

WebFOCUS

Setting Up Your Environment
Release 8.2 Version 03

April 13, 2018

Active Technologies, EDA, EDA/SQL, FIDEL, FOCUS, Information Builders, the Information Builders logo, iWay, iWay Software, Parlay, PC/FOCUS, RStat, Table Talk, Web390, WebFOCUS, WebFOCUS Active Technologies, and WebFOCUS Magnify are registered trademarks, and DataMigrator and Hyperstage are trademarks of Information Builders, Inc.

Adobe, the Adobe logo, Acrobat, Adobe Reader, Flash, Adobe Flash Builder, Flex, and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Due to the nature of this material, this document refers to numerous hardware and software products by their trademarks. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies. It is not this publisher's intent to use any of these names generically. The reader is therefore cautioned to investigate all claimed trademark rights before using any of these names other than to refer to the product described.

Copyright © 2018, by Information Builders, Inc. and iWay Software. All rights reserved. Patent Pending. This manual, or parts thereof, may not be reproduced in any form without the written permission of Information Builders, Inc.

Contents

1. Setting Up Your Environment	9
Using the Administration Console	9
Opening the Administration Console.....	9
Using the Administration Console Menu Bar.....	11
Using the Licenses Menu.....	11
Reviewing Client License Information.....	11
Reviewing User Audit Information.....	13
Reviewing Third Party Licenses.....	15
Clearing the Cache.....	16
Closing the Administration Console.....	16
Opening Administration Console Help.....	16
Configuring Security.....	16
Using Internal Security.....	17
Using External Security.....	21
Understanding Custom Settings.....	21
Understanding NLS Settings.....	23
Customizing the Dynamic Language Switch.....	25
Understanding Redirection Settings.....	27
Redirecting and Saving File Output.....	27
Saving GRAPH (PNG, SVG, GIF, JPEG, or JPG) Requests.....	29
Working With HTML5 Chart Extensions.....	30
Understanding HTML5 Chart Extension Entries.....	31
Understanding the HTML5 Chart Extensions Enable/Enabled Check Box.....	31
Uploading Additional HTML5 Chart Extensions Using the Upload and Install Extensions Page.....	32
Changing Application Settings	37
Changing Client Settings	41
InfoAssist Properties.....	41
Understanding InfoAssist Auto Drill Properties.....	50
Reporting Server Configuration Settings.....	52
Using the ReportCaster Console	56
Using the ReportCaster Console.....	56

Server Status.....	58
Viewing the Distribution Server Status.....	59
Separate Job Queues for Each Data Server.....	62
Viewing, Stopping, Suspending, and Restarting the Distribution Server.....	62
Job Status.....	63
Job Log.....	64
ReportCaster Configuration.....	65
Configuration Icons.....	65
Configuration Tab Folders.....	67
Changing Configuration Settings.....	68
Changing Default User IDs.....	69
Distribution Server Settings.....	69
Restricting Distribution Server Console Access to an IP Address List.....	72
General Preferences.....	74
Specifying Schedule Format Settings.....	75
Specifying Schedule Distribution Method Settings.....	78
Email Distribution.....	80
Validating Allowed Email Domains and Addresses.....	85
Examples of Invalid Email Addresses and Domains.....	86
Invalid Email Addresses.....	87
Invalid Email Domains.....	87
Email Domain and Address Restrictions.....	87
The Email Selection Dialog Box.....	88
A List of Only Email Addresses.....	89
A List of Email Domains and Addresses.....	90
A List of Only Email Domains.....	91
Notification.....	92
Zip Settings.....	95
Other Schedule Defaults.....	97
Log Purge.....	98
LDAP Setting.....	99
Data Servers Settings.....	102
Configuring Reporting Servers With ReportCaster.....	108

Using Blackout Periods.	110
Configuring Weekly Blackout Periods.	115
Weekly Blackout Period Settings.	116
Configuring Monthly Blackout Periods.	118
Monthly Blackout Period Settings.	119
Configuring Single Day Blackout Periods.	121
Single Day Blackout Period Settings.	121
Configuring Every Day Blackout Periods.	122
Every Day Blackout Period Settings.	123
Importing Blackout Periods.	125
Viewing Blackout Period Import File Format.	127
Single Date Blackout Period Import File Entry Layout.	127
Weekly Blackout Period Import File Entry Layout.	127
Monthly Blackout Period Import File Entry Layout.	128
Every Day Blackout Period Import File Entry Layout.	128
Extracting Blackout Period Profiles.	134
Extracting File Formats.	134
Global Updates.	136
Purge Logs.	139
Working With Domains.	140
Managing Domain Users.	141
Granting Access to a Domain.	141
Managing Domain Private Resources.	142
Deleting Domains.	142
Managing Domain Users After Deleting a Domain.	143
Working With Folders.	143
Managing Users.	148
Understanding Users.	149
Understanding User Name Requirements.	149
Importing Users.	152
Understanding User Import File Layout and Format Requirements.	152
Understanding User Record Field Format Requirements.	153
Understanding the Group Membership Report.	157

Managing Groups	159
Understanding Groups.....	160
Creating Groups From Domains.....	160
Managing Private Resources	162
Authenticating Users to Your Active Directory	162
Configuring Active Directory/LDAP Authentication.....	163
Creating User Accounts When WebFOCUS Business User Edition is Configured for Active Directory Authentication.....	166
Configuring WebFOCUS Business User Edition for SSL	167
Establishing the Self-Signed Certificate as a Trusted Certificate.....	169
Importing the Trusted Certificate into the Keystore.....	169
Updating the Connector Protocols in the Tomcat Server.xml File.....	170
Creating a Change Management Package	171
Working With CM Zip Files.....	171
Changing InfoAssist User Preferences	178
View.....	178
Layout.....	179
Format.....	179
Environment and Styling.....	179
Changing Global Preferences.....	181
Configuring Hyperstage	181
Hyperstage Overview.....	181
Hyperstage and PostgreSQL.....	181
Configuring the Hyperstage Database.....	182
Configuring Hyperstage.....	182
Configuration Tips and Examples.....	183
Using the Hyperstage Database Beyond WebFOCUS.....	184
Starting and Stopping the Hyperstage Server	184
Quick Copy For Hyperstage Using Extended Bulk Load Utility.....	186
Managing Hyperstage Tables.....	187
About the Hyperstage Database Files.....	187
About Supported Data Types.....	188
Creating and Dropping Tables.....	189

Character Set Support.....	190
Supported Character Sets.....	190
Collations and Comparisons.....	191
Padding.....	192
Hyperstage Backup and Recovery.....	192
Backup Procedure.....	192
Restore Procedure.....	193
Functions and Operators.....	193
Hyperstage Optimizer Supported Functions and Operators.....	193
Comparison Functions and Operators.....	193
Control Flow Functions.....	193
String Functions.....	193
Numeric Functions.....	194
Date and Time Functions.....	195
Text Search and Other Functions.....	196
Group By Aggregate Functions.....	196
Hyperstage Data Tools.....	197
Hyperstage Consistency Manager.....	197
Hyperstage Consistency Manager Tests.....	197
About Rebuilding or Repairing Knowledge Nodes.....	200
About Cleanup Procedures.....	201
Distributing the Quick Data Add-In File	201
WebFOCUS Quick Data Options.....	206
Configuring a Default Business User Edition Environment.....	208
Managing the Server or Global Profile	210

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](#)
 - ☐ [Changing Application Settings](#)
 - ☐ [Changing Client Settings](#)
 - ☐ [Using the ReportCaster Console](#)
 - ☐ [Working With Domains](#)
 - ☐ [Working With Folders](#)
 - ☐ [Managing Users](#)
 - ☐ [Managing Groups](#)
 - ☐ [Managing Private Resources](#)
 - ☐ [Authenticating Users to Your Active Directory](#)
 - ☐ [Configuring WebFOCUS Business User Edition for SSL](#)
 - ☐ [Creating a Change Management Package](#)
 - ☐ [Changing InfoAssist User Preferences](#)
 - ☐ [Configuring Hyperstage](#)
 - ☐ [Distributing the Quick Data Add-In File](#)
 - ☐ [Managing the Server or Global Profile](#)
-

Using the Administration Console

The Administration Console contains the settings that configure WebFOCUS Business User Edition, 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 installation, it is available only to those users with the privileges to update or reconfigure system settings. In WebFOCUS 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.

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 click *Run WebFOCUS Business User Edition*.
3. On 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, on the Menu bar, click *Administration*, and then click *Administration Console*.

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 Business User Edition.

`context`

Is the local address for WebFOCUS Business User Edition. 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.

Note: To display the Administration Console using a different language, on the Sign in page, click *Choose language*, and then click the language you want to use in the language list.

Using the Administration Console Menu Bar

The Administration Console menu bar appears above the Administration Console tab display. The commands and features it contains 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 third-party software packaged with WebFOCUS Business User Edition.

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.

The License Information dialog box 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. By default, a warning message for the client license key expiration date begins to appear fourteen (14) days before the actual expiration date. This message displays the expiration date and the number of days remaining until that date. The License Expiration Warning message appears only to Administrators during sign on, and it is written to the event.log file located in the logs directory of the WebFOCUS Business User Edition installation.
- ☐ **User Licenses.** The total number of available user licenses and the number of licenses used for each user category. For example:
 - ☐ Total Named Users
 - ☐ Portal Users
 - ☐ InfoAssist Users

- ☐ **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 Business User Edition 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:

- ☐ **Total Users.** The total number of named users in the Repository.
- ☐ **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 product 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 Information 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	
Product Edition	The name of the current product edition.
License Key	Displays your current license key.
User License	Displays the user license types that are authorized under your current license key. This can include the following: <div><input type="checkbox"/> Total Named Users</div> <div><input type="checkbox"/> Portal Users</div> <div><input type="checkbox"/> InfoAssist Users</div>
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	

License Analysis	
Group Path	<p>Displays the Groups stored in the repository. The following groups are created by the WebFOCUS Repository Creation utility, by default:</p> <ul style="list-style-type: none"> <input type="checkbox"/> /EVERYONE <input type="checkbox"/> /Getting_Started <input type="checkbox"/> /Managers <input type="checkbox"/> /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.
Groups Summary	<p>Displays counts for the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Number of groups <input type="checkbox"/> Number of groups with license types <input type="checkbox"/> Number of groups with no license types <input type="checkbox"/> Number of groups with changed user types <input type="checkbox"/> Number of groups with cleared user types <input type="checkbox"/> Number of groups with unchanged types
Analysis of Users	
User Name	<p>Displays the users stored in the repository. The following users are created by the WebFOCUS Repository Creation utility, by default:</p> <ul style="list-style-type: none"> <input type="checkbox"/> manager
License Type(s)	Displays the license types assigned to each user.

License Analysis	
# 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: <ul style="list-style-type: none"> <input type="checkbox"/> Number of users <input type="checkbox"/> Number of users with license types <input type="checkbox"/> Number of users with no license types <input type="checkbox"/> Number of users with changed user types <input type="checkbox"/> Number of users with cleared user types <input type="checkbox"/> Number of users with unchanged types

Procedure: How to Run the User Audit from the Administration Console

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:

- ☐ **Description.** The name or brief description of the third-party application.
- ☐ **Version.** The version number of the third-party application.
- ☐ **File(s).** The names of all files that comprise the third-party application.
- ☐ **License.** The name of the license that permits the use of the third-party application.
- ☐ **Third-Party Links.** The URL from which the third-party application was obtained.
- ☐ **Release.** The number of the WebFOCUS Release to which the third-party application was first applied. There is one entry for each release in which an updated version of the third-party application was applied.

- ❑ **Update History.** The name and version number of the third-party application jar file. There is one entry for each release in which an updated version of the third-party application jar file was applied.
- ❑ **Date.** The date and time on which the third-party application update was applied in YYYY-MM-DD and HH:MM:SS format. There is one entry for each third-party jar file update.

The WebFOCUS Business User Edition 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 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 Business User Edition repository, or externally in a Microsoft Active Directory or an LDAP directory that is not part of the application. You can use either the Internal page or the External page on the Security tab in the Administration Console. To configure settings for internal security, use the settings in the Internal page. To configure a connection to an external Microsoft Active Directory or LDAP Directory, use the External page.

Internal authentication and authorization is enabled by default.

Using Internal Security

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

Sign In Settings (Enable Sign In Settings)

Determines the default values assigned to the Sign In Settings on the Internal Security Page.

This check box is cleared (False), by default. Sign In Settings are inactive and unavailable, and display a value of 0.

When this check box is selected (True), Sign In Settings are activated, automatically assigned a set of pre-configured values, and made available for updates. To deactivate an individual setting while this check box is selected, type or select zero (0). When this check box is later cleared, all values assigned to the Sign In Settings return to 0, and the settings are deactivated.

This setting does not affect the value or availability of the Password Expiration Result options.

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. When the Sign In Settings check box is cleared, the default value is 0, which allows unlimited attempts. When the Sign In Settings check box is selected, the default value is 5, and managers can type or select an alternative value. To deactivate this setting when the Sign In Settings check box is selected, type or select 0.

Lockout Duration (Minutes) (IBI_Account_Lockout_Duration)

Specifies the number of minutes before the status of an account changes from locked to active. When the Sign-in Settings check box is cleared, the default value is 0 (off). When the Sign In Settings check box is selected, the default value is 3 minutes, and managers can type or select an alternative value. To deactivate this setting when the Sign In Settings check box is selected, type or select 0.

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. When the Sign-in Settings check box is cleared, the default value is 0 (off). When the Sign In Settings check box is selected, the default value is 3 minutes, and managers can type or select an alternative value. To deactivate this setting when the Sign In Settings check box is selected, type or select 0.

Days Until Password Expires (IBI_Password_Expire)

Specifies the number of days that a password will remain active. When Sign-in Settings is cleared, the default value is 0, which prevents passwords from expiring. When Sign In Settings is selected, the default value is 90 days. Once the password has expired, the user must take the action specified by the Password Expiration Result (IBI_Password_Expire_Action) setting, and managers can type or select an alternative value. To deactivate this setting when the Sign In Settings check box is selected, type or select 0.

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. When Sign-in Settings is cleared, the default value is 0, which provides no warning. When Sign In Settings is selected, the default value is 75 days. This value should be less than or equal to the value assigned to the Days Until Password Expires (IBI_Password_Expire) setting, and managers can type or select an alternative value. To deactivate this setting when the Sign In Settings check box is selected, type or select 0.

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 an administrator resets the password (DISABLE-USER).*

Enable Password Complexity (IBI_Password_Complexity)

Determines the default values assigned to the Password Settings on the Internal Security Page.

This check box is cleared (False), by default. All of the Password Settings are inactive and unavailable, and display a value of 0.

When this check box is selected (True), all of the Password Settings are activated and available for updates. WebFOCUS Business User Edition automatically assigns a pre-configured set of values to them.

When this check box is later cleared, all values assigned to the Password Settings return to 0, and the settings are deactivated.

If this check box is selected (True), passwords also must:

- ☐ Not contain the user account name or parts of the full name of the user that exceed five 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 al 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. When Enable Password Complexity is cleared, the default value is 0 characters. When the Enable Password Complexity check box is selected, the default value is 6 characters. To deactivate this setting when the Enable Password Complexity check box is selected, type or select 0.

Password Reuse (IBI_Password_Reuse)

Specifies the number of recent passwords that cannot be reused. If Password Reuse is set to 6, for example, WebFOCUS Business User Edition will track the 6 most recent password changes and prevent you from reusing them when creating a new password. When the Enable Password Complexity check box is cleared, the default value is 0 changes, and users can re-use any previously-assigned password. When the Enable Password Complexity check box is selected, the default value is 2 changes. To deactivate this setting when the Enable Password Complexity check box is selected, type or select 0.

***Procedure:* How to Configure Sign In Settings**

1. Sign in as a Manager.
2. In the Administration Console, click the *Security* tab, and on the Security page, under the Security Configuration folder, click *Internal*.
3. Select the *Sign In Settings* check box.

The Internal page displays the following default values:

- ☐ Maximum Sign-in Attempts – 5
- ☐ Lockout Duration (Minutes) – 3
- ☐ Lockout Duration Reset (Minutes) – 3

- ☐ Days Until Password Expires – 90
- ☐ Days Until Password Expiration Warning – 75
- 4. To change the default value assigned to any of these settings, type or select an alternate value in any of these boxes.
- 5. To clear all settings, clear the *Sign In Settings* check box. All values automatically return to 0.
- 6. In the Password Expiration Result section, accept the default option *To force users with expired passwords to change their passwords before signing in*, or click the alternative option *Change the status of users with expired passwords to inactive. Such users cannot sign in until an administrator resets the password*.
- 7. Continue with any other Internal Security page updates or save your changes.

Procedure: How to Configure Password Settings

1. Sign in as a Manager.
2. In the Administration Console, click the *Security* tab.
3. On the Security page, under the Security Configuration folder, click *Internal*.
4. Select the *Enable Password Complexity* check box.

The Internal page displays the following default values:

- ☐ Minimum Password Length – 6
- ☐ Password Reuse – 2
- 5. To change the default value assigned to any of these settings, type or select an alternate value in either of these boxes.
- 6. To clear all settings, clear the *Enable Password Complexity* check box. All values automatically return to 0.
- 7. Continue with any other Internal Security page updates or save your changes.

Procedure: How to Save Internal Security Page Configuration Updates

1. When all of your Internal Security Page Configuration updates are complete, click *Save*.
2. When you receive a confirmation message, click *OK*.
3. When you receive a message to clear the cache, click *OK*.
4. In the Administration Console menu bar, click *Clear Cache* and, when you receive a confirmation message, click *OK*.

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 Business User Edition.

Enable External Security

When you select this check box, internal security settings are overridden. WebFOCUS Business User Edition 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 WebFOCUS Business User Edition.
- ☐ **Custom Java Plug-In.** This value is not used with WebFOCUS Business User Edition.

Understanding Custom Settings

The Custom Settings page allows you to customize WebFOCUS Business User Edition by typing customized values for standard settings.

When you save updates to settings that you type into the Customized Setting text box, they are transferred to the site.wfs file, in the following location:

```
drive:\ibi\WebFOCUS_BUE82\WebFOCUS\client\wfc\etc\
```

When you use this page to assign new values to settings, they override the default values assigned to them. These overrides are carried over as you upgrade to new versions.

After you save a custom setting, the text continues to display on this page. You can use comments to identify specific updates and additional information about them.

Procedure: How to Configure Custom Settings

Only a manager can configure settings on the Custom Settings page.

1. In the Administration Console, on the Configuration tab, click *Custom Settings*.
2. Under the final comment statement at the top of the Custom Settings text box, or the most recent custom setting entry, type the variables, settings, commands, or comments that comprise the custom settings.

Use the format required by the application or operating system that will execute the command.

To help track changes to custom settings, use comments to identify and separate individual changes.

3. To store your custom settings in an encrypted format, select the *Encrypt* check box.

Note: Even when you select this check box, settings continue to appear in an unencrypted format in the Custom Settings text box.

4. When your configuration is complete, click *Save*.
5. When you receive a confirmation message, click *OK*.
6. When the Custom Setting page clears, click *Custom Settings* under the Application Settings folder to see your updated comments, settings, or commands in the Custom Settings text box.

Procedure: How to Configure Collation Sequence Settings

Only a manager can configure settings on the Custom Settings page.

1. In the Administration Console, on the Configuration tab, click *Custom Settings*.
2. Under the final comment statement at the top of the Custom Settings text box, type the comment line:

```
# Collation Sequence Settings
```

3. Under the comment line, type the command:

```
_site_profile=&_site_profile\nSET COLLATION={BINARY|SRV_CI|SRV_CS|  
CODEPAGE}
```

where:

BINARY

Bases the collation sequence on binary values.

SRV_CI

Bases the collation sequence on the LANGUAGE setting, and is case-insensitive.

SRV_CS

Bases the collation sequence on the LANGUAGE setting, and is case-sensitive.

CODEPAGE

Bases the collation sequence on the code page in effect, and is case-sensitive.

CODEPAGE is the default value. In most cases, CODEPAGE is the same as BINARY.

The only differences are for Danish, Finnish, German, Norwegian, and Swedish in an EBCDIC environment.

4. To store your custom settings in an encrypted format, select the *Encrypt* check box.

Note: Your settings will continue to appear in the Custom Settings text box in an unencrypted format.

5. When your configuration is complete, click **Save**.
6. When you receive a confirmation message, click **OK**.
7. When the Custom Setting page clears, click *Custom Settings* under the Application Settings folder to see your updated comments, settings, or commands in the Custom Settings text box.

Understanding NLS Settings

You can use the Administration Console to configure National Language Support and enable the Dynamic Language Switch.

Separate message files exist for every national language that WebFOCUS Business User Edition supports. If you want to customize the set of characters used in your report output, you must select the code page for every language you use.

These settings do not carry over during updates. You must repeat this customization step for each new release that you install.

Procedure: How to Configure National Language Support

1. In the Administration Console, on the Configuration tab, click *NLS Settings*.
2. On the NLS settings page, click the option for the operating system on which WebFOCUS Business User Edition resides.

The list adjusts to display the code pages that are available to the selected operating system.

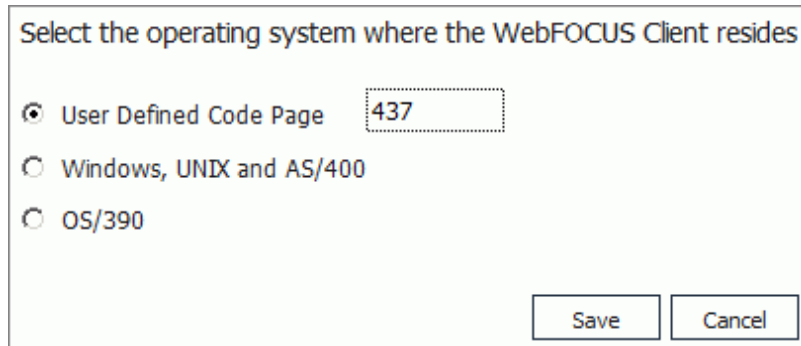
3. From the list, click a code page that configures the client for the correct display of report output in the browser.

Tip: The language selected for the Client usually corresponds to the language selected for the Server from the Reporting Server Console.

If the language chosen from the Reporting Server Console does not appear in the list, click *User Defined Code Page* and type the number of the user-defined code page.

Use this option, for example, when the server adds support for a new code page that is not yet reflected in the client software.

In the following sample configuration window, the administrator specified code page 437.



Select the operating system where the WebFOCUS Client resides

☒ User Defined Code Page 437

☐ Windows, UNIX and AS/400

☐ OS/390

Save Cancel

Unicode (UTF-8) is available for the Windows, UNIX, or AS/400 operating systems.

4. Click Save to store your NLS settings.

The Administration Console generates and updates the client configuration file (nlscfg.err), found in *drive:\ibi\WebFOCUS_BUE82\WebFOCUS\client\home\etc*, with the CODE_PAGE setting. Note that if you click NLS Settings again, your new setting is highlighted as the active code page.

Reference: Client Code Page Settings

The following code page settings are available:

- ☐ * 137 - U.S. English/Western European
- ☐ 874 - Thai
- ☐ * 942 - Japanese
- ☐ * 946 - Simplified Chinese
- ☐ 949 - Korean
- ☐ 1250 - Eastern European
- ☐ 1251 - Russian
- ☐ * 1252 - Western European
- ☐ 1253 - Greek
- ☐ 1254 - Turkish

- ☐ 1255 - Hebrew
- ☐ 1256 - Arabic
- ☐ 1257 - Baltic
- ☐ * 10942 - Japanese EUC
- ☐ * 10948 - Traditional Chinese
- ☐ * 65001 - Unicode (UTF-8)

Note: Only those code page settings marked with an asterisk are fully supported in the current release.

Customizing the Dynamic Language Switch

You can customize the languages that are made available on the Sign in pages by activating the Dynamic Language Switch.

Procedure: How to Customize the Dynamic Language Switch

1. In the Administration Console, on the Configuration tab, under the Application Settings folder, click *Dynamic Language Switch*.

The Dynamic Language Switch page opens with a list of the languages made available by the code page selected in the NLS Settings page. By default, the Enable Dynamic Language check box is unselected, and all of the language check boxes are deactivated.

The Dynamic Language Switch page also shows the Client Code Page setting specified in [How to Configure National Language Support](#) on page 23.

2. Select the *Enable Dynamic Language* check box to activate the check boxes for all of the available languages displayed in the panel, as shown in the following image:

Client Code Page: 65001 - Unicode (UTF-8)

☒ Enable Dynamic Language

<input checked="" type="checkbox"/>	Locale	Language Code
<input checked="" type="checkbox"/>	Chinese - Simplified GB	zh
<input checked="" type="checkbox"/>	Chinese - Traditional Big-5	tw
<input checked="" type="checkbox"/>	English	en
<input checked="" type="checkbox"/>	French - Canadian	fc
<input checked="" type="checkbox"/>	French - Standard	fr
<input checked="" type="checkbox"/>	German	de
<input checked="" type="checkbox"/>	Italian	it
<input checked="" type="checkbox"/>	Japanese	ja
<input checked="" type="checkbox"/>	Portuguese - Brazilian	br
<input checked="" type="checkbox"/>	Spanish	es

Selecting the Enable Dynamic Language check box and one or more languages activates the display of the Select Languages button on all of the Sign in pages. It also activates the Language menu on the portal Menu bar.

3. Select the check box next to the Locale heading if you want all of the languages to appear in the Select Languages list on the Sign in pages and in the Language menu.

OR

Clear the check box next to the Locale heading and select the individual check boxes next to the individual languages that you want to appear on the Sign in pages and in the Language menu.

4. Click Save.

Note: To remove individual languages from the Select Languages drop-down list on the Sign in pages, clear the check boxes next to the languages you want to remove.

Understanding Redirection Settings

Redirection settings specify the way in which output files using a specific file extension are handled. You can review these settings through the Redirection Settings page of the Administration Console Configuration tab. Each entry in the page identifies an output file format by its WebFOCUS Extension, Content Type, File Format, Server Extension, Client Extension, and IBFS File Format, as shown in the following image.

Redirection Settings

WebFOCUS Extension	Content Type	Format	Redirect	Server Extension	Save Report	Client Extension	IBFS Format
.wp	text/plain	ascii	no	N/A	no	.wp	ascii
.xht	application/vnd.ms-excel	ascii	no	XHT	yes	.xls	ascii
.xls	application/vnd.ms-excel	binary	yes	EXCEL	no	.xls	binary
.xism	application/vnd.ms-excel.sheet.macroEnabled.12	binary	no	XLSM	yes	.xism	binary
.xlsx	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	binary	no	XLSX	yes	.xlsx	binary
.xltm	application/vnd.ms-excel.template.macroEnabled.12	binary	no	XLTM	yes	.xltm	binary
.xltx	application/vnd.openxmlformats-officedocument.spreadsheetml.template	binary	no	XLTX	yes	.xltx	binary
.xmh	application/vnd.ms-excel	ascii	no	XMH	yes	.xls	ascii
.xml	text/xml	ascii	no	XML	no	.xml	binary
.zip	application/zip	binary	no	ZIP	yes	.zip	binary

Save Cancel ☐ Encrypt

Note: This image displays the lower half of the page to show file extensions with varying values in the Redirect and Save Report fields.

The mime.wfs file, located in the directory *drive:\ibi\WebFOCUS_BUE82\WebFOCUS\client\wfc\etc* or *drive:\ibi\WebFOCUS_BUE82\WebFOCUS\client\home\etc* contains information about format types available with WebFOCUS. When you open the Redirection Settings page, WebFOCUS retrieves redirection settings from the mime.wfs file and displays them on the Redirection Settings page. When you save changes to these settings, WebFOCUS transfers them from the Redirection Settings page to the mime.wfs file.

Before making any changes to the Redirection Settings, you must assess the impact they will have on the applications and user experience within your organization. If you require further assistance, consult Customer Support Services.

Redirecting and Saving File Output

On the Redirection Settings page, values in the Redirect and Save Report settings determine whether the output from a request is stored in a temp folder file during processing, and whether a name is to be assigned to that file automatically. The combination of values assigned to these two settings determines the way in which output from requests is to be displayed and saved.

The Redirect setting allows you to specify if the output from a request should be saved to a file in the temp folder located under the WebFOCUS BUE client directory.

- ☐ If the value in the Redirect setting is yes, the output is saved to a file in the temp folder, where a name can be assigned to it, as directed by the value assigned to the Save Report setting.
- ☐ If the value in the Redirect setting is len, the output is saved to a file in the temp folder only if it exceeds the value assigned to the IBIWF_sendbufsize setting, which, by default, is 16384 bytes. Any output that must be saved to a file in the temp folder is then sent to the browser without an additional HTTP call.
- ☐ If the value in the Redirect setting is no, output is processed as directed by the value assigned to the Save Report setting.

The Save Report setting allows you to specify if report files should be assigned names automatically when they are created.

- ☐ If the value in the Save Report setting is no, the report, chart, or other output opens directly in the Browser or application without prompting users to open or save it. Users still have the option to save the report after it is opened. A randomly-generated name is assigned to the report output file regardless of whether the request originated from the Resources tree, from InfoAssist, or from some other application tool.
- ☐ If the value in the Save Report setting is yes, the report, chart, or other output is saved to a file in the temp folder, as follows:
 - ☐ If the report request specifies an output file name, it is assigned to the output file. Then the browser makes an HTTP call to retrieve the temporary stored output file, and prompts the user to open, save, or cancel it. The output file name appends the date and time at which the file was created only if the request also includes a PCHOLD AS statement that captures this information.
 - ☐ If the report request does not specify a file name:
 - ☐ If you run the request from an item in the Resources tree, the name value of that item is assigned to the request output file, and the date and time that the file was created is automatically added to the file name.

Note: The name value of an item appears on the Properties panel in the Name field.

- ❑ If you run the request from a tool such as InfoAssist, a randomly-generated name is assigned to the output file, and the date and time that the file was created is automatically added to the file name.

Procedure: How to Change Redirection Settings

Before changing Redirection Settings, consult with a system or network administrator to assess the impact of your proposed changes on the applications involved and on the user experience within your organization. If you require further assistance, consult with Customer Support Services.

1. In the Administration Console, on the Configuration tab, click *Redirection Settings*.
2. In the Redirect list:
 - a. Click *yes* to redirect the output to a temporary directory for files using the specified extension.
 - b. Click *no* to allow the output to be processed as directed by the value assigned to the Save Report setting.
 - c. Click *len* to redirect report content to a temporary directory only when it exceeds the buffer size defined in the IBIWF_sendbufsize setting.
3. In the Save Report list:
 - a. Click *yes* to prompt users in the browser to open or save the output for files using the specified extension.
 - b. Click *no* to open output directly in the Browser or application without prompting users to open or save it.
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.

Saving GRAPH (PNG, SVG, GIF, JPEG, or JPG) Requests

In order to use the Save Report functionality for GRAPH requests that specify a PNG, SVG, GIF, JPEG, or JPG format in the procedure, you must take the following steps:






1. 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.

- 2. 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, as determined by the temporary file expiration settings in the Client Configuration.
- 3. 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 HTM output file.

Working With HTML5 Chart Extensions


The HTML5 Chart Extensions page contains all HTML5 chart extensions currently installed in your local installation of WebFOCUS Business User Edition, as shown in the following image.

HTML5 Chart Extensions				
Get more Extensions				
 com.ibi.arc	Name: Arc Chart Description: Arc Chart Version: 1.0 API Version: 1.0 Author: Three D Graphics Copyright: Three D Graphics Inc. URL: https://threedgraphics.com License:	<input checked="" type="checkbox"/> Enabled	✖	
 com.ibi.chord	Name: Chord Diagram Description: Chord Diagram Version: 1.0 API Version: 1.0 Author: Three D Graphics Copyright: Three D Graphics Inc. URL: https://github.com/ibi/vf-extensions-chart/tree/master/com.ibi.chord License: BSD 3-clause	<input checked="" type="checkbox"/> Enabled	✖	
 com.ibi.liquid_gauge	Name: Liquid Gauge Chart Description: Fancy animated gauge chart with a liquid interior Version: 1.0 API Version: 1.0 Author: Information Builders Copyright: Information Builders Inc. URL: https://github.com/ibi/vf-extensions-chart/tree/master/com.ibi.liquid_gauge License: BSD 3-clause	<input checked="" type="checkbox"/> Enabled	✖	
 com.ibi.marker	Name: Marker Chart Description: Simple Marker Chart Version: 1.0 API Version: 1.0 Author: Three D Graphics Copyright: Three D Graphics Inc. URL: https://threedgraphics.com License:	<input type="checkbox"/> Enable	✖	
 com.ibi.sankey	Name: Sankey Flow Chart Description: Sankey Flow Chart Version: 1.0 API Version: 1.0 Author: Information Builders Copyright: Information Builders Inc. URL: https://github.com/ibi/vf-extensions-chart/tree/master/simple_bar%20example License: BSD 3-clause	<input checked="" type="checkbox"/> Enabled	✖	

HTML5 chart extensions expand the standard set of InfoAssist charts to include customized charts tailored to very specific reporting and data visualization requirements. Features on this page allow you to upload HTML5 chart extensions, enable or disable their use in InfoAssist, and uninstall them from WebFOCUS Business User Edition when no longer needed.

Understanding HTML5 Chart Extension Entries

Each HTML5 Chart Extension entry contains details that identify a chart extension and its origin, and help you determine if a chart extension is appropriate for your installation of WebFOCUS Business User Edition.


com.ibi.chord


Name: Chord Diagram
Description: Chord Diagram
Version: 1.0
API Version: 1.0
Author: Three D Graphics
Copyright: Three D Graphics Inc.
URL: <https://github.com/ibi/vf-extensions-chart/tree/master/com.tdg.chord>
License: BSD 3-clause

Each entry identifies an HTML5 chart extension with a Name, Description, Version, and API Version. These details help you identify the chart extension you want to use, and the specific version of it that best matches your requirements. The Author and Copyright identify the origin of the chart extension, and the URL links you to the location where you can retrieve additional copies. License information identifies the type of license, if any, under which the chart extension is made available to you, and helps you understand any limits on the use of the chart extension and the rights and obligations licensed users have to the developer.


Understanding the HTML5 Chart Extensions Enable/Enabled Check Box

Every HTML5 Chart Extension entry includes the Enable/Enabled check box that indicates whether or not the chart extension is available for use. The use of this check box provides a second level of availability that enables managers to restrict the full availability of HTML5 Chart Extensions to those that are in active use, while retaining all other installed HTML5 Chart Extensions in readiness for when they are needed.

When this check box is cleared, it displays the Enable label to indicate that selecting the check box will make the chart extension available for use, as shown in the following image.

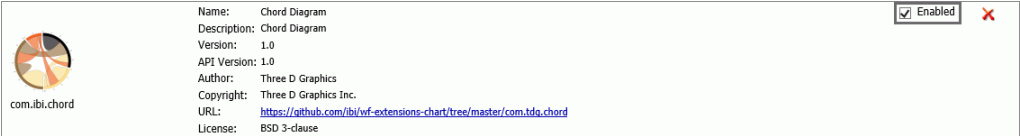

com.ibi.chord

Name: Chord Diagram
Description: Chord Diagram
Version: 1.0
API Version: 1.0
Author: Three D Graphics
Copyright: Three D Graphics Inc.
URL: <https://github.com/ibi/vf-extensions-chart/tree/master/com.tdg.chord>
License: BSD 3-clause

☐ Enable 

HTML5 Chart Extensions that have the Enable check box selected are installed, but they are not available for use.

When this check box is selected, it displays the Enabled label to indicate that the chart is already available for use, as shown in the following image.

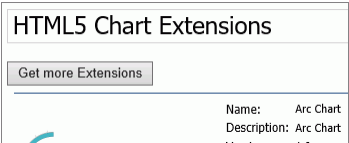


HTML5 Chart Extensions that have the Enabled check box selected are installed and are available for chart creation in InfoAssist. WebFOCUS Business User Edition identifies the files and directories included in that Chart Extension as eligible for calls from InfoAssist, and displays an icon for that Chart Extension in the Select a Chart menu that opens from the Other command in the Chart Type group, on the InfoAssist Format tab ribbon.

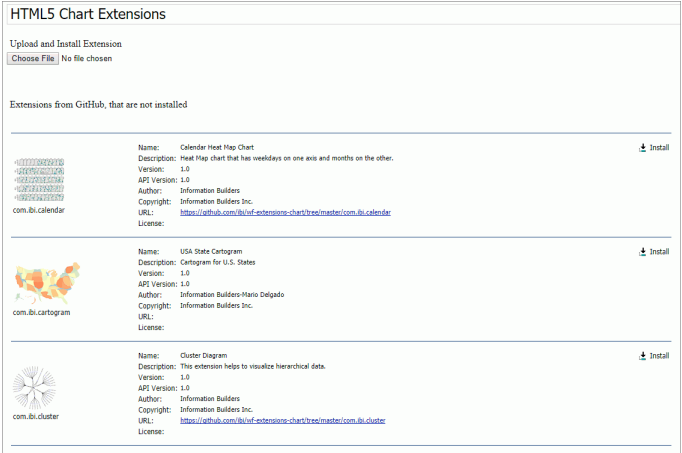
Note: The HTML5 Chart Extensions page does not manage copyright or license restrictions. You are ultimately responsible for the use of any HTML5 Chart Extension you upload. Therefore, you must ensure that you have a license or permission to use any HTML5 Chart Extension before uploading it to this page.

Uploading Additional HTML5 Chart Extensions Using the Upload and Install Extensions Page


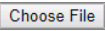
Use the Upload and Install Extensions page to install additional HTML5 Chart Extensions. To open the Upload and Install Extensions page from the main HTML5 Chart Extensions page, click *Get more Extensions*, as shown in the following image.



The Upload and Install Extensions page opens, as shown in the following image.



The Upload and Install Extensions page provides two ways to install additional HTML5 Chart Extensions:

- ☐ By clicking the *Install Extension* button  in entries for chart extensions that are found on the Information Builders public extension GitHub page, <https://github.com/ibi/wf-extensions-chart>, but are not currently installed in WebFOCUS Business User Edition.
- ☐ By clicking the *Choose File* button  to navigate to a folder on your local file system that contains a locally-developed HTML5 Chart Extension package in .zip file format.

To move back to the main HTML5 Chart Extensions page from the Upload an Install Extensions page, click *HTML Chart Extensions* under the Application Settings Folder, or click the *Back* button in your browser.

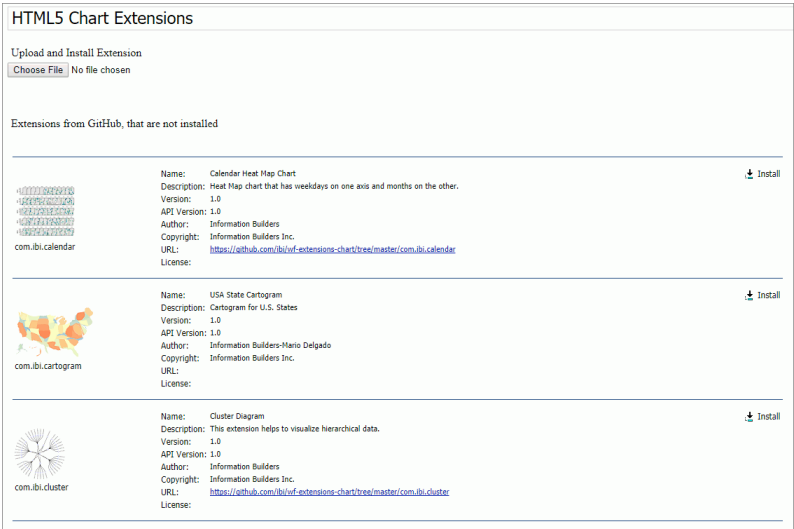
Procedure: How to Upload HTML5 Chart Extensions from the Local File System

Use this procedure to upload zip files containing HTML5 Chart Extensions from your local system.

You must ensure that you have a license or permission to use any HTML5 Chart Extension before uploading it to this page.

1. Sign in as a Manager and open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, click *HTML5 Chart Extensions*.
3. On the HTML5 Chart Extensions page, click *Get more Extensions*.

4. On the Upload and Install Extension page, click *Choose File*, as shown in the following image.



The Open dialog box opens and points to the extensions folder for your local installation of WebFOCUS Business User Edition. Typically, this is the following folder:

`drive:\ibi\install_dir\config\web_resource\extensions`

where:

`install_dir`

Is your WebFOCUS Business User Edition installation directory.

Note: If you downloaded your HTML5 Chart extension zip file to a different directory, navigate to that directory and file.

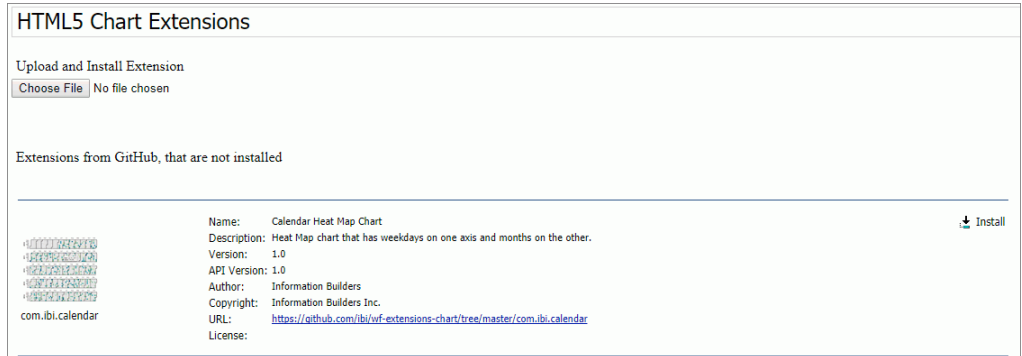
5. Click the file containing the zipped version of the HTML5 Chart extension you want to upload, and then click *Open*.
6. When the HTML5 Chart Extensions page refreshes and returns you to the top, scroll down to the entry for the new HTML5 Chart Extension.


Procedure: How to Install HTML5 Chart Extensions From the IBI GitHub Page

Use this procedure to upload HTML5 Chart Extensions from the public IBI GitHub extension page, <https://github.com/ibi/wf-extensions-chart>.

1. Sign in as a Manager and open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, click *HTML5 Chart Extensions*.

- On the HTML5 Chart Extensions page, click *Get more Extensions*.
- On the Upload and Install Extension page, review the list of extensions from GitHub that are not installed, as shown in the following image.



- If the chart extension you want to install appears in the list, click *Install Extension* .
- When the HTML5 Chart Extensions page refreshes and returns you to the top, scroll back to your entry to confirm that the chart extension is now installed.

Procedure: How to Enable an Installed HTML5 Chart Extension

When you select the Enable check box in an HTML5 Chart Extension entry, you make it available for use in InfoAssist and in your local installation of WebFOCUS Business User Edition. You must ensure that you have a license or permission to use any HTML5 Chart Extension before making it available for use.

- Sign in as a Manager and open the Administration Console.
- On the Configuration tab, under the Application Settings folder, click *HTML5 Chart Extensions*.
- On the HTML5 Chart Extensions page, scroll to the entry for the HTML5 Chart Extension that you want to enable.

Note: You can also search for the chart extension by name, using the Find or Find on this page command that is supported by the browser.

- Select the *Enable* check box, as shown in the following image.



- When the HTML5 Chart Extensions page refreshes and returns you to the top, scroll back to your entry to confirm that the check box is now selected.

An icon for the HTML5 Chart Extension appears in the InfoAssist Select a Chart menu, which opens when you click the Other command in the Chart Types group on the Format tab.

Procedure: How to Disable an HTML5 Chart Extension

When you clear the Enabled check box in an HTML5 Chart Extension entry, you make it unavailable for use in InfoAssist and in your local installation of WebFOCUS Business User Edition. However, the chart extension remains installed on the HTML5 Chart Extension page and can be enabled again when needed.

- Sign in as a Manager and open the Administration Console.
- On the Configuration tab, under the Application Settings folder, click *HTML5 Chart Extensions*.
- On the HTML5 Chart Extensions page, scroll to the entry for the HTML5 Chart Extension that you want to make unavailable.

Note: You can also search for the chart extension by name, using the Find or Find on this page command that is supported by the browser.

- Clear the *Enabled* check box, as shown in the following image.



- When the HTML5 Chart Extensions page refreshes and returns you to the top, scroll back to your entry to confirm that the check box is now cleared.

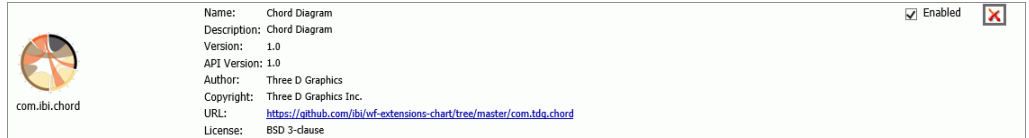
The icon for the HTML5 Chart Extension no longer appears in the Select a Chart Menu that opens from the InfoAssist ribbon.

Procedure: How to Uninstall an HTML5 Chart Extension

- Sign in as a manager and open the Administration Console.
- On the Configuration tab, under the Application Settings folder, click *HTML5 Chart Extensions*.
- On the HTML5 Chart Extensions page, scroll to the entry for the HTML5 Chart Extension that you want to uninstall.

Note: You can also search for the chart extension by name, using the Find or Find on this page command that is supported by the browser.

4. Click *Delete_CHARTNAME_Chart* as shown in the following image.



5. When you receive a message asking if you want to permanently delete the extension, click Yes.
6. When the HTML5 Chart Extensions page refreshes and returns you to the top, scroll back to your entry to confirm that the entry is now deleted.

The entry for the HTML5 Chart Extension no longer appears on the page.

Changing Application Settings

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

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

Reference: Understanding Change Management Settings

Change Management settings determine which file types can be 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 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, jpe, jpeg, jpg, js, mas, mnt, png, sty, and svg.

Retain Handles (IBI_CM_RETAIN_HANDLES)

This option is not relevant to WebFOCUS Business User Edition.

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 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 cleared, 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 cleared, 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 cleared, 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 ESRI Settings

ESRI settings defines the connection to the local application that supports Esri-based maps.

ESRI On Premise (IBI_ESRI_ON_PREMISE)

Identifies the path to the internal ArcGIS JavaScript API Source used to develop Esri-based maps for WebFOCUS Business User Edition. This setting is blank, by default, meaning that the use of an internal source is not activated. To activate the use of an internal ArcGIS JavaScript API to develop Esri maps, type the path to it in this setting, typically, /web_resource/arcgis_api.

The default API that should be referenced by this setting is the ArcGIS API for JavaScript, version 3.15, which can be found at <https://js.arcgis.com/3.15/>. The ArcGIS JavaScript API zip file is available for download from <https://developers.arcgis.com/downloads/>.

For more information about the Esri ArcGIS JavaScript API, see <https://developers.arcgis.com>.

For more information about how to configure Esri On Premise for InfoAssist, see *Configuring an Esri On Premise Environment*.

Reference: Understanding Parameter Prompting Settings

Parameter Prompting settings determine parameter prompting behavior in WebFOCUS Business User Edition.

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 that were 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 that were 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 that were 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 that were 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 Autoprompt Template (IBI_DESCRIBE_TEMPLATES)

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.

Reference: Text Generation Server Settings

Text Generation Server settings define the connections to an independent server that provides narrative descriptions for chart headers, footers, and tooltips.

Text Generation Server URL (IBI_TEXT_GENERATION_SERVER_URL)

Identifies the URL of the external natural language generation (NLG) server that provides narrative descriptions for chart headers, footers and tooltips. If your product installation supports natural language generation for charts, type the URL of the text generation server in this setting. This setting is blank, by default.

When you activate the use of an external natural language generation (NLG) server, this setting contains a value, typically:

http://machine_name:20000/yseop-manager/direct/savvy-kb/dialog.do

Where:

[*machine_name*](#)

is the name of the server that hosts the external natural language generator.

Changing Client Settings**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 v 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 selected 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. If Show is not selected, the Themes menu is removed from the InfoAssist interface.

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. If Show is not selected, the Page Heading menu is removed from the InfoAssist interface.

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. If Show is not selected, the Report Heading menu is removed from the InfoAssist interface.

Reference: Understanding InfoAssist Format Tab Properties

For reports or charts, InfoAssist displays a list of output file format options, such as, HTML, PDF, or Excel, in the Format Group of the Home tab. Other options that make additional layouts and display features available when creating a report or chart appear only on the Format tab itself. You can control the display of both types of options through the settings contained in this section. The settings that affect the Format tab display are InfoMini Run Immediate, Other Chart Types, Pages on Demand, Stack Measures, and User Selection.

Note: Settings in this section do not affect the display of Format tab features for visualizations.

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 of the InfoAssist Properties page.

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, Excel, is available for selection in the Output Format drop-down menus in the Tool Options Dialog Defaults section.

The Show check box for this setting 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.

Excel 2007 Format

Enables the use of the 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, Excel (xlsx), is available for selection in the Output Format drop-down menus in the Tool Options Dialog Defaults section.

This check box is selected, by default.

Excel 2007 Formula

Enables the use of the Excel 2007 formulas when the *Excel 2007 Format* option 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.

Excel CSV

Enables the use of the comma separated values (CSV) file format.

When this check box is selected, the Excel CSV format option is available for use in InfoAssist, and it appears on the *Home* tab in the Format group options list under the Excel format option. When it is cleared, this option is not available, and it does not appear in the Format group options list.

This check box is selected, 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 of the InfoAssist Properties page.

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.

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 the Show check box 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

Settings in the Tools Options Dialog Defaults section enables Managers to specify default tool settings. If the *Allow User Override* check box is selected 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*, and *PowerPoint 2007*. To ensure that these options are available, a Manager must select the check box for each under the Format Tab section of the InfoAssist Properties page. The default value is *HTML*.

Chart Output Format

Sets the default format for charts. Valid values are *HTML*, *HTML5*, *Active Report*, *PDF*, *EXL07*, *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 of the InfoAssist Properties page. The default value is *HTML5*.

Document Output Format

Sets the default format for documents that are generated in InfoAssist. Valid values are *HTML*, *Active Report*, *PDF*, *EXL07*, *EXL2K*, *PowerPoint 2000*, and *PowerPoint 2007*. The format options in this list are available only when their corresponding check box is selected in the Format Tab section of the InfoAssist Properties page. If that check box is cleared, you will receive a message warning you that the format option is not enabled when you select it from this list. 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 *All*, *1*, *10*, *50*, *100*, *500*, *1000*, *2000*, *5000*, and *10000* 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.

HTML Freeze Height

Determines how the Freeze option, located on the *Format* tab in the *Navigation* group of the InfoAssist ribbon, automatically freezes the height of a report area.

If the AutoFit value is assigned to this setting, reports produced when the Freeze option is selected automatically fit the height of the window or pane in which they appear. This is the default value.

If the Fixed value is assigned to this setting, reports produced when the Freeze option is selected are set automatically to a fixed height of four inches, regardless of the size of the window or pane in which they appear.

HTML Accordion

Determines whether the Accordion option, located on the *Format* tab in the *Navigation* group of the InfoAssist ribbon, displays accordion reports that automatically resize data to fit the container in which they appear.

If the AutoFit value is assigned to this setting, reports produced when the Accordion option is selected automatically resize the display of data to fit the size of the container in which they appear, and automatically adjust column widths based on the size of the largest data value or column title. This is the default value.

If the legacy value is assigned to this setting, reports produced when the Accordion option is selected do not automatically resize the display of data to fit the size of the container in which they appear, and do not automatically adjust column widths.

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).

JSON

Information is not yet available.

Understanding InfoAssist Auto Drill Properties

Settings in this section enable the use of drill-down navigation options, which are part of the Auto Drill functionality.

Single Click Navigate

Enables the use of single click navigation, which is an automatic drill down to the next level of a dimension within the body of a report or chart made in response to a single click on a top-level entry or feature.

By default, this check box is not selected, meaning that single click navigation is disabled, and top-level Auto Drill entries or features display the Drilldown menu in response to a single click. If this check box is selected, single click navigation is enabled, and instead of displaying the Drilldown menu, top-level Auto Drill entries or features automatically refresh the report or chart with results based on the next lower level of your selected dimension in response to a single click.

Breadcrumbs

Enables the display of a breadcrumb trail at the top of an Auto Drill report or chart.

By default, this check box is selected, and Auto Drill reports and charts display a breadcrumb trail. If this check box is cleared, Auto Drill reports and charts do not display a breadcrumb trail.

In an Auto Drill report or chart, a breadcrumb trail displays a series of links to previous versions that were generated as you drilled through each level of your selected dimension to reach the version currently on display.

Restore Original

Enables the display of the Restore Original option in the Drilldown menu.

By default, this check box is selected, and the Restore Original option appears in the Drilldown menu. If this check box is cleared, the Restore Original option does not appear in the Drilldown menu. In an Auto Drill report or chart, the Restore Original option returns you directly to the original version.

Drill Up

Enables the display of the Drill up option in the Drilldown menu.

By default, this check box is selected, and the Drill up option appears in the Drilldown menu. If this check box is cleared, the Drill up option does not appear in the Drilldown menu. In an Auto Drill report or chart, the selection of the Drill up option refreshes the display with results based on the next level above the current level of your selected dimension.

Drill Down

Enables the display of the Drill down option in the Drilldown menu.

By default, this check box is selected, and the Drill down option appears in the Drilldown menu. If this check box is cleared, the Drill down option does not appear in the Drilldown menu. In an Auto Drill report or chart, the selection of the Drill down option refreshes the display with results based on the next level below the current level of your selected dimension.

Note: In addition to disabling the Drill down option, clearing this setting also removes hyperlinks from top level report entries and the breadcrumb trail display from reports and charts. If the Single Click Navigate setting is also cleared, clearing the Drill Down setting effectively disables Auto Drill navigation tools in reports and charts that contain only the top level of a dimension value in their design. If the Single Click Navigate setting is selected, and the report or chart contains entries below the top level, clearing the Drill Down setting shifts the Single Click Navigation feature to those lower-level entries. However, because this setting also suppresses the display of the Drilldown menu, users will neither be able to restore the original version of the report or chart, nor will they be able to drill back up to a higher level.

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 to WebFOCUS Business User Edition.
- ☐ **HTTP Basic.** This option is not relevant to WebFOCUS Business User Edition.
- ☐ **Kerberos.** This option is not relevant to WebFOCUS Business User Edition.
- ☐ **SAP Ticket.** This option is not relevant to WebFOCUS Business User Edition.
- ☐ **Service Account.** This option is not relevant to WebFOCUS Business User Edition.

- ☐ **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 Business User Edition 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 Business User Edition 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 Business User Edition 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 Business User Edition, from WebFOCUS Business User Edition 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 Business User Edition 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 Business User Edition 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 Business User Edition 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 WebFOCUS Business User Edition to make trusted connections to the Reporting Server, you must also enable the Reporting Server to accept trusted connections.

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.

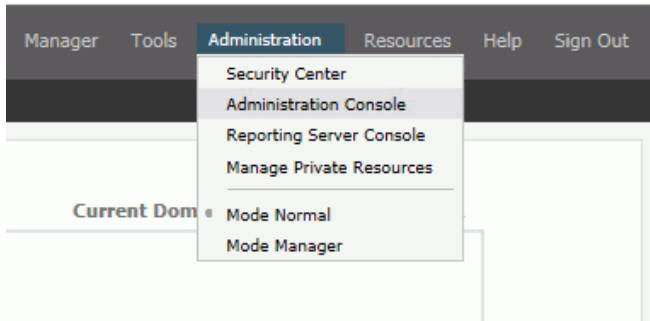
Using the ReportCaster Console

The following tools are accessible from the Console.

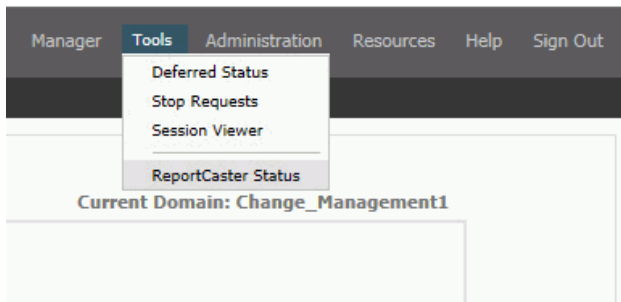
- ☐ Server Status
- ☐ Job Status
- ☐ Job Log
- ☐ Configuration
- ☐ Blackout Periods
- ☐ Global Updates

Purge Logs

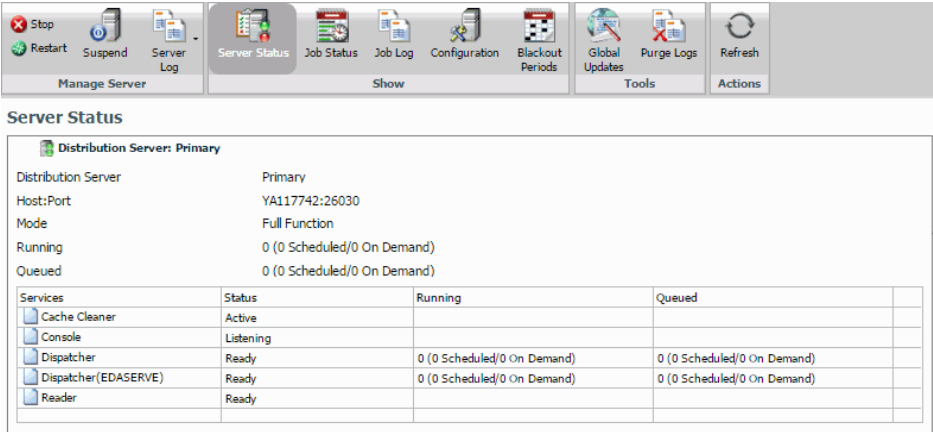
In WebFOCUS Business User Edition configurations licensed for ReportCaster, authorized users can access the ReportCaster Console through the Administration Console, from the Administration option on the menu bar, as shown in the following image.



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

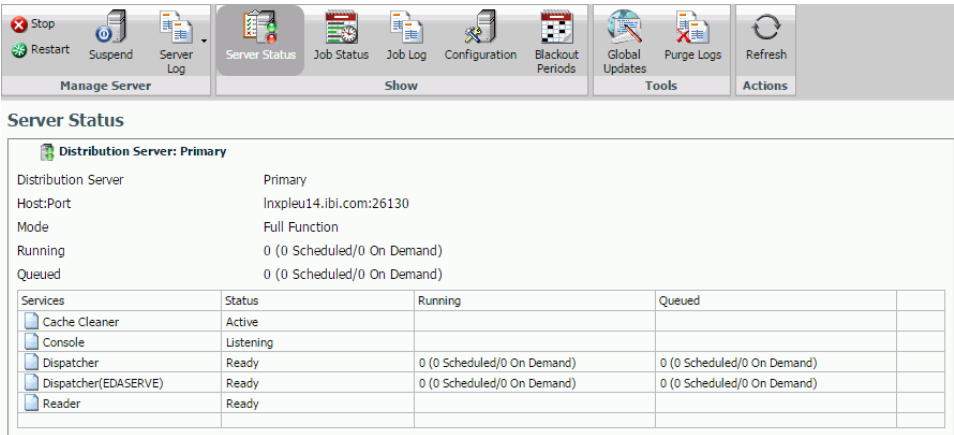


The Console intuitive ribbon displays in a new browser window, as shown in the following image. The ribbon displays a tab for each tool the user is authorized to access.



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:
 - ☐ **Active.** The service is active.
 - ☐ **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:

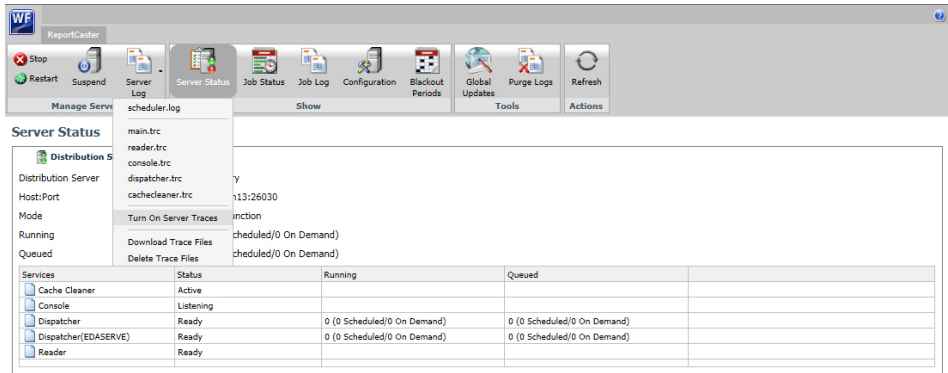
- ☐ **Refresh.** Retrieves the most current information and refreshes the Distribution Server status with this information.
- ☐ **Restart.** Recycles the Distribution Server and the Application Server.
- ☐ **Suspend.** This option is always available. Suspends the Distribution Server services, but the 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 61.

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

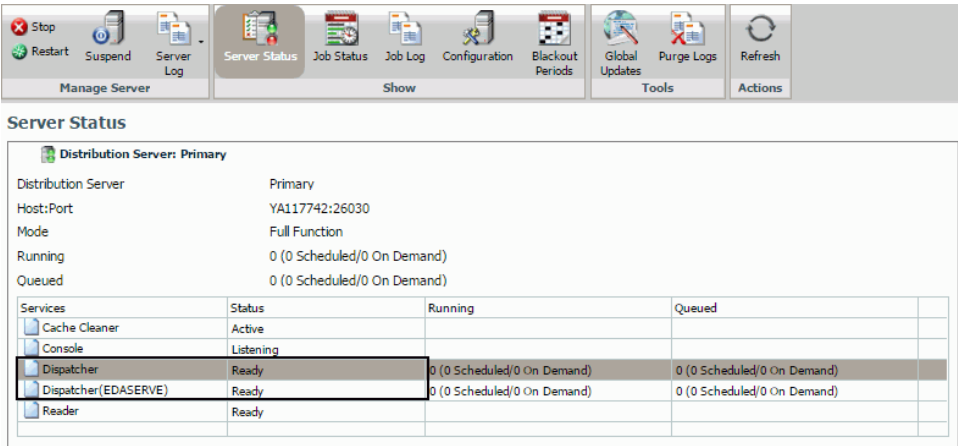
1. From the ReportCaster Console, select *Server Status*.
2. From the Distribution Server list, select a server.
3. On the toolbar, click the down arrow on the Server Log button.
4. Click *Turn On Server Traces* to turn the Distribution Server traces on, as shown in the following image.



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

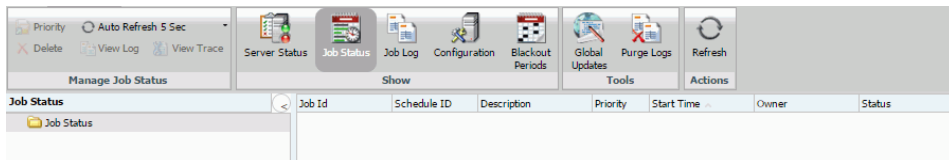
1. Select a running server and click *Stop*.

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.

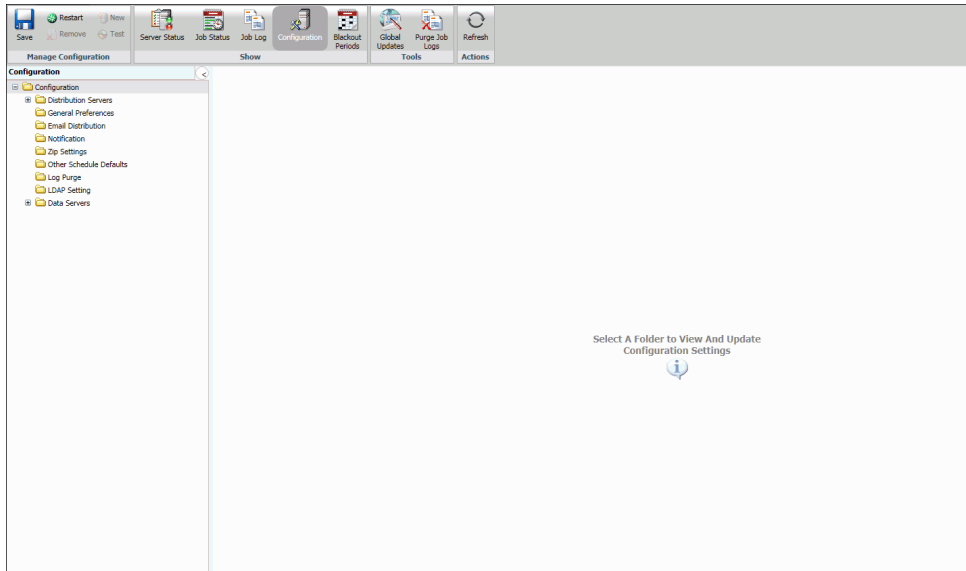
Note: The Job Log tab supports the functionality of a multiple selection, whereby you can open or delete multiple files simultaneously.

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 68

- ☐ **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 68.
- ☐ **Configuration Files.** Provides options to view and download the ReportCaster configuration files. Click the arrow to access the following individual files.
 - ☐ **dserver.xml.** Contains a record of current ReportCaster configuration settings.
 - ☐ **sendmodes.xml.** Contains information about MIME output file formats.
 - ☐ **rc_preference.xml.** Contains information about the display of options in the UI.Clicking one of these file options displays the file information in a browser window. *Download Configuration Files* to download all files as a single zip file.

☐ **Tools group**

☐ **Global Updates.**

Authorized users can make global updates for the values stored in schedules and distribution lists. Using the Global Updates interface, the following settings can be updated:

- ☐ Mail Server
- ☐ FTP Server
- ☐ Printer
- ☐ Email Address
- ☐ Email From
- ☐ Data Server

- ☐ **Notification Type**
- ☐ **Notification Reply Address**
- ☐ **Notification Subject**
- ☐ **Notification Brief Message To**
- ☐ **Notification Full Message To**
- ☐ **Purge Job 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 Job Logs on Demand](#) on page 139.
- ☐ **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 distribution formats and methods will be available to a user creating a schedule. In this folder, you can also specify 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 74.
- ☐ **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 80.
- ☐ **Notification.** Configures notification settings, such as the notification email host and default notification type. For details on these settings, see [Notification](#) on page 92.
- ☐ **Zip Settings.** Provides settings to configure how Zip files will be created and named. For details on these settings, see [Zip Settings](#) on page 95.

- ❑ **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 97.
- ❑ **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 98.
- ❑ **LDAP Setting.** Allows you to configure ReportCaster self-service users to be authenticated and authorized against an LDAP data source rather than the 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 99.
- ❑ **Data Servers.** Allows you to configure multiple Reporting Servers, including cluster servers. For details on these settings, see [Data Servers Settings](#) on page 102.


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 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 58.

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.
Restrict to IP Address	Optional.	Restricts Distribution Server console access to one or more IP Addresses.
Reader Interval	Required. Default value is 1 minute.	<p>Polling interval (in minutes) for the ReportCaster Distribution Server to check for scheduled jobs.</p> <p>An acceptable value is any positive integer from 1 to 999999. Negative numbers and zero are not allowed.</p>

Setting	Optional or Required/ Default Value	Descriptions and Possible Values
Recovery	Default value is OFF.	<p>On. During startup, the ReportCaster Distribution Server recovers scheduled jobs that were processed but not completed.</p> <p>Off (Default). During startup, the ReportCaster Distribution Server does not recover any scheduled jobs.</p>
Processing for No Report to Distribute	Required. Default value is Error.	<p>Specifies whether the <i>No Report to Distribute</i> 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:</p> <p><input type="checkbox"/> Error. The <i>No Report to Distribute</i> 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.</p> <p><input type="checkbox"/> Warning. The <i>No Report to Distribute</i> 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.</p> <p>These settings also apply to burst reports when there is a <i>No Report to Distribute</i> message for an individual burst value.</p>

Setting	Optional or Required/ Default Value	Descriptions and Possible Values
Processing for Blackout Period Job Termination	Required. Default value is Error.	<p>If a scheduled report distribution is terminated due to a previously set blackout period, this option specifies whether or not an error notification will be sent via email.</p> <p><input type="checkbox"/> Error. An error notification will be sent to the designated email recipient.</p> <p><input type="checkbox"/> Warning. An error notification will not be sent to the designated email recipient.</p> <p>For more information, see Using Blackout Periods on page 110.</p>
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		
Scan-back Type	Required. Default value is On.	<p>Possible values are:</p> <p><input type="checkbox"/> On</p> <p><input type="checkbox"/> Off</p> <p><input type="checkbox"/> Reset Next Run Time</p>

Setting	Optional or Required/ Default Value	Descriptions and Possible Values
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.

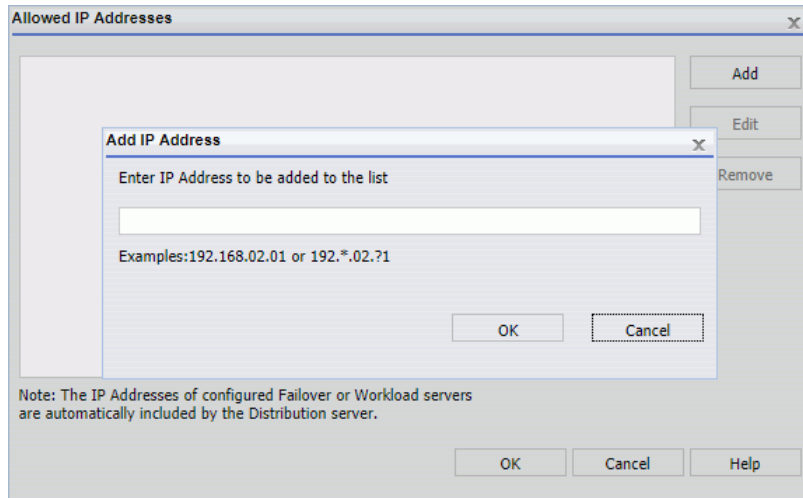
Restricting Distribution Server Console Access to an IP Address List

Limiting Distribution Server access to a preselected IP address helps prevent denial of service (DoS) attacks against your server. A DoS attack is a malicious cyber-attack that overloads a server with requests from multiple IP addresses, which blocks legitimate IP addresses from accessing the server. You can use the Restrict to IP Addresses option in the ReportCaster Console to enhance the security of your network. If you populate the Restrict to IP Addresses field with one or more IP addresses, the Distribution Server only accepts TCP/IP requests from the addresses listed. This setting is blank by default.

Procedure: How to Configure IP Address Restrictions

1. Open the ReportCaster Console.
2. On the ribbon, in the Show group, click *Configuration*.
3. In the Configuration pane, click *Distribution Servers*.
The Primary Distribution Server options display.
4. Click the *Restrict to IP Addresses* open folder button.
The Allowed IP Addresses dialog box opens.
5. Click *Add*.

The Add IP Address dialog box opens, as shown in the following image.



6. Type an IP address and click **OK**. This adds the IP address to the Allowed IP Address list.
7. Repeat steps 5-6 to add any additional IP addresses.
8. Click **OK** to save the Allowed IP Address list and return to the ReportCaster Console.
9. On the ribbon, in the *Manage Configuration* group, click **Save** to keep your allowed IP address changes.
10. On the ribbon, in the *Manage Configuration* group, click **Restart** to apply your changes.

Procedure: How to Edit an IP Address

1. Click the Restrict to IP Addresses open folder button.
The Allowed IP Addresses dialog box opens.
2. Click the IP address that you want to modify, and then click **Edit**.
The Edit IP Addresses dialog box opens.
3. Modify the IP address, and then click **OK**.
4. On the ribbon, in the *Manage Configuration* group, click **Save** to keep your allowed IP address changes.
5. On the ribbon, in the *Manage Configuration* group, click **Restart** to apply your changes.

Procedure: How to Delete an IP Address

1. Click the *Restrict to IP Addresses* open folder button.

The Allowed IP Addresses dialog box opens.

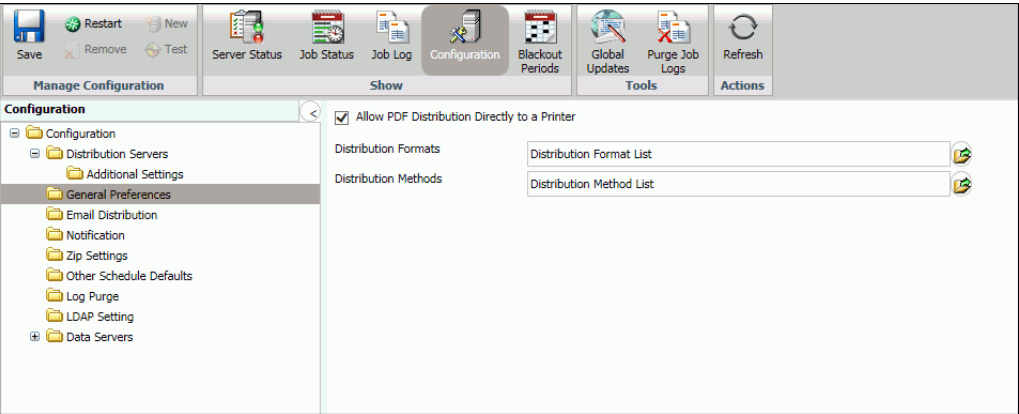
- 2. Click the IP address that you want to delete, and then click *Remove*.

The selected IP address is deleted.

- 3. Click *OK*.
- 4. On the ribbon, in the *Manage Configuration* group, click *Save* to keep your allowed IP address changes.
- 5. On the ribbon, in the *Manage Configuration* group, click *Restart* to apply your changes.

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.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
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.

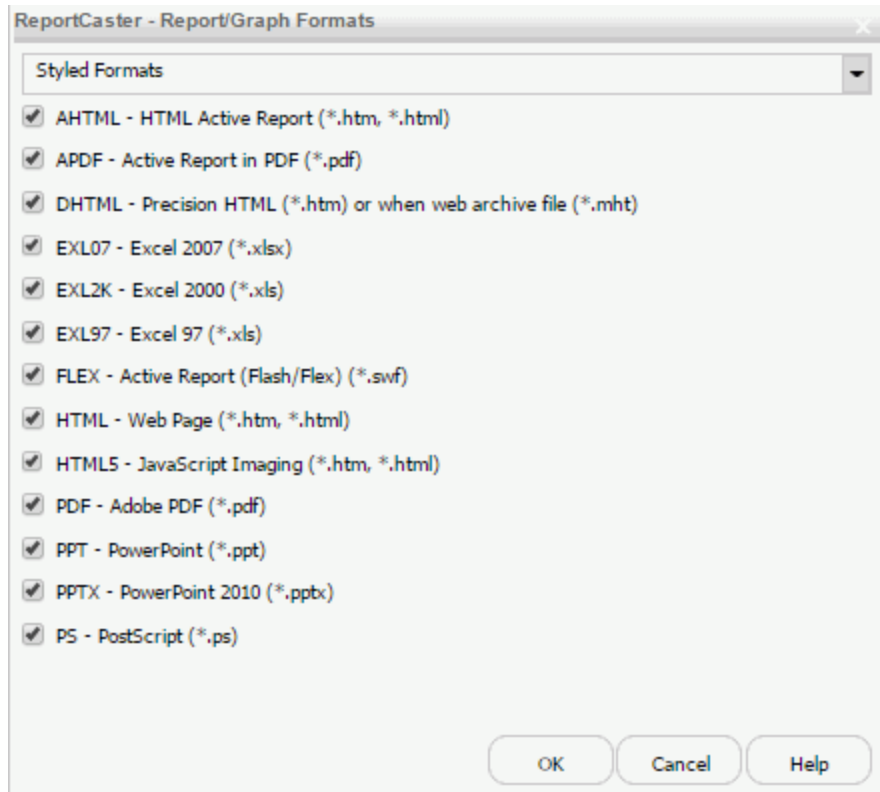
This setting only applies to WebFOCUS (Repository) procedures. By default, all report and graph formats are enabled (selected). A minimum of one report or graph format must be selected.

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.

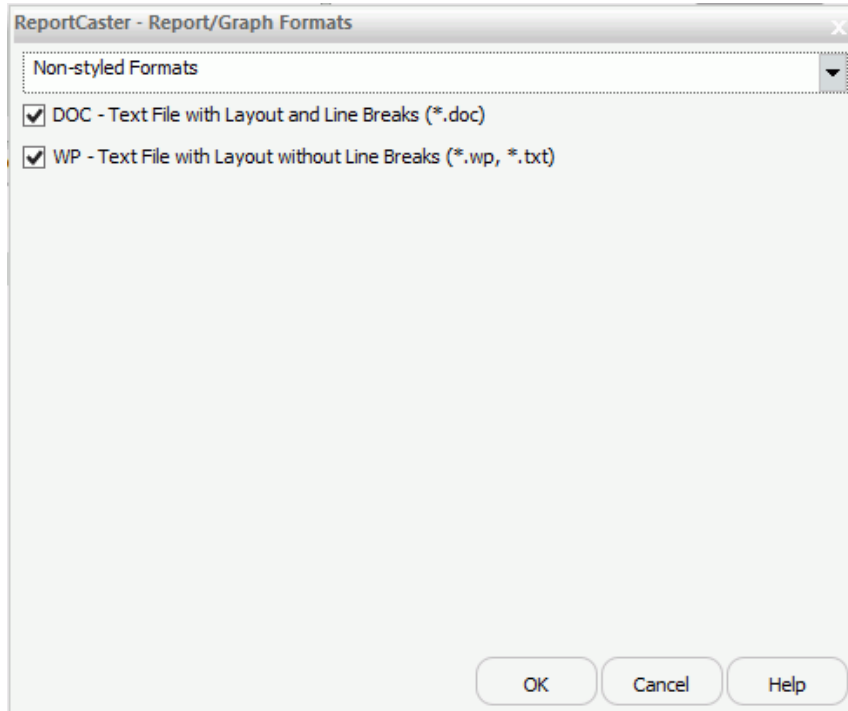


2. Using the Styled Formats drop-down list, you can select *Specialized Formats*, *Non-styled Formats*, or *Graph Images*. Optionally, you can keep the default, *Styled Formats*.

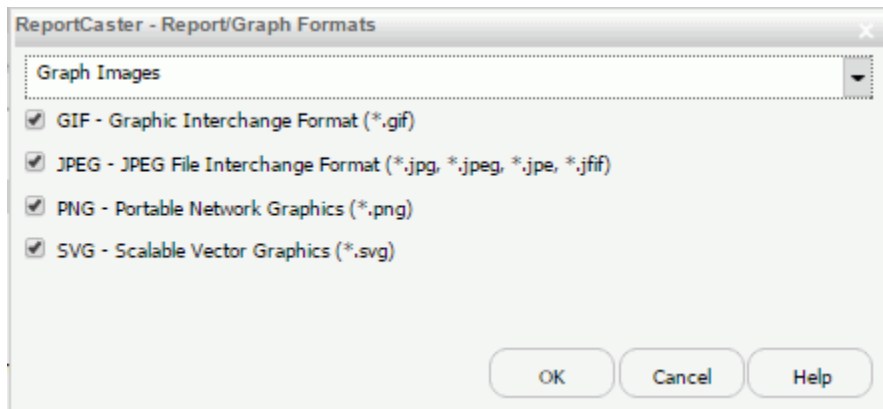
By default, *Styled Formats* are displayed with each format type selected.

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 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 the WebFOCUS Business User Edition 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).

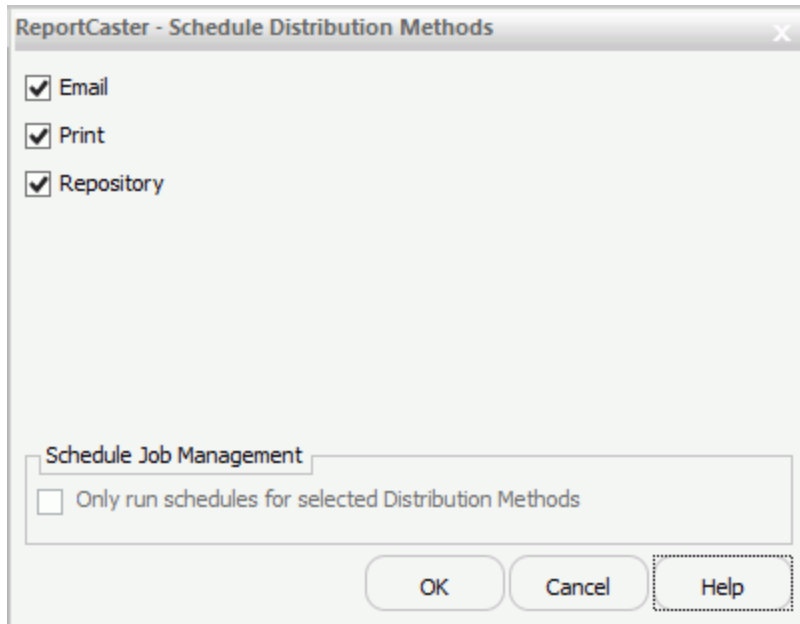
Note: A minimum of one distribution method must be selected.

The Repository option only appears if these products are enabled. Repository is an optional product component that is installed with WebFOCUS Business User Edition.

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.

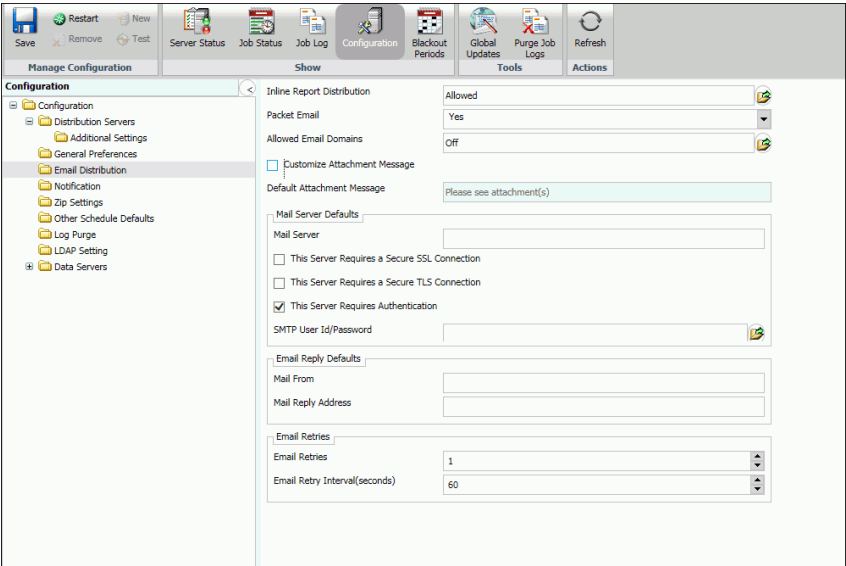
3. Optionally, select the *Only run schedules for selected Distribution Methods* check box to limit the schedules running to those that have at least one of the Distribution Methods selected.
4. When your selections are complete in the Schedule Distribution Methods dialog box, click *OK*.

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

5. To implement the configuration changes, restart the Distribution Server and WebFOCUS Business User Edition 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 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.	<p>Controls how task output and burst content are distributed through email.</p> <p>Valid values are:</p> <ul style="list-style-type: none"><input type="checkbox"/> No. Each burst value or task output is distributed in a separate email.<input type="checkbox"/> Yes. People receiving burst values or output from tasks will receive a single email with multiple attachments.<input type="checkbox"/> 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.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Allowed Email Domains and Addresses	The default value is Off.	<p>Contains the email domains and addresses that are authorized in a distribution.</p> <p>Select the <i>Restrict user input with this list</i> check box to restrict user input of email addresses and domains to the allowed addresses saved in your list.</p> <p>Note:</p> <ul style="list-style-type: none"> <input type="checkbox"/> If this list has changed before you attempt to edit email addresses for a previously saved Basic Schedule or Distribution List, the system checks if your new email addresses and domains are still valid. If you enter an invalid email address or domain, you will be prompted to change the email address or domain before saving. <input type="checkbox"/> 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.
Mail Server Defaults section		

Setting	Optional or Required/Default Value	Descriptions and Possible Values
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 <i>hostname:port</i> . 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.

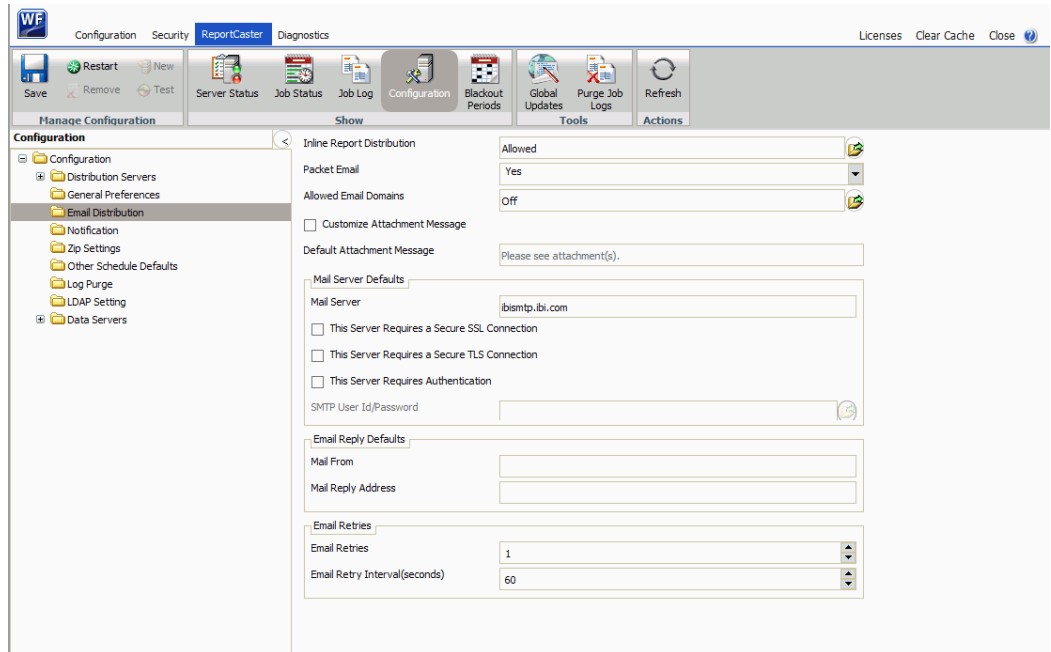
Setting	Optional or Required/Default Value	Descriptions and Possible Values
Mail Reply Address	Optional.	<p>Default email reply address when creating an email schedule.</p> <p>Note: If you do not provide a Mail Reply Address, the default Reply Address used in the Basic Scheduling tool will be the email address of the user that is signed to WebFOCUS. ReportCaster obtains the email address of the user from the WebFOCUS security system.</p>
Email Retries section		
Email Retries	The default value is 1.	<p>Number of times the Distribution server will try to connect to the email server to deliver report output.</p> <p>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.</p> <p>Valid values are 0 through 9.</p>
Email Retry Interval(seconds)	The default value is 60 seconds.	<p>Amount of time that the Distribution server will wait between retries.</p> <p>Valid values are 1 through 999.</p>

Procedure: How to Configure Email Distribution

1. From the Tools menu, click *ReportCaster Status*.

- Click the *Configuration* button, as shown in the following image.

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

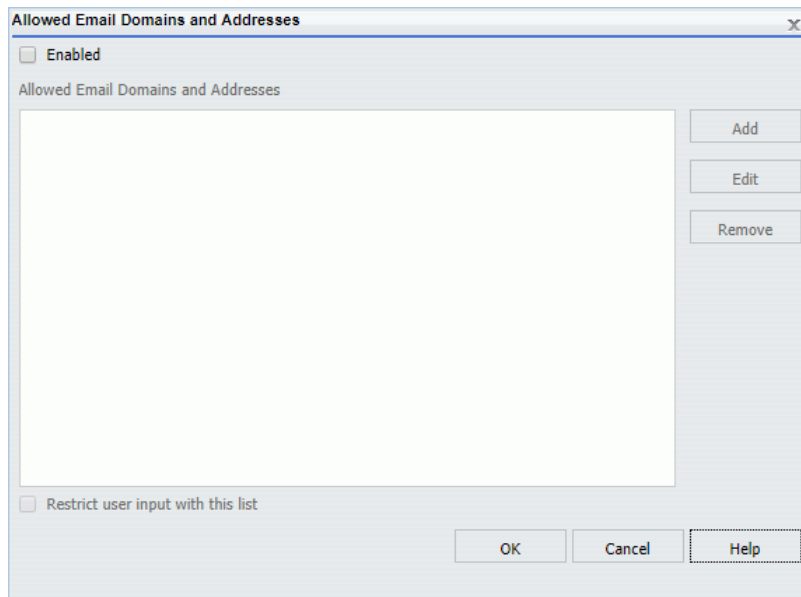


- In the left pane, select the *Email Distribution* folder.
- Populate the email distribution fields. You can:
 - ☐ Make changes to the current email settings. For more information, refer to the preceding table.
 - ☐ Supply any default values that you would like to be available at schedule creation time.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

Validating Allowed Email Domains and Addresses

When sending reports by email, you can restrict user selection of email domains and addresses from a pre-defined list.

The following image shows the Allowed Email Domains and Addresses dialog box in the ReportCaster Console, where this option is available.



Select the *Enabled* check box to restrict email distribution to a list of valid email domains and addresses. When the list is enabled, and a user enters an email address that is not on this list, the ReportCaster job cannot be saved.

If you select the *Restrict user input with this list* check box, users will only be able to use email domains and addresses selected from this list, applying another layer of email distribution restriction for other users.

Note: You must select the Enabled check box in order to select the Restrict user input with this list check box.

Examples of Invalid Email Addresses and Domains

In this example, an Administrator added the following email addresses and email domains to the Allowed Email Domains and Addresses list:

- ☐ john@ibi.com
- ☐ roger@ibi.com
- ☐ @gmail.com
- ☐ @yahoo.com

These additions to the list define what is valid and what is invalid for user input.

Invalid Email Addresses

For example, since john@ibi.com was added to the list, if a user types in John@ibi.com, with an upper case J, the email address is valid. This is because the Allowed Email Domains and Addresses feature is not case sensitive.

However, if a user types johnroger@ibi.com, which is a combination of two email addresses that were added to the list, the email address would be invalid, because this specific email address was not added to the list.

Invalid Email Domains

When entering domain addresses, if a user types in any email address with the email domain @gmail.com, it is valid, because @gmail.com is one of the domains added to the list.

However, if a user types in any email address with the email domain @outlook.com, it is not valid, because @outlook.com is not one of the domains added to the list.

Email Domain and Address Restrictions

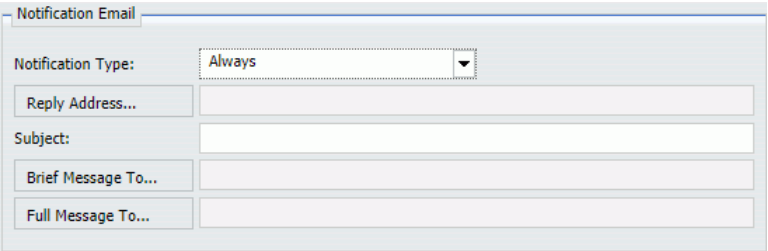
Restrictions apply during the following situations:

- ☐ Editing Email Distribution options in the Basic Scheduling tool.

The following image shows the Email Distribution options in the Basic Scheduling tool. If you select the *Restrict user input with this list* check box, you can click the *To*, *From*, and *Reply Address* fields to select or create email addresses.

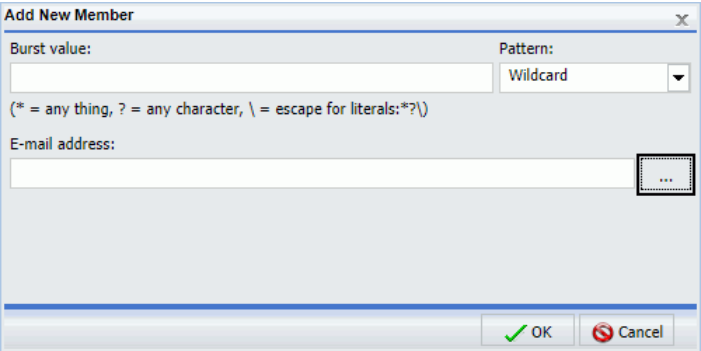
- ☐ Editing Notification Email options in the Basic Scheduling tool.

The following image shows the Notification Email options in the Basic Scheduling tool. If you select the *Restrict user input with this list* check box, you can click the *Reply Address*, *Brief Message To*, and *Full Message To* fields to select or create email addresses.

A screenshot of the 'Notification Email' dialog box. It has a title bar with a close button. Inside, there's a 'Notification Type:' label with a dropdown menu showing 'Always'. Below that are four input fields, each with a button to its left: 'Reply Address...' (button), 'Subject:' (button), 'Brief Message To...' (button), and 'Full Message To...' (button). The buttons are light blue with rounded corners.

☐ Adding new members to a Distribution List

The following image shows the Distribution List Add New Member dialog box. If you select the *Restrict user input with this list* check box, you can click the *ellipsis* button next to the E-mail address field to select or create email addresses.

A screenshot of the 'Add New Member' dialog box. It has a title bar with a close button. Inside, there's a 'Burst value:' label with an input field. To its right is a 'Pattern:' label with a dropdown menu showing 'Wildcard'. Below these is a line of text: '(* = any thing, ? = any character, \ = escape for literals: *?\\)'. Then there's an 'E-mail address:' label with an input field. To the right of the input field is a small square button with three dots (ellipsis). At the bottom right are 'OK' and 'Cancel' buttons with green and red icons respectively.

The Email Selection Dialog Box

When the *Restrict user input with this list* check box has been selected, you can click a *To*, *From*, *Cc*, *Bcc*, *Reply*, *Reply Address*, *Brief Message To*, *Full Message To*, or *ellipsis* button to display one of three dialog boxes. The dialog box that displays is based on the type of email domain and address information contained in the Allowed Email Domains and Addresses list.

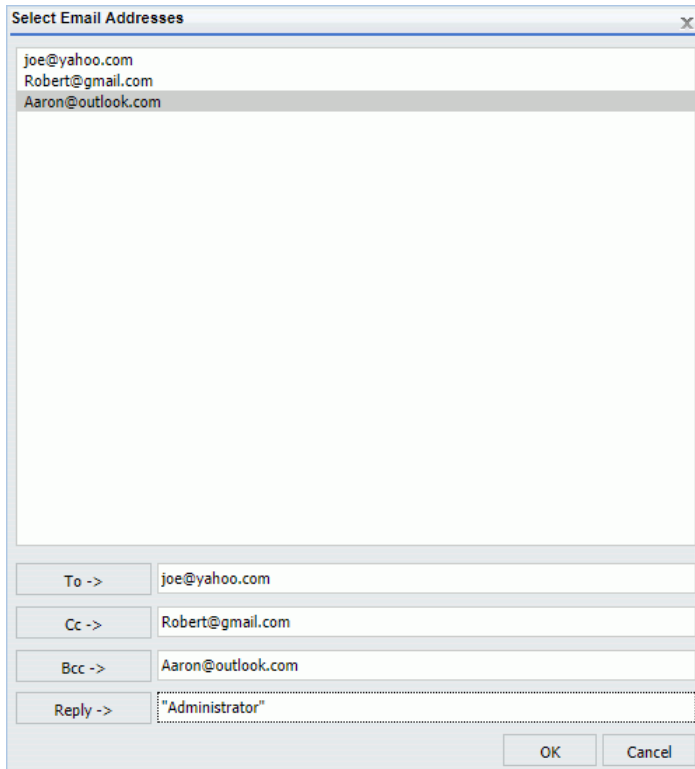
Note:

- ☐ You can enter multiple email addresses into the *To*, *From*, *Cc*, *Bcc*, *Reply*, *Reply Address*, *Brief Message To*, and *Full Message To* fields.

- ❑ To cancel the selection of an email address in the Select Email Addresses dialog box, hold the Ctrl key and select the email address.

A List of Only Email Addresses

If the Allowed Email Domains and Addresses list contains only email addresses, the Select Email Addresses dialog box allows you to select an email address for the *To*, *Cc*, *Bcc*, or *Reply* fields, as shown in the following image.



After you select an email address, click the To, Cc, Bcc, or Reply button to assign the email address to the respective field.

A List of Email Domains and Addresses

If the Allowed Email Domains and Addresses list contains both email domains and addresses, the Select or Enter Email Addresses dialog box lets you select from a list of email address. The dialog box also lets you create an email address for specific domains, as shown in the following image.

The dialog box titled "Select or Enter Email Addresses" features a search bar at the top with the text "Jackie" and a dropdown menu showing "@ outlook.com". Below the search bar is a list of email addresses: "joe@yahoo.com" and "Aaron@live.com". At the bottom of the dialog, there are four buttons: "To ->", "Cc ->", "Bcc ->", and "Reply ->". Each button is associated with a text field. The "To ->" field contains "joe@yahoo.com", the "Cc ->" field contains "Aaron@live.com", the "Bcc ->" field contains "Robert@gmail.com", and the "Reply ->" field contains "Jackie@outlook.com". At the bottom right of the dialog are "OK" and "Cancel" buttons.

After you select an email address, or enter an email address and choose a domain, click the *To*, *Cc*, *Bcc*, or *Reply* button to assign the email address to the respective field.

A List of Only Email Domains

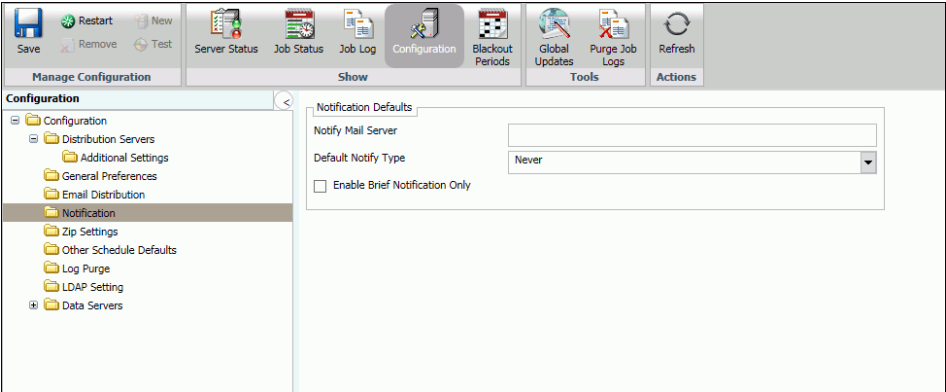
If the Allowed Email Domains and Addresses list contains only email domains, the input dialog box lets you select an email domain and enter the name of an email address, as shown in the following image.

The image shows a dialog box titled "Enter Email Addresses". At the top, there is a text input field containing "Jackie" followed by an "@" symbol and a dropdown menu currently showing "gmail.com". Below this is a large text area with the instruction "Select an email domain and enter the name of the email address". A dropdown menu is open, displaying a list of email domains: "gmail.com", "live.com", "outlook.com", and "yahoo.com". At the bottom of the dialog, there are four rows, each with a label and a text field: "To ->" with "joe@outlook.com", "Cc ->" with "Aaron@live.com", "Bcc ->" with "Robert@yahoo.com", and "Reply ->" with "Jackie@gmail.com". "OK" and "Cancel" buttons are located at the bottom right of the dialog.

After you enter an email address and choose a domain, click the *To*, *Cc*, *Bcc*, or *Reply* button to assign the email address to the respective field.

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		

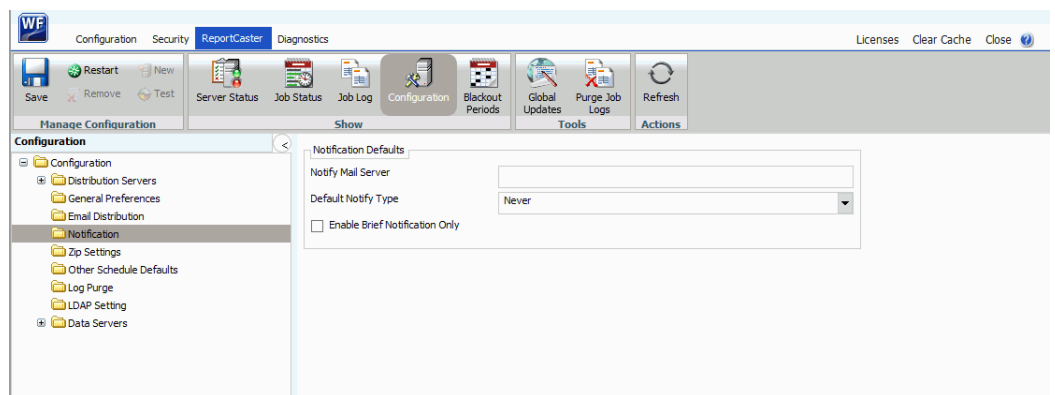
Setting	Optional or Required/Default Value	Descriptions and Possible Values
Notify Mail Server	Optional.	<p>Name of the mail server that distributes the notification email. If blank, ReportCaster uses the Mailhost setting as the notification mail server.</p> <p>Tip: Information Builders recommends using 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.</p> <p>You can also specify a port for the Notify Mailhost using <i>hostname:port</i>. If you do not specify a port or the port you specify is not present, the default port is used.</p>
Default Notify Type	The default value is Never.	<p>Specifies whether to send notification of the schedule status to a specified email address. Possible values are:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Never. This is the default value. ReportCaster does not send notification of the schedule status under any circumstance. <input type="checkbox"/> On Error. The specified users are notified when errors are encountered while running the schedule. Information Builders recommends using the On Error notification option. <input type="checkbox"/> Always. The specified user is always notified when the schedule runs.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
Enable Brief Notification Only	Optional.	<p>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.</p> <p>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.</p>

Procedure: How to Configure Notification

1. From the 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.

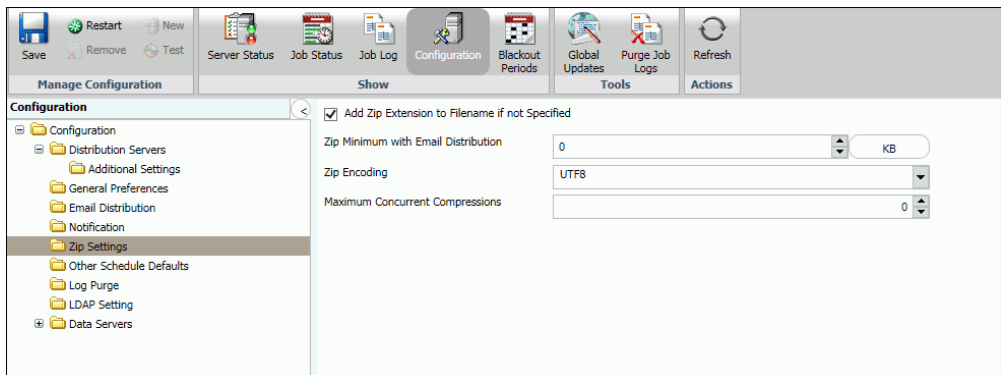
4. Populate the notification fields. You can:

- ☐ 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.
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.
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.

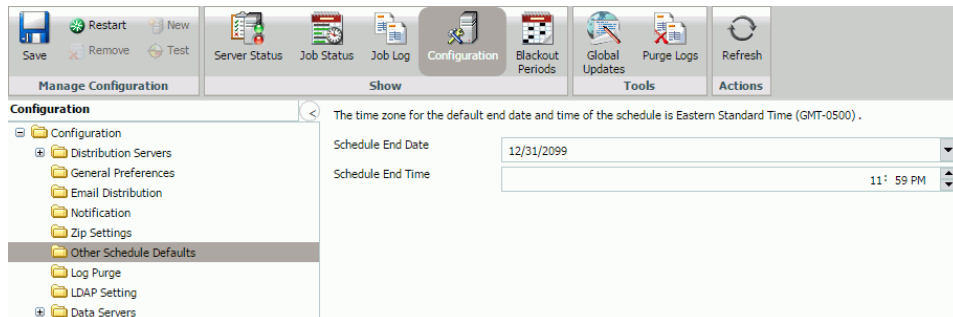
Note: Authorized users can also access the ReportCaster Configuration tool from the Administration Console.

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.

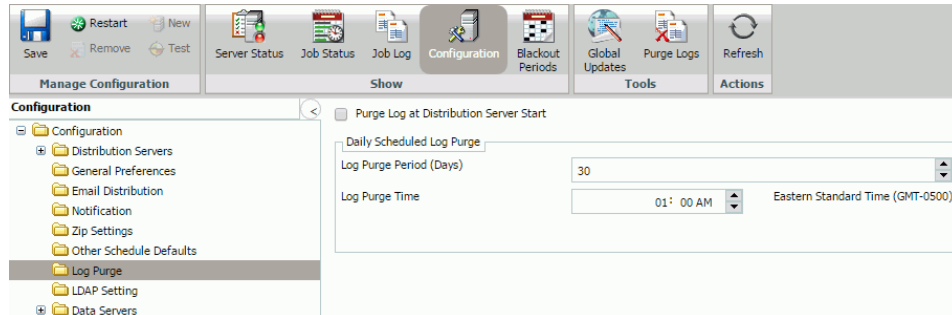


The following table lists and describes the configuration settings available in the Other Schedule Defaults folder.

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.



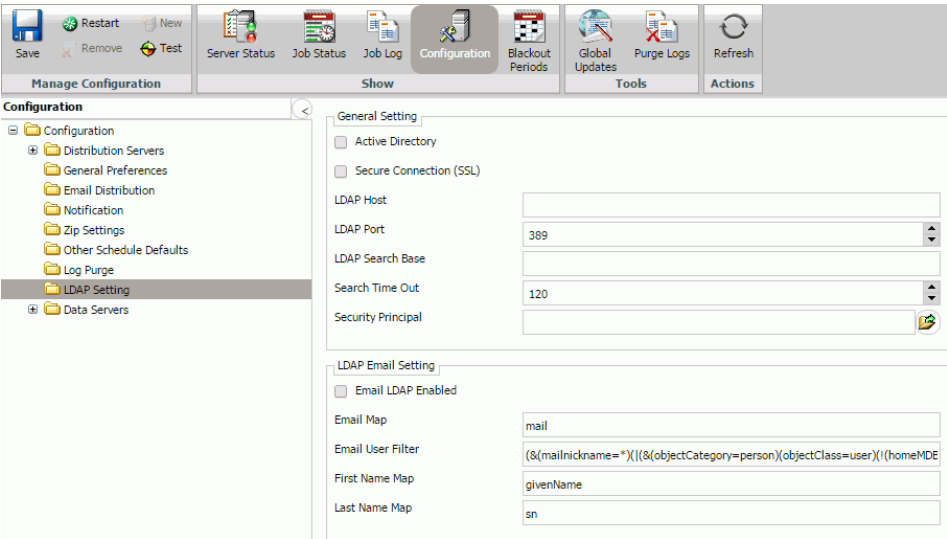
The Log Purge folder contains the following configuration settings.

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.
Log Purge Time	Optional.	Time at which log purging occurs.

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 Setting 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.
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.

Setting	Optional or Required/Default Value	Descriptions and Possible Values
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.	<p>Service account of the user performing authentication. The user must have sufficient access rights to locate user entries in the directory.</p> <p>Select the icon to the right of this option to open the User dialog box, where you can type a user name and password.</p>
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.

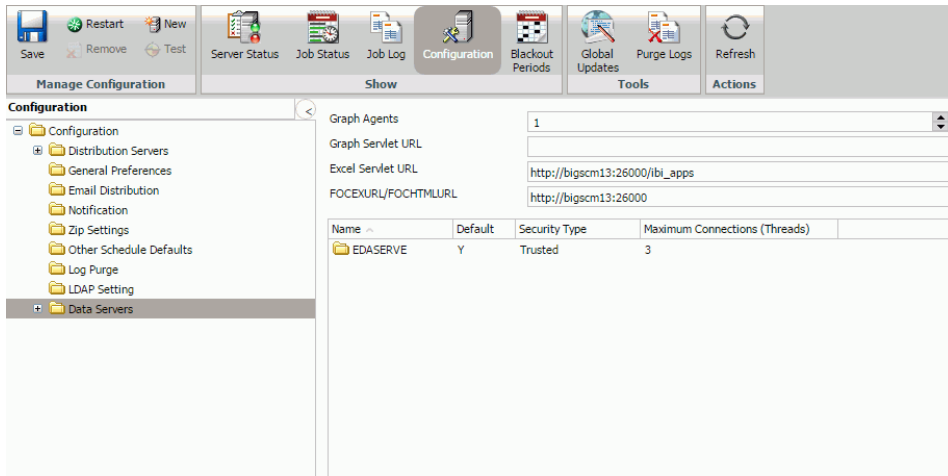
Setting	Optional or Required/Default Value	Descriptions and Possible Values
Email User Filter	Default value provided is dependent on the LDAP Type selected.	Filter for email entries to be retrieved. For example: <pre>(& (mailnickname=*) ((&(objectCategory=person) (objectClass=user) (!(homeMDB=*)) (!(msExchHomeServerName=*))) (&(objectCategory=person) (objectClass=user) ((homeMDB=*) (msExchHomeServerName=*))) (&(objectCategory=person) (objectClass=contact)) (objectCategory=group) (objectCategory=publicFolder)))</pre>
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

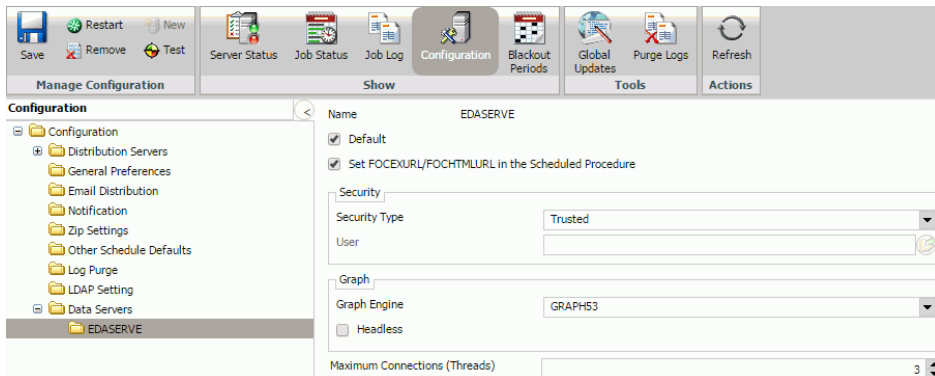
The Data Servers folder in the Configuration tab contains settings to configure the Reporting Servers associated with ReportCaster. Using the configuration settings in this folder, you can also configure multiple Reporting Servers with ReportCaster.

Note: Data Server connection information is stored in WebFOCUS Business User Edition, and not in ReportCaster. ReportCaster runs scheduled procedures through WebFOCUS Business User Edition which is installed with the Distribution Server. When a ReportCaster job is executed by Business User Edition, 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.

Setting	Optional or Required/ Default Value	Descriptions and Possible Values
Graph Servlet URL	Optional. There is no default.	<p>Overrides the default graph server setting and configures graph image files to be created on the Application Server.</p> <p>Type the following value</p> <p><code>http://hostname/context_root/IBIGraphServlet</code></p> <p>where:</p> <p><code>hostname</code></p> <p>Is the host name of the Application Server where WebFOCUS Business User Edition is installed.</p> <p><code>context_root</code></p> <p>Is the site-customized context root for the WebFOCUS Business User Edition web application deployed on your Application Server. <code>ibi_apps</code> is the default value.</p> <p>This setting is available for WebFOCUS Business User Edition Server and WebFOCUS Business User Edition procedures.</p> <p>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 Business User Edition from creating the graph.</p>

Setting	Optional or Required/ Default Value	Descriptions and Possible Values
Excel Servlet URL	Default value is <code>http://localhost:8080/ibi_apps</code>	<p>Specifies the application server to be used to zip the file components that comprise an EXCEL[®] 2007 file (.xlsx) as follows:</p> <p><code>&URL_PROTOCOL://servername/alias/IBIEXCELSERVURL</code></p> <p>where:</p> <p><code>URL_Protocol</code></p> <p>Is HTTP.</p> <p><code>servername</code></p> <p>Is the name of the application server where WebFOCUS Business User Edition is installed.</p> <p><code>alias</code></p> <p>Is the context root of the WebFOCUS Business User Edition application. The default is ibi_apps.</p> <p>This setting is available for WebFOCUS Business User Edition Server and WebFOCUS Business User Edition 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 Business User Edition from creating the Excel 2007/2010 file.</p>
FOCEXURL/ FOHTMLURL	Default value is <code>http://localhost:8080</code>	Specifies the host name and port of the FOCEXURL/ FOHTMLURL.

Settings for an individual Data Server:

Setting	Optional or Required/ Default Value	Descriptions and Possible Values
Name	Required.	Name of the selected Data Server. Note: Data Server names are case-sensitive. Data Servers are defined in WebFOCUS Business User Edition as uppercase so you should also define Data Servers as uppercase in ReportCaster.
Default	Required.	This option is selected by default.
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.	<p>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.</p> <p>User. A valid Execution Id and password must be specified when creating a schedule.</p> <p>Shared. When creating a schedule, the user ID and password is internally assigned as the Execution Id and password.</p> <p>Note: Since the actual password is not stored in the WebFOCUS Business User Edition repository, the Shared configuration can only be used when a password is not required to connect to the Reporting Server.</p> <p>Trusted. The Execution Id is the schedule owner and no password is sent to the WebFOCUS Business User Edition Reporting Server when schedules run.</p> <p>Note: The Reporting Server must be configured to accept a Trusted connection when the Trusted option is selected.</p>

Setting	Optional or Required/ Default Value	Descriptions and Possible Values
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.
Headless	By default, this option is not selected.	Determines whether a graphics card exists on the WebFOCUS Business User Edition 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.

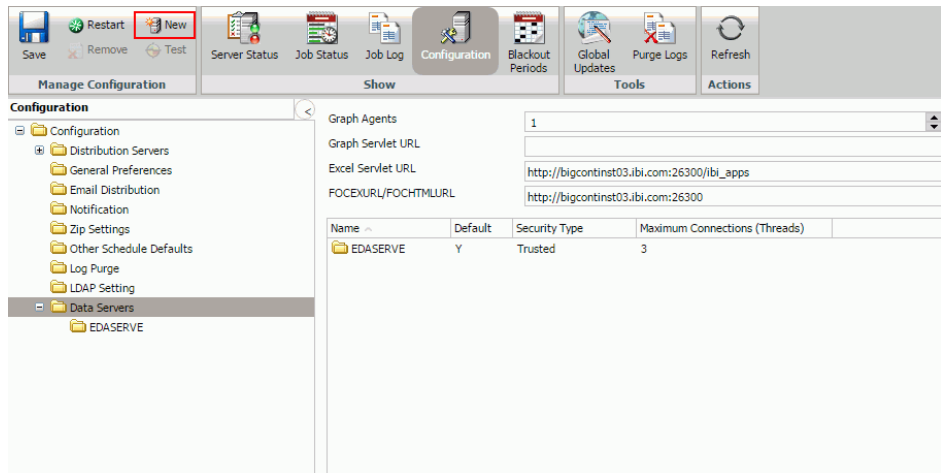
Configuring Reporting Servers With ReportCaster

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

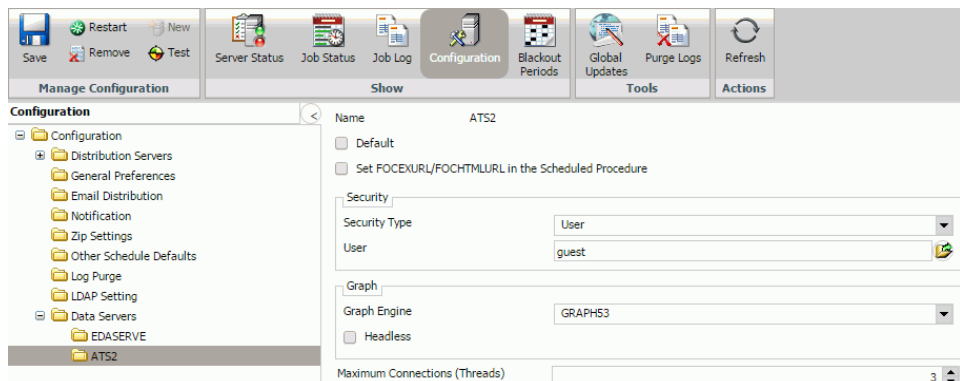
1. In the left panel of the Configuration tab, select the *Data Servers* folder, then select *New* in the toolbar, as shown in the following image.



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 Business User Edition Server Connections configuration. You can review the WebFOCUS Business User Edition 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 FOCXURL 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

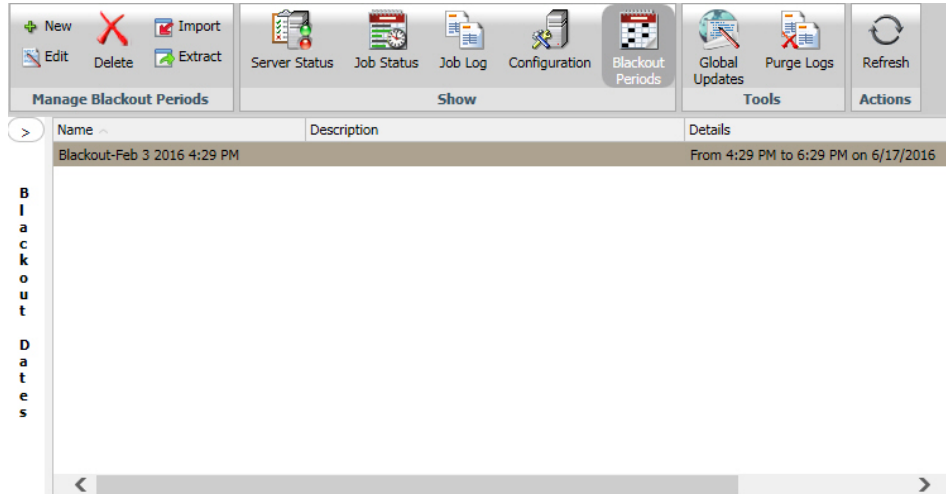
Blackout Periods are those dates and times on which schedules will not run and cannot be set to run. A user authorized to access the Blackout Periods tool can view, define, update, import, export, and delete blackout periods.

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.	<p>Selected. The Blackout Period covers the hours specified in the Start (Time) and End (Time) fields.</p> <p>Not Selected. The Blackout Period covers the entire day.</p> <p>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.</p>
Start (Time)	Optional. By default, displays the current hour and minute.	<p>The Hour and Minute in which a Blackout Period is to begin.</p> <p>This value is relevant only if the Blackout Time check box is selected.</p>
End (Time)	Optional. By default, displays the time two hours <i>after</i> the current hour and minute.	<p>The Hour and Minute in which a Blackout Period is to end.</p> <p>This value is relevant only if the Blackout Time check box is selected.</p>
Frequency	Required. By default, the Weekly option is selected.	<p>Weekly. Blackout periods that recur on a specified day of the week.</p> <p>Monthly. Blackout periods that recur on a specified monthly date.</p> <p>Single Day. Blackout periods that occur once on a specified date.</p> <p>Every Day. Blackout periods that recur at a specified time every day.</p>

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 123.

6. Click the appropriate frequency option:
 - ☐ **Weekly.** Establish the frequency for the blackout period. For configuration information, see [Configuring Weekly Blackout Periods](#) on page 115.
 - ☐ **Monthly.** Establish the frequency for the blackout period. For configuration information, see [Configuring Monthly Blackout Periods](#) on page 118.
 - ☐ **Single Day.** Select the date for the blackout period. For configuration information, see [Configuring Single Day Blackout Periods](#) on page 121.
 - ☐ **Every Day.** Establish the hours for the daily blackout period. For configuration information, see [Configuring Every Day Blackout Periods](#) on page 122.
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.)	<p>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.</p> <p>You can select one or more individual weeks.</p> <p>The Select All check box automatically selects every week of the month, establishing a blackout period that takes place every week in a month.</p>

Setting	Optional or Required/ Default Value	Descriptions and Possible Values
On Days of the Week check boxes (Right Column)	Required (At least one selection from this column).	<p>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.</p> <p>You can select one or more individual days.</p> <p>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.</p>
Months	Required (At least one selection from this group).	<p>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.</p> <p>You can select one or more individual months.</p> <p>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.</p>

***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.

The dialog box shows the following options:

- ☒ Weekly
- ☐ Monthly
- ☐ Single Day
- ☐ Every Day

On:

- ☐ Select All
- ☐ First
- ☐ Second
- ☐ Third
- ☐ Fourth
- ☐ Last

Months:

- ☐ Select All
- ☐ January
- ☐ February
- ☐ March
- ☐ April
- ☐ May
- ☐ June
- ☐ July
- ☐ August
- ☐ September
- ☐ October
- ☐ November
- ☐ December

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.	<p>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.</p> <p>You can select one or more individual dates.</p> <p>The Select All option automatically selects every day of the month, establishing a blackout period that takes place every day during your selected months.</p>
Months	Required.	<p>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.</p> <p>You can select one or more individual months.</p> <p>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.</p>

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.

The screenshot shows the 'Blackout Date and Time' dialog box with the 'Monthly' frequency selected. The 'Days' section includes a 'Select All' checkbox and a grid of checkboxes for days 1 through 31, plus a 'Last' checkbox. The 'Months' section includes a 'Select All' checkbox and a grid of checkboxes for each month from January to December. The 'Monthly' radio button is selected, and the 'Single Day' and 'Every Day' radio buttons are unselected.

Frequency	Days	Months
<input type="radio"/> Weekly	<input type="checkbox"/> Select All	<input type="checkbox"/> Select All
<input checked="" type="radio"/> Monthly	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 <input type="checkbox"/> 25 <input type="checkbox"/> 26 <input type="checkbox"/> 27 <input type="checkbox"/> 28 <input type="checkbox"/> 29 <input type="checkbox"/> 30 <input type="checkbox"/> 31 <input type="checkbox"/> Last	<input type="checkbox"/> January <input type="checkbox"/> February <input type="checkbox"/> March <input type="checkbox"/> April <input type="checkbox"/> May <input type="checkbox"/> June <input type="checkbox"/> July <input type="checkbox"/> August <input type="checkbox"/> September <input type="checkbox"/> October <input type="checkbox"/> November <input type="checkbox"/> December
<input type="radio"/> Single Day		
<input type="radio"/> Every Day		

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.

Untitled - Blackout Date and Time

Group: (Global)

Name: Blackout-Feb 3 2016 2:41 PM

Description:

Details: From 2:41 PM to 4:41 PM on 2/3/2016

☒ Blackout Time (Uncheck this box to black out the entire day)

The time zone for the Start Time and End Time is Eastern Standard Time (GMT-0500) .

Start: 2: 41 PM

End: 4: 41 PM

☐ Weekly

☐ Monthly

☒ Single Day

☐ Every Day

February 2016						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	1	2	3	4	5
6	7	8	9	10	11	12

OK Cancel

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.

Untitled - Blackout Date and Time

Group: (Global)

Name: Blackout-Feb 3 2016 2:41 PM

Description:

Details: From 2:41 PM to 4:41 PM

☒ Blackout Time (Uncheck this box to black out the entire day)

The time zone for the Start Time and End Time is Eastern Standard Time (GMT-0500) .

Start: 2: 41 PM

End: 4: 41 PM

☐ Weekly

☐ Monthly

☐ Single Day

☒ Every Day

Select the start time and end time to create a blackout time for every day of the year

OK Cancel

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 123.

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. $(44 - (12 \times 3)) = (44 - 36) = 8$
 - 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. $(44 - (12 \times 3)) = (44 - 36) = 8$.
 - 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.

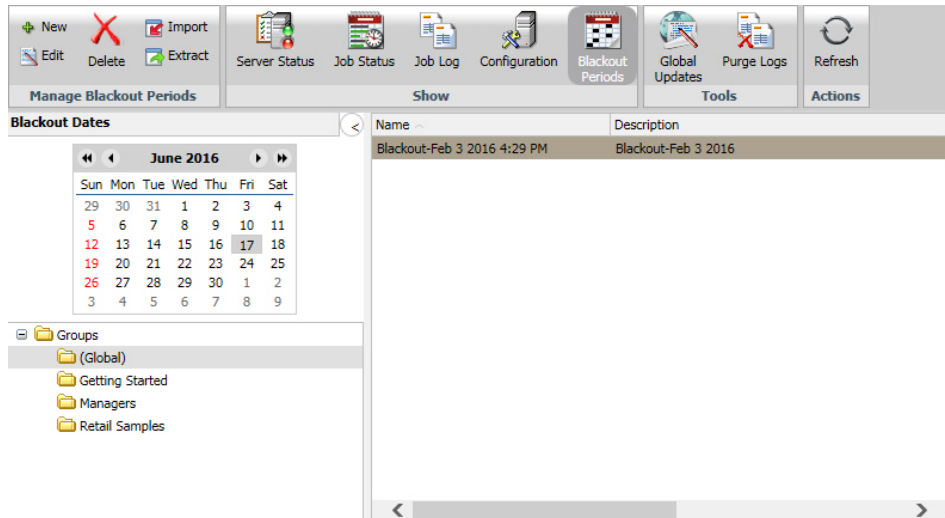
For example, if you use the Tab key to move from the Hours section of the Start field, you will move down to the Hours section of the End field, not over to the Minutes section of the Start field. To move right, you must use the right direction key instead.

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.

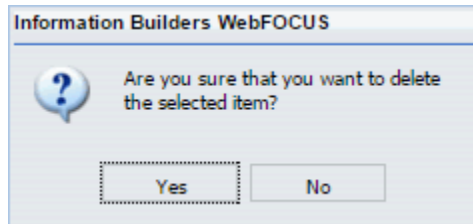
Procedure: How to Delete a Blackout Period Profile

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.

- In the right pane, click the entry for Blackout Period profile you want to delete, as shown in the following image.



- On the ribbon, in the Manage Blackout Periods group, click *Delete*.
- 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.

Note: All imported files must contain UTF-8 (National Language Support) character encoding to upload correctly.

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 127 and [Monthly Blackout Period Import File Entry Layout](#) on page 128.

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
```

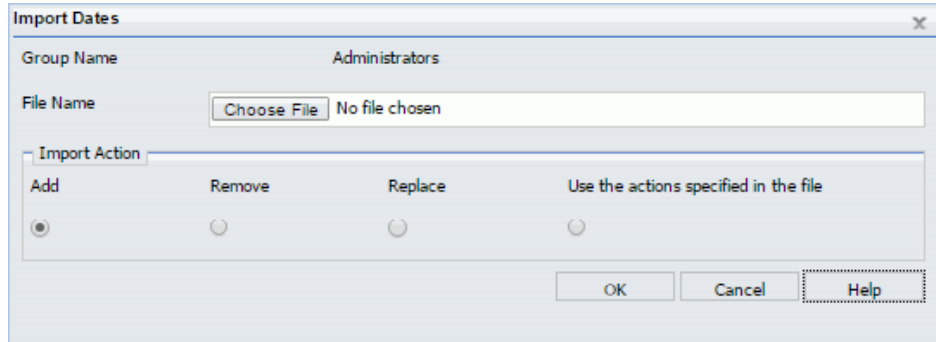
This information identifies the entry as an Every Day Blackout Period and includes its Description and Name.

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.

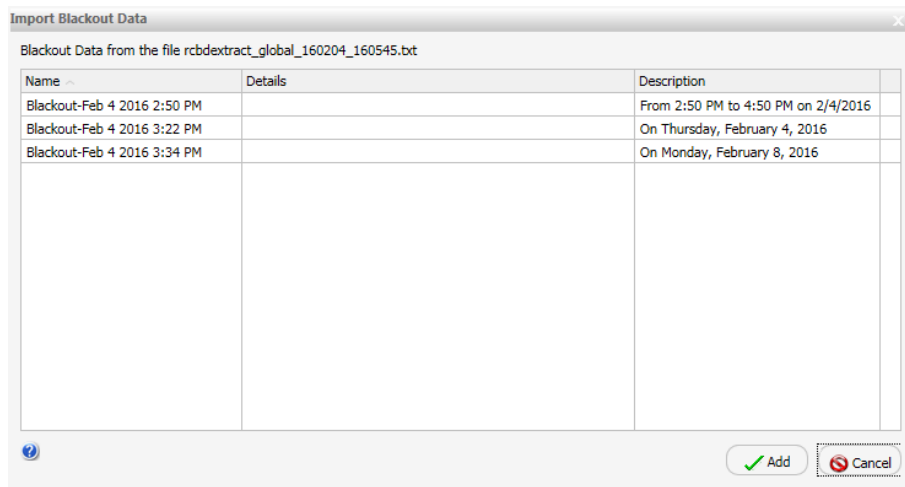
1. In the Blackout Dates pane, click the folder of the group for which you are importing Blackout Period profiles.

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



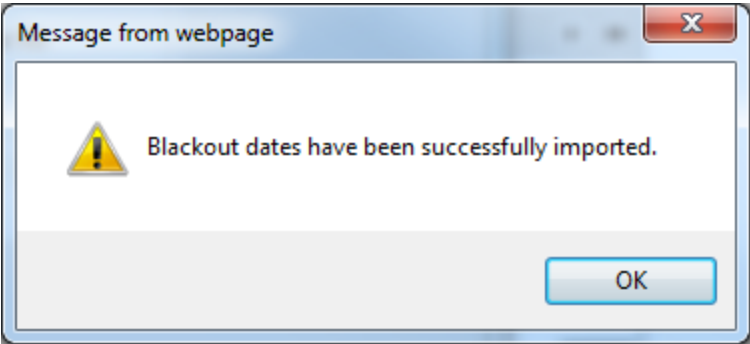
- In the File Name field, type the full path to the file, or click *Browse* and navigate to the file you want to import.
- Click *Add*, and click *OK*.

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.



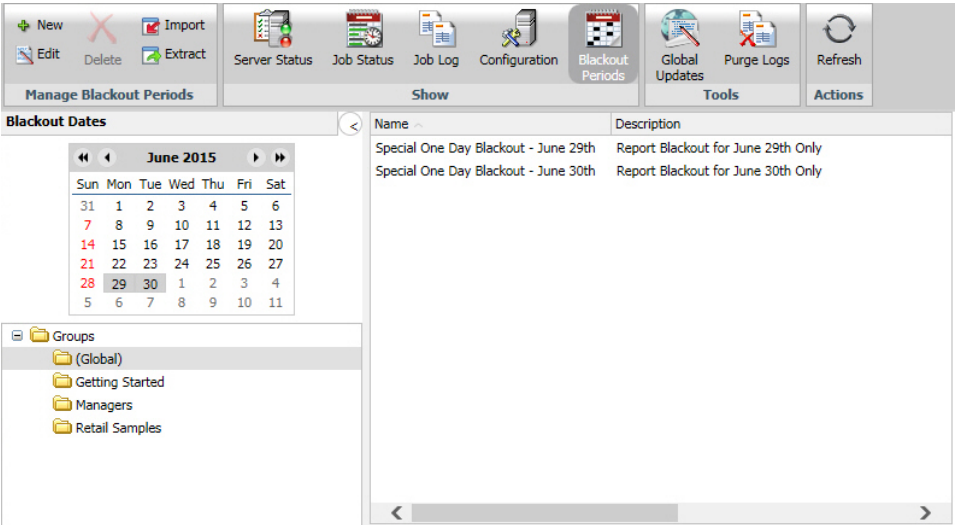
- Click *Add* to add the new Blackout Period profiles listed in the Import Blackout Data dialog box to the Blackout Dates Calendar and Group entries.

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.



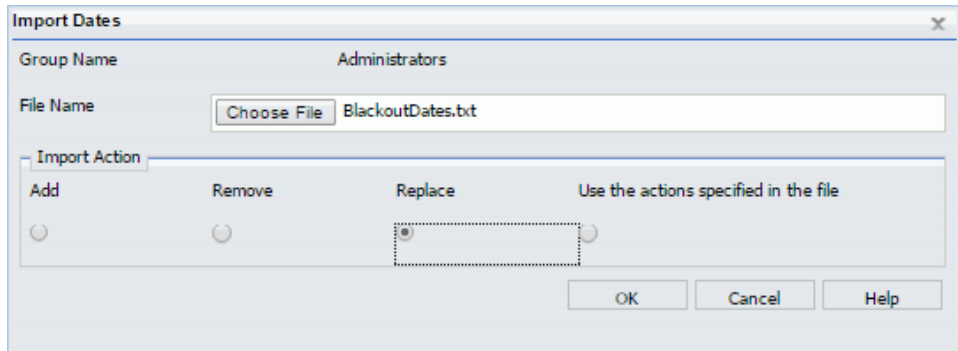
Procedure: How to Replace Blackout Periods Using an Import File

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.

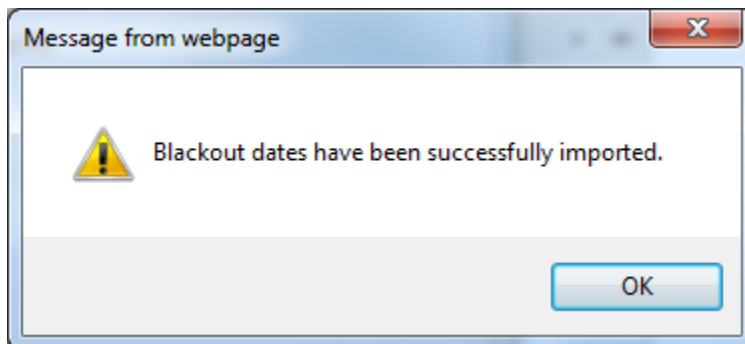


3. In the File Name field, type the full path to the file, or click *Browse* and navigate to the file you want to import.
4. Click *Replace*, and then click *OK*.

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*.

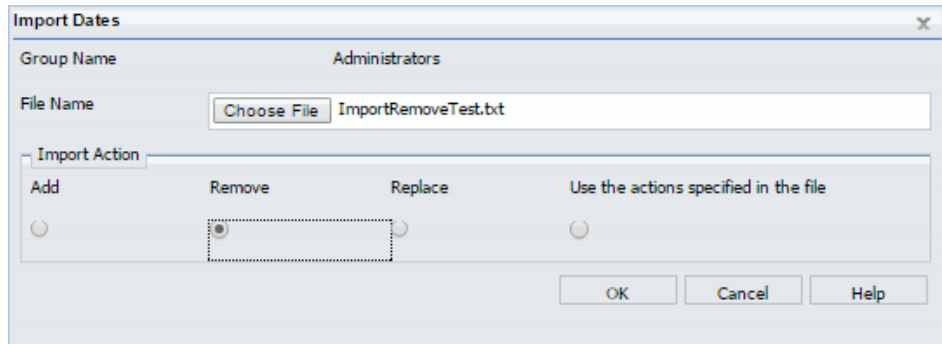
Enriched entries for the updated Blackout Period profiles appear in the right pane.

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*.

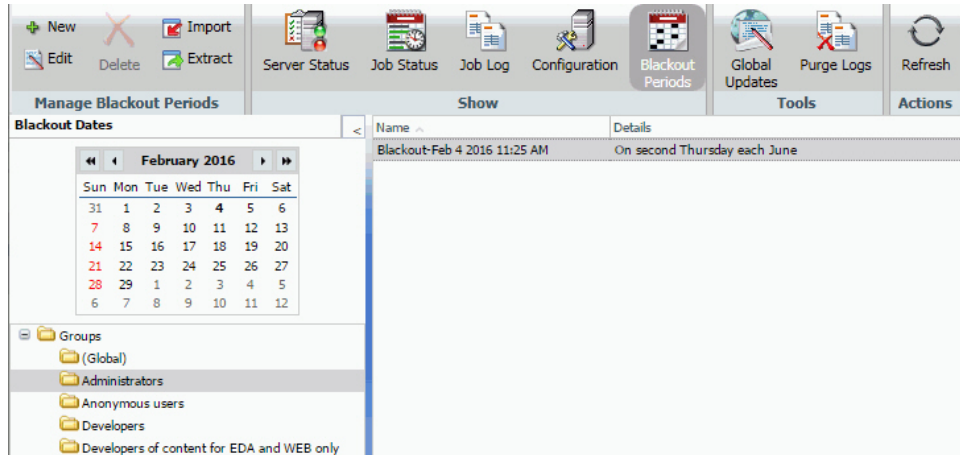
The Import Blackout Data dialog box opens, listing details from each entry in the Import file that successfully matched an existing Blackout Period profile.

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

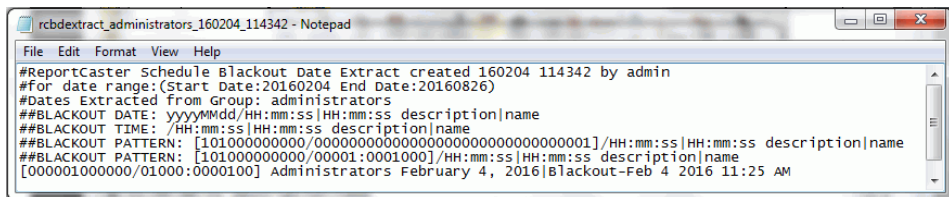
You can extract existing blackout period profile information from the ReportCaster Development Interface to a .txt file.

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.



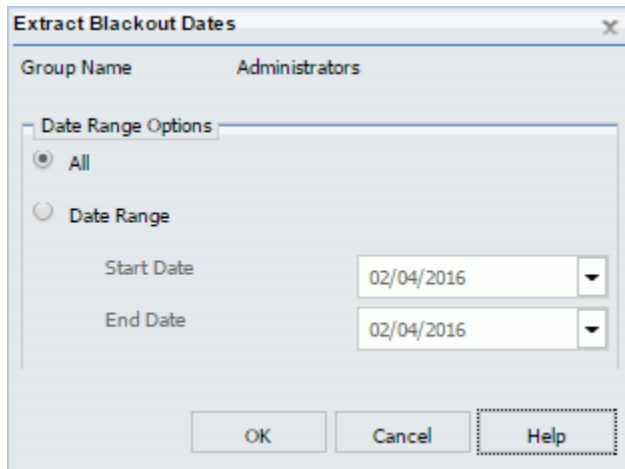
For more information about each entry type layout, see [Viewing Blackout Period Import File Format](#) on page 127.

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.

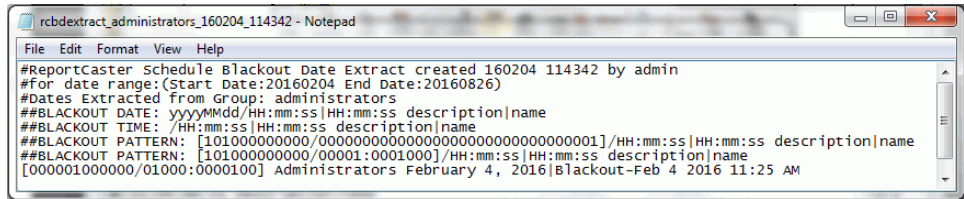


3. Select one of the following from the Date Range Options:
 - ☐ *All* to extract all currently saved blackout period profiles.
 - ☐ *Date Range* to specify the range of dates containing scheduled blackout period profiles that you want to extract.

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 for the values stored in schedules and distribution lists. Using the Global Updates interface, the following settings can be updated:

- ☐ Mail Server
- ☐ FTP Server
- ☐ Printer
- ☐ Email Address
- ☐ Email From
- ☐ Data Server

- ☐ Notification Type
- ☐ Notification Reply Address
- ☐ Notification Subject
- ☐ Notification Brief Message To
- ☐ Notification Full Message To

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).
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 and distribution lists.

Procedure: How to Make a Global Update for a Printer

1. In the Global Update interface, click the *Setting* drop-down list and select *Printer*.
2. Type the existing Printer in the *Old Value* box.
3. Type the new Printer in the *New Value* box.
4. Click *Update* to update the new Printer value in schedules and distribution lists.

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*.
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*.
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 and distribution lists.

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*.
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 and distribution lists.

Procedure: How to Make a Global Update for a Notification Type

1. In the Global Updates interface, click the *Setting* drop-down list and select *Notification Type*.

The notification options are:

- ☐ **Never.** ReportCaster will not send a notification of the schedule status under any circumstances. This is the default value.
- ☐ **Always.** Send a notification each time the schedule runs.
- ☐ **On Error.** Only send a notification when there is an error running the schedule.

For more information, see *Notification Options in the Basic Scheduling Tool*.

2. Select the existing value in the *Old Value* box.
3. Select the new value in the *New Value* box.
If the *Old Value* is *Never*, then the *Reply Address*, *Subject*, *Brief Message To*, and *Full Message To* fields will display. Provide each field with the necessary information.
4. Click *Update* to update the new Notification Type value in schedules and distribution lists.

Procedure: How to Make a Global Update for a Notification Reply Address

1. In the Global Updates interface, click the *Setting* drop-down list and select *Notification Reply Address*.
2. Type the existing Notification Reply Address in the *Old Value* box.
3. Type the new Notification Reply Address in the *New Value* box.
4. Click *Update* to update the new Notification Reply Address value in schedules and distribution lists.

Procedure: How to Make a Global Update for a Notification Subject

1. In the Global Updates interface, click the *Setting* drop-down list and select *Notification Subject*.
2. Type the existing Notification Subject in the *Old Value* box.

3. Type the new Notification Subject in the *New Value* box.
4. Click *Update* to update the new Notification Subject value in schedules and distribution lists.

Procedure: How to Make a Global Update for a Notification Brief Message To

1. In the Global Updates interface, click the *Setting* drop-down list and select *Notification Brief Message To*.
2. Type the existing Notification Brief Message To in the *Old Value* box.
3. Type the new Notification Brief Message To in the *New Value* box.
4. Click *Update* to update the new Notification Brief Message To value in schedules and distribution lists.

Procedure: How to Make a Global Update for a Notification Full Message To

1. In the Global Updates interface, click the *Setting* drop-down list and select *Notification Full Message To*.
2. Type the existing Notification Full Message To in the *Old Value* box.
3. Type the new Notification Full Message To in the *New Value* box.
4. Click *Update* to update the new Notification Full Message To value in schedules and distribution lists.

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 Job Logs on Demand

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

WebFOCUS Business User Edition 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.

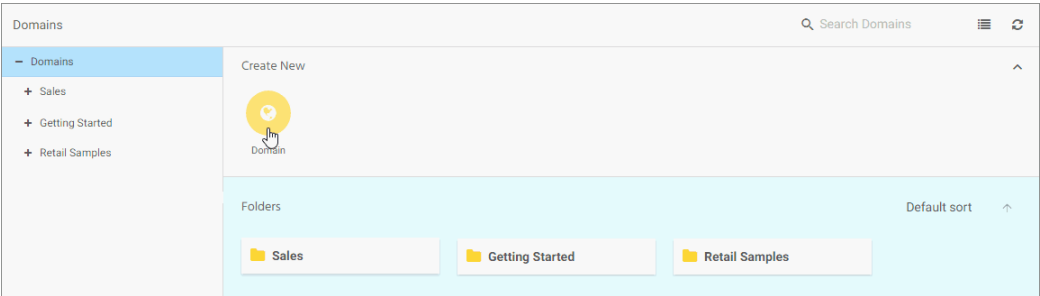
Domains comprise a collection of groups, an Application folder on the Reporting Server, and a set of rules that makes them all work together in a single workgroup. Domains partition content and metadata, and enable Managers to organize and store your content in the portal. They are the place where Developers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

Procedure: **How to Create a Domain**

1. Sign in as a Manager.
2. On the Home page, in the Resources tree, click *Domains* if it is not highlighted already.
or

In the breadcrumb trail, click *Domains*.

3. On the actions bar, click *Domain*, as shown in the following image.



4. In the Title field, type a description of the domain, as shown in the following image.

A screenshot of the 'New Domain' dialog box. It has a title bar 'New Domain' with a close button. Inside, there are two text input fields: 'Title' with the value 'Human Resources' and 'Name' with the value 'Human_Resources'. At the bottom right are 'OK' and 'Cancel' buttons.

As you type, the description you type in the Title field is automatically assigned to the Name field and adjusted to conform to format rules for file names.

Domain Titles appear in the Resources tree and in the content area. Domain Names are internal identifiers and are not shown to users.

5. Click *OK*.

Note: Within the new domain, a Hidden Content folder and a My Content folder are created for each user. The Hidden Content folder can be used to store items that are related to the domain but that should not be visible to other users, such as schedules that distribute output back to the domain, image files or style sheets used by charts. The My Content folder stores personal content for each user. Some users can share personal content with other domain users. Domain Developers and Managers can create folders and content within the domain and publish their content to enable domain users to access and interact with it.

Managing Domain Users

When a Manager creates a new domain, WebFOCUS Business User Edition automatically creates a new group for the domain itself, along with 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 159.

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, a 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. Managers can manage private resources by user, group, or domain.

Deleting Domains

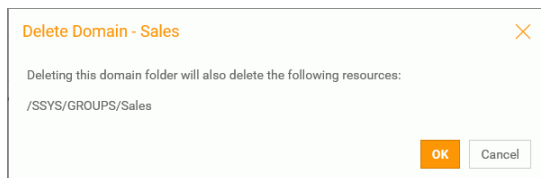
A domain can only be deleted by a Manager who has rights to delete all of the resources within it.

The process that deletes a domain first removes all users from groups in the domain, and then cascade deletes the groups and rules that were created with it.

Note: The cascade delete process only removes users from groups within a domain. It does not delete the users themselves.

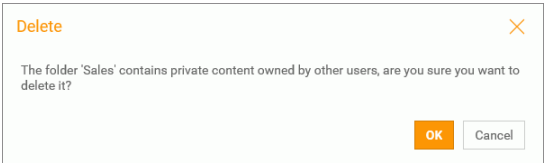
Procedure: How to Delete a Domain

1. Sign in as a Manager.
2. On the Home page, in the Resources tree, or in the content area, right-click a domain folder, and then click *Delete*.
3. When you receive a message advising you that this process will delete all resources created by this domain folder, click *OK* to delete the domain and associated resources, as shown in the following image.



Note: In this message, the list of resources that will be deleted depends upon the resources that were originally included in the domain. Therefore, the details in this message will vary with each deleted domain.

4. If you receive a message warning that the folder contains private content, as shown in the following image, click *OK* to delete the domain and its private content, or click *Cancel* to end the process without deleting the domain.



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 typically displayed to users. The file name is used as an internal reference 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**

In order to view the properties of a folder, right-click a folder in the Resources tree or content area of the Home page, and then click *Properties*. The Properties panel opens, displaying the information in the following table.

Item	Description
General Tab	

Item	Description
Language	Displays the language in which the folder and its content were created. The list attached to this field contains all languages made available by your code page selection.
View All	<p>Opens the Language Properties dialog box that identifies the list of available languages and the default language selected for the folder.</p> <p>The default language specified in this dialog box is the language in which the folder and its contents were created and are displayed, by default.</p> <p>The folder name and description appear next to the selected default language option.</p>
Title	Displays the title that appears on the folder when it is displayed in the Resources tree or content area. This is the title by which end users identify the folder, and is typically based on the contents in it.
Name	Displays a unique internal reference to the folder. This is the name used to identify the folder for internal operations. This field is dimmed and unavailable by default. Click the <i>Change Name</i> icon next to it to make this field available for name changes.
Summary	Displays a detailed explanation that provides additional information about the folder.
Path	Displays the full repository path of the parent folder.
Created	Displays the date and time the folder was created.
Modified	Displays the date and time the folder was last modified. and the ID of the user who last modified the folder.
Accessed	Displays the date and time the folder was last accessed by the Properties, Run, or Run Deferred commands, or by any of the edit tools used to update the folder. It also displays the ID of the user or tool that last accessed the folder.
Owner	Displays the ID of the User to whom the folder is currently assigned.
Publish	Specifies whether the folder and its contents are published or not.

Item	Description
Show	Specifies whether to display the folder to users who are not permitted to create content in it. This option is primarily used when the folder needs to be made temporarily unavailable to end users who would otherwise be permitted to view or work with the content in the folder.
Advanced Tab	
Folder Properties	
Automatically create My Content folders	When this check box is selected, a My Content folder is created for users with the My Content Folder privilege, giving the user a place to save the personal reports, charts, or documents that they may create using InfoAssist or other report and distribution features, such as Save Parameter reports.
Automatically open	If this check box is selected, when you open the Home page, this domain folder is automatically expanded in the Resources tree to display the My Content folder and the other folders that this folder contains. In addition, the content area automatically displays the folders and items assigned to this folder.
Explorer/Portal Properties Group	
Sort order	Specifies the order in which the folder is listed in the Resources tree and in the content area.

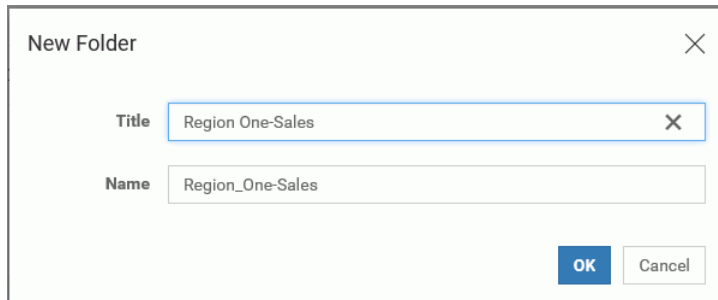
Procedure: How to Create a Folder

1. On the Home page, in the Resources tree, click the parent folder that will contain the new folder.

Or

In the breadcrumb trail, click the link to the parent folder that will contain the new folder.

2. In the New Folder dialog box, type the title for the new folder, as shown in the following image.

A screenshot of the 'New Folder' dialog box. The dialog has a title bar with 'New Folder' and a close button (X). Inside, there are two text input fields. The first field is labeled 'Title' and contains the text 'Region One-Sales'. The second field is labeled 'Name' and contains the text 'Region_One-Sales'. At the bottom right, there are two buttons: 'OK' (highlighted in blue) and 'Cancel'.

As you type, the description you type in the Title field is automatically assigned to the Name field and adjusted to conform to format rules for file names. The Name field automatically converts any spaces or special characters you type in the Title field into underscore characters. If you type an unbroken string of multiple special characters, such as &&&, in the Title field, the Name field automatically converts them into a single underscore character. If you prefer, you can modify the Name, later.

3. Click *OK*.

The new folder appears in your selected location in the Resources tree and in the content area of the Home page.

4. In order to add an optional summary description of the folder:
 - a. Right-click the new folder, and then click *Properties*.
 - b. On the Properties panel, type the description in the Summary field.
 - c. Click *Save* to save the description, and then click *Cancel* to close the Properties panel.

Procedure: How to Publish a Folder

In the Resources tree or content area of the Home page, right-click a folder, and then click *Publish*.

The Resources tree refreshes and no longer displays the folder name in italics. The content area refreshes, removes the border from the folder, and displays the folder icon in full color.

Procedure: How to Unpublish a Folder

In the Resources tree or content area of the Home page, right-click a folder, and then click *Unpublish*.

The Resources tree refreshes and displays the folder name in italics. The content area refreshes, displays a border around the folder, and displays the folder icon in gray.

Procedure: How to Duplicate a Folder

In the Resources tree or content area of the Home page, right-click a folder and then click *Duplicate*.

In the Resources Tree, a duplicate folder appears beneath the original folder. In the content area, the duplicate folder appears immediately to the right of the original or below it. 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.

Note: The Duplicate command creates a copy of the folder in the same location as the original. Use the Copy and Paste commands if you need to move a copy of a folder to a different location.

Procedure: How to Cut or Copy and Paste a Folder

1. In the Resources tree or content area of the Home page, right-click a folder, and then click *Cut* if you want to move the folder, or click *Copy* if you want to create a copy of the folder and leave the original folder in place.
2. In the Resources tree, click the folder that represents the new location. Expand the tree to display the new location if necessary.

or

If the new location appears on the Breadcrumbs trail, click the folder that represents the new location.

3. In the Resources tree, right-click the folder that represents the new location, and then click *Paste*.

or

Right-click anywhere in the content area of the new location, and then click *Paste*.

The Resources tree and the content area refresh and display the folder.

Folder names must be unique within a specific location. If you paste the folder to 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 you pasted the copy of the folder into the same 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 you paste the folder. Folder titles are updated in the same way as folder names.

Procedure: How to Change a Folder Title

1. In the Resources tree or content area of the Home page, right-click a folder, and then click *Properties*.
2. On the Properties panel, type the new Title in the Title field, and then click *Save*.
The folder name is updated. If the new name changes the position of the folder in alphabetical order, the folder is also relocated on the Resources tree and within the content area.
3. When your updates are complete, click *Cancel* to close the Properties panel.

Procedure: How to Delete a Folder

1. In the Resources tree or content area, right-click a folder, and then click *Delete*.
2. When you receive a message asking you to confirm the decision to delete the folder, click *OK*.
The Resources tree and the content area refresh and remove the deleted folder.

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 WebFOCUS Business User Edition. Managers and Group Administrators can assign users with similar responsibilities to one of the user type groups that are created automatically 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.

Each user in the repository is defined by a unique name and may also be assigned a description, an email address, and a password. The user must be placed in a group at account creation and assigned a status. By default, the user is placed in the EVERYONE group, which is the group of all users in the system, and assigned the Active status.

Any of these characteristics, except the unique user name, may be edited later by a Manager.

Understanding User Name Requirements

Because user names are defined within the repository, they need to conform to the format rules and character limitations it imposes. If your installation supports external authentication, such as that provided by Microsoft Active Directory, user names also exist in an external repository, and must conform to the format rules defined in it.

The set of characters you can use to create user names is defined by the current character encoding setting established in the application server and the Client Code pages assigned to your NLS setting. For example, if the application server is configured to support UTF-8 encoding, and the NLS Setting is also configured to support the US Unicode (UTF) code page, you can use characters in the double-byte character set (DBCS) to create user names.

To support those installations that rely on external LDAP or Active Directory authentication, user names in WebFOCUS Business User Edition support all of the characters supported by the sAMAccountName standard. Note that the range of allowable characters for User Names in WebFOCUS Business User Edition is broader than the range for the sAMAccountName standard, and administrators must be careful to avoid including characters allowed by WebFOCUS Business User Edition but prohibited by the sAMAccountName standard in user names.

Given these considerations, when creating user names, take the following rules into account:

- ☐ User names may contain alphanumeric characters, spaces, and underscores.
- ☐ Depending upon the Client Code Page assigned to your NLS setting, user names can also include single-byte or double-byte NLS characters.

Note: To prevent sign-in issues, and to conform to sAMAccountName best practices, replace characters that contain accents or other diacritical marks in user names with characters that exclude them. For example, convert Müller into Muller.

- ☐ The following characters are not supported in user names: “|;/*,?”


Note: if your user names must conform to sAMAccountName standards, you must independently ensure that user names also exclude the following characters: [] : = + < > \

- ☐ It is recommended that you limit user names to 64 characters. Longer user names may cause problems during migration.
- ☐ Do not end user names with a period (.) .

If you support external authentication, avoid including characters in user names that your external authentication repository does not support. For more information about which characters to avoid, contact Customer Support Services.

Procedure: How to Create a User

Note: Only a Manager can create a user.

1. In the Security Center, on the Users & Groups tab, click the *New User* button .

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

2. Type the user name, and optionally, type the description, email address, password, and password confirmation, and if desired, select a group and a status for the user.
3. When your input is complete:
 - a. Click *OK* to create the user and close the New User dialog box.
 - b. Click *Create* to create the user without closing the New User dialog box.

Use this button when you need to create additional users without delay. When you click this button, the New User dialog box clears, a new entry for the user appears in the Users pane of the Security Center, and you can return to the previous step to add the next user.

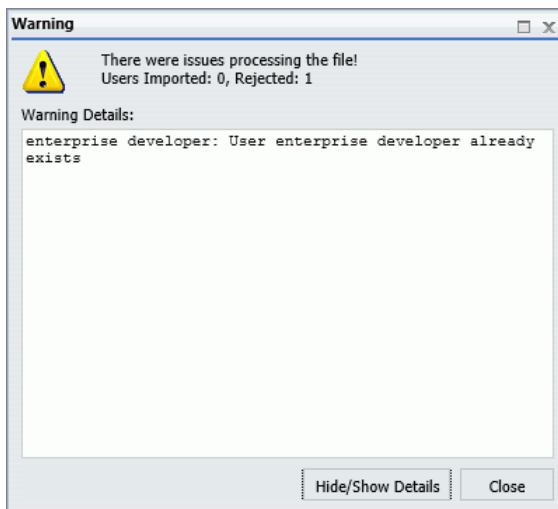
If you do not enter a description, the description defaults to the name. If you do not select a group and status for the user, the user will be created in the EVERYONE group and assigned the Active status, by default.

If you are creating a user that will be authenticated externally using AD or LDAP, and you want to synchronize user information with the authentication provider, leave the email and description fields blank.

Importing Users

The Import User command automatically creates new user accounts by importing user information from a comma-separated values (.csv) text file and transferring those records to the user accounts database in the repository. This operation streamlines the creation of multiple user accounts by eliminating the necessity to open the New User dialog box, type, and save the details for each new user account, individually.

The import does not overwrite records of existing users, nor can you use it to delete existing user records. If a record in the user import file matches an existing user account, the import generates a message identifying the record that could not be imported, as shown in the following image.



Understanding User Import File Layout and Format Requirements

You can create a new user import file by typing user information into any text editor and saving it as a comma-separated values (.csv) file. If you are exporting user information from an external source, you can create a user import file by reorganizing and reformatting the exported information, as necessary, and then saving the exported user information in a .csv file. Regardless of the method you use, you must ensure that all user import files you create conform to the format and layout requirements described in this topic and that the information within those user records conforms to the requirements described in [Understanding User Record Field Format Requirements](#) on page 153.

The user import file must not contain a header or column heading line. The first line in the file must contain the first user record. From that point on, each line within the user import file contains the record for a single new user. Multiple user records must not be placed on the same line. Because the import will end when it encounters the first blank line, do not include any blank lines between user records.

User import files that contain only those NLS characters used in the U.S. English or Western Europe code page 137 require no special encoding. However, user import files containing NLS characters from other code pages require UTF-8 encoding, without a byte order mark (BOM). To encode a user import file for UTF-8, open it in a third-party editor, change the appropriate setting to specify that the file uses UTF-8 encoding, and save it with that value.

Each user record contains the following fields: user name, password, description, email address, user status, and groups, as shown in the following image.

```
testbas,password,Getting Started Basic User,testbas@domain.com,ACTIVE,Getting_Started/BasicUsers
testadv,password,Getting Started Advanced User,testadv@domain.com,ACTIVE,Getting_Started/AdvancedUsers
testdev,password,Getting Started Developer,testdev@domain.com,ACTIVE,Getting_Started/Developers
testgrp,password,Getting Started Group Admin,testgrp@domain.com,ACTIVE,Getting_Started/GroupAdmins
testdevgrp,password,Getting Started Dev-Grp Admin,testdevgrp@domain.com,ACTIVE,Getting_Started/Developers;Getting_Started/GroupAdmins
testbas2,password,Getting Started Basic User 2,testbas@domain.com,INACTIVE,Getting_Started/BasicUsers
testbas3,password,Getting Started Basic User 3,testbas@domain.com,MUSTCHANGE,Getting_Started/BasicUsers
```

Within a user record, each field is separated by a comma. If the value assigned to a field includes a comma, the value in that field must be enclosed within quotation marks ("). For example the following new user record contains a comma in the third field, the description field, and is enclosed in quotation marks ("):

```
testadv,password,"Getting Started, Advanced
User",testadv@domain.com,ACTIVE,Getting_Started/AdvancedUsers
```

If a field in a user record contains no information, the record must still define a placeholder for the blank field by leaving two commas with no characters between them in the appropriate place in the record. For example, the following new user record omits the password typically found in the second field of a user entry:

```
testbas,,Getting Started Basic User,testbas@domain.com,ACTIVE,Getting_Started/BasicUsers
```

Understanding User Record Field Format Requirements

When creating a user record, ensure that the values you assign to individual fields conform to the following requirements:

- ❑ **User Name.** Names assigned to imported users are subject to the same restrictions on valid characters as those entered directly in the new user dialog box. For a detailed description of user names and the range of characters that you can include in them, see [Understanding User Name Requirements](#) on page 149.

- ❑ **Password.** You can assign a generic one-time password, such as *password*, to the password field, or you can assign one of the hashed passwords from the UOA_USERS table.
- ❑ **Description.** Leave this field blank if you have activated the Synchronize User Information setting, which is located on the External page of the Security tab of the Administration Console. Otherwise, type the full name of the user or a brief description in this field. The activation of the Synchronize User Information setting allows for automatic updates to the value in this field from an external authentication or authorization provider.
- ❑ **Email Address.** Leave this field blank if you have activated the Synchronize User Information setting, which is located on the External page of the Security tab of the Administration Console. Otherwise, type the email address for the new user. The activation of the Synchronize User Information setting allows for automatic updates to the value in this field from an external authentication or authorization provider.
- ❑ **User Status.** Type ACTIVE, INACTIVE, or MUSTCHANGE in this field to identify the initial status of the user when the new user account is created. Each of these values must be typed in uppercase characters. If you type ACTIVE, the user represented by the account can sign in and work within WebFOCUS Business User Edition as soon as the account is created. If you type INACTIVE, the user represented by the account can sign in and work with WebFOCUS Business User Edition only after a Manager has changed the status of that user account to Active. If you type MUSTCHANGE, the user represented by the account is prompted to change his or her one-time password the first time he or she signs in to WebFOCUS Business User Edition.
- ❑ **Groups.** Type the name of the group or groups to which the user is assigned. If you do not include a value in the group name field, the user will be assigned to the EVERYONE group automatically. If you do include a group name, make sure that it matches the spelling and capitalization of its corresponding existing group name exactly.

The format for a group name is the domain name, followed by a slash mark (/), and the group name. For example, the following new user record adds a user to the AdvancedUsers group of the Getting_Started domain, as shown in the last field in the record.

*testadv,password,Getting Started Advanced
User,testadv@domain.com,ACTIVE,Getting_Started/AdvancedUsers*

You can include more than one group name in this field. If you choose to do so, separate each group name with a semi-colon. For example, the following new user record adds a user to the Developers group *and* to the GroupAdmin group within the Getting_Started domain, as shown in the last field in the record.

*testdevgrp,password,Getting Started Dev-Grp
Admin,testdevgrp@domain.com,ACTIVE,Getting_Started/Developers;Getting_Started/
GroupAdmins*

To prevent a user record from failing to load, any group that you identify in it must already be defined within WebFOCUS Business User Edition. You cannot use the import user operation to load new groups as well as users simultaneously.

Procedure: How to Import Users

Before you begin, ensure that all groups that are identified in the user import file already appear in the Groups pane of the Security Center, and create any groups or domains that do not appear.


1. In the portal, on the Menu bar, click *Administration*, and then click *Security Center*.
2. On the Users & Groups tab, click *Import Users*.
3. In the Import Users dialog box, click *Browse*.
4. In the Choose File to Upload dialog box, navigate to the .csv file that contains the users to import and double-click the entry, or click it, and then click *Open*.
5. In the Import Users dialog box, ensure that the name of the file that contains user records for import appears in the File to Import field, and if so, click *Import*.

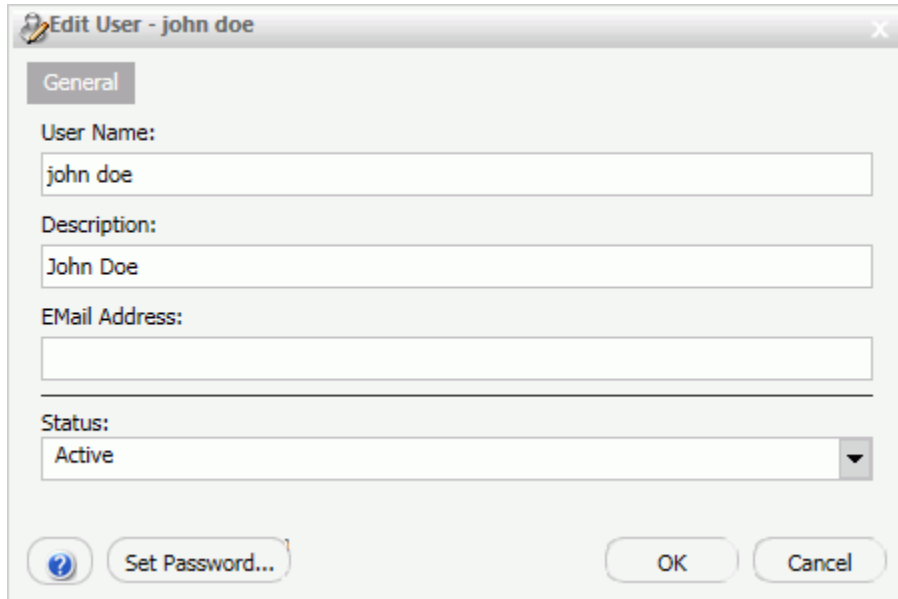
The import operation creates new user accounts for the users specified in the file records, and assigns the new users to the groups specified in each record.

- a. If you receive a message stating that there were issues processing the file, click *Hide/Show details*, review the issues listed in Warning Details dialog box, and update the import user file text or layout to address them.
- b. When your updates are complete, save the revised user import file, close the Warning Details dialog box, and return to step 2 to run the import again.
6. When the import is complete, click *Close* in the Import Users dialog box.
7. Review the Users pane and the Users in Group pane to ensure that the full set of new users was imported, and that they were appropriately assigned to all groups.

Procedure: How to Edit User Details

Only a Manager can edit user details.

1. In the 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.

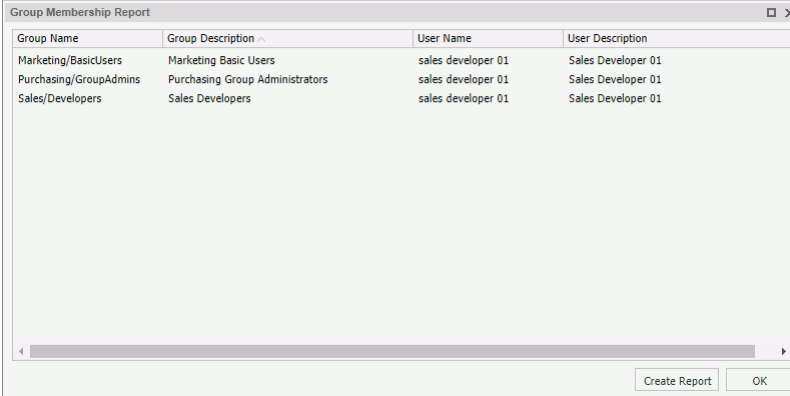
1. In the portal, on the Menu bar, click *Administration*, and then click *Security Center*.

- 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.

Understanding the Group Membership Report

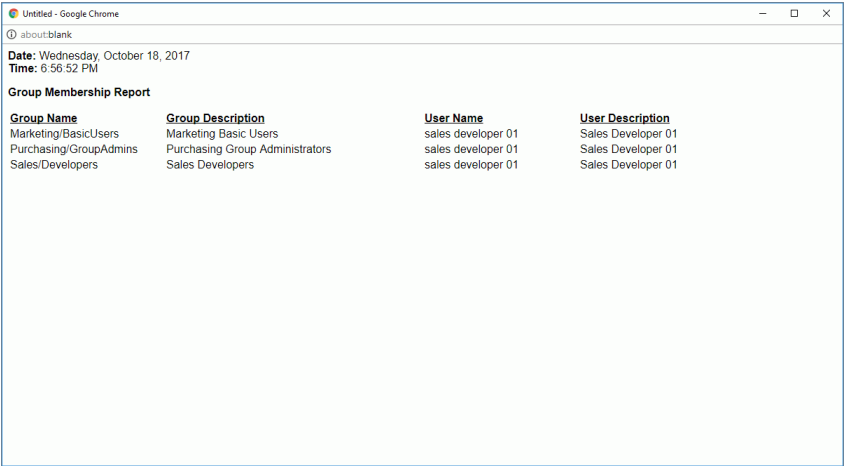
The Group Membership report lists all groups to which an individual user or selected group of users is currently assigned. The list entry for each group assignment identifies a Group Name, Group Description, User Name, and User Description, as shown in the following image.



Group Name	Group Description ^	User Name	User Description
Marketing/BasicUsers	Marketing Basic Users	sales developer 01	Sales Developer 01
Purchasing/GroupAdmins	Purchasing Group Administrators	sales developer 01	Sales Developer 01
Sales/Developers	Sales Developers	sales developer 01	Sales Developer 01

By default, the report lists entries in ascending order by Group Name. You can reorganize this default display by clicking column headings to sort the report entries in ascending or descending order based on the values in that column.

From this dialog box, you can also create an HTML version of the report, as shown in the following image.



Using commands in your browser, you can save this version of the report or send it by email to an external reviewer.

The Date and Time that appear on the HTML version of the Group Membership report use the default, locale-sensitive time format (24 hours or 12 hours AM/PM) assigned to the machine on which WebFOCUS Business User Edition is installed. Therefore, if you select a different language when you sign in to WebFOCUS Business User Edition, dates and times continue to appear in the format used by the default locale of your machine instead of the format required by the language you selected.

For example, if you install WebFOCUS Business User Edition on a machine that runs on the Windows operating system, uses English as the default language, and uses a locale-sensitive time format of 12 hours AM/PM instead of 24 hours, WebFOCUS Business User Edition displays all times in the 12 hour AM/PM format. Even if you configure WebFOCUS Business User Edition to use the UNICODE code page and include the Japanese Locale in the Dynamic Language Switch settings, times on this report and throughout the user interface continue to use the 12 hour AM/PM format. You cannot change the time display to a 24-hour time format unless you also add Japanese to the Windows Language configuration and change to a 24-hour time format within the Windows Date and Time settings on the machine that runs WebFOCUS Business User Edition.

Procedure: How to Create a Group Membership Report

1. In the Security Center, do one of the following:
 - ☐ To base the report on an individual user, in the Users pane, right-click the entry of your selected user.
 - ☐ To base the report on a group of adjacent users, in the Users pane, click the first user entry, hold down the Ctrl key, click on the final user entry, and then right-click your selection.
 - ☐ To base the report on a group of non-adjacent users, in the Users pane, hold down the Ctrl key, click on all of the individual entries you want to include in the report, and then right-click any selected entry.
2. When your selections are complete, in the shortcut menu, point to *Groups*, and then click *Group membership report*.
 The Group Membership report dialog box opens, displaying all group assignments for your selected users.
3. To rearrange the report entries, click any column heading to list report entries in ascending or descending order based on the values in that column.
4. To produce an HTML version of the report, click *Create Report*.
 Use the commands in your browser menu to print, save, or send the report.
5. To close the dialog box, click *OK*.

Managing Groups

In WebFOCUS Business User Edition, 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

Groups are created automatically whenever a Manager creates a new Domain and deleted 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.

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

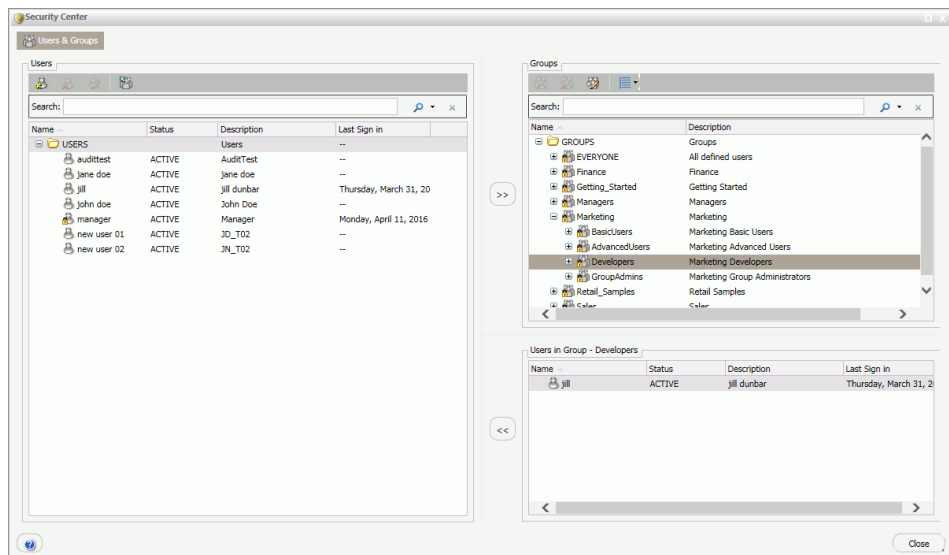
Only Managers and Group Administrators can add users to groups.

1. In the 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 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. 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 Business User Edition to authenticate users against your corporate Active Directory. The WebFOCUS Business User Edition Client passes User sign-in credentials to the WebFOCUS Business User Edition Reporting Server, which in turn, validates them within an external source. WebFOCUS Business User Edition can authenticate users against external Active Directory or LDAP directories. Users are externally authenticated whenever they access WebFOCUS Business User Edition 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 Business User Edition synchronizes user information with Active Directory. Managers no longer need to maintain separate passwords for WebFOCUS Business User Edition.
- ❑ **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 Business User Edition 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 WebFOCUS Business User Edition 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 Business User Edition 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 both in WebFOCUS Business User Edition and in Active Directory so that you can use it for access to WebFOCUS Business User Edition once you have restarted it in its new authentication configuration.

2. Configure the LDAP provider to authenticate users to Active Directory.
3. Configure WebFOCUS Business User Edition to use the LDAP provider and restart the WebFOCUS Business User Edition services.

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

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 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 as a Manager.
2. In the 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 installation.

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

The password was assigned during 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. WebFOCUS Business User Edition 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 Business User Edition.
14. Stop and restart the web application to make these changes take effect. To do so:

If this installation is based on the Windows operating system, stop and restart the WebFOCUS Business User Edition Application Server service in the Services Window.

If this installation is based on the Linux operating system, navigate to the tomcat/bin directory 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 Manager that you identified at the beginning of the configuration.

The user description on the Menu bar in the portal, and the Email Address of this account now reflect the values retrieved from the Active Directory.

Creating User Accounts When WebFOCUS Business User Edition is Configured for Active Directory Authentication

Now that you have configured WebFOCUS Business User Edition to authenticate users to Active Directory, you can create user 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 and assign 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 `getting_started_sample_users.csv` file located in the installation directory as a template. You can leave the password, user description and email values blank, but you need to preserve the same number of 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 the Security Center. The file should contain only data rows with the required number of commas on each row and contain no blank lines. For example:

```
user1, , , ACTIVE,
```

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

Configuring WebFOCUS Business User Edition for SSL

The Hypertext Transfer Protocol over Secure Socket Layer (https) establishes an encrypted Secure Socket Layer (SSL) connection, and should be used to secure communications between WebFOCUS Business User Edition and browsers assigned to end users. There are many configuration options that enable the use of this protocol, one of which is the Apache Tomcat configuration, as described in this section. WebFOCUS Business User Edition uses this configuration by default.

To activate Secure Socket Layer-based communications, create a self-signed certificate for Java. You can optionally submit it to a Certificate Authority to establish it as a trusted certificate. The `keytool` utility that creates the certificate also modifies the connection type from open to SSL. Therefore, you must comment out the default Connector Protocol setting in the Tomcat `server.xml` file, and ensure that a setting for the new SSL Connector Protocol appears there instead.

Procedure: How to Create a Self-Signed Certificate

To create a Self-Signed Certificate with Java:

1. Open the command prompt window and redirect the command prompt to the following directory:

```
drive:\ibi\WebFOCUS_BUE82\jre\bin
```

2. Type the keytool command and values as shown in the following example.

```
keytool -genkeypair -alias mykey -ext san=dns:dnsName1,dns:dnsName2... -  
keyalg RSA -validity 720 -keystore /path_to_keystore/keystore -keysize  
2048 -storepass MyPassword
```

where:

dnsName

Is the name, or alias, of the entity (the subject) that will present this certificate for authentication. You can include multiple names to ensure that all versions of the subject names are recognized. For multiple alternative names use the syntax, *dns:first_dnsName,dns:second_dnsName and so on*.

For example, *dns:bue,dns:bue.ibi.com*.

MyPassword

Is the password for this keystore. You can accept MyPassword, the default value, or you can replace it with a unique password by typing it in this field.

/path_to_keystore/keystore

Is the location information that specifies where the key file will be placed. This value is optional. If you do not specify a location for the key file, the Keytool utility places it in the default location.

Note: The name mykey is important if you need to issue a -certreq (certificate request) for a certificate signed by a Certificate Authority.

3. Press Enter.

The command prompt displays the first in a series of questions.

4. Respond to each question as follows:

- ☐ "What is your first and last name?" Type the first and last name of the certificate holder.
- ☐ "What is the name of your organizational unit?" Type the name of the organizational unit of the certificate holder.
- ☐ "What is the name of your organization?" Type the name of the organization of the certificate holder.
- ☐ "What is the name of your City or Locality?" Type the name of the city or locality of the certificate holder.
- ☐ "What is the name of your State or Province?" Type the two-letter abbreviation for the state in which the certificate holder is located.

- ❑ “What is the two-letter country code for this unit?” Type the two-letter abbreviation for the country in which the certificate holder is located.
- 5. When the command prompt displays the question, “Is CN=__, OU=__, O=__, L=__, ST=__, C=__ correct?”, review the values and type *y* if they are correct.

If they are not correct, Type *n* and retype the keytool command from step 2.

If they are correct, the new Self-Signed Certificate is ready for use.

Establishing the Self-Signed Certificate as a Trusted Certificate

Until you identify the new self-signed certificate to the browser as a Trusted Certificate, the browser will display errors when you use it. During the initial testing period, you can add the new self-signed certificate directly to the Trusted Certificate Authority of those browsers included in the test. However, to fully establish the new certificate as a trusted certificate, you typically request certification for it from a Certificate Authority using the following request:

```
keytool -certreq -alias mykey -storepass MyPassword -file ./mykey.csr -
keystore /path_to_keystore/keystore
```

where:

MyPassword

Is the password for this keystore. You can accept MyPassword, the default value, or you can replace it with a unique password by typing it in this field.

/path_to_keystore/keystore

Is the location information that specifies where the key file will be placed. This value is optional. If you do not specify a location for the key file, the Keytool utility places it in the default location.

You can then send the certificate request file (mykey.csr) to a Certificate Authority to sign, and when the authority returns the signed certificate, import it into the keystore.

Importing the Trusted Certificate into the Keystore

To import your certificate from the CA, type the following command:

```
keytool -import -alias mykey -file ./mykey.crt -keystore /path_to_keystore/
keystore
```

where:

/path_to_keystore/keystore

Is the location information that specifies where the key file will be placed. This value is optional. If you do not specify a location for the key file, the Keytool utility places it in the default location.

If your CA is an internal CA, then type the following command to import the certificate from your Certificate Authority.

```
keytool -import -alias CA -trustcacerts -file ./ca.crt -keystore /  
path_to_keystore/keystore
```

where:

/path_to_keystore/keystore

Is the location information that specifies where the key file will be placed. This value is optional. If you do not specify a location for the key file, the Keytool utility places it in the default location.

Updating the Connector Protocols in the Tomcat Server.xml File

The Tomcat server.xml file is located in the following directory:

drive:\ibi\WebFOCUS_BUE82\tomcat\conf

The keytool utility disables the http connection assigned to port 26000. Therefore you must comment out the Connector tag in the server.xml file that defines this http-based connection by typing an exclamation point (!) after the open tag symbol (<).

```
<Connector connectionTimeout="20000" maxPostSize="-1" port="26000"  
protocol="HTTP/1.1" redirectPort="26001" useBodyEncodingForURI="true"/>
```

The keytool utility also establishes an SSL connector on port 443. This connection replaces the old http based connection. Therefore, if it does not appear in the file, you must type this updated version of the connector tag, with its attributes and values, as shown in the following example.

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol" port="443"  
SSLEnabled="true" keystoreFile="C:/users/path_to_keystore/keystore"  
keystorePass="MyPassword" maxThreads="150" scheme="https" secure="true"  
clientAuth="false" sslProtocol="TLS"  
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA"/>
```

where:

/path_to_keystore/keystore

Is the location information that specifies where the key file will be placed. This value is optional. If you do not specify a location for the key file, the Keytool utility places it in the default location.

MyPassword

Is the password for this keystore. You can accept MyPassword, the default value, or you can replace it with a unique password by typing it in this field.

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.

Note: Execution IDs and passwords cannot be imported or exported through the Change Management utility. A new Execution ID and password must be created on the selected system.

Working With CM Zip Files

The zip file format compresses the resources that make up a change management package into a single file, delivering the advantages of speed and security to change management packages. They are especially useful when you must transfer change management packages from one physical location to another. Their compressed and consolidated format captures all files included in a change management package into a single file that can be emailed, copied, or cut and pasted from a source folder on one network component to a target folder on another.

WebFOCUS creates change management zip files, called CM zip files, by default. To disable this feature, clear the Zip Change Management Package (IBI_CM_ZIP) check box, which is found on the Change Management page of the Configuration tab in the Administration Console. When this feature is disabled, change management packages use the uncompressed CM file format.

The default CM zip file name format is NAME_DATE_TIME_USERID, which combines the name of the change management package, with the date and time on which it was created, and the ID of the user who created it. For example, retail_samples_20160504_161133_administrator.zip. To specify an alternative format for CM zip file names, select a template from the Name format of Zip export files (IBI_CM_ZIP_FILE_FORMAT) setting, which is found on the Change Management page of the Configuration tab in the Administration Console.

Procedure: How to Create a Change Management Extract Package

Only members of the Managers group have access to the Change Management feature, which is available as a node that contains two subfolders: Import and Export on the WebFOCUS Resources panel. To open the WebFOCUS Resources panel, in the portal Menu bar, click *Resources*.

The steps required to create a Change Management Package are:

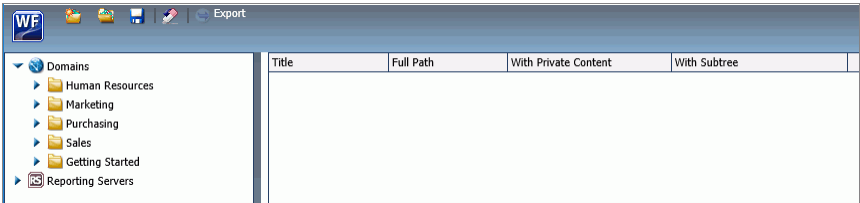
- 1. **Create a Scenario.** Utilizing the Change Management Export facility, an authorized user creates a scenario by selecting the resources to be exported. A scenario is a description of all the resources that will be exported into a Change Management Export Package.
- 2. **Export a Scenario.** After 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 *drive:\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 *drive:\ibi\WebFOCUS_BUE82\WebFOCUS\cm\import* directory. For convenience the CM zip file can be downloaded from Business User Edition using a web browser and similarly uploaded to the target Business User Edition where its content can then be imported and accessed.

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

- 1. In the portal, on the Menu bar, click *Resources*.
- 2. In the WebFOCUS Resources panel, expand the *Change Management* node.
- 3. Right-click *Export*, and click *New Scenario*.
- 4. In the New Scenario dialog box, type the scenario name, and then click *OK*.

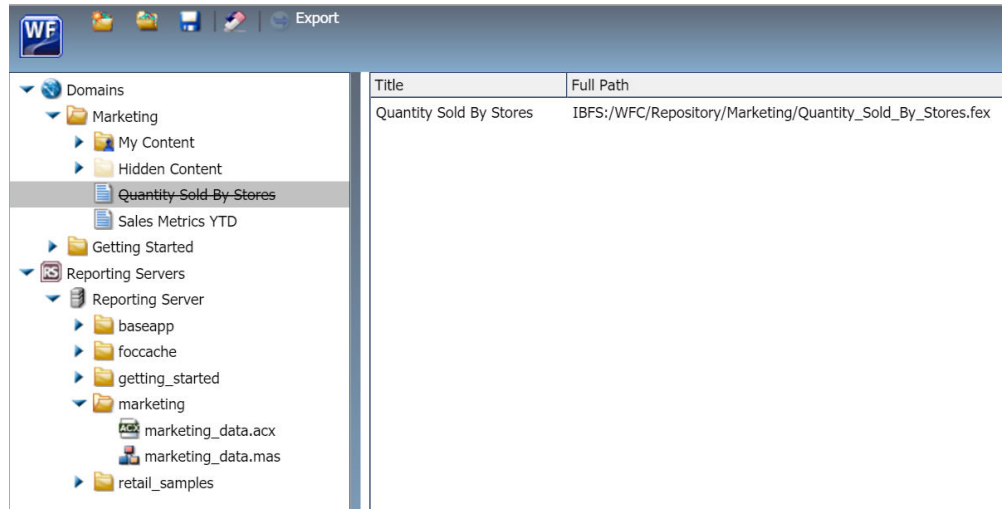
The Change Management Scenario dialog box opens, as shown in the following image.



- 5. Right-click the domain, folder, or other resource you want to include, and:
 - a. Click *Select with Sub-Tree* to include that folder and all subfolders in your selection.
 - b. Click *Select Folder Only* to include the specific folder, with no content. Typically, this is done to move rules on the folder.

- c. You can also select resources by dragging them from the Resources tree and dropping them in the right pane. When you do so, the With Subtree check box is selected, by default, and you must clear it if you wish to exclude subfolders and content from your selection.

When your selection is complete, an entry for it appears in the right pane, and a strikethrough line appears on the entry under the Resources tree, as shown in the following image.



- ☐ If you select a private resource, the With Private Content check box is automatically selected and cannot be cleared.
- ☐ If you select private content, it will only be imported if the owner of that private content already exists in the target environment.
- ☐ If you select a published folder, you can include private content within it 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 those My Content folders that are assigned to individual users, even if you do not have the privileges necessary to view that private content.
- ☐ If you select a subfolder without a parent folder, the Import process will recreate the parent folder in the target environment. A connection to the same metadata must exist within the target environment as well as the source environment.

- ☐ If the rules on the source and target environments are different, users may have access to private content in the source environment, but be denied access in the target environment. This occurs if users have access to the published folder that contains the private content in the source environment, but do not have it in the target environment.
- 6. Repeat the previous step for any additional resources you want to include in the change management scenario.
- 7. If you need to clear your unsaved selections, click *Reset Scenario*.
- 8. When you have selected all resources, click *Save*.
An entry for the new scenario appears beneath the *Export* node.
- 9. If the new scenario does not appear, right-click the *Export* node, and then click *Refresh*.

Procedure: How to Open a New Change Management Scenario from the Change Management Scenario Dialog Box

1. In the Change Management Scenario dialog box, on the toolbar, click *Create a new Scenario*.
2. If you receive a message that asks if you want to save the changes you made, click *Yes*.
3. Type the name of the new scenario, and click *OK*.
A new Change Management Scenario dialog box opens. The current Change Management Scenario dialog box also remains open.
4. Create the new scenario as described in the procedure, [How to Create a Scenario From the Change Management Export Facility](#) on page 172, starting with step 4.

Procedure: How to Open an Existing Change Management Scenario from the Change Management Scenario Dialog Box

1. In the Change Management Scenario dialog box, on the toolbar, click *Open existing Scenario*.
2. If you receive a message that asks if you want to save the changes you made, click *Yes*.
3. In the Open Scenario dialog box, navigate to the existing scenario you want to open and double-click it, or click it and then click *Open*.
Your selected Change Management scenario dialog box opens and replaces the Change Management scenario dialog box that was on display.

Procedure: How to Export a Saved Change Management Scenario Using the Change Management Facility

Before you can export a change management scenario, you must make sure that you have saved it. You cannot export an unsaved change management scenario.

1. In the Scenario dialog box Quick Access Toolbar, click *Export*.
2. When the confirmation message opens, click *OK*.

The new scenario appears in the WebFOCUS Resources panel, under the Change Management, Export node.

3. If the new scenario does not appear, right-click the Export node, and then click *Refresh*.

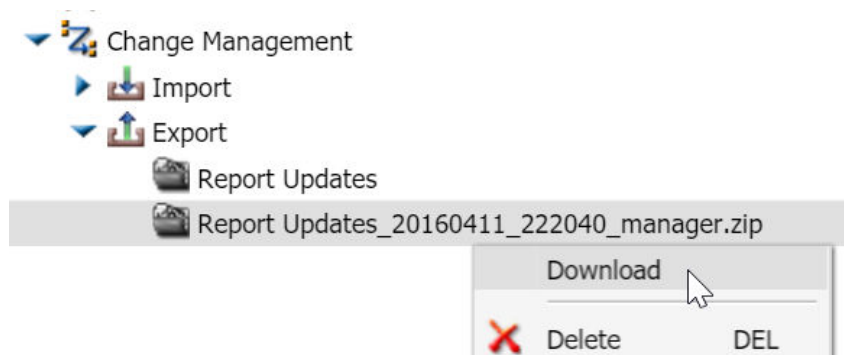
Procedure: How to Download a Change Management Package Zip File

The export process saves a CM zip file to the following location:

`drive:\ibi\WebFOCUS_BUE82\WebFOCUS\cm\export`

The download process takes that CM zip file, and downloads it to your local machine. You can then transfer the copy of that CM zip file to another environment for use as a change management package.

1. In the portal, on the Menu bar, click *Resources*.
2. In the WebFOCUS Resources panel, expand the *Change Management* node.
3. Expand the *Export* node.
4. Right-click the CM zip file you want to download, and then click *Download*, as shown in the following image.



5. Save the CM zip file to an external location as directed by your browser.

Procedure: How to Upload a Change Management Package Zip File

The zip file upload process saves a copy of a CM zip file stored on your local machine to the change management import directory on the server at the following location:

`drive:\ibi\WebFOCUS_BUE82\WebFOCUS\cm\import`

You can then import the copy of that CM zip file to WebFOCUS Business User Edition.

1. In the portal, on the Menu bar, click *Resources*.
2. Expand the Change Management node, right-click Import, and then click *Upload a Zip File*.
3. In the Upload a Zip File dialog box, click *Browse*, navigate to the location where you have saved the change management package, click the CM zip file you want to upload, and then click *Open*.
4. Ensure that the correct CM zip file appears in the File to Upload field, and decide whether or not to import files from the package as published or unpublished files.
 - ☐ To establish the contents taken from the CM zip file as published after the upload is complete, select the *Publish Documents* check box. This is the default setting.
 - ☐ To establish the contents taken from the CM zip file as private after the upload is complete, clear the *Publish Documents* check box.
5. Click *Upload*.

When you receive a confirmation message, click *OK* to complete the upload.

6. In the Upload a Zip File dialog box, click *Close*.

If an entry for the new CM zip file does not appear below the Import node, right-click it, and then click *Refresh*.

Procedure: How to Import a Change Management Package

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

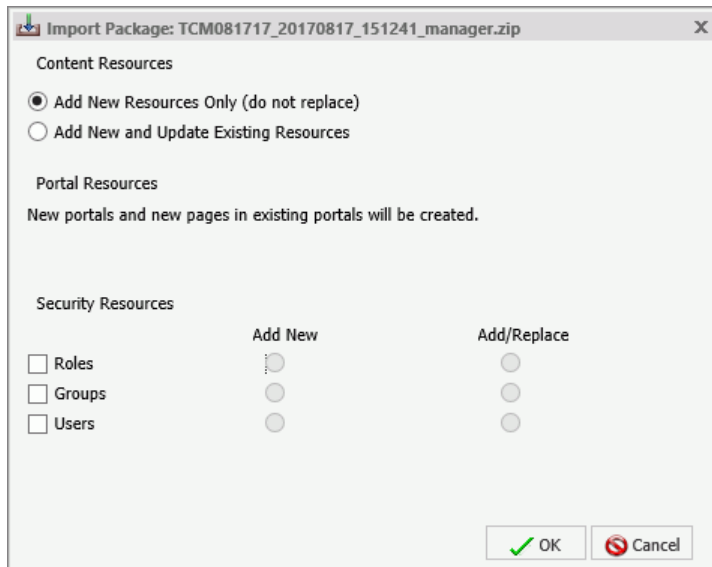
This procedure assumes that a change management zip package has been previously created on another system, the Manager is signed in to the target environment, and the CM zip file is available to the Manager.

1. In the WebFOCUS Resources panel, expand the *Change Management* node, and then expand the *Import* node.

If the CM zip file is not visible, right-click the node, and then click *Refresh*.

2. Right-click the uploaded change management package, 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 only adds new resources to the target environment. For newly created items, the Created On and Last Modified On fields are 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 are left alone and the Last Modified On field will not be updated.

Add New and Update Existing Resources. This option adds new resources to the target environment, and updates existing resources . For newly created items, this option assigns the time of the import to the Created On and Last Modified On fields. For updated items, this option retains the original value in the Created On field, but updates the value in the Last Modified On field with the time of the most recent import.

The other options on this panel are not used in WebFOCUS Business User Edition and can be ignored.

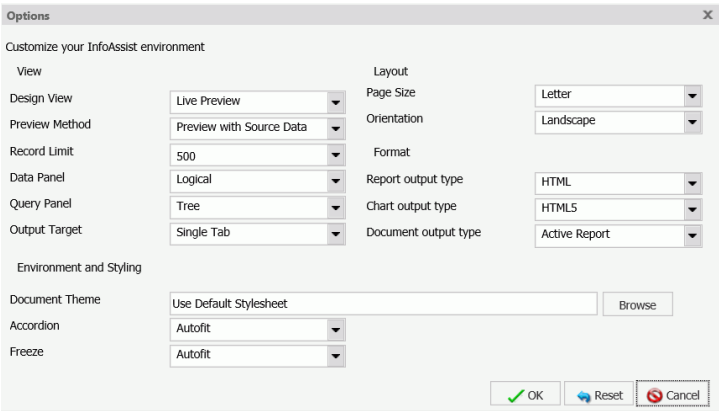
4. Click *OK*.

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 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), Excel (csv), 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.

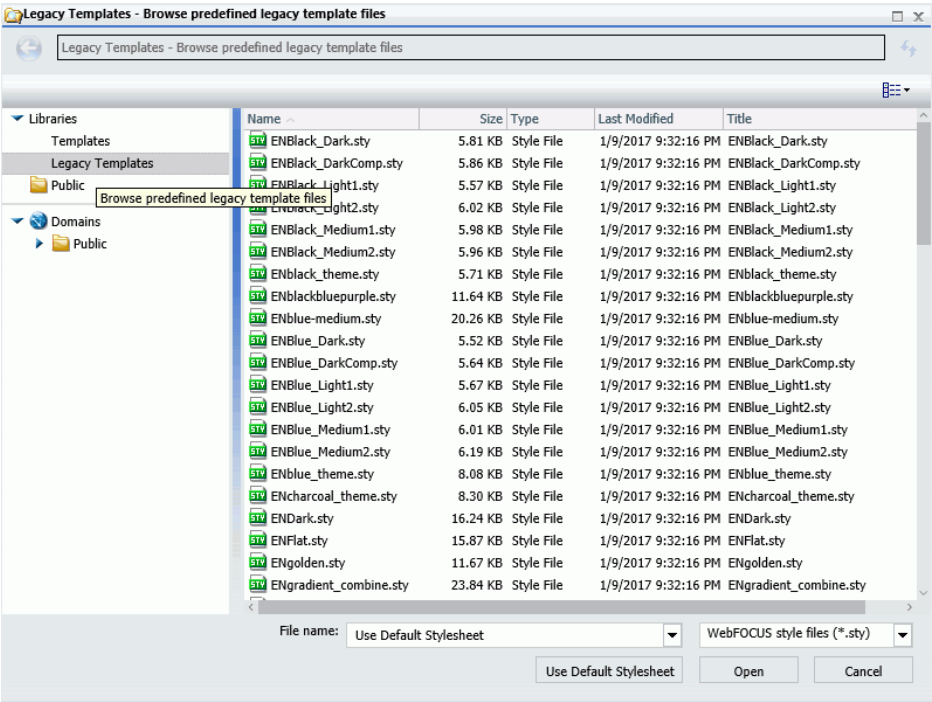
Environment and Styling

The Environment and Styling area provides settings for styling reports and charts through the specification of a Document Theme. Click the *Browse* button to open the Templates - Browse predefined template files dialog box, in which you can search for an existing WebFOCUS StyleSheet. The default StyleSheet is Warm.sty, but you can select from the other themes that are available (Dark.sty or Flat.sty).

Note: StyleSheets are stored in the following directory of your Business User Edition installation:

`drive:\ibi\WebFOCUSBUE82\IBI_HTML\ibi_themes`

In addition, you can access a repository of additional themes by accessing the Legacy Templates, under Libraries, as shown in the following image.



The theme that you select determines the coloring and hues that display within InfoAssist. The default templates in the Templates section apply to all languages, whereas some of those in the Legacy Templates sections are specific to just one language (for example, EN=English).

- ☐ **Accordion.** Values for this option are: Autofit and Legacy. The enhanced Accordion report format is built to autofit and be adaptive within windows and portal page containers. The legacy Accordion report opens in a tree structure independent of the window or container. The default value is Autofit.
- ☐ **Freeze.** The Freeze option allows you to define a scroll area within the data of your report. It locks the headings and footings in place, enabling you to scroll through the data within the container. Values for this option are: Autofit and Fixed. Autofit sizes the scroll bar to fit the container. Fixed sets the scroll height to the default 4" size. The default value is Autofit.

Changing Global Preferences

You can change global preferences for InfoAssist through the Administration Console found on the portal. To do so, in the Administration Console, on the Configuration tab, click *InfoAssist Properties*.

Configuring Hyperstage

Hyperstage is a column-oriented, high performance analytic engine designed for analytic applications and data marts that need fast query response across large data volumes. Hyperstage was designed specifically for large volume data analytics applications with up to 50 Terabytes of data.

Hyperstage Overview

Hyperstage uses a unique and patent-pending approach to compressing, storing, and processing data that allows it to be installed and run on commodity hardware with little or no DBA intervention. Hyperstage requires little tuning to support ad hoc or complex business analytic queries.

Hyperstage is a database engine utilizing the PostgreSQL database environment. As such, Hyperstage is fully compatible with all PostgreSQL-compliant Business Intelligence tools and utilizes the PostgreSQL administrative interface to reduce the learning curve for system administrators.

Hyperstage provides a versatile, highly-compressed database system optimized for analytic-type queries. The ratio of possible compression and the speed of data import and retrieval are optimized at the expense of some transactional features of the engine performance, like the frequent data updating.

Hyperstage executes complex or ad hoc queries across vast amounts of data with a low cost of ownership.

Hyperstage and PostgreSQL

Hyperstage combines the Hyperstage storage engine with PostgreSQL server implementation. Hyperstage consists of several layers. The upper layers are provided by the PostgreSQL server implementation, and the lower layers are provided by Hyperstage.

Hyperstage includes both its own optimizer and executor along with the storage engine. The PostgreSQL query engine can be used with Hyperstage. However, since the PostgreSQL storage engine interface is row oriented, it cannot take full advantage of the column orientation or the Knowledge Grid and hence query execution through this path is reduced. Queries will be directed to the Hyperstage optimizer whenever possible.

Hyperstage ships with the full PostgreSQL binaries required. PostgreSQL is used to store catalog information (as with other storage engines). You can use the PostgreSQL instance for other purposes, but joining PostgreSQL and Hyperstage tables may result in reduced performance as the PostgreSQL query engine will be used.

PostgreSQL provides:

- ❑ Mature connectors, tools and resources.
- ❑ Interconnectivity and certification with BI tools.
- ❑ Management services and utilities.

Hyperstage provides:

- ❑ Load function that compresses data.
- ❑ Column-oriented storage engine.
- ❑ Knowledge Grid metadata layer that contains information about the compressed data.
- ❑ Optimizer/executor that uses the Knowledge Grid.

Configuring the Hyperstage Database

The following section describes the configuration steps for Hyperstage.

Configuring Hyperstage

The Hyperstage configuration file is called `infobright.cnf` and is located in the `ib_data` subdirectory within the Hyperstage Data installation directory (for example, `C:\ibi\WebFOCUS_BUE82\srw\wfs\hs\ib_data`). The configuration file is a text file containing the Hyperstage configuration parameters.

Each parameter is shown on a separate line.

If a parameter is not present in the configuration file or if the configuration file does not exist, the default values are used. Blank lines and comments (lines starting with `#`) are ignored.

Be sure to customize the following parameters to optimize performance. These tuning parameters are case sensitive and must be typed as shown in the following table.

Note: The values are commented out (preceded by `#`) in the `infobright.cnf` file, which causes them to default to the application minimum allowed values of 600 and 320 for `ServerMainHeapSize` and `LoaderMainHeapSize`, respectively.

Hyperstage Configuration Parameters

Parameter Name	Description
LicenseFile	Specifies the path or name of the newly required License file.
LogLevel	Controls how much information is written to logs. This is similar to the obsolete ControlMessages parameter.
LogRotateSize	Specifies how large the log file can be before it is rotated and archived.
LogRotateFiles	Specifies how many log archive files are kept.
KNFolder	Specifies the folder where Knowledge Grid is stored.
CacheFolder	Specifies the folder where temporary objects are stored.
ServerMainHeapSize	Specifies the size (in MB) of the main memory heap.
ThrottleLimit	Controls how many SELECT queries can run concurrently.

Configuration Tips and Examples

Important: You must properly configure your memory settings to ensure optimal performance. The following table shows sample, recommended memory configurations for different systems.

System Memory	Server Main Heap Size	Loader Main Heap Size
64GB	48000	800
48GB	32000	800
32GB	24000	800
16GB	10000	800
8GB	4000	800

System Memory	Server Main Heap Size	Loader Main Heap Size
4GB	1300	400
2GB	600	320

In most cases, the loader does not benefit from larger memory settings. However, increasing the LoaderMainHeapSize can help when:

- ❑ A table to be loaded has very long text values.
- or
- ❑ The table has many columns (for example, 1000 columns).

You can use more memory at import if you are planning to execute several concurrent load tasks to different data tables. However, disk access may become a bottleneck.

ServerMainHeapSize should be as large as possible, but safely smaller than the amount of physical memory on the machine. If performance decreases because of memory swapping by the operating system, try to set lower heap sizes. We also recommend decreasing the heap size if many users are running queries in parallel.

Note: Hyperstage may use additional memory for heavy loads or queries. Also, other applications on your server will use memory for their processes. It is important that the total of ServerMainHeapSize is less than the total available physical memory. If the system needs to swap memory, performance will be severely impacted.

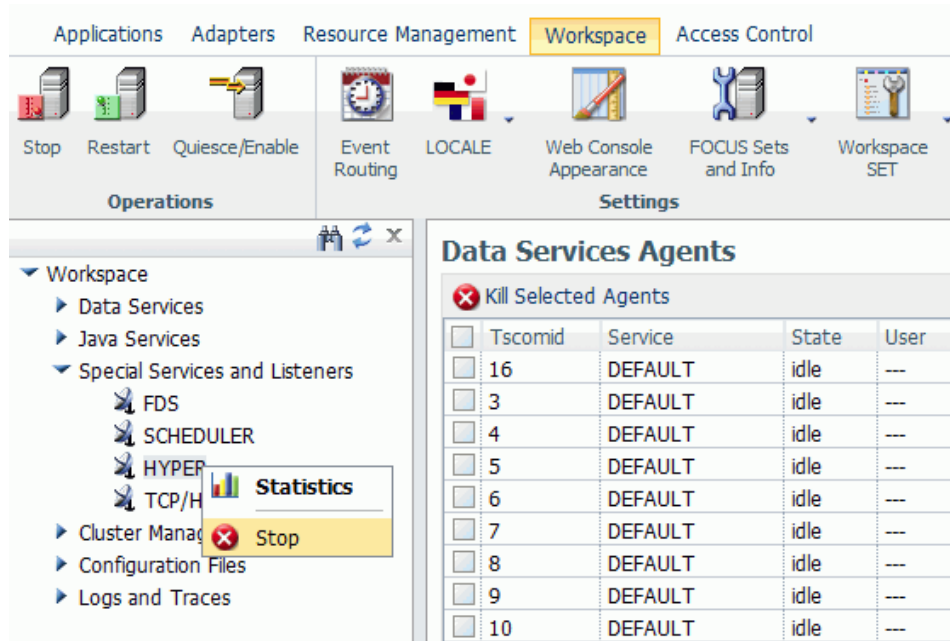
Using the Hyperstage Database Beyond WebFOCUS

The following section describes how to work with the Hyperstage server.

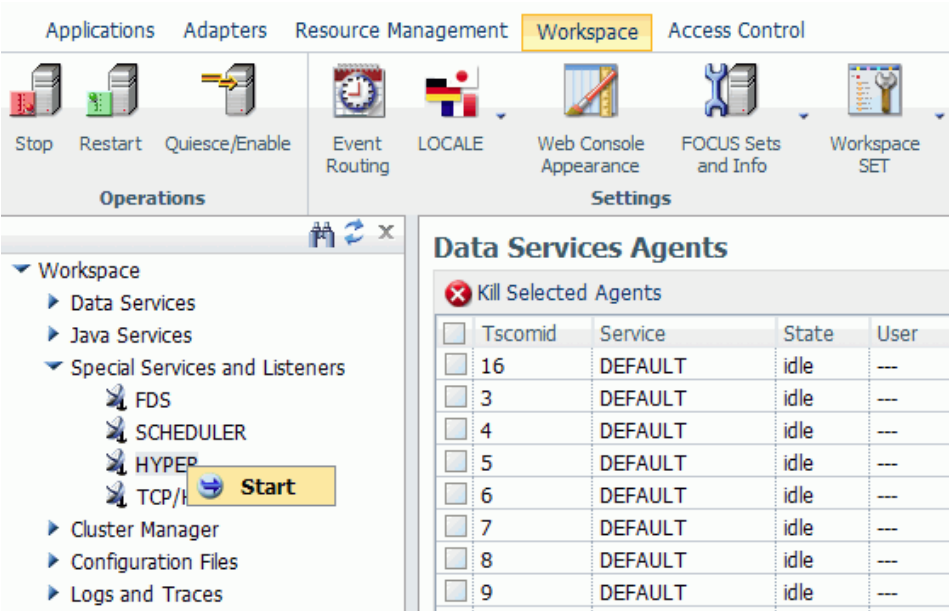
Starting and Stopping the Hyperstage Server

The Hyperstage Server starts and stops automatically when starting and stopping the Reporting Server. The Manager user ID is required to start and stop any component of the Business User Edition.

To manually stop the Hyperstage Server, from the Workspace tab, expand the *Select Special Services and Listeners* section of the Reporting Server Web Console, right-click the *HYPER* service and click *Stop*, as shown in the following image.



To manually start the Hyperstage server, from the Workspace tab, expand the *Select Special Services and Listeners* section of the Reporting Server Web Console, right-click the *HYPER* service and select *Start*, as shown in the following image.



Quick Copy For Hyperstage Using Extended Bulk Load Utility

Note: Hyperstage only supports Quick Copy, and Custom Copy as ETL tools.

The Quick Copy tool allows for the copying of all data from a Source table into Hyperstage. The *Bulk Load* option should be selected in order for data to be loaded quickly. If the *Bulk Load* option is cleared, the data will take much longer to load.

The Custom Copy tool allows for the copying of selected columns, presorting data within selected columns, and filtering of columns from a Source table into Hyperstage.

To access the Quick Copy tool, right-click the name of the synonym corresponding to the table or data you wish to copy into Hyperstage, and select *Quick Copy*.

The following configuration setting options are available:

Load Option

New/Replace. Recreate the target table before loading the data.

Append to Existing. Data is loaded to an existing table.

Adapter

The list of adapters currently configured on the Reporting Server.

Connection

The Hyperstage connection used for the load operation.

Synonym Application

The target application on the Reporting Server where the target synonym will be stored.

Synonym

The name of the target synonym defining the Target Table Name.

Table Name

The name of the Hyperstage table where the data will be loaded.

Bulk Load

When selected, data will be loaded using the Hyperstage Bulk Load functionality. Bulk Load is the recommended approach for loading data into Hyperstage.

When cleared, data will be loaded using Insert/Update. Insert/Update is not recommended and will perform extremely slow.

Managing Hyperstage Tables

The following section describes how to work with the Hyperstage tables and lists the data types supported.




About the Hyperstage Database Files

Hyperstage tables are located in the `ib_data` subdirectory in your Hyperstage installation directory. Within the `ib_data` subdirectory, Hyperstage databases are stored in separate subdirectories.

Important: Do not manually copy a data table from one database to another by copying the database files. Internal table numbering errors and Knowledge Grid inconsistencies may occur. To copy a table, backup the entire database directory (see [Hyperstage Backup and Recovery](#) on page 192).

The following path and image shows the content of the `ib_data` directory, containing the Hyperstage databases `webfocus` and `utf8test`, as well as the `BH_RSI_Repository` directory, which holds the Knowledge Notes:

C:\ibi\WebFOCUS_BUE82\src\wfs\hs\ib_data

Name	Date modified	Type
 BH_RSI_Repository	9/2/2016 1:14 PM	File folder
 cache	9/2/2016 12:00 PM	File folder
 webfocus	9/2/2016 1:10 PM	File folder

About Supported Data Types

The following data types are supported in Hyperstage. Note that numeric data types ranges are 1 less than the PostgreSQL minimums and maximums.

Numeric Types		
BOOLEAN	Values are either 0 or 1.	
SMALLINT	-32767	32767
INT (INTEGER)	-2147483647	2147483647
BIGINT	-9223372036854775807	-9223372036854775807
REAL	-3.402823466E+38	3.402823466E+38
DOUBLE PRECISION	-1.7976931348623157E+308	1.7976931348623157E+308
Numeric(M, D) where: 0 < M <= 18 and 0 <= D <= M	-(1E+M - 1) / (1E+D)	(1E+M - 1) / (1E+D)

Date and Time Types			
DATE	100-01-01	9999-12-31	YYYY-mm-dd
Time (without timezone)	00:00:00	24:00:00	HH:MM:SS

Date and Time Types			
TIMESTAMP (without timezone)	100-01-01 00:00:00	9999-12-31 23:59:59	YYYY-mm-dd HH:MM:SS
TIME0053TAM P (with timezone)	1970-01-01 00:00:00 in UTC	2038-01-01 00:59:59 in UTC	
Interval	-178000000 years	178000000 years	

String Type	
BYTEA (binary string)	$0 < N \leq 65536$
CHAR(N)	Fixed-length. Maximum length depends on character set (encoding). $0 < N * B \leq 65536$ where B is the maximum number of bytes for a single character.
VARCHAR(N)	Maximum length depends on character set (encoding). $0 < N * B \leq 65536$, where B is the maximum number of bytes for a single character. For example, for UTF-8 it is 4 bytes, so the maximum number of characters that can be stored in a (VAR)CHAR column is $65536 / 4 = 16384$

Creating and Dropping Tables

Use the standard PostgreSQL commands to create and drop tables in Hyperstage, the same as you would with a PostgreSQL table. For detailed syntax information, see the *PostgreSQL 9.2 Documentation*.

Important: Do not manually copy a data table from one database to another by copying the database files. Internal table numbering errors and Knowledge Grid inconsistencies may occur. To copy a table from one database to another, back up the entire database directory (see [Hyperstage Backup and Recovery](#) on page 192). You can rename the entire database by renaming the folder. However, you should not copy a database folder from one active instance to another, or within the same active instance.

To create a table, enter the following command:

```
psql> create table <table_name> (<column(s)>) with (ENGINE=INFOBRIGHT);
```

Note:

- ❑ 'with (ENGINE=INFOBRIGHT)' syntax is necessary when creating tables manually, to specify that the table will be stored as part of the Hyperstage-specific Infobright engine. Without this syntax, the table will be created and stored as a regular PostgreSQL table.
- ❑ When creating a table, as a matter of practice, you should always use the ENGINE= option to ensure that the correct database engine is used. Hyperstage is shipped with DEFAULT ENGINE=INFOBRIGHT, but this can be changed. The name of the engine can be specified explicitly at the end of the create table statement.

To drop a table, enter the following command:

```
psql> drop table table_name;
```

Character Set Support

The following section describes the character sets supported by Hyperstage.

Supported Character Sets

Hyperstage storage supports all ANSI and UTF-8 character sets. This means that Hyperstage can store and retrieve data encoded in 8-bit and multi-byte character sets.

Important: Queries that evaluate against UTF-8 character data columns will execute with less performance than an equivalent query against ASCII character data, due to ASCII support of Character Maps in the Knowledge Grid. UTF-8 specific Knowledge Grid extensions will be available in an upcoming release.

Collations and Comparisons

Hyperstage supports all custom UTF-8 collations supported by PostgreSQL:

<input type="checkbox"/> utf8_bin	<input type="checkbox"/> utf8_polish_ci
<input type="checkbox"/> utf8_czech_ci	<input type="checkbox"/> utf8_roman_ci
<input type="checkbox"/> utf8_danish_ci	<input type="checkbox"/> utf8_romanian_ci
<input type="checkbox"/> utf8_esperanto_ci	<input type="checkbox"/> utf8_slovak_ci
<input type="checkbox"/> utf8_estonian_ci	<input type="checkbox"/> utf8_slovenian_ci
<input type="checkbox"/> utf8_general_ci (default)	<input type="checkbox"/> utf8_spanish2_ci
<input type="checkbox"/> utf8_hungarian_ci	<input type="checkbox"/> utf8_spanish_ci
<input type="checkbox"/> utf8_icelandic_ci	<input type="checkbox"/> utf8_swedish_ci
<input type="checkbox"/> utf8_latvian_ci	<input type="checkbox"/> utf8_turkish_ci
<input type="checkbox"/> utf8_lithuanian_ci	<input type="checkbox"/> utf8_unicode_ci*
<input type="checkbox"/> utf8_persian_ci	

*utf8_unicode_ci properly handles both French and German collation, so specific collation types for these languages are not necessary.

For more information, see the *PostgreSQL 9.2 Documentation*.

The SQL standard does not define a default collation. Therefore, many DBMS engines have different default collations and produce different results. As a result, there are several differences between Hyperstage and other DBMS engines.

- ☐ For Hyperstage, character data types are case-sensitive. For example, the condition 'toronto'='Toronto' is not true in Hyperstage. Similarly, the condition, LIKE 'Abc%' is not true for 'abcde'.
- ☐ The Hyperstage sorting order is A...Z a...z (for example 'Zeta' < 'alfa'), which is the same sorting order as used by Oracle. The Hyperstage sorting order is different than the default PostgreSQL sorting order, which mixes lowercase and uppercase. The SQL Server order, which is aAbB...zZ; and the DB2 order, which is AaBb...Zz.

- ❑ The Hyperstage sorting order affects ORDER BY results, GROUP BY results (which is the order of groups and their definitions (for example, 'aaa' and 'AAA' define different groups) and DISTINCT results. WHERE conditions may also be affected if you are expecting a different sorting order than the one used by Hyperstage.
- ❑ To simulate Hyperstage collation in the PostgreSQL engine, set latin1_bin collation while creating a table (for more information, see the *PostgreSQL 9.2 Documentation*). Enter the following command:

```
psql> create table ... collate ascii_bin;
```

Padding

Hyperstage treats padding differently than other DBMS engines. Hyperstage assumes literal comparisons of text fields, including all whitespace characters. Therefore, a string containing two spaces is different than a string containing one space or an empty (0 length) string, which is also different than the NULL value.

The Hyperstage padding definition is compatible with the SQL standard. However, most DBMS systems have defined less restricted, customizable rules regarding text comparison. For example, 'abc ' = 'abc' may be true in some databases, but is not true in Hyperstage.

Note: In CHAR columns, trailing spaces are trimmed on LOAD, INSERT, and UPDATE, whereas in VARCHAR columns values are loaded with all spaces.

Hyperstage Backup and Recovery

The following section provides instructions on how to backup and restore the Hyperstage databases.

Backup Procedure

Use the following procedures to back up Hyperstage.

- ❑ To back up the Hyperstage databases, copy the ib_data and pg_data directories.
- ❑ You can take advantage of incremental backups, since only some of the database files are updated when new data is imported. Be sure to do a full backup occasionally.

Important: Some files in the KNFolder are updated when queries (using JOIN) are run, so be sure to back up the KNFolder on a regular basis.

Restore Procedure

To restore the Hyperstage databases from a backup copy, do the following:

1. Replace the `ib_data` and `pg_data` directories with the backup copy.
2. Replace the `KNFolder` with the backup copy (if the `KNFolder` is not inside the data directory).

Important: Do not manually modify database files or move them from one database to another. This may lead to data corruption and unpredictable results.

Functions and Operators

The following section lists the functions and operators supported by Hyperstage.

Hyperstage Optimizer Supported Functions and Operators

Comparison Functions and Operators

COALESCE	YES
----------	-----

Control Flow Functions

CASE	YES
COALESCE	TBD
NULLIF	YES

String Functions

BIT_LENGTH	YES
CONCAT	YES
LEFT	YES
LENGTH	YES
LOCATE	YES

LOWER	YES
LPAD	YES
LTRIM	YES
OCTET_LENGTH	YES
POSITION	YES
RIGHT	YES
RPAD	YES
RTRIM	YES
SUBSTR	YES
TRIM	YES
TRUNC	TBD
UPPER	YES

Numeric Functions

Modulo (%)	YES
--------------	-----

ABS	YES
ACOS	YES
ASIN	YES
ATAN2, ATAN	YES
ATAN	YES
CEIL	YES
COS	YES

COT	YES
DEGREES	YES
EXP	YES
FLOOR	YES
LN	YES
LOG	YES
MOD	YES
PI	YES
POWER	YES
RADIANS	YES
RANDOM	TBD
SIGN	YES
SIN	YES
SQRT	YES
TAN	YES

Date and Time Functions

CURRENT_DATE	YES
CURRENT_TIME	YES
DATE	YES
DAY	YES
DAYOFYEAR	YES
FROM_UNIXTIME	YES

HOUR	YES
MINUTE	YES
MONTH	YES
NOW	YES
QUARTER	YES
SECOND	YES
TIME	YES
YEAR	No

Text Search and Other Functions

CAST	YES
MD5	TBD

Group By Aggregate Functions

AVG	YES
BIT_OR	No
BIT_AND	No
COUNT(DISTINCT)	TBD
COUNT	YES
MIN	YES
MAX	YES
STD, STDDEV	YES
STDDEV_POP	YES

STDDEV_SAMP	YES
SUM	YES
VAR_POP	YES
VAR_SAMP	YES
VARIANCE	YES

Hyperstage Data Tools

The following section describes the data tools used by Hyperstage.

Hyperstage Consistency Manager

Hyperstage provides a tool to validate Hyperstage-specific metadata structures. The Hyperstage Consistency Manager is an external stand-alone application that can be run against a Hyperstage instance to verify and repair most Hyperstage data structures, including the Knowledge Grid and Data Packs.

If you are seeing unexpected behavior with Hyperstage, such as server crashes, it can help to run the Hyperstage Consistency Manager for information for support and to perform repairs.

Note: Currently, the Hyperstage database must be offline in order to run the Hyperstage Consistency Manager.

Hyperstage Consistency Manager Tests

The Hyperstage Consistency Manager runs tests, as described in the following table.

Test	Description
Delete mask consistency check	Checks that the delete mask headers contain the proper sum for the delete mask body. If any inconsistency is found between the header and body, the Hyperstage Consistency Manager returns the list of blocks of delete mask where inconsistencies were found.
Number of objects in columns equality	Compares the stored number of objects in each column file related to the table. If any inconsistency is found in the number of objects, the Hyperstage Consistency Manager returns the first two columns with different object numbers.

Test	Description
Comparison of maximal value in DIMENSION dictionary versus DPN	Executes only for DIMENSION columns. Compares the maximal key value stored in the DIMENSION column dictionary and in DPNs. If the values differ, the Hyperstage Consistency Manager writes them to the log.
Comparison of number of objects in first-column DPN versus delete mask	Compares the metadata stored in the headers of the delete mask and DPN file related to the number of objects. If any inconsistencies are found, the Hyperstage Consistency Manager returns both numbers. The Hyperstage Consistency Manager compares only the first column because there is an independent test comparing this value between columns. If the test does not find the proper delete mask file or the proper DPN file, the Hyperstage Consistency Manager reports corruption.
Knowledge Grid consistency for column	Checks if the histograms report the proper value of the fixed parameter. A basic test of the Knowledge Node, ensuring the file has a proper format and the type of Knowledge Node corresponds to the column.
Knowledge Grid format for column	Each Knowledge Node is stored in a separate file. This test validates that the header data of each file is in the proper format.
Test for overlapping Data Packs in data files	Checks if there are Data Packs in files that overlap each other. If this situation occurs, the Hyperstage Consistency Manager returns a list of pairs of Data Packs numbers that are overlapping.
Tests of table metadata consistency	Verifies if the table metadata is valid. Includes verification of files used to store items, such as table name, number of columns and their names, types, and constraints like NOT NULL. These are the files created on CREATE TABLE and modified only on ALTER TABLE.
Test of DPNs for non-binary collation	Verifies Data Packs specifically for non-binary collation types (for example: Latin1_swedish.ci). If errors exist, they can be repaired using the Hyperstage Consistency Manager - -repair option.

Syntax: **How to Run the Hyperstage Consistency Manager**

To view the run options, run Hyperstage Consistency Manager with the - -help flag:

```
Icm-pure --help
```

To run Hyperstage Consistency Manager, use the following command:

```
Icm-pure --datadir=/data_directory_path [parameters]
```

For example:

```
c:\ibi\srv77\home06Hyperstage\hs\bin>icm-pure.exe
--datadir=C:\HyperstagePG\ib_data --log-file=C:\temp\icm-pure.log
```

Note: Hyperstage Consistency Manager should be run by the 'postgres' user. It should not be executed by 'root' or any rebuilt knowledge nodes will be owned by root (and cannot be edited), which will result in issues when loading any subsequent data into the 'corrected' tables.

The following table describes the Hyperstage Consistency Manager parameters.

Parameter	Description
- -help	Displays help message and exit.
-V [- - version]	Displays version information and exit.
- -basedir arg	Absolute path to Hyperstage installation directory.
- -datadir arg	Absolute path to directory. Mandatory.
- -database arg	Name of database chosen for data integrity testing. Optional. If specified, no other databases will be tested.
- -table arg	Name of table chosen for data integrity testing. Optional. If specified, no other tables will be tested.
- -log-file arg	Prints output to log file. Optional. If not specified, the logs will be printed to the console.

Parameter	Description
-F [- -full-check]	Runs full set of tests (may be time-intensive). Running Hyperstage Consistency Manager without the full-check option will result in a quicker test. However, the "Knowledge Grid consistency for column" test will not be run.
- -repair	Repairs found problems.
- -rebuild-kns	Rebuilds the Knowledge Grid. For more information, see About Rebuilding or Repairing Knowledge Nodes on page 200.
- -stop-on-error	Stops tests on first error and report.
- -cleanup	In case of an error in the Hyperstage Consistency Manager repair procedure, this option enables Hyperstage Consistency Manager to manually revert the datadir to its previous state. Running Hyperstage Consistency Manager with the - -cleanup option removes the old DPN files (containing incorrect DPNs) from the datadir and also makes the changes performed by Hyperstage Consistency Manager impossible to undo. If the - -cleanup option is not used, the old DPN files remain in the datadir.

About Rebuilding or Repairing Knowledge Nodes

Executing a rebuild of the Knowledge Nodes (using the - -rebuild-kns option) will run the following tests:

- ☐ Test of table metadata consistency
- ☐ Test of Knowledge Grid format for column
- ☐ Test of Knowledge Grid consistency for column

The - -rebuild-kns option will fix any issues found for the first two tests ("Test of table metadata consistency" and "Test of Knowledge Grid format for column").

You can also use the - -repair option along with the - -full-check option to achieve the same results as - -rebuild-kns. Using either of these methods will rebuild any Knowledge Nodes that have been deleted.

About Cleanup Procedures

The Hyperstage Consistency Manager creates backup files when repairing problems related to "Test of DPNs for non-binary collation" (backup files are not created for any other tests). These backup files can be used to revert back to the original data if the Hyperstage Consistency Manager encounters an error during the repair procedure. To revert to the original data, copy or rename the TAXXXXXDPN.icm_bck files to the TAXXXXXDPN.ctb files (found in the ib_data directory).

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 an option for Business User Edition, 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 wfquickdata.cfg configuration file, 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.

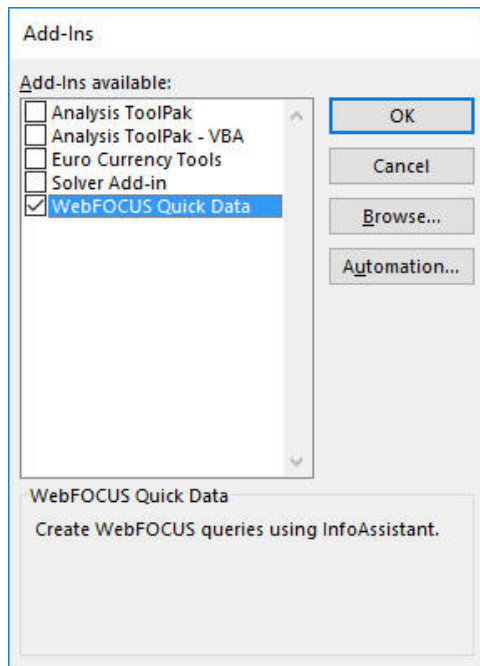
Note: If you already have Quick Data installed in your environment, be sure to backup your existing wfquickdata.cfg file to preserve all your customizations. You can then copy your edits from the existing wfquickdata.cfg file to the new file.

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.

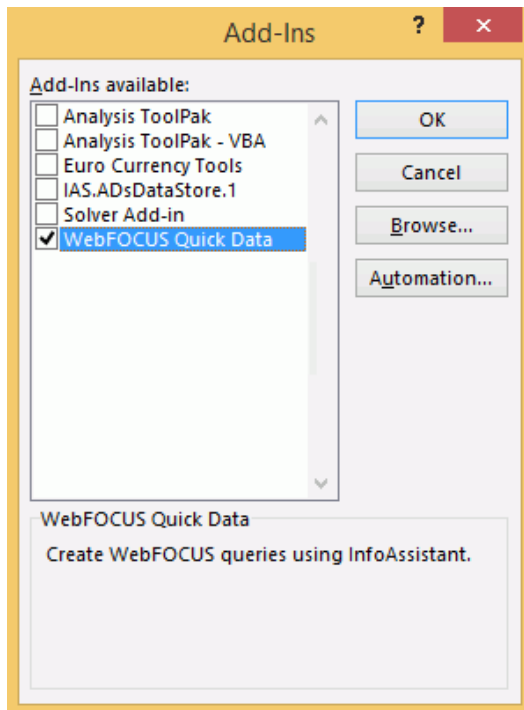
4. Select the WebFOCUS Quick Data check box and click *OK*.

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.

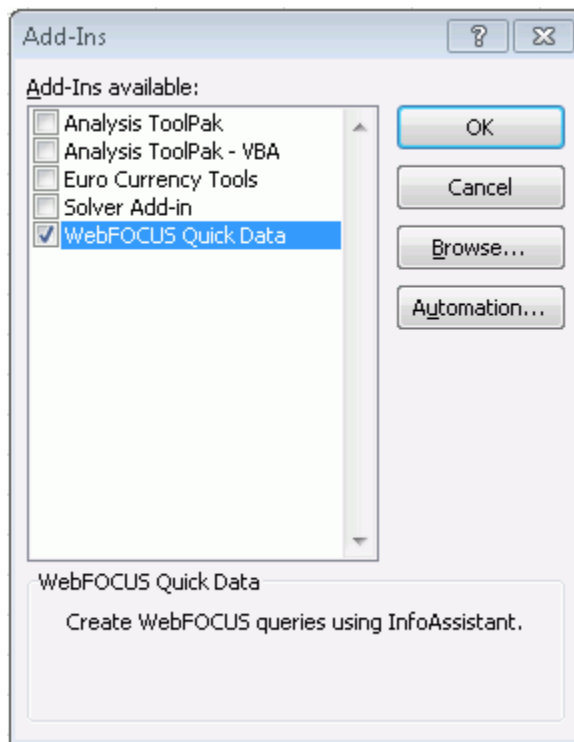
4. Select the WebFOCUS Quick Data check box and click *OK*.

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.

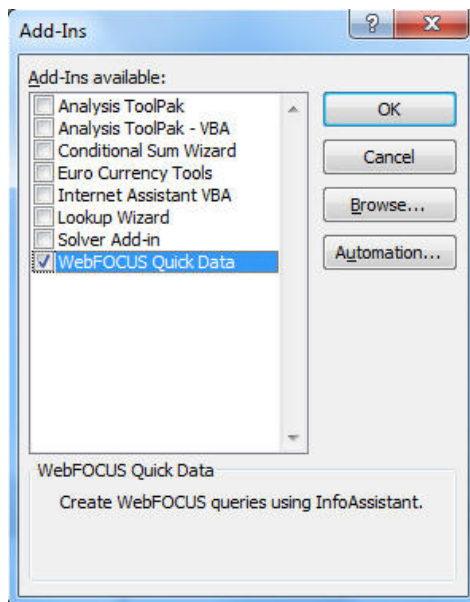
4. Select the WebFOCUS Quick Data check box and click *OK*.

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:

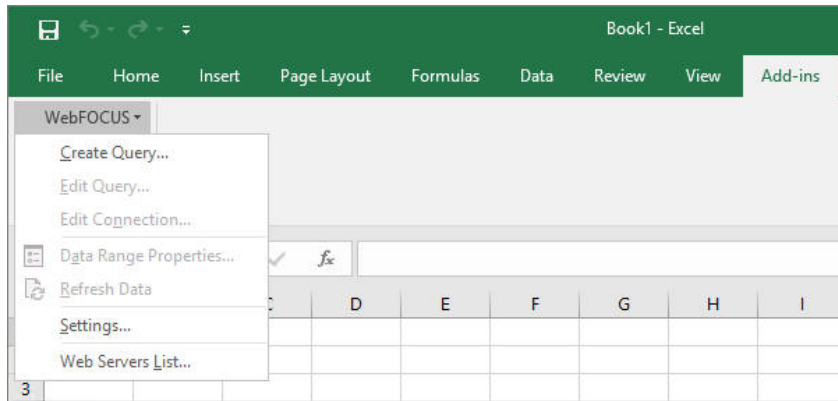
1. Launch Microsoft Excel 2007.
2. Click the Microsoft Office Button  in the top-left corner.
3. Click *Excel Options* and then click *Add-Ins* in the Excel Options dialog box.
4. From the Manage drop-down list, select *Add-ins*, and click *Go*.

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.



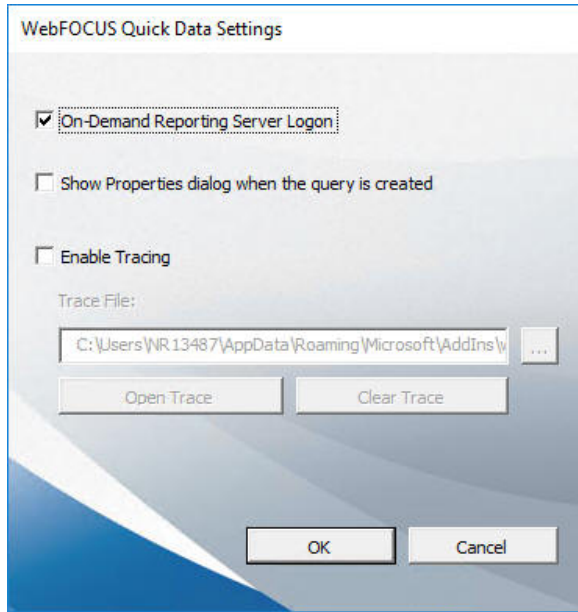
WebFOCUS Quick Data Options

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 Business User Edition. It continues by opening the Data Source Selection dialog box, so that you can select a Master File, and then create a query.
- ☐ **Edit Query.** Available for existing queries only, 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.

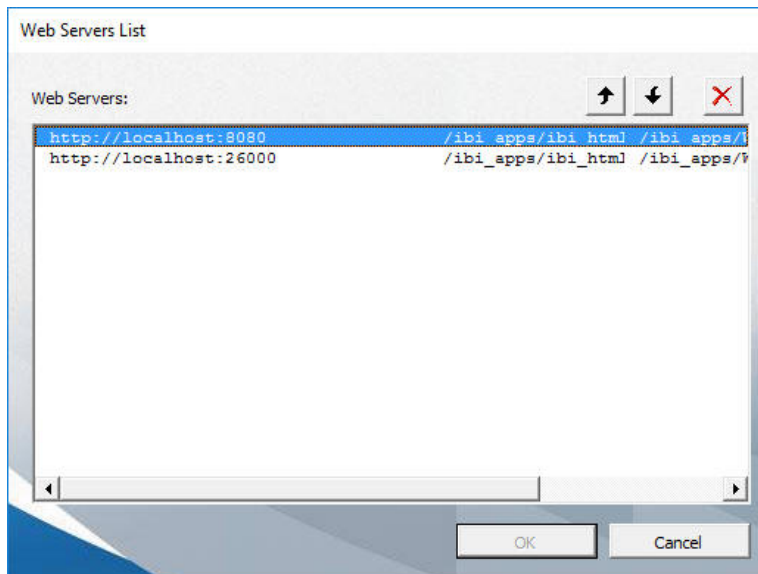
When you select Enable Tracing, the Trace File field is automatically populated with the full path to the trace file. The path includes the trace file name. You can change the location and name of the trace file by either typing the changes in this field, or by clicking the ellipsis and browsing to a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

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

Providing users with a default 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 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 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 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 Business User Edition:
 - ❑ **PROTOCOL.** The protocol used in the environment running Business User Edition. If Business User Edition 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 web application is installed.
 - ❑ **PORT.** The port number of the application server on which Business User Edition is installed.
 - ❑ **HTML_ALIAS.** The alias of the web server or application server on which the static pages are located. The default value is `/ibi_apps/ibi_html`.
- Note:** The leading slash is required.
- ❑ **CLIENT_PATH.** The path to the Servlet, as defined in the web application file, `web.xml`. The default value is

`/ibi_apps/WFServlet.ibfs`

where:

`/ibi_apps`

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

`WFServlet.ibfs`

Is the name of the Servlet.

Managing the Server or Global Profile

A server or global profile, `edasprof.prf`, is created during installation of WebFOCUS Business User Edition. You can customize this profile, which is applied to all users.

The server profile can include almost any command that a client application can send to the server. However, the server profile is used most frequently for application setup commands, such as SET commands.

The server profile remains in effect throughout a user session. You can modify the server profile default settings. You can also add any commands or code that all connected users require before application processing begins.

Procedure: How to Manage the Server or Global Profile

1. Sign in as a Manager.
2. In the portal, on the Menu bar, click *Administration*, and then click *Reporting Server Console*.
3. Click the *Workspace* tab.
4. On the Workspace tree panel, expand *Configuration Files*.

5. Right-click *Server Profile* and click *Edit*.

The server profile, `edasprof.prf`, opens.

6. Type the desired command, such as an application setup command, at the end of the file.

An example of an application setup command is `SET ACRSVRBTITL = ON`. For an Active Technologies report, this command displays the title specified in the Master File, instead of the name, to identify a column in an ACROSS group.

7. Click *Save*.

All commands typed in the profile in step 6 are in effect for any user who submits a request for a report.

Index

A

adding a Reporting Server [109](#)

Address Book access types

 configuring [74](#)

Administration Console

 accessing [9](#)

authentication

 by Active Directory [162](#)

 by LDAP [162](#)

 external [162](#)

B

Blackout Dates [110](#)

 defining [114](#)

 extracting [134](#)

 importing [128](#)

C

Cache Cleaner [59](#)

cache clearing [16](#)

Change Management [171](#)

Change Management settings [37](#)

 IBI_CM_Export_WFRS_File_Extensions [37](#)

 IBI_CM_Retain_Handles [37](#)

 IBI_CM_Zip [37](#)

 IBI_CM_Zip_File_Format [38](#)

 IBI_CM_Zip_File_Verify_Signature [38](#)

Clear Cache [16](#)

Client

 license management [12](#)

configuration [65](#)

 change default user IDs [69](#)

 Data Server Settings [102](#)

 Distribution Server settings [69](#)

 Email Settings [80, 92](#)

 General Preferences [74](#)

 LDAP Setting [99](#)

 Log Settings [98](#)

 Other Schedule Defaults [97](#)

 ZIP Settings [95](#)

configuring

 InfoAssist for MR [12](#)

 Magnify license [12](#)

 Mobile Favorites [12](#)

 Quick Data [12](#)

D

Data Server settings [102](#)

Deferred Reporting settings

 IBI_Deferred_Custom_Description [38](#)

 IBI_Deferred_Notify_Submitted [38](#)

 IBI_Deferred_Ticket_Delete_Confirm [38](#)

Distribution Server [58](#)

 configuring [69](#)

 start [62](#)

 status [59](#)

 stop [62](#)

domain templates [140](#)

E

Enable(d) check box [31](#)

Enterprise domain template [140](#)

external authentication [162](#)

External Security settings [21](#)

F

folders [143](#)

- changing title [148](#)

- creating [145](#)

- deleting [148](#)

- duplicating [147](#)

- publishing [146](#), [147](#)

- viewing properties [143](#)

G

Get More Extensions [32](#)

Global Updates

- Data Server [138](#)

- Email Address [137](#)

- Email From [137](#)

- Mail Server [137](#)

- Notification Brief Message To [139](#)

- Notification Full Message To [139](#)

- Notification Reply Address [138](#)

- Notification Subject [138](#)

- Notification Type [138](#)

- Printer [137](#)

Group Membership Report [157](#)

- Creating [159](#)

groups

- adding users [161](#)

- deleting users [161](#)

H

HTML5 Chart Extensions [30](#)

HTML5 Chart Extensions Entries [31](#)

I

IBI_CM_Export_WFRS_File_Extensions [37](#)

IBI_CM_Retain_Handles [37](#)

IBI_CM_Zip [37](#)

IBI_CM_Zip_File_Format [38](#)

IBI_CM_Zip_File_Verify_Signature [38](#)

IBI_Deferred_Custom_Description [38](#)

IBI_Deferred_Notify_Submitted [38](#)

IBI_Deferred_Ticket_Delete_Confirm [38](#)

IBI_DESCRIBE_TEMPLATES [40](#)

IBI_TEXT_GENERATION_SERVER_URL [41](#)

IBI_WFDescribe_Default [40](#)

IBIF_Describe_Null [41](#)

IBIMR_Prompting [39](#)

IBIMR_PromptingUnset [40](#)

InfoAssist

- license configuration [12](#)

J

Job Logs [64](#)

Job Status [63](#)

L

LDAP [99](#)

configuration [99](#)

email settings [99](#)

settings [99](#)

license code configuration [12](#)

M

Magnify license [12](#)

Manage Private Resources [162](#)

mime.wfs configuration file [27](#)

redirection settings [27](#)

Mobile Favorites license [12](#)

O

Options window [178](#)

P

Parameter Prompting settings

IBI_Describe_Templates [40](#)

IBI_WFDescribe_Default [40](#)

IBIF_describe_null [41](#)

IBIMR_Prompting [39](#)

IBIMR_PromptingUnset [40](#)

Properties panel [143](#)

Q

Quick Data license [12](#)

R

Redirection Settings [27](#)

ReportCaster configuration folders [67](#)

Reporting Server settings [108](#)

Reporting Servers

adding servers [109](#)

resource templates [140](#)

S

SaaS Tenant domain template [140](#)

sMAAccountName [150](#)

schedule blackout dates [110](#)

Schedule Distribution Method Settings [78](#)

Schedule Format settings [75](#), [76](#)

schedule formats

configuring [74](#)

Schedule Method setting [78](#)

schedule methods

configuring [74](#)

T

Text Generation Server Settings

IBI_TEXT_GENERATION_SERVER_URL [41](#)

U

Upload and Install Extensions Page [32](#)

user preferences

- changing [178](#)
- environment and styling [179](#)
- format [179](#)
- layout [179](#)
- view [178](#)

users [149](#)

- adding to groups [161](#)
- deleting [156](#)
- editing details [156](#)
- removing from groups [161](#)

W

WebFOCUS Reporting Servers

- configuring multiple [108](#)

Z

Zip distribution

- configuring [95](#)
- settings [95](#)



Feedback

Customer success is our top priority. Connect with us today!

Information Builders Technical Content Management team is comprised of many talented individuals who work together to design and deliver quality technical documentation products. Your feedback supports our ongoing efforts!

You can also preview new innovations to get an early look at new content products and services. Your participation helps us create great experiences for every customer.

To send us feedback or make a connection, contact Sarah Buccellato, Technical Editor, Technical Content Management at Sarah_Buccellato@ibi.com.

To request permission to repurpose copyrighted material, please contact Frances Gambino, Vice President, Technical Content Management at Frances_Gambino@ibi.com.



WebFOCUS

/ Setting Up Your Environment
Release 8.2 Version 03



**Information
Builders**

Information Builders, Inc.
Two Penn Plaza
New York, NY 10121-2898