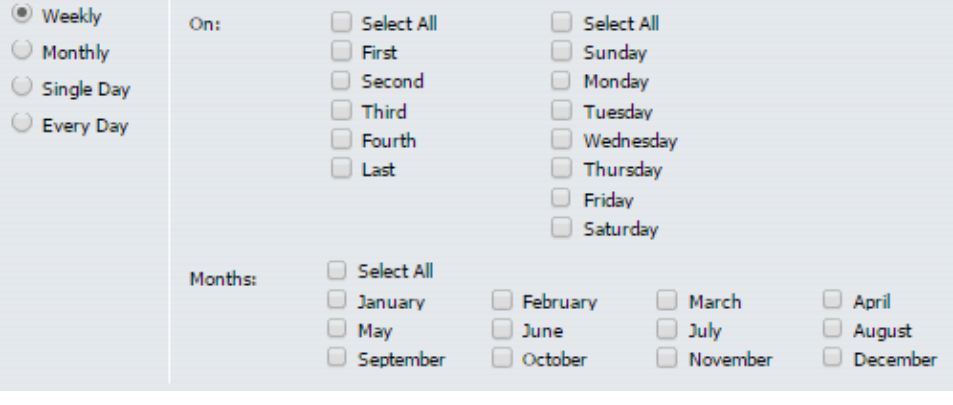
Setting	Optional or Required/Default Value	Descriptions and Possible Values
Months	Required (At least one selection from this group).	The Month check boxes list the months of the year. When you select one, you define the month of the year in which this weekly black out period will occur. That is, in January, February, and so on. You can select one or more individual months. The Select All check box automatically selects every month of the year, establishing a blackout period that takes place during every month on your selected week and day.

Procedure: **How to Configure Weekly Blackout Period Settings**

To configure weekly blackout period settings:

1. From the Blackout Date and Time dialog box, click *Weekly*.

   The dialog box displays check boxes that support the Weekly frequency schedule, as shown in the following image.



Note: In order to enable the *OK* button and save the profile, you must select at least one week, day, and month check box.

2. Select the check boxes for the week or weeks of the month in which the Blackout Period is to occur, or click *Select All* to select every week automatically.
3. Select the check boxes for the day or days of the week on which the Blackout Period is to occur, or click *Select All* to select every day of the week automatically.
4. Select the check boxes for the month or months in which the Blackout Period is to occur, or click *Select All* to select every month automatically.

Configuring Monthly Blackout Periods

The Monthly Blackout Period configuration bases its recurrence on a specified monthly date. It suits events that recur on the same date, regardless of the day of the week on which that date falls.

Even though the name implies that this Blackout Period occurs only once a month, Blackout Periods using this configuration can occur more or less frequently. They can occupy the entire day, or they can be limited to a range of hours within a single day.

The tools in this configuration enable you to specify:

- The day, or days, of the month on which the blackout period will occur.
- The month, or months, of the year in which the blackout period will occur.

Instead of requiring you to enforce blackout periods on the same day of the month, each and every month, this flexible configuration enables you to schedule Blackout Periods that occur more than once a month. It also enables you to configure Blackout Periods that skip one or more months.

Monthly Blackout Period Settings

If you select the *Monthly* option, the Blackout Date and Time dialog box displays a unique set of options that enables you to schedule Blackout Periods for specified dates of the month.

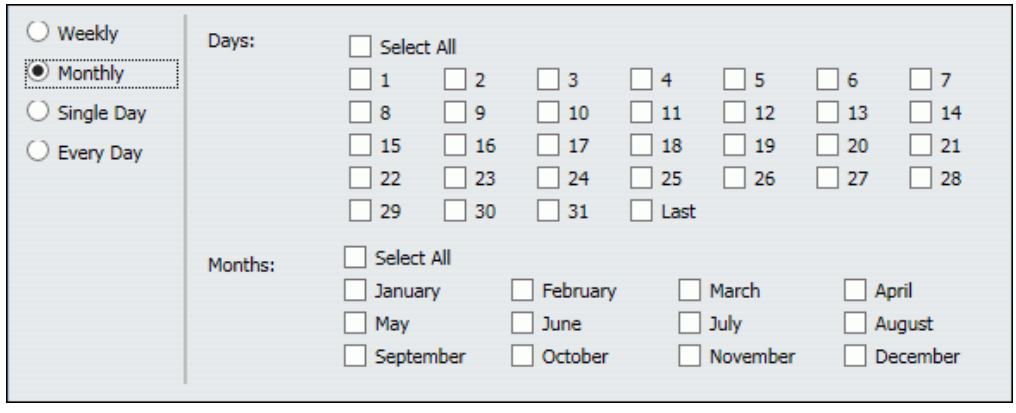
Setting	Optional or Required/Default Value	Descriptions and Possible Values
Days	Required.	The Days check boxes list the dates within a month. When you select one, you define the day of the month on which this blackout period will occur. That is, on the first day of the month, the second, the third, and so on. You can select one or more individual dates. The Select All option automatically selects every day of the month, establishing a blackout period that takes place every day during your selected months.
Months	Required.	The Months check boxes list the months of the year. When you select one, you define the month in which this black out period will occur. That is, in January, February, and so on. You can select one or more individual months. The Select All option automatically selects every month of the year, establishing a blackout period that takes place during every month on your selected day or days.

Procedure: **How to Configure Monthly Blackout Period Settings**

To configure monthly blackout period settings:

1. From the Blackout Date and Time dialog box, click *Monthly*.

The Blackout Date and Time dialog box displays the check boxes that support the Monthly frequency, as shown in the following image.

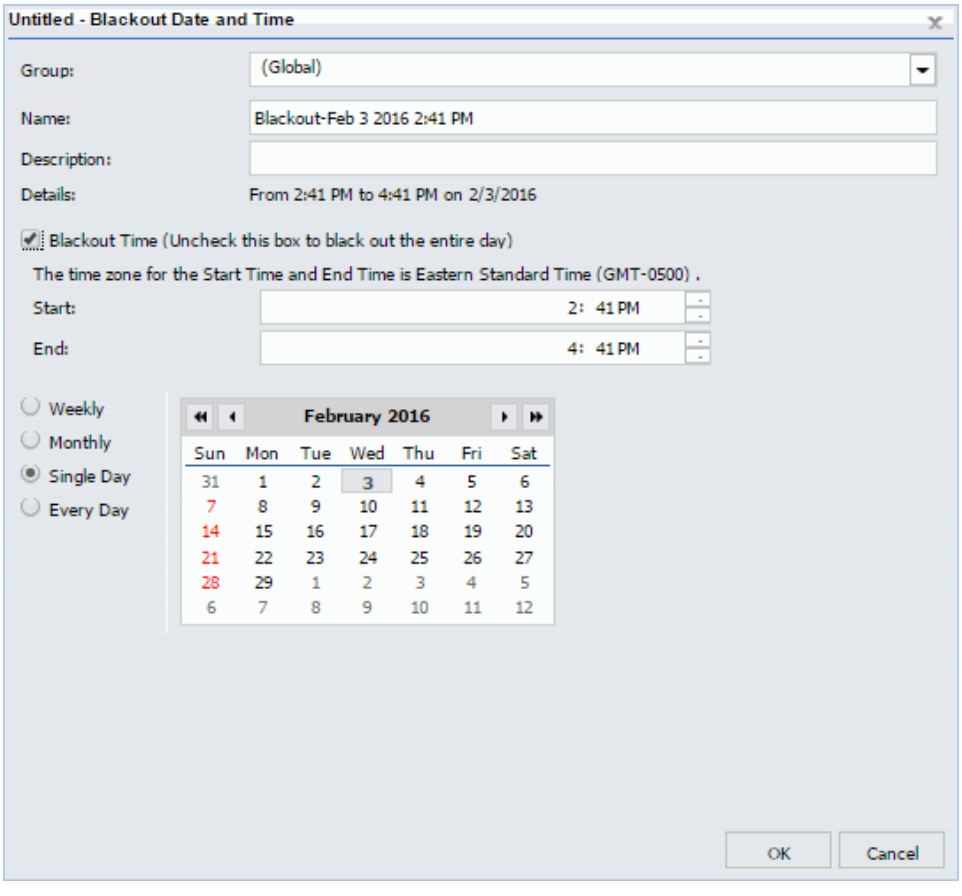


Note: At a minimum, you must select a check box for one day and a check box for one month. Until you do, the OK button will be unavailable, and you will be unable to save the profile.

2. Select the check boxes for the day or days of the month on which the Blackout Period is to occur, or click *Select All* to select every date in the month automatically.
3. Select the check boxes for the month or months in which the Blackout Period is to occur, or click *Select All* to select every month automatically.

Configuring Single Day Blackout Periods

Single Day Blackout Periods occur once, on a single, specified date. They can occupy the entire day, or they can be limited to a range of hours within a single day. The settings for Single Day Blackout Periods are shown in the following image.



Single Day Blackout Period Settings

If you select the *Single Day* option, the Blackout Date and Time dialog box displays a copy of the Blackout Dates calendar, which enables you to select a single date for a scheduled Blackout Period.

Procedure: How to Configure Single Day Blackout Period Settings

1. From the Blackout Date and Time dialog box, click *Single Day*.

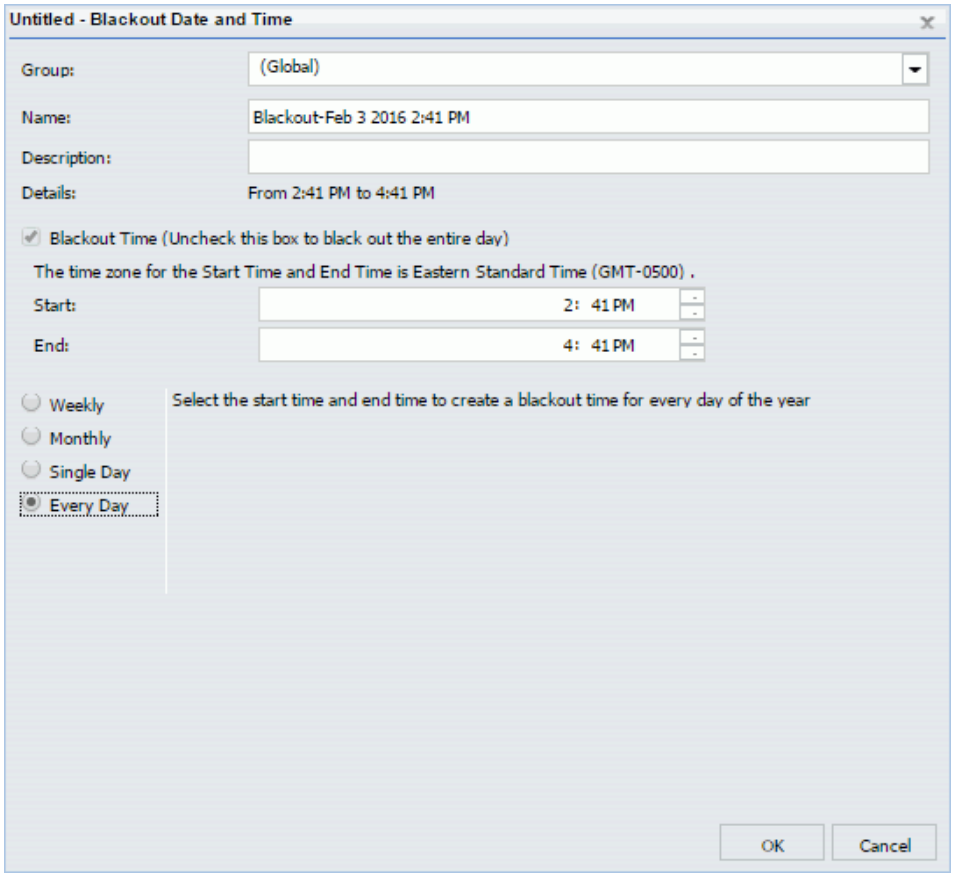
The dialog box appears, displaying the calendar automatically set to the current date.

2. Click the single arrows to change the month and click the double arrows to change the year.
3. When you have found the month and year for the scheduled single day blackout period, click on the date on which you want the Blackout Period to occur.

   The calendar highlights the new date.

Configuring Every Day Blackout Periods

Every Day Blackout Periods recur every day. To prevent Every Day Blackout Periods from blocking the release of any reports, you must limit them to a range of hours within the day. The settings for Every Day Blackout Periods are shown in the following image.



Every Day Blackout Period Settings

If you select the *Every Day* option, the Blackout Date and Time dialog box limits its display to the Beginning and End time for the Blackout Period. No other options are relevant.

Procedure: How to Configure Every Day Blackout Period Settings

1. From the Blackout Date and Time dialog box, click *Every Day*.

   The Blackout Time check box is selected automatically, and the dialog box displays a note reminding you to select the start and end time.

   The Start time is automatically set to the current time, and the End time is automatically set to a value two hours later.

2. To change the Start or End Time values, see *How to Configure a Start Time and End Time for a Blackout Period* on page 94.

Procedure: How to Configure a Start Time and End Time for a Blackout Period

From the Blackout Date and Time dialog box:

1. To change the hour of the start time, click in the *Hour* section of the Start field.

   a. Click the up or down arrow to move the value ahead one hour or back one hour, respectively.

   b. You can also type the hour in this section, but be careful to stay within the twelve hour range. If you enter a value outside of this range, the dialog box will automatically recalculate your value in terms of a twelve hour clock. For example, 44 hours would become 8. (44-(12X3))=(44-36)=8

   c. Ensure that the start time is earlier than the end time.

2. To change the minutes of the start time, click in the *Minutes* section of the Start field.

   a. Click the up or down arrow to move the value ahead one minute or back one minute, respectively.

   b. You can also type the minutes in this section, but be careful to stay within the sixty minute range. If you enter a value outside of this range, the dialog box will automatically recalculate your value in terms of the number of minutes within an hour. For example, 88 minutes would become 28. (88-60) = 28).

   c. Ensure that the start time is earlier than the end time.

3. To change the start time from AM to PM, click in the AM/PM section of the Start field.

   a. Click the up arrow to move from AM to PM.

b. Click the down arrow to move from PM to AM.

c. You can also type AM or PM directly into this section.

4. To change the hour of the end time, click in the *Hour* section of the End field.

   a. Click the up or down arrow to move the value ahead one hour or back one hour, respectively.

   b. You can also type the hour in this section, but be careful to stay within the twelve hour range. If you enter a value outside of this range, the dialog box will automatically recalculate your value in terms of a twelve hour clock. For example, 44 hours would become 8. (44-(12X3))=(44-36)=8.

   c. Ensure that the end time is later than the start time.

5. To change the minute of the end time, click in the *Minutes* section of the End field.

   a. Click the up or down arrow to move the value ahead one minute or back one minute, respectively.

   b. You can also type the minute in this section, but be careful to stay within the sixty minute range. If you enter a value outside of this range, the dialog box will automatically recalculate your value in terms of the number of minutes within an hour. For example, 88 minutes would become 28. (88-60 = 28).

   c. Ensure that the end time is later than the start time.

6. To change the end time from AM to PM, click in the *AM/PM* section of the End field.

   a. Click the up arrow to move from AM to PM.

   b. Click the down arrow to move from PM to AM.

   c. You can also type AM or PM directly into this section.

Important: You must use the right or left arrow keys to move between the Hour, Minutes, and AM/PM sections of the Start and End fields.

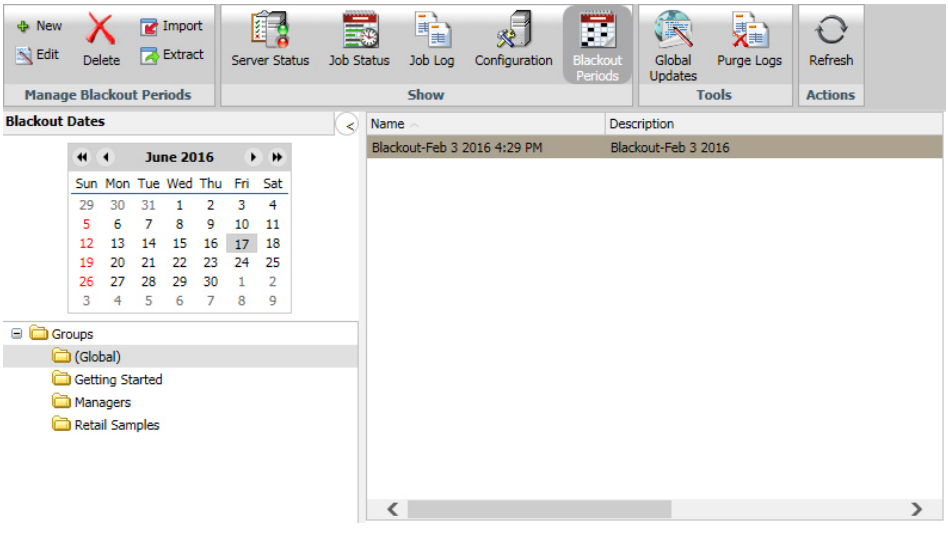
If you try to use the Tab key to move between sections, you will move down to the next option instead of across to the next section of the Start or End field.

For example, if you use the Tab key to move from the Hours section of the Start field, you will move down to the Hours section of the End field, not over to the Minutes section of the Start field. To move right, you must use the right direction key instead.

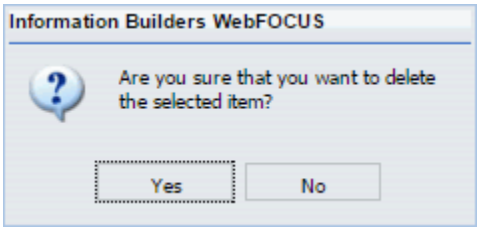
Similarly, the Shift+Tab key combination will move you to the previous option, not back to a previous section within the Start or End field. To move left, you must use the left direction key instead.

Procedure: How to Delete a Blackout Period Profile

1. In the left pane of the Blackout Dates dialog box, click the folder for the Group to which the Blackout Period profile you want to delete is assigned.
2. In the right pane, click the entry for Blackout Period profile you want to delete, as shown in the following image.



3. On the ribbon, in the Manage Blackout Periods group, click *Delete*.
4. When you receive a confirmation message, click *Yes*, as shown in the following image.



Your newly deleted entry disappears from the right pane and the dates assigned to that entry are no longer highlighted on the Blackout Dates calendar in the left pane.

Importing Blackout Periods

You can use the Blackout Period Import operation to automate Blackout Period management tasks. Using a properly formatted import file with this tool, you can:

- Create new Blackout Period profiles.

- Remove Blackout Period profiles.
- Enrich Blackout Period information.

The source file for the import contains the following information about a Blackout Period Profile:

- **Date.** The date on which the Blackout Period profile becomes effective. This date can be omitted for Every Day Blackout Period profiles.
- **Start Hour.** The time (HH:MM:SS) at which the Blackout Period becomes effective. This value is optional for all but Every Day Blackout Period profiles.
- **End Hour.** The time (HH:MM:SS) at which the Blackout Period ceases to be effective. This value is optional for all but Every Day Blackout Period profiles.
- **Description.** A detailed description of the Blackout Period profile.
- **Name.** The unique name assigned to a Blackout Period profile.

Note: Additional Codes precede entries for Weekly or Monthly Blackout Period profiles. For more information, see *Weekly Blackout Period Import File Entry Layout* on page 98 and *Monthly Blackout Period Import File Entry Layout* on page 99.

The task you select when you run an import operation determines the way in which ReportCaster uses the information in the source file for the Import.

If you select:

- *Add*, the import creates new Blackout Period profiles from the records in the import source file.
- *Remove*, the import compares date and additional information in import file records to that of existing Blackout Period profiles and removes those profiles that match the file records.
- *Replace*, the import compares date information in import file records to that of existing Blackout Period profiles and adds Name and Description information to them.
- *Use the actions specified in the file*, the import runs the add, remove, and replace operations as required by commands included in the Import file along with entries for the Blackout Period profiles affected by them.

The automation of these tasks frees you from manually creating, updating, or deleting Blackout Period profiles when operational changes, such as monthly, quarterly, or annual operation schedule updates, require a sweeping review and revision of your reporting schedule.

For example, at the start of the year, you have a file containing the dates and names of all scheduled holidays that must be incorporated into your reporting schedule. The Blackout Period Import enables you to import that file and establish the holiday blackout schedule for an entire year in a single operation. Without the import you would have to create a Single Date Blackout Date and Time profile for each holiday in the coming year.

Viewing Blackout Period Import File Format

Even though entries in the Import File format for Blackout Period records use the same basic structure, each profile type contains minor variations that identify the type of Blackout Period profile ReportCaster must create from the entry details.

Single Date Blackout Period Import File Entry Layout

You can import Single Date Blackout Date and Time profiles from a flat file that lists the information for each profile on a separate line. Each line must follow the following layout:

```
[Date]/[Start Hour]| [End Hour] [Description]|[Name]
```

For example:

```
20150629/08:59:00|10:59:00 Report Blackout for June 29th Only|Special One
 Day Blackout - June 29th
```

- Dates use the format YYYYMMDD
- Hours use the format HH:MM:SS
- You can omit the hours to schedule an all day blackout.

The Weekly, Monthly, and Every Day Blackout Date and Time profiles use a variation of this format.

Weekly Blackout Period Import File Entry Layout

You can import Weekly Blackout Date and Time profiles from a flat file that lists the information for each profile on a separate line. Each line must follow the following layout:

```
[Blackout Pattern] [Description]|[Name]
```

For example:

```
[111111111111/10000:0000010]/17:00:00|23:59:00 Report Blackout First Friday
 of Every Month 5:00 PM to 11:59 PM|First Friday Afternoons
```

This information identifies the entry as a Weekly Blackout Period, and includes its Description and Name. The Blackout Pattern indicates the selected Month(s) and Selected Day(s) of the Week. A '1' means that a month or day is selected. A '0' means that a month or day is not selected.

Monthly Blackout Period Import File Entry Layout

You can import Monthly Blackout Date and Time profiles from a flat file that lists the information for each profile on a separate line. Each line must follow the following layout:

```
[Blackout Pattern]/[Start Hour]|[End Hour] [Description]|[Name]
```

For example:

```
[111111111111/10000:0000010]/17:00:00|23:59:00 Report Blackout First Friday
 of Every Month 5:00 PM to 11:59 PM|First Friday Afternoons
```

This information identifies the entry as a Monthly Blackout Period, and includes its Description and Name. The Blackout Pattern indicates the selected Month(s) and Selected Day(s) of the Month. A '1' means that a month or day is selected. A '0' means that a month or day is not selected.

Every Day Blackout Period Import File Entry Layout

You can import Every Day Blackout Date and Time profiles from a flat file that lists the information for each profile on a separate line. Each line must follow the following layout:

```
/[Start Hour]|[End Hour] [Description]|[Name]
```

For example:

```
/21:04:00|23:04:00 Every Day Blackout between 3:00 PM and Midnight|Daily
Afternoon Blackout
```

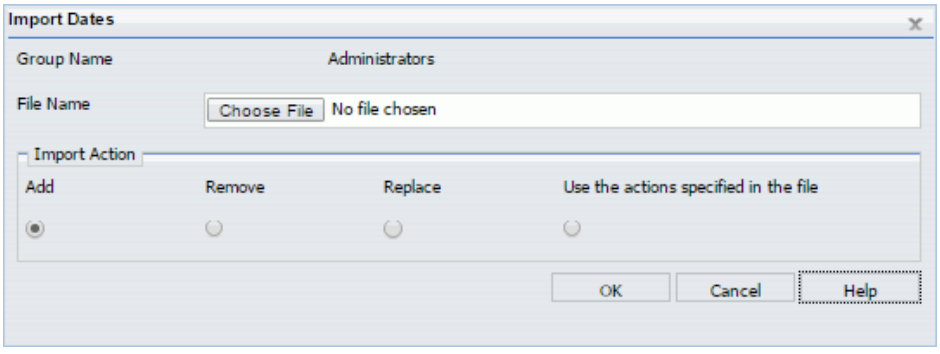
This information identifies the entry as an Every Day Blackout Period and includes its Description and Name.

Procedure: How to Add Blackout Period Profiles Using an Import File

To add a Blackout Period profile through the import is to create a new Blackout Period profile from information in the import file. Your Import file must therefore contain records for all Blackout Period profiles you want to add to ReportCaster through this import operation.

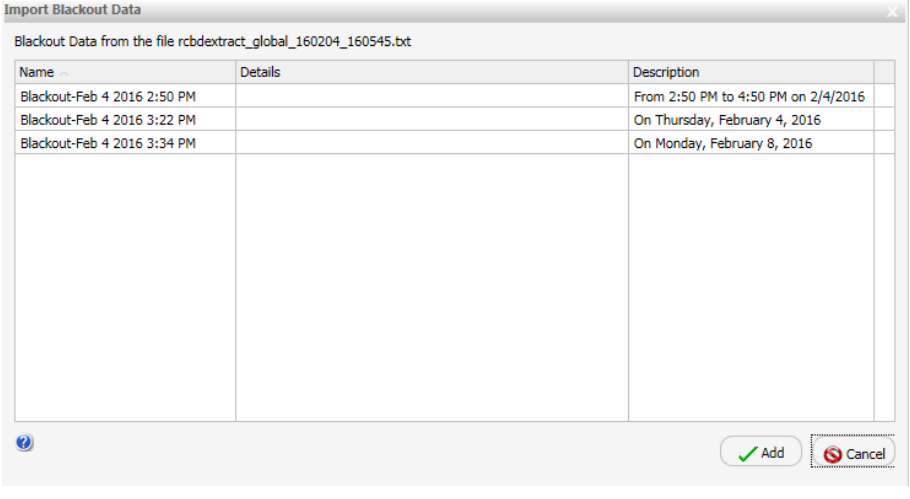
1. In the Blackout Dates pane, click the folder of the group for which you are importing Blackout Period profiles.

2. On the ribbon, in the Manage Blackout Periods group, click *Import*.



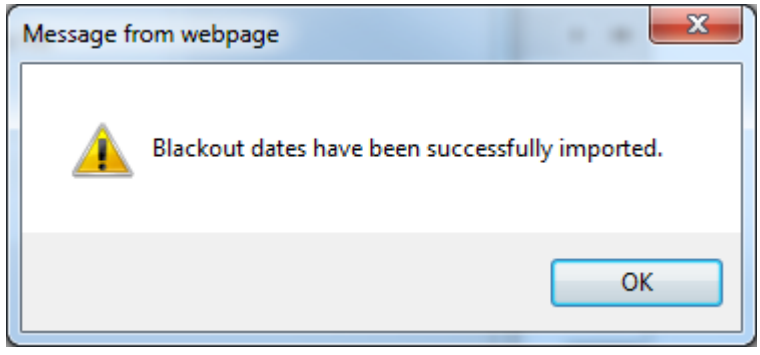
3. In the File Name field, type the full path to the file, or click *Browse* and navigate to the file you want to import.
4. Click *Add*, and click *OK*.

   The Import Blackout Data dialog box opens, listing details of the new Blackout Profiles based on each entry in the Import file as shown in the following image.



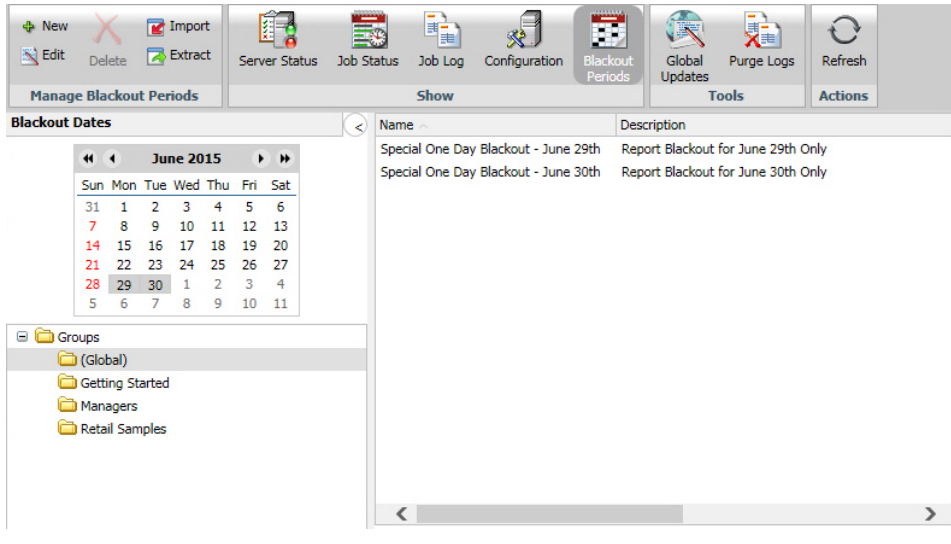
5. Click *Add* to add the new Blackout Period profiles listed in the Import Blackout Data dialog box to the Blackout Dates Calendar and Group entries.

A message displays, informing you that the blackout dates have been successfully imported, as shown in the following image.



6. Click *OK*.

   The Blackout Dates calendar highlights the newly imported Blackout Period Dates in the left pane of the Blackout Dates window and entries for the new Blackout Period profiles appear in the right pane, as shown in the following image.



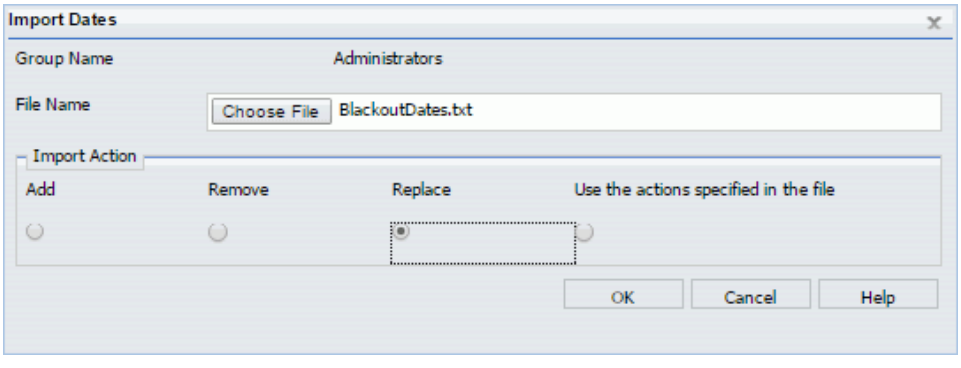
Procedure: How to Replace Blackout Periods Using an Import File

To replace a Blackout Period profile through the import is to add updated information to its Name and Description fields. To ensure that the import-based update affects the proper profiles, your Import file must contain records whose dates match those of the existing Blackout Period profiles that must be enriched by this Import operation.

> **Note:** You *must* use this procedure to update or enrich information assigned to a Blackout Period profile created from an Import.

1. In the right pane of the Blackout Dates dialog box, select the group for which you are importing Blackout Period profiles.
2. On the ribbon, in the Manage Blackout Periods group, click *Import*.

   The Import Dates dialog box opens, as shown in the following image.

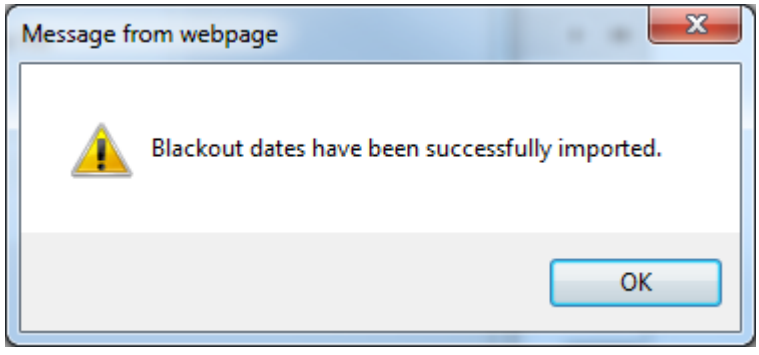


3. In the File Name field, type the full path to the file, or click *Browse* and navigate to the file you want to import.
4. Click *Replace*, and then click *OK*.

   The Import Blackout Data dialog box opens, listing the details from each entry in the Import file that will be added to their corresponding Blackout Period profiles.

5. Click *Replace* to add new the information listed in the Import Blackout Data dialog box to the designated Blackout Period profiles.

A message displays, informing you that the blackout dates have been successfully imported, as shown in the following image.



6. Click *OK*.

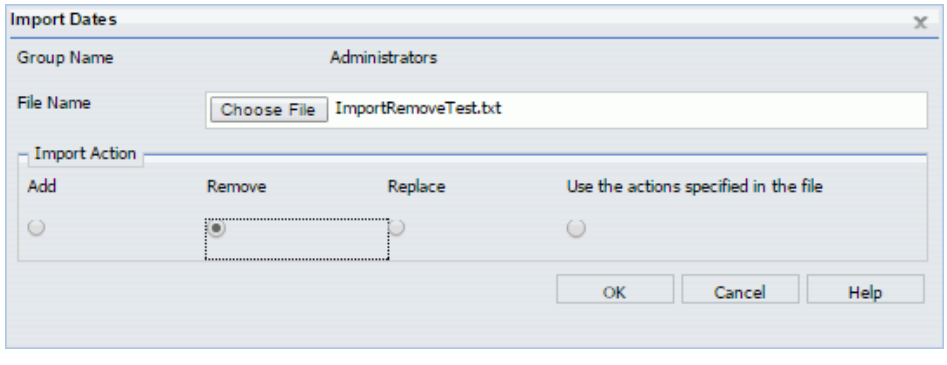
   Enriched entries for the updated Blackout Period profiles appear in the right pane.

Procedure: How to Remove Blackout Periods Using an Import File

Removing a Blackout Period profile through the import deletes it. To ensure that the import-based deletion affects the proper profiles, your Import file must contain records whose dates match those of the existing Blackout Period profiles that are to be deleted by this Import operation.

1. In the Blackout Dates tab pane, select the group containing blackout period profiles that must be removed.
2. On the ribbon, in the Manage Blackout Periods group, click *Import*.

   The Import Dates dialog box opens, as shown in the following image



3. In the File Name field, type the full path to the file, or click *Browse* and navigate to the file you wish to import.

4. Click *Remove*, and then click *OK*.

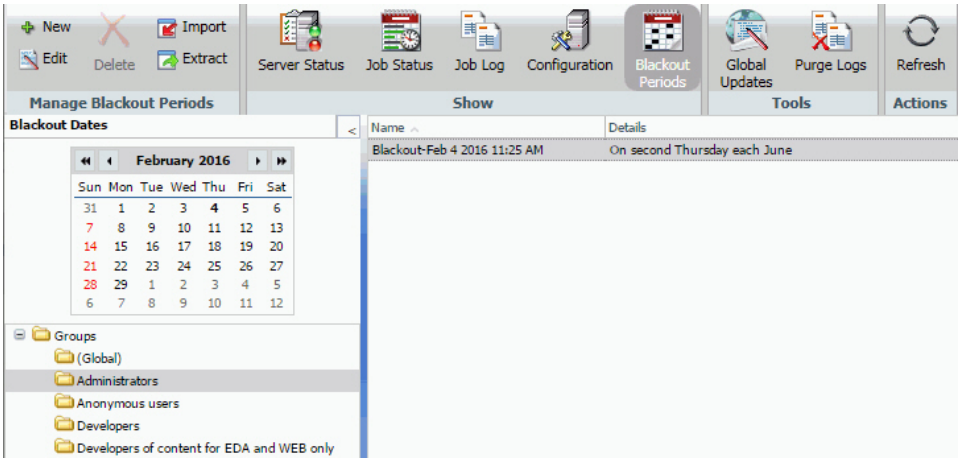
   The Import Blackout Data dialog box opens, listing details from each entry in the Import file that successfully matched an existing Blackout Period profile.

5. Click *Remove* to delete those Blackout Period profiles listed in the Import Blackout Data dialog box.

   A window opens, informing you that the blackout dates have been successfully imported.

6. Click *OK*.

   Blackout Period profiles removed by this operation are no longer highlighted in the left pane of the Blackout Dates window or as entries for the new Blackout Period profiles in the right pane, as shown in the following image.



Procedure: How to Manage Multiple Blackout Period Updates Using an Import File

The *Use the actions specified in the file* option allows the import process to add, remove, and replace multiple Blackout Period profiles in a single operation. Your Import file must therefore contain the all necessary commands followed by entries representing Blackout Period profiles that must be added, removed, or enriched by the import operation.

1. In the right pane of the Blackout Dates dialog box, select the group for which you are managing Blackout Period profiles.
2. On the ribbon, in the Manage Blackout Periods group, click *Import*.

   The Import Dates dialog box opens.

3. In the File Name field, type the full path to the file, or click *Browse* and navigate to the file you want to import.
4. Click *Use the actions specified in the file*, and then click *OK*.

   The Import Blackout Data dialog box opens, listing details from each entry in the Import file and a note about its proposed update.

5. Click *OK*.
6. When you receive the *Blackout Dates have been successfully imported* message, click *OK*.

   The Blackout Dates calendar highlights the dates of the newly imported Blackout Periods in the left pane of the Blackout Dates window. Entries for the new and enriched Blackout Period profiles appear in the right pane. Calendar highlights and entries for profiles removed by the Import no longer appear.

   Note: You will be unable to use the Edit command to update Blackout Period profiles created from a direct file import. You will be required to update these profiles using the Replace option in the Import operation.

Extracting Blackout Period Profiles

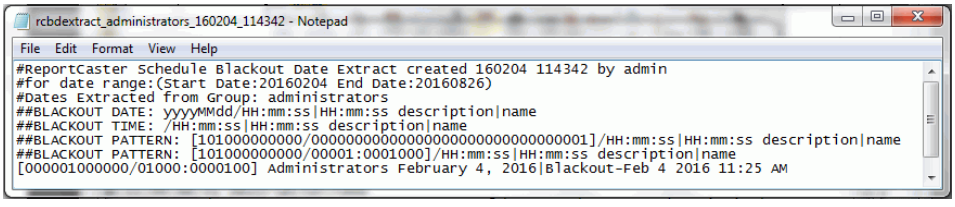
You can extract existing blackout period profile information from the ReportCaster Development Interface to a .txt file.

A direct file extract minimizes the time it would take to transfer information about multiple Blackout Periods to a text file that can serve as a backup of your Blackout Calendar configuration or as the source of an import to an external system for reporting or auditing purposes.

For example, if your group is required to maintain a backup copy of blackout dates for the coming six months, the extract operation enables you to transfer the Description, Date, and Name of all scheduled blackout periods during that time. You can recreate basic information about these profiles from the backup file in an emergency, shortening the time required to reconstruct your reporting schedule.

Extracting File Formats

The Import and Extract file operations use the same layout and format conventions. The Extract file contains additional comments that document the range of dates selected for the extract and templates for the format of the entries it contains, as shown in the following image.



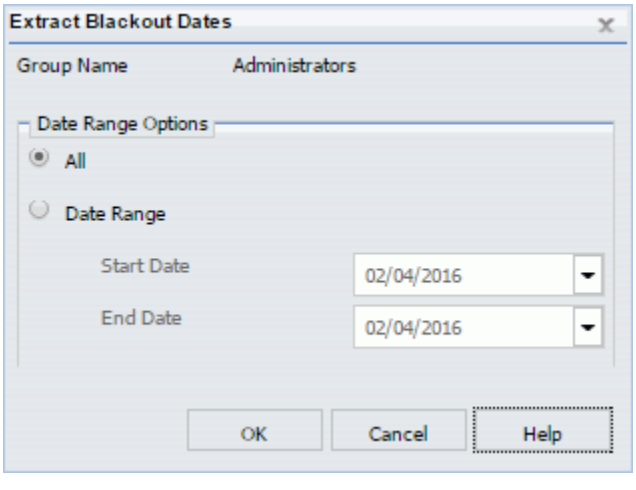
For more information about each entry type layout, see *Viewing Blackout Period Import File Format* on page 98.

Procedure: How to Extract Schedule Blackout Period Profiles to a File

To extract schedule blackout period profiles:

1. In the Blackout Dates pane, select the group from which you are extracting blackout period profiles.
2. In the Manage Blackout Periods Toolbar group, click *Extract*.

   The Extract Blackout Dates dialog box opens. The Group Name from which you are extracting the blackout dates appears at the top of the dialog box, as shown in the following image.



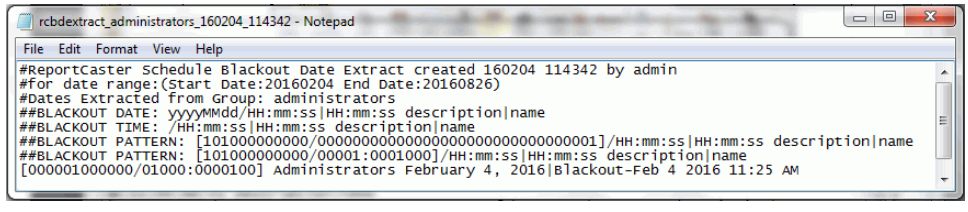
3. Select one of the following from the Date Range Options:

- *All* to extract all currently saved blackout period profiles.
- *Date Range* to specify the range of dates containing scheduled blackout period profiles that you want to extract.

If you select Date Range, type or select the Start Date and End Date. To select a date, click the down arrow next to the field. A calendar opens, from which you can choose a date.

4. Click *OK*.
5. To open the file, click the *Open* button when your browser presents it.

   A window opens, displaying the contents of the extracted content profiles, as shown in the following image.



   You can save and close the file using the commands in the File menu.

6. To accept an automatic download of the extract file, click the *Save* button (users of Google Chrome need only close the page displaying the new file name).

   You can later retrieve the file from the Downloads folder of your computer, rename it if necessary, and save a copy of it in another folder for archival or other purposes.

7. To rename and save the file in a different location, click the *Open* or *Open With* button, and select the *Save As* command from the program that opens the file.
8. From the Save As window, navigate to the folder in which you want to save the file, rename the file if necessary, and click *Save*.

   You can close any additional web pages that may remain open after you save the file.

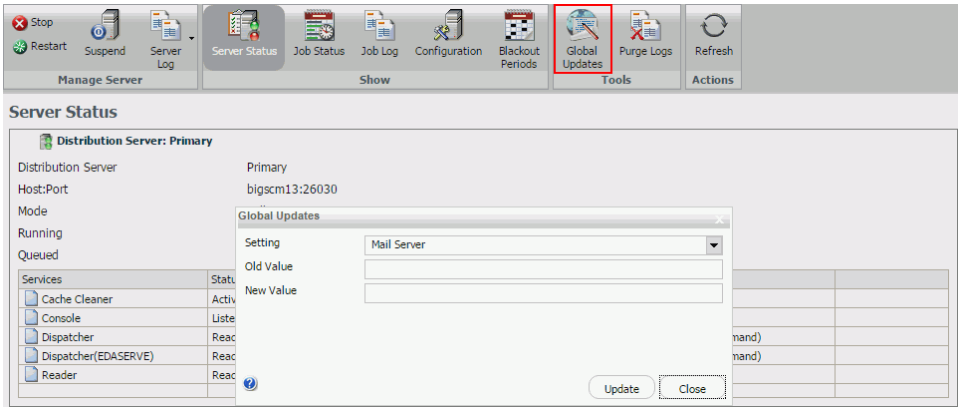
> **Note:** The default extract file name is *rcbdextract_GroupName_YYMMDD_HHMMSS.txt*, where *GroupName* is the name of the group from which the blackout dates are extracted, YYMMDD and HHMMSS are the date (year, month, day) and time (hour, minute, second) that the file was created.

Global Updates

Authorized users can make global updates in the Global Updates interface for the Mail Server, Printer, Email Address, Email from, and Data Server values stored in schedules and distribution lists.

Procedure: How to Make a Global Update for a Mail Server

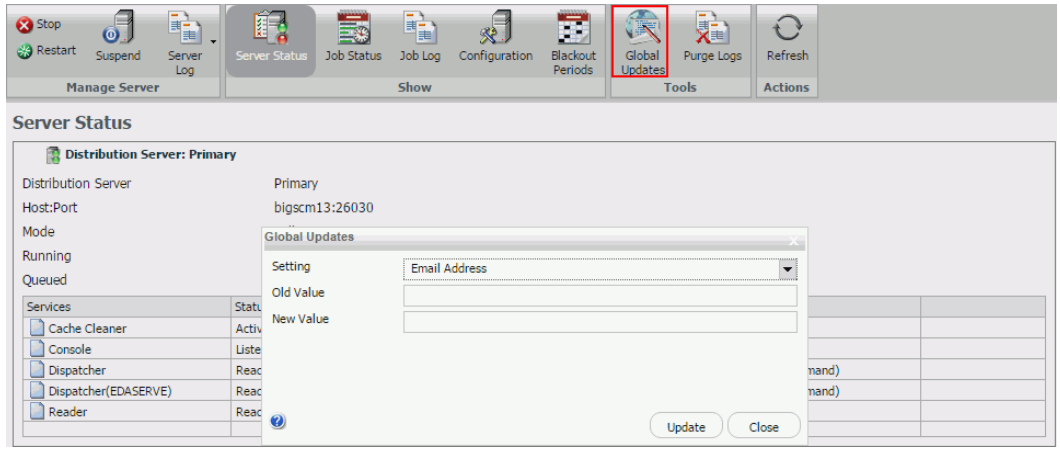
1. In the Global Updates interface, click the *Setting* drop-down list and select *Mail Server* (the default), as shown in the following image.



2. Type the existing Mail Server in the *Old Value* box.
3. Type the new Mail Server in the *New Value* box.
4. Click *Update* to update the new Mail Server value in schedules.

Procedure: How to Make a Global Update for an Email Address

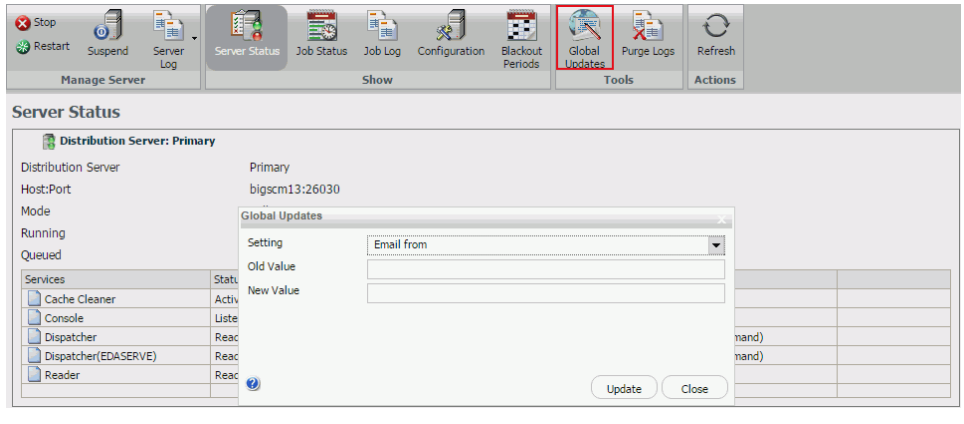
1. In the Global Update interface, click the *Setting* drop-down list and select *Email Address*, as shown in the following image.



2. Type the existing Email address in the *Old Value* box.
3. Type the new Email address in the *New Value* box.
4. Click *Update* to update the new Email address value in schedules and distribution lists.

Procedure: How to Make a Global Update for an Email From

1. In the Global Update interface, click the *Setting* drop-down list and select *Email from*, as shown in the following image.

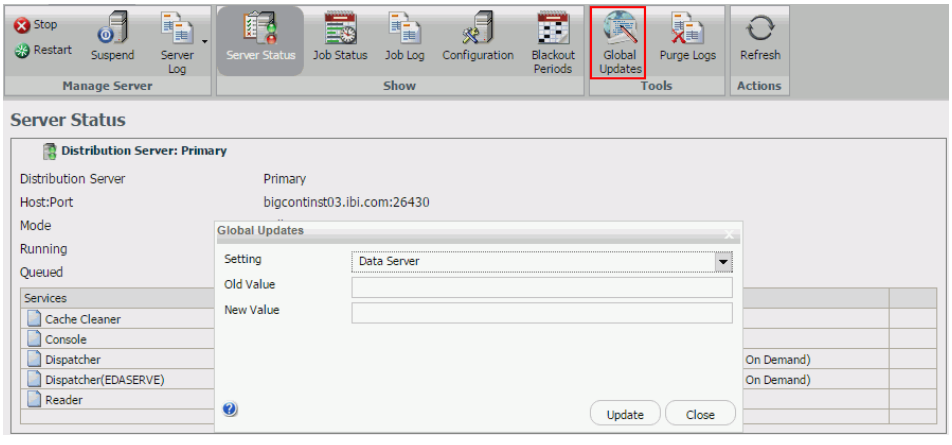


2. Type the existing Email from in the *Old Value* box.

3. Type the new Email from in the *New Value* box.
4. Click *Update* to update the new Email from value in schedules.

Procedure: How to Make a Global Update for a Data Server

1. In the Global Update interface, click the *Setting* drop-down list and select *Data Server*, as shown in the following image.



2. Type the existing Data Server in the *Old Value* box.
3. Type the new Data Server in the *New Value* box.
4. Click *Update* to update the new Data Server value in schedules.

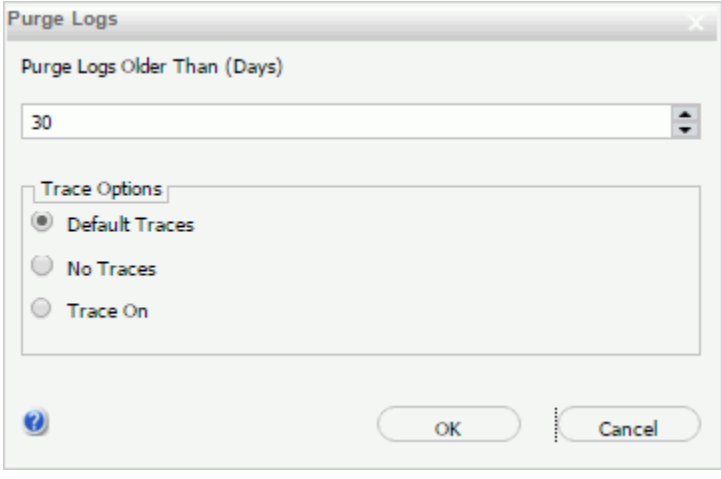
Purge Logs

The Purge Logs functionality provides on-demand options for purging logs, including the ability to specify a number of days (past) for which to purge logs. For example, if you want to purge logs for the past month, you would use the default number of days, which is 30. You can also specify an option for traces: Default Traces, No Traces, or Trace On.

Procedure: How to Purge Logs on Demand

1. From the Tools group in the ReportCaster Console, click *Purge Logs*.

The Purge Logs dialog box displays, as shown in the following image.



2. In the *Purge Logs older than (days)* field, accept the default number of days or specify another value. The default number of days is 30.
3. Under Trace Options, you can accept the default of *Default Traces,* or select *No Traces* or *Trace On*.
4. Click *OK*.

Working With Domains

The BUE uses Domains, and the groups of users they define, to support workgroups. Domains enable users to maintain private content, to share that content if their user role permits, and to access governed content published by others. Domains are available to multiple users, who, based on their role, have access to their own view of the Domain. This built-in workgroup security makes your data analysis and reporting activities easier to configure and manage.

In the Resources tree, Domains appear as root-level folders under the Domains node.

Domains comprise a collection of groups, an Application folder on the Reporting Server, and a set of rules that makes them all work together in a single workgroup. Domains partition content and metadata, and enable Managers to organize and store your content in the BUE portal. They are the place where Developers and Advanced Users create and manage content.

Procedure: How to Create a Domain

Only a Manager can create a Domain.

1. In the Resources tree, right-click *Domains*, point to *New*, and then click *Domain*.

The New Domain dialog box opens.

2. Type a title and a name.

   Domain titles are shown to BUE users in the Resources tree. Managers can localize the title for different languages by going into the Property dialog after the Domain is created.

   The Domain name is an internal identifier used by BUE, and is not shown to users.

3. Click *OK* to create the Domain.

   A confirmation dialog appears. Click *OK*.

   A folder that contains the title of the new Domain appears below the Domains node in the Resources tree.

   Note: Within the new Domain, the BUE creates a Hidden Content folder as well as a My Content folder for each user. The Hidden Content folder can be used to store things that are related to the Domain but which you do not want users to see. For example, schedules that distribute output back to the Domain and image files or style sheets that are used by charts. The My Content folder is used by each user to store their personal content. Some users can share personal content with Domain users. Domain Developers and Managers can create folders and content within the domain and publish it so Domain users can access and interact with it.

Managing Domain Users

When a Manager creates a new Domain, the WebFOCUS Business User Edition automatically creates a new group for the Domain itself, and creates subgroups for each of the four user types within it. A Domain accommodates multiple users, maintaining independent views and levels of availability for each one. By assigning users to different groups within a Domain, a Manager or Group Administrator can set security options for each user at the Domain level.

To review these groups, open the Security Center. From there, a Manager can create new users for these Domain groups or add existing users to them. For more information about Groups, see *Managing Groups* on page 122.

Granting Access to a Domain

When a Manager first creates a Domain, it is available only to the Manager that created it.

To update this setting, the Manager must right-click a Domain, point to *General Access*, and then select one of the following settings.

- **Domain Groups.** Protects the Domain by limiting its availability to those users who are assigned to it and work within it. This is the default setting for all new Domains.
- **All Users.** Gives everyone Basic User access to the Domain. Using this setting, the Manager that created the Domain can make content and resources available to all users in a single action instead of individually assigning each user to the Domain.

The four Domain groups represent the four user types: Basic User, Advanced User, Developer, and Group Administrator. When the Manager or a Group Administrator assigns users to one of these groups, those users automatically obtain the privileges assigned to the user role represented by that group when working with content in that Domain.

Managing Domain Private Resources

The Manage Private Resources feature allows Managers and Group Administrators to identify and manage private resources owned by users or groups. In the BUE, Managers can manage private resources by user, group, or Domain.

Procedure: How to Delete a Domain

Only a Manager can delete a Domain.

1. In the Resources tree, right-click a Domain, and then click *Delete*.

   A confirmation dialog box opens.

2. Click *Yes* to delete the Domain.

   If there is private user content in the Domain, a message will appear that the Domain could not be deleted. To delete the Domain along with all private content switch into Manager Mode (under the Administration menu in the menu bar), optionally review the private user content shown in the domain, and then delete the domain again while in manager mode.

Managing Domain Users After Deleting a Domain

Even though deleting a Domain automatically deletes the groups associated with it, this action does not delete the users assigned to those groups. Users from the deleted groups remain in the Users pane in the Security Center, but, unless they are assigned to another group, they are limited to view only privileges. To completely remove users from deleted groups, a Manager must delete them from the Security Center.

Working With Folders

Folders contain all repository content. Whenever a user creates a folder, it will always be created as a private folder. If the creator is permitted the necessary privileges, folders and their contents can be shared with other users or published for general use.

Folders have both titles and file names. The title is what is typically displayed to users. The file name is used as an internal reference by WebFOCUS BUE to provide an unambiguous context. Titles can be duplicated within a container, but file names cannot.

The folder path may have up to 1,040 characters for the path information (not including the object name), and up to 64 characters for the object name. For example, a folder may be named: /WFC/Repository/AmericaBank/Finance. In this example, /WFC/Repository/AmericaBank/ is 28 characters and Finance is 7 characters.

Procedure: How to View Folder Properties

Right-click the folder or item and click *Properties*. The Properties dialog box opens, displaying the information in the following table.

Item	Description
Language	Provides a list of languages that you can click.
View All	Opens the Language Properties dialog box, where you can click a language.
Title	Displays the value in the Resources tree, so users can identify the content within the folder.
Folder Name	Unique reference to the folder. click the *Change Name* check box to change the name of the folder.
Summary	Provides a detailed explanation with additional information about the folder.
Parent Folder	Shows the previous folder in the folder path of the WebFOCUS Repository.
Full Path	Displays full repository path of the folder in the WebFOCUS Repository.
Created On	Identifies the date and time the folder was created.

Item	Description
Created By	Identifies the user who created the folder.
Last Modified On	Shows the date the folder was last modified.
Last Modified By	Displays the user ID that last modified the folder.
Last Accessed On	Shows the date the folder was last opened.
Last Accessed By	Identifies the user who last opened the folder.
Properties	Shows a string of name value pairs that identify the properties of the folder.
Size	Displays N/A bytes for folders.
Run	Displays N/A, as this property is not applicable to folders.
Sort Order	Specifies the order to list the folder in the Resources tree or list items within a folder.
Status	Indicates whether the folder is Published or Private. Private will also display the owner information.

In addition, the following options are available to control the usage of content within the folder:

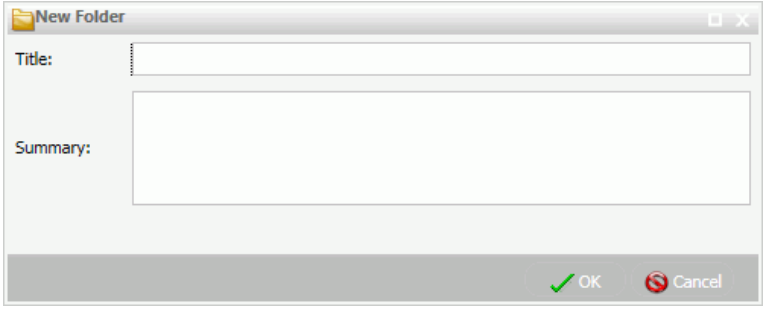
Authorized users can view or edit the access rules, effective policy, or sharing permissions by click *Security*.

The Server Properties tab shows the Assigned Server and available Application Paths. When a Reporting Server is not specified, the report request is submitted to the default Reporting Server specified in the Client configuration. When an Application Path is not specified, the Application Path defined during the processing of the Client configuration and the Reporting Server configuration is used.

Procedure: How to Create a Folder

1. In the Resources tree, right-click a domain or folder and click *New Folder*.

The New Folder dialog box opens, as shown in the following image.



2. Type the title and summary for the new folder.

> **Note:** The unique folder name is derived from the title. The following characters are not permitted to be used within a folder name:
> (Blank Space) & * ( ) | : ; " , ? /
> If you use restricted characters in the Title when creating a new folder or item, it is automatically removed from the Folder Name or File Name.

3. Click *OK*.

Procedure: How to Publish a Folder

In the Resources tree, right-click a folder, and click *Publish*.

Procedure: How to Duplicate a Folder

In the Resources tree, right-click a folder, and click *Duplicate*.

A duplicate folder appears. The name and title of the duplicate folder are the same as those of the original, appended with an underscore and an integer that increases each time the folder is duplicated.

Procedure: How to Cut or Copy and Paste a Folder

1. In the Resources tree, right-click a folder, and click *Cut* if you want to move the folder, or *Copy* if you want to leave the original folder in place.
2. Right-click the desired location and click *Paste*.

Folder names must be unique within a specific location. If the folder is pasted in a different parent folder, its name remains the same, as long as no folder of that name already exists in the new parent. If a folder of that name already exists, or if the pasted folder has the same containing folder as the original, the name of the copy is the same as the original, appended with an underscore and an integer that increases each time the folder is pasted. The folder titles update in the same way as the folder names.

Procedure: How to Change a Folder Title

1. In the Resources tree, right-click a folder, and click *Change Title*.

   A cursor appears in the folder title field in the Resources tree.

2. Type the new name and press the Enter key.

   The folder name is updated.

Procedure: How to Delete a Folder

1. In the Resources tree, right-click a folder, and click *Delete*.

   A confirmation dialog box opens.

2. Click *Yes* to proceed with the deletion.

Managing Users

The Users pane of the Security Center lists all users. The Search field in this tab allows you to search the name and description fields for users. Simple wildcard searches are supported. The full range of features that manage users is available only to Managers. Group Administrators can see the Security Center, but can only assign existing users to groups. Basic Users, Advanced Users, and Developers cannot see the Security Center, nor can they create, update, or delete users or assign users to groups.

The toolbar above the User pane allows Managers to perform the following actions:

- Create, edit, or delete users.
- Import users.
- View when users last signed in.

Understanding Users

Users are those individuals who have access to the WebFOCUS Business User Edition, the BUE. Managers and Group Administrators can assign users with similar responsibilities to one of the user type groups that the BUE automatically creates within a domain. This assignment allows users to take advantage of those features and content that supports their daily activities, but prevents them from using features or content that are beyond the range of their responsibilities and authority. The four user types are:

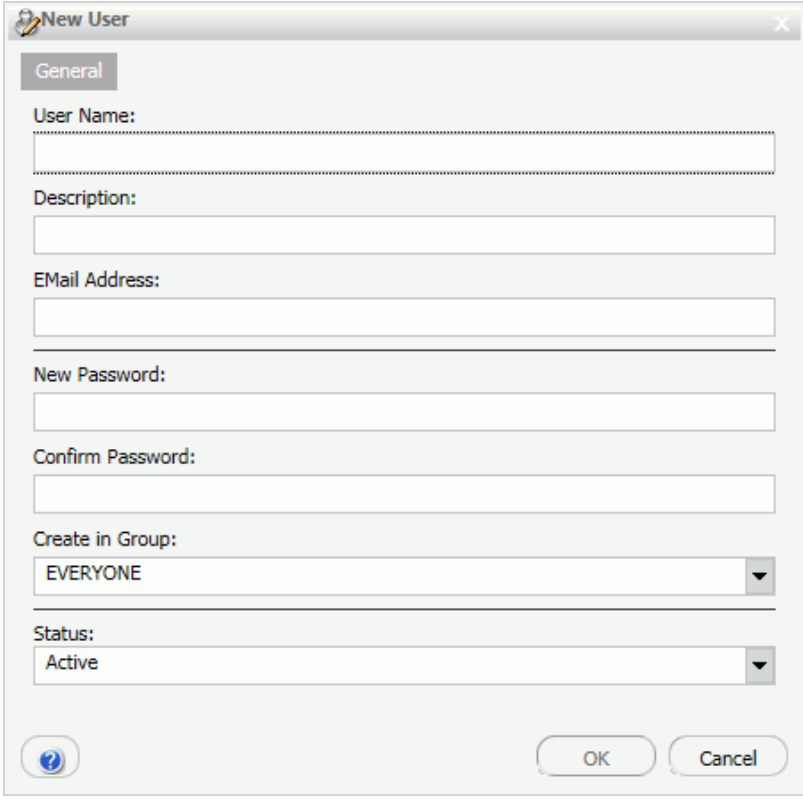
- **Basic Users.** Can view reports and content in the domains accessible to them. They can save deferred reports to their My Content folders, or copy parameters from a previously created report. They cannot share, publish, copy, or paste any folder or content.
- **Advanced Users.** Can do everything that Basic Users can do, and can also create original reports, charts and other content for their My Content folders. They can share folders and the content they contain with everyone or with selected users or groups.
- **Developers.** Can do everything that Advanced Users can do, and can view and publish content in their Hidden Folder. They can also copy and paste folders and content from their domain to another domain, but they must be sure that the domain they target for this operation maintains the same metadata as that used to create the content they are copying.
- **Group Administrators.** Can assign users to Groups. They can also switch to Manager Mode and manage private resources.

Procedure: How to Create a User

Only a Manager can create a user.

1. In the BUE Portal, on the Menu bar, click *Administration*, and then click *Security Center*.
2. On the Users & Groups tab, click the *New User* button  .

The New User dialog box opens, as shown in the following image.



3. Type the user name, description, email address, password, and password confirmation, and if desired, select a group and a status for the user, and then click *OK*.

   If you do not enter a description, the description defaults to the name. If you do not select a group and status for the user, the user will be created in the EVERYONE group and assigned the Active status by default.

Procedure: How to Import Users

A Manager can import a .csv file containing multiple users. This can be quicker and more efficient than individually creating multiple users with the New User dialog box.

The import file must contain the following columns: user name, password, description, email address, user status, and groups. A sample .csv import file, getting_started_sample_users.csv, is provided in the BUE file installation directory for your use as a template.

- Values are separated by commas.
- To use a comma in a description, enclose the description within double quotes.
- Multiple groups are separated by semicolons.

Note: Do not include a header in the user .csv file.

1. In the BUE Portal, on the Menu bar, click *Administration*, and then click *Security Center*.
2. On the Users & Groups tab, click the *Import Users* button  .

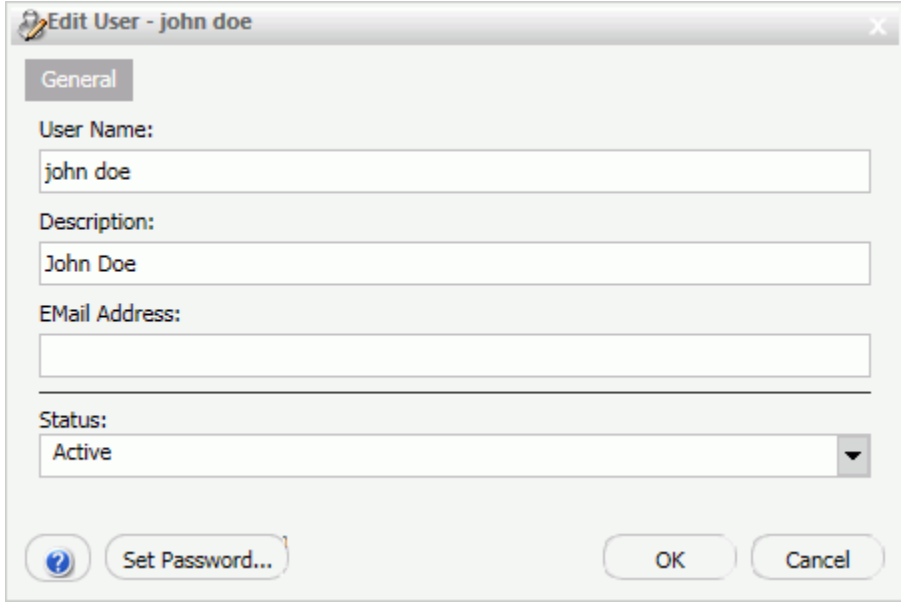
   The Import Users dialog box appears.
3. Browse to find the desired .csv file and click *Import*.

   The new users are created within the specified groups.

Procedure: How to Edit User Details

Only a Manager can edit user details.

1. In the BUE Portal, on the Menu bar, click *Administration*, and then click *Security Center*.
2. On the Users & Groups tab, double-click a user, or right-click the user and select *Edit*, or click the user and then click the *Edit User* button . The Edit User dialog box opens, as shown in the following image.



3. If desired, type new information in the User Name, Description, or EMail Address field.
4. To change the status of a user, select *Active*, *Inactive*, or *Must Change Password* from the Status drop-down list.

> **Note:** If you select *Must Change Password*, users will be prompted to change their password when they attempt to sign in.

Procedure: How to Delete a User

Only a Manager can delete a user. The action of deleting a user also deletes that user's private content. Be sure to publish or share any private content assigned to that user if it supports ongoing activities.

1. In the BUE Portal, on the Menu bar, click *Administration*, and then click *Security Center*.
2. On the Users & Groups tab, right-click a user and select *Delete*, or select the user and click the *Delete User* button .

A confirmation dialog box opens. Click *Yes* to delete the user.

Managing Groups

In the BUE, only Managers and Group Administrators can open the Security Center and review groups. The Groups field in the Users & Groups tab of the Security Center lists all the groups in the repository in alphabetical order. Subgroups appear indented below their parent groups. The Users in Group field lists the members of the selected group. If no group is selected, the field is blank. The Search field in this tab allows Managers and Group Administrators to search the name and description fields for groups. Simple wildcard searches are supported. A toolbar allows Managers and Group Administrators to perform the following actions:

- View the groups to which a user belongs.
- Add users to groups or remove them from groups.
- View the members of a group.

Understanding Groups

Groups are formed of users or subgroups that require similar capabilities or access to the same resources. All users are members of the EVERYONE group, which is the set of all named users in the system.

A group is a collection of similar users. Typically, users are permitted actions based on rules that apply to groups, although rules may also apply to individual user roles. Users may belong to more than one group.

Creating Groups From Domains

The BUE automatically creates groups whenever a Manager creates a new Domain and deletes them whenever a Manager deletes a Domain.

This feature simplifies group management by limiting it to the assignment of users to previously created groups. Managers and Group Administrators are not obligated to create or delete groups independently.

Each Domain creates one master group that uses its name. This group does not contain any users.

The Domain also creates four groups within that master group that correspond to the four basic user types within the BUE.

Members of the Basic User group can view content within their Domain and can save copies of reports they run deferred to their My Content folder for their own use.

Members of the Advanced User group have all the privileges of basic users, and they can create, share, and distribute their own content.

Members of the Developers group have all the privileges of basic and advanced users, and they can upload and connect to data, edit metadata, and create and organize Domain content. They can also manage the content other users see.

Group Administrators determine the role each user can have within a Domain by adding users to or removing users from groups and can change the General Access setting assigned to the Domain.

Users can be members of more than one of these groups and can have different privileges in different Domains. This capability is especially relevant to Group Administrators. In almost all cases, this group assignment, and the privileges it grants, is combined with membership in another group.

Procedure: How to Add a User to a Group

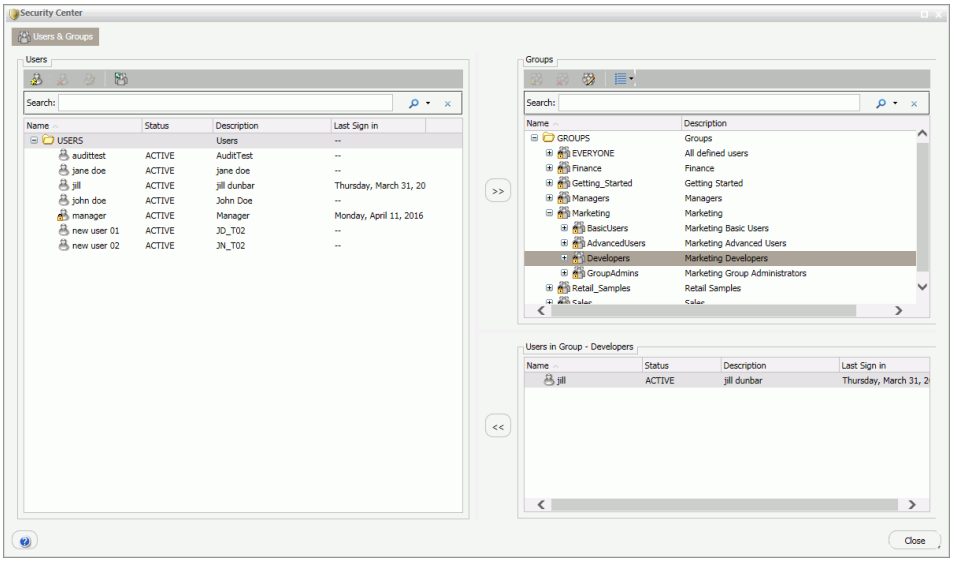
Only Managers and Group Administrators can add users to groups.

1. In the BUE Portal, on the Menu bar, click *Administration*, and then click *Security Center*.
2. On the Users & Groups tab, under Groups, select a group.

   Note: When you select a group, the members of the group appear in the Users in Group field.

3. Drag a user from the Users field into the Users in Group field, or select the user and click the *Add selected users to group* button >>.

The user you added now appears in the Users in Group field, as shown in the following image.



4. Click *OK*.

Procedure: How to Remove a User From a Group

Only Managers and Group Administrators can remove users from groups.

1. In the BUE Portal, on the Menu bar, click *Administration*, and then click *Security Center*.
2. On the Users & Groups tab, under Groups, select a group.
3. Select a user and click the *Remove selected users from group* button  , or drag the user into the Users field.

   You can also remove a user from a group by right-clicking on the user and selecting *Groups*, then *Remove from*, then the group from which the user should be removed.

Managing Private Resources

Sometimes it is necessary for a manager to view or modify the private resources owned by another user. For example, when employees leave the company and their status is set to inactive, their private resources may need to be deleted or transferred to another user. It can also be useful for managers to have access to the private resources of the groups they manage in order to share resources or troubleshoot procedures. BUE Managers and Domain Group Administrators have access to this feature. Managers can access the private resources of all users. Group Administrators can access the private resources of the users in their Domain groups.

You can perform most actions on non-output resources owned by other users, such as FOCEXECs, and schedules. For output resources, such as PDFs or Libraries, your abilities are limited to deleting the resources or changing their titles.

You can view and manage private resources by domain or by user or group.

Authenticating Users to Your Active Directory

You can configure WebFOCUS BUE to authenticate users against your corporate Active Directory. The WebFOCUS BUE Client passes User sign in credentials to the WebFOCUS BUE Reporting Server, which in turn, validates them within an external source. WebFOCUS BUE can authenticate users against external Active Directory or LDAP directories. Users are externally authenticated whenever they access WebFOCUS BUE and when they access the Reporting Server Console.

The benefits of authenticating users to the Active Directory include:

- **Improved usability.** Users only need to remember a single user ID and password.
- **Reduced administration.** WebFOCUS BUE synchronizes user information with Active Directory. BUE Managers no longer need to maintain separate BUE passwords.
- **Improved maintenance.** Each time a user signs in, their user description and email is updated using the information found in the Active Directory, simplifying WebFOCUS BUE administration.

Configuring Active Directory/LDAP Authentication

To convert to external Active Directory or LDAP authentication, you must override the default setting of internal authentication in both the BUE Client and the Reporting Server, and establish a connection between the Reporting Server and LDAP provider that will support authentication activities.

Here is an overview of the configuration steps:

1. Create a new WebFOCUS BUE Manager account whose name matches an account in Active Directory.

   Since the default Manager account manager generally does not exist in the external source, it cannot be authenticated once external authentication has been successfully configured. The new Manager account that you create will exist in both WebFOCUS and in Active Directory so that you can use it for access to the BUE once you have restarted WebFOCUS in its new authentication configuration.

2. Configure the BUE LDAP provider to authenticate users to Active Directory.
3. Configure BUE to use the LDAP provider and restart the BUE services.

In the steps which follow, you will be required to provide credentials for two service accounts. The first is a BUE Reporting Server account, PTH\srvadmin, that is used by WebFOCUS BUE to delegate authentication to the Reporting Server. The password for this account is pre-configured during BUE installation to be the same as the password you supplied for the BUE Manager account.

The second is an Active Directory account of your choice that is used by the Reporting Server to authenticate users and retrieve their full description and email information, which in turn is passed back to the BUE to update the user account. This service account simply needs read access to Active Directory. Generally, any Active Directory account can be used for this purpose but you must make sure its password is set to never expire.

Procedure: How to Create the Externally Authenticated Manager Account

1. Sign in to WebFOCUS BUE as a Manager.
2. In the BUE Portal, on the Menu bar, click *Administration*, and then click *Security Center*.
3. In the Security Center, under Users, click *New User*.
4. Type the Active Directory ID of the person who will be the new Manager for the BUE after Active Directory authentication is established, in the User Name field.

   You do not need to enter a description or email address because this information will be automatically updated during sign in based on information retrieved by the BUE from Active Directory.

5. Click *Managers* in the Create in Groups list.
6. Click *OK*.

   An icon for the new user appears under Users and under Users in Group, when you click the Managers group.

Procedure: **How to Establish LDAP as the Primary Security Provider on the Reporting Server**

1. Sign in to WebFOCUS BUE as a Manager.
2. In the BUE Portal, on the Menu bar, click *Administration*, and then click *Reporting Server Console*.
3. In the Reporting Server Console, click the *Access Control* tab.

   The Navigation pane displays an expandable LDAP folder.
4. Right-click the *LDAP* folder, and then click *New*.
5. In the LDAP Security Provider Configuration page, accept the default name, LDAP01, or type a new descriptive name for the LDAP security provider in the LDAP_PROVIDER field.
6. In the Connection Section, type the host name of your Active Directory server in the ldap_host field.

   In some cases, you can also enter the domain name of your organization, for example: ibi.com.
7. Change the value in the LDAP port field only if your installation uses a different port number.

   Most installations use the default port number, 389.
8. Click *Explicit* in the security list.

   The section expands and displays the fields, ldap_principal, and ldap_credentials.
9. Type the name of a Service Account that has read access to the Active Directory, in the ldap_principal field.

   It is important that this account has a non-expiring password to avoid disruption to the BUE.
10. Type the password of the Service Account in the ldap_credentials field.
11. Click *Next*.

    If you receive a message that the Discover LDAP server attributes failed, click *OK*, and then review and update the settings you entered up to this point.

    If all settings are correct, the page refreshes and displays additional headings. Fields in the User Search section contain values populated directly from the Reporting Server.
12. Click the *Trusted Connection* section heading.
13. In the Trusted Connection section, click *y* in the trust_ext list.
14. Click *Test User Authentication*.
15. Type the Active Directory User ID and Password of the person that you previously identified as the new BUE Manager, and then click *Continue*.

If you receive a message that the connection or password failed, review and update your settings if necessary, and try again.

If the password succeeded, continue with the next step.

16. Click *Save*.
17. In the Activate Providers page, in the LDAP entry that is identified by LDAP01, or by the descriptive name you typed in the LDAP_PROVIDER field, click *Primary* in the Status list.

    The Status of the LDAP entry changes to Primary, and the Status of the PTH<internal> Security provider entry changes to Secondary automatically.

18. Click *Save Provider's Status*.

    The screen refreshes and displays the Change Effective Security Provider page.

19. Click *Apply and Restart Server*.

    When the confirmation dialog box opens, click *OK*.

    The Reporting Server Console refreshes and displays the Applications tab.

20. Click the *Access Control* tab.
21. Review the new LDAP Security Provider and its Primary status.
22. Close the Reporting Server Console.

Procedure: How to Enable External Security in the WebFOCUS Client

1. Sign in to WebFOCUS BUE as a Manager.
2. In the BUE Portal, on the Menu bar, click *Administration*, and then click *Administration Console*.
3. In the Administration Console, click the *Security* tab.
4. Under the Security Configuration folder, click *External*.
5. On the External page, select the *Enable External Security* check box.

   The External page displays the settings currently assigned to the Reporting Server.

6. Type *PTH\srvadmin* in the *Server Administrator ID* field.

   This is a Reporting Server administrator account that was installed automatically during the BUE installation.

7. Type the password for this account in the *Password* field.

   The password was assigned during BUE installation, and is initially set to the same value that you entered for the manager account during installation.

> **Note:** The placement of this ID and its associated Password in the Server Administrator ID field enables the Client to present them to the Reporting Server when sending User authentication requests.

8. Click *Connect* to verify the credentials you provided.
9. Leave User Authorization set to Internal and ignore the Account Creation on Sign In settings. The BUE does not support changes to these options.
10. Select the *Synchronize User Information with Authentication Provider* check box.
11. Click *Save*.

    When the confirmation dialog box opens, click *OK*.
12. In the Administration Console menu, click *Close*.
13. Sign out of WebFOCUS BUE.
14. Stop and restart the Web Application to make these changes take effect. To do so:

    If this installation of the BUE is based on the Windows operating system, stop and restart the WebFOCUS BUE 82 Application Server service in the Services Window.

    If this installation of the BUE is based on the Linux operating system, navigate to drive/ibi/WebFOCUS_BUE82/tomcat/bin and run the shutdown.sh and startup.sh utilities.
15. When the Web Application restarts, sign in again using the Active Directory User ID and Password of the new BUE Manager that you identified at the beginning of the configuration.

    The user description on the Menu Bar in the BUE Portal, and the Email Address of this account now reflect the values retrieved by the BUE from the Active Directory.

Creating BUE User Accounts When Configured for Active Directory Authentication

Now that you have configured BUE to authenticate users to Active Directory, you can create BUE accounts and assign them to the appropriate groups. This can be done in two ways:

Security Center. To use the Security Center to create and assign accounts to groups, create accounts the normal way including assigning them to the desired groups. However, since you are configured for Active Directory authentication you do not need to assign passwords for these users and you do not need to populate the Description and Email fields for them. As you have seen, this information will be automatically retrieved from Active Directory as each user signs in.

Import Users. To use the Import Users feature, simply define a CSV file containing one row for each user account. You can use the following file located in your BUE installation directory getting_started_sample_users.csv as a template. You can leave the password, user description and email values blank but you need to preserve the same number commas in the file to properly delimit all the required fields. You can adjust the group membership data in the CSV for each user account to suit your requirements or you can leave it blank and assign users in Security Center. The file should contain only data rows with the required number of commas on each row and contain no blank lines. Here is an example:

user1, , , ,ACTIVE,

user2, , , ,ACTIVE,Getting_Started/Developers;Retail_Samples/AdvancedUsers

Creating a Change Management Package

Many organizations do not grant developers write access to the user acceptance test and production environments. Access to these environments is strictly controlled and granted only to administrators, production control personnel, or automated change management processes.

Only developers know which changes are ready to be moved into the test environment. The Change Management Export facility presents developers with a graphical view of the resources they manage and allows them to build a change management package. This package is then loaded into another environment by production control personnel or automated processes.

Procedure: How to Create a Change Management Extract Package

Only members of the BUE Managers group have access to the Change Management feature, which is available on the Resources tree as a node that contains two subfolders: Import and Export.

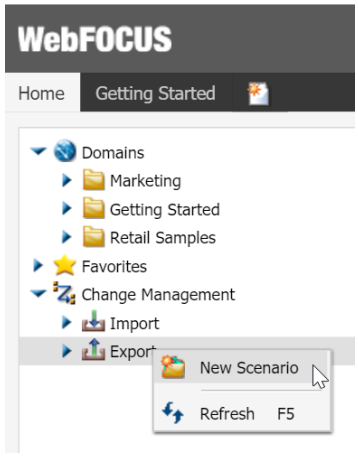
The steps required to create a Change Management Package are:

1. **Create a Scenario.** Utilizing the Change Management Export facility, an authorized user will create a scenario by selecting the resources to be exported. A scenario is a description of all the resources that will be exported into a Change Management Export Package.
2. **Export a Scenario.** After a scenario is created, a user can export this scenario into a Change Management Export Package. This Change Management Export Package is placed in the ibi\WebFOCUS_BUE82\WebFOCUS\cm\export directory in two formats: a zip file and a folder, which contains the expanded contents of the zip file.

   The zip file or the exported folder is then copied to the target environment and placed in the ibi\WebFOCUS_BUE82\WebFOCUS\cm\import directory. For convenience the CM zip file can be downloaded from the BUE using a web browser and similarly uploaded to the target BUE where its content can then be imported and accessed.

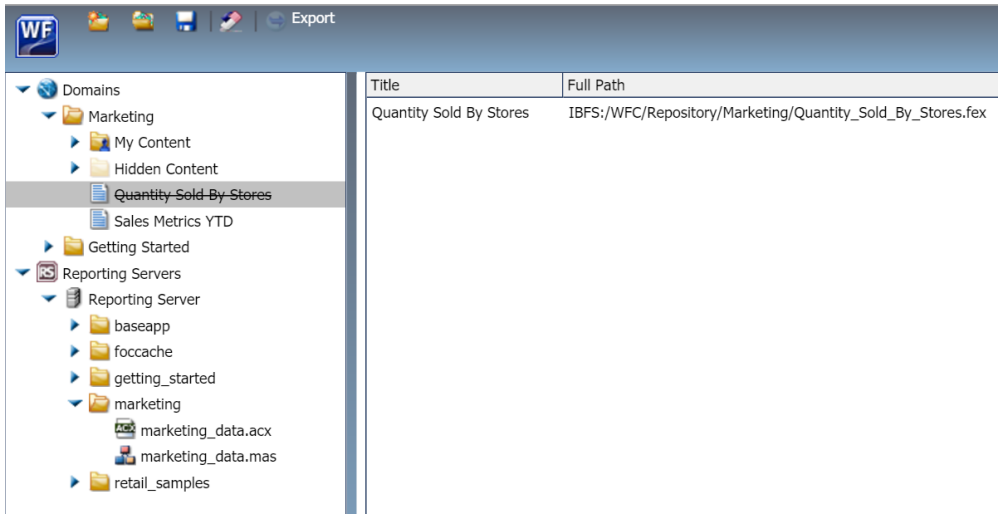
Procedure: **How to Access the Change Management Export Facility to Create a Scenario**

1. In the Resources tree, expand the *Change Management* node.
2. Right-click *Export* and click *New Scenario*, as shown in the following image.



3. You will then be prompted to enter the scenario name.

   The Scenario Creation dialog box appears, as shown in the following image.



Selecting Resources

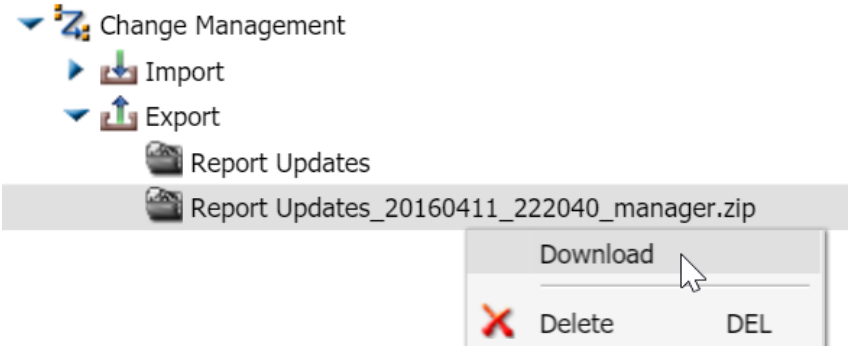
- You can select resources by dragging content from the Resources tree to the right pane. You can also right-click the content you want to move and select *Select With Subtree* or *Select Folder Only*.
  - *Select With Subtree* selects that folder and all subfolders.
  - *Select Folder Only* selects the specific folder, with no content. Typically, this is done to move rules on the folder.
- If a private resource is selected, the With Private Content check box is automatically selected and cannot be cleared.
- If a published folder is selected, you can include private content within that folder by selecting the With Private Content check box for that resource. This will export ALL of the private content in that folder and its subfolders, including user My Content folders, even if you do not have the privileges necessary to view that private content.

Note:

- If private content is selected, it will only be imported if the owner of that private content already exists in the target environment.
- If a subfolder is selected, its parent folder must exist in the target system.

Now that resources are selected, click *Save* to save the scenario.

4. Click *Export* to create a Change Package based on the saved scenario file. You can do this from within the interface or by right-clicking the scenario file item in the Resources tree.
5. From the Resources tree, refresh the Export node under Change Management. If you do not see the zip file, refresh the Export node again. You can now download the zip file, so that it can be moved to the target system, as shown in the following image.



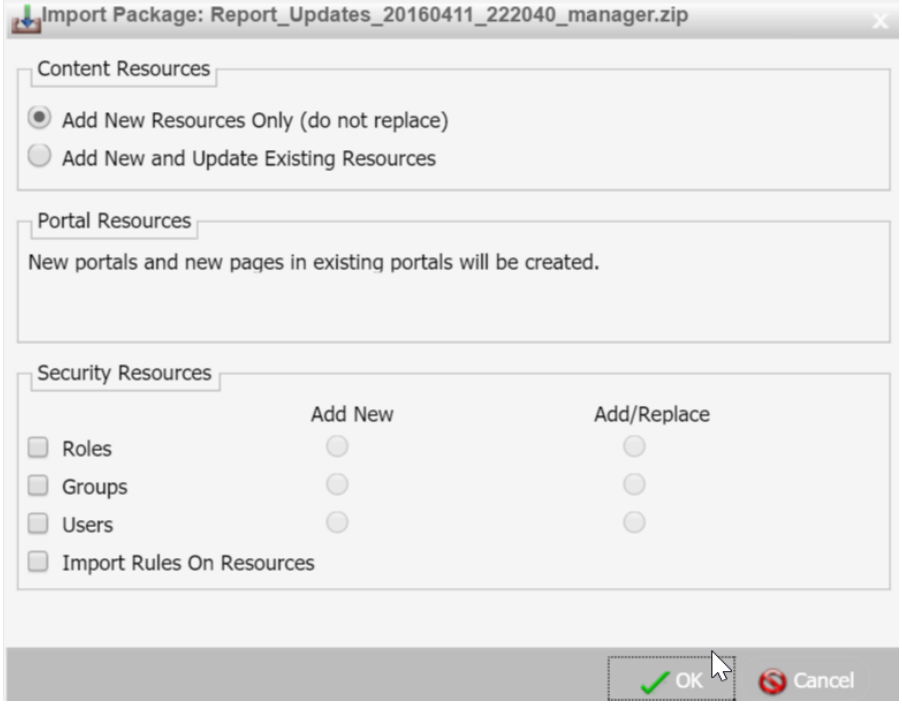
Procedure: How to Import a Change Management Package

Only members of the BUE Managers group can import Change Packages.

This procedure assumes that a change management zip package has been previously created on another system, the Manager is signed in to the target BUE environment, and the CM zip file is available to the Manager.

1. In the Resources tree, expand the *Change Management* node, then expand the *Import* node.
2. Right-click the package that you just uploaded and click *Import*.

   The Import Package dialog box appears, as shown in the following image.



3. Select one of the following options:

   Add New Resource Only (do not replace). This option will only add new resources to the target environment. For newly created items, the Created On and Last Modified On fields will be updated with the time at which they were imported. To view the Created On and Last Modified On fields, right-click an item and click *Properties*.

If an item already exists in the target environment but is also part of the change management export package, the target resource will be left alone and the Last Modified On field will not be updated.

Add New and Update Existing Resources. This option will add new resources to the target environment if they do not exist and update existing resources if they already exist. For newly created items, the Created On and Last Modified On fields will be updated with the time at which they were imported. For updated items, the Created On value for the target will be retained, but the Last Modified On field will be updated with the time at which it was imported.

The other options on this panel are not used in BUE and can be ignored.

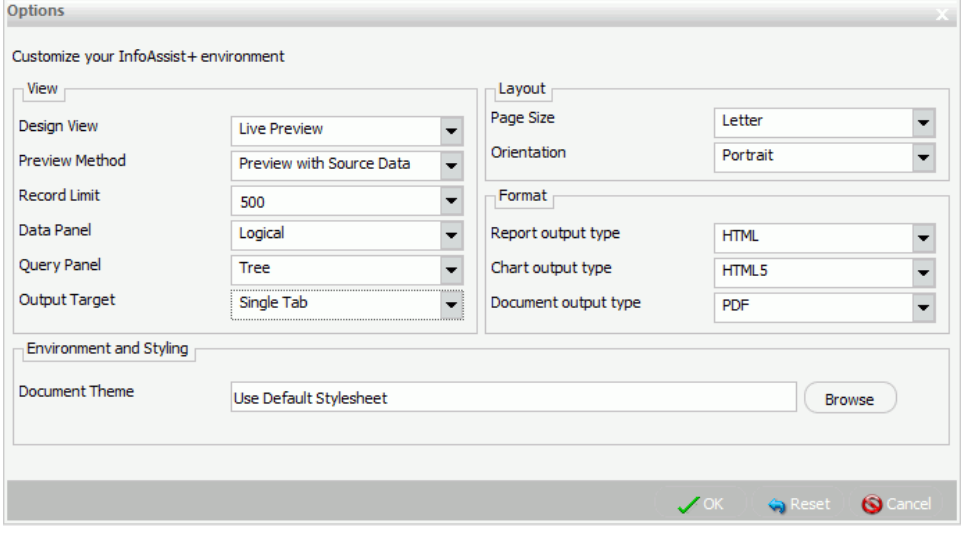
4. Click *OK*.

Changing InfoAssist+ User Preferences

You can change the default user preferences to customize the way that InfoAssist+ behaves when you create reports and generate output. The application theme, which is inherited from the BUE portal, customizes the InfoAssist+ interface, including all menus and dialog boxes.

You can style your reports by selecting a document theme independent from the interface. On the InfoAssist+ application main menu, click *Options*.

The Options window, as shown in the following image, opens to provide you with a user-friendly interface for customizing the InfoAssist+ application.



Note: If you make changes to the default selections in the Options dialog box, changes will take effect the next time InfoAssist+ launches.

If any of the options are unavailable, contact your administrator for assistance.

View

The View area provides settings for establishing the design view in which you will work, the type of data you will use when you preview your output, the limit you need to set on your record input, how your data and query panels will look, and the output target that you will use.

- **Design View.** Values are Live Preview and Query. Select *Live Preview* to activate the Preview Method drop-down menu. The default value is Live Preview.
- **Preview Method.** Values are Preview with Source Data and Preview with Sample Data. This menu becomes active when you select Live Preview from the Design View drop-down menu. The default value is Preview with Source Data.
- **Record Limit.** Values are All records, 1, 10, 50, 500, or you can type a numeric value directly in the menu. The default value is 500.
- **Data Panel.** Values are Logical, List, and Structured. The default value is Logical.
- **Query Panel.** Values are 2x2 (2 columns by 2 rows), 1x4 (1 column by 4 rows), and Tree. The default value is Tree.
- **Output Target.** Values are Single Tab, New Tab, Single Window, and New Window. The default value is Single Tab.

Layout

The Layout area provides settings for printing reports and charts.

- **Page Size.** Values are A4, A3, A5, Letter, Tabloid, and Legal. The default value is Letter.
- **Orientation.** Values are Portrait and Landscape. The default value is Portrait.

Format

The Format area provides settings for the output types for reports, charts, and documents.

- **Report output type.** Values are HTML, PDF, PowerPoint (pptx), Excel (xlsx), Excel (xlsx Formula), Excel, Excel (Formula), and active report. The default value is HTML.
- **Chart output type.** Values are HTML, HTML5, PDF, PowerPoint (pptx), Excel (xlsx), Excel, and active report. The default value is HTML5.

- **Document output type.** Values are HTML, PDF, PowerPoint (pptx), Excel (xlsx), Excel (xlsx Formula), Excel, Excel (Formula), and active report. The default value is active report.

Environment and Styling

The Environment and Styling area provides settings for styling reports and charts through the specification of a Document Theme.

You can use the default style sheet or select from a list of available themes. Click the *Browse* button to open the Templates - Browse predefined template files dialog box, in which you can search for an existing WebFOCUS StyleSheet. You can also click *Use Default Stylesheet* to revert back to the default style sheet.

Changing Global Preferences

You can change global preferences for InfoAssist+ through the Administration Console found on the BUE Portal.

Distributing the Quick Data Add-In File

WebFOCUS Quick Data add-in allows you to bring a large amount of enterprise information to the familiar Excel environment, and interact with this information without learning any additional software. You can install the WebFOCUS Quick Data Add-in on your desktop, and you can create and edit queries by accessing predefined data sources. You can save a query in an Excel document, and you can refresh it at any time.

Because all WebFOCUS connection and report information can be saved in an Excel workbook, users with the proper security and access rights can share spreadsheets throughout an organization. As a result, you spend less time recreating reports and more time analyzing information for effective decision-making.

Note: Quick Data is a WebFOCUS Business User Edition option, which requires a separate license and installation. For more information about licensing Quick Data, contact your Information Builders representative.

To distribute and enable the Quick Data Add-in in your environment, follow the procedures below.

Procedure: How to Distribute the Quick Data Add-in File

1. Copy the wfquickdata.xla add-in file and the configuration file, wfquickdata.cfg, located in one of the following directories:
   - For Windows, drive:\ibi\WebFOCUS_BUE82\WebFOCUS\utilities\quickdata

- For Unix, /ibi/WebFOCUS_BUE82/utilities/quickdata

2. Add the files to the following directory on the machines that use Quick Data.

   C:\Users*userid*\AppData\Roaming\Microsoft\AddIns\

   where:

   `userid`

   Is the name of the user logged on to the PC.

After the WebFOCUS Quick Data Add-in file is in the proper directory, you must open Excel and select the WebFOCUS Quick Data option in the Add-Ins dialog box, as described in the following procedure.

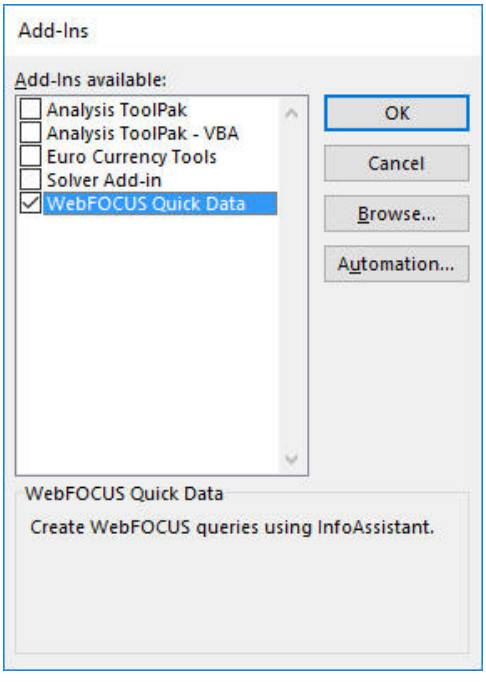
Note: If you already have Quick Data installed in your environment, be sure to beckup your existing wfquickdata.cfg file to preserve all your customizations. You can then copy your edits from the existing wfquickdata.cfg file to the new file.

Procedure: How to Enable the Quick Data Add-In in Excel 2016

Use the following steps to enable the Quick Data Add-in in Excel 2016:

1. Launch Microsoft Excel 2016.
2. Click the File tab, click *Options*, and then click the Add-Ins category.
3. From the Manage dialog box, select *Excel Add-ins*, and then click *Go*.

The Add-Ins dialog box opens, as shown in the following image.



Note: If WebFOCUS Quick Data is not listed in the Add-Ins dialog box, make sure that the add-in is installed and placed in the correct directory.

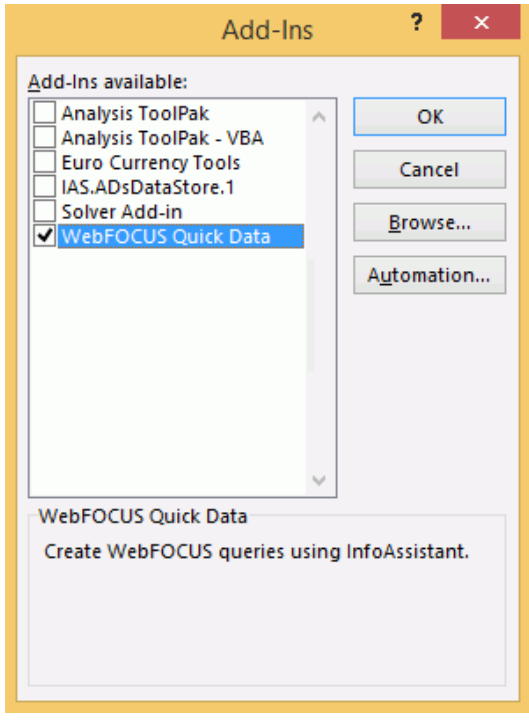
4. Select the WebFOCUS Quick Data check box and click *OK*.

Procedure: How to Enable the Quick Data Add-In in Excel 2013

Use the following steps to enable the Quick Data Add-In in Excel 2013:

1. Launch Microsoft Excel 2013.
2. Click the File tab, click *Options*, and then click the Add-Ins category.
3. In the Manage dialog box, select *Excel Add-ins*, and then click *Go*.

The Add-Ins dialog box opens, as shown in the following image.



Note: If WebFOCUS Quick Data is not listed in the Add-Ins dialog box, make sure that the add-in is installed and placed in the correct directory.

If the Quick Data Add-in was installed in a different directory, use the Browse button in the Add-Ins dialog box to locate it.

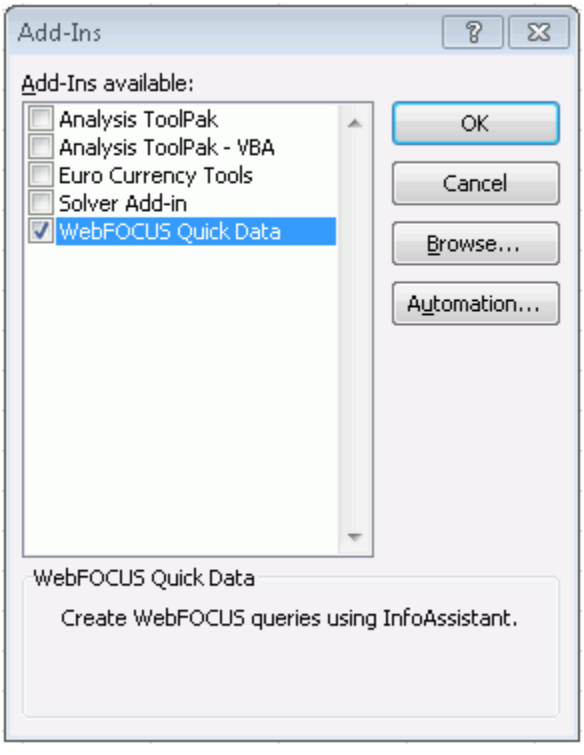
4. Select the WebFOCUS Quick Data check box and click *OK*.

Procedure: How to Enable the Quick Data Add-In in Excel 2010

Use the following steps to enable the Quick Data Add-In in Excel 2010:

1. Launch Microsoft Excel 2010.
2. Click the File tab, click *Options*, and then click the Add-Ins category.
3. In the Manage dialog box, click *Excel Add-ins*, and then click *Go*.

The Add-Ins dialog box opens, as shown in the following image.



Note: If WebFOCUS Quick Data is not listed in the Add-Ins dialog box, make sure that the add- in is installed and placed in the correct directory.

If the Quick Data Add-in was installed in a different directory, use the Browse button in the Add-Ins dialog box to locate it.

4. Select the WebFOCUS Quick Data check box and click *OK*.

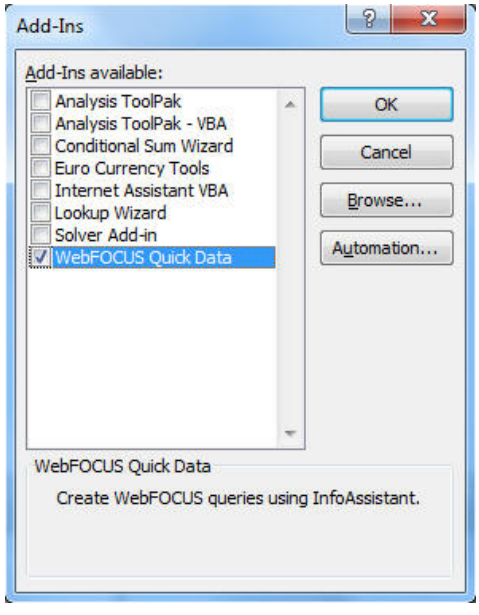
Procedure: How to Enable the Quick Data Add-In in Excel 2007

Use the following steps to enable the Quick Data Add-In in Excel 2007:

1. Launch Microsoft Excel 2007.
2. Click the Microsoft Office Button  in the top-left corner.
3. Click *Excel Options* and then click *Add-Ins* in the Excel Options dialog box.

4. From the Manage drop-down list, select *Add-ins*, and click *Go*.

   The Add-Ins dialog box opens, with WebFOCUS Quick Data listed as an add-in option, as shown in the following image.

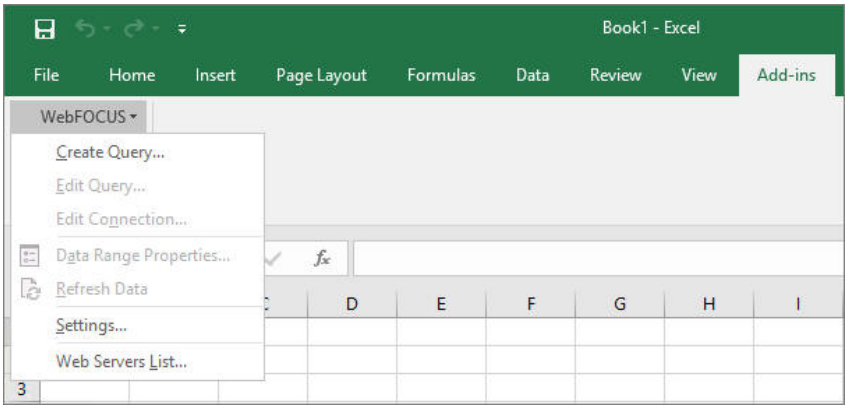


Note:

- If WebFOCUS Quick Data is not listed in the Add-Ins dialog box, make sure that the add-in is installed and placed in the correct directory.
- If the Quick Data Add-in was installed in a different directory, use the Browse button in the Add-Ins dialog box to locate it.

5. Select *WebFOCUS Quick Data*, and click *OK*.

A WebFOCUS menu opens in the Add-Ins tab. The following image shows an example of the WebFOCUS menu in Excel 2016.



WebFOCUS Quick Data Options

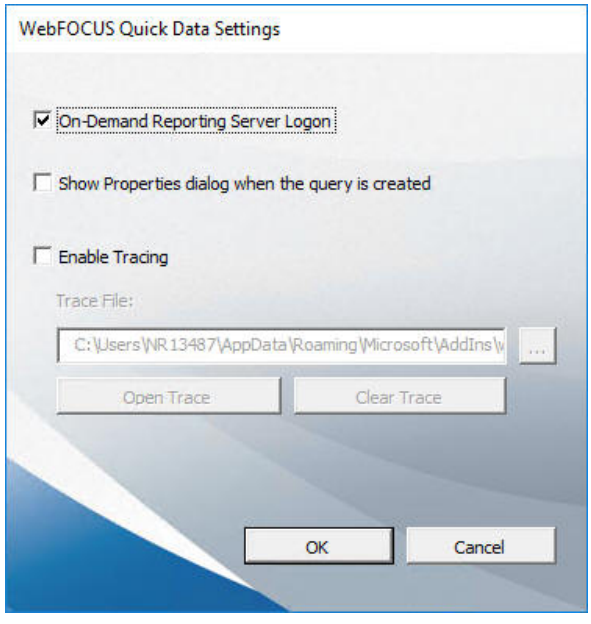
Once you have distributed the Quick Data Add-in, you can access the WebFOCUS Quick Data Options, which are described in this topic. Except for Settings and Web Servers List, these options are also available from Excel right-click context menus.

- **Create Query.** Available for new queries only, this option opens the Web Server Connection dialog box so that you can connect to WebFOCUS BUE. It continues by opening the Data Source Selection dialog box so that you can select a Master File. It then opens InfoAssist+, where you can create a query.
- **Edit Query.** Available for existing queries only, this option opens InfoAssist+, where you can edit a query.

  Edit Query is not enabled for password-protected cells.
- **Edit Connection.** Available for existing queries only, this option opens the Web Server Connection dialog box, where you can edit the connection settings including the Web Server URL, the HTML Alias, and the Client Path. The ability to edit connection information saves time when you are reusing reports and helps facilitate the sharing of workbooks across an organization.
- **Data Range Properties.** Available for existing queries only, this option opens the External Data Range Properties dialog box, where you can set Excel query properties.
- **Refresh Data.** Available for existing queries only, this option refreshes the data in the existing report query.

Refresh is not enabled for password-protected cells.

- **Settings.** This option opens the WebFOCUS Quick Data Settings dialog box, as shown in the following image.



The WebFOCUS Quick Data Settings dialog box provides the following settings:

- **On-Demand Reporting Server Logon.** This setting determines if the user will be prompted to log on to the Reporting Server the first time that a connection to the server is made during an Excel session (check this setting), or each time that a request is made to the Reporting Server during an Excel session (do not check this setting).
- **Show Properties dialog when the query is created.** When this setting is selected, a dialog box with options on how to insert data into Excel opens each time that a new query is executed.
- **Enable Tracing.** This option allows you to capture WebFOCUS Quick Data information in a trace file to troubleshoot communication problems and issues that may occur when you attempt to create and run report requests.

The captured information includes tasks performed by the tool when it attempts to connect to the web server and Reporting Server, when requests are made for data, and when data is retrieved. The default name of the trace file is wfquickdata.txt. It is created in the same directory as the WebFOCUS Quick Data Add-in file, for example:

```
C:\Users\user_id\AppData\Roaming\Microsoft\Addins\
```

Traces are captured for the duration of a single active Excel session. Tracing is automatically turned off when you close an Excel session. The trace file content is cumulative. Added to the file is trace information from each session in which tracing is enabled.

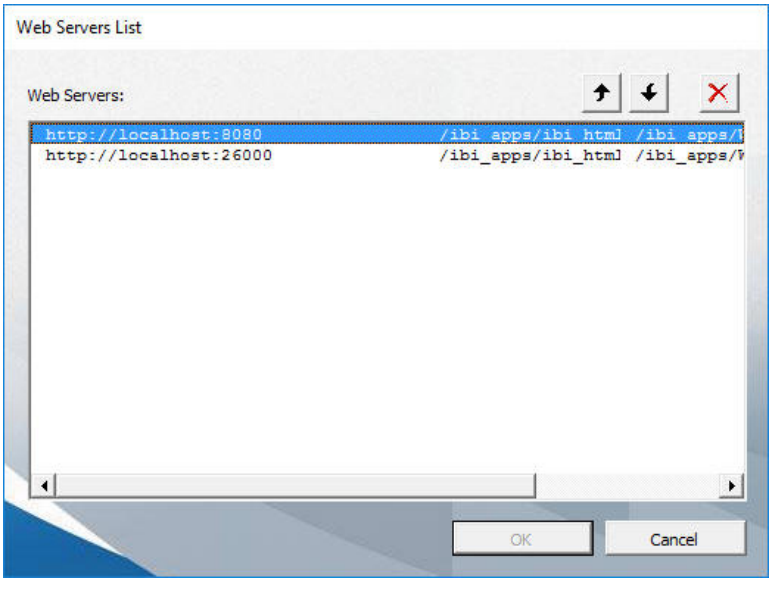
When you select Enable Tracing, the Trace File field is automatically populated with the full path to the trace file. The path includes the trace file name. You can change the location and name of the trace file by either typing the changes in this field, or by clicking the ellipsis and browsing to a new trace file location.

To view the current trace file, click *Open Trace*.

To delete the contents of the current trace file, click *Clear Trace*.

You can forward your trace file to Information Builders Customer Support Services (CSS) for analysis by the technical support team.

- **Web Servers List.** This option opens a dialog box that displays a list of the configured web servers, as shown in the following image. You can move the servers up or down in the list to change the order of appearance, and delete servers from the list.



Configuring a Default WebFOCUS BUE Environment

A configuration file is provided with the Quick Data add-in for the Administrator to use as a template when designing a default WebFOCUS BUE environment. The configuration file defines items such as the WebFOCUS BUE web server port number, alias, and client path.

Providing users with a default WebFOCUS BUE environment allows them to bypass the additional step of manually defining web server connection parameters.

The configuration file is named wfquickdata.cfg. It is originally located in the following directory: ..\ibi\WebFOCUS_BUE82\WebFOCUS\utilities\quickdata. After you have distributed the Quick Data Add-in in your environment, the configuration file is placed in the new directory, such as: C:\Users\userid\AppData\Roaming\Microsoft\AddIns.

The configuration file can contain multiple WebFOCUS configurations. Keep in mind that if the configuration file contains more than one WebFOCUS configuration, the last one appearing in the file is the configuration that is used when Quick Data is opened.

The configuration file provided as a template with the Quick Data add-in contains examples of configurations and instructions to help you create your own configuration. The following example displays a typical configuration:

```
SERVER_START
     PROTOCOL="http"
     HOST="localhost"
     PORT="26000"
     HTML_ALIAS="/ibi_apps/ibi_html"
     CLIENT_PATH="/ibi_apps/WFServlet.ibfs"
SERVER_END
```

Note:

- The use of double quotation marks around a parameter value, as shown in the example, is optional.
- Begin a comment line in the file with a number sign (#).

Use the following guidelines to create the configuration file:

- The configuration file must have the same name as the Quick Data Add-in file, and must have the extension .cfg, such as wfquickdata.cfg
- The configuration file must reside on the machine running the Quick Data Add-in, in the same directory as the .xla file.

- Each WebFOCUS configuration must begin with the delimiter, SERVER_START, and end with the delimiter, SERVER_END.
- Each configuration must contain the following parameters in order to connect to WebFOCUS BUE:
  - **PROTOCOL.** The protocol used in the environment running WebFOCUS BUE. If WebFOCUS BUE is running in a Secure Sockets Layer (SSL) environment, you must specify https as the protocol value. The default value is http.
  - **HOST.** The name of the server on which the WebFOCUS BUE web application is installed.
  - **PORT.** The port number of the application server on which WebFOCUS BUE is installed.
  - **HTML_ALIAS.** The alias of the web server or application server on which the WebFOCUS BUE static pages are located. The default value is /ibi_apps/ibi_html.

    Note: The leading slash is required.
  - **CLIENT_PATH.** The path to the WebFOCUS BUE Servlet, as defined in the WebFOCUS BUE web application file, web.xml. The default value is

    `/ibi_apps/WFServlet.ibfs`

    where:

    `/ibi_apps`

    Is the default context root of the WebFOCUS BUE web application. The leading slash is required. You can configure this value.

    `WFServlet.ibfs`

    Is the name of the WebFOCUS BUE Servlet.

Index

R

S

U

W

Z