precisely

Assure DQ

System Administrator's Guide

Notices

Trademarks

Infogix, the Infogix logo, ACR, ACR/Detail, ACR/Summary, ACR/Workbench, ACR/Connector, Infogix Assure, Infogix Insight, ACR/Instream, ACR/File, Infogix ER, Infogix Perceive, Data3Sixty, and Data360 are registered trademarks of Precisely. Data3Sixty Analyze, Data3Sixty Govern, Data3Sixty DQ+, Data360 Analyze, Data360 Govern and Data360 DQ+ are trademarks of Precisely. Any other trademarks or registered trademarks are the property of their respective owners.

1700 District Ave Ste 300
Burlington MA 01803-5231
USA

www.precisely.com

Contents

Chapter 7 Integration

Chapter 8 Result Actions

Index

1

Introduction

This guide explains how to maintain the Assure DQ® system in a production environment. The guide describes common system administration tasks, including renewing the license, exporting controls into production, maintaining the Assure DQ database, integrating with other products, and making post-installation configuration changes.

About This Guide

This guide has the following chapters:

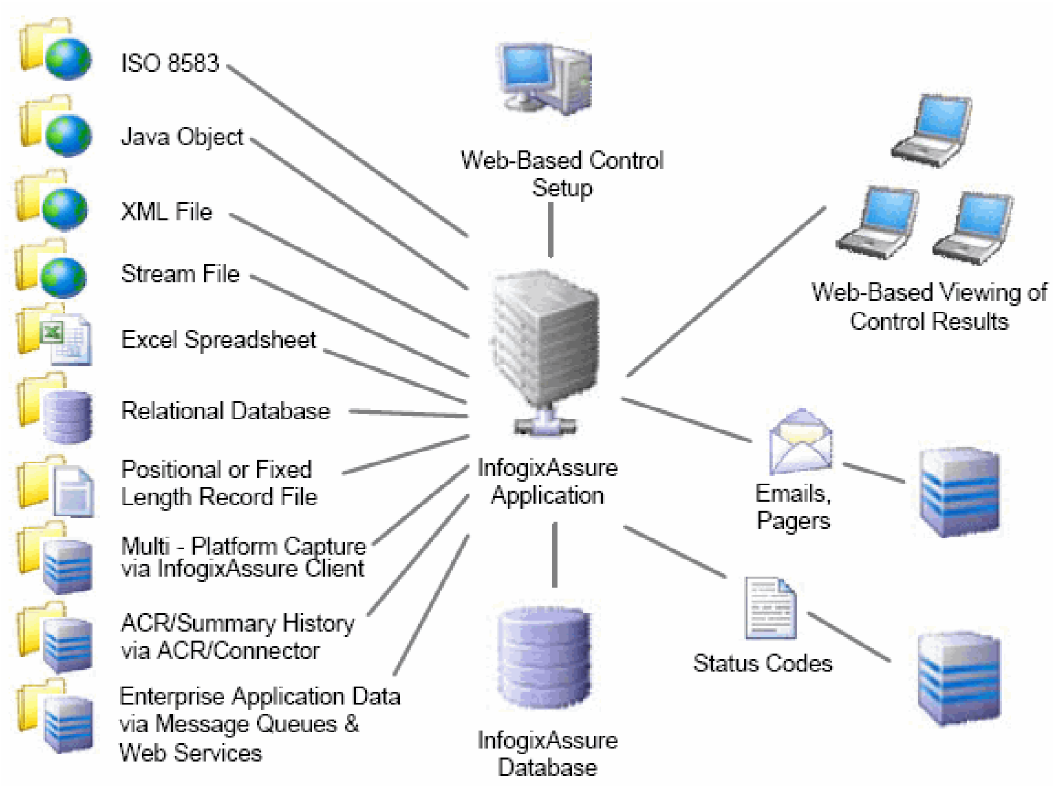
- Chapter 2, “Licensing”—Check and update your Assure DQ license and change license checking frequency and users to notify of license expiration.
- Chapter 3, “Exporting and Importing Definitions”—Export and import definitions from test to production.
- Chapter 4, “User-Specified Normalization Rules”—Optionally, set up hash capture normalization rules and import them into Assure DQ. Normalization rules specify specific characters or categories of characters to include or exclude when hashing input data sources.
- Chapter 5, “Database Maintenance”—Use utilities that automatically purge the Assure DQ database.
- Chapter 6, “Application Server Maintenance”—Configure the application post installation, set up JMS message queues for data capture sources, generate and install jars for Web Service data sources, and configure IMS® database connections.
- Chapter 7, “Integration”—Configure Assure DQ to communicate with ER™, ACR/Connector®, and Insight®. Freeze the internal clock to faciliatate system integration testing.
- Chapter 8, “Result Actions”—See the default location and categorization of log messages generated by log actions; configure user preferences (including email notfications), configure the format and content of email alerts sent by Assure DQ; write messages to multiple logs based on log category.

Command Line Utilities

Command line utilities are available to perform many of the tasks that are covered in this guide. See the table below for a list of the utilities, a description of each, and a link to the information.

Utility	Description	
aboutAssure	Display version and build number, licensed modules, and upcoming license expirations.	See page 11.
deletealerts	Remove expired alerts or alerts that are older than a specified date or age.	See page 48.
deleteControlData	Delete control data by cycle and run range.	See page 52.
deleterun	Delete control run results and reports by catalog ID, or by date range and control name.	See page 50.
exportCalendar, exportLayouts, exportTranslations, exportResultTemplates, exportResultActions	Export definitions from a test environment.	See chapter 3.
exportce, importce, exportapp, importapp	Export/Import control entities or applications and their associated layouts, translations, result templates, calendars, and result actions.	See chapter 3.
loaddigestfilter	Import an XML file that contains normalization rules into Assure DQ.	See page 34.
systemimportexport	Export definitions for import into another instance of Assure DQ.	See page 25.
updateUserPreferences	Configure email and pager alert preferences for individual users.	See page 91.

Assure DQ Operating Environment



Contacting Customer Support

If you need assistance, contact Infogix Customer Support.

Support Website: http://support.infogix.com

Visit our Website: www.precisely.com

2

Licensing

The system checks for upcoming license expirations and writes warning messages to the server log beginning 90 days prior to expiration. Email notifications to specified users occur on the same schedule, if you provide a list of email addresses to notify. In the user interface, Help > About Us lists all licensed modules and upcoming license expirations.

To avoid disruptions to control processing, contact Infogix customer support as soon as you receive license expiration warnings.

The procedures that follow describe how to update your license and how to change license checking frequency and users to notify:

- Renewing or Reinstating a License
- Rescheduling License Expiration Checking
- Changing Users to Notify

Checking License Status

You can run a command line utility or log in to the user interface to determine which Assure DQ modules are licensed to your organization and check for upcoming license expirations.

To run the command line utility, open <install_folder>/Infogix/server-util /<config_name>/IA and run aboutAssure.bat or aboutAssure.sh.

To check license status in the user interface, select Help > About Us. "Enabled" appears on the Modules list next to any modules currently licensed to your organization. Expiration dates appear in red next to any modules with upcoming expirations.

Renewing or Reinstating a License

To renew or reinstate licenses for Assure DQ, complete the following steps:

1. Contact Infogix Customer Support and request the Infogix license file.

   U.S. and Canada: Call us at +1.630.505.1890 or send a fax to +1.630.505.1883. You can also send an email to support@infogix.com.

   Outside the U.S. and Canada: Infogix maintains offices around the world. Check our Web site at www.infogix.com for the closest office or email us at support@infogix.com.

2. Place the license file in the Infogix licenses directory, which is <install_folder>/Infogix/licenses.
3. Run the update-config script located in <install_folder>/Infogix/bin to install the license.

   Allow five minutes for the license to take effect.
4. Open <install_folder>/Infogix/server-util/<config_name>/IA and run aboutAssure.bat or aboutAssure.sh to verify that you have successfully reactivated your license.

Rescheduling License Expiration Checking

The system checks for upcoming license expirations once a week and notifies specified users by e-mail. Notifications and warning messages in Help > About Us and the server log begin 90 days prior to license expiration.

To change the frequency of license checking and email notifications, complete the following steps:

1. Log in to the Assure DQ user interface as an Administrator, Integrity Rule Administrator, or Superuser.
2. Select Rules > Calendars.
3. Select the Infogix License Check Schedule from the calendar list.
4. In the bottom pane, click Edit Events.
5. Follow the directions in the online help to edit the schedule.

   The default schedule checks for upcoming license expirations once a week. The system notifies specified users beginning 90 days prior to license expiration.
6. Click Apply and then OK.

Changing Users to Notify

The system can notify specified users of upcoming license expirations. To specify users to notify or to update the existing list, customize the LICENSE_EXPIRING_ EMAIL_LIST property in the appserver.properties file. The file is located in <install_folder>/Infogix/config/config_name. User notifications are optional but strongly recommended.

Property	Description
LICENSE_EXPIRING_ EMAIL_LIST	Specify the email addresses of users to notify when the Assure DQ license is about to expire. Enter a comma-separated list similar to the following example: sysadmin@mycompany.com, asmith@abc.org

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

3

Exporting and Importing Definitions

This chapter explains how to export and import definitions from one instance of Assure DQ to another, such as from test to production. To migrate definitions from one instance of Assure DQ to another, use the export and import capabilities in the user interface or command line utilities.

This chapter has the following sections:

- Exporting and Importing Controls
- Exporting and Importing Definitions

Exporting and Importing Controls

The export and import capabilities in the user interface enable you to back up or migrate control entities or applications from one instance of Assure DQ to another. When you export controls, the associated reusable rules are also included. These consist of layouts, translations, calendars and, for control entities only, result templates. When you import with the user interface, you can choose which of these associated reusable rules to bring in to the current environment.

Command line utilities for importing controls are also available. Optionally, a job scheduler can invoke these utilities to perform imports on a scheduled basis rather than manually.

To avoid unexpected loss of production data, review the retention policies for each control before migrating it from test to production. Assure DQ automatically applies user-specified data retention policies to purge control data, reports, and results from the database.

Exporting Controls

You can export controls by using a command line utility or the user interface. The export process creates a ZIP file of one or more controls and the associated rules that they depend on.

Exporting Controls With the User Interface

The export capability in the user interface creates a ZIP file of one or more control entities or applications and their associated layouts, translations, calendars and, for control entities only, result templates. You can use this ZIP file to back up controls and to migrate controls from one instance of Assure DQ to another. To export controls, complete the following steps:

1. Log in to the Assure DQ user interface.
2. Select Rules > Controls or Rules > Quality Controls.
3. Optionally, you can pre-select control entities or applications to export from the current page of the list.

   To select all control entities or applications, click the check box above the first column of the list.
4. Click Export.
5. To select controls for export, click Add.
6. For control entities only, click Find Referenced Controls to see a list of other control entities referenced by the entities listed for export.

   These are entities that you may need to export in order to avoid import errors. The Depth column indicates the relationship of each entity to an entity already on the export list or a referenced entity. Entities on the export list directly depend on depth 1 entities for things such as history data, cycle and run numbers, or triggering. Depth 2 entities directly depend on depth 1 entities on the list of referenced controls. Depth 3 entities depend on depth 2 entities, and so on.
7. For more information on references, select the check box next to any control entity and click View Referenced By Report.

   Use the report to determine which entities reference the selected entity and why. A control entity import will fail if an entity that provides a cycle and run number or history data is missing in the target environment. An import will not fail if an entity contains a control point triggered by a missing entity. However, control runs will not be triggered.
8. If you decide not to export a referenced entity, select it and click Remove.
9. To add the remaining referenced entities to the export list, click OK.
10. When you are ready to export the entities or applications on the export list, click Finish.
11. Specify a name and path for the ZIP file and click Save.

Exporting Control Entities From the Command Line

You can use the export control entity command line utility to export control entities and their associated layouts, translations, result templates, and calendars.

To run the utility, go to <install_folder>/Infogix/server-util/<config_name>/IA. Execute exportce.bat (for Windows) or exportce.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if you specified your username and password in the application server properties file, you do not have to specify them as parameters.

Export Control Entity Parameters	Description
-file	Specify the name of the ZIP file to be produced by the utility.
-name	Optional. You can specify a comma separated list of control entity names to export. If the name of a control entity contains blanks, enclose the control entity name in double quotes.
-namelike	Optional. You can specify a wildcard selection of control entities. Use the underscore (_) character for any single character wildcard. Use the percent (%) character for matching any number of characters. For example, FOO% selects all control entities that begin with FOO.
-securedby	Optional. You can specify the export of all control entities that are secured by a particular security profile by specifying the name of the security profile. If the security profile name contains blanks, enclose the name in double quotes.
-modifiedsince	Optional. You can specify a date in YYYY-MM-DD format. Any control entity which was modified on or after that date, including modification of any of its control points, is selected for export.
-findallrefs	Optional. When specified, the system will find all control entities that are referenced by the initially selected control entities, or by one of the found referenced control entities, and include them in the export.

Export Control Entity Parameters	Description
-username	User ID to connect to http server (optional).
-password	User password to connect to http server (optional).
-proxypassword	User password to connect to http proxy server (optional).
-proxyusername	User ID to connect to http proxy server (optional).

To export particular control entities by name, enter a command similar to the following example:

Windows®: `exportce -file rules.zip -name "ce name1","ce name2"`

UNIX®/Linux®: `./exportce.sh -file rules.zip -name "ce name1","ce name2"`

To export the set of controls that are secured by a particular security profile that were modified since a particular date, enter a command similar to the following example:

Windows: `exportce -file rules.zip -securedby "My Profile Name" -modifiedsince 2014-05-01`

To additionally export all controls referenced by selected controls, enter a command similar to the following example:

UNIX®/Linux®: `./exportce -file rules.zip -securedby "My Profile Name" -modifiedsince 2014-05-01 -findallrefs`

To pass a username and password, enter a command similar to the following example:

UNIX/Linux: `./exportce.sh -file rules.zip -namelike XYZ% -username` *`user_id`* `-password` *`user_password`*

Exporting Applications From the Command Line

You can use the export application command line utility to export applications and their associated layouts, translations, and calendars.

To run the utility, go to <install_folder>/Infogix/server-util/<config_name>/IA. Execute exportapp.bat (for Windows) or exportapp.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if you specified your username and password in the application server properties file, you do not have to specify them as parameters.

Export Application Parameters	Description
-file	Specify the name of the ZIP file to be produced by the utility.
-name	Optional. You can specify a comma separated list of application names to export. If the name of an application contains blanks, enclose the application name in double quotes.
-namelike	Optional. You can specify a wildcard selection of applications. Use the underscore (_) character for any single character wildcard. Use the percent (%) character for matching any number of characters. For example, FOO% selects all applications that begin with FOO.
-securedby	Optional. You can specify the export of all applications that are secured by a particular security profile by specifying the name of the security profile. If the security profile name contains blanks, enclose the name in double quotes.
-modifiedsince	Optional. You can specify a date in YYYY-MM-DD format. Any application which was modified on or after that date, including modification of any of its control points, is selected for export.
-findallrefs	Optional. When specified, the system will find all control entities that are referenced by the initially selected control entities, or by one of the found referenced control entities, and include them in the export.
-username	User ID to connect to http server (optional).
-password	User password to connect to http server (optional).
-proxypassword	User password to connect to http proxy server (optional).
-proxyusername	User ID to connect to http proxy server (optional).

To export particular applications by name, enter a command similar to the following example:

Windows®: `exportapp -file rules.zip -name “ce name1”,”ce name2”`

UNIX®/Linux®: `./exportapp.sh -file rules.zip -name “ce name1”,”ce name2”`

To export the set of controls that are secured by a particular security profile that were modified since a particular date, enter a command similar to the following example:

Windows: `exportapp -file rules.zip -securedby “My Profile Name” -modifiedsince 2014-05-01`

To additionally export all controls referenced by selected controls, enter a command similar to the following example:

UNIX®/Linux®: `./exportapp -file rules.zip -securedby “My Profile Name” -modifiedsince 2014-05-01 -findallrefs`

To pass a username and password, enter a command similar to the following example:

UNIX/Linux: `./exportapp.sh -file rules.zip -namelike XYZ% -username` *`user_id`* `-password` *`user_password`*

Importing Controls

You can import controls by using a command line utility or the user interface. The import process checks to see which calendars, layouts, translations, and result templates currently exist in the target environment.

To selectively import definitions, import using the user interface. For example, you might use a simple calendar during testing that does not account for scheduled production system downtimes. You would not want to overwrite your production calendar with the test calendar when you import controls.

Security profiles control which groups and users can access and modify definitions, results, and reports for individual control entities and applications. When you import a control entity or application from one instance of Assure DQ to another, the name and ID of the security profile assigned to the entity or application are imported too. However, the user and group permissions associated with the profile are not imported.

If a profile with the same ID exists in the target instance, the permissions associated with that profile are assigned to the imported entity or application. If no matching profile ID exists in the target instance, the system assigns the default security profile. See the *Security Administrator's Guide* for more information on security profiles.

Importing Controls With the User Interface

To import control entities or applications from the user interface, complete the following steps:

1. Log in to the Assure DQ user interface.
2. Select Rules > Controls or Rules > Quality Controls.
3. Click Import.

   The system displays the Import Controls window.
4. Click Browse and navigate to the ZIP file to import.
5. Select the file and click Open.
6. Click Open to see the control entities or applications and referenced calendars, layouts, translations, and result templates (for control entities) included in the ZIP file.
7. Review the list of referenced rules included in the ZIP file.

   The Status column indicates whether the system will add or update the control entity or application as a result of the import. If a rule does not exist in the target environment, you must import it. New rules are added to the system. Updated rules are overwritten.
8. Select Do Not Import for any rule you do not want to overwrite or update.

   Other controls may share the calendars, layouts, translations, or result templates associated with the control entities or applications you are about to import. In a production system, you may not want to update shared rules that already exist in the system.
9. To toggle the Import/Do Not Import setting for all referenced rules, click Import Referenced Rules.

   You can still change the setting for individual rules, as needed.
10. Click Finish.
11. Click Close to return to the Manage Controls or Manage Applications list.

Importing Control Entities From the Command Line

You can use the import control entity command line utility to import control entities and their associated layouts, translations, result templates, and calendars. Optionally, a job scheduler can invoke this utility to perform imports on a scheduled basis rather than manually.

To run the utility, go to <install_folder>/Infogix/server-util/<config_name>/IA. Execute importce.bat (for Windows) or importce.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if you specified your username and password in the application server properties file, you do not have to specify them as parameters.

Import Control Entity Parameters	Description
-input	Specify the name of the ZIP file containing the rules to import. Generate the ZIP file by following the export procedure described on page 15.
-ignoredeps	Optional. Before importing a control entity from the ZIP file, the system determines if the entity has any field-level dependencies that are missing from the ZIP file. By default, the system does not import a control entity if required field-level definitions (such as layout fields used in extraction) are missing. To override the default behavior, specify -ignoredeps; the system will import the control entities even if required definitions are missing.
-delete	Optional. Before importing a control entity from the ZIP file, the system compares the rules for import to those currently in the target environment. By default, the system does **not** import a control entity if its cycle numbering method or identity control fields do not match those in the target environment. To override the default behavior, specify -delete; if cycle numbering or identity field differences exist, the system will **delete** any control data stored in the database.
-username	User ID to connect to http server (optional).

Import Control Entity Parameters	Description
-password	User password to connect to http server (optional).
-proxypassword	User password to connect to http proxy server (optional).
-proxyusername	User ID to connect to http proxy server (optional).

To import a ZIP file named rules.zip, enter a command similar to the following examples:

Windows®: `importce -input rules.zip`

UNIX®/Linux®: `./importce.sh -input rules.zip`

To ignore missing field-level definitions and delete control data if cycle numbering or identity fields have changed, enter a command similar to the following example:

Windows: `importce -input rules.zip -ignoredeps -delete`

To pass a username and password, enter a command similar to the following example:

UNIX/Linux:
```
./importce.sh -input rules.zip
-username user_id -password user_password
```

Importing Applications From the Command Line

You can use the Import Application command line utility to import data quality applications and their associated layouts, translations, and calendars. Optionally, a job scheduler can invoke this utility to perform imports on a scheduled basis rather than manually.

The system compares the data elements defined for any existing application to those in the import file. The system deletes any control data history previously stored in the database for data elements that are not defined in the imported application.

To run the utility, go to <install_folder>/Infogix/server-util/<config_name>/IA. Execute importapp.bat (for Windows) or importapp.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if you specified your username and password in the application server properties file, you do not have to specify them as parameters.

Import Application Parameters	Description
-input	Specify the name of the ZIP file containing the rules to import. Generate the ZIP file by following the export procedure described on page 15.
-ignoredeps	Optional. Before importing an application from the ZIP file, the system determines if the application has any field-level dependencies that are missing from the ZIP file. By default, the system does not import an application if required field-level definitions are missing (such as layout fields used as source fields for data elements). To override the default behavior, specify -ignoredeps; the system will import the applications even if required definitions are missing.
-username	User ID to connect to http server (optional).
-password	User password to connect to http server (optional).
-proxypassword	User password to connect to http proxy server (optional).
-proxyusername	User ID to connect to http proxy server (optional).

To import a ZIP file named applications.zip, enter a command similar to the following examples:

Windows®: `importapp -input applications.zip`

UNIX®/Linux®: `./importapp.sh -input applications.zip`

To ignore missing field-level definitions, enter a command similar to the following example:

Windows: `importapp -input applications.zip -ignoredeps`

To pass a username and password, enter a command similar to the following example:

UNIX/Linux: `./importapp.sh -input applications.zip -username` *`user_id`* `-password` *`user_password`*

Exporting and Importing Definitions

The export and import capabilities in the system enable you to back up or copy layouts, translations, result actions, or result templates from one instance of Assure DQ to another. The export process creates a ZIP file that contains the definitions of your choice and the names of the associated security profiles.

The export file also includes references to any dependent or related definitions. In the user interface, the import function verifies that the referenced definitions exist in the target environment. In addition, the import function indicates whether the definitions will replace existing definitions. You can cancel the import if you are concerned about missing definitions or if you do not want to overwrite existing definitions.

Exporting Definitions

You can export definitions by using a command line utility or the user interface. The exception is Calendars, which can only be exported using the command line.

Exporting Definitions With the User Interface

The export function in the user interface creates a ZIP file of one or more layouts, translations, result actions, or result templates. You can use this ZIP file to back up or import definitions into another instance of Assure DQ.

Note that you cannot export Calendars from the user interface. See the next section for instructions on how to export calendars from the command line.

To export definitions from the user interface, complete the following steps:

1. Log in to the Assure DQ user interface.
2. From the Rules menu, select one of the following types of definitions to export:
   - Results (that is, result templates)
   - Result Actions
   - Layouts
   - Translations

3. Optionally, filter the list of definitions.
4. Select the definitions you want to export.
5. Click Export.

   You will be prompted to save a ZIP file containing the definitions for export. Once you choose to save the file, you can accept a default directory and file name or specify different ones.

Exporting Definitions From the Command Line

You can use the export definition command line utilities to export layouts, translations, results, result actions, and calendars.

To run the utility, go to <install_folder>/Infogix/server-util/<config_name>/IA. For the different types of definitions, the following utilities are available:

- Results - exportResultTemplates.bat (for Windows) or exportResultTemplates.sh (for UNIX or Linux)
- Result Actions - exportResultActions.bat (for Windows) or exportResultActions.sh (for UNIX or Linux)
- Layouts - exportLayouts.bat (for Windows) or exportLayouts.sh (for UNIX or Linux)
- Translations - exportTranslations.bat (for Windows) or exportTranslations.sh (for UNIX or Linux)
- Calendars - exportCalendar.bat (for Windows) or exportCalendar.sh (for UNIX or Linux)

Execute the desired utility, followed by the appropriate parameters from the table below. Note that if you specified your username and password in the application server properties file, you do not have to specify them as parameters.

Export Definition Parameters	Description
-file	Specify the name of the ZIP file to be produced by the utility. This must be a full path name, and must be accessible by the running server.
-name	Optional. You can specify a comma separated list of definition names to export. If the name of an definition contains blanks, enclose the name in double quotes.

Export Definition Parameters	Description
-namelike	Optional. You can specify a wildcard selection of definitions. Use the underscore (_) character for any single character wildcard. Use the percent (%) character for matching any number of characters. For example, FOO% selects all definitions that begin with FOO.
-securedby	Optional. You can specify the export of all definitions that are secured by a particular security profile by specifying the name of the security profile. If the security profile name contains blanks, enclose the name in double quotes.
-modifiedsince	Optional. You can specify a date in YYYY-MM-DD format. Any definition which was modified on or after that date is selected for export.
-username	User ID to connect to http server (optional).
-password	User password to connect to http server (optional).
-proxypassword	User password to connect to http proxy server (optional).
-proxyusername	User ID to connect to http proxy server (optional).

Importing Definitions

You can import layouts, translations, result actions, or result templates with the user interface or a command line utility. You can import calendars using a command line utility.

Security profiles determine which groups and users can access and change definitions. When you import definitions with a security profile ID that exists in the target instance, the permissions associated with that profile are assigned to the imported definitions. If you import definitions that do not exist in the current instance and that lack a security profile because they are from an older version of Assure DQ, the system applies the default security profile. The system also applies the default profile if you import a layout with a security profile that does not exist in the current instance.

Importing Definitions With the User Interface

When you import definitions with the user interface, the system automatically unzips the file and checks to see if any related definitions are missing from your target environment. If these elements are missing, you can still import the definitions, but references to the missing definitions will be removed.

To import definitions with the user interface, complete the following steps:

1. Log in to the Assure DQ user interface.

   You must be a superuser or an integrity rule administrator to import definitions.
2. From the Rules menu, select one of the following types of definitions to import:
   - Results (that is, result templates)
   - Result Actions
   - Layouts
   - Translations
3. Click Import.
4. Browse for the ZIP file to import and click Open.
5. Click Open in the top pane.

   The system lists the definitions included in the ZIP file. The Action column indicates whether the definitions in the ZIP file are new or will replace existing definitions in the current environment.
6. If you do not want to replace existing definitions, click Cancel to stop the import.
7. Review the list of any missing dependent definitions in the bottom pane.

   These existed in the original export environment, but are not in the current import environment.
8. Click cancel if you want to stop the import because dependent definitions are missing.

   You can return to your export system and export the missing definitions.
9. Click Import when you are ready to bring the definitions into the current instance of Assure DQ.

   The system will remove references to any missing definitions.

Importing Definitions From the Command Line

You can use the system import/export utility to import calendars, layouts, translations, result actions, or result templates in ZIP files generated by the user interface export facility. Optionally, a job scheduler can invoke this utility to perform imports on a scheduled basis rather than manually.

To run the utility, go to <install_folder>/Infogix/server-util/<config_name>/IA. Execute systemimportexport.bat (for Windows) or systemimportexport.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if you specified your username and password in the application server properties file, you do not have to specify them as parameters.

System Import/ Export Parameters	Description
-import	The -import parameter must be the first parameter. The command will import all data in the ZIP file specified by the -file parameter.
-file	Specify the full path and name of the ZIP file that contains the definitions to import.
-username	Specify the username to use to connect to an http server. Optional.
-password	Specify the password to use to connect to an http server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.
-?	Describe the command line arguments.

Windows:

```
systemimportexport -import -file C:\foldername\rules.zip
```

UNIX/Linux:

```
./systemimportexport.sh -import -file /foldername/rules.zip
```

4

User-Specified Normalization Rules

When hashing and normalizing a data source, it is sometimes necessary to exclude characters that are represented differently on different platforms. Otherwise, the same file may produce different hashes as it transfers among platforms. For example, square brackets are represented differently in ASCII versus EBCDIC.

To resolve this problem, you can set up hash capture normalization rules and import them into Assure DQ. Normalization rules specify specific characters or categories of characters to include or exclude from hashing. Excluded characters are hashed as blanks or white space.

To create normalization rules, use a text editor and follow the guidelines in the next section of this chapter. Then, import the rules into Assure DQ using the Load Digest Filter utility described on page 34. Imported normalization rules are available for selection on the Capture/Source tab on the Normalize Character Rule drop-down list.

When exporting control entity rules, any normalization rules used by the control entity are automatically exported as part of the .zip file.

Defining Rules

To include and exclude various characters and symbols from normalization, use a text editor to create rules similar to the samples on page 32. You can apply one rule per data source, but the same rule can include and exclude multiple characters or categories of characters.

The first sample rule specifies normalization of letters of the alphabet and numbers only. Note that if you specify ANY characters to include, you must specify ALL the characters you want to include in the hash.

The second sample rule specifies normalization of all characters except currency symbols and asterisks. If you specify only characters to exclude, any other characters will be included by default.

Place the XML header highlighted in bold at the beginning of each rule file, and save the file with an .xml extension.

Letters and Numbers Only

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<digestFilter xmlns="/generated/export/capture/
digestFilter">

   <includeChars>
   <category type="LOWERCASE_LETTER"/>
   <category type="UPPERCASE_LETTER"/>
   <category type="DECIMAL_DIGIT_NUMBER"/>
   </includeChars>

   <excludeChars/>

</digestFilter>
```

All Characters Except Currency Symbols and Asterisks

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<digestFilter xmlns="/generated/export/capture/
digestFilter">

   <includeChars/>

   <excludeChars>
   <category type="CURRENCY_SYMBOL"/>
   <charValue value="*"/>
   </excludeChars>

</digestFilter>
```

Supported Formats

Use the following categories of characters when specifying characters to include or exclude. Enclose the category names in quotes and use the exact capitalization and spelling shown.

For descriptions of the characters included in each category, see http://www.fileformat.info/info/unicode/category/index.htm.

Numbers and Letters

"DECIMAL_DIGIT_NUMBER"

"LETTER_NUMBER"

"LOWERCASE_LETTER"

"MODIFIER_LETTER"

"OTHER_LETTER"

"OTHER_NUMBER"

"TITLECASE_LETTER"

"UPPERCASE_LETTER"

Symbols

"CONTROL"

"CURRENCY_SYMBOL"

"MATH_SYMBOL"

"MODIFIER_SYMBOL"

"OTHER_SYMBOL"

"SURROGATE"

Punctuation

"CONNECTOR_PUNCTUATION"

"DASH_PUNCTUATION"

"ENCLOSING_MARK"

"END_PUNCTUATION"

"FINAL_QUOTE_PUNCTUATION"

"INITIAL_QUOTE_PUNCTUATION"

"OTHER_PUNCTUATION"

"START_PUNCTUATION"

Formatting Characters

"COMBINING_SPACING_MARK"

"FORMAT"

"LINE_SEPARATOR"

"NON_SPACING_MARK"

"PARAGRAPH_SEPARATOR"

"SPACE_SEPARATOR"

Importing Rules

Use the loaddigestfilter utility to import an xml file containing normalization rules into Assure DQ. On the server, the utility is in <install_folder>/Infogix/server-util/<config_name>/IA. The utility is also in the same directory where the Assure DQ client is installed, normally <infogix_client_install_folder>/Assure_Client.

To see syntax information for the utility, go to the directory where the utility is located and enter the name of the utility followed by -?. On Windows, enter a command similar to the following example:

loaddigestfilter -?

You must have Integrity Rule Administrator authorization to run the utility. Navigate to the directory where the utility is located and enter the name of the utility at the command prompt, followed by the appropriate parameters from the table below.

Load Digest Filter Parameters	Description
-file	Specify the full path and name of the file containing the rule.
-name	A name for the rule. Enclose the name in quotes if it contains spaces.
-dispName	A user friendly name for the rule, for display in the user interface. The display name can be the same as the rule name above, or not. Enclose the name in quotes if it contains spaces.
-desc	Description of the rule. Optional.
-username	Specify the username to use to connect to an http server. Optional.
-password	Specify the password to use to connect to an http server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.
-?	Describe the command line arguments.

To load normalizeABC.xml on the server and name it Application ABC Rule, enter a command similar to the following example:

Windows:

```
loaddigestfilter -file C:\home\user2\normalizeABC.xml
-name ApplicationABCRule -dispName "Application ABC Rule"
-username user_id -password user_password
```

UNIX/Linux:

```
./loaddigestfilter.sh -file /home/websph1/normalizeABC.xml
-name ApplicationABCRule -dispName "Application ABC Rule"
-username user_id -password user_password
```

To verify that the rule loaded successfully, navigate to Rules > Controls > Capture tab in the user interface. Select Hash Capture. For Data Digest, select one of the normalized formats: CRC32 Normalized or MD5 Normalized. Your imported rule should appear on the Normalize Character Rule list.

5

Database Maintenance

This chapter describes database maintenance activities and system configuration properties related to data retention. The chapter has the following sections:

- Data Retention and Archiving
- Changing the Alert Deletion Schedule
- Changing Audit History Retention
- Rule Text Search Options
- Changing Storage Options
- Database Performance Optimization
- Rerunning Controls
- Database Maintenance Utilities

Data Retention and Archiving

Retention policies determine when to purge old control data, results, and reports from the system. The rules writer specifies an appropriate retention period for each control entity or data quality application on the Storage tab for the entity or application.

For data quality applications, the system default retention policy is 120 days. If you would like to change the default policy, edit the DEFAULT_APP_RETENTION_DAYS property in the IA.properties file. The file is located in <install_folder>/Infogix/config /<config_name>/IA. A similar, system level default property does not exist for control entities.

By default, the Infogix Apply Retention Policy Schedule applies retention processing daily at 00:00. This is a single, shared schedule that applies the retention policies to all control entities and applications.

Rules writers can select an option on the control entity or application Storage tab to apply retention to an individual entity on a different, separate schedule. Consider using this feature if an entity generates a lot of results or reports that you want to purge on a different, separate schedule or at a time when fewer resources are required for production processing.

In production, it is advisable to archive results and reports to an external location before retention processing deletes them from Assure DQ. The section that follows describes how to enable the automatic archiving feature, which runs archival processing on a scheduled basis.

Automatic Archiving

The system can automatically archive results and reports to an external location of your choice. If you enable automatic archiving, a scheduled system utility generates archivable results and reports.

Configuration properties enable archival processing. You can archive result catalogs, control reports, recap reports, user reports, reconciliation task reports, failed value reports, and match set audit reports. Available file formats include PDF, csv, and text.

Results and reports must be successfully archived before retention processing can remove them from the system. When necessary, you can override this safeguard to skip archiving of unwanted or problematic results or reports and proceed with retention processing. See the *Operator's Guide* for instructions on how to skip archiving.

To enable archiving, edit the archive properties in the IA.properties file located in <install_folder>/Infogix/config/<config_name>/IA.

Property	Description
SYSTEM_ARCHIVE_ENABLED	Set to true to enable automatic archiving for the current instance of Assure DQ.
SYSTEM_ARCHIVE_FORMAT	This property specifies the format for reports generated for archiving. The available options are pdf (default), text, or csv. Match Set Audit reports are always generated in text format, and Failed Value reports are always generated in csv format, regardless of the output format specified. The system generates result catalogs as pdfs if you specify csv format.

In addition, specify a suitable destination for your archived files in the archive.properties file located in <install_folder>/igx-data /<config_name>/IA/config.

Property	Description
ARCHIVE _HOME	Specify the full path to a shared directory accessible to the Assure DQ server. To avoid data loss and performance issues, choose a location external to the Assure DQ server suitable for storing large volumes of data.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

The Infogix Archival Schedule runs archival processing daily at 21:00. See the instructions in the *Operator's Guide* on how to edit this schedule to ensure archival processing occurs during off peak processing times prior to retention processing.

When possible, daily archival processing is desirable to prevent archiving from taking too long on any given day. This is because the system only has to archive control data and reports generated within the previous 24 hours.

If you need to disable archiving at any time, simply reset the SYSTEM_ARCHIVE_ENABLED property to false and run update-config.

Changing Audit History Retention

Audit history provides a record of Assure DQ control point executions and changes to control rules or control data. Internal auditors and superusers can view and print this information, as needed.

By default, the system retains audit history for a period of one year. To change the retention period, customize the property below in the IA.properties file located in <install_folder>/Infogix/config /<config_name>/IA.

Property	Description
AUDIT_HISTORY_RETPD	By default, the system retains audit history for a period of one year, specified as P1Y. To specify a different retention period, retain the P (period) parameter and specify years, months, and days in the format P*n*Y*n*M*n*D. For example, P1Y3M14D retains audit history for one year, three months, and 14 days.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Rule Text Search Options

The system can be configured to allow rules developers to search the contents of rules for things that they need to maintain (names, constants, etc...). When rule text search is enabled, the system builds a search index on the file system of the application server. The system places this search index in a folder called “search” under the DATA_HOME folder defined for the installation.

To enable rule text search, edit the search properties in the IA.properties file located in <install_folder>/Infogix/config/<config_name>/IA.

Property	Description
SEARCH_TEXT_ENABLED	Set to true to enable text search. When true, search data is generated under DATA_HOME at least once per day. You might choose to enable rule search in all environments except production.
SEARCH_INDEX_ON_RULECHANGE	If this property is set to true, the system updates its search index every 5 minutes. Otherwise, rule search index data is only updated once per day. You might choose to enable this level of update in the lowest rules development environment, but not in the higher test or pre-production environments.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Two scheduled jobs are installed by the system for search indexing. The job “Search Index Daily Update”, which uses the schedule calendar “Infogix Rules Indexing Schedule”, performs the primary indexing of rules once per day. The job “Search Index Recently Changed Rules”, which uses the schedule calendar “Infogix Search Index On Event Schedule”, runs on an every 5 minute schedule to search index those rules that were changed within the last 5 minutes.

You can rebuild the entire search index by deleting the “search” folder under the DATA_HOME folder, and then performing a “Run Job Immediately” on the “Search Index Daily Update” job from the System > Scheduler page.

Configuring Storage for Reports

To change the storage and compression options for Control Reports and Match Set Audit Reports, customize the properties below in the appserver.properties file, located in <install_folder>/Infogix/config/<config_name>. If you change the settings, the system does not apply the new settings to data that already exists in the database or on the file system.

Property	Description
FILESTORE_BACKEND	Specify Database to store Control Reports and Match Set Audit Reports in the database rather than on the file system. Specify FileSystem to store the reports on the file system.
ENABLE_FILESTORE_ ENCRYPTION	Specify true to encrypt Control Reports and Match Set Audit Reports stored on the file system. Specify false to disable encryption.
ENABLE_FILESTORE_ COMPRESSION	Set to true to compress Control Reports and Match Set Audit Reports stored in the database or on the file system.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Changing the Alert Deletion Schedule

Assure DQ is delivered with a maintenance calendar that automatically deletes expired alerts: Infogix Delete Alerts Schedule. This schedule specifies when and how often to delete expired alerts based on the user-defined specification. Alert expiration is defined at the action rule level; a setting in user preferences overrides this setting.

Alert deletion typically runs once a day, when the system load is low. The default settings delete expired alerts seven days a week, once each day, at 10pm.

You can change this schedule to satisfy your company's business requirements. Complete the following steps:

1. Log in to the Assure DQ user interface as an administrator, integrity rule administrator, or superuser.
2. Select Rules > Calendars.
   The system displays the Manage Calendars window. The top pane lists all calendars.
3. Select Infogix Delete Alerts Schedule and then click Edit Events.
4. Select deleteAlerts, the default event for this calendar.
   The bottom pane displays the settings for this event.
5. You can modify the following settings:
   - The name for the event
   - The start date
   - The start time
   - The end time, if this is not a recurring event
   - Whether the event occurs monthly or each week
   - The days when the event occurs, if applicable
   - The number of hours, minutes, and seconds to elapse before the event reoccurs
6. Apply each change, click OK, and then save your changes.

Changing Storage Options

Because of their potential size, the system stores Control Reports, Match Set Audit Reports, and Match Data control data on the file system.

For better manageability and access control, you can choose to store the reports in the Assure DQ database. Storage in the database will increase the database load and increase the time it takes to produce and access the reports. You can also choose to compress the reports, regardless of whether they are stored in the database or on the file system.

Optionally, the system can encrypt reports stored on the file system. Both encryption and compression will increase the time it takes to produce and access the reports.

Configuring Storage for Reports

To change the storage and compression options for Control Reports and Match Set Audit Reports, customize the properties below in the appserver.properties file, located in <install_folder>/Infogix/config/<config_name>. If you change the settings, the system does not apply the new settings to data that already exists in the database or on the file system.

Property	Description
FILESTORE_BACKEND	Specify Database to store Control Reports and Match Set Audit Reports in the database rather than on the file system. Specify FileSystem to store the reports on the file system.
ENABLE_FILESTORE_ENCRYPTION	Specify true to encrypt Control Reports and Match Set Audit Reports stored on the file system. Specify false to disable encryption.
ENABLE_FILESTORE_COMPRESSION	Set to true to compress Control Reports and Match Set Audit Reports stored in the database or on the file system.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Encrypting Match Data

To encrypt match data stored on the file system, complete the following steps:

1. Open <install_folder>/Infogix/server-util/<config_name>/IA/conf/persistence.properties.
2. Locate the sam.encrypt parameter and change the value to true to enable encryption.
   To change the encryption strength, see Changing Encryption, next.
3. Redeploy and restart the Assure DQ application.

Changing Encryption

The encryption property uses the standard Java key length of 128 and the AES algorithm. The DES and Triple DES algorithms are also supported. For stronger encryption, complete the following steps:

1. Open <install_folder>/Infogix/server-util/<config_name>/IA /conf/persistence.properties.
2. Locate the encrypt.AES.key.length parameter and change the value. Specify one of the following key length values:
   - 128
   - 192
   - 256
3. Redeploy and restart the Assure DQ application.

Warning:	Any changes that you make to encryption strength will affect all data encrypted on the file system. You may be unable to read data that was stored on the file system prior to the change.

Database Performance Optimization

During control setup, rules writers specify what types of data to store in the database for use in future control processing or for audit and analysis purposes. To avoid storing unneeded data, rules writers can consider the following control data history storage options as they set up controls:

- **Control Point**—For control entities, this setting retains a history of control field values throughout each cycle. For data quality applications, this setting retains a history of element measurements throughout each cycle.
- **Control Points and Trace**—Stores the same data as the Control Point option, plus detailed control trace information. Trace information consists of all data used to apply controls during a control run, such as derived values and the results of intermediate calculations used to arrive at a final validation pass/fail outcome. This option is resource-intensive and should only be applied to control entities requiring detailed analysis and auditing. Not available for data quality applications.
- **None**—This setting retains only the final control field values or element measurements for each cycle. This setting is the least resource-intensive. However, it is not appropriate for control entities that have point-to-point fields or that are referenced by a tracking rule.

The Control Data History options above are available on the control entity and application Storage tabs in the user interface.

Rerunning Controls

You can rerun one or more control points to replace control data, results, and reports in the Assure DQ database in case of a processing error or system failure. Reruns may or may not replace existing control data in the database, depending on a variety of factors. The examples below demonstrate the expected behavior for several common rerun scenarios.

Suppose a Summary control entity or a single capture Detail entity has two control points and two control fields. The control points have the following properties:

- Control point 1 (CP1) must create the control entity instance in the database.
- Control point 2 (CP2) may create or update the database instance.
- Control point 1 populates control field A1.
- Control point 2 populates control field B2.

The original control run populates the database with the following values:

Cycle 20090130 Run 0				
Input Value	**Control Field**	**CP1**	**CP2**	**End of Run**
10	A1	10	10	10
50	B2		50	50

The system operator discovers that the system processed the wrong input file at control point 1 during the original control run. The operator reruns CP1 using the correct input file. The database contains the following values at each control point:

Cycle 20090130 Run 0				
Input Value	**Control Field**	**CP1 Rerun**	**CP2**	**End of Run**
15	A1	15	15	15
	B2	50 (leftover from original run)	50	50

Suppose instead that the system processed the wrong input files at both control points during the original control run. The operator reruns both control points using the correct input files. The database contains the following values at each control point:

Cycle 20090130 Run 0				
Input Value	**Control Field**	**CP1 Rerun**	**CP2 Rerun**	**End of Run**
15	A1	15	15	15
30	B2	50 (leftover from original run)	30	30

Database Maintenance Utilities

Database maintenance utilities are located in <install_folder>/Infogix /server-util/<config_name>/IA.

To see usage information for any utility, go to the directory described above and enter the name of the utility followed by -?. On Windows, enter a command similar to the following example: deletealerts -?

The table below briefly describes each utility. For more information, see the corresponding sections of this chapter.

Database Maintenance Utilities		
Windows Name	**UNIX Name**	**Description**
deletealerts.bat	deletealerts.sh	Maintain alerts in the database.
deleterun.bat	deleterun.sh	Delete control run results and associated reports by date range and control name, or by result catalog ID.
deleteControlData.bat	deleteControlData.sh	Delete control data by cycle and run, creation date, or update date.
hashKeyLoader.bat	hashKeyLoader.sh	Loads a secret key for use with function hash_secure into the database.

You must have administrator authorization to run these utilities.

Delete Alerts Utility

The deletealerts utility removes expired alerts or alerts older than a specified date or age from user inboxes. The expiration period is defined by the rules writer when setting up an alert. Individual users can specify a shorter retention period for their own alerts by navigating to System > Preferences.

Delete Alerts Parameters	Description
-d *yy/mm/dd*	Delete alerts older than the specified date. Overrides individual user preferences and individual alert expiration periods. Optional.
-n *days*	Delete alerts older than the specified number of days from the current date. Overrides individual user preferences and individual alert expiration periods. Optional.
-password	Specify the password to use to connect to an http server. Optional.

Delete Alerts Parameters	Description
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-r	Omit alerts currently marked as unread from deletion, even if they are expired.
-username	Specify the username to use to connect to an http server. Optional.

To delete inbox alerts older than seven days for all users, enter a command similar to the following example:

Windows:

```
deletealerts -n 7
```

UNIX/Linux:

```
./deletealerts.sh -n 7
```

Delete Control Run Results Utility

The deleterun utility deletes control run results for specific result catalog IDs or for a specified date range and controls. The utility also deletes reports that are linked to the same process history as the deleted results. You may want to delete unneeded results and reports in a development or test environment, or in production if an aberrant control point execution produces large volumes of results or reports.

The system records a Delete Control Data event in the audit history trail.

Delete Run Parameters	Description
-catalogID	Optionally, you can delete specific control run results by catalog ID. You can specify one or multiple catalog IDs. To specify multiple IDs, enter a comma separated list with no spaces between IDs, for example, -catalogID 1200,1250,1275 The catalog ID displays on the Summary tab when you view results by control point. To delete results, you must specify the catalogID parameter, or a combination of the date and controlsLike or control parameters, below.
-fromDate *datetime* -thruDate *datetime*	Use these parameters to delete control run results produced between specified dates and times. If you specify a date range, you must specify the control or controlsLike option, as well. Do not specify catalog IDs, above, if you specify a date range. The date portion of the from and thru date range is required. The time portion is optional and defaults to T00:00:00 for the fromDate and T23:59:59 for the thruDate.
-controlsLike	Use this parameter in conjunction with the fromDate and thruDate options above if you want to delete results for multiple controls. To delete all control run results produced during the from/thru date range, specify -controlsLike %. To delete results for control entities and applications with names that contain a particular character string, specify -controlsLike %*characterstring.* To delete results for control entities and applications that begin with a particular character string, specify -controlsLike *characterstring%.*

Delete Run Parameters	Description
-control	Use in conjunction with the from and thru date options if you want to delete results for a single control entity or application only. Specify the control entity or application name. Optionally, to further narrow the scope of results to delete, specify a control point, below.
-point	Use in conjunction with the -fromDate, -thruDate, and the -control option, above, if you want to delete results for a single control point only. Specify the control point name. Optional.
-password	Specify the password to use to connect to an http server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-username	Specify the username to use to connect to an http server. Optional.

To delete results and reports for catalog IDs 1503, 1504, and 1506 enter a command similar to the following example:

Windows:

```
deleterun -catalogID 1503,1504,1506
```

UNIX/Linux:

```
./deleterun.sh -catalogID 1503,1504,1506
```

To delete all results and reports created on or between March 1, 2013 at 6:00 am and March 31, 2013 at 23:59:59 for control entity ABC123 and control point CP1, use commands similar to the following examples:

Windows:

```
deleterun -fromDate 2013-03-01T06:00:00 -thruDate 2013-03-31
-control ABC123 -point CP1
```

UNIX/Linux:

```
./deleterun.sh -fromDate 2013-03-01T06:00:00
 -thruDate 2013-03-31 -control ABC123 -point CP1
```

To delete all March 2013 results and reports for control entities and applications with names that contain the character string ABC, use commands similar to the following examples:

Windows:

```
deleterun -fromDate 2013-03-01 -thruDate 2013-03-31
-controlsLike %ABC
```

UNIX/Linux:

```
./deleterun.sh -fromDate 2013-03-01 -thruDate 2013-03-31
-controlsLike %ABC
```

To delete all March 2013 results and reports for control entities and applications with names that begin with the character string ABC, use commands similar to the following examples:

Windows:

```
deleterun -fromDate 2013-03-01 -thruDate 2013-03-31
-controlsLike ABC
```

UNIX/Linux:

```
./deleterun.sh -fromDate 2013-03-01 -thruDate 2013-03-31
-controlsLike ABC
```

Delete Control Data Utility

The deleteControlData utility deletes unwanted control data from the database. The utility deletes control data for control entities, but not for data quality applications. However, the Assure DQ user interface enables users to delete control data for data quality applications and control entities. The user must select Results > Control Data and have appropriate roles and permissions to access and delete control data.

Use this utility to delete control data for a control entity by cycle, creation date, or update date range. When you delete control data, the system records a control data change event in audit history.

Parameter	Description
-entity	Specify the control data to delete by control entity name. This utility does not delete control data for data quality applications.
-fromcycle -tocycle	Optionally, specify the cycle numbers that begin and end the range of control data to delete. If you specify a cycle range, do not specify a creation date range or update range.

Parameter	Description
-fromrun -torun	If you specified a cycle range, above, you can also specify the run numbers that begin and end the range of control data to delete. Optional.
-fromCreation *datetime* -toCreation *datetime*	Optionally, use these parameters to delete control data created between specified dates and times. If you specify a cycle or update range, do not specify a creation date range. The date portion of the creation date range is required. The time portion is optional and defaults to 00:00:00.
-fromUpdate *datetime* -toUpdate *datetime*	Use these parameters to delete control data updated between specified dates and times. If you specify a cycle or creation date range, do not specify an update range. The date portion of the update range is required. The time portion is optional and defaults to 00:00:00.
-password	Specify the password to use to connect to an http server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-username	Specify the username to use to connect to an http server. Optional.

Specify dates (and optionally, times in hours, minutes, and seconds) in standard ISO 8601 datetime format. See http://www.w3.org/TR/NOTE-datetime.

To delete all control data with cycle numbers between 20080101 and 20090315, enter a command similar to one of the following examples:

Windows:

```
deleteControlData -entity SOME_ENTITY_NAME -fromcycle
20080101 -tocycle 20090315
```

UNIX/Linux:

```
./deleteControlData.sh -entity SOME_ENTITY_NAME -fromcycle
20080101 -tocycle 20090315
```

To delete all control data for cycle 20080101 with run numbers between 1 and 5, enter a command similar to one of the following examples:

Windows:

```
deleteControlData -entity SOME_ENTITY_NAME -fromcycle
20080101 -tocycle 20080101 -fromrun 1 -torun 5
```

UNIX/Linux:

```
./deleteControlData.sh -entity SOME_ENTITY_NAME -fromcycle
20080101 -tocycle 20080101 -fromrun 1 -torun 5
```

To delete control data created on or between March 1, 2008 at 8:30 am and March 31, 2008 at 10:00 pm, enter a command similar to one of the following examples:

Windows:

```
deleteControlData -entity SOME_ENTITY_NAME -fromCreation
2008-03-01T08:30:00 -toCreation 2008-03-31T20:00:00
```

UNIX/Linux:

```
./deleteControlData -entity SOME_ENTITY_NAME -fromCreation
2008-03-01T08:30:00 -toCreation 2008-03-31T20:00:00
```

To delete all control data created on March 1, 2008, enter a command similar to one of the following examples:

Windows:

```
deleteControlData -entity SOME_ENTITY_NAME -fromCreation
2008-03-01 -toCreation 2008-03-01T23:59:59
```

UNIX/Linux:

```
./deleteControlData -entity SOME_ENTITY_NAME -fromCreation
2008-03-01 -toCreation 2008-03-01T23:59:59
```

Note that the time portion is optional and defaults to 00:00:00, which is the correct time for the fromCreation parameter in the example above.

Hash Key Loader Utility

The hashKeyLoader utility loads a “secret key” that is used by the hash_secure function to produce hash values that cannot be reverse engineered into the original value. Normally, this utility is run during the installation database population processing, and no further action is necessary. However, if it is felt that the secret key has been compromised, a new secret key can be generated by running this utility with the -force option. After a new secret key has been loaded, the hash values produced by function hash_secure will no longer be comparable to the hash values produced with the old secret key.

.

Parameter	Description
-force	Specify this option to force the generation of a new secret key.
-password	Specify the password to use to connect to an http server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-username	Specify the username to use to connect to an http server. Optional.

6

Application Server Maintenance

This chapter describes system configuration changes that the Assure DQ administrator may apply post-installation. The chapter has the following sections:

Changing Audit Commentary Settings

The audit commentary feature is useful in a staging or production environment. When this feature is enabled, the system prompts the user to enter a descriptive comment and change control ID for any auditable event. You can require the user to fill in the comment and/or the ID, or not.

Optionally, you can specify a pattern for the change control ID using a JavaScript™-style regular expression. You can also supply a hint to the user regarding the appropriate format for the ID, or a hyperlink to a reference page on your file system with guidelines for the ID to enter. The hint and link are both optional. If you specify them, they will display when the system prompts the user for an audit comment.

Auditors can view audit comments as part of the audit history provided in the user interface, on the Audit History Report, or in the audit history extract file.

Examples of auditable events include adding, changing, or deleting control data, control entities, or control points; duplicating a control entity or control point; testing a control point; and importing control entities and result actions.

The audit commentary properties are in the IA.properties file located in <install_folder>/Infogix/config/<config_name>/IA.

Property	Description
AUDIT_COMMENTARY_ENABLED	Set to true to prompt the user to enter a descriptive comment and change control identifier before completing an auditable event.
AUDIT_COMMENTARY_COMMENT_REQUIRED	Set to true to require the user to enter a descriptive comment. When this property is false, the user can dismiss the prompt without entering a comment.
AUDIT_COMMENTARY_CCID_REQUIRED	Set to true to require the user to enter a change control identifier, such as a change control system tracking number. When this property is false, the user can dismiss the prompt without entering a change control ID.
AUDIT_COMMENTARY_CCID_PATTERN	Optionally, specify a JavaScript-style regular expression if you want to mandate the format of the CCID. For example, the regular expression for a pattern beginning with IA-, ia-, IR- or ir- followed by digits is ^[Ii][AaRr]-\d+$. The ^ and $ symbols indicate that the ID must fully match the enclosed pattern, with no leading or trailing characters. IA-123 will match but IA-IA-123 will not. See http://www.regular-expressions.info/javascriptexample.html to test your regular expression with JavaScript or JScript. When you enter your expression in the application server properties file, use four slashes to represent a single slash. For example, to enter the expression above in the application server properties file, specify ^[Ii][AaRr]-\\\\d+$.

Property	Description
AUDIT_COMMENTARY_CCID_HINT	Optionally, enter a text hint here to display to users indicating the appropriate pattern for the CCID, such as “ID format is IA-9999, where 9999 is the change control number.” Leave this property blank if you do not want to provide a hint.
AUDIT_COMMENTARY_CCID_ HYPERLINK	Optionally, specify the URL of a document on your file system containing reference information for entering a CCID.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Limiting Results and Reports

To limit the number of results and Control Reports output by individual control point runs, customize the result limit properties below. This is desirable in production to prevent control runs that detect a high volume of errors from monopolizing system resources. For instructions on how to override report and result limits at runtime, see the online Help and the *Operator's Guide*.

The result limit properties below are in the IA.properties file located in <install_folder>/Infogix/config/<config_name>/IA.

Property	Description
VALIDATION_RESULTS_ LIMIT	Specify the maximum number of results for data capture and Scan control points to output. When the limit is met, control point processing stops and the system issues a fatal error. To permit unlimited results, accept the default value of **-1**.
VALIDATION_CTLRPTS_ LIMIT	Specify the maximum number of Control Reports for data capture control points to output. When the limit is met, control point processing stops and the system issues a fatal error. To permit unlimited Control Reports, accept the default value of **-1**.

Property	Description
FAILED_DATA_OUTPUT_LIMIT	Specify the maximum number of failed data values to record for a single Measurement control point run. The default setting of -1 records an unlimited number of failed values. This setting can be overridden for individual control points.
RECON_RESULTS_LIMIT	Specify the maximum number of results for Reconciliation control points to output. When the limit is met, control point processing stops. To permit unlimited results, accept the default value of -1.
RECON_FATAL_ERROR_ON_RESULTS_LIMIT	Accept the default value of false to stop control point execution without issuing an error when the reconciliation result limit is met. Set to true to stop control point execution and issue a fatal error when the result limit is met.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Limiting Reconciliation Control Point Searches

In a testing environment, a search and select task for a reconciliation control point may take too long to complete if a rules writer specifies search criteria that are too general. To avoid this problem, specify a search limit. The limit specifies the maximum number of left input source transactions to attempt to match to right input transactions. The Recon Task Search Limit Exceeded Fatal property determines the action to perform when the search limit, above, is exceeded. Rules writers can override both properties for individual tasks.

The reconciliation control point search limit properties are in the IA.properties file located in <install_folder>/Infogix/config /<config_name>/IA.

Property	Description
RECON_TASK_SEARCH_LIMIT	The search limit applies to Reconciliation control point search and select tasks. The limit specifies the maximum number of left input source transactions to attempt to match to right input transactions. Set the search limit to about 1000 to prevent imprecise search criteria from adversely affecting system performance. The default limit of -1 permits unlimited searches.
RECON_TASK_SEARCH_LIMIT_ EXCEEDED_FATAL	Indicates the action to perform when the search limit, above, is exceeded. Accept the default setting of true to halt execution of the control point and report an error in the result catalog. Set to false to halt execution of the select/search task and report an error in the result catalog.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Changing the Session Timeout

The default setting for the session timeout is 30 minutes. If there is no activity in Assure DQ within a 30-minute period, a user must log in again to continue.

Changing the Setting

To change the timeout setting, complete the following steps:

1. Edit the application properties:
   <install_folder>/Infogix/config/<cfgname>/appserver.properties
   Where <cfgname> is the configuration name of the installation, or “default” if a configuration name was not specified.
2. Change the SESSION_TIMEOUT value. Also review and change the SESSION_TIMEOUT_WARNING value.
3. Redeploy the application server.

Changing the Refresh Rate

To refresh results displayed in the user interface, the user sets the Period filter to display results for the current 30 minute time period. The system then refreshes the results based on a configured refresh rate. The default setting refreshes results every 30 seconds. You can change this rate in increments of milliseconds.

To change the refresh rate, create or edit
<install_folder>/Infogix/config/<cfgname>/IA/override.properties
Where <cfgname> is the configuration name of the installation, or "default" if a configuration name was not specified. Specify the following property:

Property	Description
RESULT_REFRESH_TIME	The default result refresh time is every 30 seconds. To specify a different refresh rate, enter the rate you prefer, in milliseconds. For example, to refresh every 10 seconds, enter 10000.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Changing Remember User ID

When a user logs in to Assure DQ, the user can check the option "Remember My User ID." If the user selects the option, the system remembers the User ID and populates the User ID field from a previous login to Assure DQ. After the initial login, the user is required to only enter a password to login.

The ALLOW_REMEMBER_USER_ID property can be changed so the "Remember My User ID" option does not display on the login page. A User ID and Password must be entered each time the user logs in.

The remember user ID property is in the appserver.properties file, located in <install_folder>/Infogix/config/<config_name>.

Property	Description
ALLOW_REMEMBER_USER_ID	This property controls the ability of the system to populate the User ID field from a previous login. The property defaults to true, which displays the “Remember My User ID” check box on the login page. After an initial login, the user only needs to enter a password to log in. Set to false to require the user to always enter a User ID and Password to login. The “Remember My User ID” check box does not display on the login page.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Specifying a Default EDI Dictionary Layout

Support for EDI data sources is a separately licensable feature of Assure DQ. To save time and ensure standardization, EDI layouts can reference and reuse an existing EDI layout as a dictionary. Rules writers can quickly define new EDI layouts by referencing sublayouts in the dictionary layout. To change the default EDI dictionary layout, create or edit
<install_folder>/Infogix/config/<cfgname>/IA/override.properties
Where <cfgname> is the configuration name of the installation, or "default" if a configuration name was not specified. Specify the following property:

Property	Description
DEFAULT_EDI_ DICTIONARY_RULE	Specify the name of an EDI layout to use as the default dictionary for new EDI layouts. The name is case-sensitive and must exactly match the name of the layout in the system. After a default dictionary layout is specified, rules writers can accept the default or select a different layout to use as the dictionary when creating a new EDI layout.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Saving Configuration Overrides

If you make site-specific modifications to component-level configuration properties, the system can automatically reapply your overrides when you run update-config or deploy. You can save and reapply configuration overrides for individual properties or entire properties files.

To save overrides for individual properties, follow the procedure to create an override.properties file. This procedure is in the Advanced Deployment chapter of the *Infogix Server Installation Guide* and the *Infogix Server Upgrade Guide*.

To save entire properties files containing overrides, complete the steps below:

1. Create a dedicated configuration override directory accessible to Assure DQ.

You will use this directory to store copies of any component-level configuration properties files you change post installation.

2. Open the appserver.properties file, located in <install_folder>/Infogix/config/<config_name>.
3. Locate the CONFIG_OVERRIDE property and specify the absolute path of your configuration override directory created in step 1, above.
4. Copy any component-level configuration properties files you have changed to the configuration override directory.
5. Run the update-config script located in <install_folder>/Infogix/bin.

   Allow five minutes for your overrides to take effect.
6. If you make additional changes to component-level properties in the future, repeat step 4 and step 5, above.

Configuring JMS Queues

This section explains how to configure Assure DQ to retrieve input data for control processing from JMS queues. Assure DQ can process any of the following types of inputs from a JMS queue:

- delimited records
- EDI files
- fixed length records
- ISO 8583 files
- Java objects
- XML files

JMS message data may consist of records, documents, or a continuous stream of bytes. Some types of inputs require additional licensing.

To set up JMS message queues and configure Assure DQ to retrieve messages from them, complete the following steps:

1. Set up JMS queues accessible to the Assure DQ server for each data capture source.
2. Log in the Assure DQ user interface and create a layout for each capture source.
3. Complete the Details tab for each layout. Specify the following channel information for the queue where Assure DQ will retrieve the messages:
   - Data Access Method—JMS Message Queue

- Queue Factory—The JNDI name of the queue connection factory for your queue, for example, queue/*IA_MYQUEUECF*
- Record Ending—For fixed, delimited, ISO 8583, and EDI records, choose an option based on how individual records on the queue are physically defined.
- Path/URL—The JNDI name of the queue, for example, queue/ *IA_MYQUEUE*.

Adding Plug-Ins

Optionally, you can create a directory for plug-ins on the same server where you install the Assure DQ application. Controls developers can upload plug-ins from their local hard drives or network. The system will place these plug-ins stored in jar files on the system classpath.

For example, if your control points capture data from Java object files, jar files containing the corresponding java classes must be on the system classpath. Place the jar files in the plug-ins directory and Assure DQ will place them on the classpath.

To create the directory and add plug-ins to it, complete the following steps:

1. Open the IA.properties file located in <install_folder>/Infogix /config/config_name/IA on the system where the Assure DQ server is installed.
2. Locate the PLUGINS_DIR property.

   This property may have been filled in during the installation process. If the property is blank or you want to change it, specify the full path of a directory where controls developers can place plug-ins for use with Assure DQ. The Assure DQ application server must be able to access this directory.
3. Copy any jar files or other plug-ins you want to place on the Assure DQ system classpath to the plug-ins directory.
4. Redeploy and restart the Assure DQ application.
5. If you add plug-ins in the future, repeat step 3 and step 4, above.

Setting Up an IMS Database Connection

An IMS database can serve as a data source if you have the IMS Universal JDBC™ Driver and are willing to perform the preliminary setup steps described below. You will need to download the DLIModel utility plug-in for Eclipse from the IBM® Web site in order to complete these steps.

1. Install the IMS Universal JDBC Driver on the Assure DQ installation server.
2. Download and install the IMS DLIModel utility plug-in for Eclipse.

   The plug-in transforms IMS database information (program specification blocks, database descriptions, and COBOL copybooks or PL/I includes) into application-independent metadata.
3. Use Eclipse to create a DLI model metadata class for your IMS source.

   Eclipse creates a .java class and a .txt report describing your IMS source.
4. Compile the .java class output by Eclipse into a .jar file (such as mymodel.jar) and place it in the Assure DQ plug-ins directory.

   To determine the path of the plug-ins directory, look for the PLUGINS_DIR property in the Assure DQ IA.properties file.

   The properties file is located in <install_folder>/Infogix/config /<config_name>/IA.
5. If the PLUGINS_DIR property is blank or you want to change it, specify the full path of a directory where controls developers can upload plug-ins for use with Assure DQ.

   The Assure DQ application server must be able to access this directory.
6. Redeploy Assure DQ.
7. Provide the following information to the controls developer who will set up the IMS database layout in the Infogix Asssure user interface:
   - IMS database host name or number
   - Port number
   - Metadata URL
   - Options (such as the datastore name)
   - Database user ID and password
   - SQL query

     For guidelines on formatting SQL statements, see the IBM documentation on “Writing SQL queries to access an IMS database with the IMS Universal JDBC driver” at http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/topic/com.ibm.ims11.doc.apg/ims_odbjdbccomparehierandreldbs.htm

8. See the Database Connections topic in the Online Help for more information on how to set up the database layout in the user interface.

Changing the Password Encryption Level

During installation, if the system administrator chooses to encrypt passwords in the properties files on the server and client, the system uses 56 bit PBE-DES encryption by default. If you prefer to switch to AES 256 bit encryption post-installation, complete the procedures that follow.

AES 256 Bit Encryption on the Server

Complete the procedure below to switch to AES 256 bit encryption for passwords in the installation properties files:

1. Open the advanced.appserver.properties file in <install_folder>/Infogix/config/<config_name> and change the DEFAULT_ENCRYPTION_LEVEL property to AES.
2. Run the crypt-properties.bat or crypt-properties.sh script with the AES parameter.

   On Windows, enter a command similar to the following example:

   ```
   <install_folder>/Infogix/bin >
   crypt-properties.bat -t AES
   ```

   On UNIX/Linux, enter a command similar to the following example:

   ```
   <install_folder>\Infogix\bin >
   ./crypt-properties.sh -t AES
   ```
3. Redeploy Assure DQ.

AES 256 Bit Encryption on the Client

Complete the procedure below to switch the password in the client properties file to AES 256 bit encryption:

1. Run the crypt-properties command with the AES parameter.

   Windows:

   ```
   > crypt-properties.bat –c <configname> -t AES
   ```

   UNIX/Linux or z/OS®:

   ```
   > ./crypt-properties.sh –c <configname> -t AES
   ```

   where <configname> is the name of your configuration, such as test. Do not specify -c <configname> to encrypt passwords for the default configuration.
2. Open <install_folder>/InfogixClient/bin. Run the deploy client program by using a command such as the one below:

   ```
   deploy-client.bat –c <configname> IA
   ```

Changing the Database Commit Interval

Normally, when a database is an input data source for Assure DQ controls, the database keeps any read locks on the data read until the entire result set is processed. However, for large databases, you may want to specify a finite number of rows to read and then commit. This allows the database to release accumulated read locks periodically.

If you configure your system to offer the database commit interval option, rules writers can specify the number of rows to read before releasing database read locks. The option will appear on the Database Layout Details tab in the user interface. To enable the database commit interval option, complete the following steps:

1. Create or edit <install_folder>/Infogix/config/<cfgname>/IA/override.properties Where <cfgname> is the configuration name of the installation, or “default” if a configuration name was not specified.
2. Specify db.ALLOW_READ_COMMIT_INTERVAL parameter with a value of true.
3. Run the update-config script located in <install_folder> /Infogix/bin.

   Allow five minutes for your changes to take effect.

Overriding Default Filenames for Reports

When the generateReports utility and the archiveReports utility generate results and reports, each report or result catalog file is labeled with a unique process history ID generated by the system. The filename also includes the control entity and control point name, and the cycle and run number, if applicable.

The table below shows the default filenames.

Report or Result	Default Filename
Control Report, Recap Report, Recon Task Report, User Report	`{Process History ID}{Cycle}{Run}{Report ID}{Control Entity Name}{Control Point Name}{Report Name}{Report Type}.{File Type}`
Matched Set Audit Report	`MatchSetArchiveRpt_{Control Point Name}_{Report Name}_P{Process History ID}_C{Cycle}_R{Run}.{File Type}`
Result Catalog	`{Process History ID}{Control Entity Name}.{Control Point Name}.ResultCatalog.{File Type}`

Optionally, you can override the filenames to conform to your own naming standards. If you want to overwrite (replace) previously generated or archived reports, override the default names with non-unique names.

To override the default filenames, edit the report.properties file and redeploy Assure DQ. Complete the following steps:

1. Create or edit
<install_folder>/Infogix/config/<cfgname>/IA/override.properties
Where <cfgname> is the configuration name of the installation, or "default" if a configuration name was not specified.

2. Specify the properties to customize the filenames based on your naming conventions.

Property Name	Purpose
ARCHIVE_USER_REPORT_FILE_NAME_FMT	User Report
ARCHIVE_RECAP_REPORT_FILE_NAME_FMT	Recap Report
ARCHIVE_RECON_TASK_REPORT_FILE_NAME_FMT	Reconciliation Task Report
ARCHIVE_CONTROL_DETAIL_REPORT_FILE_NAME_FMT	Control Report
ARCHIVE_AUDIT_REPORT_FILE_NAME_FMT	Matched Set Audit Report
ARCHIVE_EXCEPTION_CATALOG_REPORT_FILE_NAME_FMT	Exception Catalog Report
ARCHIVE_DECONTROL_REPORT_FILE_NAME_FMT	Data Quality Control Report
ARCHIVE_DERECAP_REPORT_FILE_NAME_FMT	Data Quality Recap Report
ARCHIVE_INVALID_VALUES_REPORT_FILE_NAME_FMT	Data Quality Invalid Values Report

See the table below for a list of available variables and page 72 for syntax examples. Filenames can also include text strings, such as report names.

Filename Variables	Description
CE	The name of the control entity that generated the report or results.
CP	The name of the control point that generated the report or results.
CYCLE	The cycle number of the control run.
RUN	The run number.

Filename Variables	Description
PHIST	A unique ID generated by the system for control runs. Use this variable for control entities that do not have cycle and run numbers to uniquely identify the control run and correlate reports and result catalogs.
REPORT_ID	A unique ID generated by the system for reports. Not available for result catalogs. Use this variable if you want to create unique filenames for multiple reports generated by the same control run. For example, a single control run may generate multiple Control Reports, Recon Task Reports, and Match Set Audit Reports.
REPORT_NAME	Defaults to the name of the control point that generated the report or results. The rules writer can specify a fixed or variable name of up to 40 characters. Variable names are substituted at runtime.
REPORT_TYPE	The contents of the file, such as EZRecap, ReconTask, MatchSetAudit, ResultCatalog, User, or Control.
RERUN	Indicates whether the report or results were generated by rerunning a control point. "R" indicates a rerun. Otherwise, the indicator is blank.

3. Save and close the properties file.
4. After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin.

   Allow five minutes for your changes to take effect.

Syntax Examples

Suppose you want to create unique filenames for Control Reports generated by Detail control entities. If users call these daily control reports, you might decide to prefix the file name with DailyControlReport.

```
ARCHIVE_CONTROL_DETAIL_REPORT_FILE_NAME_FMT=
DailyControlReport_{CE}_{CP}_{CYCLE}_{RUN}_{REPORT_ID}
```

Suppose you want to create unique filenames for reports generated by Detail and Match Data control entities that lack cycle and run numbers. To do this, include the PHIST (Process History) variable in the filename. The Process History variable is a unique ID generated by the system.

```
ARCHIVE_CONTROL_DETAIL_REPORT_FILE_NAME_FMT=
DailyControlReport_{CE}_{CP}_{PHIST}
```

Finally, suppose you want to keep the Control Report for only the most recent run. Create a non-unique filename similar to the example below by omitting the PHIST variable.

```
ARCHIVE_CONTROL_DETAIL_REPORT_FILE_NAME_FMT=
DailyControlReport_{CE}_{CP}
```

7

Integration

You can configure Assure DQ to communicate with ER, ACR/Connector, Insight, Data360 DQ+, and Data360 Govern. To facilitate system integration testing, you can apply an offset to the Assure DQ internal clock. This eliminates the need to reset the system clock, which could potentially disrupt other applications running on the same server.

Integrating with ER

To configure Assure DQ to communicate with ER, customize the following properties in the IA.properties file located in <install_folder>/Infogix/config/<config_name>/IA.

Property	Description
ENABLE_ERGATEWAY	Set to true to enable integration with ER.
ERGATEWAY_INVOKER	Accept the default setting of httpinvoker.
ERGATEWAY_HTTP_ CONTEXT_ROOT	Specify the context root value for ER. The value must match that of the solution.context.root property for the ER instance.
ERGATEWAY_HTTP_ HOST_NAME	If ER is on its own JVM, you must edit this value to point to the ER instance. This property identifies the hostname of the server that hosts the ER application. By default, the system uses the value for the HOST_NAME property in the appserver.properties file.
ERGATEWAY_HTTP_ PORT	If ER is on its own JVM, you must edit this value to point to the ER instance. This property identifies the port on the host above where the ER gateway listens for an http request. By default, the system uses the value for the HTTP_ PORT_NUMBER property in the appserver.properties file.

Property	Description
ERGATEWAY_HTTP_SCHEME	Specify whether to connect to the ER gateway using http (default) or https protocol.
ERGATEWAY_HTTP_USER_NAME	If ER is on its own JVM, you must edit this value to point to the ER instance. This property identifies an Assure DQ user with authority to log in to the ER gateway. By default, the system uses the value for the SECURITY_USER_ID property in the appserver.properties file.
ERGATEWAY_HTTP_USER_PASSWORD	If ER is on its own JVM, you must edit this value to point to the ER instance. This property identifies the password for the Assure DQ user, above. By default, the system uses the value for the SECURITY_USER_PASSWORD property in the appserver.properties file.
ERGATEWAY_LOCALINVOKER_RUNAS_USERNAME	This property identifies a user name for Assure DQ, used if Assure DQ locally invokes ER. By default, the system uses the value for the SECURITY_USER_ID property in the appserver.properties file.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Integrating with ACR/Connector

To configure Assure DQ to communicate with ACR/Connector, you will need to customize the following properties in the IA.properties file located in <install_folder>/Infogix/config/<config_name>/IA.

Property	Description
IIA_HOST	The hostname of the machine where ACR/Connector runs.
IIA_PORT	The port on the above machine where ACR/Connector listens for requests.

Property	Description
XPG_GATEWAY_ ENABLED	Set to true to enable ACR/Connector support.

XPG_LIST_PLATFORMS_ DYNAMIC	Set to true to have Assure DQ dynamically query the list of platforms that are available in ACR/Connector.
	Set to false if you prefer to specify a list of platform IDs and names in the XP Gateway properties file. Use the following format:
	platform.*platformNumber*=*platform name*
	Examples:
	`platform.1=My Node Name`
	`platform.2=XYZ`

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Integrating with Insight

To configure Assure DQ to communicate with Insight, customize the following properties in the IA.properties file located in <install_folder>/Infogix/config/<config_name>/IA.

Insight Gateway Properties

Property	Description
INSIGHT_GATEWAY_ ENABLED	Set to **true** to enable integration with Insight.
INSIGHT_GATEWAY_ HTTP_ CONTEXT_ROOT	Specify the context root value for Insight. The value must match that of the solution.context.root property for the Insight instance.

Property	Description
INSIGHT_GATEWAY_ HTTP_ HOST_NAME	If Insight is on its own JVM, you must edit this value to point to the Insight instance. This property identifies the hostname of the server that hosts the Insight application. By default, the system uses the value for the HOST_NAME property in the appserver.properties file.
INSIGHT_GATEWAY_ HTTP_ PORT	If Insight is on its own JVM, you must edit this value to point to the Insight instance. This property identifies the port on the host above where the Insight gateway listens for an http request. By default, the system uses the value for the HTTP_ PORT_NUMBER property in the appserver.properties file.
INSIGHT_GATEWAY_ HTTP_ SCHEME	Specify whether to connect to the Insight gateway using http (default) or https protocol.
INSIGHT_GATEWAY_ HTTP_ USER_NAME	If Insight is on its own JVM, you must edit this value to point to the Insight instance. Specify a username for Assure DQ with authority to log in to the Insight gateway. By default, the system uses the value for the SECURITY_USER_ID property in the appserver.properties file.
INSIGHT_GATEWAY_ HTTP_USER_PASSWORD	If Insight is on its own JVM, you must edit this value to point to the Insight instance. This property identifies the password for the Assure DQ user, above. By default, the system uses the value for the SECURITY_USER_PASSWORD property in the appserver.properties file.
PLATFORM_ID	This property identifies the Assure DQ instance. This is usually the hostname of the machine where Assure DQ runs.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Sending Control Point Results to Insight

You can use the control run sender utility to manually send results to Insight for an Assure DQ control point execution. This is useful for recovery if communication is temporarily disrupted between Assure DQ and Insight.

The ControlRunSender utility is in <install_folder>/Infogix/server-util/<config_name>/IA.

Enter ControlRunSender.bat (for Windows) or ControlRunSender.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if the username and password are specified in the application server properties file, you do not have to specify them as parameters.

ControlRunSender Parameters	Description
-catalog	Specify the catalog ID of the result catalog you want to send to Insight. To determine a catalog ID, log in to the user interface and select Results > By Control Point. Select a result of interest. The catalog ID appears on the Summary tab for the result. The result catalog ID is also returned to a Web Service caller in the response.
-username	Specify the username to use to connect to an http server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-password	Specify the password to use to connect to an http server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.

Integrating with Data360 Govern

To configure Assure DQ to communicate with Data360 Govern, customize the following properties in the IA.properties file located in <install_folder>/Infogix/config/<config_name>/IA.

Property	Description
GOVERN_INTEGRATION_ENABLED	Set to true to enable integration with Data360 Govern.
GOVERN_INTEGRATION_COMPLIANCE_ONLY	Specify true if only those controls marked "For Compliance Report" should be sent to Data360 Govern. Specify false to send information for all controls to Data360 Govern.
GOVERN_SERVER_URL	Specify the http/https URL for Assure DQ to use to communicate with Data360 Govern.
GOVERN_API_KEY	Specify the API key of a Data360 Govern user account through which Assure DQ will send its information.
GOVERN_API_SECRET	Specify the API secret of a Data360 Govern user account through which Assure DQ will send its information.
GOVERN_ROOT_ASSURE_SERVER_UID	Specify the Asset unique identifier (UID) of an Assure DQ Server asset under which Assure DQ will supply all of its control point, report and field assets and their relationships. If Data360 Govern does not yet have a definition of the Assure artifact types, you may have to add this later.
GOVERN_UPDATE_ON_RULE_CHANGE	Specify true to have Assure DQ send updates about control points, fields and reports as they occur. Specify false to only send updates when the governDefs utility is manually run.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Establish Assure Artifact Types in Data360 Govern

Data360 Govern may or may not have up-to-date knowledge of the Assure DQ artifact and relationship configuration. To perform an initial assessment of artifact type information in Data360 Govern, use the Govern Types utility. The utility can also be used to create the necessary artifact types in Govern. Note that a Data360 Govern user cannot create the Assure DQ Server artifact (see GOVERN_ROOT_ASSURE_SERVER_UID above) until the artifact type exists.

The governTypes utility is in <install_folder>/Infogix/server-util/<
config_name>/IA

Enter governTypes.bat (for Windows) or governTypes.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if the username and password are specified in the application server properties file, you do not have to specify them as parameters.

governDefs Parameters	Description
-username	Specify the username to use to connect to an http server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-password	Specify the password to use to connect to an http server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.
-c	Create the Assure DQ artifact types and relationships in Data360 Govern. If omitted, only an assessment of what artifact types and relationships exist is performed.

If the utility reports *** Not Defined *** for any artifact type, relationship predicate, or relationship, run the utility again with the -c option to have Assure DQ create the missing type information in Data360 Govern.

Synchronizing All Assure Artifacts with Data360 Govern

You can use the Govern Definitions utility to manually synchronize Assure DQ definitions with Data360 Govern. This utility synchronizes all definitions currently in Assure DQ and establishes them in Data360 Govern. After verifying the artifact types, run the initial load of assets using this utility.

The governDefs utility is in <install_folder>/Infogix/server-util/<
config_name>/IA

Enter governDefs.bat (for Windows) or governDefs.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if the username and password are specified in the application server properties file, you do not have to specify them as parameters.

governDefs Parameters	Description
-username	Specify the username to use to connect to an http server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-password	Specify the password to use to connect to an http server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.

Synchronizing Changed Assure Artifacts with Data360 Govern

You can use the Update Govern Definitions utility to manually push Assure definitions that have changed to Data360 Govern. This utility synchronizes those definitions changed in Assure since the last run of synchronization with Data360 Govern.

The governUpdates utility is in <install_folder>/Infogix/server-util/<
config_name>/IA

Enter governUpdates.bat (for Windows) or governUpdates.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if the username and password are specified in the application server properties file, you do not have to specify them as parameters.

governDefs Parameters	Description
-username	Specify the username to use to connect to an http server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-password	Specify the password to use to connect to an http server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.

Synchronizing Assure Executions Artifacts with Data360 Govern

You can use the Govern Executions utility to manually push Assure control point execution counts to Data360 Govern. This utility synchronizes the execution counts data changed in Assure since the last run of executions synchronization with Data360 Govern. In an installation using the internal scheduler, this runs once a day, after the shared retention process has updated execution counts for all control points.

The governExecutions utility is in <install_folder>/Infogix/server-util/< config_name>/IA

Enter governExecutions.bat (for Windows) or governExecutions.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if the username and password are specified in the application server properties file, you do not have to specify them as parameters.

governDefs Parameters	Description
-username	Specify the username to use to connect to an http server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.

governDefs Parameters	Description
-password	Specify the password to use to connect to an http server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.

Delete Assure Artifacts in Data360 Govern

If you no longer wish to have the Assure DQ artifact information in Data360 Govern, run the Clean Govern Definitions utility. This utility will delete all of the control points, control reports, and control fields that were established under the configured Assure DQ Server artifact.

The cleanGovernDefs utility is in <install_folder>/Infogix/server-util/<config_name>/IA

Enter cleanGovernDefs.bat (for Windows) or cleanGovernDefs.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if the username and password are specified in the application server properties file, you do not have to specify them as parameters.

governDefs Parameters	Description
-username	Specify the username to use to connect to an http server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-password	Specify the password to use to connect to an http server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.

Integrating with Data360 DQ+

To configure Assure DQ to communicate with Data360 DQ+, customize the following properties in the IA.properties file located in <install_folder>/Infogix/config/<config_name>/IA.

Property	Description
CAFE_GATEWAY_ENABLED	Set to true to enable integration with Data360 DQ+.
CAFE_DEPLOYMENT_MODE	Specify enterprise if Data360 DQ+ is installed within your enterprise. Specify cloud if Data360 DQ+ is running in the cloud.
CAFE_URL	Specify the http/https URL for Assure DQ to use to communicate with Data360 DQ+.
CAFE_USER_NAME	Specify the user ID for Assure DQ to use to authenticate with Data360 DQ+.
CAFE_USER_PASSWORD	Specify the password for Assure DQ to use to authenticate with Data360ER DQ+.
CAFE_ENVIRONMENT	Specify the name of an environment defined in Cafe. Cafe supports multiple Assure installations using a single Cafe installation, where the Assure installations may be for Development, Test, and Production.
CAFE_SOLUTION_UNIQUE_ID	Specify an ID that identifies this Assure DQ instance. For example, if you deploy separate Assure systems for different lines of business, and they will both use the same Cafe system, use different unique IDs for each Assure line of business installation.
CAFE_PUSH_DEFINITIONS	Specify true to cause Assure DQ to push definition information to Cafe. Typically, Assure installations where rules are developed will push definitions to Cafe, and those Assure installations where rules are promoted by import (such as Production) do not push definitions to Cafe.

Property	Description
READ_TIMEOUT_DEFAULT	Specify the default read timeout to set for the connection to Cafe in seconds.
READ_TIMEOUT_PUSH_DATA	Specify the read timeout to set for the connection to push data to Cafe in seconds.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Pushing Assure Definitions to Data360 DQ+

You can use the Cafe Definitions utility to manually push Assure definitions to Data360 DQ+. This utility recreates all definitions currently in Assure DQ and pushes them to Data360 DQ+.

The cafeDefs utility is in <install_folder>/Infogix/server-util/<

config_name>/IA

Enter cafeDefs.bat (for Windows) or cafeDefs.sh (for UNIX or Linux), followed by the appropriate parameters from the table below. Note that if the username and password are specified in the application server properties file, you do not have to specify them as parameters.

cafeDefs Parameters	Description
-username	Specify the username to use to connect to an http server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-password	Specify the password to use to connect to an http server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.

System Integration Testing

To test scheduled controls and system utilities, you can apply an offset to the Assure DQ internal clock. This capability is useful for system integration testing and to verify that control points or system utilities execute according to schedule.

To test ER in conjunction with Assure DQ, you can “freeze” the internal clocks in both systems. This permits ER testers to simulate case resolution while stopping the flow of exceptions from Assure DQ.

Freezing the Internal Clock

For testing purposes, you can apply an offset to the Assure DQ internal clock. This eliminates the need to reset the system clock, which could potentially disrupt other applications running on the same server. For example, when testing ER in conjunction with Assure DQ, you can freeze the system clock to prevent control points from generating exceptions and passing them on to ER.

Do not attempt to change or freeze the internal clock in a production environment. To change the time on the internal clock in a test environment, complete the following steps:

1. Find out the location of the configuration files for the Assure DQ Web application.
   The location is specified by the CONFIG_HOME parameter in the appserver.properties file, located in <install_folder>/infogix /config/<config_name>.
2. Go to the directory containing the configuration files and open kernel.properties.
   Use a text editor such as WordPad or vi.
3. Change the INTERNAL_CLOCK_ENABLE parameter to true.
   ```
   INTERNAL_CLOCK_Enable=true
   ```

4. If you want to “freeze” the clock, change INTERNAL_CLOCK_ FIXED_TIME to true and specify the date and time in MM/dd/yyyy HH:mm:ss format.
   The example, below, freezes the date and time to 8:25:31 on February 1, 2008:
   ```
   INTERNAL_CLOCK_FIXED_TIME=true
   INTERNAL_CLOCK_FIXED_TIME_VALUE=02/01/2008 08:25:31
   ```
5. If you prefer to reset the internal clock to a past or future time, leave INTERNAL_CLOCK_ FIXED_TIME set to false and uncomment INTERNAL_CLOCK_OFFSET_TIME_VALUE.
   Specify an offset time value in only one of the following increments: days (d), hours (h), minutes (m), or seconds (s). If you do not enter a d, h, m, or s, the system interprets the time as milliseconds. Use a leading negative sign if you want to specify a time in the past.
   The example, below, resets the internal clock to 500 days in the past:
   ```
   INTERNAL_CLOCK_ENABLE=true
   INTERNAL_CLOCK_FIXED_TIME=false
   INTERNAL_CLOCK_OFFSET_TIME_VALUE=-500d
   ```
6. Save and close the properties file.
7. Your changes will take effect in about five minutes.
8. When testing is complete, open the file and change the INTERNAL_CLOCK_ENABLE property back to false.

8

Result Actions

Result actions, or action rules, specify the system response when controls produce a specified type of result. The installation procedure installs a default result action, which the system executes based on the severity threshold, and the override settings for user-defined result actions.

A system schedule calendar, the Infogix Action Rule Processing Schedule, specifies when and how often the system runs action rule processing.

To implement a result action, you must assign at least one action type: an alert or a log action. Alerts can be inbox alerts, email alerts, or pager alerts. Log actions write a message to the system action log.

This chapter covers maintenance and configuration tasks that pertain to result actions and to the action types that you can assign to result actions.

This chapter includes the following topics:

Changing Default Action Rule Severity Threshold

The installation procedure installs a default result action. The implementation of this default action is based on the severity threshold. The default threshold is W, which applies the rule to results at a severity level of warning or higher.

The system applies the default result action for any generated result that is not covered by a user-defined result action. The system also applies this result action to results that have an associated result action rule that does not override the default rule.

You can change the severity level for the default result action rule. Open the exm.properties file located in <install_folder>/igx-data/<config_name>/IA/config and edit the property below.

Property	Description
DEFAULT_ACTION_ SEVERITY_THRESHOLD	By default, the system applies this action rule to results at a severity level of warning or higher. The following options are available: I applies the rule to results for all severity levels: informational, warning, error, and fatal results. W applies the rule to warnings, errors, and fatal results. E applies the rule to errors and fatal results. F applies the rule to fatal results.

After updating the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Changing the Action Rule Processing Schedule

Assure DQ is delivered with a maintenance calendar that automatically controls action rule processing: Infogix Action Rule Processing Schedule. This action rule schedule specifies when and how often to notify users to alert them to control processing results. This schedule controls the processing for all defined actions rules, including inbox alerts, email alerts, pager alerts, and log actions.

Action rule processing typically runs regularly throughout every processing day. The default settings process action rules seven days a week, every five minutes, beginning at midnight.

To change this schedule to satisfy your company's business requirements, complete the following steps:

1. Log in to the Assure DQ user interface as an administrator, integrity rule administrator, or superuser.
2. Select Rules > Calendars.

   The system displays the Manage Calendars window. The top pane lists all calendars.

3. Select Infogix Action Rule Processing Schedule and then click Edit Events.
4. Select generateEvents, the default event for this calendar.
   The bottom pane displays the settings for this event.
5. You can modify the following settings:
   - The name for the event
   - The start date
   - The start time
   - The end time, if this is not a recurring event
   - Whether the event occurs monthly or each week
   - The days on which the event occurs, if applicable
   - The number of hours, minutes, and seconds to elapse before the event reoccurs
6. Apply each change, click OK, and then save your changes.

Configuring User Preferences (Including Email)

The system administrator can configure email and pager alert preferences for individual users with the updateUserPreferences utility. This is useful if a particular user cannot log in to the user interface to set their own preferences. The user must exist in the user information directory specified for your Assure DQ installation.

Users who can log in to the user interface can set or override their email and pager preferences by selecting System > Preferences.

To run the utility, go to <install_folder>/Infogix/server-util /<config_name>/IA. Execute updateUserPreferences.bat (for Windows) or updateUserPreferences.sh (for UNIX or Linux), followed by the appropriate parameters from the table that follows. Note that if you specified your username and password in the application server properties file, you do not have to specify them as parameters.

Update User Preferences Parameters	Description
-prefUserId	The user ID of the user to configure. The user must exist in the user information directory specified for your Assure DQ installation.
-alertExpires	This option controls the number of days alerts are retained in the user's inbox in Assure DQ. Alerts are automatically deleted after the expiration period. This setting overrides the setting for a specific alert.
-emailAlert	Specify Yes to send email alerts to this user in addition to inbox alerts. Specify No to send inbox alerts only. The default setting is determined by an application server property configured at installation time.
-fontSize	This option controls the size of text that displays in the user interface. The options are small, medium, or large. This setting does not affect the size of text in online Help.
-itemsPerPage	This option limits the number of items that display on a page in the user interface. You can choose 25, 50, 100, 250, 500, 750, or 1000.
-pagerAlert	Specify Yes to send pager alerts to this user in addition to inbox alerts. Specify No to send inbox alerts only. The default setting for this option is No.
-pagerNumber	If you enabled the pagerAlert option, specify a pager address in email format, such as bsmith@infogix.com.
-username	Specify the username to use to connect to an http server. Optional.
-password	Specify the password to use to connect to an http server. Optional.
-proxyusername	Specify the username to use to connect to an http proxy server. Optional.
-proxypassword	Specify the password to use to connect to an http proxy server. Optional.
-?	Describe the command line arguments.

To enable email alerts for user bsmith, enter a command similar to one of the following examples:

Windows:

```
updateUserPreferences -prefUserId bsmith -emailAlert Yes
```

UNIX/Linux:

```
./updateUserPreferences.sh -prefUserId bsmith
 -emailAlert Yes
```

Configuring Email Alerts

The Assure DQ Web application references a configuration file named alert.properties to determine the format and content of email alerts. Email alerts notify users when control runs generate results of interest to them. Alerts include hyperlinks to the user's Assure DQ inbox or to individual results. You can change the following properties in the alert properties file:

- The sender that appears in the From field for all email alerts. Defaults to Infogix@YourCompany.com.
- Lower and upper limits that control the result information that email alerts contain, based on how many results a control run generates. By default, runs that generate up to 10 results include result summaries and links to each result. Runs that generate more than 10 results include up to 100 subject lines and a link to the user's inbox.
- The subject line for the email alert. Defaults to "You have *n* new alerts in your inbox."

Changing the Default Email Properties

To change the default email properties, edit the alert.properties file and restart the application. Complete the following steps:

1. Go to <install_folder>/Infogix/igx-data/<config_name>/IA/config/ and open alert.properties.

   Use a text editor such as WordPad or vi.
2. Edit the properties to customize the format and content of email alerts.

   See the table on page 96 for descriptions of the properties and how to edit them.
3. After you update the properties file, run the update-config script located in <install_folder>/Infogix/bin. Allow five minutes for your changes to take effect.

Sample Limit 1 Style Email

By default, control runs that generate up to 10 results produce an email summarizing each result, with View Alert links to result details. A sample of this type of email is shown below.

Control Entity: Month End Accounting
Control Point: General_Ledger_Summary
Description: Balance Sheet totals are not equal to General Ledger Summary totals

Name	Value
BS and GLS Are Not Equal	
Balance Sheet Cash Total	$1,200.00
Balance Sheet Accts Payable Total	$900.00
Balance Sheet Owner Equity Total	$300.00
General Ledger Cash Total	$1,200.00
General Ledger Accts Payable Total	$1,000.00
General Ledger Owner Equity Total	$300.00

View alert

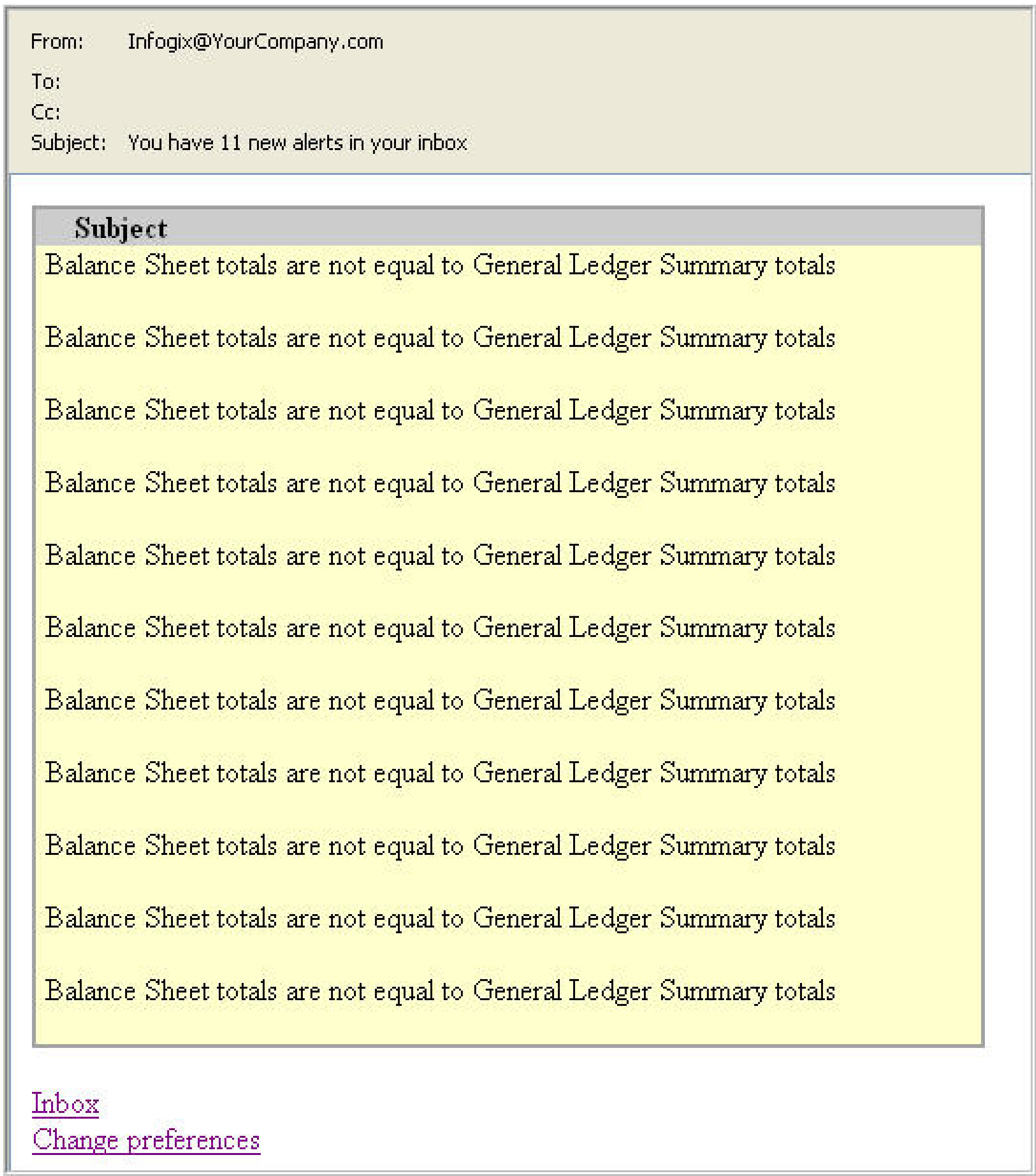
If the email recipient is logged in to Assure DQ, clicking a View Alert link displays more result details in the user interface. Otherwise, the login screen displays when the user clicks the link. The Change Preferences link enables users to change their email preferences to stop receiving emails.

The subject line of the email depends on how many results the email contains. If there is only one result, the subject line matches the subject of the email alert. If there are multiple results, the subject line says, “You have *n* new alerts in your inbox.” You can change this wording by editing the EMAIL_ALERT_SUBJECT property in the alert properties file.

To increase or decrease the limit on summarized results to include in emails, edit the EMAIL_ALERT_LIMIT1 property in the alert properties file.

Sample Limit 2 Style Email

By default, control runs that generate more than the limit 1 number of results produce an email listing only the subjects of up to 100 results. The email also includes a link to the user's Assure DQ inbox. A sample of this type of email is shown below.



From: Infogix@YourCompany.com
To:
Cc:
Subject: You have 11 new alerts in your inbox

Subject
Balance Sheet totals are not equal to General Ledger Summary totals
Balance Sheet totals are not equal to General Ledger Summary totals
Balance Sheet totals are not equal to General Ledger Summary totals
Balance Sheet totals are not equal to General Ledger Summary totals
Balance Sheet totals are not equal to General Ledger Summary totals
Balance Sheet totals are not equal to General Ledger Summary totals
Balance Sheet totals are not equal to General Ledger Summary totals
Balance Sheet totals are not equal to General Ledger Summary totals
Balance Sheet totals are not equal to General Ledger Summary totals
Balance Sheet totals are not equal to General Ledger Summary totals
Balance Sheet totals are not equal to General Ledger Summary totals

Inbox
Change preferences

If the email recipient is logged in to Assure DQ, clicking the Inbox link displays the user's Assure DQ inbox. Otherwise, the login screen displays when the user clicks the link. The Change Preferences link enables users to change their email preferences to stop receiving emails.

By default, the subject line of the email says, "You have *n* new alerts in your inbox." You can change this wording by editing the EMAIL_ALERT_SUBJECT property in the alert properties file.

To increase or decrease the limit on the number of subject lines to include in emails, edit the EMAIL_ALERT_LIMIT2 property in the alert properties file.

Email Properties

The table that follows describes the email properties and how to edit them.

Email Properties	Description
DEFAULT_ALERT_ SENDER	Specifies the sender to list in the From field for all email alerts. Substitute the sender you prefer for EMAIL_FROM_ ADDRESS. For example, you could change @EMAIL_FROM_ADDRESS@ to @Assure DQ@. If you don't edit this parameter, the sender defaults to Infogix@YourCompany.com.
EMAIL_ALERT_LIMIT1	Specifies the maximum number of result summaries and links to include in email alerts. When a control point run generates up to this number of results, the email will include a summary of each result and a link to the result in the user interface. Defaults to 10.
EMAIL_ALERT_LIMIT2	Specifies the maximum number of result subject lines to include in email alerts. When a control point run generates more results than limit 1, above, emails will include subject lines only for each result, up to the limit 2 maximum. Links to the user's inbox and preferences will appear at the end of the email. Defaults to 100.

Email Properties	Description
EMAIL_ALERT_ SUBJECT	Specifies the subject line for email alerts. Defaults to “You have {0} new alerts in your inbox,” where {0} is a variable corresponding to the number of new alerts. If there is only one result, the subject line of the email matches the subject line of the result.

Setting Up Log Actions

Log actions are an optional feature of Assure DQ. When a control point generates a result, the system can write a user-specified message to an action log. The message indicates the severity of the result. The message can also include additional information, such as a description of the result, the name of the control entity and control point that generated the result, and a hyperlink to the result in the user interface.

An administrator sets up log actions and assigns them to log categories in the user interface. The administrator defines the log categories.

Log categories serve two purposes:

- To label log messages in the log, based on which control generated them, the department responsible for resolving them, or other criteria.
- To direct log messages to different log files by category (optional).

By default, the system writes all action log messages to a single file, named log-action.log. The file is in <install_folder>/Infogix/logs/config.name /IA.

To set up a log action in the user interface, complete the following steps:

1. Navigate to Rules > Actions > New Action.
2. In the bottom pane, enter a name and description for the action on the Details tab.
3. On the Apply To tab, click Add.
   The Add Control Point and/or Result Template window displays.

4. Select a result template and/or control point to trigger the action.

   When the selected control point generates a result that uses the selected result template, the system performs the log action you specify. If you select a control point only, the system performs the log action when the control point produces any result. If you select a result template only, the system performs the log action each time any control point generates a result that uses the result template.
5. Click OK to return to the Apply To tab.
6. To associate the action with additional result templates or control points, repeat step 3 through step 5, above.
7. On the Actions tab, click Add Log.

   The Add Log window displays.
8. Specify a Log Category.
9. Optionally, change the Log Level to a specific severity, ranging from Debug (least severe) to Fatal (most severe).

   The log level defaults to Result Severity. If you accept the default, the log message shows the severity of the result that triggered the action.
10. Enter the message you want the system to write to the action log.

    In addition to your own text, you can include any or all of the following items in the log message:

    - **Result Subject**—A description of the result that triggered the log action, as shown on the Subject tab for the associated result template.
    - **Control Entity Name**—The name of the control entity that triggered the log action.
    - **Control Point Name**—The name of the control point that triggered the log action.
    - **Result Link**—A hyperlink to the result that triggered the log action.

Modifying the Action Logging Process

You must edit the log4j configuration file if you want to change the name and path of the log file, or write messages to different log files based on log category. The default configuration is usable without modification if you are satisfied with a single action log file in the default location.

To modify the default configuration, be sure to follow the appropriate procedure for your installation (JBoss or WebSphere).

Modifying Action Logging under JBoss

This section explains how to modify action logging under JBoss. If Assure DQ runs under WebSphere at your site, see "Modifying Action Logging under WebSphere" on page 102.

By default, the system writes all action log messages to a file named log-action.log. The file is in <install_folder>/Infogix/logs /<config_name>/IA.

Action Log Name and Location

To change the name or location of the action log, complete the following steps:

1. Go to the config directory for your Assure DQ server installation and open log4j.xml with a text editor such as WordPad or vi.

   To find out the location of the config directory, open the appserver.properties file in <install_folder>/Infogix /config/<config_name>. The CONFIG_HOME parameter specifies the location of the config directory.
2. In log4j.xml, notice that the File parameter under the FINDING appender specifies the path and name of the log file, as shown below:

```
<!-- A time/date based rolling appender to log Assure findings -->
       <appender name="FINDING"
class="org.jboss.logging.appender.RollingFileAppender">
       <errorHandler
class="org.jboss.logging.util.OnlyOnceErrorHandler"/>
       <param name="File"
value="${jboss.server.home.dir}/log/log-action.log"/>
                .
                .
                .
     </appender>
```

3. To change the location or name of the log file, change the value of the File parameter, above, and save your changes.
4. Stop and restart the Assure DQ server for your changes to take effect.

Directing Messages to Multiple Log Files

This section describes how to configure the system to write action log messages to different log files based on log categories specified in the user interface. Review the example below and then complete the procedure for "Writing Messages to Different Logs Under JBoss" on page 101.

Example

Suppose you assign log actions to either MyFirstCategory or MySecondCategory. You want to direct MyFirstCategory messages to a FINDING1 log in a file named log-action1.log. MySecondCategory messages go to a FINDING2 log in a file named log-action2.log. To make this change, edit the log4j.xml file.

Specify the log action categories and the destination logs for messages in each category, as shown below:

```
<!-- route the log action category to the logaction appender -->
<category name="logaction.com.infogix">
  <appender-ref ref="FINDING1"/>
</category>
<!-- route the log action category to the logaction appender -->
<category name="logaction.com.infogix.MyFirstCategory">
  <appender-ref ref="FINDING1"/>
</category>
<!-- route the log action category to the logaction appender -->
<category name="logaction.com.infogix.MySecondCategory">
  <appender-ref ref="FINDING2"/>
</category>
```

Add appender specifications for the FINDING1 and FINDING2 logs. In this example, direct FINDING1 logging to log-action1.log; direct FINDING2 logging to log-action2.log.

```
<!-- A time/date based rolling appender to log Assure findings -->
    <appender name="FINDING1"
class="org.jboss.logging.appender.RollingFileAppender">
       <errorHandler
class="org.jboss.logging.util.OnlyOnceErrorHandler"/>
       <param name="File"
value="${jboss.server.home.dir}/log/log-action1.log"/>
            .
            .
            .
```

```
    </appender>
    <appender name="FINDING2"
class="org.jboss.logging.appender.RollingFileAppender">
       <errorHandler
class="org.jboss.logging.util.OnlyOnceErrorHandler"/>
       <param name="File"
value="${jboss.server.home.dir}/log/log-action2.log"/>
            .
            .
    </appender>
```

Writing Messages to Different Logs Under JBoss

To write log messages to different log files based on log categories, complete the following steps:

1. Go to the config directory for your Assure DQ server installation and open log4j.xml with a text editor such as WordPad or vi.

   To find out the location of the config directory, open the appserver.properties file in <install_folder>/Infogix /config/<config_name>. The CONFIG_HOME parameter specifies the location of the config directory.
2. In log4j.xml, use the category name parameter to specify each user-defined category.

   The system appends the category name to the default log4j category, logaction.com.infogix, to define the full log4j category.
3. Use the appender-ref parameter to associate messages in each category with a log.
4. Use the appender name parameter to direct messages from each log to a log file.
5. Save your changes.
6. Stop and restart the Assure DQ server for your changes to take effect.

   When a control point performs a log action, the system looks up the log action category and associated appender in log4j.xml. Based on the appender, the system writes a log message to the appropriate log file.

Modifying Action Logging under WebSphere

This section explains how to modify action logging under WebSphere. If Assure DQ runs under JBoss at your site, see "Modifying Action Logging under JBoss" on page 99.

By default, the system writes all action log messages to a file named log-action.log. The file is in the log subdirectory of the Assure DQ server installation directory.

Action Log Name and Location

To change the name or location of the action log, complete the following steps:

1. Go to the config directory for your Assure DQ server installation and open cee.log4j.properties with a text editor such as WordPad or vi.

   To find out the location of the config directory, open <install_folder>/Infogix/logs/<config_name>/IA. The CONFIG_HOME parameter specifies the location of the config directory.
2. In cee.log4j.properties, notice that the log4j.appender.finding.File parameter specifies the path and name of the log file, as shown below:

```
log4j.appender.finding=org.apache.log4j.RollingFileAppender
log4j.appender.finding.File=/opt/WebSphere/AppServer/5114/logs/server
1/log-action.log
log4j.appender.finding.MaxFileSize=5000KB
log4j.appender.finding.MaxBackupIndex=5
log4j.appender.finding.layout=org.apache.log4j.PatternLayout
log4j.appender.finding.layout.ConversionPattern=%d{ISO8601} %-5p
[%c{1}]: %m%n
```

3. To change the location or name of the log file, change the value of the log4j.appender.finding.File parameter, above, and save your changes.
4. Stop and restart the Assure DQ server for your changes to take effect.

Directing Messages to Multiple Log Files

This section describes how to configure the system to write action log messages to different log files based on log categories specified in the user interface. Review the example below and then complete the procedure for "Writing Messages to Different Logs Under WebSphere" on page 104.

Example

Suppose you assign log actions to either MyFirstCategory or MySecondCategory. You want the system to write MyFirstCategory messages to a finding1 log named log-action1.log, and MySecondCategory messages to a finding2 log named log-action2.log. To make this change, edit the cee.log4j.properties file, as follows:

Specify the two log action categories and the destination logs for messages in each category, as shown below:

```
log4j.category.logaction.com.infogix.MyFirstCategory=INFO, finding1
log4j.additivity.logaction.com.infogix.MyFirstCategory=false

log4j.category.logaction.com.infogix.MySecondCategory=INFO, finding2
log4j.additivity.logaction.com.infogix.MySecondCategory=false
```

Add appender specifications for the finding1 and finding2 logs. In this example, direct finding1 logging to log-action1.log; direct finding2 logging to log-action2.log.

```
log4j.appender.finding1=org.apache.log4j.RollingFileAppender
log4j.appender.finding1.File=/opt/WebSphere/AppServer/5114/logs/server1/
log-action1.log
log4j.appender.finding1.MaxFileSize=5000KB
log4j.appender.finding1.MaxBackupIndex=5
log4j.appender.finding1.layout=org.apache.log4j.PatternLayout
log4j.appender.finding1.layout.ConversionPattern=%d{ISO8601} %-5p
[%c{1}]: %m%n

log4j.appender.finding2=org.apache.log4j.RollingFileAppender
log4j.appender.finding2.File=/opt/WebSphere/AppServer/5114/logs/server1/
log-action2.log
log4j.appender.finding2.MaxFileSize=5000KB
log4j.appender.finding2.MaxBackupIndex=5
log4j.appender.finding2.layout=org.apache.log4j.PatternLayout
log4j.appender.finding2.layout.ConversionPattern=%d{ISO8601} %-5p
[%c{1}]: %m%n
```

Writing Messages to Different Logs Under WebSphere

To write log messages to different log files based on log categories, complete the following steps:

1. Go to the config directory for your Assure DQ server installation and open cee.log4j.properties with a text editor such as WordPad or vi.

   To find out the location of the config directory, open the appserver.properties file in <install_folder>/Infogix /config/<config_name>. The CONFIG_HOME parameter specifies the location of the config directory.
2. In cee.log4j.properties, use the category name parameter to specify each user-defined category.

   The system appends the category name to the default log4j category, logaction.com.infogix, to define the full log4j category.
3. Use the appender-ref parameter to associate messages in each category with a log.
4. Use the appender name parameter to direct messages from each log to a log file.
5. Save your changes.
6. Stop and restart the Assure DQ server for your changes to take effect.

   When a control point performs a log action, the system looks up the log action category and associated appender in cee.log4j.properties. Based on the appender, the system writes a log message to the appropriate log file.

Index