Oracle® Universal Content Management

Content Integration Suite Administration Guide

10*g* Release 3 (10.1.3.3.3)

November 2008

ORACLE®

Oracle Content Integration Suite Administration Guide, 10*g* Release 3 (10.1.3.3.3)

Primary Author: Will Harris

Contributor: Adam Stuenkel

Contents

Preface

The Oracle Content Integration Suite (CIS) Administration Guide contains information to assist administrators responsible for the configuration of Content Integration Suite. This guide contains introductory information, configuration notes, and the online Help topics. These Help topics are opened within CIS Administration Application by clicking the Help icons on the pages of the user interface. Each topic explains the page being viewed.

Audience

This guide is intended for application developers and integrators. The CIS Administration Guide contains information on the configuration of Content Integration Suite using the CIS Administration Application.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Related Documents

For more information, see the following documents in the Oracle Content Integration Suite (CIS) documentation set:

- Oracle Content Integration Suite (CIS) Developer Guide
- Oracle Content Integration Suite (CIS) Release Notes
- Oracle Remote Intradoc Client (RIDC) Release Notes

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Introduction

Content Integration Suite (CIS) enables communication with Oracle Content Server and is deployable on a number of J2EE application servers, in addition to working in non-J2EE environments. This guide explains the CIS Administration Application and provides information on general administration tasks.

This chapter contains the following sections:

1.1 CIS Architecture

Content Integration Suite has a layered architecture that allows for its deployment in a number of different configurations. The architecture, at its core, is based on the standard J2EE Command Design Pattern. The layers on top of the commands provide the APIs that are exposed to the end user.

This version of CIS uses the Universal Content and Process Management API (UCPM API) which uses the SCS API for communication to the content server. The SCS API wraps communication from the content server into an object model that allows access to the individual object metadata.

The UCPM API allows application developers to focus on presentation issues rather than being concerned with how to access content server services (IdcCommand services). The UCPM API comprises a set of command objects that encapsulate distinct actions that are passed to the UCPM API and then mapped to the content server. These commands include common functions such as search, checkout, and workflow approval. Each command is tied to one or more service calls. The UCPM API command objects have been developed in accordance with the J2EE Command Design Pattern.

This infrastructure is deployable in any J2EE-compliant application server or stand-alone JVM application. When deployed, the UCPM API will leverage the features in the environment, whether this is a J2EE application server or non-J2EE.

The UCPM API encapsulates content server business logic and validates the parameters of the incoming calls. The UCPM API handles communication to the content server, encapsulates socket communication logic (opening, validating, and streaming bits through the socket), and provides a strongly typed API to the available services.

1.2 Internationalization / Character Encoding

We recommend that encoding for CIS be set to the same encoding as the Java Virtual Machine running content server. However, if CIS is communicating with multiple instances of content server in different languages, the ISCSContext.setEncoding method can be used to set the encoding to match that of the JVM running CIS.

2

CIS Administration Application

The CIS Administration Application is the administration interface for Content Integration Suite (CIS). Deploying the CIS Administration Application separately from CIS allows administrators to choose to not install it on a production server for security purposes. The CIS Admin WAR file (cis-admin-10g.war) is included with the CIS distribution file. Follow your application server or servlet engine instructions to deploy the WAR file.

> **Note:** This guide uses the forward slash (/) to separate directories. Depending on your operating system, you may need to change the separation markers when defining directories.

This chapter contains the following sections:

2.1 Content Server Configuration

You must configure the content server to communicate with CIS by enabling the IP address of the application server. You must also install and enable the CIS_Helper component on your content server instance.

> **Note:** Ensure that the CIS_Helper component on your content server instance is enabled. Refer to the Oracle Content Server administration documentation for more information.

Enabling the IP Address on the Content Server

You must enable the IP address of the application server. This allows the content server to listen for connections from the application server.

1. On your content server instance launch the System Properties editor:

   Select **Content Server** then ***instance name*** then **Utilities** and then **SystemProperties**.

2. Select the Server tab.

3. Enter your application server specific information for the **Hostname Filter** and **IP Address Filter**.

   The wildcard (*) is accepted, but IP addresses must take the form x.x.x.x regardless of wildcards, and must be separated by a vertical bar.

   Example: `12.34.56.*|12.34.57.*|12.35.*.*`

4. You must restart the content server for these changes to take effect.

2.2 Using the CIS Administration Application

After deploying the CIS Administration Application, you will need to perform several configuration steps to communicate with your content server instance and to validate the connection.

This section contains the following topics:

2.2.1 Modifying the Global Configuration

Once you have deployed the CIS Administration Application and restarted the application server, you can modify the global configuration.

1. Launch the CIS Administration Application.
2. Click **Adapter Configuration.**
3. Click **Modify Global Configuration**.
4. Enter the SCS Command Web URL (the web address clients use to communicate with the CIS servlets).

   Optional: Enter the Server JNDI Properties (the JNDI properties used by the server to make JNDI connections).

5. Click **Apply**.

If this is a new installation, you must also configure the adapters for content server to communicate with the application server.

2.2.2 Configuring an Adapter for Content Server

You must configure an adapter for each content server instance.

1. Launch the CIS Administration Application.
2. Click **Adapter Configuration**.
3. For new installations, click **Create New SCS Adapter**.
4. To update an existing installation; click the adapter name (e.g., myadapter) on the Available Adapters to Configure list.
5. On the Adapter Properties page, specify these properties:
   - **Name**: The name of the adapter (e.g., myadapter).

- **Adapter Type**: Type of communication transport. Select **Socket** for open communication directly through the content server or **Web** for communication via the web server which requires individual authentication for each request.
- **Host**: The name or IP address of the content server instance.
- **Port**: The content server port number (e.g., 4444).
- **Use Persistent Connections**: Enable this checkbox if you want to keep the connection alive after a request is completed.

  If you enable persistent connections, you also need to configure them on your content server instance (via the providers interface). Refer to the Oracle Content Server administration documentation for more information.
- **Connection Timeout**: When using persistent connections, this value is the maximum amount of time the connection will wait for response. Default is 20000 milliseconds.
- **Version**: The content server version. Choose **Default** if you are using version 7.5 or greater or 7.0 if you are using version 7.0.
- **Resource Pool Initial Size**: The initial size of the adapter connection resource pool. Default is 10.
- **Resource Pool Initial Size**: The maximum size of the adapter connection resource pool. Default is 20.

6. Click **Apply**.

After configuring the CIS adapter you may want to run a sample command such as a search. To do this, restart the application server and then see "Running CIS Validation Tests" on page 2-3 for more information.

2.2.3 Running CIS Validation Tests

Two validation tests for installed adapters are available by clicking the **Actions** icon:

- **Validate Mapped Directory Configuration**: This will only pass if the properties for Content Mapping Location have been validly set.
- **Validate Communication with Content Server**: Returns configuration validation results. If communication is validated the message, *Communication to the content server is functioning correctly* will display.

Figure 2–1 Actions Icon

Once you have validated your configuration, click the **View/Execute Installed Commands** and run some commands against the content server.

2.3 Enabling CIS Administration Application Security

By default, the CIS Administration Application has no security. Enabling security provides a login screen.

Note: The system administrator may need to modify these steps, depending on the configuration of the particular application server environment.

Follow these steps to enable security:

1. If you have not already done so, unbundle the CIS distribution file.
2. Unbundle the CIS Admin Web WAR file (e.g., cis-admin-web-10g.war depending on version number). To avoid confusion with other files, you may want to create a sub-directory named *unbundled-admin-web-war* and unbundle to that location.
3. In the WEB-INF directory, open the **web.xml** file in a text-only editor.
4. In the **web.xml** file, add security-constraint and security-role information. Depending on your application server, these entries may vary.

   Example:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>staticfiles</web-resource-name>
    <url-pattern>/ui/resources/*</url-pattern>
  </web-resource-collection>
</security-constraint>

<security-constraint>
  <web-resource-collection>
    <web-resource-name>secure</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>CISAdministrator</role-name>
  </auth-constraint>
</security-constraint>

<login-config>
  <auth-method>FORM</auth-method>
  <form-login-config>
    <form-login-page>/login.do</form-login-page>
    <form-error-page>/login.do</form-error-page>
</login-config>

<security-role>
  <description>CIS Administrator</description>
  <role-name>CISAdministrator</role-name>
</security-role>
```

5. Change the default security role-name entries (optional step).

```
<role-name>CISAdministrator</role-name>
```

   When you access the CIS Administration Application, you will encounter a login screen. Only those assigned the defined security role-name will be allowed access. You will need to create this role in your application server and assign it to the appropriate users. Consult your application server documentation for more details.

6. Save the **web.xml** file.
7. Rebundle CIS Admin Web WAR file (including the edited web.xml file). If you followed the steps above, this would be the contents of the *unbundled-admin-web-war* directory.

For WebSphere only, if you have enabled Global Security, do not check the Enforce Java 2 Security option.

2.4 Command Caching

CIS features a robust command caching mechanism that allows users to turn on/off caching for different commands and allows users to specify a timeout value for the cache and the size of the cache. The caching mechanism allows a command to be tied to a content server subject so that when a subject change happens, the command cache is expired. Finally, it provides the idea of either sharing the cache with all users or isolating the caching resources to a single user.

When a command is cached, the request is intercepted by the CIS layer and an already existing response for that request is returned through the system. This implies that there are less round-trips to the content server as many of the requests will be handled before reaching the content server.

All data is cached per command; there is no sharing of data between commands. The cache data can live in one of two caches: a user cache or a global cache. A user cache is a cache that only the current user can access. It is determined by the ICommand.getUser() return value; all command requests, for a given command, that return the same value will share the same cache.

This section contains the following topics:

2.4.1 Cache Expiration

All cache values have a *time-to-live* in the cache. This value determines how long a cache is valid; the larger the value the better performing the cache but also the greater chance the cache will become full of items that are out of date. This value, specified in milliseconds, can be configured from the adapter configuration screen under the Command Cache Properties tab.

The value should be set high enough so the caching helps performance. Setting the value too low will cause CIS to spend too much time adding and removing items from the cache which will remove any performance benefit caching may provide. Alternatively, setting the value to high will create a greater frequency of having cache full of items that are out of date (a *dirty cache*).

2.4.2 Enabling Command Caching

Caching be enabled for any standard command from within the Active API. By default, caching is enabled on the file.getFileStream command (needed in conjunction with file caching) on the document.information.getInformationByID.

Follow these steps to enable command caching:

1. Launch the CIS Administration Application.
2. Click **Adapter Configuration**.
3. Click the adapter to configure (e.g., myadapter).
4. Select the **Command Cache Properties** tab.
5. Click the **View/Modify** actions link.
6. Click the **Create** actions link.
7. Select a command from the drop-down list.

8. Click **Select**.
9. Set these properties (or use the defaults):
   - **Cache Enabled**: Select **true** from the drop-down list to enable caching.
   - **Cache Type**: Select the type of cache: User (per user) or All (globally shared). The cache type should almost always be set to User as setting to All shares the same cache with all users.
   - **Cache Timeout**: Timeout of items in the cache in milliseconds (Default: 1800000).
   - **Cache Subjects**: Subjects from the content server on which this cache is dependent (documents, users, subscriptions, etc.).

     The cache subjects associate the Command Cache with subjects in the content server. By default, the subject is documents meaning that when any documents are updated in the content server (i.e., created, deleted, or modified) the cache for this command will be cleared.

     When it is determined the a content server subject has been updated, all cached commands corresponding to the subject will be flushed. Refer to the Oracle Content Server administration documentation for more information.
10. Click **Submit**.

2.4.3 Event Polling

The event polling mechanism in CIS is related to the Command Cache, in that it polls the content server on a scheduled interval and if changes are found, it sends out events through the CIS layer. These events tell the Command Cache that content has been updated, a subject has changed, etc., and to clear the cache appropriately. If the event poller is not enabled (via the Event Polling Properties tab on the adapter configuration page), then no events will be generated and the cached items will only be expired via their timeout values.

The EventPoller looks for two types of events:

- Subject events
- Document events (added/deleted/updated)

Subject events are indications by the content server that something has changed under a given subject. These subjects are items such as documents, users, subscriptions, etc. Any of these subjects can be used to dirty an item in the command cache. Refer to the Oracle Content Server administration documentation for more information

2.5 Logging

CIS uses the Apache Commons Logging framework for logging bundled with the log4j implementation of the Apache Commons framework. Thus, all logging calls are routed to the log4j system. The log4j system is controlled by an XML file that describes which log categories will be displayed.

Refer to the Apache documentation for more information:
`http://jakarta.apache.org/commons/logging/`

The *cis-logging.xml* log4j configuration file is located in the /conf directory of the unbundled distribution file. This directory also contains the adapterconfig.xml file and should be in your Classpath.

Using the defaults entries, only CIS warnings and some important information are displayed upon startup. All logging calls are routed to both the application System.out (i.e. to the console) and outputs to the /bin/scsadapter.log file:

Example (default entry):

```
<param name="File" value="scsadapter.log"/>
```

For logging in a servlet, add the following to the XML file:

```
<category name=my_servlet additivity=false>
  <priority value=debug/>
  <appender-ref ref=ALL/>
</category>
```

Logging Categories

This table provides some important categories for CIS logging. In general, the categories correspond to the class names where the log message originated.

Category	Description
com.stellent.cis	The root category; should catch all the CIS-related messages. Note that most messages are at a DEBUG or INFO level; set to WARN to only get actual warnings or errors.
com.stellent.cis.impl.CISApplication	Category used to print out the initialization banner. Set this to INFO to see the startup banner.
com.stellent.cis.server.api.scs	Category for all the content server interactions. Set this to INFO or DEBUG to see logging related to pooling, communication, etc.The DEBUG level returns the most logging.
com.stellent.cis.server.api.scs.protocol.impl.HDAProtocol.write	Category to see what is written to the content server.
com.stellent.cis.server.api.scs.protocol.impl.HDAProtocol.read	Category to see what is read from the content server.

3 Online Help

These Help topics are opened within CIS Administration Application by clicking the Help icons on the pages of the user interface. Each topic explains the page being viewed. From any topic, you can gain access to the complete Help system:

> **Note:** This guide uses the forward slash (/) to separate directories. Depending on your operating system, you may need to change the separation markers when defining directories.

This chapter contains the following sections:

3.1 CIS Administration Options

From this page you can perform these functions:

- Click **Adapter Configuration** to modify the global configuration and/or create new adapters.
- Click **Browse UCPM Commands** to view command information and to execute a command.
- Click **Search For Commands** to search for a command by category, command name, or service name.
- Click **Validate Configuration** to validate the CIS configuration.
- Click **Support** to download the adapter configuration XML file. This file may be requested by support to assist in configuration issues.
- Click **About** to view the server properties and configured adapters.

3.2 Configuration Options

From this page you can modify the global configuration, create new adapters, and update existing adapters.

Configuration Options

- Click **Modify Global Configuration** to edit/update the SCS Command Web URL.
- Click **Create new SCS Adapter** to configure an adapter for a content server.

To update an existing adapter; click the adapter name on the Configure Existing Adapter list.

Configure Existing Adapter

- Click the adapter name (e.g., myadapter) to view the current configuration information for the adapter or to update the adapter configuration.
- Click the **Actions** icon (Figure 3–1) and choose **Set As Default** or **Delete** for this adapter.

Figure 3–1 Actions Icon

3.2.1 Global Configuration Options

From this page you can define or update the SCS Command Web URL.

SCS Command Web URL: The web address clients use to communicate with the CIS servlets (i.e., http://<servername>:<port>/cis-server).

3.2.2 Create a New Adapter

From this page you can create a new content server adapter. If this is a new installation, you must create an initial adapter. These settings are stored in the adapter configuration file (adapterconfig.xml).

To create a new SCS adapter, specify the properties below and then click **Apply**.

Name: The name of the adapter (e.g., myadapter).

Adapter Type: Type of communication transport.

- **Socket**: Using a socket connection opens communication directly to your content server instance (typically port 4444). This implied that you have established a trust relationship between your client machine and the content server.
- **Web**: Using Web Authentication, every call to the content server will require credentials (all communication with content server must be authenticated). This allows CIS to call services on the content server without opening up port 4444. This also means that you can only perform an operation in content server with the authenticated ID; since there is no trust relationship to perform an operation as *sysadmin* you must have the credentials for the sysadmin user.

Host: The name or IP address of your content server instance.

Port: The content server port number (e.g., 4444).

Use Persistent Connections: Enable this checkbox if you want to keep the connection alive after a request is completed. If you enable persistent connections, you also need to configure them on your content server instance (via the providers interface). Refer to the Oracle Content Server administration documentation for more information.

Connection Timeout: When using persistent connections, this value is the maximum amount of time the connection will wait for response. Default is 20000 milliseconds.

Version: The content server version. Choose **Default** if you are using version 7.5 or greater or 7.0 if you are using version 7.0.

Resource Pool Initial Size: The initial size of the adapter connection resource pool. Default is 10.

Resource Pool Initial Size: The maximum size of the adapter connection resource pool. Default is 20.

3.2.3 Content Server Adapter Properties

From this page you can update the configuration of an existing adapter. These settings are stored in the adapter configuration file (adapterconfig.xml).

These properties can be updated by selecting the appropriate tabs:

- "Standard Properties" on page 3-3
- "Vault Properties" on page 3-4
- "SSL Properties" on page 3-5
- "Command Cache Properties" on page 3-5
- "Event Polling Properties" on page 3-5

3.2.3.1 Standard Properties

These properties can be set:

Name: The name of the adapter (e.g., myadapter).

Adapter Type: Type of communication transport.

- **Socket**: Using a socket connection opens communication directly to your content server instance (typically port 4444). This implied that you have established a trust relationship between your client machine and the content server.
- **Web**: Using Web Authentication, every call to the content server will require credentials (all communication with the content server must be authenticated). This allows CIS to call services on the content server without opening up port 4444. This also means that you can only perform an operation in content server

with the authenticated ID; since there is no trust relationship to perform an operation as *sysadmin* you must have the credentials for the sysadmin user.

Host: The name or IP address of your content server instance.

Port: The content server port number (e.g., 4444).

Use Persistent Connections: Enable this checkbox if you want to keep the connection alive after a request is completed. If you enable persistent connections, you also need to configure them on your content server instance (via the providers interface). Refer to the Oracle Content Server administration documentation for more information.

Connection Timeout: When using persistent connections, this value is the maximum amount of time the connection will wait for response. Default is 20000 (in milliseconds).

Version: The content server version. Choose your version from the drop-down list. If your content server is version 7.6.x or 7.5.x you must make the appropriate selection when configuring your adapter.

Resource Pool Initial Size: The initial size of the adapter connection resource pool. Default is 10.

Resource Pool Initial Size: The maximum size of the adapter connection resource pool. Default is 20.

3.2.3.2 Vault Properties

These options (Default, Web Transfer, and Mapped Vault) define the method for transferring files from the content server. In most instances the default option may be used. However, enabling mapped vault will result in a performance improvement.

Web Transfer

Enables the *web transfer* method for transferring files from the content server. This method retrieve files via the content server web server.

- **Web Vault Prefix**: The prefix for the web address (usually http://<servername>:<port>) to the content server vault directory.
- **Web Layout Prefix**: The prefix for the web address (usually http://<servername>:<port>) to the content server weblayout directory.
- **Web Vault User Name**: The username to use when retrieving files.
- **Web Vault Password**: The password to use when retrieving files.

Mapped Vault

Enables the *mapped vault* method for transferring files from the content server (will improve performance, if used).

- **Mapped Server Vault**: The path to the content server vault directory as seen from the application server. This needs to be accessible from the application server.
- **Mapped Server Weblayout**: The path to the content server weblayout directory as seen from the application server. This needs to be accessible from the application server.
- **Content Server Vault**: The path to the content server vault directory as seen from the content server.

The application server needs to have WRITE privileges to the Mapped Server Vault directory.

3.2.3.3 SSL Properties

CIS supports Secure Socket Layer (SSL) communication with the content server. You must have completed the preliminary setup before proceeding:

- You must have a valid KeyStore / TrustManager with signed trusted certificates on both the client (CIS) and server (content server).
- You must have installed the Security Providers component and configured content server for SSL communication.

Enter the appropriate values (these will vary, depending on your configuration):

Enable SSL: Check this box to enable SSL communication for this adapter.

Keystore File Path: The absolute path to client-side keystore.

For example: /tmp/ssl/client_keystore

Keystore Alias: The alias to use when accessing keystore.

Keystore Password: The password used to access keystore.

Keystore Alias Password: The password to use when accessing keystore with specified alias.

Trust Manager File Path: The absolute path to the client-side trust manager.

Trust Manager Password: The password used to access the trust manager.

Encryption Algorithm: The encryption algorithm to use (e.g., sunx509).

3.2.3.4 Command Cache Properties

These properties can be set:

Cache Enabled: Check this box to enable caching for this adapter.

User Cache Capacity: The capacity of the cache for each user. These are the cached items or responses from the server. Default is 1000.

Global Cache Capacity: The capacity of the global cache. These are the cached items or responses from the server. Default is 1000.

Actions

Click the **View/Modify command cache policies** link to modify command cache policies.

3.2.3.5 Event Polling Properties

These properties can be set:

Enabled: Check this box to enable to enable the event polling system.

Polling Interval: The amount of time between content server cache update queries (in milliseconds).

User Authentication Type: The type of authentication to use for background process.

- **Basic**: Perform user authentication via HTTP Basic User Authentication.
- **NTLM**: Perform user authentication via the NTLM protocol. This protocol is supported by all versions of the Internet Explorer and is mainly useful for intranets. Depending on your preferences setting this will supply your windows logon credentials to the web server when the server asks for NTLM authentication. This saves the user to type in their password again.

NTLM authentication works only when KeepAlive is on.

3.2.4 Cache Policies

From this page you can configure your cache policies and create new command cache policies.

Configured Cache Policies

The currently configured cache policies are listed.

See "Browse Commands" on page 3-8 for information on selecting and executing a service.

Actions

- Click **Create** to create a new command cache policy.
- Click **Clear** to create the command cache of all commands.
- Click the **Actions** icon (Figure 3–2) and then **Delete** to delete this command.

Figure 3–2 Actions Icon

Select Cache Policies

From this page you can select the command for your cache policies and configure your cache policies.

1. Select a command from the drop-down list.
2. Click **Select**.

These properties can be set:

Command Name: The Name of the command this policy represents.

Cache Enabled: Select **true** from the drop-down list to enable caching.

Cache Type: Select the type of cache: **User** (per user) or **All** (globally shared). The cache type should almost always be set to User as setting to All shares the same cache with all users.

Cache Timeout: Timeout of items in the cache in milliseconds (Default: 1800000).

Cache Subjects: Subjects from the content server on which this cache is dependent (documents, users, subscriptions, etc.). The cache subjects associate the Command Cache with subjects in the content server. By default, the subject is documents meaning that when any documents are updated in the content server (i.e., created, deleted, or modified) the cache for this command will be cleared.

When it is determined the content server subject has been updated, all cached commands corresponding to the subject will be flushed. For a list of subjects, Refer to the Oracle Content Server administration documentation for more information.

See "Command Caching" on page 2-5 for more information.

3.2.5 Command Cache Policies

From this page you can view your configured command cache policies and create new command cache policies.

Configured Command Cache Policies

The currently configured cache policies are listed.

Actions

- Click the **Create** link to create a new command cache policy.
- Click the **Clear** link to clear the command cache of all commands.
- Click the **Actions** icon (Figure 3–3) and then **Delete** to delete this command.

Figure 3–3 Actions Icon

Command Cache Properties

Size: The amount of disk space being used (in bytes).

Count: The number of items cached.

Location: The location where items are cached.

See "Command Caching" on page 2-5 for more information.

Select Command

To create a new command cache policy:

1. Click the **Create** link.
2. Select the command from the **Select Command** drop-down menu.
3. Click **Submit**.

3.2.6 File Cache Policies

From this page you can view your configured file cache policies, create new file cache policies, and view your configured command cache policies.

Configured File Cache Policies

The currently configured cache policies are listed.

Actions

- Click the **Create** link to create a new command cache policy.
- Click the **Clear** link to clear the command cache of all commands.
- Click the **Actions** icon (Figure 3–4) and then **Delete** to delete this command.

Figure 3–4 Actions Icon

Command Cache Properties

Global Cache Size: The number of items in the global cache.

User Count: The number of user caches currently allocated.

User Cache Size: The number of total items in the user cache for all users.

See "Command Caching" on page 2-5 for more information.

Select Command

To create a new command cache policy:

1. Click the **Create** link.
2. Select the command from the **Select Command** drop-down menu.
3. Click **Submit**.

3.3 Browse Commands

From this page you can browse the CIS commands. This allows you to view command information and also execute a command.

To execute a command

1. Select an API to browse (e.g. Active).
2. Select an API category (e.g., administrative).
3. Select a command (e.g., administrative.pingServer).
4. Click the Method name (e.g., pingServer).
5. Enter the required parameters:
6. **User ID:** An authorized content server User ID (e.g., sysadmin).
7. **Adapter:** Select an adapter from the drop-down list.
8. **Credentials:** The content server password (e.g., idc).
9. Other parameters as applicable (for example, **Document ID**, **monitoredSubjects**, **monitoredTopics**, etc.).
10. Click **Execute Command**.

3.3.1 Categories

From this page you can browse the various categories for the API and also execute a command.

To execute a command

1. Select a category (e.g., file).
2. Select a command (e.g., file.getFile).
3. Click the Method name (e.g., getFile).
4. Enter the required parameters:
5. **User ID:** An authorized content server User ID (e.g., sysadmin).
6. **Adapter:** Select an adapter from the drop-down list.
7. **Credentials:** The content server password (e.g., idc).
8. Other parameters as applicable (for example, **Document ID**, **monitoredSubjects**, **monitoredTopics**, etc).
9. Click **Execute Command.**

3.3.2 Commands

From this page you can browse the various commands for the API and also execute a command.

To execute a command

1. Select a command (e.g., administrative.pingServer).
2. Click the Method name (e.g., pingServer).
3. Enter the required parameters:
4. **User ID:** An authorized content server User ID (e.g., sysadmin).
5. **Adapter:** Select an adapter from the drop-down list.
6. **Credentials:** The content server password (e.g., idc).
7. Other parameters as applicable (for example, **Document ID**, **monitoredSubjects**, **monitoredTopics**, etc.).
8. Click **Execute Command**.

3.3.3 Methods

This page provides method name, return type, and parameter information.

To execute a command

1. Click the Method name (e.g., getFile).
2. Enter the required parameters:
3. **User ID:** An authorized content server User ID (e.g., sysadmin).
4. **Adapter:** Select an adapter from the drop-down list.
5. **Credentials:** The content server password (e.g., idc).
6. Other parameters as applicable (for example, **Document ID**, **monitoredSubjects**, **monitoredTopics**, etc.).
7. Click **Execute Command**.

Click the **JavaDoc** icon for detailed method and parameter information.

3.3.4 Execute a Command

To execute a command, enter the required parameters and click Execute Command.

Example:

1. **User ID:** An authorized content server User ID (e.g., sysadmin).
2. **Adapter:** Select an adapter from the drop-down list.
3. **Credentials:** The content server password (e.g., idc).
4. Other parameters as applicable (for example, **Document ID**, **monitoredSubjects**, **monitoredTopics**, etc.).

Click the **JavaDoc** icon for detailed method and parameter information.

3.3.5 Response

This page provides response information on the executed command.

View properties: Select **strongly typed** (to view relevant properties) or **all available** from the drop-down list. Selecting **all available** will return additional properties such as UserDateFormat, clientEncoding, and MonitoredTopics.

Click the **JavaDoc** icon for detailed method and parameter information.

3.4 Search for Commands

This page allows you to search for a command by category, command name, or by the name of a content server service.

Category: The name of the category to query (e.g., administrative).

Command Name: The name of the command to query (e.g., getDocInfoByID).

Service Name: The name of the content server service to query (e.g., DOC_INFO).

Match all criteria: Select **true** to search for a match on all criteria or **false** to search for a match on any of the criteria. The default is **false**.

3.5 Validate Configuration

This page allows you to check the configuration of installed adapters.

Adapter: Select the adapter to view the current adapter configuration.

Tests: Click the **Actions** icon (Figure 3–5) and select an option to perform a test.

- Validate Mapped Directory Configuration
- Validate Configuration with the Content Server

Figure 3–5 Actions Icon

3.6 Support

This page allows you to download the adapter configuration file. You can copy and paste the contents of this file to assist Support Services in diagnosing issues.

3.7 About

This page provides the CIS Server and CIS Client properties such as the build number, the build date, and services URL.

Index