Oracle® Enterprise Manager

Configuration Change Console User's Guide

10*g* Version 10.2.0.5 for Windows or UNIX

E12913-02

June 2009

ORACLE®

Oracle Enterprise Manager Configuration Change Console User's Guide 10*g* Version 10.2.0.5 for Windows or UNIX

E12913-02

Primary Author: Leo Cloutier

Contributing Author: Jerry Russell

Contributor: Daniel Hynes

Contents

Preface xi

Audience xi
Documentation Accessibility xi
Conventions xiv
Support and Contact Information xiv

1 Overview of Configuration Change Console

1.1 Getting Started 1-1
1.2 Accessing the Console: User Accounts 1-2
1.3 Configuration Change Console Architecture 1-3
1.3.1 Configuration Change Console Agents 1-3
1.3.2 Configuration Change Console Database 1-3
1.3.3 Configuration Change Console Application Server 1-4
1.3.4 Configuration Change Console Messaging Broker Server 1-4
1.4 Using the Configuration Change Console Interface 1-4
1.4.1 User Interface Language and Locale 1-4
1.4.2 Navigation Conventions 1-5
1.4.3 Moving Between Screens 1-5
1.4.4 Accessing Online Help 1-5
1.4.5 Applying Filters to Displays 1-5

2 About the Dashboard

2.1 Frameworks and Policies 2-1
2.2 Understanding the Policy Summary Portlet 2-1
2.3 Viewing Policy Status Details 2-2
2.4 Top-Level Dashboard Status 2-2
2.4.1 Alerts 2-2
2.4.2 Most Active Applications - Today 2-3
2.4.3 Total Events 2-3
2.5 Second Level Dashboard Tabs: Control, Application, User, Device 2-3
2.5.1 Control Summary 2-3
2.5.2 Application Summary 2-4
2.5.3 User Summary 2-4
2.5.4 Device Summary 2-4
2.5.4.1 Most Active Users 2-5
2.5.4.2 Account Management 2-5
2.5.4.3 Database Management Summary 2-5
2.6 Change Management Portlets 2-5

3 Setting Up the Environment

3.1 Configuring People and Teams 3-1
3.1.1 People 3-1
3.1.2 Teams 3-1
3.1.2.1 Configuring People 3-2
3.1.2.2 Add or Update a Person 3-2
3.1.2.3 Person to User Assignment 3-3
3.1.2.4 Configuring Teams 3-3
3.2 Adding Managed Devices and Device Groups 3-3
3.2.1 Adding and Updating a Managed Device 3-3
3.2.2 Adding or Updating Device Groups 3-4
3.3 Assigning Teams to Managed Device Groups 3-6
3.4 Validating Team and Device Group Assignments 3-7
3.5 Working With A Large Environment 3-7
3.5.1 Device Groups 3-7
3.5.2 Team Support Assignments 3-7
3.5.3 UI Screen Scaling 3-8

4 Understanding Policy Configuration

4.1 Rule Set Types 4-1
4.2 Data and Events to be Monitored 4-2
4.2.1 Monitoring Applications 4-2

5 Operations Management

5.1 Steps for Modeling a Business Application 5-3
5.2 Understanding Components 5-3
5.3 Step 1: Creating Components 5-4
5.3.1 Add or Update a Component 5-5
5.3.2 Importing Components 5-5
5.3.3 Creating Custom Component Types 5-6
5.4 Step 2: Defining Component Rules 5-6
5.4.1 General Monitoring Guidelines: Rule Sets 5-7
5.4.2 Selecting Component Rule Sets 5-8
5.4.3 Adding Component Rule Sets 5-9
5.4.4 Monitoring Files 5-10
5.4.5 Monitoring Processes 5-11
5.4.6 Monitoring Operating System Users 5-12
5.4.7 Monitoring Component Internal Rule Sets 5-13
5.4.7.1 Configure Internal Rule Sets 5-14
5.4.7.2 Override Rules and Configuration for Instances 5-15
5.4.8 Internal Rule Sets: Database Snapshot type Rule Sets 5-15
5.4.8.1 SQL Query Parameters 5-15
5.4.8.2 Baseline Recording 5-16
5.4.8.3 Include/Exclude Parameters 5-16
5.4.9 Internal Rule Sets: Specific Pattern Types 5-17
5.4.9.1 Patterns Types for Trace and Audit Rule Sets 5-18

5.4.10 Active Directory Monitoring 5-18
5.5 Step 3: Mapping Components to Managed Devices 5-20
5.6 Step 4: Assign Controls to a Component 5-20
5.7 Step 5: Applications 5-21
5.7.1 Creating Applications 5-21
5.7.2 Adding Component Instances to an Application 5-22
5.8 Step 6: Defining Application Audit Actions 5-22
5.8.1 Change Management Integration: Detecting Authorized/Unauthorized Events 5-22
5.8.2 Defining Audit Policies 5-23

6 Policy Management

6.1 Frameworks 6-1
6.1.1 Modifying or Creating New Frameworks 6-2
6.1.2 Copying a Framework 6-2
6.2 Policies 6-3
6.2.1 Modifying or Creating New Policies 6-4
6.2.2 Copying a Policy 6-4
6.3 Controls 6-5
6.3.1 Modifying or Creating New Controls 6-6
6.3.2 Copying a Control 6-6
6.3.3 Assigning Components To a Control 6-7

7 Integrating With A Change Management Server

7.1 Step 1: Configuring Change Management Integration 7-2
7.2 Step 2: Configuring the Outbound Ticket Template 7-3
7.3 Step 3: Assigning Categorizations to Component Instances 7-5
7.4 Step 4: Configuring Audit Actions for Authorized/Unauthorized Events 7-5
7.5 Emergency Change Process Flow 7-5
7.6 Monitoring Change Management Server Integration 7-6
7.6.1 Inbound Ticket History 7-6
7.6.2 Outbound Ticket History 7-7

8 Configuring Threshold Monitoring

8.1 Understanding Threshold Rule Sets 8-1
8.1.1 Threshold Rule Types 8-1
8.1.2 Notification Options 8-2
8.1.3 Escalation Priorities 8-2
8.2 Defining Threshold Rules 8-3
8.2.1 Defining Threshold Rule Sets 8-6
8.3 Assigning Rule Sets to Devices 8-6
8.4 Validating Threshold Assignments 8-7

9 Updating Agents With Policies

10 Responding to Notifications

10.1 Responding to Notifications by Email 10-1

10.2 Responding to Notifications with the Pending Notifications Screen 10-1

11 Viewing and Analyzing Change Events

11.1 Activity Summaries 11-1
11.1.1 Using the Activity Dashboard 11-1
11.1.2 Viewing Event Summary Statistics 11-2
11.1.3 Using the Audit Summary Screen 11-2
11.2 Visualizing Change 11-2
11.2.1 Viewing Changes to Servers 11-3
11.2.2 Viewing Changes by User 11-4
11.2.3 Viewing Application Changes 11-6
11.2.4 Visualizing Changes Across Devices (Global Events) 11-6
11.2.5 Visualizing Changes Over Time 11-7
11.2.6 Visualizing Database Inventory 11-7
11.3 Analyzing Infrastructure Change Trends 11-8

12 Administering Servers and Agents

12.1 Server Administration 12-1
12.1.1 Configuring Email Access 12-1
12.1.2 Configuring SNMP Server Information 12-2
12.1.3 Managing Database Size 12-3
12.1.4 Setting Database Purging Policies 12-3
12.1.5 Disabling or Enabling Team Device Limiting 12-4
12.1.6 Configuring Archived File Storage 12-4
12.1.7 Configuring Administrative Alerts 12-4
12.1.8 Configuring Dashboard Thresholds 12-6
12.1.9 Configuring LDAP Integration 12-6
12.1.10 Viewing Server Information: Server Reports 12-6
12.2 Agent Administration 12-7
12.2.1 Viewing Agent Schedule Templates 12-7
12.2.2 Creating/Assigning Schedule Groups 12-8
12.2.3 Assigning a Schedule Template to a Schedule Group 12-8
12.2.4 Stopping, Holding, Resuming and Pausing Agents 12-9
12.2.5 Upgrading Agents From the Server 12-9
12.2.6 Viewing Agent Information (Agent Reports) 12-10

13 Configuring, Generating, and Viewing Reports

13.1 BI Publisher Server Configuration 13-1
13.2 BI Publisher Deployment 13-2
13.2.1 Update a BI Publisher Deployment 13-4
13.3 Configuring Report Instances 13-4
13.3.1 Selecting Devices for Report Instances 13-5
13.3.2 Configuring the Report Distribution List 13-5
13.4 Generating and Viewing Reports 13-6
13.5 Viewing Online Reports 13-7

A Predefined Component Templates

B Operating System Rule Set Capability Details

Files B-1
Rules B-1
Processes B-2
Rules B-2
Processes On OS/400 ..... B-3
Rules B-3
OS Users B-4
Rules B-4

C Component Internal Rule Set Capability Details

Oracle 8i/9i/10g (Audit) C-2
Rule Set Configuration C-2
Rules C-2
Oracle 8i (Snapshot) and Oracle 9i/10g (Snapshot) C-4
Rule Set Configuration C-4
Rules C-5
Microsoft SQL Server 2000 (Audit) C-7
Rule Set Configuration C-8
Rules C-8
Microsoft SQL Server 2000 (SQL Trace) C-9
Rule Set Configuration C-9
Rules C-10
Microsoft SQL Server (Snapshot) C-11
Rule Set Configuration C-11
Rules C-12
Microsoft Active Directory (Trace) C-14
Rule Set Configuration C-14
Rules C-14
Microsoft Active Directory/LDAP (Snapshot) C-15
Rule Set Configuration C-16
Rules C-16
Microsoft Windows Registry C-17
Rule Set Configuration C-17
Rules C-17
SNMP Traps C-18
Rule Set Configuration C-18
Rules C-19

D Accessing Data Through Third Party Tools

Description of Views D-1

E Third Party Licenses

Apache Software Foundation Licenses E-2

Apache Software License, Version 1.1 ..... E-2
Apache Avalon 4.1.3 ..... E-3
Apache Crimson 1.1.1 ..... E-3
Xerces 2.6.2 ..... E-3
Ant 1.5.1 ..... E-3
Apache Software License, Version 2.0 ..... E-3
Log4J 1.2.8 ..... E-4
Apache Axis, Version 1.2RC2 ..... E-4
LogKit E-4
Codehaus Plexus E-4
Spring 2.0.2 ..... E-4
Pluto 1.1.0 ..... E-4
Apache Commons 1.0 ..... E-4
Apache Tomcat Commons E-4
CGILIB 2.0.1 ..... E-4
Jaxen E-4
Xalan E-4
ODMG Library E-4
Catalina E-5
SNMP4J E-5
Castor 0.95 ..... E-5
Sun Binary Code License Agreement E-5
Javamail E-10
BSH-CORE 1.3.0 ..... E-13
DOM4J E-14
ANTLR 3 ..... E-14
JAVA SERVICE WRAPPER E-15
JNI REGISTRY 3.1.3 ..... E-16
WSDL4J E-16
AOPAlliance E-17
XDOCLET 1.2.3 ..... E-17
JDOM 1.0B9 ..... E-18
MSVP60.DLL E-19
PDH.dll 5.0.2195.2668 ..... E-21
MIBBLE 2.8 ..... E-22
Robohelp 5.0 ..... E-25
Microsoft SQL SERVER DRIVER 2005, 1.2 ..... E-33
Install Anywhere E-35
Additional Licensing Information E-40

Glossary

Preface

This guide describes the basic features and functionality of the Oracle Enterprise Manager Configuration Change Console.

Audience

The overview describes the overall solution and the user interface components. It is applicable to all users of the Configuration Change Console.

Administrators of the Configuration Change Console should also read the sections on setting up the environment, administering the product, defining policies, responding to notifications, and viewing/analyzing infrastructure changes. These sections assume that you are already familiar with the business applications you intend to monitor using Enterprise Manager.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. 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

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711.

Configuration Change Console Navigation

The Configuration Change Console user interface is composed of four primary parts. There is a region at the top which contains navigation tabs with drop down menus and other links for common actions. To navigate the drop down menu, the TAB key or equivalent will move across the tabs. Pressing the Return key will open the drop-down menu. Pressing the Enter key again will close it. When a tab drop-down menu is open, press the Tab key to navigate to the screen you want to open.

Below this region is an iframe which contains three functional areas. The first area is the header for the page which can have a header and a subheading. There are also icons for reloading the page, printing the current page, showing/hiding the filter bar, and showing the context sensitive help (new window) for the current page.

The next region is the filter bar. A filter bar will be hidden for any screen where there is no appropriate filter content. You can toggle showing/hiding this filter content by clicking on the filter bar icon in the header row. This region has an H1 level tag at the beginning to indicate the start of the filter bar and to provide a point to jump to in navigation.

The final region is the page content. All content will be shown in this area. This region has an H1 level tag at the beginning to indicate the start of the content area and to provide a point to jump to in navigation.

Synthesized Controls

The Configuration Change Console has a few areas where an action or link may cause a change somewhere else on the screen.

1. In some filter bars in screens, making a selection from a drop down will cause the entire page to reload to populate filter bars that are below the selected filter bar. If a change to a form element in a filter bar causes a page to reload, all other information that has already been selected above the most recently changed element will be preserved.

   An example of this can be found when you navigate to the following screen:

   Policy --> Operations Management --> Component

   Selecting the first filter bar option and changing it to *Predefined Components* will cause the entire page to automatically load and change the view from *Custom Components* to *Predefined Components*.

2. Screens in which rules are edited have a control with multiple form elements in one horizontal line. This row is rendered as a structural table. There is a link at the bottom right of this table labeled *Add Instance* that adds a new row to the end of the table to allow a new rule to be added. This is the only case where clicking on a link will affect some element above the area where the click happened.

   An example of this can be found on the following screen:

   Policy --> Operations Management --> Components

   After creating a component, click on the 0 link under Rule Sets. Then add a new rule set. Click on the **Edit Rules** link for the rule set. There will be a table with one row for a rule set available. Clicking on the **Add Instance** link to the bottom right of this table will add another row.

Disabling Screen Autoreloading

The product utilizes auto reloading of some screens, such as on the dashboard to reload the page every five minutes. If needed for accessibility purposes, this can be disabled product-wide by following these steps:

1. Stop the Configuration Change Console Server service
2. Connect to the database as the gateway user:

   ```
   sqlplus gateway/password@sid
   ```

   Where you replace password with the password for the gateway user, and sid with the sid of the database you created at product installation time. If you used a username other than gateway, also change this username here as well.
3. Execute the following SQL statements:

   ```
   update serverproperty set prop_value=0 where prop_name =
   'autoreload_enabled';

   commit;
   ```
4. Restart the Configuration Change Console Server

There is still one case where autoloading is not disabled and this is in a part of the jsp code that checks every five minutes to determine whether the session is still active. If the session is lost, then the user will be redirected to the login page with a note that their session expired. This cannot be changed, however the session time out period can be extended. There is another section in this document related to this server property.

Installing the Server and Agents

Both the agent and server installer use a third party installation product that has the capability to install in a text-based console mode. Instead of launching the graphical installer, you can launch the installer from a DOS prompt or Unix console by typing one of the following two commands:

```
Server.exe -i console
```

```
Agent-win.exe -i console
```

You will then walk through the installation steps in the console.

You can also use a pre-filled response file and perform a silent installation where there is no interactive actions.

For more information about both of these options, see the server or agent installation sections of the *Configuration Change Console Installation Guide*.

Stylesheet

The product uses one stylesheet */gateway/stylesheet.css* for its screens other than the login screen. This style sheet can be found in the following directory and can be changed as needed.

CCC Install Directory}\deploy\activereasoning.ear\gateway.war\stylesheet.css

After making changes to the stylesheet, you should stop and start the Configuration Change Console Server service to ensure it is not cached in the web container.

The most commonly used style classes are:

- *Headerstl, SimpleHeaderstl, DashboardHeaderstl* - For table headers
- *Datastl* - Used for all content in tables and on screen
- *Buttonstl* - Used for form buttons
- *ErrorDatastl, WarningDatastl, SuccessDatastl* - Used for on screen messages

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. It can also emphasize or introduce new terms.
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.

Support and Contact Information

Contact your Oracle support representative for technical support.

1

Overview of Configuration Change Console

Enterprise Manager Configuration Change Console supports best practices policies by enabling you to validate user actions against established IT Controls, thereby helping to reduce unauthorized change and uncontrolled access attempts made to the IT infrastructure. By automatically monitoring critical applications and infrastructure components for changes, and then comparing detected changes to planned changes, the software can track activity, generate reports, trigger alert notifications, and identify policy violations.

Used as part of your IT compliance effort, the Configuration Change Console ensures adherence to internal controls supporting essential systems by monitoring, managing and auditing changes against corporate best practices policies. Although the products focus on IT control validation and compliance, they may also support other essential IT operations, including:

- Monitoring Change: Providing visibility into change in the infrastructure, and linking ticketed changes to actual changes.
- Troubleshooting/Forensics: Identifying the changes that could have contributed to outages or problems and putting safeguards in place. You even can archive critical configuration files so you can roll back problematic changes.
- Overall IT Management: Identifying trends in CPU utilization, disk utilization, and so on, for critical applications, and alerting administrators to potential problems before they cause outages.

You decide which infrastructure components you want to monitor. The Configuration Change Console collects data from those components according to the data collection rules you have defined, generates notifications according to those rules, and maintains a database of the changes made to those infrastructure components.

You can then explore and analyze that data for compliance or for forensic purposes, displaying information in a time-based information model to accurately track exactly what changed and when. The user interface offers graphical visualization tools and the ability to drill down to specific devices, time intervals, and events. The solution provides both packaged and ad hoc reporting capabilities.

1.1 Getting Started

To start using the product, you must complete several basic setup tasks before you can start monitoring and collecting data. The following table provides an overview of the steps and the documentation where you can find details.

Table 1–1 Initial Setup Steps

Initial Setup	Details
1. Install the Configuration Change Console server and database.	Refer to the *Enterprise Manager Configuration Change Console Installation Guide*.
2. Configure your web browser to refresh the display every time you access a page.	For Microsoft Internet Explorer: **1.** Tools -> Internet Options -> General: Settings **2.** Select **Every visit to the page**.
3. Install agents on the devices you want to manage.	Refer to the *Enterprise Manager Configuration Change Console Installation Guide*.

Once you have performed this basic configuration, the Configuration Change Console user interface provides access to the tools that you will need to analyze changes, configure notifications for critical events or changes, and generate regular reports.

Table 1–2 Post Initial Setup Steps

After Initial Setup	Details
1. Provide basic configuration information about your IT infrastructure: People, Teams, Devices, and Device Groups.	See Chapter 3, "Setting Up the Environment".
2. Define monitoring and compliance policies and apply them to components and devices. When a component is applied to a device, it is called an instance.	See the following sections in this User Guide: Chapter 5, "Operations Management"and Chapter 8, "Configuring Threshold Monitoring"
3. Set up application to provide a logical view of your component instances.	See Section 5.7, "Step 5: Applications"

1.2 Accessing the Console: User Accounts

Use a web-based interface, such as Mozilla Firefox or Microsoft Internet Explorer, to log on to the Configuration Change Console application. Initial access is available using a default administrator account. When installing the server, you were prompted for a password to use for this account.

Administrator: Has full privileges for all policy configuration and application administration. This account cannot be deleted, renamed, or have its administrative privileges revoked. This account name is in lower case.

The user interface supports different roles corresponding to the ways that users may need to interact with the application. New user accounts can be created with the following roles:

- Super-administrator (full access to all configuration, including team support assignments)
- Administrator (full access to policy configuration for devices visible through team support assignments)
- Regular (view-only privileges for collected change events; no access to configuration screens)

For details on adding users, see Section 3.1, "Configuring People and Teams".

Once you have successfully logged in, you will be taken immediately to the top level dashboard. For details, see Chapter 2, "About the Dashboard".

1.3 Configuration Change Console Architecture

The Configuration Change Console is built on a distributed architecture. Lightweight agents installed on servers in the IT infrastructure serve as data-collectors. Events collected by the agents are sent to a set of central servers and populate a time-based information model stored in a back-end Oracle database. The server hosts the compliance applications, providing access to a web-based user interface for data analysis, solution configuration, audits, change notification, and integration with change management systems.

Figure 1 - Configuration Change Console Architecture

The overall architecture is J2EE-compliant, incorporating an Oracle database and a web application server with Java Servlet and Java Server Pages (JSP) technologies. This open, standards-based architecture integrates easily into complex IT environments.

As shown in Figure 1 - Configuration Change Console Architecture, several major components comprise the solution:

- Agents on Managed Devices
- Database
- Application Servers
- Messaging Servers

1.3.1 Configuration Change Console Agents

Agents are lightweight processes that perform data collection on managed servers by interacting with operating system, security, database, and other system interfaces. Agents can perform the following tasks:

- Collect information about specific files, processes or user accounts
- Track changes to the contents and structure of databases
- Monitor message queues
- Track Windows Registry and Active Directory changes
- Gather performance and inventory information (such as CPU usage and memory capacity).

Agents are available for servers running the Windows Server, Windows NT, Solaris, AIX, HP-UX, Linux, and OS/400 operating systems. The *Enterprise Manager Configuration Change Console Installation Guide* will outline the versions of each operating system that is supported.

Agents aggregate and compress data for transmission to the database server. You can pause, resume, stop, and even upgrade agents remotely from the server.

1.3.2 Configuration Change Console Database

Configuration Change Console uses an Oracle database to maintain the time-based information model of infrastructure events and information, serving the graphical user interfaces as well as the reporting capabilities of the solution.

The database size depends on the number of managed infrastructure components, the number of changes monitored on those components, and the retention periods for the data. These factors are controlled by monitoring and application policies.

1.3.3 Configuration Change Console Application Server

Each installation has one master application server that presents the graphical user interface for configuration, review, and reporting. This interface is accessible using any standard browser. In addition, some installations may have one or more secondary application servers that manage the gathering of data from the agents and population of the time-based information model. For small deployments or low change volumes, you may not need a secondary server.

For information about administering the Configuration Change Console infrastructure components, see Chapter 12, "Administering Servers and Agents".

1.3.4 Configuration Change Console Messaging Broker Server

In a clustered environment where you have one primary server and one or more secondaries, there will also be one or more Messaging Broker Servers that facilitate the bidirectional communication between the agents and the servers. All communication goes through these messaging brokers rather than agents talking directly to the primary or secondary server. In a simple non-clustered environment where you only have the primary server, the messaging broker is bundled in with the primary server.

For information about administering the Configuration Change Console infrastructure components, see Chapter 12, "Administering Servers and Agents".

1.4 Using the Configuration Change Console Interface

The Configuration Change Console offers a graphical user interface that lets you browse compliance and change information. This section describes the user-interface features that are common among the many functions of the product.

Agents, installed on managed devices, collect and update the information from the infrastructure. Visualization screens provide views of this collected data. You can specify the types of changes you want to see for specific time periods and for specific portions of the infrastructure. The interface then displays the requested information, with drill-down details on each detected change. Likewise, on configuration screens, you can specify which files, processes, or applications to monitor on which devices.

1.4.1 User Interface Language and Locale

The Configuration Change Console interface supports the following 10 languages:

- English [en-US]
- Japanese [jp-JP]
- Italian [it-IT]
- French [fr-FR]
- Spanish [es-ES]
- Brazilian Portuguese [pt-BR]
- German [de-DE]
- Korean [ko-KR]
- Simplified Chinese [zh-CN]
- Traditional Chinese [zh-TW]

This only includes the user interface for the product. The online help is only available in English. Any content for events detected from an agent will be stored in the language of the server/software the agent is monitoring. Any user entered content in the UI will be stored in the repository in that language without translation.

To choose the language that you want to use, set your browser language and locale to match one of the above supported languages.

There is a global language and locale setting that is used by the server for things that are generated that are not tied to a user's session. These include some pre-generated reports, notifications and things that are not tied to the user interface. This language and locale is set depending on the primary server installer language you use. You can also change the setting in the repository at a later time if needed. See the Server Configuration Properties appendix of the Configuration Change Console Installation Guide for instructions on which property to change.

1.4.2 Navigation Conventions

The user interface displays tabs that organize the tasks by function. When you click a tab, a number of task links appear, enabling you to drill down to a specific task.

Throughout this book, a navigation path is provided so that you can easily reference the steps to access a particular task screen.

Example: *Administration --> Server Configuration --> Devices*

In this example, Administration refers to the label on the tab that provides the entry point to a series of functional tasks.

1.4.3 Moving Between Screens

To navigate to different screens, use one of the following methods:

- Use your browser's back and forward arrows to move to the previous and next screen.
- Click on an underlined link to jump immediately to a screen displaying information or configuration options for the selected item.

1.4.4 Accessing Online Help

Two types of online help are available:

- Help tab: To access the table of contents for the full set of online help, click the Help tab in the toolbar at the top of the screen.
- Context-sensitive help: Available from each screen; click on the question mark icon to view detailed descriptions of the screen's configuration parameters.

Just like the language settings for the user interface in general, the language and locale of the online help that will be shown when you access help will be dependent on what locale and language your browser is set to. This setting will be detected and used to determine which content to display on the screen.

1.4.5 Applying Filters to Displays

Most screens provide filters that allow you to more narrowly define the information of interest to you. Many of the screens allow you to specify date ranges and other filters to limit the information. In general, we suggest that you use timeframes to focus on the information you want. For example, in the following screen you would enter the

time frame and scale (Month, Day, Hour, 15-Minute) and click **Apply Filters**. When moving from screen to screen, some of the most commonly used attributes are retained to make it easier to move to different screens without having to select the items from the filter bar again. For instance, device group, devices, and time scale are all examples of filter options that will be retained as you move from screen to screen.

Figure 2 - Example of Filtering the Data Displayed on a Screen

2

About the Dashboard

Dashboards provide a high level view of how changes in your environment are affecting your compliance policies and controls. The top level dashboard shows a series of dials that relate to a policy. All of the displayed dials belong to the same Framework. By default, a *Generic* framework with its own policies and controls comes packaged with the product. You can configure Frameworks, Policies and Controls to mimic the compliance structures used in your own organization like PCI, COBIT, ITIL, COSO, and so on.

Each policy dial has an associated Details link, described later in this chapter.

2.1 Frameworks and Policies

From the top level dashboard, select the Framework that displays the policy for which you want to see a report.

The default framework that ships with the product is called the Generic Framework. It is a starting point that you can use in creating your own framework. The following predefined policies exist in this framework:

- Change Management
- Configuration
- Database Management
- Direct Access
- Emergency Change
- IT Operations
- Segregation of Duties
- Network and Security

This top level dashboard will display one dial for each of these policies of the selected framework. Each policy consists of one or many controls. It is the changes that are made against these controls that result in a good or bad value being displayed for the policy dial.

To modify or create a new framework, go to *Policy --> Policy Management --> Framework*.

2.2 Understanding the Policy Summary Portlet

The Policy Summary dashboard portlet displays several pre-defined policies with status gauges.

These gauges or dials provide a summary view of a policy's performance, as defined by configured thresholds. Each colored section remains fixed at one-third of the dial, while the needle moves to reflect the current status as it relates to the thresholds that have been configured for the policy.

If you do not integrate with a Change Management system, the Configuration Change Console calculates the gauge settings by using a rolling average, taking into account the number of days during which change has occurred and also the number of changes during that timeframe. This rolling average for a known time period is called a *baseline*. The dashboard automatically develops an internal model of your pattern of operations, based upon observations taken over the period of operation. When the system is first deployed, Configuration Change Console begins to generate the historical model. Within a short period of operation (days or weeks), the system begins to understand the site's patterns and then responds accordingly, setting the needle to represent a deviation from the baseline.

If you are integrating with a Change Management system, the dials will represent percentage of unauthorized activity as detected through the Change Management reconciliation. If you have a Change Management server integrated, you can also change this Policy Summary portlet to be based on a baseline view in addition to the CM View.

Use the Dashboard Threshold Configuration screen to establish the thresholds for the dials, You can access the screen by navigating to *Administration --> Server Configuration --> Dashboard Threshold Configuration*.

2.3 Viewing Policy Status Details

A policy represented by a single dial in the top level dashboard's policy summary has additional data that can be accessed by clicking on the *Details* link in the heading of the dial portlet. Clicking on this link takes you to the second level dashboard where you will see additional change details.

2.4 Top-Level Dashboard Status

The main Monthly Control Status dashboard displays several additional graphs and lists. The panes to the right of the screen categorize relevant summaries and enable access to more detailed information.

2.4.1 Alerts

To the right of the Policy Status portlet, a status box lists the five most recent and highest priority notifications. Click a specific alert to drill down to the next level of detail, the Notification Log.

The *Notification Log* includes an ID number followed by a message describing the activity. For example:

File c:\finance\bin\copy of personnel_details.txt of application GlobalPayroll on device CorpHR was modified by user ultrabiz\thomas.obon at 08/16/2006 22:18:17 GMT (Local OCC Time 08/16/2006 15:18:17 PDT)

This message includes:

- Object Type - Lists the type of event that triggered the alert, such as file, process, or user login
- Application - Denotes the specific application that was affected

- Action - Describes the activity related to the object type; for example, created, modified, or logged in
- Time - Lists the time the event occurred

2.4.2 Most Active Applications - Today

The current day's most active applications are listed, along with associated event counts. Only applications that have been explicitly created for your environment will be shown in this list. For details on configuring an application, see Section 5.7, "Step 5: Applications".

Click on a specific application to view the Applications screen so that you can access the details.

2.4.3 Total Events

A graph at the lower right side of the Policy Status portlet displays the total events for the current day.

2.5 Second Level Dashboard Tabs: Control, Application, User, Device

Clicking on the Details link for a specific policy from the top level dashboard takes you to the second level dashboard. For the selected policy, several charts and graphs that provide an at-a-glance view of the data are shown. Just below the Change Status pie chart, four tabs enable access to change and compliance summaries organized by Control, Application, User, and Device.

To access this screen, navigate to *Top Level Dashboard --> Policy Dial Details link*.

Change Status Pie Chart. The green area of the pie chart shows the percentage of all events that are authorized, while the red area represents the percentage of all events that are unauthorized. Not Audited events are not shown in the pie chart. If you do not have a Change Management system, this pie chart is not shown.

Authorized/Unauthorized Changes Charts. The blue line on each column chart represents a rolling average for the selected time range. If you do not have a Change Management System, this blue line is flat, reflecting the baseline value for the entire range.

Each summary contains a table related to the particular dashboard control. Click on the column headers to sort the values from highest to lowest or to toggle back to a lowest-to-highest sorting order.

2.5.1 Control Summary

A control has a mapping to a component, which can be further expanded to reveal all the instances associated with the control.

- **Control** -- Click a specific link in the Control column to display the Application Event Visualization view associated with the application group.
- **Status** -- If you have a Change Management system, such as Remedy or Peregrine, the status column is calculated as:

  *status % = authorized/(authorized + unauthorized) * 100%*

  Any "not audited" events are not included in this calculation. If you do not have a Change Management (CM) system, the Authorized, Unauthorized, and Not Audited columns will display a "-" and the status is calculated as:

*status % = (count/baseline - 1) * 100%*

Note that without a CM system, the status percentage could be negative, depending on how the count deviates from the baseline value.

Refer to the legend to evaluate the symbols shown in this column.

- **Count** -- The Count column simply displays the total number of events associated with each control; for example, the number of Database Privilege Changes. This data is collected by a configured agent.
- **Authorized/Unauthorized/Not Audited** -- If you do not have a Change Management system, the Authorized and Unauthorized events columns will not be displayed. If you have a Change Management system, the count of each will be shown in the table and the status column will show compliance percentage based on percentage of authorized events.
- **Baseline** -- This baseline value represents an average of event counts and does not relate to authorized, unauthorized, or unaudited events. The baseline value is the number of events typical for a given period. For example, if you are viewing a month of data, the baseline is the number of events that will be expected to occur during the range this view covers depending on your scale setting. Likewise, for days, the baseline is the average count of events by day, for all days in the range.
- **Priorities and Baseline Score** -- If you have a Change Management Server, you will see columns labeled Priority 1, Priority 2. These priorities are related to Audit Actions. When an audit action is created, a notification priority is assigned to it. The Priority counts shown in this table reflect the number of events (process, file, login/logout, component internal) that are mapped to an audit action with the associated priority.

2.5.2 Application Summary

The Application Summary table lists active application groups, along with a total row. Each row in this table represents an application. The values shown with an application represent the data collected from the component instances associated with the application. Component instances that are not associated with an application are not included in these values. If a component instance maps to two different applications, the events are counted in each of its application rows in the table.

Except for the first column labeled Application, the other columns contain data as described under Section 2.5.1, "Control Summary".

2.5.3 User Summary

The User Summary reflects all changes by the listed users: file, process, application internals, and logins/logouts. Except for the first column, labeled User, the other columns contain data as described under Section 2.5.1, "Control Summary".

2.5.4 Device Summary

The Device Summary table lists counts associated with the five most active device groups that contain component instances. See Section 2.5.1, "Control Summary" for column details, except for the first two columns:

- **Device Group** -- Click a specific link in the Device Group column to display the Server Event Visualization view associated with the application.
- **Control Instances** -- The Control Instances show two numbers: X of Y, where:

Y, the number of all component instances that exist on all devices of the group.
X, the number of those instances that are part of the control because their components are assigned to the selected control.

> **Note:** Because this table represents a subset of the entire group, as noted in the Control Instances column, the counts reflect a percentage of the instances within the device group.

2.5.4.1 Most Active Users

The Most Active Users summary lists the five most active users for the current day, their associated direct access application or operating system, and the count of events. This list provides a view of changes across all devices and applications by a specific user name. Click on a specific user to display details via the User Event Visualization screen.

2.5.4.2 Account Management

This list shows a summary of the account changes in the current day. The counts reflect the number of user accounts that were added, deleted, or modified.

2.5.4.3 Database Management Summary

This summary provides a basic list of database user activity for the current day: Users added/deleted, changed privileges, and the average session length.

The Most Active DBAs summary lists the five most active Database Administrators for the current day, along with an event count for each. The event count is a sum of the change counts for database internal changes and the login/logout events.

2.6 Change Management Portlets

To enable adherence to IT Best Practices, you must be able to validate actual changes against approved change orders. The Change Management Portlets at the bottom of the second level dashboard help provides at-a-glance change status, with access to detailed views.

The data that is displayed depends on your particular environment. If you do not have a Change Management System, these portlets will not contain data. If, however, you have a Change Management System, you will see a rich set of graphs summarizing change activity.

- **Planned Changes - Next 7 Days** -- This column chart shows future changes based on open tickets and the planned end time of those tickets. Emergency tickets are also factored into the counts since they have a planned end time. The chart represents seven days, starting with the current day at 12:00 a.m.
- **Ticket Details** -- This chart displays the current counts for the following ticket states:
  - New - tickets that are open and do not have any authorized changes associated with them
  - Initiated - tickets that are open and have had at least one change authorized against them
  - No Changes - tickets that are now closed and had no changes authorized against them

  - Emergency - tickets that have an emergency status, but are not yet approved
  - Emergency/Approved - emergency tickets that have been approved
- **Resolution Time - Hours** -- This chart augments the Ticket Details graph. Use this chart to evaluate your organization's responsiveness to change tickets. The resolution times take into account a ticket's planned start time until one of the following activities occurs:
  - First Change - The time is calculated from a ticket's planned start until the ticket's first authorized change event. The resolution time is an average of all tickets that match these criteria. For example, 8.4 hours means that all tickets, from create time to first change time, have an average resolution time of 8.4 hours.
  - Last Change - This category represents the time from "ticket planned start" until "last authorized event."
  - Emergency Ticket First Change - This is similar to First Change, but for emergency tickets only.
  - Emergency Ticket Last Change - This is similar to Last Change, but for emergency tickets only. For this count, emergency tickets must fit the following criteria: emergency ticket was approved and closed OR the emergency ticket is still open.
  - Emergency Ticket to Ticket Approval - This count represents an emergency ticket's time from planned start (or creation) until the ticket was approved.
  - Ticket Close - This resolution value is simply derived from ticket open to ticket close times.
  - Last Change to Close - This value is derived from the time of the last authorized event until the ticket close time.

3

Setting Up the Environment

When initially configuring the Configuration Change Console, you must specify both the hierarchy of people who will use the solution and the grouping of your infrastructure's managed devices that will be monitored by the solution.

- People: Defines the members of your organization, including their reporting responsibilities and the teams of the organization that interact with the IT infrastructure. By default, you have only the one default account, *administrator*.
- Infrastructure: Configures the managed devices and their groups. By default, every device with a Configuration Change Console Agent will appear in the interface automatically. Device groups can be created through the interface and are useful for simplifying reporting and configuration.

Once you have defined these elements, you can start defining the policies for monitoring and managing change in the IT infrastructure.

Configure the environment by clicking the Administration tab and then selecting the relevant tasks under People and Devices.

3.1 Configuring People and Teams

The individuals in your organization may interact with Configuration Change Console monitoring policies and the IT infrastructure in many ways as described in the sections below.

3.1.1 People

The term *people* refers to individuals in your organization who can log in and view data within the Configuration Change Console using a configured username and password. The term *user* refers to the individual user accounts detected by Configuration Change Console Agent on managed devices. Configured people may or may not be associated with one or many detected users, and vice versa.

3.1.2 Teams

People comprise a *team* that is responsible for a given set of infrastructure components. Each team should have responsibilities that are distinct from other teams. For example, one team may administer production machines while another manages development machines.

Teams should mirror your organization's operations. Some organizations may find it beneficial to create teams based on geographic locations, while others may create teams for functional areas. Team assignments are used in the routing of notifications

when escalations are required, and can be used to limit the view of devices and data individuals can access.

3.1.2.1 Configuring People

Use the People screen to view, update or add user information.

You can display this screen by navigating to *Administration --> People --> People*.

If you already have defined people in the interface, they will appear in this view. If you are just beginning, this screen will include only the default account.

Login Name is the name used to access the Configuration Change Console interface. This link takes you directly to the *Add or Update a Person* screen to modify the individual's information.

Primary Email Address is the email address used for notifications. Click this link to add or update an email address for the individual.

User Assignment allows you to map individual people in your organization to detected user accounts on monitored devices.

- To add a person, select the **Add Person** button to access the *Add or Update a Person* screen.
- To update a person, click on the person's link in the *Login Name* column to access the *Add or Update a Person* screen.
- To update a user assignment, click the number link in the *User Assignments* column to access the *Add Person to User Assignment* screen to add or modify user assignments

3.1.2.2 Add or Update a Person

Use the *Add or Update a Person* screen to view, update or add user information.

To get to this screen navigate to either *Administration --> People --> People --> Login Name link* or *Administration --> People --> People --> Add Person button.*

- *Account Information* -- Name, password, and email address are required. Supports Long Messages is selected by default, signifying support for messages greater than 252 characters. If a person's address will go to a cell phone or a similar device, uncheck this box.
- *Locale Settings* -- Select the country, language and time zone from the pull-down menus.
- *Organizational Settings* -- Select the Manager from the pull-down menu and check the appropriate teams from the available selections. Managers are used when routing escalations for notifications. If you have not yet defined teams, the team settings will not be available.
- *Product role* -- The following product roles are available:
  - Regular: A person with access to all features except configuration features. Every person must have at least a Regular product role.
  - Administrator: A person with access to all features. View of some devices may be limited through the Team Support Assignment.
  - Super Administrator: A person with access to all features.

Click **Save** to save your changes or **Cancel** to exit without saving changes.

Note: Changes to a person's role and team settings will take effect the next time the person logs in.

3.1.2.3 Person to User Assignment

The *Person to User Assignment* screen allows you to map individual people in your organization to detected user accounts on monitored devices.

Warning: It is extremely important that you do not map the Windows domain Administrator account or root account to a user in the *User Assignments* screen.

To get to this screen, navigate to *Administration --> People --> People --> User Assignments link*.

The following fields are described below:

- Username -- The user account
- Device -- The devices where the user account exists
- Component -- Component on which the user account exists

Click **Modify Assignment** to select or de-select users on devices.

3.1.2.4 Configuring Teams

The *Teams* screen provides details about any configured teams. Use this screen to add a new team or modify existing team information, including team membership.

To get to this screen, navigate to *Administration --> People --> Teams*.

To add a team, click the **Add Team** button. To update a team, click the link under the Team Name column. Either way, the *Add or Update a Team* screen will be displayed.

Enter a team name and select an administrator. The Team Administrator is specified primarily for company record-keeping, but also serves as the final escalation point for notifications associated with the team.

Once you have created a team, click its associated Members link in the Teams page to display the *Edit Membership* screen.

Note that all current team members are displayed in bold with a marked checkbox.

To edit Team Membership, follow these steps:

1. Select or unselect members from the available list
2. Click **Save** to save changes or **Cancel** to exit without changes

3.2 Adding Managed Devices and Device Groups

Once you have created People entries, you must identify the servers (managed devices) that will be monitored. The following sections describe this process.

3.2.1 Adding and Updating a Managed Device

New managed devices are automatically added to the server following a successful agent installation. You can verify a successful installation, as well as review the list of all managed devices, from the *Devices* screen.

To get to this screen, navigate to *Administration --> Devices --> Devices*.

You can modify the agent status, such as pausing and stopping an agent, from this screen by clicking the link under *Agent: Last Known State*. For additional information about remotely managing agents, see Chapter 12, "Administering Servers and Agents".

Note: Devices can be added manually using the *Add a Device* button. It is recommended that you do not manually add a device unless specifically directed to do so by technical support for resolving an issue. Installing an agent with a pre-determined agent ID will require additional manual steps to be performed after installation.

To review or modify device details or to delete a device, click the link in the Device Name column in the *Devices* window. The *Add or Update a Device* screen is displayed. Use this screen to add or modify a device, or to delete a managed device. When you save changes, the Devices screen will reflect the changes you have made.

To add or update a device, enter the following fields:

- *Type*. Device type. Currently, only servers are supported.
- *Operating System*. Operating system of the device. Note that no matter which operating system you use, if the agent detects a different OS, it will automatically adjust this setting.
- *Device Name*. Name assigned to the device. If you change this value, the agent will change it back to the real device name next time the appropriate message is received from the agent.
- *OS Instance Name*. The instance name can be a descriptive title for the OS. For example: Win2k Server SP3.
- *Owning Team*. Select the team, if any, that owns this device. This is for reference only and does not affect any configured rules in the system.
- *Device Groups*. Select the device group(s) to which this device belongs.
- *Asset Tag*. Enter an asset tag (if appropriate) and a description for the device. Note that asset tags serve as the integration point with a Change Management server. The asset tag specified here will be compared to the device asset tag in the Change Management server.

Click **Save** to save changes, or **Cancel** to exit without changes.

To delete a device, click the **Delete** button. Upon subsequent restarts of the device, the agent on the deleted device will be stopped by the server. You must uninstall the agent manually from the managed device, as this delete action does not uninstall the agent.

Note: If the managed device (on which the agent is installed) is restarted, and the old agent has not been uninstalled, the old agent will restart and continue to send unwanted messages to the server.

3.2.2 Adding or Updating Device Groups

IT organizations often classify servers to form logical groupings based upon shared characteristics, such as operating systems, server types, or geographical locations. By grouping managed devices, you can apply device policies to a group of devices,

thereby simplifying management and reporting of changes across complex or large IT infrastructures.

Managed devices can belong to one or more *device groups*. Groups are used to sort change-management data based on user-defined associations. For example, to simplify retrieval of change data for a group of devices, you can group all web servers under a parent group, or group all of the components that comprise a specific distributed application.

Device groups are hierarchical. One device can belong to one or many groups, but each group can have only one parent. For example, you can group all web servers under a parent group called Production Servers. In fact, you can represent your organization with multiple "generations" of parents, as shown in the following example:

Continent --> Country --> Region --> Organization --> Production Servers --> Device

The following are device group attributes:

- A device can belong to any number of device groups
- A group can have only one direct parent
- Multiple parent levels (generations) can be used to represent your organization

The screens for Device Group management and related activities are all accessible from the following navigation path: *Administration --> Devices --> Device Groups*.

The *Device Groups* screen displays all defined device groups. Use this screen to add or update device groups. Note that the device counts listed indicate device membership within the listed group only; they do not factor in devices belonging to any member child groups.

To get to this screen, navigate to *Administration --> Devices --> Device Groups*.

To add a new device group, click **Add a Device Group**. To modify an existing device group, click on the link in the *Group Name* column. Either way, the *Add or Update a Device Group* screen will be displayed, enabling you to create new device groups or edit the membership of an existing device group.

Use this screen to add, modify, or delete a device group.

> **Note:** If you delete a group, the devices that belonged to that group will be unassigned from the group. If the group selected for deletion has sub-groups, those groups will become sub-groups of the deleted group's parent. If no parent group exists, those groups will become independent, without parent affiliations.

Enter the following Device Group information:

- **Group name** -- Enter a meaningful name for this group
- **Parent Group** -- Select from the drop-down list of existing groups

Click **Save** to save changes or **Cancel** to exit without changes.

After creating a group, you can change the devices that belong to a group from the *Device Groups* screen. Under the column Devices, clicking on the count of devices in the group takes you to a screen that lists all devices currently in the group. From this screen you can select devices and remove them from the group in bulk.

Note: You cannot remove a device from a group if it does not already belong to another group. A device must always belong to at least one device group.

Clicking on the *Modify Device Assignments* button will take you to a screen listing all of the devices filtered by group in the filter bar. By default, all devices are added to the group called *Default Group*. To move the device to another group, you would choose Default Group on this screen, select the devices you want to add to your group and click Save. The devices will now belong to both default group and this new group. You can now go back to the default group and remove these devices from that group.

The *Modify Device Assignments* screen has a selection helper at the bottom of the device list to make it easier to select many devices at once. You can use various filters to select or unselect all items based on some starting text, ending text, or containing text.

3.3 Assigning Teams to Managed Device Groups

By assigning teams to managed device groups, you can restrict which device group team members can access when using the Configuration Change Console. This feature limits the device groups on which team members can administer policies and view change event data. For example, when viewing data on relevant *Event Visualization* screens, if the Finance team is assigned the Finance device group, then members of the finance team will only see changes that are detected on device groups belonging to the Finance device group. Note that users with Super Administrator privileges can access all device groups.

To get to this screen, navigate to *Administration --> People --> Team Support Assignments*.

To view current team assignments for a device group, click the associated link in the *Number of Teams* column. To add a team assignment, click **Add Assignment**.

Note: To Add a Team Support Assignment you must have an available, unassigned team configured.

To add a new team assignment, enter information into the following fields:

- *Team*. Select the team from the pull-down list.
- *Group*. Select one or more device groups, if shown, or select and expand device groups to select specific device groups. When doing this assignment, only the device groups that are in the group at the time you make the assignment are actually assigned. If you change the group membership, you must return to this screen and edit the assignment and save again for it to pick up the group changes.
- *Time Window*. Optionally, select the Time Window during which the team is allowed to access the device group, for documentation purposes. Currently the only available time window is *Always*.

Click **Save** to save changes or **Cancel** to exit without changes.

After assigning teams to device groups using *Team Support Assignments*, you must enable the *Team Device Limiting under Administration --> Server Configuration --> Team Device Limiting* screen for the limits to be put in place. Any user that has the Super Administrator product role will see all device groups, while any user that only has regular or administrator product roles will only see the device groups their team is allowed to see under *Team Support Assignments*.

3.4 Validating Team and Device Group Assignments

Once you have defined the people, teams, devices and device groups, you can verify the accuracy of the definitions and assignments.

To identify any unused teams, navigate to *Administration --> People --> Validate People Assignments*. This displays a screen listing elements within the monitored environment that have been created but remain unused; for example, teams without members.

From this screen you can click on a count link to jump to the appropriate details screen, where further information can be viewed and assignments corrected, if needed.

3.5 Working With A Large Environment

There are some considerations to make when working in a large clustered environment with more than 1000 agents. In these situations, there are various ways to organize your configurations to make them easier to manage and to make the UI work faster.

3.5.1 Device Groups

When you have a large number of agents, it is recommended that you create a device group structure to break these sets of devices down into more management groups. Although you can put device groups inside of other device groups, it is recommended that at a top level device group, you do not have that group containing more than 1000 devices (in that group or any group under that one).

For instance, you might have a structure like this:

```
West Coast Production group  (contains  900 total devices summing up all child
groups)
     North                   (contains 300 devices)
     Central                 (contains 300 devices)
     South                   (contains 300 devices)

East Coast Production Group - 900 total devices summing up all child groups
     North                   (contains 300 devices)
     Central                 (contains 300 devices)
     South                   (contains 300 devices)
```

If you had a group say, West Coast Production Group > North that had 2000 devices in itself, it would be better to organize multiple top level groups where each group had no more than 1000 devices.

When a device is added to the server through an agent connecting the first time a server, it will be put into the group called "Default Group". After this, you should add the device to a group that fits into the desired grouping model and then remove the device from the Default Group. A device must belong to at least one group. You cannot remove a device from a group without first reassigning it to another group.

3.5.2 Team Support Assignments

Once your group structures are understood and you have set up your device grouping so that each top level group has at most 1000 devices under it then you can create what is called a Team Support Assignment where you assign a different CCC team to each group. Team Support Assignments are discussed earlier in this chapter. You may have one set of IT people that only deal with one group. If you configure the team support assignments and turn on Team Device Limiting (Server Administration option) then

when a person in that group logs in to the Configuration Change Console interface, they will only have to look at the information related to the devices in their teams.

Even if you have one person that manages all devices, you might want to consider using team support assignments where that one user has multiple Configuration Change Console people accounts to log in to see the view for various devices independently of others.

3.5.3 UI Screen Scaling

Some screens in the Configuration Change Console product will have slightly different behavior if your instance has more than 1000 devices. This is a built in trip point where screens will behave differently to handle the larger number of devices. The most common behavior change is that on some screens you can only choose device groups when looking at data/managing configuration rather than individual devices.

In screens that normally might have ALL as a filter option in the Device Group filter, this option for ALL will go away once your agent count has reached a size where there would be too many devices to show in the screen. After this point, you would have to select a specific group instead of being able to filter on all groups.

4

Understanding Policy Configuration

Configuration Change Console responds to infrastructure changes according to component and audit action definitions. The rule sets that you define for a component will depend in part on how you are using the product. You can define rule sets for different uses and enable or disable them as needed. Audit actions define what actions you want to occur when an event takes place for a component.

Use components and audit actions to:

- Monitor and report on critical infrastructure or application files, processes, databases or internal components. You can use the user interface to generate reports to analyze this information.
- Respond to specific events or states on monitored infrastructure objects through the help of system-generated notifications and reports.
- Audit changes against a change management solution to identify approved and unapproved changes to the infrastructure.

4.1 Rule Set Types

Configuration Change Console provides two rule set types for monitoring different elements of your infrastructure.

Table 4–1 Rule Set Types

Rule Set Type	Use to Monitor:	Configure these Configuration Change Console Objects:
Component Rule Sets	Specific configuration items for an application such as your CRM, ERP, HRIS application. A component rule set includes the specific configuration that needs to be monitored: name and version of a component, operating system on which it runs, and a list of internal and/or external rules where changes may be made by the application.	*Component*: A granular part of a larger business application such as a database, application server, patch. *Rule Sets*: The types of data you want to monitor as part of this component; for example: files, processes, database changes, etc. *Rules*: A set of items to monitor for each rule set. *Application*: Collection of component instances that together represent a complete business application.

Table 4–1 (Cont.) Rule Set Types

Rule Set Type	Use to Monitor:	Configure these Configuration Change Console Objects:
Threshold Rule Sets	Critical thresholds or events on managed devices	Threshold Rule Sets monitor specific resources such as CPU usage, system log errors, database errors, and user activity.
	A Threshold Rule Set enables you to take action when activities and events exceed your specified thresholds.	For details, see Section 8.1, "Understanding Threshold Rule Sets".

4.2 Data and Events to be Monitored

Before defining policies, you need to identify what you want to monitor. Keep in mind that your goal is to collect data in order to monitor potential deviations from compliance and change management policies. The amount of data collected by the agents affects the size of the Configuration Change Console database and the responsiveness of reports and interactive displays.

In deciding what to monitor, consider the purpose of the policy:

- Critical application components: Select critical configuration files, operating system parameters, and tables that define application operations. Multiple policies can be used to monitor the same application when the information collected must be segregated for notification, reporting and auditing purposes.
- Control points: Compliance policies typically monitor a few well-defined control points identified through an external compliance exercise.
- Infrastructure: Troubleshooting policies may monitor a broader set of components and may be enabled only when there is instability in critical applications or infrastructure.

Note: To prevent extraneous data from being collected, certain events should never be monitored. For example, if you choose to monitor log files that undergo constant change, you potentially will store an excessive amount of unnecessary data in the Configuration Change Console database.

4.2.1 Monitoring Applications

Use Applications to classify how various defined components fit together to make a business application. Applications allow you to combine elements running on different operating systems to give a view of your changes as they relate to your business applications. For example, a customer order-processing application might include an Oracle database instance, an application server instance, a messaging system, or a firewall. The individual elements in this case are called components. These components could be grouped into an application that represents the customer ordering application.

A component instance can participate in multiple applications. This can prove useful for reporting and management purposes. In the above example, the Oracle instance for the customer order-processing application might also be part of the Finance application.

Tip: Decide on a naming convention before naming components or applications. Make sure the name provides an indication as to the purpose of the component and application. This will make managing the Configuration Change Console product much easier.

5

Operations Management

Operations Management relates to the configuration aspects of the Configuration Change Console that relate to your physical infrastructure and how it should be monitored. This is opposed to Policy Management as discussed in Chapter 6, "Policy Management", which relates to your Compliance Policy frameworks, policies and controls.

Configuration Change Console enables you to monitor and audit essential application components, detecting and reporting changes to application infrastructure through assigned application policies.

Operations Management configuration consists of the following elements:

- *Component* -- Specifies important files, processes, databases and internal objects to monitor in an application. These monitoring points may be common across many different instances of the application in the infrastructure. For example, a component for an Order Processing application would identify specific files and processes that should be monitored for changes.
- *Component Instance* -- When you assign a component to one or many monitored devices, each of these assignments is called a Component Instance. A single component can be mapped to one or many devices depending on what the purpose of the component is. For example, you may define a component such as an antivirus program that should run on every server in your environment. Each of these is considered a component instance.
- *Application* -- Once you have assigned components to managed devices, you can create applications comprised of those component instances. Applications help you monitor, report, and manage change data for many components that make up the business application. For example, the Order Processing application may require a database, application server, and web server to run. All of these components can be designated in the Order Processing Application to simplify reporting.
- *Audit Action* -- An audit action defines various actions you want the server to perform when an event for a given component or application occurs. Among the actions that can be configured are email notifications, SNMP traps, report generation, and annotations being sent to an integrated Change Management System.

> **Note:** If you are integrating with a change management system to detect authorized and unauthorized events, you must perform additional configuration steps, described in Chapter 7, "Integrating With A Change Management Server".

Before defining components, you will need to decide:

- What files, processes, and internal objects to monitor in each component (Rules)
- How do these file, process, and internal objects relate to each other? Are some important because they are critical configuration files? Are some important because they are processes that must always be running or users that should never be accessing a set of files? (Components)
- Which changes to audit and notify (audit actions)
- How to group component instances into applications to relate to your business application structures (for reporting, management and change analysis purposes)

When defining components, remember the following:

- You cannot mix operating system platforms within a single component. If an application has components with several operating systems, you must define separate components for each operating system's component. You can then group the different component instances into an application that represents the real world business application.
- A single component instance may be assigned to many applications. For example, you can group component instances by application/business function, by operating system, and by region.
- Only a single internal monitoring capability or agent module can be configured per component. This limitation is primarily to ensure that component definitions remain granular enough that reporting against the component instance is meaningful. The internal monitoring modules include:
  - Active Directory (Snapshot)
  - Active Directory (Trace)
  - Oracle 8*i* (Snapshot)
  - Oracle 8*i*/9*i*/10*g* (SQL Trace)
  - Oracle 9*i*/10*g* (Snapshot)
  - SQL Server (Snapshot)
  - SQL Server 2000 (SQL Audit)
  - SQL Server 2000 (SQL Trace)
  - Windows Registry (Trace)
- You may wish to alter components over time. For example, early in the Configuration Change Console's lifecycle you may monitor many rules in a component, while over time you may narrow the focus to changes that are relevant to compliance initiatives or change management processes. This tuning is an ongoing process and will become less frequent over time.
- A component can be very specific or can be very generic. For instance, you can have a component called Critical OS Files that is configured to monitor a set of files on every device in your entire company. This component would then be assigned and have an instance for every device. You may also create a component that is very specific, such as a component that defines a patch to one part of an application. For instance, if you have a Finance Application Server and you will be applying a patch to it, you can create a component to monitor the files that would change as part of the patch.

5.1 Steps for Modeling a Business Application

The following table provides a high-level view of the basic steps required to model the components and create applications in the product to resemble a business application that may be running in your IT environment. Detailed procedures are provided later in this chapter.

Table 5–1 Steps for Modeling a Business Application

Step	Task	Description
1	Create one or more components.	Create your own component or copy one of the predefined components that comes with the product for each part of your business application; for example: the database instance, application server, firewall, messaging bus, critical OS files, database tables containing sensitive data, application server security files are all examples of a component.
2	Choose the rule sets and specify the rules for each component.	You can monitor rule sets such as files, processes, users, and/or internal objects such as database tables. Note that certain rule sets require additional configuration parameters. For each rule set, you specify a number of include/exclude rules that control what is monitored as part of this component.
3	Map the component to managed devices to create component instances.	This step essentially applies the monitoring rules to specific installations of a related component, telling an installed agent what elements to monitor for changes.
4	Create an application to simplify management and reporting.	Logically group component instances by function. The application in this sense would be related to your business application, such as The Finance Application.
5	Define audit actions for component instances or the entire application.	If you are integrating with a change management system, these audit actions are created automatically once you configure the component and outbound ticket template. If you want to specify additional actions such as notifications, you can create additional audit actions or modify the ones that were automatically created.

5.2 Understanding Components

The first step in configuring the product to map to your IT organization is to understand the components that make up your applications and model those components. The component serves as a blueprint of the important elements involved in an application used within your environment. These components, once applied to running installations on managed devices, determine what monitoring will be performed by the agents.

Components identify operating system and application rule sets to monitor, such as:

- Files
- Processes
- OS Users
- Application-specific internal objects
  - Database Objects
  - Active Directory/LDAP objects
  - Other application objects

The Configuration Change Console provides a set of predefined components that include monitoring rules for various operating systems and applications (See Appendix A, "Predefined Component Templates" for a list.) You can use these predefined components as starting points, customizing them to suit your monitoring, compliance, or auditing needs.

You can create a single component and assign it to many instances in your environment. You do not need to specify your rules in multiple components. For instances where there are minor differences in rules, you can override the global settings for the component for a specific instance. You can configure as many components as necessary to model your applications in any of the following ways:

- Use a Predefined Component to create a Custom Component
- Add a Custom Component using the *Component* screen
- Import a Component created on another server or by creating the XML file manually

5.3 Step 1: Creating Components

Use the Components screen to create custom components for the applications you want to monitor.

To get to this screen, navigate to *Policy --> Operations Management --> Components*.

Several views are available from the Components screen:

1. Predefined Components - Displays components included with the product. All Predefined Components specify monitoring rules based on the input of industry-leading application specialists. Use them as a basis for custom components that meet your specific audit requirements. You cannot directly assign a predefined component to a device, you must save a predefined component as a custom component before using it.
2. Device View - Displays a list of devices showing the number of component instances associated with each device. Click the instance number link to see which components are assigned to the device.
3. Custom Components - Lists user-defined components. Components that were created by copying a predefined component are also shown here as they are also custom components.

Note: Only Custom components can be assigned to a managed device.

The Component screen provides a centralized entry point that enables access to key configurations. From the Component screen you can:

- View the predefined components by selecting **Predefined Components** from the *View* menu.
- View custom components by selecting **Custom Components** from the *View* menu.
- View all components you have assigned to a device from the *Device* View.
- Make a copy of a predefined component by clicking the component name link when in the predefined components view and saving it as a Custom Component. You can then customize the component to reflect any unique requirements of your environment.

- Edit the information for an existing component by clicking on the link in the *Component Name* column to display the *Add or Update Component* screen.
- Add custom components by clicking the **Add Custom Component** button to display the *Add or Update Component* screen.
- Define Rule Sets, which identify what types of data you will monitor as part of the component. Click the count link in the *Rule Sets* column to access the *Add or Update Component Rule Sets* screen.
- Create or modify Component Instances by assigning a Component to one or more specific devices. Click the count link in the *Instances* column to access the *Component Instances* screen.
- Define or modify Audit Actions to associate actions to take when an event occurs that is related to the component. Click the count link in the *Audit Actions* column to access this screen.
- Assign Controls to a Component. Controls are part of the Compliance Policy area of the product.

5.3.1 Add or Update a Component

The *Add or Update Component* screen appears when you choose to add or edit a template.

To get to this screen, navigate to *Policy --> Operations Management --> Components: Add Custom Component*.

1. Enter the following information:
   - *Component Type*. The type of component. (For new custom components only.) Select from all currently configured Component Types. Application Types can be created through the Add Application Type link on the Component listing screen that lists components.
   - *Component OS*. The platform on which the application is running. (For new custom templates only.) Once you create a component, you cannot change the OS because rules are dependent on the OS you chose when creating the component.
   - *Name*. A unique name that describes the component.
   - *Version*. The version of the component.
   - *Description*. An optional, brief description that explains the function of the component.
2. Click **Save As** if you are modifying a predefined component to save it with a new name, or **Save** if you are creating a new component or modifying an existing custom component. You can also use the **Save As** capability to make a copy of an existing custom component into another custom component.

5.3.2 Importing Components

An alternative to creating a brand new component is to import a component used on another server. For example, you can create and test your components in a development environment, and then export the components using the Export button on the *Components* screen. You could then import the component by clicking on the Import button on the *Components* screen in the production environment. Any components configured on a server may be exported by selecting the check box in

front of the components name and clicking the **Export Selected** button. Note that you can export all, or selected components through this method.

To import an Component:

1. From the *Components* screen, click the **Import** button. A pop-up dialog box appears prompting you to choose a file to import.
2. Browse to the location where the component XML is saved and click **Submit**.
3. A dialog box will indicate whether the file is a valid component for importing. Click **Continue Import** to finish importing the component.

5.3.3 Creating Custom Component Types

Custom Component Types can be created for use in Components through the *Component Types* screen. Creation of custom Component Types allows an organization to logically group the components used in their environment under classifications used in their organization.

To get to this screen, navigate to *Policy --> Operations Management --> Components --> Add Component Type link*.

The *Component Types* screen displays all currently configured Custom Components Types, including the description, creation date and time, and number of components currently using each custom type.

Table 5–2 Tasks on the Component Types Screen

Task	Action
View a filtered version of the Components screen, which shows only the Components currently associated with the Component Type.	Click the # of Components count link.
Modify the configured Component Type.	Click the Component Type's Name link.
Add a new Component Type.	Click the Add Component Type button to name a new type and provide a description.

When finished, click **Save**. The Component Type will now be selectable when filtering or creating Custom Components.

You can delete custom component types that you create, but not while there is a component using the component type. To delete a component type, you must first edit existing components and assign them to different component types first. Also, you cannot delete the Default component type that comes with the product. For component types that you cannot delete the delete option will not be available.

5.4 Step 2: Defining Component Rules

Once you have created a component, you need to choose Rule Sets to monitor and define the rules. Each component has a set of rules relating to the rule sets (processes, files, users, and internal objects) related to a component making up your business application. You can include or exclude up to 50 rule patterns per component Rule Set. To deal with larger number of rules per rule set, break your component up into smaller components. If your component is too large, it makes the reporting of events less meaningful.

Add the monitoring rules via the *Component* screen. To get to this screen, navigate to *Policy --> Operations Management --> Components*.

For a component:

- Select the link in the *Rule Sets* column to choose the **Rule Sets** and configure the rules for each set.
- Select the link in the *Instances* column to assign a Components to a device to create a running Component Instance.
- Select the **Audit Actions** link to configure and enable actions to perform when events tied to this component happen; such as notifications, sending SNMP traps, and so on.

The details for each type of rule set are described in the following sections.

5.4.1 General Monitoring Guidelines: Rule Sets

The following headings describe the various rule sets.

- Files -- Typically, organizations do not monitor files or directories that change during normal operation of the application (such as transaction logs), to prevent collecting unnecessary data. For compliance purposes, only monitor files that have a significant impact on the application's function or performance, such as configuration files or tables that define the operation of an application. Through monitoring file rule sets, you will monitor file changes in real time and be able to capture who made the change and some other attributes of the event. Changes to permissions are also monitored.
- Processes -- Configuration Change Console agents collect information about when monitored processes start and stop. Select processes that represent compliance control points, or for which a change in state (a process start or stop) represents exceptional activity in the environment. For instance, when the main process that is needed for your finance application stops, this would be an event you would want to know about.
- Users -- Configuration Change Console agents collect information about when OS users log on and off a machine, through both local, regular system log ons and external log ons such as telnet or ftp access. For this aspect of compliance, you should select users and/or connection methods associated solely with the application being monitored, thus providing a record of user sessions (starts and stops) for the application.
- Include/Exclude Rules -- Nothing is monitored unless it is first included in monitoring. You can start with a general include (include=*) and then start excluding elements you do not want to monitor, or you can make your inclusion rules more selective.

  The most specific include/exclude rule always takes precedence over a less specific include/exclude.

  If you define two conflicting rules for the same object or the same specific pattern, the include rule takes precedence and will collect the data in this situation.

  The following monitoring rules apply when creating include/exclude rules:

  – Patterns that do not include a wildcard (*) are more specific than patterns with a wildcard for the same entity type. For instance, */program/files/a.txt* is more specific than */program/files/a.**

  – Longer (string length) patterns are more specific than shorter patterns for patterns of the same type. For example */program/files/user* is more specific than */program/files*

  - Pattern types for the database monitor follow a hierarchy of object types such as:
    * tables, views, procedures
    * columns, constraints, indexes
    * attributes
  - Event and resource pattern types are more specific than the *both* pattern type when the pattern lengths are the same.

For additional details, refer to Appendix C, "Component Internal Rule Set Capability Details".

5.4.2 Selecting Component Rule Sets

The first step in configuring your component rules is specifying what types of data can be monitored for the component. For example, for one application component you may be interested in monitoring changes made to files, while in another you may be interested in process starts and stops as well as changes made within a database.

To add individual rule sets to your components:

1. Select the **Rule Set** from the drop-down menu in the *Add or Update Component Rule Sets* screen. See Section 5.3.1, "Add or Update a Component".
2. Monitoring rules can then be added to the rule set by clicking the *Edit Rules* link in the rule set heading. If you have integrated the Configuration Change Console server with one or more LDAP or Active Directory servers, you can specify your user include/exclude rules based on these LDAP users or groups instead of entering them manually on this screen. If you include a group in a rule, and if that group in LDAP/AD server changes, that change will automatically be reflected in the component and the agent will be instructed to modify its monitoring requirements.
3. Monitoring Component Internal Rule Sets.

Some Rule Sets involve a specific type of monitoring, shown in parentheses following the rule set name, for example: *Active Directory (Snapshot)*. These modules often require extra configuration before monitoring can be performed. Such rule sets, once added, will feature an additional *Configure* link in the rule set header.

There are two classifications of rule sets that can be added to a component; *External Rule Sets* are rule sets that deal with artifacts outside of an application or at the OS level such as files, processes and OS users. *Internal Rule Sets* are rule sets that deal with object monitoring inside of an application, such as a table in a database or an object in an Active Directory server.

Only one Internal Rule Set can be added to a component. This is to maintain components that are simple to manage and understand. Making components too detailed renders it harder to track your events back to your compliance frameworks.

There are several classes of internal rule sets available:

- *Snapshot*. Used for databases and Microsoft Active Directory. This rule set provides two monitoring functions: snapshot and inventory. The Snapshot portion stores an image of the selected application or database content at regular intervals. As each new snapshot is grabbed it is compared with the previously stored snapshot. A change event is generated if differences are found between the two images. The snapshot rule set provides a lightweight monitoring mechanism for tracking updates, additions, or deletions made to the data associated with the application

or database. Note that the Snapshot rule set detects differences only; it will not tell you exactly what item triggered the change event, or the user responsible. Using the *Database Inventory* screen, you can see when a snapshot had a change since a previous snapshot and you can choose to "diff" two snapshots to identify specific changes.

In a similar manner, the SQL Inventory portion of the Snapshot runs user defined SQL queries on the monitored database at regular intervals and stores the results of each for later review through the *Change Visualization/Database Inventory* screen. Note that this rule set does not report information pertaining to the user responsible for detected change events.

- *SQL Audit*. Used for supported databases. The SQL audit rule set reports audit trails generated by the built-in auditing functionality of the monitored database. The difference between SQL audit and SQL trace is that the audit module reports events in object type (for example, table, view, process), object name (sales, employee), and operation (select, create, insert), whereas SQL trace simply reports on SQL statements.
- *SQL Trace*. Used for supported databases. The SQL Trace rule set logs all SQL statements executed by users of the database, often by utilizing the built-in auditing functionality of the monitored database. The rule set can be configured through a component to capture a specific user's activity, the activity of an application that interacts with the database, and/or search for and capture segments of SQL statements that may be used to alter important data within the database. The rule set generates a detailed forensic data trail that can be used by an administrator to track exactly what query or statement caused a specific change event, the time of its execution, and the user responsible. Note that due to the broad scope of data collected, and the fact this rule set may require the use of a database's internal auditing functionality, use of this rule set may result in reduced database performance.
- *Trace*. Used for Active Directory and the Windows Registry. The Trace rule set leverages operating-system specific mechanisms to audit internal events of an associated application. For example, the Windows Registry (Trace) rule set can be used to report all changes made to specified registry keys and values associated with a specific application.

5.4.3 Adding Component Rule Sets

You can add Modules using the *Add or Update Component Rule Sets* screen.

To get to this screen, navigate to *Policy --> Operations Management --> Components: Rule Sets count link*.

For each Component:

- Select the Rule Set from the Add drop-down menu. Click **Go** to add the rule set to the Component.
  - **a.** File Event
  - **b.** Process Event
  - **c.** User Event
  - **d.** Active Directory (Snapshot)
  - **e.** Active Directory (Trace)
  - **f.** Oracle 8i (Snapshot)

g. Oracle 8i/9i/10g (SQL Trace)

h. Oracle 9i/10g (Snapshot)

i. SQL Server (Snapshot)

j. SQL Server 2000 (SQL Audit)

k. SQL Server 2000 (SQL Trace)

l. Windows Registry (Trace)

The first three are *External* Rule Sets and exist at the Operating System level, outside of another system being monitored. The remaining rule sets are *Internal* Rule Sets and exist to internally monitor other systems.

- If the selected rule set requires additional setup, a Configure link will display in the rule set header. Click the **Configure** link to be forwarded to the *Update Internal Configuration* screen for the rule set. Connection parameters for supported rule sets can be found in Appendix D, "Component Internal Monitoring Parameters".
- Click the **Edit Rules** link to specify the monitoring rules for the application component. You will be forwarded to the appropriate screen for the component type. The individual rule set rule screens are documented in the next section.

Once all rule sets have been configured for the given component, click **Done** to return to the component listing screen.

5.4.4 Monitoring Files

Configure a Component to monitor specific files or directories.

To get to this screen, navigate to *Policy --> Operations Management --> Components*.

To monitor files, follow these steps:

1. In the *Components* screen, click a component's Rule Sets count link to display the *Add or Update Component Rule Sets* screen.
2. From the drop-down *Add* list, select **File Event** and click **Go**.
3. Click the **Edit Rules** link for the File Event rule set.

Note: The *Add or Update Component Files* screen will initially contain only one field for entering a rule pattern. To add more rules, click the **Add Instance** link.

When you configure a file for a monitoring policy, you can set the path as relative to a user-specified base path (to save typing when the same base path is used over and over again), or you can specify the absolute path. Using a relative path, when you assign a component to multiple devices, you can add to, or modify, the relative path so that it correlates with the actual directory path used on the device rather than having different components for each device.

You can direct Configuration Change Console to archive a monitored file when it is changed by checking the Archive box for the file. For example, you might archive an essential database configuration file. If detected changes to the file introduce problems, you can restore the previous version of the configuration file. You can also use the console to diff two versions of the file and see exactly what changed. When you send a new configuration to the agent using Update Agents, the agent will take an initial

archive copy of the file before any changes occur and then will save another copy each time a change happens.

By default, Configuration Change Console stores up to five versions of a file for each device. You can change this number by navigating to *Administration --> Server Configuration --> Archived Files Configuration*.

You cannot specify a directory to archive. If the agent cannot find a specific file with the pattern you specified, the archive action will simply be ignored.

Archiving will consume disk space in the directory the agent is stored in, so use this feature carefully.

Enter the following information:

- *Is Relative Path*. Select whether you wish to use a specified Default Path for the paths specified as relative. The default path is entered in a field lower on this form.
- *Include/Exclude*. Select the appropriate radio button to either monitor the file or exclude the file from being monitored.
- *Files*. Enter the file name. A single wildcard (*) is supported anywhere after the final slash. See Appendix C, "Component Internal Rule Set Capability Details" for wildcard support details.
- *Effective File/Directory Path*. This field is automatically generated by the system, and is used to display the full directory path including the relative path, if it has been specified in the *Default Path* field.
- *Description*. (optional) Enter a brief note describing the purpose of the rule.
- *Archive*. (optional) Select to store a variation of the monitored file when changes occur. The five most recent versions of the file will be stored on the computer where the agent monitoring the file is installed. Archived files can be reviewed on the *Archived Files* screen, and compared using a file diff method. There is an administrative screen to change the number of archived copies to store for files.
- *Default Path*. If you have checked the Is Relative Path box for any of the rules, enter a default absolute path. When you create an instance of a component, you can choose to change this default path at an instance level.
- *User Filtering*. Check this box to filter all detected changes by the user rules configured in the same component. For example, if you only wanted to capture file changes for the file rules you specified for the Administrator user, you would add the OS User Rule set to the component with a rule for including the Administrator user. The *OS User Rule Set* screen has an option to specify that the user rules are used to filter other event types. Then you also check this User Filtering checkbox on the *File Rule Set* screen to complete the filtering. Only file change events associated with the Administrator user will be captured.

Click **Save** to save the changes or **Cancel** to exit the screen without making any changes.

5.4.5 Monitoring Processes

Configure the processes that are meaningful to a component to be monitored as part of the component.

To get to this screen, navigate to *Policy --> Operations Management --> Components*.

To monitor processes, follow these steps:

1. In the *Components* screen, click a component's Rule Sets count link to display the *Add or Update Component Rule Sets* screen.
2. From the drop-down Add list, select **Process Event** and click **Go**.
3. Click the **Edit Rules** link for the Process Event rule set.

> **Note:** The *Add or Update Component Processes* screen will initially contain only one field for entering a process pattern. To add more rules, click the **Add Instance** link.

Enter the following information:

- *Include/Exclude*. Select the appropriate radio button to either monitor the process or exclude the process from being monitored. You can create rules such that you include * and then exclude specific processes from being monitored; or you can exclude all processes by excluding * and then including specific processes.
- *Pattern*. The process name you want for this rule.
- *Pattern Type*. Select whether you want to collect events (starts/stops), resource (CPU) utilization information associated with the specified process, or both. If you want to collect resource usage for processes, you must also ensure that you have configured your Agent schedule templates to include Performance Data. By default, the default schedule group only monitors change event data. See the sections related to Agent Schedule Groups and Agent Schedule Templates for more information.
- *Description*. Enter an optional, brief note describing the purpose of the process.
- *User Filtering*. Check this box to filter all detected changes by the user rules configured in the same component. For example, if you only wanted to capture process changes (starts and stops) for the process rules you specified for the Administrator user, you would add the OS User Rule set to the component with a rule for including the Administrator user. The *OS User Rule Set* screen has an option to specify that the user rules are used to filter other event types. Then you also check this User Filtering checkbox on the *Process Rule Set* screen to complete the filtering. Only process change events associated with the Administrator user will be captured.

Click **Save** to save the changes or **Cancel** to exit the screen without making any changes.

5.4.6 Monitoring Operating System Users

Configure a component to monitor specific operating system user login or logout events.

To get to this screen, navigate to *Policy --> Operations Management --> Components*.

To monitor users, follow these steps:

1. In the *Components* screen, click a component's **Rule Sets count link** to display the *Add or Update Component Rule Sets* screen.
2. From the drop-down Add list, select **OS User Event** and click **Go**.
3. Click the **Edit Rules** link for the OS User Event Rule Set.

Note: The *Add or Update Component OS Users* screen will initially contain only one field for entering a user pattern. To add more rules, click the **Add Instance** link.

Enter the following information:

- *Include/Exclude*. Select the appropriate radio button to either monitor the user or connection type or exclude it from being monitored. You can use wildcards to include all users then exclude specific users or vice-versa to exclude all users then include specific users.
- *Pattern*. Enter the user name or connection method (for example, ftp, telnet, rdp). A single wildcard (*) is supported in this field. See Appendix C, "Component Internal Rule Set Capability Details" for wildcard support details. Note that, by default, no users are included in monitoring.
- *Pattern Type*. Select the appropriate type for the element specified in the Pattern field. Available options include user, for user names, and connect type, for connection methods.
- *Description*. Enter an optional, brief note describing the user and why its important to the component.
- *User Filtering*. Check this box if this list of users is used to filter events from other rule sets in the component. See the relevant documentation for other rule set types to see how this filtering is used for these rule sets.

Click **Save** to save the changes or **Cancel** to exit the screen without making any changes.

If you have integrated the Configuration Change Console server with one or more LDAP or Active Directory servers, you can specify your user include/exclude rules based on these LDAP users or groups instead of entering them manually on this screen. If you include a group in a rule, if that group in LDAP/AD server changes, that change will automatically be reflected in the component and the agent will be instructed to modify its monitoring requirements.

5.4.7 Monitoring Component Internal Rule Sets

Internal rule sets are those rule sets that are added to a component that define internal aspects of an application that should be monitored. Examples of internal rule sets are database table monitoring, Active Directory object monitoring, Windows Registry monitoring, and so on.

The following list covers some of the internal rule sets that are available to components. The available components depend on the release and OS version of the component you are defining:

- Active Directory (Snapshot)
- Active Directory (Trace)
- Oracle 8i (Snapshot)
- Oracle 8i/9i/10g (SQL Trace)
- Oracle 9i/10g (Snapshot)
- SQL Server (Snapshot)
- SQL Server 2000 (SQL Audit)

- SQL Server 2000 (SQL Trace)
- Windows Registry (Trace)

Each internal rule set has one or more ways of performing its monitoring (Snapshot, SQL Audit, SQL Trace, Trace). As discussed earlier in this book, each has its advantages and disadvantages.

A component can have all three external rule sets (file, process, and OS user), but can only have one internal rule set at a time. This is mostly to ensure that component definitions remain specific enough for the reporting and auditing features of the product to be usable.

If the component rule set supports internal monitoring, use the *Configure* link for the appropriate Rule Sets on the *Add or Update Component Rule Sets* screen to enable it. Some rule sets require that you specify connection parameters, such as login credentials, in order to access the application being monitored. These parameters are unique to each application and must be configured to properly enable monitoring. For example, an Oracle database requires specific database user permissions and login credentials.

To get to this screen, navigate to *Policy --> Operations Management --> Components*.

To monitor internal component rule sets, follow these steps:

1. In the *Components* screen, click an component's Rule Sets count link to display the *Add or Update Component Rule Sets* screen.
2. From the drop-down Add list, select one of the internal rule sets and click **Go**.
3. Click the **Edit Rules link** for the internal rule set.

> **Note:** The *Add or Update Component Processes* screen will initially contain only one field for entering a rule pattern. To add more rules, click the Add Instance link.

4. Back in the *Add or Update Component Rule Sets* screen, click the **Configure link** in the component rule set header. You will be forwarded to the *Update Internal Configuration* screen for the component.

> **Note:** Only rule sets that support internal monitoring capabilities will feature the Configure link.

5. Click the *Is Enabled* checkbox to enable or disable the rule set and provide any necessary connection parameters for the rule set.

The content of the *Update Internal Configuration* screen varies depending on the rule set selected for the component and what is being monitored. The screen shown above shows only one example. For a full list of all connection parameter settings required for each rule set see Appendix B, "Application-Specific Internal Monitoring Capabilities".

5.4.7.1 Configure Internal Rule Sets

To configure internal rule sets, follow these steps:

1. Access the Update Internal Configuration screen by navigating to *Policy -> Operations Management -> Components -> Rule Sets count link -> Configure link*

2. Enter the following information, if needed by the selected rule set:
   - *Connection URL*. (see Appendix D, "Component Internal Monitoring Parameters")
   - *Username*. The user name that the agent will need to connect as to this system to perform monitoring. The agent needs the permissions required for the monitoring. For instance, for Database trace rule sets, the agent needs to be able to read the database's audit logs.
   - *Password*. The password for this user.
   - *Rule Set-Specific Monitoring Option*s (see Appendix D, "Component Internal Monitoring Parameters")
3. Click the **Is Enabled** box to enable the rule set.
4. Click **Save** to save changes or **Undo Changes** to reset the fields.

> **Note:** The enabled configuration will not go into effect until you update your agents through the *Update Agents* screen. The Update Agents screen is accessible through the Update Agents button in the upper right-hand corner of the user interface.

5.4.7.2 Override Rules and Configuration for Instances

When this screen is accessed through the *Component Instance* screen none of the fields will be editable. Click the **Override** button to make edits to the information for the specific Component Instance only. This will not change the base component that other instances are using itself. When overriding, you can change the rules as well as the configuration needed to connect to the other system being monitored.

5.4.8 Internal Rule Sets: Database Snapshot type Rule Sets

To access this screen, navigate to *Policy --> Operations Management --> Components*.

From the *Add or Update Component Rule Sets* screen, click the **Edit Rules** link of a rule set that is for database (snapshot) type monitoring. This link takes you to the *Add or Update Component Rule Sets* screen. Depending on the agent module selected, you may be presented with the individual *SQL Query or Internal Monitoring* screens or a hybrid version featuring the functionality of both in the same screen, as is the case with the Oracle Snapshot modules.

For rule set-specific details related to rule configuration, see Appendix B, "Application-Specific Internal Monitoring Capabilities".

5.4.8.1 SQL Query Parameters

The SQL Query section of the rule screen lets a user enter a query that will run on a scheduled basis. When this query runs, it compares the output with the output from the previous run. If there is a change between the snapshots, that change is counted as a change event. Also, you can specify to record baseline query so that not only are the intermediate snapshots stored, but you can save a baseline on a regular basis. The *Database Inventory* screens let you see these baseline/snapshots and see differences between snapshots.

- *Name*. The name of the query. This name is used in the reports to identify the query.

- *SQL Query*. The fully qualified SQL query for your database. When specifying a SQL query, you must include the full database object name. For example, when entering a query to select all customer data from the HR database schema, you would enter: `select * from HR.customer`. The query that you enter should not have a semicolon at the end.

  Note: This screen does not check the validity of the schemas that you enter in a query. If the schema does not exist in your database structure, your monitoring results will be incomplete. There will be an error in the agent's logs that the table or query could not be executed.

- *Record Baseline*. Check the box to record periodic baselines on the server side. The baseline interval is based on the local calendar of the device. The baseline interval is set under the Configure link for the rule set.

5.4.8.2 Baseline Recording

Baseline recording enables your snapshots to include periodic recording of baseline data on the server side. The baseline interval is driven by the monitored devices local time.

The following types of internal monitoring module rules support baseline recording:

- Oracle 8*i* (Snapshot)
- Oracle 9*i*/10*g* (Snapshot)
- SQL Server (Snapshot)

From the Configure link of the rule set, there is an option for the rule sets listed above that let you choose the baseline. The baseline options are:

Table 5–3 Baseline Rule Options

Option	Description
NONE	Do not record a baseline even if rules specify
HOUR	Record baseline every hour on the hour.
DAY	Record baseline every day at midnight of that day.
WEEK	Record baseline every day at midnight of the first day.
MONTH	Record baseline every month at midnight of the first day.

5.4.8.3 Include/Exclude Parameters

The Include/Exclude section of this rule screen lets a user choose which schema objects they want to monitor. The monitor performed since this is a snapshot type of rule set is to record the state of a schema and then compare it to the next run and treat the difference as a change event.

A snapshot module with this type of rule only monitors structural schema changes, not content changes.

- *Include/Exclude*. Select the appropriate radio button to either monitor the object or exclude the object from being monitored.
- *Patterns*. Enter the object pattern. The agent will match the full name of the object or attribute specified in the inclusion/exclusion policy. You may use an asterisk as

a wildcard to match any strings of a similar format to the object name. Note that you should be careful when using fully qualified names of database objects, as the name must match exactly for monitoring to occur.

- *Pattern Type*. Select the appropriate pattern type from the drop-down menu. The pattern types available depend on the application being monitored and the rule set used. The full list of module-specific pattern types can be viewed in the following section.
- *Description*. Enter a brief note describing the purpose of the policy.

The fully qualified object name formats for supported databases include:

- *Oracle. <schema>.<tablespace-name>*
- *SQL Server. <database name>.<owner>.<tablespace-name>*

As noted above, the agent will run the configured queries at the default five minute interval unless otherwise configured in the component. Depending on the type of monitoring selected, the query may be used to simply collect data from the database, as with SQL Trace, or to monitor for changes made to the data stored in the database, as with the Snapshot modules. Keep in mind that Configuration Change Console has a built-in limit of 1000 rows when it comes to data returned by selection queries. Therefore, you will need to focus your queries so as to return only relevant data.

For example, if an overly broad query is used with a Snapshot-based agent module, and a change event occurs in a row beyond the 1000th row returned, the change will not be detected and thus not display in the report screens. Make sure to balance such queries with exception clauses so that only necessary data is returned and thereby ensuring accurate change detection. The limit of 1000 rows can be configured in the Rule Set Configure link from the *Rule Sets* screen for the component.

5.4.9 Internal Rule Sets: Specific Pattern Types

The available pattern types found on the *Add or Update Component Rule Sets* screen vary depending on the rule set you are working with.

For additional details, see:

- Appendix B, "Application-Specific Internal Monitoring Capabilities"
- Appendix C, "Component Internal Rule Set Capability Details"

The supported pattern types for rule sets include:

- Active Directory (Snapshot) - Choose from changes to individual users (user), monitored computers (computer), user or device groups (group), or all of the above (all) configured on the Active Directory or LDAP server.
- Active Directory (Trace) - Choose from computers (computer), groups (group), and users (user), as configured within Active Directory.
- Oracle 8*i* (Snapshot) - See Appendix B, "Application-Specific Internal Monitoring Capabilities"
- Oracle 9*i*/10*g* (Snapshot) - See Appendix B, "Application-Specific Internal Monitoring Capabilities"
- Oracle 8*i*/9*i*/10*g* (SQL Trace) - Choose from changes to users (user), specific machines used to connect to the database (host), operating system user (osuser), terminal (terminal), event (event), or object name (objname) within the database
- Windows Registry (Trace) - Choose from registry keys (key), registry values (value), or all registry information (all) to include in registry monitoring

- SQL Server (Snapshot) - See Appendix B, "Application-Specific Internal Monitoring Capabilities"
- SQL Server 2000 (SQL Audit) - Choose from changes to users (user), specific machines used to connect to the database (host), specific applications connected to the database (appname), or specific databases (dbname), or object name (objname) within the database
- SQL Server 2000 (SQLTrace) - Choose from individual users who execute SQL queries (user), specific machines used to connect to the database (host), specific applications connected to the database (appname), or a specific string to look for within an executed SQL query (sqltext). Note that the appname pattern type is case sensitive. Further note that wildcards are not supported by the sqltext pattern type

5.4.9.1 Patterns Types for Trace and Audit Rule Sets

The following table provides a quick reference for the pattern types supported for Trace and Audit modules:

Table 5–4 Pattern Types for Trace and Audit Rule Sets

Trace Modules	Audit Modules
SQL Server 2000 ■ sqltext ■ user ■ appname ■ host	SQL Server 2000 ■ user ■ host ■ appname ■ objname ■ dbname
Oracle 8*i*/9*i*/10*g* ■ user ■ host ■ terminal ■ osuser ■ objname ■ event	N/A

5.4.10 Active Directory Monitoring

Active Directory rule sets track and report user additions, user permission changes and account deletions as well as device and group changes. The Configuration Change Console agent can be installed on the same device on which the Domain Controller is running for audit level monitoring where the user that makes a change can be captured, or it can monitor the Domain Controller remotely using the snapshot rule set which will detect changes, but not the user that made the change.

Active Directory monitoring reports the following change events for users, groups, and computers:

Table 5–5 Change Events for Users, Groups, and Computers

Event ID	Event Description	Entity Type	Entity Name	Event Type
624	A user account was created	user	entityname	added

Table 5–5 (Cont.) Change Events for Users, Groups, and Computers

Event ID	Event Description	Entity Type	Entity Name	Event Type
627	A user password was changed	user attribute	entity.password	modified
628	A user password was set	user.attribute	entity.password	modified
630	A user account was deleted	user	entityname	deleted
631	A global group was created	group	entityname	added
632	A member was added to a global group	group.member	entityname.member-name	added
633	A member was removed from a global group	group.member	entityname.member-name	deleted
634	A global group was deleted	group	entityname	deleted
635	A local group was created	group	entityname	added
636	A member was added to a local group	group.member	entityname.member-name	added
637	A member was removed from a local group	group.member	entityname.member-name	deleted
638	A local group was deleted	group	entityname	deleted
639	A local group account was changed	group.attribute	entityname.-	modified
641	A global group account was changed	group.attribute	entityname.-	modified
642	A user account was changed	user.attribute	entityname.-	modified
645	A computer account was created	computer	entityname	added
646	A computer account was changed	computer	entityname	modified
647	A computer account was deleted	computer	entityname	deleted
	*Entity Type = Pattern Type in the Module Rule definition			
	*Entity Name = Domain Name + "\\" + AccountName			

For Active Directory Monitoring, you can include/exclude rules by following some basic guidelines:

- Rules are based on users, groups, login names, and devices
- All patterns are case-insensitive, meaning that AbC matches ABC

- To target specific entities, use a combination of include and exclude rules
- Do not apply include and exclude rules to the same pattern, except if you use *include*=* or *exclude* = *

If you want to exclude specific targets, use *include*=* and then add some specific exclude rules. Likewise, if you want to include only specific targets, use an *exclude*=* rule with some rules with explicit exclude patterns.

5.5 Step 3: Mapping Components to Managed Devices

After configuring components for your applications, you must specify the devices on which each component is running. A single component can be assigned to one or many devices.

Before mapping components to devices:

- You must install a Configuration Change Console agent on the device you wish to monitor. Note that certain database rule sets allow remote database access, and therefore can use an agent installed on a device other than that where the database is installed.
- The component must be configured with rule sets and rules. If your components have no monitoring rules defined, configure or edit their monitoring details from the Components screen by clicking on the count link for Rule Sets.

The *Component Instances* screen displays all devices to which the component is currently assigned.

To access this screen, navigate to *Policy --> Operations Management --> Components: Instances count link*.

The name of the device assigned to the component instance is displayed in the Device Name column. The Overridden column displays whether or not the global component rule set rules have been altered for the associated application instance. Clicking the **Overridden Status** link will forward you to a version of the *Component Rule Set* screen for this instance only where you can edit the rules and connection settings for the selected instance only. Not all of the rule sets allow modifications at the instance level.

To add or update a component's device assignment, click the **Modify Device Assignments button**. The *Assign New Device* screen will display.

The *Assign New Device* screen displays all currently configured device groups and all their member devices. You can assign a component to an entire device group by checking the box next to the device group name, or expand the device group tree to select individual devices. Once all devices have been selected, click **Save** to exit the screen. The device group structure is not maintained when choosing a group. If you add or remove a device from a group, it will not impact the component assignment.

5.6 Step 4: Assign Controls to a Component

If you have already configured the Policy Management portion of the product as discussed in the next chapter, you can assign Policy controls to your component.

To access this screen, navigate to *Policy --> Operations Management Controls --> Control count link*.

This screen enables you to change the controls that are assigned to this component. Control assignment is the way that component changes get reported up through the control/policy/framework reporting structure. For instance, to report changes on the

top level dashboard, you need to assign components to a control and likewise have that control assigned to a policy.

The subtitle of the screen provides a context for the component. For example:

Component: Finance Application Server 1.0 WINNT

Click on the + to expand the Control Framework and Policy hierarchy to view the list of controls. After each policy name will be a number of selected controls in [ ] behind the policy name.

Clicking on the checkbox on the bottom most level of the hierarchy will select a control to assign to the selected component.

Select the controls to assign to the selected component by using one of these methods:

Clicking the check box for the control which is the deepest level represented in the hierarchy.

Clicking on the policy name (or framework name) to assign all controls under that policy (or control) to the component.

Click the Selection Helper link to select a group of templates based on pattern matching. Note that pattern matching is case sensitive.

After making a new assignment or unassigning a control, returning to the component listing screen will show an updated count of assigned controls to the component.

5.7 Step 5: Applications

Grouping component instances into applications allows you to model your real world business applications and make reporting line up with your business. Most large-scale enterprise applications rely on the interaction of multiple application components on multiple servers. For example, a web-based customer service application will likely include a web server, application server, and database, all running on different servers. You can create a component for each of these elements, define instances based on the servers where the applications run, and then create an Application that allows you to easily view change events that affect the application as a whole rather than only looking at the components.

A component instance can be part of multiple applications. This can prove useful for reporting and management purposes. For instance, a firewall may be a component that is used to protect your HR application servers and also your finance application servers at the same time. Any change to this firewall configuration settings may impact both applications at the same time.

To use applications you will need to first create your components, then create component instances by assigning them to devices.

5.7.1 Creating Applications

The *Applications* screen displays a list of existing applications, the number of component instances that are associated with each group, and the number of Audit Actions currently configured for each application.

Note: The links under the # of Component Instances column in the Applications screen will display "0" until a Component Instance is added to the group.

To access this screen, navigate to *Policy --> Operations Management --> Applications*.

To add an application, click the **Add Application** button. To modify an existing application's information, click the link for the application name. Either action displays the *Add or Update Application* screen. Enter a name and optional description for the application. Click **Save** to save the changes. The group will then appear on the *Applications* screen.

5.7.2 Adding Component Instances to an Application

Once you have created an application, you can add one or many component instances to it.

To access this screen navigate to *Policy --> Operations Management --> Applications*.

Click the link in the # of Component Instances column for the desired application to display the *Assign New Component Instances* screen. Select one or more component instances from the available instance tree. Click **Save** to save the changes or **Undo Changes** to reset the fields.

5.8 Step 6: Defining Application Audit Actions

Audit Actions specify what actions should be taken when an event occurs. The types of events you can specify for an audit action are File, Process, OS User, and Component Internal (database, registry, active directory, for example) changes. These events can trigger email notifications, report generations, SNMP traps, and Change Management Reconciliation.

See Chapter 12, "Administering Servers and Agents" for information on configuring SNMP notifications.

5.8.1 Change Management Integration: Detecting Authorized/Unauthorized Events

Configuration Change Console integrates with a Change Management server to monitor and categorize events as authorized or unauthorized. The Audit Action compares the change event against tickets and configured CTIs on the Change Management server. If the detected changes match an open ticket for the configured CTI, the change is determined to be authorized, and the corresponding ticket is updated in the Change Management server with the event details. If detected changes do not match any open tickets for the configured CTI, they are determined to be unauthorized. Once a change has been determined to be unauthorized, one of two things may happen, depending on the Change Management server configuration.

1. A new ticket will be created for each unauthorized change if CT Consolidation is not enabled.
2. If CT consolidation is enabled, all unauthorized events matching an existing unauthorized ticket's CTI will be appended to the unauthorized ticket. If no matching CTI is found, a new unauthorized ticket will be created using the Default Outbound Ticket information.

The Audit Action provides the final integration point with the Change Management application.

For the integration to work, you must have specified the connection parameters used for your Change Management Application, selected your default Outbound Ticket Configuration, and have assigned categories to individual component instances through the user interface. Refer to Chapter 7, "Integrating With A Change Management Server" for details on configuring this integration.

5.8.2 Defining Audit Policies

When you create a component when a Change Management system is integrated (Change Management integration fully configured through the *Change Management Configuration* screen), an audit action is generated automatically. Auto-generated actions appear in the *Audit Actions* screen with the string "AUTO ACTION" appended to the name. These audit actions are incomplete until you assign component instances or applications to them.

If you do not have a Change Management system integrated, you can create audit actions manually by going to the *Audit Actions Policy* screen.

To access this screen, navigate to *Policy --> Operations Management --> Audit Actions*.

To add a new Audit Action, click the **Add New Audit Action** button. To edit an existing action, click the **Audit Action**'s name link. Either way, the *Add or Modify Audit Action* screen is displayed. Enter the following information:

- *Audit Action Name*. Unique name assigned to the audit action. It is helpful to define a consistent naming convention for action names.
- *Description*. Optional brief note explaining the function of the action.
- *Component Instances/Application*. You must specify either a component Instance or an Application to audit. The defined audit action will only apply to events associated with the selected Component or Application. Select the Component Instance or Application from the available drop-down options. It is possible to have multiple audit actions per component instance or application depending on different needs; for instance you may want to get notifications for file changes, and get SNMP traps sent for process changes for the same component instance.
- *Events to Detect*. Select from the following: file, process, OS user or component internal change events.
- *Notify*. Select the person to notify for each event that occurs. The person specified must have a primary email address configured to receive notifications. No notification is sent if *None* is selected.
- *Priority. Priority level for notification escalations*. Priority levels are as follows: P1, P2, P3, P4, or P5, with P1 having the highest priority.
- *SNMP Servers*. If you have configured an SNMP server to receive traps from the Configuration Change Console server, select an SNMP server where the notification can be sent. You can select more than one SNMP server.
- *Report*. Reports can be generated and sent as an attachment with the email notification
- *Ticket Actions*. If the Authorized Change option is selected, the Change Management Server will be updated with the details of the authorized events if an authorized event occurs. If the Unauthorized Change option is selected, Configuration Change Console creates a ticket using the Default Outbound Ticket configuration for all unauthorized events detected by the agent. If CT Consolidation is enabled the unauthorized event will be first compared to CTIs of existing unauthorized tickets. If a matching CTI is found, the ticket will be appended with the change event information. If no matching CTI is found, a new unauthorized ticket will be created using the Default Outbound Ticket configuration.
- *Ticket Category*. Specify the Default Outbound Ticket configuration to use for unauthorized change events.

Click **Save** to save your changes.

From the *Audit Actions* screen, complete the Audit Action by assigning a component instance or application to the policy, by clicking the appropriate count link and then selecting from the displayed instances. You cannot assign an audit action to both a component instance and an application at the same time.

6

Policy Management

Policy Management relates to your Compliance Policy frameworks, policies, and controls. This is opposed to Operations Management as discussed in Chapter 5, "Operations Management" which relates to the configuration aspects of the Configuration Change Console that relate to your physical infrastructure and how it should be monitored.

6.1 Frameworks

The Framework screen displays policy frameworks available in the product. There are predefined frameworks that come with the product as templates and there are custom frameworks which are frameworks that you can create.

A Framework is simply a grouping used to contain policies. Frameworks are intended to mirror your compliance framework used in your organization. For instance, you may use the COBIT, COSO, or PCI framework. Each of these is an example of what a framework in this product would be.

Configuration Change Console comes with a set of predefined frameworks which can be used to create custom frameworks specific to your environment. Once a custom framework has been created, it will be displayed on the *Framework* screen. Only custom frameworks may be used for reporting purposes. In order to use a predefined framework, you first need to save the predefined framework as a custom framework and modify it as necessary.

A user can create as many frameworks as necessary if they follow more than one policy framework. For instance, a large company may use both SOX and PCI frameworks for different parts of their environment.

To access this screen, navigate to *Policy --> Policy Management --> Frameworks*.

The frameworks screen lists all predefined frameworks. You can choose the view drop down in the filter bar to see predefined frameworks instead. Predefined frameworks cannot be instantiated in your environment, but they can be copied to a new custom framework.

The fields shown on this screen are listed below:

- *Framework* - The name of the framework. A framework name must be unique from all other framework names defined through this screen.
- *Description* - User-entered descriptive field of the framework for reference.
- *Policies* - A count of custom policies that have been created that are part of this framework. A policy is only part of one framework. However you can have two policies with the same name if they belong to different frameworks.

Clicking on the count link will display the *Policy Listing* screen which will be filtered by the selected framework.

The filter bar allows you to change the view for this screen. The following are the two views available.

- *Predefined Frameworks* - Lists only predefined frameworks that come prepackaged with the product. From here, you can navigate and view policies and controls that are defined for the framework, but you cannot use them for reporting. You need to find a framework to use and then on the framework edit screen click the **Save As** button to save this framework as a custom framework.
- *Custom Frameworks* - Custom frameworks are the frameworks that you create that match real life policy frameworks in your organization. They can be based on industry standard frameworks like PCI, COBIT, COSO, or can be custom in-house structured frameworks.

6.1.1 Modifying or Creating New Frameworks

To access this screen, navigate to either *Policy -> Policy Management-> Frameworks > Add Custom Framework* or *Policy -> Policy Management-> Frameworks > Framework name link.*

The *Add or Update Framework* screen allows an administrator to create or update a framework. A Framework is simply a grouping used to hold policies. Frameworks should mirror your compliance framework used in your organization. For example, you may use the COBIT, COSO, or PCI framework.

Once you create a framework, you then create (or copy from predefined frameworks) policies that comprise the policy framework you are going to use.

The following fields are displayed:

- *Framework* - Name for the framework.
- *Description* - Brief note describing the function of the framework.
- *Framework Text* - This can be a much more detailed description of the framework describing the use cases and purpose of the framework.

Note: An asterisk next to a field indicates required input.

6.1.2 Copying a Framework

Use the following steps to copy an existing predefined or custom framework.

Click on the **Save As** button when viewing the *Add or Update Framework* screen for a custom or predefined framework.

Change the name and descriptive fields as necessary. Check the appropriate check boxes indicating what other objects you want to save when copying the framework. These check boxes are mutually inclusive, in other words, you cannot copy controls without also copying policies.

- *Policies* - Will additionally make a copy of all policies and assign them to the new framework name
- *Controls* - Will make a copy of all controls and assign them to each policy that is also copied.

Selecting this option should be used with care. In normal situations, controls can be shared across policies. Checking this box will actually copy all of the controls rather than mapping already existing ones, so you will have a new version of the controls with the string *copy of* prepended to each control.

- *Components* - Will also copy the components assigned to the controls if you check this check box.

Click **Save** to save the changes or **Reset** to reset the fields. You can click **Cancel** at any time to exit the screen without saving the copy.

6.2 Policies

To access this screen, navigate to *Policy --> Policy Management --> Policies*.

The *Policies* screen displays compliance policies available in the product for reporting. There are policies that are predefined that come with the product as templates and there are custom policies which are the ones that you can create.

A policy in the console maps directly to the compliance policies you use in your organization. For instance, there is a "Manage Installation" policy in the COBIT standard framework. This would be one policy configured on this screen.

Configuration Change Console comes with a set of predefined frameworks each with their own policies, which can be used to create custom policies specific to your environment. Once a custom policy has been created, it will be displayed on this *Policies* screen. Only custom policies may be used for reporting purposes. In order to use a predefined policy, you first must save the predefined policy as a custom policy and modify it as necessary.

A user can create as many policies as necessary to map to their internal compliance structure. The fields shown on this screen are displayed below:

- *Framework* - The name of the framework the policy belongs to. A policy can only belong to one framework. It is possible however to have many policies with the same name as long as each belongs to a different framework.
- *Policy* - The name of the policy. A policy can only belong to one framework. It is possible however to have many policies with the same name as long as each belongs to a different framework.

  The link on this field takes the user to the *Add or Update a Policy* field where the user can modify the existing policy or save a copy as a new policy.
- *Description* - User-entered descriptive field of the policy for reference.
- *Controls* - A count of custom controls that have been created that are assigned to this policy. A control can be shared across many framework/policy combinations.

Clicking on the count link will display the *Controls* listing screen which will be filtered by the selected framework and policy.

The filter bar has a field that allows you to change the view for this screen. The following are the three views available:

- *Predefined Policies* - Lists only predefined policies that come prepackaged with the product. From here you can navigate and view controls that are already defined and assigned to the policy, but you cannot use them for reporting. You must find a policy you would like to use, and then on the policy edit screen click the **Save As** button to save this policy as a custom policy.

- *Custom Policies* - Custom policies are the policies that you create that match real life policies in your organization. They can be based on industry standard framework policies like COBIT's "Manage Installation", or can be custom in-house structured policies.
- *Framework* - This filter option lets you see only policies associated with a specific framework. This is useful if your organization uses more than one framework for compliance reporting.

6.2.1 Modifying or Creating New Policies

To access this screen, navigate to either *Policy -> Policy Management-> Policies > Add Custom Policy* or *Policy -> Policy Management-> Policies > Policy name link*.

The *Add or Update a Policy* screen allows an administrator to create or update a policy. A policy in the console maps directly to the compliance policies you use in your organization. For instance, there is a "Manage Installation" policy in the COBIT standard framework. This would be one policy configured on this screen.

Once you create a policy, you then create (or copy from predefined policies) controls that will be assigned to components defined to mimic your organizations applications components.

The following fields are displayed:

- *Policy Name* - Name for the policy
- *Framework* - Drop-down list that allows you to select which framework to which this policy belongs. You cannot create a policy without at least one custom framework already existing
- *Description* - Brief note describing the function of the policy
- *Policy Text* - This can be a much more detailed description of the policy describing the use cases and purpose of the policy
- *Reference URL* - A URL that will be used to link the user to a document or application that contains the policy details
- *Owner* - An assigned owner of the policy selected from configured people in the Console product

---

Note: An asterisk next to a field indicates required input.

6.2.2 Copying a Policy

Follow these steps to copy an existing predefined or custom framework:

1. Click on the **Save As** button when viewing the *Add or Update Policy* screen for a custom or predefined policy.
2. Change the name in the *Save As Name* field and descriptive fields as necessary
3. Check the appropriate check boxes indicating what other objects you want to save when copying the policy. These check boxes are mutually inclusive. In other words, you cannot copy components without also copying controls.
   - *Controls* - Will make a copy of all controls and assign them to each policy that is also copied

     Selecting this option should be used with care. In normal situations, controls can be shared across policies. Checking this box will actually copy all of the

controls rather than mapping already existing ones, so you will have a new version of the controls with the string *copy of* prepended to each control.

- *Components* - Will copy the components assigned to the controls also if you check this check box.

4. Click **Save** to save the changes or **Reset** to reset the fields. You can click **Cancel** at any time to exit the screen without saving the copy.

6.3 Controls

The *Controls* screen displays compliance policy controls available in the product for reporting. There are controls that come predefined with the product as templates and there are custom controls which you create manually or can be created by copying a predefined control.

A control in the console maps directly to the granular policy controls that you use in your organization. For instance, there is a "Testing Changes" control which is part of the Cobit "Manage Installation" policy in the COBIT standard framework. A control is the most granular element in the compliance mapping capability of the product. Controls are mapped to components so that events that happen to each component can be reported against those mapped controls. This mapping relationship is effectively what relates an event to a policy.

Configuration Change Console comes with a set of predefined controls, which can be used to create custom controls specific to your environment. Once a custom control has been created, it will be displayed on the *Controls* screen. Only custom controls may be used for reporting purposes and mapped to components. In order to use a predefined component, you first need to save the predefined component as a custom component and modify it as necessary.

A customer can create as many controls as necessary to map to their internal compliance structure. A single control can also be assigned to any number of policies. For instance, you may have two policies that both have the same *Emergency Changes* control.

The fields shown on this screen are displayed below:

- *Control* - The name of the control. A control can be assigned to many policies. Clicking on this control name to get to the *Add or Update Control* screen displays the policies to which this control is mapped
- *Version* - A user-defined version for this control
- *Description* - User-entered descriptive field of the control for reference
- *Components* - A count of components that have been created that are assigned to this control. All instances of the component are assigned to the control automatically. Any event that happens to a component will be mapped to the controls that are assigned to the component

Clicking on the count link will display the *Assign Components to Control* screen where the assignments can be modified.

The filter bar displays a field that allows you to change the view for this screen. The following are the options available:

- *View > Predefined Policies* - Lists only predefined controls that come prepackaged with the product. From here, you can navigate and view controls that are already defined but you cannot use them for reporting. To save a control as a custom

control, find a control you would like to use and on the control edit screen click the **Save As** button.

- *View > Custom Policies* - Custom controls are controls that you create that match real life policy controls in your organization. They can be based on industry standard framework policy controls like COBIT's "Emergency Changes" control which is part of the Manage Installation policy, or can be custom in-house structured components.
- *Framework* - This filter option lets you see only controls associated with a specific framework. This is useful if your organization uses more than one framework for compliance reporting.
- *Policy* - This drop-down list lets you filter the controls to view only controls that are mapped to a specific policy. Since controls can be mapped to multiple policies, it is possible to see the same results even if you change the policy drop-down filter.

6.3.1 Modifying or Creating New Controls

To access this screen, navigate to either *Policy -> Policy Management-> Controls > Add Custom Control* or to *Policy -> Policy Management-> Controls > Control name link*.

From the *Add or Update Control* screen, you can define a control that will later be associated with a component. Enter or select the following parameters:

- *Control Name* - Original name for the control you are copying
- *Version* - A user-defined version number for the control used to distinguish multiple iterations of the same control that may be in use at the same time in an organization
- *Description* - Brief note describing the function of the control
- *Control Text* - This can be a much more detailed description of the control describing the use cases and purpose of the control
- *Document URL* - A URL that will be used to link the user to a document or application that contains the control details
- *Policies* - Select the Framework/Policy combinations to which you want to assign this control. You can select more than one by holding down the Control (CTRL) key while you select

You can unselect all by clicking on the None line at the top without holding down the Control (CTRL) key.

6.3.2 Copying a Control

To access this screen, navigate to *Policy -> Policy Management-> Controls > Control name link > Save As button*.

The *Copy a Control* screen allows an administrator to copy an existing custom or predefined control. A control in the console maps directly to the granular policy controls that you use in your organization. For instance, there is a "Testing Changes" control which is part of the COBIT "Manage Installation" policy in the COBIT standard framework. A control is the most granular element in the compliance mapping capability of the product. Controls are mapped to components so that events that happen to each component can be reported against those mapped controls. This mapping relationship is effectively what relates an event to a policy.

When you view one existing custom or predefined control and click the *Save As* button to make a copy, the following fields are displayed. Filling out this form and clicking *Save* will create the copy.

The following fields are displayed:

- *Control Name* - Original name for the control you are copying
- *Save As Name* - The name you want to give to the new custom control this copy will be saved as
- *Version* - A user-defined version number for the control used to distinguish multiple iterations of the same control that may be in use at the same time in an organization
- *Description* - Brief note describing the function of the control
- *Control Text* - A more detailed description of the control describing the use cases and purpose of the control
- *Document URL* - A URL that will be used to link the user to a document or application that contains the control details
- *Policies* - Select the Framework/Policy combinations to which you want to assign this control. You can select more than one by holding down the Control (CTRL) key while you select. You can unselect all by clicking on the None line at the top without holding down the Control (CTRL) key
- *Include* - Choose whether you want to also copy the components that are assigned to the control

6.3.3 Assigning Components To a Control

To access this screen, navigate to *Policy -> Policy Management-> Controls > Components count link*.

This screen enables you to change the components that are assigned to this control. Control assignment is how component changes get reported up through the control/policy/framework reporting structure. For instance, to report changes on the top level dashboard, you must assign components to a control and likewise have that control assigned to a policy. Through the component screens, you can also assign controls to components in the other direction.

The subtitle of the screen provides a context for the control to which you will be assigning components. For example:

Control: Application Change

Click on + to expand the Component Types to view the list of components of each type. Already selected components will be both checked and listed in a bold font.

Select the components to assign to the control by using one of these methods:

- Clicking the check box for the control
- Clicking the **Selection Helper** link to select a group of templates based on pattern matching. Note that pattern matching is case sensitive

7

Integrating With A Change Management Server

Configuration Change Console provides features for auditing applications for authorized and unauthorized events. As a major function of its compliance-auditing feature, Configuration Change Console compares planned changes to the IT infrastructure, as approved through your Change Management system, with the actual changes detected by Configuration Change Console.

Detected changes that can be matched with an approved change request are considered authorized. Authorized changes are reported back to your Change Management system as a record of the work done to carry out the planned change. Detected changes that cannot be matched to an approved change are considered unauthorized. Configuration Change Console opens a new ticket in your Change Management system each time it detects unauthorized actions and reports the time, location, user, and application associated with the unauthorized change.

Configuration Change Console matches monitored events against a ticket categorization. The structure of a ticket categorization depends on the Change Management server being used. For instance, BMC Remedy uses a categorization structure of Category/Type/Item.

Example of a Category/Type/Item definition:

- Category: Software
- Type: Finance
- Item: Application Server

To audit authorized and unauthorized events against the Change Management Server, follow these steps:

1. Configure the connection parameters for the Change Management Server. This allows Configuration Change Console to communicate with the Change Management server.
2. Configure a Default Outbound Ticket Definition using Categorizations from the Change Management Server. This configuration determines how tickets will be created in the Change Management server by Configuration Change Console when unauthorized changes are detected.
3. Map Categorizations to the component instances or applications that you want to monitor for authorized or unauthorized change events.
4. Configure Audit Actions to audit specific events (file, process or application-internal changes) on the component instances or applications.

Note: If steps 1 through 3 are completed successfully, a default audit policy is created automatically for all new components so the only part of step 4 that must be completed is assignment of the audit action to the component instance.

In addition to managing authorized/unauthorized changes following normal processes, the product also can work in an environment where IT staff may create emergency tickets to fix a problem without having authorization.

The following chart depicts the event-detection and ticket-generation process flow.

Important: Before configuring Change Management integration through the user interface, you must customize your Change Management Server by following the instructions in the Configuration Change Console Installation guide.

7.1 Step 1: Configuring Change Management Integration

Configuring your Change Management Server is a two-step process handled through a single screen. First, specify the type of Change Management Server used along with all necessary connection parameters. Then indicate the default Categorization definition used to create a ticket for detected unauthorized changes. Using the Change Management Server screen, you can specify the type of Change Management server used, provide necessary connection information for the agent to connect to the server, and set up the default Outbound Ticket Configuration used in Auditing.

To access this screen, navigate to *Administration --> Server Configuration --> Change Management Server*.

To configure Change Management integration, follow these steps:

1. *Ticket Management Type*. Select the type of Change Management application used from the Ticket Management Type drop-down menu.
2. *Device*. Select the device whose agent will be used to connect to the ticket management server from the Device drop-down menu.
3. *Server IP*. Enter the IP address or hostname of the Change Management server. The agent does not have to be installed on this machine. If the agent is installed on the device where the application is running, you can enter localhost in the *Server IP* field.
4. *Username and Password*. Provide the username and password for the Change Management server. Be sure to specify the correct password. If an invalid password is used, the password must be corrected on this screen before categorization information can be collected. If you do not see the bottom half of the configuration screen appear after some time, the connection to the server most likely has failed either due to network connectivity or authentication.
5. *Consolidate CTI*. Specify whether to consolidate Change Ticket Information for change events. Specify the Consolidate CTI settings to control the number of unauthorized tickets created in your Change Management System. The field can accept a value of CT (one ticket will be generated per unique unauthorized Change Ticket combination and the ticket will be updated until the ticket is closed or the stop ticket update flag is set on the Change Management software), CT+D (one ticket will be generated per unique category and type combination and the

device the change happened on), or None (each unauthorized change will generate one new ticket).

6. *Ticket Correlation Criteria*. Select the following criteria by clicking the associated check boxes. Correlation enables you to gather details about whether a change was authorized or unauthorized. Note that the CTI to Component Mapping is selected by default and is not configurable.
   - *CTI to Component Mapping*. Checks the Change Management server for a CTI for the current event application and a ticket state of Open or Emergency.
   - *Time Window for Required Change (from Ticket)*. Checks whether the event change time is between the ticket's planned start and end times.
   - *Devices(s) Where Change is to be Executed (from Ticket)*. Checks whether the event change device is in the ticket's device list.
   - *User Assigned to Make Specified Changes (from Ticket)*. Checks whether the event change user is in the ticket's user list.
   - *Approval timeout status for emergency ticket*. Checks for an emergency ticket that has an expired approval status.
7. Click **Save**. Note that other configuration tabs Outbound Ticket, Ticket Expiry, and Emergency Ticket-can be configured at a later time.
8. Click the **Update Agents** button (to the right of the toolbar at the top of the screen) to update the agent on the device specified in step 2.

After you provide the connection parameters and update the Configuration Change Console agent, the agent will collect all categorization attributes from the Change Management server and save them within the Configuration Change Console database.

Depending on which Change Management Server with which you are integrating, you may have additional parameters that must be set in addition to the ones above. Here are some descriptions of these fields:

- Risk Level (used by the Remedy 7 adapter). The value you must set here needs to be a defined risk level in your Remedy 7 instance, such as “Risk Level 1”
- Impact (used by the Remedy 7 adapter). The value you must set here needs to be a defined impact in your Remedy 7 instance, such as “4-Minor/Localized”
- Location Company (used by Remedy 7 adapter). The value you must set here needs to be a defined company in your Remedy 7 instance, such as “Oracle Enterprise Manager” as given as an example in the installation guide on integrating with Remedy 7.
- Support Company (used by Remedy 7 adapter). The value you must set here needs to be a defined company in your Remedy 7 instance, such as “Oracle Enterprise Manager” as given as an example in the installation guide on integrating with Remedy 7.

7.2 Step 2: Configuring the Outbound Ticket Template

Configuration Change Console detects an unauthorized event for any monitored application, and if CT consolidation is not enabled, it creates a ticket on the Change Management server using the Outbound Ticket template. The outbound ticket template must be filled out before the server can create tickets for unauthorized events.

Note that Outbound Tickets are sent to the Change Management server with an "open" status. You can view a list of all Outbound Tickets from the *Visualization ' Change Visualization ' Outbound Ticket History* screen.

There are three ways to close a ticket created by the Configuration Change Console:

- An administrator closes the ticket on the Change Management server.
- The ticket expires upon reaching the ticket's planned end date. Unauthorized tickets have a default planned end date set to 24 hours following the ticket's creation.
- An administrator sets the "stop ticket update" flag on the Change Management server.

To access this screen, navigate to *Administration --> Server Configuration --> Change Management Server*.

Tabs at the bottom of the *Change Management Server* screen enable the three types of outbound ticket and emergency ticket settings.

To update the Outbound Ticket Configuration, follow these steps:

1. In the Outbound Ticket Configuration section of the screen, enter the following information:
   - *Category Definition*. The Categorization that the ticket being created for unauthorized events will receive. Drop-downs will be populated with the categorizations available from the Change Management System. This means that the Unauthorized/Unauthorized/Unauthorized categorization must be created on the Change Management Server.
   - *Supervisor*. The user on the Change Management server who will own the tickets created by Configuration Change Console. The list of users is populated by the users from the Change Management server that have the Send-to-AR flag checked on the user form.
   - *Group*. Optional field which allows you to assign the newly-created tickets to a group of people. The group name you enter here must exist on the Change Management Server.
   - *Urgency*. The urgency to which you want to set newly created unauthorized tickets. The urgency must be a valid value that is available in the Change Management server. Note that this field is case sensitive.
   - *Priority*. The priority to which you want to set newly created unauthorized tickets. The priority must be a valid value that is available in the Change Management server. Note that this field is case sensitive.

   Note: If you delete a setting on which the Outbound Ticket is dependent, such as a Categorization, ticket server or a specified supervisor, the Outbound Ticket will become invalid. The Audit Actions will not generate tickets for unauthorized activities until the Default Outbound Ticket is reconfigured.
2. Click **Save** to save the Outbound Ticket Configuration.
3. Click the **Update Agents** button (to the right of the toolbar at the top of the screen) to update the agent for the Change Management server.

7.3 Step 3: Assigning Categorizations to Component Instances

After setting up the Change Management Server and Outbound Ticket Configuration, you must assign categorizations to all component instances on which you want to audit authorized or unauthorized events.

Assign categorizations from the *Category Component Assignments* screen. Use the Category View to display a list of categorizations to which you can assign component instances. Alternatively, you can filter the screen output with the Component View, which displays a list of component instances to which you can assign categorizations.

To access this screen, navigate to *Policy --> Operations Management --> Category Component Assignment*.

To assign categorizations to a Component Instance (Category View), follow these steps:

1. Select the Category screen display mode from the Selection Mode.
2. Select the Change Management Server.
3. Filter the Category, Type and Item drop-down options or select All and then click **Apply Filters**.
4. From the categorization options shown in the table, select the checkbox for the ones you want to assign and click **Assign New Component Instances**.
5. From the Assign New Component Instances screen, select all component instances that should be associated with the categorization and click **Save**.

7.4 Step 4: Configuring Audit Actions for Authorized/Unauthorized Events

The last step in setting up auditing against the Change Management Server is to configure Audit Actions to perform Change Management actions on authorized/unauthorized events. The Audit Actions specify for certain component instances/applications if you want to create tickets for unauthorized events and/or update tickets for authorized events. Refer to the Configuring Audit Actions section to configure an audit action.

The created audit action will check events on the associated application against their mapped categorizations under the following circumstances:

- If detected changes are authorized, the tickets are updated in the Change Management Server with the event details.
- If Categorization Consolidation is disabled, a ticket will be created in the Change Management Server using the Outbound Ticket Template for each event that is unauthorized.
- If Consolidation is enabled, the unauthorized ticket with a categorization matching that of the unauthorized change event will be appended with the information for the change event. If no matching unauthorized ticket with matching categorization consolidation rules is found, a new ticket will be created using the Default Outbound Ticket configuration.

7.5 Emergency Change Process Flow

When an emergency ticket is received from a Change Management system, the Change Management Server retains the status of emergency (rather than open), to

indicate that the ticket has not yet gone through the standard approval process. For the following 24 hours, any changes associated with this emergency ticket are treated as authorized. During this 24-hour timeframe, if no authorization action is taken and the emergency changes do not get approved, all changes associated with the emergency ticket are set to unauthorized and Configuration Change Console generates a new unauthorized ticket and populates it with relevant unauthorized events. The time out period of 24 hours can be configured when setting up the Change Management Integration.

A Ticket can have three states: Open, Closed, and Emergency. The following table lists the ticket states to the Configuration Change Console as they relate to Emergency Change Requests. Your Change Management server may have hundreds of possible states, but the definitions that are loaded at integration time will translate those states to one of these three states.

Table 7–1 Ticket States

Ticket State	What this means . . .
Open	The emergency ticket was approved on the Change Management server and changes are authorized.
Closed	The emergency ticket was rejected by the Change Management server and therefore any authorized changes will be changed to unauthorized.
Emergency	Ticket has not yet gone through the approval process within the initial 24-hour window.

This emergency ticket feature is optional and can be enabled/disabled via the Change Management Server screen.

To enable emergency ticket configuration and also to configure emergency tickets, navigate to *Administration --> Server Administration --> Change Management Server*.

View the Outbound Ticket History for a list of authorized and unauthorized changes. Each entry shows the emergency ticket number, change event, application instance, and device. Navigate to *Visualization --> Change Visualization --> Outbound Ticket History*.

7.6 Monitoring Change Management Server Integration

Once you have configured the ticket management integration, use the Inbound Ticket History and Outbound Ticket History screens to view the tickets sent between the ticketing server and the Configuration Change Console.

The *Inbound Ticket History* screen shows all tickets sent from the Change Management Server that may be used to determine whether events are authorized. This screen can also show unauthorized tickets that were created by the Configuration Change Console. The *Outbound Ticket History* screen shows the tickets sent to the Change Management Server for either authorized or unauthorized events.

7.6.1 Inbound Ticket History

The Inbound Ticket History screen displays a list of all tickets sent from the Change Management server. To access this screen, navigate to *Visualization --> Change Visualization --> Inbound Ticket History*.

Use the filters to restrict the incoming tickets that are displayed. Click on the link in the Ticket Number column to view a record of any events detected by Configuration Change Console that were mapped to this ticket.

7.6.2 Outbound Ticket History

To access tickets sent from the Configuration Change Console to the Change Management Server, use the *Outbound Ticket History* screen. To access this screen, navigate to *Visualization --> Change Visualization --> Outbound Ticket History*.

Click the link in the Event column to view additional details of the change detected by the Configuration Change Console.

In the *Outbound Ticket History* screen, certain options are available based on the authorized/unauthorized status. If the value in the Authorized column is "Yes", then clicking on the link displays the ticket number to which the change was mapped and a complete history of all events that have mapped to that ticket. If the value in the Authorized column is "No", then clicking the link displays details of the application associated with the change.

> **Note:** Overriding the unauthorized status applies only to reporting within the Configuration Change Console. The change that is overridden will appear as authorized only in the Configuration Change Console dashboards and related reports. It will not affect the ticket's authorization status in the Ticket Management application where the ticket originated.

There are three fields of note on this screen:

- *Override Authorized/Unauthorized status*. Check the box for one or more tickets and click the Override Checked button. You can use override an authorized event to make it unauthorized or vice-versa. Also ticket status can be overridden many times.
- *View Inbound Ticket History*. Click the Authorized link for the selected ticket to view its Inbound Ticket History.
- *View Change Details*. Click the Event status link for the selected ticket. You will be forwarded to the *Trend Analysis* screen for the specific change event.

8

Configuring Threshold Monitoring

Threshold monitoring generates actions in the form of email notifications, SNMP traps and/or reports when specific events occur or thresholds are reached. The actions taken are determined by individual threshold rules, which are aggregated into threshold rule sets to simplify the process of assigning them to devices.

To implement threshold rule sets, use the following general steps:

1. Define threshold rules. These rules vary for the types of resources monitored and can include event- or threshold-driven responses to specific resource states. For example, a rule can generate a notification when CPU utilization reaches a specific threshold or every time a certain account logs on or off.
2. Define threshold rule sets from the rules you have already defined. The rule sets aggregate threshold rules for deployment to specific devices.
3. Assign threshold rule sets to specific devices.
4. Update the agents to put the new rule sets into action.

The following sections describe how to perform these steps in more detail.

8.1 Understanding Threshold Rule Sets

A threshold rule set is a collection of threshold rules. Threshold rules are defined separately and later combined under the umbrella of a Threshold Rule Set.

When defining threshold rule sets, you can do one of two things:

- Create the rules first, then create rule sets from the rules
- Create empty rule sets, and then populate them with rules as you define them

You should begin by deciding what kind of notifications you want to create. You will need to decide what to monitor/act on, who to notify, and what the escalation priority should be.

8.1.1 Threshold Rule Types

Threshold rules monitor specific resources and either act on thresholds being crossed or the occurrence of specific events. The Configuration Change Console supports a number of threshold rule types, depending on the resource being monitored:

Table 8–1 Threshold Rule Types

Rule/resource type	Notification based on…	Description
Process activity (CPU%) User activity (CPU%) CPU load Memory usage File system disk usage Agent inactivity	Predefined thresholds	Generate email notification, an SNMP trap or a report when a resource crosses above or below specified threshold for a specified period of time
User login/logout Error logs Errors in database	Detection of specific events occurring	Generate email notification, SNMP trap or a report on specific events, such as user login/logout or administrative events.

8.1.2 Notification Options

Notification may take place by email and/or SNMP trap.

- Configure SNMP server information using the Administration task:

  Administration --> Server Configuration --> SNMP Administration

- Configure email server information using the Administration task:

  Administration --> Server Configuration --> Email Administration

- If you are notifying via email, you will enter the Configuration Change Console user (defined in the *People* screen) to receive the notification. The email accounts for individuals are created in:

  Administration --> People --> People

8.1.3 Escalation Priorities

When the software sends a notification, it awaits an acknowledgement by the recipient. If the acknowledgement does not arrive within a certain time period, the software escalates the notification according to the rules defined in the priority levels below. The priority levels define how rapidly escalation occurs or if it occurs at all.

This process continues until the notification reaches a recipient without a direct manager.

Table 8–2 Escalation Priorities

Priority	Definition
P1	If the notification has not been acknowledged by the recipient within 5 minutes, the notification is escalated to the direct manager of the recipient. The notification is then escalated every 5 minutes to the next direct manager in the organization hierarchy until it is finally acknowledged, or it reaches the recipient that has no direct manager. The notification will remain in that final manager's inbox whether or not it is acknowledged.
P2	If the notification has not been acknowledged by the recipient within 30 minutes, the notification is escalated to the recipient's direct manager. The notification is then escalated every 30 minutes to the next direct manager in the organization hierarchy until it is finally acknowledged, or it reaches the recipient that has no direct manager. The notification will remain in that final manager's inbox whether or not it is acknowledged.

Table 8–2 (Cont.) Escalation Priorities

Priority	Definition
P3	Notifications that are not acknowledged by their recipient within 4 hours will be forwarded to the next highest peer. If the peer fails to respond within 4 hours, the notification will be escalated to their direct manager. The notification will follow this escalation pattern every 4 hours, alternating between peer and manager, until it is acknowledged or reaches a recipient that has no direct manager. At this point the notification will remain in the final manager's inbox whether or not it is acknowledged.
P4	Notifications that are not acknowledged by their recipient within 24 hours will be forwarded to the next highest peer. If the peer fails to respond within 24 hours, the notification will be forwarded to the next highest peer. If the peer fails to respond within 24 hours, the notification will be escalated to their direct manager. The notification will follow this escalation pattern every 24 hours, alternating between peer and manager, until it is acknowledged or reaches a recipient that has no direct manager. At this point the notification will remain in the final manager's inbox whether or not it is acknowledged.
P5	This priority level has no escalation, whether or not the recipient acknowledges the notification. This priority is useful for informational notifications that do not require an action or an acknowledgement from users.

The escalation sequence continues until the notification is acknowledged or the top of the specified management hierarchy has been reached. All escalations are recorded in the Notification History. Individuals also can manually escalate notifications when responding to a notification.

8.2 Defining Threshold Rules

The Threshold Rules screen, in the Threshold Rule Sets view mode, displays any Threshold rule sets already defined on the system and gives you the opportunity to create new threshold rule sets.

To access this screen, navigate to *Policy --> Threshold Monitoring --> Threshold Rules (Threshold Rule Sets view)*.

A threshold rule set aggregates threshold rules for assignment to devices or device groups. For this reason, it is helpful to first define the rules, and then create the rule sets.

To view rules already defined in the system, select **Threshold Rules** from the View drop-down menu of the *Threshold Rules* screen.

The *Threshold Rules* screen in Rule View lists all predefined rules.

You can restrict the rules displayed according to:

- Rule Type: The type of threshold rule (CPU utilization, user activity, etc.)
- Priority: The escalation/notification priority (P1-P5)

To add a new rule, select from the drop-down menu at the bottom of the screen. The system displays the *Rule Definition* screen for the type of rule you are defining. The resulting screen will vary depending on the type of rule you select.

Every rule has a name, associated administrator, and description.

- The rule name is a required field.
- The administrator is an optional setting for documentation purposes.

- The optional description field is used to document the function of the threshold rule.

The exact options requested on the screen depend on the type of rule you are defining. The rule-specific options are summarized in the following table:

Table 8–3 Rule-Specific Options

Rule type	Type-specific fields/actions
Process activity	Specify the process name or pattern. Enter the CPU threshold and whether to notify when the system is over/under the threshold. Enter the time that the system must remain in the specified state before the policy sends a notification.
User activity	Select login users to monitor from the Users menu. Select the CPU utilization threshold and whether to respond when the system is over or under the threshold. Enter the time that the user account exceeds or falls below the CPU utilization threshold before the policy sends a notification.
CPU load activity	Select the specific CPU name or all CPUs to monitor from the CPU menu. Select the Threshold (% CPU utilization), and whether to respond when the system is over or under the threshold. Select the time in minutes that the system must remain in the specified state before the policy sends a notification. For example, if you select 70% utilization, over, and 10 minutes, then the system must remain at over 70% CPU utilization for a notification to occur.
Memory used activity	Use this rule to monitor memory usage on a managed device. On Windows platforms, memory includes both physical and virtual memory. On UNIX systems, it includes physical memory and swap space. Enter the memory usage threshold (percentage). Select whether to respond when the system is over or under the threshold. Select the time in minutes that the system must remain over or under the threshold before the notification is sent.
Disk used activity	Enter the file system to monitor from the File System menu. Enter the threshold percentage for available disk storage, and select whether to notify when conditions are over or under the threshold. Select a time that the system must remain in the specified state before the policy sends a notification.
Agent no message activity	Select the time in minutes after which to create a notification if there is no message received from the agent. You can optionally select to be notified when the agent starts sending messages after a period of inactivity.

Table 8–3 (Cont.) Rule-Specific Options

Rule type	Type-specific fields/actions
Errors in log	Use this type of rule to monitor errors in the Configuration Change Console log. Specify the error pattern or select a predefined error from the menu to search for in the log. See Appendix E: Predefined Errors for Threshold Rules for a description of predefined errors and a list of potential error messages. If you don't select a predefined error, select the module to monitor. Module options include database, agent, JMS and user interface (UI). If you don't select a predefined error, select the severity level for the error at which to take action. Severity levels are S1-S5, with S1 being the most severe. Each level includes all the severity levels under it. For example, if S3 is selected, the notifications will be triggered for S1, S2 or S3.
Errors in database	Use this type of rule to monitor predefined errors in database logs or specific error messages or error numbers. Enter the client name or a pattern for the client accessing the database. See Appendix D, "Operating System Rule Set Capability Details" for a description of predefined errors and a list of potential error messages. Select a predefined error, or specify the error text. Note that using patterns with an asterisk (*) as a wildcard is allowed.

Once you define the rule, you also define the actions to take:

Field	Description
Notify	Enter the person to notify (from the Configuration Change Console People screen). This sends the notification to the email account associated with that individual.
Priority	Select the escalation priority: P1, P2, P3, P4, or P5. For a description of these priorities, see Section 8.1.3, "Escalation Priorities".
SNMP Servers	Select an SNMP server to which to send a trap. You can select more than one. SNMP Servers have to be configured under *Administration > Server Configuration > SNMP Administration*
Generate Report	Choose a preconfigured report from the drop-down menu to automatically generate this report when notification occurs.

Once you have decided what the threshold or event should be and what the level of response should be, you can define or modify the threshold rule as follows:

1. Enter the name and administrator for the policy.
2. Enter the rule-specific options, described in the table above.
3. Select the notification options, described in the table above.
4. Select **Reports** from the *Generate Report* drop-down menu. Note that reports should be run minimally and on as few devices as possible to avoid unnecessary database load. The report will be sent to the people specified as the notification recipient.
5. Enable or disable the rule: Temporarily suspend notification by unselecting the **Enabled** checkbox.

6. Apply the rule to rule sets. If you already have defined rule sets, you can add this rule to available rule sets. Select a rule set from the *Available Rule Sets* area and move it to the *Selected Rule Sets* area using the >> button.
7. Click **Save** when you are done.
8. To deploy the rules, click the **Update Agents** button in the toolbar at the top of the screen.

8.2.1 Defining Threshold Rule Sets

A threshold rule set aggregates a number of threshold rules and lets you assign them to specific devices.

To access all existing Threshold Rule Sets, select the *Threshold Rules* screen and the Threshold Rule Sets view. To access this screen, navigate to *Policy --> Threshold Monitoring --> Threshold Rules (in Threshold Rule Sets view)*.

To modify an existing rule set, click on the link under the Rule Set Name column for the desired rule set. To add a new rule set, scroll to the bottom of the screen and select the Create Rule Set button. Either way, the *Add or Modify Threshold Rule Set* screen will be displayed.

This screen prompts you to provide information and select available rules for the rule set. Enter the following information for the rule set:

1. Enter a rule set name.
2. Select an administrator to associate with the rule set.
3. Enter a description for the rule set (optional).
4. Select threshold rules for the rule set by highlighting rules from the *Available Rules* window and clicking the **>>** button to move them to the *Selected Rules* window.
5. Click **Save** when you are done. You also can save a rule set under a different name by clicking the **Save As** button, Delete the rule set by clicking the **Delete Rule Set** button, or exit the screen without making changes by clicking the **Cancel** button.

8.3 Assigning Rule Sets to Devices

Once you have defined your threshold rule sets, you must assign them to specific devices.

To access this screen, navigate to *Policy --> Threshold Monitoring --> Threshold Rules (Threshold Rule Set view)*. This screen displays a count device or device group assignments per policy in the Device Assignments and Group Assignments columns respectively. You can assign rule sets to individual devices or to device groups.

To assign a rule set to a device, select the *Threshold Rule Set* view from the view drop-down menu, and click the **Device Assignments** number link for the rule set to assign. This displays the *Device Mode* view of the *Assign Devices to Rule Set* screen.

To assign a policy to a device group, click the **Group Assignments** link for the rule set. This displays the *Group Mode* view of the *Assign Devices to Policy* screen.

Note: You can set up either device assignments or group assignments, but not both at the same time. For example, if you attempt to assign individual devices to a policy that is already assigned to device groups, the established group assignments will become invalid.

The screen can be switched into the following modes through the Selection Mode drop-down menu:

- Device mode displays individual devices in a tree structure based on device groups
- Group mode displays device groups
- Device index mode displays the alphabetical index of available devices

Assign Devices (for all selection modes). Select the device(s) or group(s) to assign the policy and then click **Save**.

8.4 Validating Threshold Assignments

Use the *Validate Threshold Assignments* screen to view summaries of attributes related to threshold rules to help determine if some configuration is missing or incomplete. To access this screen, navigate to *Policy --> Threshold Monitoring --> Validate Threshold Assignments.*

Use the links to view devices without rule sets or devices without team support assignments.

9

Updating Agents With Policies

Whenever you assign or modify a component, rule set, audit action, and so on, you need to update the related agent(s) before the configuration will go into effect. To do this, use the *Update Agents* button in the toolbar at the upper right of the screen.

This displays the *Update Agents* screen.

Use the Group drop-down menu to filter devices by a specific device group.

The Configuration XML link displays the agent's XML-based configuration file in a popup window. This can be used to visually inspect the content that would be sent to the agent if an update agents action is taken.

Either select the individual devices for which to update agents and click **Update Selected**, or click the **Update All** button to update all agents with the relevant configuration.

When updating agents, the request to update agents goes into a queue and agents are updated as the server has resources to do the updates. If only a few agents are updated, they should be updated very quickly after the request. If you are updating the schedule for thousands of agents, only a few will be updated per second. This helps prevent the server and network from becoming overwhelmed when requesting a large number of updates at once.

10

Responding to Notifications

Configuration Change Console offers notification of change events, and escalation of notifications, as defined by audit actions or threshold rules.

There are two ways to respond to notifications:

- Reply to a notification email. All that is required to acknowledge the notification is to reply to the notification email. You do not need to enter any special text.
- Use the Configuration Change Console user interface. From the user interface, you can acknowledge/accept the notification or escalate the notification to the next person, based on the escalation priority. You can also reassign the notification to anyone else in the organization, regardless of the escalation rules.

10.1 Responding to Notifications by Email

When a person receives a notification, it appears in the *Pending Notifications* screen. The same notification will also be sent to the person's primary email address.

The email notification displays both the audit action name and the priority level in the subject line. The content of the email itself lists the reason for the notification and instructions for responding.

To acknowledge an email notification, simply reply to the email without changing any content. To reassign or escalate the notification, you must log in to the Configuration Change Console and use the *Pending Notifications* screen.

10.2 Responding to Notifications with the Pending Notifications Screen

To access all notifications that are sent and unsent and awaiting responses, use the *Pending Notifications* summary screen. To access this screen, navigate to *Visualization --> Activity Summaries --> Pending Notifications*.

Use the following filters to restrict the pending notifications displayed:

- View notification details. Click on the link for the notification ID to view details about the notification.
- Respond to a pending notification. Click the **Respond** button under the notification ID. If you want to respond the same way to several notifications, select the notification check boxes and click the **Respond to Checked** button at the bottom of the table. These options are only available to you if you are the current recipient for the notification.

- View audit action details. Click the **Audit Action** name link for a notification. You will be directed to the *Add or Modify* screen for the selected Audit Action or Threshold rule.

When you respond to a notification, you are prompted to acknowledge, escalate, or reassign the notification. If you have selected multiple notifications, this response will apply to all of them.

To respond to the notification, follow these steps:

1. Choose the action you would like to take:
   - Acknowledge the notification and stop escalation
   - Escalate the notification according to the escalation policy
   - Reassign the notification. If you select this option, you must select the person to receive the notification from the drop-down menu
2. Select **Save** to save your response and return to the *Pending Notification* screen.

11

Viewing and Analyzing Change Events

Configuration Change Console offers several options for examining change within the monitored IT infrastructure.

- Activity Summaries -- These screens provide high-level views of activity in your infrastructure, and include the Activity Dashboard, Pending Notifications, Change Summary and Audit Summary screens.
- Change Visualization -- Use these screens to interactively explore the change events occurring in your infrastructure. You can search by server, user account or application, or look at changes across specific time intervals, and drill down to specific change events.
- Infrastructure Trend -- Use these screens to look at change trends over time. You can examine trends affecting processes, users, files and file systems, memory, CPU utilization, and OS user activity.

In addition, the Configuration Change Console offers reports that can be configured for specific needs through integrating with Oracle BI Publisher.

11.1 Activity Summaries

The *Visualization* > *Activity Summary* menus offer several ways to view change status and related activity across the infrastructure.

Table 11–1 Activity Summaries

Summary	Description
Activity Dashboard	Displays current change or message activity.
Pending Notifications	Displays any notifications that are currently open (not acknowledged)
Change Summary	Summarizes device, process and user account activities during the last hour. Note that change events resulting from internal monitoring are not factored into Change Summary counts.
Audit Summary	Summarizes authorized and unauthorized audit activities in the last hour

11.1.1 Using the Activity Dashboard

The Activity Dashboard displays changes across the infrastructure over a selected timeframe. The data displayed on the dashboard is updated every five minutes. By default, the screen displays change data for the last two hours, but it can be toggled to show data across a user defined time frame by unchecking the Current Data checkbox.

To access this screen, navigate to *Visualization --> Activity Summaries --> Activity Dashboard*.

Refine the view by selecting individual device groups or devices from the drop-down menu. By unchecking the Current Data box, you can specify the exact time period for the graph. Note that the Message Count graph can only be viewed in the two hour live view.

You can also choose whether to display overall change counts, file changes, or agent messages from the drop-down Count menu. The message count indicates that the agent is functioning and communicating.

11.1.2 Viewing Event Summary Statistics

The Event Summary screen is a read-only screen displaying device, process, and user activity during the last hour. To access this screen, navigate to *Visualization --> Activity Summaries --> Event Summary*.

The data shown in this report is summarized in the following table:

Table 11–2 Event Summary Statistics

Category	Description
Top Devices	The most active devices based on the number of process and file changes.
Top User Accounts	The most active user accounts, based on the number of recorded process changes for those users.
Notification Summary	Count of notifications by status: Escalated, Acknowledged, Pending, or Sent.
Top Notification Recipients	The recipients that received the most notifications.

11.1.3 Using the Audit Summary Screen

The Audit Summary screen offers a read-only summary of all authorized and unauthorized audits in the last hour. To access this screen, navigate to *Visualization --> Activity Summaries --> Audit Summary*.

The Audit Summary report includes the following summaries:

Table 11–3 Audit Summary Report Summaries

Category	Description
Top Component	InstancesThe most active component instances based on the number of events.
Top Five Authorized Categories	The five most-used Ticket category combinations with authorized events.
Top Five Unauthorized Categories	The five most-used Ticket category combinations with unauthorized events.
Ticket Summary	The number of ticket updates sent to the Change Management server for both authorized and unauthorized events

11.2 Visualizing Change

Configuration Change Console provides views of your IT infrastructure change activity via the following screens:

- *Server Events* -- Change activity on a specific device or group of devices

- *User Events* -- Change activity made by a specific user account on a specific device
- *Application Events* -- Changes made to specific applications
- *Global Events* -- Changes made to specific files, processes, users, or internal objects across any specified device or device groups during a given time frame
- *Policy Events* -- Changes made ordered by the framework and policy that those changes affect
- *Time Change Journal* -- All changes made to one or more devices over a small period of time
- *Database Inventory* -- Archives of data returned by configured database queries, for database instances monitored by an Inventory agent module

Using these screens you can answer questions such as:

- What changes occurred on this server last night?
- What changes happened across the infrastructure in the hours before a failure of a critical system?
- Did any application changes happen on the financial system during the quarter's closing?
- What changes did a user make from a point we determined the user was not following the proper process?

Each of these screens provides summary details and the ability to drill down to detailed information regarding specific changes.

11.2.1 Viewing Changes to Servers

The *Server Events* screen displays changes that occurred on servers during a defined time period. It offers visibility into process, file changes, user logins/logouts, and component internal events on a specific server.

To access this screen, navigate to *Visualization --> Event Visualization --> Server Event*.

Select **Individual Devices** from the Selection Mode drop-down menu to access individual devices, or select **Device Groups** to view logical groups. The Device Group mode is the default.

- Expand an individual group to list its members, or select **Expand All** to expand all groups.
- Use the Selection Helper to look for devices in specific groups by name or pattern.

Once you have selected the device(s), click **Show Selected** to display the *Server Events* screen.

Use the fields at the top of the screen to select the appropriate timeframe and click **Apply Filters**.

This top level screen that shows counts across multiple devices does not let you click on a count of events. You first must choose a device to view.

Note: The following actions will increase the time it takes to retrieve and report results, and may cause the result set to be truncated:

- Selecting a month time interval
- Selecting a large number of managed devices
- Clicking on a count for a large number of changes instead of narrowing down the time range.

From this screen, you can drill down to view additional information in a number of ways:

- Drill down to a specific server

  Click on the link for a Server name to view how the changes break down by server.

- Drill down to changes within a time window

  Click on a number link in a time column to view the changes in that time window. If the number is larger than 250, it will not be a link. Use the filters at top to narrow down the scope for smaller numbers.

If you drill down to changes by server, you can access the changes broken down into login/logouts, files, processes, and component-internal events.

Use the following to drill down to view details on changes:

- Click on the **Files** link to drill down to a navigation tree of directory or file changes.
- Click on the **Login/Logout** link to display a navigation tree of user logins and logouts, connection types, and related session information.
- Click on the **Processes** link to display process change details
- Click on the **Component Internal** link to list details of internal application changes.
- Click on an individual number link to view the details for changes in that time period. If there are more than 250 changes in a time window, the number will not be a link. Use the Filters to change the time range covered by this screen.

11.2.2 Viewing Changes by User

To display changes by user, use the *User Events* screen. This screen allows you to browse actions taken by a specific user account on monitored devices. To access this screen navigate to *Visualization --> Event Visualization --> User Events*.

Use the alphabet links or search input at the top to narrow the list of accounts displayed, or search for a specific user name.

The User Accounts links list the user names for all user accounts. If the account is a domain account, the account will be displayed as the domain name followed by a slash and the user name. If a user name exists on many servers, it will be displayed here only once. Some user names listed on this screen may be OS users or component internal users such as database users.

Once you click the link for a user account, the *User Events* screen lists the managed devices (for OS users) or component instances (for component internal users) where the account exists. Click the link for the device whose changes you want to view to display the Activity Summary Report.

The *Activity Summary Report* screen lists login/logoffs and process and file activity. It also displays CPU activity associated with the account as a percentage of all CPU usage. The Login/Logoff, Process Activity, File Activity, and CPU Usage rows display an X if there are reported activities during the time period.

- Change or adjust the time period

  Select the time and scale and click Apply Filters

- Drill down to a specific time period

  Click on a column entry to access the details about that time period.

- View a detailed report

  Click **View Details** to display the Activity Details Report described below.

The *Activity Details Report* summarizes user processes, file changes, login activity and CPU usage for the specific device and timeframe if you chose an OS user. If you chose a component internal user, such as a database user, you will see component internal object change events (such as database tables) instead of files and processes. The login/logout for a component internal user will be based on login/logout of the component being looked at.

To list the files that the specific user changed, select the box to show files changed by user. Otherwise, the list will include all file changes during the time period on the device by any user.

> **Note:** The number of files changed can be significant. To reduce the number of changes displayed, reduce the time interval using the filter feature.

For process activity, there are two types of X markers that can be in any time slot. An X that is not a link means that the given process was running during this time period, but did not start or stop (for example: no change activity). If there is an X with a link, that means that there was at least one start or stop of that process during this time period. Clicking the X will take you to a screen to see the actual events.

To view details, you can:

- Click on a column entry to view the process, file changes and login/logout activity details.
- Click on the numbers under the date to zoom into the next time scale.

View files changed by user. The following fields are displayed:

1. Pattern. Enter the process or file pattern to filter the search output. Use the wildcard "*" character to create a search string.
2. Specify User. Select the option Files Changed by User to only view files that have been changed by the specified user. Unselecting this option will show counts of all file changes by all users on the selected device during the specified time interval. This feature can only be used when the audit log has been enabled on the managed device.
3. Start Time. Specify the session time frame by selecting the time, date and scale.
4. Click **Apply Filters**.

To view details for User Login Logout Events, display the *User Change Visualization* screen. To access this screen, navigate to *Visualization --> Event Visualization --> User Events --> Click a Username in User Change Visualization*.

From the *User Change Visualization* screen:

1. Click on a device where the user exists.
2. In the *Activity Summary Report* screen, click the **View Details** button.
3. In the *Activity Detail Report* screen, click an X link in the time column for an activity to display a list of events.

11.2.3 Viewing Application Changes

The *Application Change Visualization* screen enables you to view changes to an application within a specific portion of the monitored infrastructure.

To access this screen, navigate to either *Visualization --> Change Visualization --> Application Events* or *Visualization --> Event Visualization --> Application Events*.

You can select from several modes to define the view:

- Application View (the default). View and select specific applications and component instances.
- Component View. Displays applications categorized by Component Type and Component.

Expand individual applications or component types or select **Expand All** to list and select individual elements.

Once you have selected the component(s) or application(s), click **Generate Report**. The resulting *Application Events Visualization* screen displays details on the changes to the selected set of applications.

Click the application name link to view a change report listing the component instances that make up the application. The rows display the number of reported activities during the time window for each component instance.

If you click on a count link from any of the screens, the details screen will display where you see the events that occurred in that time range on that given component instance. If you instead click on a component instance link under the device column, you walk through each object type and object that had changes.

11.2.4 Visualizing Changes Across Devices (Global Events)

The *Global Events Visualization* screen displays changes across devices within a specific time period. Select the devices or device groups, then apply further filters for processes, files, users or component internal events.

To access this screen, navigate to *Visualization --> Event Visualization --> Global Events*.

- Select the groups or devices you want to report on, or use the Selection Helper to search for a specific device.
- Click **Show Selected**. You will be prompted to refine the report parameters.

Refine the filters for the report by completing these steps:

1. Select Process, File, User, or Component Internal from the pull-down menu.
2. Enter a name for a process or user, or a path for a file.
3. Select the time frame.

4. Click **Apply Filters**.

11.2.5 Visualizing Changes Over Time

Use the *Time Event Journal* to view changes across devices over a specific hour or 15-minute block of a specific date. This screen lets you track activity by user, process, file, or application-internal entity, across devices.

To access this screen, navigate to *Visualization --> Event Visualization --> Time Event Journal*. Follow these steps to fill in the screen:

1. Select the start time and scale for the time event journal.
2. Select the Operating System and Application Internal Users for which to track activity. Use the Ctrl-click key sequence to select multiple users from the drop-down lists.
3. Enter a process, filename, or component internal entity to track. Patterns are allowed.
4. Select the devices or device groups.
5. Click **Show Selected** to create the time change report.

11.2.6 Visualizing Database Inventory

Use the *Database Inventory* screen to view snapshot results of queries run against a component instance monitored by a Snapshot type rule set. This screen displays a chronological listing of logged query results. Each query time stamp displays as a link through which you can view the full archived query result. Selecting a new component instance from the drop-down list will automatically display all queries associated with that application.

To access this screen, navigate to *Visualization --> Event Visualization --> Database Inventory*.

In the list of query results, the second column indicates whether there has been a change from the previous snapshot. The oldest snapshot will always be listed as N/A. In cases where an older version of the agent is running, you may see N/A for other entries because the older versions of the agent did not keep track of changes between snapshots.

Use the drop-down filters to select the component instance for which to display archived query results. Complete these steps:

1. Select the device group from the filter bar.
2. Select the device whose agent is responsible for monitoring the database instance from the Device drop-down menu.
3. Select the individual component instance from the Component Instance drop-down menu.
4. Select the start time and scale for the stored query results.
5. Click **Apply Filters**.
6. From the list of snapshot query results, you can choose the following actions:
   - Locate the query you wish to review. Click a timestamp link to view the archived query result.
   - Check two queries for which you want to contrast the results to view specific differences between the two snapshots.

For each stored query the following information will display:

- *Query Name*. The name given to the query within the component template.
- *Description*. Description of the query's function, as defined in the component template.
- *Query Statement*. Displays the configured SQL query run within the database.
- *Snapshot Time*. Date and time the query was executed in the database server.
- *Row(s) Truncated*. Indicates whether all rows that exist in the database table were returned for the database query. Displays the values true (there are rows in the tablespace not featured in the snapshot) or false (all rows are represented in the snapshot).
- *Column(s) Truncated*. Indicates whether all columns in the database table were returned for the database query. Displays the values true (there are columns in the tablespace not featured in the snapshot) or false (all columns are represented in the snapshot).
- *Query Result*. The results of the SQL Statement presented in the format returned by the database.

11.3 Analyzing Infrastructure Change Trends

The *Trend Analysis* screens provide access to a rich variety of infrastructure trend information for managed devices and applications.

To access this screen, navigate to *Visualization --> Infrastructure Trends*.

The following table displays the infrastructure components.

Table 11–4 Infrastructure Change Trends

Component	Description
Current Processes	Information about active processes, as defined in monitoring policies, currently running on managed devices
Processes	CPU utilization and memory usage for specific processes over a fixed period of time
Files	File changes for a managed device
CPU	CPU utilization trends for a specific time interval on a managed device: Average, minimum and maximum percentage of CPU usage. Note that under the monthly view, the maximum value reflects the average maximum throughout the month.
Memory	Total and virtual memory usage for a managed device over a time interval: Average, minimum and maximum percentage of Memory usage. Note that under the monthly view, the maximum value reflects the average maximum throughout the month.
File System	Available and consumed file storage capacity on a managed device
Component Internal	Changes to component internal objects and specified data points within the component
Detected Users	Information about users with login activity to a monitored application
OS User Activity	CPU usage for all processes a user runs during a specific time interval

By displaying information in a graphical format, these screens help you spot unusual patterns, trends, or potential problems before they become significant. Most of the screens are updated every five minutes, as the various agents that gather information report back to the Configuration Change Console server. To access the screens, select the appropriate screen from the Infrastructure Trends menu.

Each of the screens will prompt you to select specific device groups and devices, and may also prompt for time windows, applications, CPU, and so on. Where possible, information is displayed in a graphical format, making it easier to spot trends. For example, the *Memory* screen shows Memory utilization trends over time.

12

Administering Servers and Agents

This section describes the various tasks involved with administering the Configuration Change Console server and agents.

> **Note:** You must be using a Configuration Change Console account with the super-administrator role to use all of the screens described in this chapter.

The Server Configuration and Reports section of the Administrative menu helps you manage the Configuration Change Console server and database.

The Agent Configuration and Reports section helps you monitor agent status and schedules, remotely pause, stop or start agents, and upgrade agent software versions.

12.1 Server Administration

The following sections describe the server configuration options available, including:

- Configuring the email server connection information for notification emails
- Configuring the SNMP server connection information for SNMP traps
- Managing database size with size thresholds and automated purging
- Disabling/enabling team device limitation settings
- Configuring agent archive file limits
- Configuring administrative alerts
- Configuring dashboard thresholds
- Viewing server/database statistics

12.1.1 Configuring Email Access

Configuration Change Console uses email to send and receive responses to notifications generated by audit actions or threshold rules. Use the *Email Configuration* screen to specify the email address used in email notifications, along with the necessary mail server connection information. This account will be used to both send email notifications and receive notification confirmations.

> **Warning:** Use an email account dedicated to Configuration Change Console notification. The software will purge email from this account on a regular basis.

To access this screen, navigate to *Administration --> Server Configuration --> Email Administration*.

To configure email, follow these steps:

1. Enter the login name and password for the email account to use.

   Use an account that is dedicated to Configuration Change Console notifications, as the software will regularly purge the email from the account.

2. Enable or disable email notifications using the Email Send enabled check box.
3. Enter the mail server and mail store information, and the account to send emails from.
4. Enabled or disable acknowledgements using the Email acknowledgements enabled check box.
5. Enter the mail server type for receiving acknowledgements and the mail store information.
6. The system sends a confirmation email to the selected administrator to confirm that the settings are correct. If authorization fails, the screen appears with the same information. In this case you must update the information or cancel the changes.
7. Click **Save** to save the changes.

12.1.2 Configuring SNMP Server Information

The Configuration Change Console can generate SNMP traps for notifications generated with audit actions, threshold rules, or administrative alerts. Use the SNMP Administration screen to configure or change information about your available SNMP servers. You can configure more than one SNMP server in your environment to receive SNMP traps.

To access this screen, navigate to Administration --> Server Configuration --> SNMP Administration. The screen displays information about any configured SNMP servers.

To modify an existing SNMP server, select the link under the Instance Name column. To add an SNMP server, click the Add SNMP Server button. Either way, the Add/Edit SNMP Server screen is displayed.

Enter or modify the SNMP server information by following these steps:

1. Assign an instance name for the SNMP server. This is a name you will see when you configure audit actions, threshold rules or administrative alerts and want to choose an SNMP server to send traps to.
2. Enter the host name or IP address of the SNMP server.
3. Enter the server's Trap Listen Port. This is the port that the SNMP server is listening to traps on. This port is typically 162.
4. Optionally, add a description of the instance.
5. Select Save to save changes.

After you configure your server, you also must import the two MIBs that are listed in Appendix A of the Install Guide into your software that receives the SNMP traps. This allows the OIDs published to be converted into readable text.

After you set up these SNMP servers, you can choose this SNMP server to send a trap to when a notification would normally happen.

When your SNMP trap receiver gets a trap, the content will typically look like this:

Table 12–1 SNMP Trap Receiver Content

OID	Type	Value
SysUpTime.0	TimeTick	17 days 10h:03m:48s
snmpTrapOID	OID	occNotifNotificationSent
occNotifInfoMessage	String	File c:\oracle\configurationchangeconsoleagent\config\probe.properties of application component Oracle EMCCC Agent on device SERVERABC was modified by user nt authority\system at 05/04/2009 17:07:35 GMT (Local OCC Time 05/04/2009 13:07:35 EDT).

12.1.3 Managing Database Size

Configuration Change Console provides administrators with tools for managing database size. The database size protection feature sets a threshold for the Configuration Change Console database. You can configure notifications to occur when the database size reaches this threshold. Database purging configuration automatically delete older data from the database based on retention rules.

The *Database Size Protection* screen sets a notification threshold to protect the database from filling up with collected events and running out of space.

Set the minimum amount of free space as a percentage of total allocated space for the tablespace. When the available free space falls below this threshold, the software writes an entry to the server log. You can configure a threshold rule to notify an administrator when this event occurs.

To access this screen, navigate to *Administration --> Server Configuration --> Database Size Protection*.

To configure a threshold rule, follow these steps:

1. Enter a threshold as a percentage of total allocated space. Allowed percentage values range from 0 to 20. The tablespace name is set at installation and should not be changed unless the tablespace settings have been changed.
2. Click **Save** to save changes.

12.1.4 Setting Database Purging Policies

Configuration Change Console automatically purges database data after a predefined period, whether or not the database is full. This period can vary according to the type of data.

The *Database Purging* screen displays purging details for select types of change data stored in the database. Details include the number of days that the data will be kept in the database and the date and time of the last purge.

The following Data Types are displayed:

- App Internal Events -- Member tables contain information related to internal application events, such as registry and database changes.
- File Events -- Member tables contain information related to file changes, including creations, modifications, and deletions.
- Notifications -- Member tables contain information related to notifications generated by the 2 solution.

- Outbound Tickets -- Member tables store information related to Outbound Tickets.
- Process Events -- Member tables contain information related to process changes, including starts and stops.
- Process Running -- Member table contains information related to processes currently running in the monitored environment.
- Product Logging -- Member tables contain information related to Configuration Change Console log files.
- SQL Queries -- Member tables contain information related to data returned by SQL Queries run against monitored database instances though SQL Inventory, Snapshot, and SQL Trace agent modules.
- System Resource Stats -- Member tables contain information regarding system resource usage, including CPU, memory, and disk space utilization.
- User Events -- Member tables contain information related to changes initiated by users.

To change the default retention period for a specific data type, click on the link in the *Days to Keep* column for a specific category and table. This displays a screen in which you can set a new limit for the data retention period.

12.1.5 Disabling or Enabling Team Device Limiting

The Team Device Limiting feature lets you limit the Configuration Change Console so that team members can view only the configurations and data for devices assigned to their team. This configuration screen enables or disables team device limiting, but configuration of Team Support Assignments must also be done for this change to take affect.

Team Device Limiting is enabled by default, but only takes effect if you create Team Support Assignments. To disable this feature, use *Administration --> Server Configuration --> Team Device Limiting*.

12.1.6 Configuring Archived File Storage

You can configure Configuration Change Console to automatically archive critical files when they change.

Use the *Archived Files Configuration* screen to set the maximum number of files that can be archived, and the maximum number of copies for any specific archived file. This is used to ensure that not too many copies are stored on the agent-monitored machine.

12.1.7 Configuring Administrative Alerts

You can configure the Configuration Change Console to automatically notify an administrator of critical events, requiring direct administrator actions, occurring within the Configuration Change Console. Once enabled, an email will be sent to the specified administrator when such a critical event is encountered. The email notification will list the date and time of the event, any applicable event trace information (for example, a stack trace), and escalation options for the notification.

To access this screen, navigate to *Administration --> Server Configuration --> Administrative Alerts*. Available Alerts include:

- *Database column precision is too low*. Occurs when an attempt is made to insert a value into a column that is larger than the value type allowed by the column. For example, when a string of 100 characters is inserted into a column handling only

64, or a decimal number is inserted into a column that only accepts whole numbers.

- *Database Shutdown in progress*. Occurs when a database operation is attempted during a database shutdown.
- *Database Size Exceeded Threshold*. Occurs when database table space usage exceeds the threshold specified on *Database Size Protection* screen.
- *Database Unique Constraint Violation*. Occurs when an attempt is made to insert a repeat value (non-unique) into a tablespace column that accepts only unique values.
- *Database Table Usage Rate Exceeded Threshold*. Occurs when database table space usage growth is exceeding a calculated growth rate.
- *Database Value too large for column*. Occurs when the value selected to be written to the database is too large for the selected column.
- *Database Snapshot too old*. Occurs most often when the database rollback segments have been sized too small.
- *Fatal Error in Report*. Occurs when a scheduled report fails to generate.
- *Outbound Email volume exceeded threshold*. Occurs when too many emails are sent during a specific time period.
- *Agent Internal Monitoring connectivity error*. Occurs when the agent is unable to successfully perform an application-internal monitoring operation due to a lack of a connection.
- *Agent SQL Trace/DB2 Data loss*. Occurs when the data pipe within DB2 becomes clogged, thus causing interrupted, or restricted data flow to the agent.
- *Report PDF Run-Time Exceeded Threshold*. Occurs when data for a generated report exceeded the maximum size. In this case, only the data up to the size limit would be included in the report.
- *State Change on Agent*. Occurs when an agent changes its status, for example when an agent changes from "Running" to "Hold".
- *Agent command failure*. Occurs when an agent attempts to run a native command, such as sysinfo or filewatch, and fails.
- *Notifications: outbound E-mail volume exceeded threshold*. Occurs when too many emails are sent during a specific time period.

To activate administrative alerts:

1. Checkmark the Active box for the alert.
2. Select an administrator to receive notifications.
3. Select an SNMP server through which to send email notifications (optional).
4. Select an escalation priority level for the notification. For a description of these priorities, see Escalation Priorities.
5. Click **Save**.
6. If the alert requires a device assignment, click the **Device Assignments** count link.
7. Assign the policy to the devices through the *Assign Device to Policy* screen.
8. Update the agents on the associated devices.

12.1.8 Configuring Dashboard Thresholds

Use the Dashboard Threshold Configuration screen to establish the thresholds that are used on the dashboards for policy compliance. Control thresholds affect how the dashboard dials report event activity.

To access this screen, navigate to *Administration --> Server Configuration --> Dashboard Thresholds*.

Select a framework and associated policy. See Frameworks and Policies for a list of the available framework and policy combinations that come with the product.

Set the low and high thresholds for each of the listed summaries. Each summary maps to either a dashboard dial or a tab in a dashboard screen. For a control's Summary Dial, the low threshold defines when the needle appears in the green section of the dial, while the high threshold defines when the needle moves to the red portion of the dial. The values between the low and high threshold would indicate the needle would be in the yellow region.

Note: Threshold values cannot be below 0 or above 100. Also, the low threshold cannot be equal to or greater than the high threshold. All threshold fields are required.

12.1.9 Configuring LDAP Integration

For rule creation for components, the user can optionally get user based rules from an integrated LDAP server. The *Configuring LDAP Integration* screen lets the user integrate their installation of Configuration Change Console with one or more LDAP servers.

Clicking on the **Add New Instance** button or clicking on a linked instance name will take you to the screen to add or update an LDAP Server.

12.1.10 Viewing Server Information: Server Reports

The following administrator screens (reports) are available from Administration --> Server Reports.

Table 12–2 Administrator Reports

Report	Description
Active Sessions	Provides information about the people currently logged into the Configuration Change Console server.
System and Database Log	Displays system and database error messages encountered during a specified time period.
Log files	Lists all logs generated by the system and allows you to view or download individual log files. For the *ar-server.log* file, you can also empty the log and copy its contents to another file (provided by the Roll Over link.)
Specification Change Log	Displays logs of changes to policy specifications, based on policy assignment types and monitoring methods, during a user specified time frame.
Data Growth Trends	Displays data growth over time for selected Configuration Change Console agent modules, during a user specified time period.
Diagnostics Report	Displays configuration and current monitoring info for the monitored environment that can be used to diagnose issues with the deployment.

12.2 Agent Administration

Configuration Change Console agents, installed on each monitored server collect change events from the monitored server and report these changes back to the Configuration Change Console server. The agent communicates with the server through a JMS (Java Messaging Services) bus.

If an agent's connection to the JMS bus is lost for any reason, the agent buffers the data on the local monitored device until the connection is restored. The collected data buffered in the agent will then be sent to the server and the agent will resume normal operation. There is a limit to the maximum size of the buffer. Each agent can hold 5MB or 2 hours' worth of data, whichever occurs first. This size limit can be configured during the agent installation.

The agents collect and send data to the database according to a schedule, which varies according to the type of agent and information being monitored. An agent schedule template defines the intervals for agent data collection/transmission and which modules are used in monitoring. These modules are described in the following section.

An agent schedule group is a group of agents assigned to a specific schedule template.

The *Agent Schedule Template Group Assignment* screen allows an administrator to specify which device groups use each Agent Schedule Template. Each schedule group can have only one template associated with it at a given time.

The following agent modules are used in Agent Schedule Templates:

- HostConfig -- Collects basic system information
- CPUConfig -- Takes inventory of processor configuration
- CPURunning -- Tracks processor resource usage
- MapiMonitor --Tracks all MAPI related system and notification information
- MemConfig -- Takes inventory of physical and virtual memory configuration
- MemRunning -- Tracks all physical and virtual memory resource usage
- FSConfig -- Takes inventory of the existing file system structure
- FSRunning -- Tracks all file system resource usage
- IPConfig -- Takes inventory of network configurations
- FileRunning -- Track changes to files
- UserRunning -- Tracks user logins and logouts
- ProcessRunning -- Tracks process starts, stops, and resource usage

12.2.1 Viewing Agent Schedule Templates

Configuration Change Console comes prepackaged with the following default agent schedule templates:

- Performance and Change -- Tracks all performance and change-related issues. Comprised of all modules
- Performance Only -- Tracks resource usage related to performance
- Change Only -- Tracks all change-related issues. Comprised of Change Modules only: HostConfig, FSConfig, FSRunning, IPConfig, FileRunning, UserRunning, and ProcessRunning modules
- MAPI Broker -- Tracks all MAPI related issues

- NT Lite -- Tracks performance and change related issues on Windows NT based devices. Comprised of a minimal set of modules meant for NT devices that do not have WMI 1.5 installed. Includes HostConfig, FSConfig, and FileRunning modules
- OS/400 -- Tracks performance and change related issues on OS/400 based devices. Includes all modules supported by the OS/400 agent: HostConfig, FSConfig, and FileRunning
- Default -- Tracks basic system information. Includes only the HostConfig module

To access this screen, navigate to *Administration --> Agent Configuration --> Schedule Templates*.

To view the schedule details for each module, click on the link in the # of Enabled Modules column. This displays a screen that lists the interval and offset for each module and contains the following fields:

- The interval (in seconds) is how frequently the agent sends the data.
- The offset is the time offset for the initial run of the module. For example, if the Interval is 60 and the offset is 30, the initial process will take 90 seconds to complete a cycle, but adhere to the regular 60 second interval thereafter.

The intervals that are defined on this screen can be changed by clicking on the link on the agent module name. The interval and offset values that are set by default are the recommended intervals. There are some times however that it is desired to extend the interval so that the agents are not reporting events as often.

There are some caveats though to setting the intervals to be too long. For instance, the AppRunning interval is used to control reporting and monitoring intervals for all component internal modules such as Database monitoring and Active Directory Monitoring. If you extend the interval too long, events that may have occurred may roll off of the audit log and may not be available to be reported against anymore.

12.2.2 Creating/Assigning Schedule Groups

The *Agent Schedule Groups* screen displays the agent schedule groups and the number of devices in each group.

To access this screen, navigate to *Administration --> Agent Configuration --> Schedule Groups*.

Each managed device must belong to a schedule group. Devices can belong to only one group at a time, and each group can be assigned only one schedule template. The assigned schedule template will apply to all devices within the schedule group.

- To modify an agent schedule group, click the link in the **Group Name** column.
- To add a new schedule group, click **Add a Schedule Group**.

Either way, the *Add or Update a Schedule Group* screen will be displayed. From this screen you can name the group and select devices to assign to the schedule group.

12.2.3 Assigning a Schedule Template to a Schedule Group

Use the *Schedule Template Group Assignment* screen to assign a schedule group to a schedule template. In the *Agent Schedule Templates* screen, click the link for the **# of Schedule Groups** to add a schedule group to a specific schedule template.

A schedule template can be assigned to multiple schedule groups, but each group can only be assigned one schedule template. The assigned schedule template will apply to all devices within a schedule group.

To access this screen, navigate to *Administration --> Agent Configuration --> Schedule Templates: # of Schedule Groups link*.

12.2.4 Stopping, Holding, Resuming and Pausing Agents

Administrators can stop, pause, hold, resume or restart the agent service from a centralized location without having to access the machine directly.

> **Note:** An agent that has been stopped must be restarted manually from the device on which it is installed.

The available options are:

- Hold -- The agent continues collecting data and buffering it locally, but does not send the data until you resume the agent's communications
- Pause -- Pauses the agent; the agent does not collect data nor send data until you resume the agent's communications
- Resume -- Causes an agent which is in a Pause or Hold state to resume collecting and sending data
- Restart -- Restarts a running agent
- Stop -- Stops the agent. The agent must be restarted manually on the managed device after this command

The *Manage Agents* screen allows you to change the current state of an agent by device(s) or device group(s).

To access this screen, navigate to *Administration --> Agent Configuration --> Manage Agents*.

Manage agents by following these steps:

1. Select the device group or devices to manage.
2. Select either **Hold**, **Pause**, **Resume**, **Stop**, or **Restart**.
3. Click **Submit** to put the operation into effect on the agent.
4. A confirmation message will appear asking you to confirm the action; click **OK**.

12.2.5 Upgrading Agents From the Server

The Configuration Change Console allows for upgrading agents remotely from the primary server's web-based interface. The server installation already comes packaged with the agent upgrade code to match the version of the server. When upgrading your environment, you would upgrade the repository and servers first and then perform the upgrade to the agents from the new version of the server. This means that for some time between server upgrade and agent upgrade, the agents will still be running the previous version.

To access this screen, navigate to Administration --> Agent Configuration --> Upgrade.

On this screen you can filter your device list by the device groups and select one or more devices to upgrade. The table that shows the devices lists the device name, operating system, current agent version and the most recent version available to upgrade to. The status column lists the upgrade status. The agent for 10.2.0.4 has a version of 5.1.0 and the agent for 10.2.0.5 has a version of 5.1.1.

From the table, you can choose a single device to upgrade or select to upgrade all. After choosing the devices to upgrade, you can schedule the time to upgrade or perform the upgrade now.

Depending on the scheduling and success of an upgrade, the following may display in the Status column of the Upgrade screen.

- Pending. The upgrade has been scheduled, but has not yet been executed.
- Executing. The upgrade is currently in progress.
- -- (Normal status). Following a Pending or Executing status, the -- indicates that the upgrade has completed successfully.
- Cancelled. The scheduled agent upgrade has been cancelled. The agent status will remain in this state until another upgrade is scheduled.
- Failed. There was no response from the agent after 15 minutes of executing an agent upgrade.

12.2.6 Viewing Agent Information (Agent Reports)

Configuration Change Console offers a number of read-only screens that provide you with information about agent availability and statistics, and allow you to view agent log files.

Available agent reports include:

- Statistics -- The Agent Statistics screen provides information about processes run by the agent on managed devices. The screen displays a count of messages and instances sent since the counters were last cleared. Each instance represents a single change. You can clear the counters from this screen.
- Log Files -- Lists all or a group of agent devices, and lets you retrieve zipped log files from specific devices.
- Availability Report -- This screen provides a graphical representation of an agent's availability on a specific device over a specified time period.

13

Configuring, Generating, and Viewing Reports

Configuration Change Console provides a library of predefined reports to aid in analyzing compliance with policies and spotting potential problems. These reports can be viewed online, printed, or distributed to specific individuals. To create reports specific to your environment, you must create report instances, based on predefined reports.

Several steps are required to complete the report-configuration process. Some tasks must be completed prior to using Configuration Change Console Auditor and other steps can be taken using the Configuration Change Console report features.

Before you can use the Configuration Change Console report features:

1. Install and configure the BI Publisher Server, if it is not already available in your enterprise. Refer to the *Configuration Change Console Installation Guide*.
2. Publish the Configuration Change Console reports to the BI Publisher Server. This step integrates the Configuration Change Console reports into the BI Publisher Enterprise system. You can select from a list of reports provided with the Configuration Change Console product. Refer to the *Configuration Change Console Installation Guide*.

Using the Configuration Change Console report features, described in this chapter:

1. Configure the Configuration Change Console BI Publisher Server, described in Section 13.1, "BI Publisher Server Configuration".
2. In the Configuration Change Console *BI Publisher Deployment* screen, described in this chapter, customize the run-time parameters and make report instances available for users to run.
3. Create a report instance (a specific, customized version of the deployed report), based on a predefined report.

13.1 BI Publisher Server Configuration

The *BI Publisher Server Configuration* screen completes the integration with your BI Publisher software. Using this screen, you can establish the connection with your BI Publisher Server.

To access this screen, navigate to *Administration --> Server Administration --> BI Publisher Server*.

Configure the following parameters:

- WSDL Definition. The full Web Service Description Language definition for the supported BI Publisher Web Service is accessible through the hostname or IP address and the port of the BI Publisher server. The default port is 9704.

  http:// <servername>:<port>/xmlpserver/services/PublicReportService_v11?wsdl

- User name -- Used to connect to the BI Publisher server web portal interface. This field is case sensitive
- Password -- The password used to connect to the BI Publisher server web portal interface
- Password (verify) -- Used to verify accuracy of the password entered in the Password field
- Report folder -- The name of the folder in which the published reports are stored, in the format */folderName*

  You can verify the folder through the BI Publisher Central Management Console, located in the following location where *servername* is the BI Publisher server hostname or IP address, and *port* is the access port number:

  http://<servername>:<port>/xmlpserver/

  Following console login, click the "Shared Folders" link and enter the folders page. Locate the folder and verify the folder name.
- Is Enabled. Used to enable or disable the BI Publisher server configuration. If the configuration is disabled, all the activities (such as synchronizing the report templates from the BI Publisher, running the report, and so on) between the Configuration Change Console server and Publisher server will be stopped or disabled. Users can only view the existing reports in the Configuration Change Console system.

13.2 BI Publisher Deployment

This section provides instructions for deploying BI Publisher Reports through the Oracle Enterprise Manager 10g Configuration Change Console user interface. Follow these steps to deploy BI Publisher Reports:

1. Log into the Oracle Enterprise Manager 10*g* Configuration Change Console Product interface using the Administrator login
2. From the Navigation tree, select *Administration* > *Server Configuration* > *BI Publisher Reports Deployment*
3. The *BI Publisher Reports Deployment* screen will display. This screen shows all reports that have been published on the BI Publisher Server. The columns displayed include:
   - *Report Name* -- The name of the report as published in the BI Publisher server
   - *Description* -- A brief description of the report, specified in the BI Publisher Server
   - *Deployed* -- Indicates whether the report can be seen/run by users in the Oracle Enterprise Manager 10g Configuration Change Console server
   - *Default Parameters* -- Indicates whether default parameters have been configured through the Oracle Enterprise Manager 10g Configuration Change Console user interface, for use by the Oracle Enterprise Manager 10g Configuration Change Console server in report generation

- *Last published in BIP Report Server* -- The date the report was published into BI Publisher Server

Click on a **report name link** to configure default parameters for the report, as well as to modify the deployment status.

Check the checkbox and click the **Deploy checked reports** button to make the report available in the Oracle Enterprise Manager 10g Configuration Change Console server.

4. Click on a **Report Name link** to configure any default parameters for the report, as well as modify the report deployment status.
5. The *Update a BI Publisher Reports Deployment* screen will display. Click the deployed checkbox to make the report available in the Oracle Enterprise Manager 10g Configuration Change Console server.
6. Specify the following report elements:
   - *Report Start and End times* -- Specify the start and end time for report data set. The report will include data collected within the time interval specified. Note that certain reports feature an Include Current Hour option which can be toggled to include all data collected during the hour leading up to the report.
   - *Report Parameters* -- Specify a range of data elements to include by default in each report. Depending on the report type, you will have a different set of configurable Default Parameters. These include such things as individual monitored devices, or device groups, application users, and/or individual files (The report in the screenshot below features an input field for file rules). Note that most reports feature only device and group report parameter selections. Further note that you can select device groups or individual devices, but not both at the same time.

   Repeat steps 4 through 6 for all reports that you want to make visible through the Oracle Enterprise Manager 10g Configuration Change Console user interface. Once the reports have been deployed they will be viewable by all users on the Oracle Enterprise Manager 10g Configuration Change Console server.
7. Navigate to *Reports* > *Configure Your Reports* > *Reports* to view all the report instances created by the available reports that have been deployed into the Oracle Enterprise Manager 10*g* Configuration Change Console server
8. Click the **Add Report Instance** button or the report instance name link to create/update the report instance. Fill in the following information:
   - *Report Instance Name* -- The unique instance name
   - *Report* -- The report list that has been deployed into the Oracle Enterprise Manager 10*g* Configuration Change Console server (we can call them report templates)
   - *Description* -- the description from the selected report template. Also you can change it
   - *Run Schedule* -- Specify the schedule for this report instance. Currently we support Daily, Weekly, Monthly, First day of the month and None (means no schedule)
   - *Run on Demand?* -- If you uncheck it, the report can't be run
   - *On demand parameter?* -- Specify whether you should re-configure the parameter's value before running the report instance or not. Checking it means need to re-configure the parameter's value, otherwise not

- *Priority* -- Use to define the priority when sending notification for the generated report. The range is from P1 to P5, P1 is most urgent

9. Click the number link under the Recipients column on the *Configure Report Instances* screen and navigate to the *Report Distribution List* screen.

   You can specify the person who can receive the notifications.

10. After the report instance is created, navigate to *Reports > View Your Reports > View Reports*. You can generate a report by clicking the report's **Run Now** link. When running a report you will have the option to specify unique runtime parameters only when the *On demand parameter?* checkbox is checked. By specifying runtime parameters you can override the default parameters configured for the report.

11. Once a report has generated you can click the page icon next to the report name to view the report.

13.2.1 Update a BI Publisher Deployment

Using the *Update a BI Publisher Reports Deployment* screen, you can modify the deployment or active status of a configured BI Publisher Report.

To access this screen, navigate to *Administration --> Server Configuration --> BI Reports Deployment --> Report Name link*.

The following details are displayed for each report, with the capability of configuring the Deployed status and the default parameters:

- *Report* -- The report name is displayed as a link in the *BI Publisher Deployment* screen to direct you to the *Update a BI Publisher Deployment* screen
- *Last Published Date* -- Date and time the report was last published
- *Description* -- Brief description of the information contained in the report (optional)
- *Deployed* -- Indicates whether or not the current report is active
- *Default Parameters* -- If the report accepts parameters, you can select which parameters are included by default. For example, you may be able to include start and end times for each event in the report, or you might be able to specify device groups or individual devices for application instances

13.3 Configuring Report Instances

To configure an offline report, define the general report and then assign and configure report modules from the predefined report library supplied with the installation package. The *Configure Report Instances* screen displays a list of reports that have already been configured.

To access this screen, navigate to *Reports --> Configure Your Reports --> Reports*.

To create a new report instance, click the **Add Report Instance** button. To modify an existing report instance, click the link in the *Report Instance Name* column. Either way, the *Configure Report Instance* screen is displayed. Enter the following report details:

- Instance Name -- Unique name identifying the report
- Report -- Select one of the packaged reports from the drop-down list
- Description -- Brief description of the content or purpose of the report
- Run Schedule -- Enter the options for when the report will run, if scheduled. Select **None** if there is no need to have the report run at regular intervals

- Run on demand -- Check this box to enable a user to run reports when needed. When this box is checked, the default parameter values are used at run-time
- On demand parameter -- Check this box to require a user to supply parameters, such as the start time and distribution list, at run-time. If you check *Run on demand* without checking the *On demand* parameter, the report will use the default parameter values at run-time
- Priority -- Set the notification priority. See Escalation Priorities

Click **Save** to save changes or **Reset** to reset the fields.

13.3.1 Selecting Devices for Report Instances

By default, no devices or device groups are selected for any report; you must assign them to a report instance. In Devices mode, you can select devices individually. In Group mode, if devices are added or removed from the group, the report will change dynamically, but you cannot change the selection of individual devices using the group mode. By default, a group includes all devices in that group.

To access this screen, navigate to *Reports --> Configure Your Reports --> Reports --> Report Name link*.

To select device(s) for a report, follow these steps:

1. Select a Device Mode: either Groups or Devices
2. Select specific devices or device groups
3. Click **Save** to save changes or **Reset** to reset the fields

13.3.2 Configuring the Report Distribution List

The *Report Distribution List* screen allows you to select the people or team(s) that will receive reports.

If you assign a report to a team, new members will receive the report on joining the team. If you unselect a person from a team, then that person will be excluded from receiving the report. If you do not select a team and you select only select individuals from that team, then the report will only be sent to the specified individuals, even as the team membership changes.

From the *Configure Report Instances* screen, click a link in the **Recipients** column.

To access this screen, navigate to *Reports --> Configure Your Reports --> Reports --> Recipients link*.

Note: You also can access this screen if you have configured a report instance to enable on-demand parameters. When you click the **Run Now** link in the *BI Publisher* screen, you will see this screen as the second set of on-demand parameters.

To specify the distribution list, follow these steps:

1. Select **Individual People** or **Teams** from the drop-down option. If you select Teams, expand the teams to display a list of all users assigned to the team.
2. Select specific users or teams to receive the report.
3. Click **Save** to save changes or **Reset** to reset the fields.

13.4 Generating and Viewing Reports

By default, all BI Publisher reports can be viewed by a user through the Configuration Change Console user interface. The administrator also has the option of sending the generated PDF report to specified users via email.

To access this screen, navigate to *Reports --> View Your Reports --> View Reports*.

To instantly run a report, click the **Run Now** link to instantly generate the selected report. If the report is configured as an On-Demand report, you will be prompted to supply parameters. The report will generate and its status will change to Running until it has run successfully. If problems are encountered, the *Last Run Status* will display an error message. To view an existing report, click on the **Report Name** or the PDF icon to report as of the last run date. You need Adobe Acrobat Reader on the local system to view the PDF file.

The *BI Publisher* screen displays the following details:

- Instance Name -- The report name is displayed as a link that directs you to the *Configure Report Instance* screen where you can view items such as the run schedule and report settings. A PDF icon will be displayed next to the report name if the report has been generated. Click the PDF icon to view the PDF file.
- Description -- The content and purpose of the report as provided by the user
- Report Name -- The deployed report to which the instance is related
- Last Run Date -- Date that the report was last run
- Last Run Status:
  - Completed -- The last report generation completed successfully
  - Report ran too long -- The last attempt to generate a report took an excessive amount of time. The report did not generate correctly
  - Report too large, truncated -- The last report generation resulted in an excessively large file. The final report made available did not include all the available information so as to remain within file-size constraints
  - Exceptions encountered -- The last report generation attempt ran into errors. The report did not generate successfully
  - Could not write report -- The last report generation attempt could not write the data to a PDF file. The report did not generate successfully
  - Unknown fatal error -- An error was encountered during an attempted report run. Report did not generate successfully
  - Running -- A report run is currently in progress. The generated report will be available shortly.
- Run Now -- This option is only available if the report has been configured to run "on demand" from the *Configure Report Instance* screen. An *On Demand Report Parameters* window will prompt you to verify your action. If you click **No**, the report will run using the default parameters as defined in the *BI Publisher Deployment* screen. If you click **Yes**, the first of two *BI Publisher Report Instance Parameters* screens will display.

The parameters shown on this screen depend on what has been configured for the report instance. At a minimum, you will need to specify the Time or Time Range:

- Specific Time Report Start and End -- The report will generate data starting from the specified number of days and hours before the scheduled report run time.

Then the report will stop collecting data ending at the specified number of days and hours before the scheduled report run time.

- Time Range -- As an alternative to a specific run time, you can configure a broader time period in which the report should run. Specify the *Report Start and End* range by entering the number of days and hours before the report run. To include the current hour, select the *Include Current Hour* checkbox.

Click the **Next** button to configure the Report Distribution List. Select **Individual People** or **Teams** from the drop-down option. Click **Apply Filter**.

13.5 Viewing Online Reports

The Configuration Change Console solution comes with a number of other online reports available from the Reports menu.

- Notification History -- Lets you examine notifications generated by the Configuration Change Console solution
- Inventory History -- Displays detailed information about infrastructure components. For each device, offers information about CPU, file system, network configuration, and so on
- Archived Files -- Displays information about archived files
- Device Rules Summary -- Displays information about all component rules defined for specific devices

For each of these reports, you can select specific devices and timeframes to confine or filter the information displayed.

A

Predefined Component Templates

The following Predefined Component Templates are packaged with Configuration Change Console:

- Apache 1.3.x Linux
- Apache 1.3.x Solaris
- Apache 2.0.52 Linux
- Apache 2.0.x Fedora
- Apache 2.0.x RedHat 9
- Apache 2.0.x SuSE 9.1
- IIS 5
- IIS 6
- Microsoft SQL Server 2000
- Microsoft SQL Server 7
- Oracle 9i for Windows
- Oracle Assets
- Oracle 9i Auditing
- Oracle Cash Management
- Oracle EM CCC Server
- Oracle EM CCC Agent
- Oracle General Ledger
- Oracle Payables
- Oracle Receivables
- Solaris 9
- VMWare GSX / Linux
- VMWare GSX / Windows
- Windows 2000
- Windows NT

B

Operating System Rule Set Capability Details

Descriptions of the various Operating System rule sets are already included earlier in the document, but this appendix is meant to capture the details that might not be covered earlier.

As discussed earlier in the users guide, there are two types of monitoring capabilities, or rule sets, in the Configuration Change Console. The first is the monitoring done at the OS level, such as Files (changes, reads), Processes (starts and stops), and OS Users (login and logouts). The second type is referred to as Component Internal Rule Sets. These are monitoring capabilities for entities inside of an application or piece of software.

The following lists the operating system rule set capabilities that this release of Configuration Change Console supports with a description of capabilities.

- Files
- Processes
- OS Users

Each rule set is discussed in detail in the rest of this chapter.

Files

This monitoring capability uses the various operating system capabilities to monitor file changes in near real-time. This rule set can capture file changes and reads, as well as the user that performed the action, exact time, process id and type of change.

The operation of the file rule set depends on many specific setup requirements per operating system. To view requirements, please see the *Configuration Change Console Installation Guide* for instructions related to the agent for your operating system.

Rules

You can create up to 50 include or exclude rules for this rule set in a single component. The following pattern types are available for creating rules.

Table B–1 Pattern Types for Rules

Pattern Type	Description
Write	For this rule, you are only looking for write activity of a file or the directory name specified in the Files column.
Read	For this rule, you are only looking for read activity of a file or the directory name specified in the Files column.

Table B–1 (Cont.) Pattern Types for Rules

Pattern Type	Description
Access	For this rule, you are only looking for access activity of a file or the directory name specified in the Files column.

You can use the *Is Relative Path* option to specify that the first part of the pattern in the File column is relative to some other directory. Then in the *Default Path* field, enter the prefix path that is used in front of each rule that has *Is Relative Path* selected. You can see the actual full path that will be used under the *Effective File/Directory Path* column. Later after you create multiple instances of this component by assigning it to multiple devices, you can override the default path for specific devices. For instance, on some devices your default path might be *c:* and on some others it might be *d:*. You can still handle this with just one component definition.

To filter the changes against files by the user that made them, you can add an OS User rule set to the same component and check the box on the OS rule set that indicates these users are for filtering other types of rule sets. Then in this file rule screen, check the *Filter change data by Users defined in component* box.

To save a copy of a file when it changes so that it can be recovered later or used to compare other versions, click the *Archive* checkbox for the rule. This checkbox will only work if the rule specifies one specific file. If a directory is specified for this rule, then the archive checkbox will be ignored.

The following guidelines should be followed when creating rules for this rule set:

1. On Unix platforms, file separator is '/'; on Windows platform, file separator is '\'.
2. A pattern matching a directory includes all of its sub-directories and files under the directories.
3. Use a wildcard (*) after the last slash for pattern matching.

   Example: Pattern *c:\mydocs*.doc* matches any file under *c:\mydocs* ending in *.doc*.
4. If two or more patterns match the same file/path, the pattern with greater length takes precedence.

   Example: Include *c:\mydocs*.doc* and Exclude *c:\mydocs*oc* match file *c:\mydocs\calc.doc*. Since *c:\mydocs*.doc* takes precedence because it is longer, the file *c:\mydocs\calc.doc* will be included.
5. Include patterns take precedence over excludes when the pattern lengths are the same for a given pattern type.

   For example: With two rules for *User* pattern type: Include *, exclude *, all events will be captured.

Processes

This monitoring capability uses the various operating system capabilities to monitor process starts and stops in near real-time.

Rules

You can create up to 50 include or exclude rules for this rule set in a single component. The following pattern types are available for creating rules.

Table B–2 Pattern Types for Creating Rules

Pattern Type	Description
Event	For this *Include Processes* rule, only monitor for process start or stop activity.
Resource	For this rule, only monitor the cpu, memory usage of the process with a single value recorded every 5 minutes which is a rolling average calculation of multiple time points within that 5 minute period. These performance data are visible under Trend Visualization screens. This option will only work if you have set the devices this component is assigned to using the *Change and Performance Agent Schedule* template. See *Agent Schedule Templates* for more information.
Both	For this rule, capture both starts and stops as well as performance data. See the note for Resource as it also applies to this option.

If you want to filter the changes against process by the user that made them, you can add an OS User rule set to the same component and check the box on the OS rule set that these users are for filtering other types of rule sets. Then in this process rule screen, check the box that says *Filter change data by Users defined in component*.

The following guidelines should be followed when creating rules for this rule set:

1. On Unix platforms, process names are case sensitive.
2. The process pattern should only contain the process name. It should not contain the file path. For example, use "bash", but not "/bin/bash" in the process name.
3. Use a wildcard (*) to match any characters. For example: use "v*" to match any process starting with "v".
4. If two or more patterns match the same file/path, the pattern with greater length takes precedence. For example: Include v* and Exclude pattern *ix match process fix. Since *ix takes precedence because it is longer, the process *vix* will be excluded.

Processes On OS/400

This monitoring capability is a little different than processes on other operating systems. On the OS/400, there are two elements monitored under the processes rule set; jobs and commands. The way you configure the rules is similar to processes on other operating systems, but there are some minor differences.

Rules

You can create up to 50 include or exclude rules for jobs and commands for this rule set in a single component. The following pattern type is available for creating rules.

Event -- For this Include Processes rule, only monitor for process start or stop activity.

The pattern name for Job and Command is the name of the Job or Command you want to monitor for activity.

If you want to filter the changes against process by the user that made them, you can add an OS User rule set to the same component and check the box on the OS rule set that these users are for filtering other types of rule sets. Then in this process rule screen, check the box that says *Filter change data by Users defined in component*.

The following guidelines should be followed when creating rules for this rule set:

1. Job names and Command names are case-sensitive.
2. Job and Command pattern should only contain the name. It should not contain the file path.
3. Use a wildcard (*) to match any characters. For example: use "v*" to match any job or command starting with "v".
4. If two or more patterns match the same name, the pattern with greater length takes precedence. For example: Include v* and Exclude pattern *ix match process vix. Since *ix takes precedence because it is longer, a command named *vix* will be monitored.

OS Users

This monitoring capability uses the various operating system capabilities to monitor user login and logouts in near real-time.

Rules

You can create up to 50 include or exclude rules for this rule set in a single component. The following pattern types are available for creating rules.

Table B–3 Pattern Types for Creating Rules

Pattern Type	Description
User	The pattern will have a user name pattern you want to include or exclude.
Connecttype	The pattern is a connect type to filter events by. Values are like console, telnet, ssh, ftp, and rdp for windows only.

If you want to use these user definitions in this rule set of this component to filter other types of events like file changes, process starts and stops, or windows registry changes, you can do this by creating rules and selecting the checkbox *User for filtering other types only, not for inclusion/exclusion of user login/logout events*. Then in the other rule sets of this component, check the box that says *Filter change data by Users defined in component*.

If you have integrated your Configuration Change Console server with an LDAP server, you can also import groups and users from your LDAP server instead of entering them directly as patterns. If the group structure changes in your LDAP server, it will be automatically updated to the agent to adjust the monitoring needs. You can add LDAP users and groups by clicking on the *Add Instance()* link under *LDAP Users and Groups* section of the Rules screen.

When adding patterns for pattern type user or osuser, you can also populate these patterns by selecting users that have been detected over time by the Configuration Change Console agent. Click on the *Select from Detected Users* link to select previously discovered users instead of entering the patterns manually.

The following guidelines should be followed when creating rules for this rule set:

1. User names are case-sensitive. Users root and ROOT are two different user names.
2. The relationship between connecttype and name rule is "and", which means, if both specified, only events that satisfy both will be reported.

3. You can use a wildcard '*' to match zero or more characters in the pattern. Pattern "ro*" matches user name root and ronald.
4. If two or more patterns match the same file/path, the longer pattern has higher priority. For example both include r* and exclude *ot match the user name root, but exclude *ot is longer, so the user name root will be excluded.

C

Component Internal Rule Set Capability Details

Descriptions of the various Component Internal rule sets are already included earlier in the document, but this appendix is meant to capture the details that might not be covered earlier.

As discussed earlier in this book, there are two types of monitoring capabilities, or rule sets, in the Configuration Change Console. The first is the monitoring done at the operating system level, such as Files (changes, reads), Processes (starts and stops), and operating system Users (login and logouts). The second type is referred to as Component Internal Rule Sets. These are monitoring capabilities for entities inside of an application or piece of software.

The following lists the component internal rule set capabilities that this release of Configuration Change Console supports with a description of capabilities.

- Oracle 8*i*/9*i*/10*g* (Audit) - Monitor any database entity or user for change or select activity. Uses the Oracle audit capability of the database for near real-time monitoring.
- Oracle 8*i* (Snapshot) - Monitor schema changes or change to the output of a SQL query that runs periodically.
- Oracle 9*i*/10*g* (Snapshot) - Monitor schema changes or change to the output of a SQL query that runs periodically.
- Microsoft SQL Server 2000 (Audit) - Monitor any database entity or user for change or select activity. Uses the SQL Server auditing capability of the database for near real-time monitoring.
- Microsoft SQL Server 2000 (SQL Trace) - Monitor any pattern in SQL statements for activity. Uses the SQL Server auditing capability of the database for near real-time monitoring.
- Microsoft SQL Server (Snapshot) - Monitor schema changes or change to the output of a SQL query that runs periodically.
- Microsoft Active Directory (Trace) - Monitor changes to User, Group, or Computer entities in near real-time using the auditing capabilities of Active Directory.
- Active Directory/LDAP (Snapshot) - Monitor changes to User, Group, or Computer entities using a polling/snapshot capability. Uses standard LDAP interfaces for access.
- Microsoft Windows Registry - Monitor key or value changes using Microsoft APIs for near real-time monitoring.

- SNMP Traps - Receive SNMP traps from any system that can send traps like network hardware or another application.

Each component internal monitoring rule set is discussed in detail in the rest of this appendix. For each rule set, the Configuration parameters and rule definition options are discussed in detail.

Oracle 8i/9i/10g (Audit)

This monitoring capability uses the Oracle audit subsystem to gather audit trails of changes. The Configuration Change Console filters the audit log and uses its rule set and rule configurations for a component to determine what is important for Configuration Change Console.

The agent will not set the audit subsystem settings. These need to be done manually as part of installing the agent to monitor Oracle in audit mode. See the installation documentation for instructions on how to set up an Oracle database for audit monitoring. The rest of this chapter assumes that the database you are monitoring is already configured for auditing and that you have already set up the audit system to audit the entities you will be monitoring from within Configuration Change Console.

Rule Set Configuration

When you add this rule set to a component, you must set the options under the *Configure* link shown for the rule set. The following are the options to be configured:

Table C–1 Options for Rule Sets

Option	Description
Is Enabled	Check this box to enable this rule set.
Connection URL	The connection URL to the database of the format *jdbc:oracle:thin:@localhost:1521:oraclesid* Under normal operations, the only things to change here are the hostname (shown as localhost above) and the sid of the database (shown as *oraclesid* above).
User Name	A database user that has read access to the audit trail data in the Oracle database. This user should not have write access to any production data.
Password	The password for the audit read-only user.
Ignore Events Prior to Agent Update	Check this if you want CCC monitoring to start only when the component was created. If the audit log in the database has old records and you do not check this box, then those historic events will also be monitored.
User Login Filter	Selects whether the agent should capture login/logout events for users defined in the rules in addition to other types of events.
Report Success Event Only	Select whether you want to capture only events that were successful or also failed attempts as well, as in cases when someone tries to delete a record but the delete failed.

Rules

You can create up to 50 include or exclude rules for this rule set in a single component. The following pattern types are available for creating rules.

Table C–2 Pattern Types for Rules

Pattern Type	Description
User	The database user name that is making a change. A single wildcard can be used anywhere in the pattern. For instance you can include any users starting with the letter A by using pattern "A*".
Host	The host from which a database connection is connecting. You can use this to monitor activity from a specific host versus another host. A single wildcard can be used anywhere in the pattern.
Terminal	The terminal on a host from which a database connection is connecting. You can use this to monitor activity from a specific terminal on a host versus another terminal. A single wildcard can be used anywhere in the pattern.
Osuser	The operating system user that is connecting to the database. A change in a database will be done by a database user, but there was an operating system user that first connected, for example using SQL*PLUS to make the change. A single wildcard can be used anywhere in the pattern.
Objname	The name of the object to monitor. The object name may or may not include the schema owner depending on your needs. If you do not include the owner, then the same object name in all schemas will trigger an event if they change. A single wildcard can be used anywhere in the entity name (not the schema owner name) part of the pattern.
Event	The event type to capture, for instance: ■ Select ■ Create ■ Delete ■ Update

If you have integrated your Configuration Change Console server with an LDAP server, you can also import groups and users from your LDAP server instead of entering them directly as patterns. If the group structure changes in your LDAP server, it will be automatically updated to the agent to adjust the monitoring needs. You can add LDAP users and groups by clicking on the *Add Instance()* link under the *LDAP Users and Groups* section of the Rules screen.

When adding patterns for a pattern type user or OS user, you can also populate these patterns by selecting users that have been detected over time by the Configuration Change Console agent. Click on the *Select from Detected Users* link to select previously discovered users instead of entering the patterns manually.

The following guidelines should be followed when creating rules for this rule set:

1. If no rules are defined, no events will be captured.
2. If rules are defined for only some pattern types, only those patterns types will be evaluated.
3. For pattern type *Objname*, both *Objname* and *Schema.Objname* formats are supported. For example: The pattern include *foo* will capture all events on *foo* in any schema. Include *system.foo** will only capture them in the system schema.
4. If using *Schema.Objname* pattern, wildcards are not supported in the schema name. Use only one wildcard (*) in *Objname* if needed.

5. Patterns without a wildcard (*) take precedence over patterns with a wildcard of the same pattern type. For example: With two rules for "User" pattern type: Include system, Exclude syst*, and actions by "system" user will be captured.
6. Include patterns take precedence over excludes when the pattern lengths are the same for a given pattern type. For example: With two rules for "User" pattern type: Include *, exclude *, all events will be captured.

Oracle 8i (Snapshot) and Oracle 9i/10g (Snapshot)

This monitoring capability uses the SQL queries that runs periodically, each time the output of the queries are compared to look for changes. The difference between these snapshot rule sets and the Audit rule set is that the events are not detected in real time and there are certain pieces of information lost such as the user that made the change, the exact time a change happened. There are some benefits to these rules sets, however, in that you can get the before and after values of an entity or query monitored.

The user that is configured to do schema monitoring using include/exclude rules (as opposed to SQL query rules) must have read access to the following tables to perform the monitoring:

For Oracle 8*i* (Snapshot)

- sys.dba_tables
- sys.dba_tab_columns
- sys.dba_constraints
- sys.dba_views
- sys.dba_objects

For Oracle 9*i*/10*g* (Snapshot)

- sys.dba_tables
- sys.dba_tab_columns
- sys.dba_constraints
- sys.dba_views
- sys.dba_objects
- sys.dba_procedures

Rule Set Configuration

When you add this rule set to a component, you must set the options under the *Configure* link shown for the rule set. The following are the options to be configured:

Table C–3 Options for Rule Sets

Option	Description
Is Enabled	Check this box to enable this rule set.

Table C–3 (Cont.) Options for Rule Sets

Option	Description
Connection URL	The connection URL to the database of the format: *jdbc:oracle:thin:@localhost:1521:oraclesid* Under normal operations, the only things to change here are the hostname (shown as localhost above) and the sid of the database (shown as *oraclesid* above).
User Name	A database user that has read access to the *sys.** tables that store schema definition as well as any tables you will monitor through SQL queries. Any SQL query that you create as part of a snapshot rule set needs to be executable by the user defined here. This user MUST not have write access to any critical/production data.
Password	The password for the audit read-only user.
Include Schemas/Databases	The schemas to include in this monitoring. For instance, if you were only SYS, enter *SYS* here.
Max Rows Returned	When you use this rule set to monitor a SQL query that you define and if you set a baseline interval, the output of this query will be brought back to the server, stored and be available to show on the UI. This input lets you limit how many rows to return in each SQL query execution to ensure you do not overwhelm the Configuration Change Console. It is not recommended to return more than 1000 rows. If you need more than this, consider creating multiple SQL queries to break your request up into smaller ones.
Baseline Interval	The interval that the agent should store a copy of the SQL results it captures. The agent will execute the query automatically every 5 minutes, but will only save a copy of the results based on this interval. The options are: ■ None ■ Day - once a day at 00:00 ■ Hour - once an hour at 00 minutes ■ Month - once a month on the 1st at 00:00 ■ Week - once a week on the first day at 00:00

Rules

There are two types of rules you can add to the Database snapshot rule sets.

1. SQL Query - lets you define any ad hoc SQL query that will run periodically by the agent. When the output of the SQL query changes, that will lead to one event being reported by the Configuration Change Console agent.

   You can create up to 50 SQL statements to execute for this rule set in a single component. When creating the SQL query, you must ensure that the user configured in the rule set configuration settings above can execute the query. The query should not have a semicolon ";" or other terminating string at the end.

   If you want to save a copy of the output from the SQL statement according to the *Baseline Interval* defined in the Rule Set Configuration screen, click the *Record Baseline* option. These baselines will be viewable along with the ability to perform a *Comparison in the Database Inventory* screen.

2. Include/Exclude - monitors only the schema of the selected schemas/databases (defined in the *Rule Set Configuration* screen as described above). Here you can include/exclude patterns of schema elements you want to monitor for changes.

You can create up to 50 include or exclude rules for this rule set in a single component. The following pattern types are available for creating rules.

Table C–4 Pattern Types for Rules

Pattern Type	Description
Table	The entered pattern is a table name. Events will be reported at the table level, for example, table added, deleted, or modified (one event per table changed). A single wildcard can be used anywhere in the pattern.
Table.attribute	The entered pattern is a *table.attribute* name. Events will be reported at the attribute level when an attribute changes (one event per attribute changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
Table.column	The entered pattern is a *table.column* name. Events will be reported at the column level when a column is added, deleted, or modified (one event per column changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
Table.column.attribute	The entered pattern is a *table.column.attribute name*. Events will be reported at the attribute level when an attribute changes (one event per column attribute changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
Table.constraint	The entered pattern is a *table.constraint* name. Events will be reported at the constraint level (one event per constraint changed). A single wildcard can be used anywhere in the pattern.
Table.constraint.attribute	The entered pattern is a *table.constraint.attribute* name. Events will be reported at the attribute level (one event per constraint attribute changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
View	The entered pattern is a *view* name. Events will be reported at the view level when a view is created, deleted or modified (one event per view changed). A single wildcard can be used anywhere in the pattern.
View.attribute	The entered pattern is a *view.attribute* name. Events will be reported at the attribute level (one event per attribute changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
View column	The entered pattern is a *view.column* name. Events will be reported at the column level (one event per column changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
View.column.attribute	The entered pattern is a *view.column.attribute* name. Events will be reported at the attribute level (one event per column attribute changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
Procedure	The entered pattern is a procedure name. Events will be reported at the procedure level (one event per procedure changed). A single wildcard can be used anywhere in the pattern.
Procedure.attribute	The entered pattern is a *procedure.attribute* name. Events will be reported at the attribute level (one event per attribute changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').

Table C–4 (Cont.) Pattern Types for Rules

Pattern Type	Description
All	The entered pattern applies to all pattern types. Events will be reported at the table level. One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.'). You can also specify a pattern of only "*" to monitor every schema object for schema change.

For Oracle 8*i*, Packages and objects within packages are not monitored in the current version. For Oracle 9 agent modules, procedure objects within packages can be tracked for change activity, assuming they are defined as public rather than private. Procedures with packages are monitored as if they were any other procedure. Packages themselves are not monitored, nor are any of their attributes.

If you have integrated your Configuration Change Console server with an LDAP server, you can also import groups and users from your LDAP server instead of entering them directly as patterns. If the group structure changes in your LDAP server, it will be automatically updated to the agent to adjust the monitoring needs. You can add LDAP users and groups by clicking on the *Add Instance()* link under the *LDAP Users and Groups* section of the Rules screen.

When adding patterns for pattern type user or osuser, you can also populate these patterns by selecting users that have been detected over time by the Configuration Change Console agent. Click on the *Select from Detected Users* link to select previously discovered users instead of entering the patterns manually.

The following guidelines should be followed when creating rules for this rule set:

1. If no rules are defined, no events will be captured.
2. If rules are defined for only some pattern types, only those patterns types will be evaluated.
3. Patterns without a wildcard (*) take precedence over patterns with a wildcard of the same pattern type. For example: With two rules for the *User* pattern type: Include system, Exclude syst*, actions by "system" user will be captured.
4. Include patterns take precedence over excludes when the pattern lengths are the same for a given pattern type. For example: With two rules for *User* pattern type: Include *, exclude *, all events will be captured.

Microsoft SQL Server 2000 (Audit)

This monitoring capability uses the SQL Server tracing subsystem to gather audit trails of changes. The difference between this module and the Trace version is that this module uses the objects that were accessed or changed instead of the SQL statements that were executed. The Configuration Change Console filters the log and uses its rule set and rule configurations for a component to determine what is important for Configuration Change Console.

The agent will not configure the trace subsystem settings. These need to be done manually as part of installing the agent. See the Installation Documentation for instructions on prerequisites for monitoring SQL Server 2000 in audit mode. The rest of this chapter assumes that the database you are monitoring is already configured for auditing and that you have already set up the audit system to audit the entities you will be monitoring from within Configuration Change Console.

Rule Set Configuration

When you add this rule set to a component, you must set the options under the Configure link shown for the rule set. The following are the options to be configured:

Table C–5 Options for Rule Sets

Option	Description
Is Enabled	Check this box to enable this rule set.
Connection URL	The connection URL to the database of the format: *jdbc:sqlserver://localhost:1433;databaseName=<server-name>* Under normal operations, the only things to change here are the hostname (shown as *localhost* above) and the name of the database (shown as <*server-name*> above).
User Name	A database user that has read access to the audit trail data in the database. This user should not have write access to any production data.
Password	The password for the audit read-only user.

Rules

You can create up to 50 include or exclude rules for this rule set in a single component. The following pattern types are available for creating rules.

Table C–6 Pattern Types for Rules

Pattern Type	Description
User	The database user name that is making a change. A single wildcard can be used anywhere in the pattern. For instance you can include any users starting with the letter A by using pattern "A*".
Host	The host from which a database connection is connecting. You can use this to monitor activity from a specific host versus another host. A single wildcard can be used anywhere in the pattern. The pattern for this pattern type is case insensitive.
Appname	The application name used to connect to the database to make the change or access. A single wildcard can be used anywhere in the pattern. The pattern for this pattern type is case sensitive.
Objname	The name of the object to monitor. The object name may or may not include the schema owner depending on your needs. If you do not include the owner, then the same object name in all schemas will trigger an event if they change. A single wildcard can be used anywhere in the entity name (not the schema owner name) part of the pattern.
Dbname	The name of the database in the SQL Server installation to monitor.

If you have integrated your Configuration Change Console server with an LDAP server, you can also import groups and users from your LDAP server instead of entering them directly as patterns. If the group structure changes in your LDAP server, it will be automatically updated to the agent to adjust the monitoring needs. You can add LDAP users and groups by clicking on the *Add Instance()* link under *LDAP Users and Groups* section of the Rules screen.

When adding patterns for pattern type user or osuser, you can also populate these patterns by selecting users that have been detected over time by the Configuration Change Console agent. Click on the *Select from Detected Users* link to select previously discovered users instead of entering the patterns manually.

The following guidelines should be followed when creating rules for this rule set:

1. If no rules are defined, no events will be captured.
2. If rules are defined for only some pattern types, only those patterns types will be evaluated.
3. Patterns without a wildcard (*) take precedence over patterns with a wildcard of the same pattern type. For example: With two rules for the *User* pattern type: Include system, Exclude syst*, and actions by "system" user will be captured.
4. Include patterns take precedence over excludes when the pattern lengths are the same for a given pattern type. For example: With two rules for *User* pattern type: Include *, exclude *, all events will be captured.

Microsoft SQL Server 2000 (SQL Trace)

This monitoring capability uses the SQL Server tracing subsystem to gather audit trails of changes. The difference between this module and the Audit version is that this module uses the SQL statements that were used instead of monitoring by the objects that had change or access. The Configuration Change Console filters the log and uses its rule set and rule configurations for a component to determine what is important for Configuration Change Console.

The agent will not configure the trace subsystem settings. These need to be done manually as part of installing the agent. See the Installation Documentation for instructions on prerequisites for monitoring SQL Server 2000 in audit mode. The rest of this chapter assumes that the database you are monitoring is already configured for auditing and that you have already set up the audit system to audit the entities you will be monitoring from within Configuration Change Console.

Rule Set Configuration

When you add this rule set to a component, you must set the options under the Configure link shown for the rule set. The following are the options to be configured:

Table C–7 Options for Rule Sets

Option	Description
Is Enabled	Check this box to enable this rule set.
Connection URL	The connection URL to the database of the format: *jdbc:sqlserver://localhost:1433;databaseName=<server-name>* Under normal operations, the only things to change here are the hostname (shown as *localhost* above) and the name of the server (shown as <*server-name*> above).
User Name	A database user that has read access to the audit trail data in the database. This user should not have write access to any production data.
Password	The password for the audit read-only user.

Rules

You can create up to 50 include or exclude rules for this rule set in a single component. The following pattern types are available for creating rules.

Table C–8 Pattern Types for Rules

Pattern Type	Description
User	The database user name that is making a change. A single wildcard can be used anywhere in the pattern. For instance you can include any users starting with the letter A by using pattern "A*".
Host	The host from which a database connection is connecting. You can use this to monitor activity from a specific host versus another host. A single wildcard can be used anywhere in the pattern.
Appname	The application name used to connect to the database to make the change or access. A single wildcard can be used anywhere in the pattern.
sqltext	The name of the object to monitor. The object name may or may not include the schema owner depending on your needs. If you do not include the owner, then the same object name in all schemas will trigger an event if they change. A single wildcard can be used anywhere in the entity name (not the schema owner name) part of the pattern.
Dbname	A pattern of SQL text to match. No wildcard is supported in this input, but the text is considered to be a fragment of a larger SQL statement automatically. You can search for any part of the statement, such as the table name or where clause, for example.

If you have integrated your Configuration Change Console server with an LDAP server, you can also import groups and users from your LDAP server instead of entering them directly as patterns. If the group structure changes in your LDAP server, it will be automatically updated to the agent to adjust the monitoring needs. You can add LDAP users and groups by clicking on the *Add Instance()* link under *LDAP Users and Groups* section of the Rules screen.

When adding patterns for pattern type user or osuser, you can also populate these patterns by selecting users that have been detected over time by the Configuration Change Console agent. Click on the *Select from Detected Users* link to select previously discovered users instead of entering the patterns manually.

The following guidelines should be followed when creating rules for this rule set:

1. If no rules are defined, no events will be captured.
2. If rules are defined for only some pattern types, only those patterns types will be evaluated.
3. Patterns without a wildcard (*) take precedence over patterns with a wildcard of the same pattern type. For example: With two rules for "User" pattern type: Include system, Exclude syst*, and actions by the "system" user will be captured.
4. Include patterns take precedence over excludes when the pattern lengths are the same for a given pattern type. For example: With two rules for "User" pattern type: Include *, exclude *, all events will be captured.

Microsoft SQL Server (Snapshot)

This monitoring capability uses the SQL queries that run periodically, each time the output of the queries are compared to look for changes. The difference between these snapshot rule sets and the Audit rule set is that the events are not detected in real time and there are certain pieces of information lost such as the user that made the change and the exact time a change happened. There are some benefits to these rules sets, however, in that you can get the before and after values of an entity or query monitored.

The user that is configured to do schema monitoring using include/exclude rules (as opposed to SQL query rules) must have read access to the following tables to perform the monitoring:

- *<database_name>.dbo.sysuserssystables*
- *<database_name>.dbo.sysobjectssysprocedures*
- *<database_name>.dbo.syscolumnssyscolumns*
- *<database_name>.dbo.systypessysconstraints*
- *<database_name>.dbo.sysconstraintssyschecks*

Rule Set Configuration

When you add this rule set to a component, you must set the options under the *Configure* link shown for the rule set. The following are the options to be configured:

Table C–9 Options for Rule Sets

Option	Description
Is Enabled	Check this box to enable this rule set.
Connection URL	The connection URL to the database of the format: *jdbc:sqlserver://localhost:1433;databaseName=<server-name>* Under normal operations, the only things to change here are the hostname (shown as *localhost* above) and the name of the server (shown as *<server-name>* above).
User Name	A database user that has read access to the *dbo.** tables that store schema definition as well as any tables you will monitor through SQL queries. Any SQL query that you create as part of a snapshot rule set needs to be executable by the user defined here. This user MUST not have write access to any critical/production data.
Password	The password for the audit read-only user.
Include Schemas/Databases	The schemas to include in this monitoring.
Max Rows Returned	When you use this rule set to monitor a SQL query that you define and if you set a baseline interval, the output of this query will be brought back to the server, stored and be available to show on the UI. This input lets you limit how many rows to return in each SQL query execution to ensure you do not overwhelm the Configuration Change Console. It is not recommended to return more than 1000 rows. If you need more than this, consider creating multiple SQL queries to break your request up into smaller queries.

Table C–9 (Cont.) Options for Rule Sets

Option	Description
Baseline Interval	The interval in which the agent should store a copy of the SQL results it captures. The agent will execute the query automatically every 5 minutes, but will only save a copy of the results based on this interval. The options are: ■ None ■ Day - once a day at 00:00 ■ Hour - once an hour at 00 minutes ■ Month - once a month on the 1st at 00:00 ■ Week - once a week on the first day at 00:00

Rules

There are two types of rules you can add to the Database snapshot rule sets.

1. SQL Query - lets you define any ad hoc SQL query that will run periodically by the agent. When the output of the SQL query changes, that will lead to one event being reported by the Configuration Change Console agent.

   You can create up to 50 SQL statements to execute for this rule set in a single component. When creating the SQL query, you must ensure that the user configured in the rule set configuration settings above can execute the query. The query should not have a semicolon ";" or other terminating string at the end.

   If you want to save a copy of the output from the SQL statement according to the Baseline Interval defined in the *Rule Set Configuration* screen, click the *Record Baseline* option. These baselines will be viewable along with the ability to perform a *Comparison in the Database Inventory* screen.

2. Include/Exclude - monitors only the schema of the selected schemas/databases (defined in the *Rule Set Configuration* screen as described above). Here you can include/exclude patterns of schema elements you want to watch for changes.

   You can create up to 50 include or exclude rules for this rule set in a single component The following pattern types are available for creating rules.

Table C–10 Pattern Types for Rules

Pattern Type	Description
Table	The entered pattern is a *table* name. Events will be reported at the table level, for example, table added, deleted, modified (one event per table changed). A single wildcard can be used anywhere in the pattern.
Table.column	The entered pattern is a *table.column* name. Events will be reported at the column level when a column is added, deleted, or modified (one event per column changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
Table.column.attribute	The entered pattern is a *table.column.attribute* name. Events will be reported at the attribute level when an attribute changes (one event per column attribute changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').

Table C–10 (Cont.) Pattern Types for Rules

Pattern Type	Description
Table.constraint	The entered pattern is a *table.constraint* name. Events will be reported at the constraint level (one event per constraint changed). A single wildcard can be used anywhere in the pattern.
Table.constraint.attribute	The entered pattern is a *table.constraint.attribute* name. Events will be reported at the attribute level (one event per constraint attribute changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
View	The entered pattern is a *view* name. Events will be reported at the view level when a view is created, deleted or modified (one event per view changed). A single wildcard can be used anywhere in the pattern.
View.attribute	The entered pattern is a *view.attribute* name. Events will be reported at the attribute level (one event per attribute changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
View column	The entered pattern is a *view.column* name. Events will be reported at the column level (one event per column changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
View.column.attribute	The entered pattern is a *view.column.attribute* name. Events will be reported at the attribute level (one event per column attribute changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
Procedure	The entered pattern is a *procedure* name. Events will be reported at the procedure level (one event per procedure changed). A single wildcard can be used anywhere in the pattern.
Procedure.attribute	The entered pattern is a *procedure.attribute* name. Events will be reported at the attribute level (one event per attribute changed). One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.').
All	The entered pattern applies to all pattern types. Events will be reported at the table level. One wildcard can be used anywhere in each element of the pattern (each element is separated by a period '.'). You can also specify a pattern of only '"*" to monitor every schema object for schema change.

If you have integrated your Configuration Change Console server with an LDAP server, you can also import groups and users from your LDAP server instead of entering them directly as patterns. If the group structure changes in your LDAP server, it will be automatically updated to the agent to adjust the monitoring needs. You can add LDAP users and groups by clicking on the *Add Instance()* link under the *LDAP Users and Groups* section of the Rules screen.

When adding patterns for the pattern type user or osuser, you can also populate these patterns by selecting users that have been detected over time by the Configuration Change Console agent. Click on the *Select from Detected Users* link to select previously discovered users instead of entering the patterns manually.

The following guidelines should be followed when creating rules for this rule set:

1. If no rules are defined, no events will be captured.
2. If rules are defined for only some pattern types, only those patterns types will be evaluated.

3. Patterns without a wildcard (*) take precedence over patterns with a wildcard of the same pattern type. For example: With two rules for "User" pattern type: Include system, Exclude syst*, and actions by "system" user will be captured.
4. Include patterns take precedence over excludes when the pattern lengths are the same for a given pattern type. For example: With two rules for "User" pattern type: Include *, exclude *, all events will be captured.

Microsoft Active Directory (Trace)

This monitoring capability uses the Active Directory audit APIs to gather audit trails of changes. The difference between this module and the snapshot version is that this module can capture the exact time that a change occurred and can also capture the user that made the change. This rule set must be assigned to an agent that is actually on the device on which the Microsoft Active Directory is installed. The Configuration Change Console filters the log and uses its rule set and rule configurations for a component to determine what is important for Configuration Change Console.

The Active Directory rule set can detect the following types of activities:

- Add or delete users
- User password changes
- Add or remove a user from a group
- Assign a user to manage a computer
- Add or delete a group
- Add or remove a computer into or from the domain
- Change a computer attribute

Rule Set Configuration

When you add this rule set to a component, you must set the options under the *Configure* link shown for the rule set. The following are the options to be configured:

Table C–11 Options for Rule Sets

Option	Description
Is Enabled	Check this box to enable this rule set.

There are no other configuration parameters for this rule set because it is understood that the device being monitored for this rule set is the same device on which the Active Directory is installed. All APIs required will be available locally to the agent.

Rules

You can create up to 50 include or exclude rules for this rule set in a single component. The following pattern types are available for creating rules.

Table C–12 Pattern Types for Rules

Pattern Type	Description
User	Monitor changes to users defined in the Active Directory. A single wildcard can be used anywhere in the pattern.

Table C–12 (Cont.) Pattern Types for Rules

Pattern Type	Description
Computer	Monitor changes to computers defined in the Active Directory. A single wildcard can be used anywhere in the pattern.
Group	Monitor changes to groups defined in the Active Directory. A single wildcard can be used anywhere in the pattern.

If you have integrated your Configuration Change Console server with an LDAP server, you can also import groups and users from your LDAP server instead of entering them directly as patterns. If the group structure changes in your LDAP server, it will be automatically updated to the agent to adjust the monitoring needs. You can add LDAP users and groups by clicking on the *Add Instance()* link under *LDAP Users and Groups* section of the Rules screen.

When adding patterns for a pattern type user or osuser, you can also populate these patterns by selecting users that have been detected over time by the Configuration Change Console agent. Click on the *Select from Detected Users* link to select previously discovered users instead of entering the patterns manually.

The following guidelines should be followed when creating rules for this rule set:

1. If no rules are defined, no events will be captured.
2. If rules are defined for only some pattern types, only those patterns types will be evaluated.
3. Patterns without a wildcard (*) take precedence over patterns with a wildcard of the same pattern type. For example: With two rules for the "User" pattern type: Include system, Exclude syst*, and actions by the "system" user will be captured.
4. Include patterns take precedence over excludes when the pattern lengths are the same for a given pattern type. For example: With two rules for the "User" pattern type: Include *, exclude *, all events will be captured.

Microsoft Active Directory/LDAP (Snapshot)

This monitoring capability uses the LDAP APIs to monitor either Active Directory or any other standard compliance LDAP server for changes to Users, Groups, or Computers. The difference between this module and the trace version is that this module uses a polling/snapshot approach where the content is checked periodically and compared to identify changes. Using this rule set, you cannot find the exact time of a change, or the user that made the change. This rule set can exist on an agent that is on a different device than the LDAP server.

The Active Directory rule set can detect the following types of activities:

- Add or delete users
- User password changes
- Add or remove a user from a group
- Assign a user to manage a computer
- Add or delete a group
- Add or remove a computer into or from the domain
- Change a computer attribute

Rule Set Configuration

When you add this rule set to a component, you must set the options under the *Configure* link shown for the rule set. The following are the options to be configured:

Table C–13 Options for Rule Sets

Option	Description
Is Enabled	Check this box to enable this rule set.
LDAP URL	Connection URL to the LDAP server, of the format where you replace the host name where 127.0.0.1 is located and the port where 389 is located. *ldap://127.0.0.1:389*
Username	The username to connect to in LDAP to monitor the entities. This user needs read only access to the LDAP entities you are monitoring.
Password	Password for the monitoring user.
Template Base	LDAP template base from which to start monitoring. The *template.base* value should be in entered in the format of: *DC=<node element>* For all node values. If the node name features a period (.) you will need to add an additional *DC=<node element>* marker, separated by a comma (,) for each string following a period. Note that the period itself is not included. For example, if you wish to specify domain/base node *mydomain.com* as the template.base value you would enter the following in the template.base field: *DC=mydomain,DC=com*

Rules

You can create up to 50 include or exclude rules for this rule set in a single component. The following pattern types are available for creating rules.

Table C–14 Pattern Types for Rules

Pattern Type	Description
User	Monitor changes to users defined in Active Directory. A single wildcard can be used anywhere in the pattern.
Computer	Monitor changes to computers defined in Active Directory. A single wildcard can be used anywhere in the pattern.
Group	Monitor changes to any of these using a single pattern. A single wildcard can be used anywhere in the pattern. If you want to monitor every object in LDAP, you could have a single rule to include * for all pattern types.

If you have integrated your Configuration Change Console server with an LDAP server, you can also import groups and users from your LDAP server instead of entering them directly as patterns. If the group structure changes in your LDAP server, it will be automatically updated to the agent to adjust the monitoring needs. You can add LDAP users and groups by clicking on the *Add Instance()* link under *LDAP Users and Groups* section of the Rules screen.

When adding patterns for the pattern type user or osuser, you can also populate these patterns by selecting users that have been detected over time by the Configuration

Change Console agent. Click on the *Select from Detected Users* link to select previously discovered users instead of entering the patterns manually.

The following guidelines should be followed when creating rules for this rule set:

1. If no rules are defined, no events will be captured.
2. If rules are defined for only some pattern types, only those patterns types will be evaluated.
3. Patterns without a wildcard (*) take precedence over patterns with a wildcard of the same pattern type. For example: With two rules for the "User" pattern type: Include system, Exclude syst*, and actions by "system" user will be captured.
4. Include patterns take precedence over excludes when the pattern lengths are the same for a given pattern type. For example: With two rules for the "User" pattern type: Include *, exclude *, all events will be captured.

Microsoft Windows Registry

This monitoring capability uses the Microsoft Windows Registry audit APIs to gather audit trails of changes. This rule set must assigned to an agent that is actually on the device of the registry you want to monitor.

Rule Set Configuration

When you add this rule set to a component, you must set the options under the *Configure* link shown for the rule set. The following are the options to be configured:

Table C–15 Options for Rule Sets

Option	Description
Is Enabled	Check this box to enable this rule set.

There are no other configuration parameters for this rule set because it is understood that the device being monitored for this rule set is the same device you are monitoring. All APIs required will be available locally to the agent.

Rules

You can create up to 50 include or exclude rules for this rule set in a single component. The following pattern types are available for creating rules.

Table C–16 Pattern Types for Rules

Pattern Type	Description
Key	Monitor changes based only on a key value. You can use only the first *n* characters in a key name, and all keys matching this pattern will be monitored (similar to file monitoring rules.) You can use one wildcard in the last element (separated by "/") only.
Value	Monitor changes based only on a value for a key. You can use only the first *n* characters in a value name, all keys matching this pattern will be monitored (similar to file monitoring rules.) You can use one wildcard in the last element (separated by "/") only.

Table C–16 (Cont.) Pattern Types for Rules

Pattern Type	Description
All	Check this pattern against both the key and the value. You can use only the first *n* characters in a key name, and all keys matching this pattern will be monitored (similar to file monitoring rules.) You can use one wildcard in the last element (separated by "/") only.

If you want to filter the changes against Windows Registry by the user that made them, you can add an OS User rule set to the same component and then check the box on this rule set that indicates that these users are for filtering other types of rule sets. Then in this Windows Registry rule screen, check the box that says *Filter change data by Users defined in this component*.

The following guidelines should be followed when creating rules for this rule set:

1. If no rules are defined, no events will be captured.
2. If rules are defined for only some pattern types, only those patterns types will be evaluated.
3. Patterns without a wildcard (*) take precedence over patterns with a wildcard of the same pattern type. For example: With two rules for the "User" pattern type: Include system, Exclude syst*, and actions by "system" user will be captured.
4. Include patterns take precedence over excludes when the pattern lengths are the same for a given pattern type. For example: With two rules for the "User" pattern type: Include *, exclude *, all events will be captured.

The Windows Registry monitoring policies are based on additions, modifications and deletions of Registry keys and values.

The Patterns must start with HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_CLASSES_ROOT, HKEY_USERS or HKEY_CURRENT_CONFIG.

You may specify exclusion of sub-directories under the inclusion directories. For example, to monitor HKEY_LOCAL_MACHINE\Software, but not HKEY_LOCAL_MACHINE\Software\Oracle:

Include HKEY_LOCAL_MACHINE\Software

Exclude HKEY_LOCAL_MACHINE\Software\Oracle

Any changes under HKEY_LOCAL_MACHINE\Software will be reported. No changes will be reported under HKEY_LOCAL_MACHINE\Software\Oracle or child keys.

SNMP Traps

This monitoring capability allows the agent to listen for SNMP traps which may be sent from any system. Network hardware can be configured to send SNMP traps when a configuration change occurs. Many software applications can also send traps when there are configuration or critical alerts that need to be monitored. This rule set will configure the agent to listen for traps and is used to define rules to filter which SNMP traps are meaningful for this agent to collect and send back to the server.

Rule Set Configuration

When you add this rule set to a component, you must set the options under the *Configure* link shown for the rule set. The following are the options to be configured:

Table C–17 Options for Rule Sets

Option	Description
Is Enabled	Check this box to enable this rule set.
Transport	The transport mechanism that will be used to listen for traps. The default here is UDP. This should only be changed if you know your system will use another transport mechanism such as TCP.
Port	The port on which the agent will listen to traps. This needs to match the port that your external system will be connecting to when sending a trap.
OIDs	A list of OIDS separated by commas that contain the user name that made the change. This is important when reporting who made a change. Example: 1.2.4,5,1.2.3.5

There are no other configuration parameters for this rule set because it is understood that the device being monitored for this rule set is the same device you are monitoring. All APIs needed will be available locally to the agent.

Rules

You can create up to 50 include or exclude rules for this rule set in a single component. The following pattern types are available for creating rules.

Table C–18 Pattern Types for Rules

Pattern Type	Description
Community	The community string (for example: "public") on which to match. This pattern can have one wildcard anywhere in the string.
Enterprise	The enterprise OID string (for example: "1.3.4.*") on which to match. This pattern can have one wildcard anywhere in the string.
AgentAddress	IP Addresses to match from where a change occurred. This pattern can have one wildcard anywhere in the string.
SourceAddress	IP Addresses to match from where a change occurred. This pattern can have one wildcard anywhere in the string. Source and agent address normally would be the same unless some proxy system exists between the person making a change and the system triggering the trap.
GenericType	A number matching the *GenericType* from a trap.
SpecificCode	A number matching the *GenericType* from a trap.
Binding	Plain text search on a value of an OID. For instance, to capture only events where OID 1.3.6.1.2.1.2.2.1 contains the text *IP Packet*, then this pattern would be: *1.3.6.1.2.1.2.2.1=IP Packet*

The following guidelines should be followed when creating rules for this rule set:

1. If no rules are defined, no events will be captured.
2. If rules are defined for only some pattern types, only those patterns types will be evaluated.

3. Patterns without a wildcard (*) take precedence over patterns with a wildcard of the same pattern type. For example: With two rules for the "User" pattern type: Include system, Exclude syst*, and actions by the "system" user will be captured.
4. Include patterns take precedence over excludes when the pattern lengths are the same for a given pattern type. For example: With two rules for the "User" pattern type: Include *, exclude *, all events will be captured.

D

Accessing Data Through Third Party Tools

There are database views available to access the most commonly used information in third part data analysis and reporting tools. The following section offers a description of each of the views.

> **Note:** All date and time fields are in GMT time zone as all dates in the Configuration Change Console repository are stored in GMT.

Description of Views

The following are the views you can use to access information in third party data analysis.

- **View: custview_allfileevents**

  Returns all file events for all devices.

  Fields:

  EVENT_ID: The unique identifier for the event record

  DEVICE_NAME: The name of the device that the event happened on

  DEVICE_ASSETTAG: The asset tag of the device that the event happened on

  FILE_NAME: The name of the file the event affected. If the event is a rename, this field stores the new file name after the rename event.

  EVENT_TIME: The time of the event.

  FILE_SIZE: The size of the file after the event

  EVENT: The event that occurred: Create, Deleted, Modified, Renamed

  RENAMED_FROM_FILE_NAME: The name of the original file for renamed event type

  EVENT_USER: The user that performed the event

  Example Usage:

  ```
  select * from custview_allfileevents where EVENT_TIME between
  ? and ?
  ```

- **View: custview_allprocessevents**

  Returns all process events for all devices

  Fields:

  ID: The unique identifier for the event

DEVICE_NAME: The name of the device that the event happened on

DEVICE_ASSETTAG: The asset tag of the device that the event happened on

PROCESS_NAME: The name of the process the event affected.

PROCESS_ID: The OS-supplied ID of the process

EVENT_TIME_GMT: The time of the event.

EVENT: The event that occurred: Started, Stopped, Short Lived

PROCESS_USER: The user who owns the process

- **View: custview_allincomingtickets**

  Returns all incoming tickets that have come from the change management server. If an incoming ticket is associated with many devices, there will be one result for each association.

  Fields:

  TICKET_ID: The unique identifier for the ticket from the change management server

  STATE: Current state of the ticket as used by CCC: Open or Closed

  SUMMARY: The ticket summary content from the ticket management application

  SUPERVISOR: The assigned supervisor from the change management server

  DEVICE_NAME: The name of the device the ticket is associated with. If a single ticket is associated with many devices, there will be one result from this view for each device.

  DEVICE_ASSETTAG: The assigned asset tag for the device the ticket is associated with

  PLANNED_START: The set planned start date and time from the change management server.

  PLANNED_END: The set planned end date and time from the change management server.

  CREATED_TIME_GMT: Time the ticket was created.

  UPDATED_TIME_GMT: Time the ticket was last updated

  TICKET_CATEGORY: The name of the CTI for the ticket

  Example Usage:

```
Select * from custview_allincomingtickets where state = 'OPEN'
Select * from custview_allincomingtickets where state = 'CLOSED'
Select * from custview_allincomingtickets where planned_start between ? and ?
and planned_end between ? and ?
Select * from custview_allincomingtickets where ticket_category like
'%:Software:%'
```

- **View: custview_appfileeventslastday**

  Returns count of events from files associated with applications by application in the last 24 hours.

  Fields:

  APPLICATION: The name of the application instance and the type of application

  EVENT_COUNT: The count of file changes for that app in the last day

- **View: custview_appfileeventslasthour**

  Returns count of events from files associated with applications by application in the last 1 hour.

  Fields:

  APPLICATION: The name of the application instance and the type of application

  EVENT_COUNT: The count of file changes for that app in the last hour

- **View: custview_appinteventslastday**

  Returns count of events from internal elements associated with applications by application in the last 24 hours.

  Fields:

  APPLICATION: The name of the application instance and the type of application

  EVENT_COUNT: The count of internal changes for that app in the last day

- **View: custview_appinteventslasthour**

  Returns count of events from internal elements associated with applications by application in the last 1 hour.

  Fields:

  APPLICATION: The name of the application instance and the type of application

  EVENT_COUNT: The count of internal changes for that app in the last hour

- **View: custview_appproceventslastday**

  Returns count of events from processes associated with applications by application in the last 24 hours.

  Fields:

  APPLICATION: The name of the application instance and the type of application

  EVENT_COUNT: The count of process changes for that app in the last day

- **View: custview_appproceventslasthour**

  Returns count of events from processes associated with applications by application in the last 1 hour.

  Fields:

  APPLICATION: The name of the application instance and the type of application

  EVENT_COUNT: The count of file changes for that app in the last hour

- **View: custview_autheventslastday**

  Returns history of all outbound tickets to a change management server in response to authorized events in the last 24 hours.

  Fields:

  ID: The unique identifier of the outbound ticket.

  DEVICE_NAME: The name of the device that the event happened on

  ENTITY_TYPE: The type of entity that had the event: File, Process, Internal

  ENTITY_NAME: The name of the entity: File name, Process Name, or Internal key name

EVENT_TYPE: The event, events for files are Created, Deleted, Modified, Renamed. For Processes types are Started and Stopped. For internal changes, the available type is Modified.

EVENT_TIME: The time the event occurred

PR_ID: The unique identifier for the process event

FR_ID: The unique identifier for the file event

APPR_ID: The unique identifier for the application internal event

TICKET_ID: The ID of the ticket from the change management server that gave authorization for the change

AFFECTED_TICKET_CATEGORY: The CTI that is associated with the ticket that gave authorization for the change

- **View: custview_autheventslasthour**

  Returns history of all outbound tickets to a change management server in response to authorized events in the last hour.

  Fields:

  ID: The unique identifier of the outbound ticket.

  DEVICE_NAME: The name of the device that the event happened on

  ENTITY_TYPE: The type of entity that had the event: File, Process, Internal

  ENTITY_NAME: The name of the entity: File name, Process Name, or Internal key name

  EVENT_TYPE: The event, events for files are Created, Deleted, Modified, Renamed. For Processes types are Started and Stopped. For internal changes, the available type is Modified.

  EVENT_TIME: The time the event occurred

  PR_ID: The unique identifier for the process event

  FR_ID: The unique identifier for the file event

  APPR_ID: The unique identifier for the application internal event

  TICKET_ID: The ID of the ticket from the change management server that gave authorization for the change

  AFFECTED_TICKET_CATEGORY: The CTI that is associated with the ticket that gave authorization for the change

- **View: custview_fileeventsperhour**

  Returns count of file events per hour per device.

  Fields:

  DEVICE_NAME: The name of the device for which events are aggregated

  DEVICE_ASSETTAG: The asset tag of the device

  EVENT_COUNT: Number of file events during the hour

  HOUR_GMT: The hour for this count

- **View: custview_notifcountlastday**

  Returns count of notifications for each person by priority and status in the last 24 hours.

Fields:

NOTIFICATION_COUNT: Count of notifications

RECIPIENT: The login name of the person the notifications were for

PRIORITY: The priority of the notifications ranging from 1 to 5 with 1 being highest

STATUS: Current status of the notification: Pending, Closed, Pending But Escalation Failed

ACTION_TAKEN:

- **View: custview_notifcountlasthour**

  Returns count of notifications for each person by priority and status in the last hour

  Fields:

  NOTIFICATION_COUNT: Count of notifications

  RECIPIENT: The login name of the person the notifications were for

  PRIORITY: The priority of the notifications ranging from 1 to 5 with 1 being highest

  STATUS: Current status of the notification: Pending, Closed, Pending But Escalation Failed

  ACTION_TAKEN:

- **View: custview_processeventsperhour**

  Returns count of process events per hour per device.

  Fields:

  DEVICE_NAME: The name of the device for which events are aggregated

  DEVICE_ASSETTAG: The asset tag of the device

  EVENT_COUNT: Number of process events during the hour

  HOUR_GMT: The hour for this count

- **View: custview_unautheventslastday**

  Returns history of all outbound tickets to a change management server in response to unauthorized events in the last 24 hours.

  Fields:

  ID: Unique ID for the outbound ticket

  Device_Name:Name of the device event occurred on

  Entity_Type: Type of event (file, process, etc)

  Entity_Name: Name of the entity that changed (file name, etc)

  Event_Type: Type of event (started, stopped, created, deleted, etc)

  Event_Time: Time the event occurred in GMT

  PR_ID: ID of the process event (fk to processrunning table)

  FR_ID: ID of the file event (fk to the filerunning table)

  APPR_ID: ID of the app internal event (fk to the apprunning table)

Affected_Ticket_Category: Change Management categorization the event is related to.

- **View: custview_unautheventslasthour**

  Returns history of all outbound tickets to a change management server in response to unauthorized events in the last 1 hour.

  Fields:

  ID: Unique ID for the outbound ticket

  Device_Name:Name of the device event occurred on

  Entity_Type: Type of event (file, process, etc)

  Entity_Name: Name of the entity that changed (file name, etc)

  Event_Type: Type of event (started, stopped, created, deleted, etc)

  Event_Time: Time the event occurred in GMT

  PR_ID: ID of the process event (fk to processrunning table)

  FR_ID: ID of the file event (fk to the filerunning table)

  APPR_ID: ID of the app internal event (fk to the apprunning table)

  Affected_Ticket_Category: Change Management categorization the event is related to.

- **View: custview_usereventsperhour**

  Returns count of user events per hour per device.

  Fields:

  Device_Name: name of device changes occurred on

  Device_AssetTag: asset tag of the device

  Event_Count: count of changes on the device

  Hour_GMT: The hour the events occurred in GMT

- **View: custview_userproccountlastday**

  Returns count of processes run by each user in the last 24 hours.

  Fields:

  Device_Name: name of device changes occurred on

  Device_AssetTag: asset tag of the device

  Event_Count: count of changes on the device

  Username: user that made the changes

- **View: custview_userproccountlasthour**

  Returns count of processes run by each user in the last 1 hour.

  Fields:

  Device_Name: name of device changes occurred on

  Device_AssetTag: asset tag of the device

  Event_Count: count of changes on the device

  Username: user that made the changes

- **View: custview_all_app_changes**

  Returns count of all events by component ID and hour.

- **View: custview_app_chng_viz**

- **View: custview_procappeventlog**

  Returns a log of all process events and component associations

  Fields:

  EventId: The event ID assigned by the server

  Time_GMT: Time of the event in GMT

  Device: Name of the device the event occurred on

  Type:Fixed as "Process"

  Event: Type of event, either process started or stopped

  EventUser: The OS user that caused the event

  Application: The name of the component this event is tied to

- **View: custview_userlogoffeventlog**

  Returns a log of all user logoff events and component associations

  Fields:

  EventId: The event ID assigned by the server

  Time_GMT: Time of the event in GMT

  Device: Name of the device the event occurred on

  Type: Fixed as "Access"

  Name: Fixed as '-'

  Event: Fixed as 'Logoff'

  EventUser: The OS user that caused the event

  Application: The name of the component this event is tied to

  Example Usage:

```
SELECT * FROM custview_userlogoffeventlog
    WHERE
    DEVICE in ('deviceabc','devicecde')
    AND
    TIME_GMT BETWEEN
    TO_DATE('12/10/04 00:00:00','mm/dd/yy HH24:mi:ss')
    AND
   TO_DATE('12/10/04 04:00:00','mm/dd/yy HH24:mi:ss')
    AND
    EVENTUSER = 'username';
```

- **View: custview_userlogoneventlog**

  Returns a log of all user logon events and component associations

  Fields:

  EventId:The event ID assigned by the server

  Time_GMT: Time of the event in GMT

Device: Name of the device the event occurred on

Type: Fixed as "Access"

Name: Fixed as '-'

Event: Fixed as 'Logon'

EventUser: The OS user that caused the event

Application: The name of the component this event is tied to

Example Usage:

```
SELECT * FROM custview_userlogoneventlog
    WHERE
    DEVICE in ('deviceabc','devicecde')
    AND
    TIME_GMT BETWEEN
    TO_DATE('12/10/04 00:00:00','mm/dd/yy HH24:mi:ss')
    AND
   TO_DATE('12/10/04 04:00:00','mm/dd/yy HH24:mi:ss')
    AND
    EVENTUSER = 'username';
```

- **View: custview_policy_user_changes**

  Count of events by OS user or component internal user grouped by the policy that is affected and by the hour the event occurred.

  Fields:

  Cnt: Count of events

  Policyid: The ID of the Policy (fk to custview_policy_name)

  Time_hours: Date and Time by hour in GMT

  Usertype: Whether the user is an OS user or Component Internal User

- **View: custview_policy_event**

  Get count of events by event priority 1 or 2, authorized and unauthorized grouped by the component, policy and control.

  Fields:

  Policy_id: The ID for the framework policy (fk to custview_policy_name)

  appid: The ID for the component (fk to appconfig)

  time_hours: Date and Time by hour in GMT

  controlid: The ID for the framework control (fk to controlconfig)

  controlname: the name of the framework control

  count: total count of events

  p1_cnt: total count of events that are Priority 1

  p2_cnt: total count of events that are Priority 2

  authcnt: total count of events that are Authorized

  unauthcnt: total count of events that are Unauthorized

- **View: custview_policy_pr_changes**

  Count of process changes by frameowork policy by hour.

Fields:

Cnt: count of events

Policyid: The ID for the framework policy (fk to custview_policy_name)

Time_hours: Date and Time by hour in GMT

- **View: custview_policy_name**

  Returns all framework ID, Policy Ids and the framework and policy name

  Fields:

  Framework_id: The ID for the framework

  Policy_id: The ID for the policy

  Full_name: the full name of the framework and policy combination.

- **View: custview_appgroup_user_changes**

  Count of User events by hour and by application.

  Fields:

  Cnt: Count of events

  Groupid: The ID of the application (fk)

  Time_hours: Date and time by hour in GMT

  Usertype: type of user, OS User or Component Internal User

- **View: custview_appgroup_pr_changes**

  Count of Process events by hour and by application.

  Fields:

  Cnt: Count of events

  Groupid: The ID of the application (fk)

  Time_hours: Date and time by hour in GMT

- **View: custview_appgroup_file_changes**

  Count of File events by hour and by application.

  Fields:

  Cnt: Count of events

  Groupid: The ID of the application (fk)

  Time_hours: Date and time by hour in GMT

- **View: custview_policy_file_changes**

  Count of file changes by framework policy by hour

  Fields:

  Cnt: count of events

  Policyid: ID of the framework policy (fk to custview_policy_name)

  Time_hours: Date and time by hour in GMT

- **View: custview_policy_app_changes**

  Count of component internal changes by framework policy by hour

Fields:

Cnt: count of events

Policyid: ID of the framework policy (fk to custview_policy_name)

Time_hours: Date and time by hour in GMT

- **View: custview_appgroup_app_changes**

  Count of Component Internal events by hour and by application.

  Fields:

  Cnt: Count of events

  Groupid: The ID of the application (fk)

  Time_hours: Date and time by hour in GMT

- **View: custview_person_productrole**

  Returns all product roles for each person configured

  Fields:

  ProductRole: The product role

  LoginName: The person's login name

  FirstName: The person's first name

  LastName: the person's last name

- **View: custview_dev_group_assignment**

  Fields:

  Group_id: The ID of the device group (fk to devicegroupconfig)

  Group_name: The name of the device group

  Device_id: The ID of the device (fk to deviceconfig)

  Device_name: The name of the device

- **View: custview_fileappeventlog**

  Returns a log of all file events and component associations.

  Fields:

  EventId: The event ID assigned by the server

  Time_GMT: Time of the event in GMT

  Device: Name of the device the event occurred on

  Type:Fixed as "Access"

  Name: Fixed as '-'

  Event: Fixed as 'Logon'

  EventUser:The OS user that caused the event

  Application: The name of the component this event is tied to

  Example Usage:

```
SELECT * FROM custview_fileappeventlog
WHERE
DEVICE in ('deviceabc','devicecde')
```

```
AND
TIME_GMT BETWEEN
TO_DATE('12/10/04 00:00:00','mm/dd/yy HH24:mi:ss')
AND
TO_DATE('12/10/04 04:00:00','mm/dd/yy HH24:mi:ss')
AND
EVENTUSER = 'username'
```

- **View: custview_app_comp_assignment**

  Returns the assignment of component instances to applications so you can recreate the model for an application. Component instances that are not assigned to an application at all will belong to an application called "Components not assigned to an application".

  Fields:

  App_id: The ID of the application (fk to appgroupconfig)

  App_name: The name of the application

  Component_id: The ID of the component instance (fk to appconfig)

  Component_name: The name of the component

- **View: custview_all_policy**

  Returns all Framework policies and Ids configured in the product. This includes predefined and custom policies.

  Fields:

  Policyid: The ID of the policy (fk to controlsetconfig)

  Policyname: The name of the policy

- **View: custview_all_applicationgroup**

  Returns all applications and their Ids configured in the product.

  Fields:

  Groupid: The ID of the application (fk to appgroupconfig)

  Groupname: The name of the application

- **View: custview_appgrp_change_summary**

  Reports counts of each type of event by the application they are associated with by the hour the events happened.

  Fields:

  Group_id: The ID of the application (fk to appgroupconfig)

  Group_name: The name of the application

  Cnt_file: Count of file events

  Cnt_process: Count of process events

  Cnt_app: Count of component internal events

  Cnt_appu: Count of component internal user events

  Cnt_osu: Count of OS user events

  T_hour: Data and time by hours in GMT

- **View: custview_all_user_process**

Count of all user process events by hour.

Fields:

Dev_id: The ID of the device where the event occurred (fk to deviceconfig)

Time_hours: Date and time by hours in GMT

User_name: The user name for these events

Count: Count of events

- **View: custview_all_unauth_changes**

  Count of all unauthorized changes by component instance by hour.

  Fields:

  Cnt: Count of changes

  App_id: The ID of the component instance where events occurred (fk to appconfig)

  T_hour: Date and time by hours in GMT

E

Third Party Licenses

This appendix contains licensing information about certain third party products included with Configuration Change Console 10*g* Release. Unless otherwise specifically noted, all licenses herein are provided for notice purposes only.

The sections in this chapter describe the third party licenses:

- Apache Software Foundation Licenses
  - Apache Software License, Version 1.1
    - Apache Avalon 4.1.3
    - Apache Crimson 1.1.1
    - Xerces 2.6.2
    - Ant 1.5.1
  - Apache Software License, Version 2.0
    - Log4J 1.2.8
    - Apache Axis 1.2RC2
    - LogKit
    - Codehaus Plexus
    - Sprint 2.0.2
    - Pluto 1.1.0
    - Apache Commons 1.0
    - Apache Tomcat Commons
    - CGILIB 2.0.1
    - Jaxen
    - Xalan
    - ODMG Library
    - Catalina
    - SNMP4J
    - Struts 1.2.9
    - Castor 0.95
- Sun Binary Code License Agreement
  - Sun JSDK 1.5

  - Javamail
  - BSH-Core 1.3.0
- DOM4J
- ANTLR 3
- Java Service Wrapper 3.2.3
- JNI Registry 3.1.3
- WSDL4J
- Concurrent Library
- AOP Alliance Library
- Xdoclet 1.2.3
- JDOM 1.0B9
- MSVP60.DLL
- PDH.DLL 5.0.2195.2668
- Mibble 2.8
- Robohelp 5.0
- Microsoft SQL Server Driver 2005, 1.2
- Install Anywhere
- Additional Licensing Information

Apache Software Foundation Licenses

The following sections provided licensing information for the following versions of Apache software licenses:

- Version 1.1
- Version 2.0

Apache Software License, Version 1.1

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see http://www.apache.org.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

This product includes the following software from the Apache Software Foundation (http://www.apache.org) licensed to Oracle under Apache License 1.1 and that include the following copyright notices:

Apache Avalon 4.1.3

Copyright © 2008 The Apache Software Foundation, Licensed under the Apache License, Version 2.0.

Apache Crimson 1.1.1

Copyright © 2008 The Apache Software Foundation, Licensed under the Apache License, Version 2.0.

Xerces 2.6.2

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Ant 1.5.1

Copyright (c) 2000-2003 The Apache Software Foundation. All rights reserved.

Apache Software License, Version 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

This product includes the following software from the Apache Software Foundation (http://www.apache.org) licensed to Oracle under Apache License 2.0 and that include the following copyright notices:

Log4J 1.2.8

Copyright © 2008 The Apache Software Foundation, Licensed under the Apache License, Version 2.0.

Apache Axis, Version 1.2RC2

Copyright © 2008 The Apache Software Foundation, Licensed under the Apache License, Version 2.0.

LogKit

Copyright 2004 Apache Software Foundation.

Codehaus Plexus

© 2001-2007 Codehaus

Spring 2.0.2

© 2002-2007 The Spring Framework (http://springframework.org).

All Spring projects are licensed under the terms of the Apache License, version 2.0

Pluto 1.1.0

© 2003-2008 Apache Software Foundation

Apache Commons 1.0

All source and documentation of the Commons project is copyrighted by the Apache Software Foundation, and made available under the Apache License, version 2.0

Apache Tomcat Commons

All source and documentation of the Commons project is copyrighted by the Apache Software Foundation, and made available under the Apache License, version 2.0

CGILIB 2.0.1

Copyright © 2002-2003 cglib. All Rights Reserved.

Jaxen

Copyright © 2001-2007, Codehaus.

We use an Apache-style open source license which is one of the least restrictive licenses around, you can use jaxen to create new products without them having to be open source.

Xalan

Copyright © 2005 The Apache Software Foundation. All Rights Reserved.

ODMG Library

Copyright © 2002-2006 The Apache Software Foundation. All Rights Reserved. Published under the Apache License 2.0

Catalina

SNMP4J

Struts 1.2.9

Castor 0.95

Sun Binary Code License Agreement

Sun JSDK 1.5

Sun Microsystems, Inc. Binary Code License Agreement

for the JAVA 2 PLATFORM STANDARD EDITION DEVELOPMENT KIT 5.0

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1. DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "General Purpose Desktop Computers and Servers" means computers, including desktop, laptop and tablet computers, or servers, used for general computing functions under end user control (such as but not specifically limited to email, general purpose Internet browsing, and office suite productivity tools). The use of Software in systems and solutions that provide dedicated functionality (other than as mentioned above) or designed for use in embedded or function-specific software applications, for example but not limited to: Software embedded in or bundled with industrial control systems, wireless mobile telephones, wireless handheld devices, kiosks, TV/STB, Blu -ray Disc devices, telematics and network control switching equipment, printers and storage management systems, and other related systems are excluded from this definition and not licensed under this Agreement. "Programs" means Java technology applets and applications intended to run on the Java Platform Standard Edition (Java SE) platform on Java-enabled General Purpose Desktop Computers and Servers.
2. LICENSE TO USE. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable,

limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.

3. RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

5. DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

6. LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

7. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

8. EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

9. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.

10. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

11. GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

12. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

13. INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement . These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

1. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software "README" file incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

2. License to Distribute Software. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README

file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

3. License to Distribute Redistributables. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the Software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agr eement that protects Sun's interests consistent with the terms contained in the Agreement, (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

4. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

5. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM 2 Platform Standard Edition Development Kit 5.0; (iv) The Software must be reproduced in its entirety and wit hout any modification whatsoever (including, without limitation, the Binary Code License and Supplemental License Terms

accompanying the Software and proprietary rights notices contained in the Software); (v) The Media label shall include the following information: Copyright 2006, Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Sun, Sun Microsystems, the Sun logo, Solaris, Java, the Java Coffee Cup logo, J2SE, and all trademarks and logos based on Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. This information must be placed on the Media label in such a manner as to only apply to the Sun Software; (vi) You must clearly identify the Software as Sun's product on the Media holder or Media label, and you may not state or imply that Sun is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the Soft ware; (viii) You shall indemnify Sun for all damages arising from your failure to comply with the requirements of this Agreement. In addition, you shall defend, at your expense, any and all claims brought against Sun by third parties, and shall pay all damages awarded by a court of competent jurisdiction, or such settlement amount negotiated by you, arising out of or in connection with your use, reproduction or distribution of the Software and/or the Publication. Your obligation to provide indemnification under this section shall arise provided that Sun: (a) provides you prompt notice of the claim; (b) gives you sole control of the defense and settlement of the claim; (c) provides you, at your expense, with all available information, assistance and authority to defend; and (d) has not compromised or settled such claim without your prior written consent; and (ix) You shall provide Sun with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Sun Microsystems, Inc., 4150 Network Circle, M/S USCA12-110, Santa Clara, California 95054, U.S.A , Attention: Contracts Administration.

6. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

7. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

8. Termination for Infringement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

9. Installation and Auto-Update. The Software's installation and auto-update processes transmit a limited amount of data to Sun (or its service provider) about those specific processes to help Sun understand and optimize them. Sun does not associate the data with personally identifiable information. You can find more information about the data Sun collects at http://java.com/data/.

For inquiries please contact: Sun Microsystems, Inc., 4150

Network Circle, Santa Clara, California 95054, U.S.A.

(LFI#143333/Form ID#011801)

Javamail

Sun Microsystems, Inc. ("Sun") ENTITLEMENT for SOFTWARE

Licensee/Company: Entity receiving Software.

Effective Date: Date of delivery of the Software to You.

Software: JavaMail 1.4.

License Term: Perpetual (subject to termination under the SLA).

Licensed Unit: Software Copy.

Licensed unit Count: Unlimited.

Permitted Uses:

1. Definitions.
   a. "Entitlement" means the collective set of applicable documents authorized by Sun evidencing your obligation to pay associated fees (if any) for the license, associated Services, and the authorized scope of use of Software under this Agreement.
   b. "Licensed Unit" means the unit of measure by which your use of Software and/or Service is licensed, as described in your Entitlement.
   c. "Permitted Use" means the licensed Software use(s) authorized in this Agreement as specified in your Entitlement. The Permitted Use for any bundled Sun software not specified in your Entitlement will be evaluation use as provided in Section 3.
   d. "Service" means the service(s) that Sun or its delegate will provide, if any, as selected in your Entitlement and as further described in the applicable service listings at www.sun.com/service/servicelist.
   e. "Software" means the Sun software described in your Entitlement. Also, certain software may be included for evaluation use under Section 3.
   f. "You" and "Your" means the individual or legal entity specified in the Entitlement, or for evaluation purposes, the entity performing the evaluation.
2. License Grant and Entitlement.

   Subject to the terms of your Entitlement, Sun grants you a nonexclusive, nontransferable limited license to use Software for its Permitted Use for the license term. Your Entitlement will specify (a) Software licensed, (b) the Permitted Use, (c) the license term, and (d) the Licensed Units.

   Additionally, if your Entitlement includes Services, then it will also specify the (e) Service and (f) service term.

   If your rights to Software or Services are limited in duration and the date such rights begin is other than the purchase date, your Entitlement will provide that beginning date(s).

   The Entitlement may be delivered to you in various ways depending on the manner in which you obtain Software and Services, for example, the Entitlement may be provided in your receipt, invoice or your contract with Sun or authorized Sun reseller. It may also be in electronic format if you download Software.
3. Permitted Use.

   As selected in your Entitlement, one or more of the following Permitted Uses will apply to your use of Software. Unless you have an Entitlement that expressly

permits it, you may not use Software for any of the other Permitted Uses. If you don't have an Entitlement, or if your Entitlement doesn't cover additional software delivered to you, then such software is for your Evaluation Use.

a. Evaluation Use. You may evaluate Software internally for a period of 90 days from your first use.

b. Research and Instructional Use. You may use Software internally to design, develop and test, and also to provide instruction on such uses.

c. Individual Use. You may use Software internally for personal, individual use.

d. Commercial Use. You may use Software internally for your own commercial purposes.

e. Service Provider Use. You may make Software functionality accessible (but not by providing Software itself or through outsourcing services) to your end users in an extranet deployment, but not to your affiliated companies or to government agencies.

4. Licensed Units.

Your Permitted Use is limited to the number of Licensed Units stated in your Entitlement. If you require additional Licensed Units, you will need additional Entitlement(s).

5. Restrictions.

a. The copies of Software provided to you under this Agreement are licensed, not sold, to you by Sun. Sun reserves all rights not expressly granted.

b. You may make a single archival copy of Software, but otherwise may not copy, modify, or distribute Software. However if the Sun documentation accompanying Software lists specific portions of Software, such as header files, class libraries, reference source code, and/or redistributable files, that may be handled differently, you may do so only as provided in the Sun documentation.

c. You may not rent, lease, lend or encumber Software.

d. Unless enforcement is prohibited by applicable law, you may not decompile, or reverse engineer Software.

e. The terms and conditions of this Agreement will apply to any Software updates, provided to you at Sun's discretion, that replace and/or supplement the original Software, unless such update contains a separate license.

f. You may not publish or provide the results of any benchmark or comparison tests run on Software to any third party without the prior written consent of Sun.

g. Software is confidential and copyrighted.

h. Unless otherwise specified, if Software is delivered with embedded or bundled software that enables functionality of Software, you may not use such software on a stand-alone basis or use any portion of such software to interoperate with any program(s) other than Software.

i. Software may contain programs that perform automated collection of system data and/or automated software updating services. System data collected through such programs may be used by Sun, its subcontractors, and its service delivery partners for the purpose of providing you with remote system services and/or improving Sun's software and systems.

j. Software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility and Sun and its licensors disclaim any express or implied warranty of fitness for such uses.

k. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement.

6. Term and Termination.

The license and service term are set forth in your Entitlement(s). Your rights under this Agreement will terminate immediately without notice from Sun if you materially breach it or take any action in derogation of Sun's and/or its licensors' rights to Software. Sun may terminate this Agreement should any Software become, or in Sun's reasonable opinion likely to become, the subject of a claim of intellectual property infringement or trade secret misappropriation. Upon termination, you will cease use of, and destroy, Software and confirm compliance in writing to Sun. Sections 1, 5, 6, 7, and 9-15 will survive termination of the Agreement.

7. Java Compatibility and Open Source.

Software may contain Java technology. You may not create additional classes to, or modifications of, the Java technology, except under compatibility requirements available under a separate agreement available at www.java.net.

Sun supports and benefits from the global community of open source developers, and thanks the community for its important contributions and open standards-based technology, which Sun has adopted into many of its products.

Please note that portions of Software may be provided with notices and open source licenses from such communities and third parties that govern the use of those portions, and any licenses granted hereunder do not alter any rights and obligations you may have under such open source licenses, however, the disclaimer of warranty and limitation of liability provisions in this Agreement will apply to all Software in this distribution.

8. Limited Warranty.

Sun warrants to you that for a period of 90 days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Some states do not allow limitations on certain implied warranties, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

9. Disclaimer of Warranty.

UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

10. Limitation of Liability.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE

DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

11. Export Regulations.

All Software, documents, technical data, and any other materials delivered under this Agreement are subject to U.S. export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with these laws and regulations and acknowledge that you have the responsibility to obtain any licenses to export, re-export, or import as may be required after delivery to you.

12. U.S. Government Restricted Rights.

If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

13. Governing Law.

Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

14. Severability.

If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

15. Integration.

This Agreement, including any terms contained in your Entitlement, is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

Please contact Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054 if you have questions.

BSH-CORE 1.3.0

BeanShell is a free software project. It's continued development depends on the interest and support of users and developers like you. The source code is available for you to use and extend or integrate into your software freely under either the terms of the Sun Public License or the GNU Lesser Public License (see below).

The "cost" of this software is simply to let us know how you are using BeanShell. You can do this by filling out the BeanShell User Info Form. Please feel free to wait until you have started using BeanShell to do this.

Dual Licensing: Sun Public License / Gnu Lesser Public License

BeanShell is dual licensed under both the SPL and LGPL. You may use and develop BeanShell under either license.

DOM4J

BSD style license

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name "DOM4J" must not be used to endorse or promote products derived from this Software without prior written permission of MetaStuff, Ltd. For written permission, please contact dom4j-info@metastuff.com.

Products derived from this Software may not be called "DOM4J" nor may "DOM4J" appear in their names without prior written permission of MetaStuff, Ltd. DOM4J is a registered trademark of MetaStuff, Ltd.

Due credit should be given to the DOM4J Project - http://www.dom4j.org

THIS SOFTWARE IS PROVIDED BY METASTUFF, LTD. AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL METASTUFF, LTD. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 2001-2005 (C) MetaStuff, Ltd. All Rights Reserved.

ANTLR 3

[The BSD License]

Copyright (c) 2003-2008, Terence Parr

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the author nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

JAVA SERVICE WRAPPER

Copyright (c) 1999, 2006 Tanuki Software, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Java Service Wrapper and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sub-license, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Portions of the Software have been derived from source code developed by Silver Egg Technology under the following license:

Silver Egg Techology License ----------

Copyright (c) 2001 Silver Egg Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sub-license, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

END Silver Egg Techology License ----------

JNI REGISTRY 3.1.3

Release 3.1.3, September 11, 2003

The com.ice.jni.registry package is a Java native interface for the Windows Registry API. This allows Java program to access, modify, and export Windows Registry resources.

The com.ice.jni.registry package has been placed into the public domain. Thus, you have absolutely no licensing issues to consider. You may do anything you wish with the code. Of course, I always appreciate it when you properly credit my work.

The package will work only with Java 1.1 and greater, and uses the Javasoft native interface, not the Netscape interface. The package also includes a DLL that implements the interface. The package has been used with JDK1.2, and JDK1.3, JDK1.4, as well as JDK1.1.8.

The package includes the pre-built DLL (debug and release), source code (both the Java and the DLL's C code), as well as the compiled Java classes.

The original release was posted on November 17, 1997. The current release is 3.1.3, which was posted on September 11, 2003.

WSDL4J

Permission to copy and display the Java APIs for WSDL Specification, in any medium without fee or royalty is hereby granted, provided that you include the following on ALL copies of the Java APIs for WSDL Specification, or portions thereof, that you make: 1. A link or URL to the Java APIs for WSDL Specification at this location: http://www-124.ibm.com/developerworks/projects/wsdl4j/ 2. The copyright notice as shown in the Java APIs for WSDL Specification. Except for the limited copyright license granted above, the material contained herein is not a license, either expressly or impliedly, to any intellectual property owned or controlled by any of the authors or developers of this material. The material contained herein is provided on an "AS IS" basis and to the maximum extent permitted by applicable law, this material is provided AS IS AND WITH ALL FAULTS, and the authors and developers of this material hereby disclaim all other warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THIS MATERIAL. IN NO EVENT WILL ANY AUTHOR OR DEVELOPER OF THIS MATERIAL BE LIABLE TO ANY

OTHER PARTY FOR THE COST OF PROCURING SUBSTITUTE GOODS OR SERVICES, LOST PRO FITS, LOSS OF USE, LOSS OF DATA, OR ANY INCIDENTAL, CONSEQUENTIAL, DIRECT, INDIRECT, OR SPECIAL DAMAGES WHETHER UNDER CONTRACT, TORT, WARRANTY, OR OTHERWISE, ARISING IN ANY WAY OUT OF THIS OR ANY OTHER AGREEMENT RELATING TO THIS MATERIAL, WHETHER OR NOT SUCH PARTY HAD ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES. The name and trademarks of the Authors may NOT be used in any manner, including advertising or publicity pertaining to the Java APIs for WSDL Specification or its contents without specific, written prior permission. Title to copyright in the Java APIs for WSDL Specification will at all times remain with the Authors. No other rights are granted by implication, estoppel or otherwise.

Concurrent.jar

All classes are released to the public domain and may be used for any purpose whatsoever without permission or acknowledgment. Portions of the CopyOnWriteArrayList and ConcurrentReaderHashMap classes are adapted from Sun JDK source code. These are copyright of Sun Microsystems, Inc, and are used with their kind permission, as described in this license (http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/sun-u.c.license.pdf).

AOPAlliance

LICENCE: all the source code provided by AOP Alliance is Public Domain. (http://aopalliance.sourceforge.net/)

XDOCLET 1.2.3

Copyright (c) 2000-2004, XDoclet Team

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the XDoclet team nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY

DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Other Licenses

Licenses of the products XDoclet depends on:

Jakarta Ant (http://xdoclet.sourceforge.net/xdoclet/licenses/ant-license.html)

Xerces (http://xdoclet.sourceforge.net/xdoclet/licenses/xerces-license.html)

JDOM 1.0B9

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.
3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact <request_AT_jdom_DOT_org>.
4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management <request_AT_jdom_DOT_org>.

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)." Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter <jhunter_AT_jdom_DOT_org> and Brett McLaughlin <brett_AT_jdom_DOT_org>. For more information on the JDOM Project, please see <http://www.jdom.org/>.

MSVP60.DLL

Vcredist.exe installs the latest run-time components for Visual C++ applications

View products that this article applies to.
(http://support.microsoft.com/default.aspx?scid=kb;en-us;259403#appliesto)

Article ID:259403

Last Review: July 18, 2007

Revision: 6.7

This article was previously published under Q259403

SUMMARY

Vcredist.exe is a self-extracting executable file that installs the latest version of the Microsoft Visual C++ run-time files and operating system components that are required by most projects created with Visual C++ 6.0. These files include fixes that are included with Visual Studio 6.0 Service Pack 4 (SP4).

Beginning with Visual Studio 6.0 Service Pack 5, Vcredist.exe is included with the service pack. The Vcredist.exe pointed to by this article will continue to be the Visual Studio 6.0 Service Pack 4 version. To obtain the latest version of Vcredist.exe, you will need to get a copy of the latest service pack. For details, see the following Microsoft Developer Network (MSDN) Web site:

http://msdn2.microsoft.com/en-us/vstudio/aa718359.aspx
(http://msdn2.microsoft.com/en-us/vstudio/aa718359.aspx)

MORE INFORMATION

To obtain the Vcredist.exe update, download and run the following application, which installs Vcredist.exe to the directory that you specify.

The following file is available for download from the Microsoft Download Center:

Download the VC6RedistSetup_enu.exe package now.
(http://download.microsoft.com/download/vc60pro/update/1/w9xnt4/en-us/vc6redistsetup_enu.exe)

For more information about how to download Microsoft support files, click the following article number to view the article in the Microsoft Knowledge Base:

119591 (http://support.microsoft.com/kb/119591/) How to obtain Microsoft support files from online services

Microsoft scanned this file for viruses. Microsoft used the most current virus-detection software that was available on the date that the file was posted. The file is stored on security-enhanced servers that help prevent any unauthorized changes to the file.
Download the VC6RedistSetup_deu.exe package now.
(http://download.microsoft.com/download/vc60pro/update/2/w9xnt4/en-us/vc6redistsetup_deu.exe)

Release Date: November 16, 2000

For more information about how to download Microsoft support files, click the following article number to view the article in the Microsoft Knowledge Base:

119591 (http://support.microsoft.com/kb/119591/) How to obtain Microsoft support files from online services

Microsoft scanned this file for viruses. Microsoft used the most current virus-detection software that was available on the date that the file was posted. The file is stored on security-enhanced servers that help prevent any unauthorized changes to the file.

For more information about how to download files from the Microsoft Download Center, please visit the Download Center at the following Web address:

http://www.microsoft.com/downloads/Search.aspx
(http://www.microsoft.com/downloads/Search.aspx)

VC6RedistSetup.exe will present you with an End User License Agreement. When you accept the agreement, a single file, Vcredist.exe, is extracted.

Vcredist.exe installs the following core files, which are included with Visual Studio 6.0 SP4. These files are base dependencies for most components and applications created with Visual C++ 6.0:

File Name	Version	Size
Asycfilt.dll	2.40.4275.1	144KB (147,728 bytes)
Atl.dll (Windows 95 and Windows 98)	3.0.8449.0	72KB (73,785 bytes)
Atl.dll (Windows NT)	3.0.8449.0	57.5KB (58,938 bytes)
Comcat.dll	4.71.1460.1	21.7KB (22,288 bytes)
Comctl32.dll (Windows 95 and Windows 98)	5.80.2614.3600	564KB (577,808 bytes)
Comctl32.dll (Windows NT)	5.80.2614.3600	544KB (557,328 bytes)
Mfc42.dll	6.0.8665.0	972KB (995,383 bytes)
Mfc42u.dll (Windows NT only)	6.0.8665.0	972KB (995,384 bytes)
Msvcirt.dll	6.0.8168.0	76KB (77,878 bytes)
Msvcp60.dll	6.0.8168.0	392KB (401,462 bytes)
Msvcrt.dll	6.0.8797.0	272KB (278,581 bytes)
Oleaut32.dll	2.40.4275.1	584KB (598,288 bytes)
Olepro32.dll	5.0.4275.1	160KB (164,112 bytes)
Stdole2.tlb	2.40.4275.1	17.5KB (17,920 bytes)

In addition, the following files are also installed by Vcredist.exe. These are supporting files for the Vcredist.exe Setup program:

File Name	Version	Size
Advpack.dll	4.71.1015.0	73.2KB (74,960 bytes)
W95inf16.dll	4.71.704.0	2.21KB (2,272 bytes)
W95inf32.dll	4.71.16.0	4.50KB (4,608 bytes)

Vcredist.exe supports the following command-line switches:

no switches = non-quiet mode, displays progress bar and reboot prompt

/q = semi-quiet mode, displays reboot message, and no progress bar

/q /r:n = no reboot message or progress bar

Vcredist.exe is not a full-featured installation package. As such, it is not a recommended redistribution method for the preceding files. This package does not communicate error messages back to the program or user that is starting Vcredist.exe. Therefore, we highly recommend that programs starting Vcredist.exe first check for available disk space (approximately 10 MB), read-only system files, administrator privileges, and a valid TEMP directory. The absence of any of these prerequisites can cause this package to incorrectly install some of the files onto the target system.

In addition, this package does not install any database components or localized satellite dynamic-link libraries (DLLs). For information about how to install database components such as ODBC, ADO, or DAO, please refer to the following Redistributing Microsoft Visual C++ 6.0 Applications article on the Microsoft Developer Network (MSDN) Web site:

http://msdn2.microsoft.com/en-us/library/aa260978(VS.60).aspx (http://msdn2.microsoft.com/en-us/library/aa260978(VS.60).aspx)

For more information about installing localized resource DLLs for MFC, click the following article number to view the article in the Microsoft Knowledge Base:

208983 (http://support.microsoft.com/kb/208983/) How to use MFC LOC DLLs

Note This package does not install these components on computers that are running Microsoft Windows 2000 or Microsoft Windows Millennium (Me) systems. On computers that are running Windows 2000 and Windows Millennium, these components can only be updated through operating system updates and service packs for these operating systems.

Vcredist.exe can be freely redistributed with your application. You should also provide a copy of this Knowledge Base article.

PDH.dll 5.0.2195.2668

FILE: Latest Redistributable PDH.dll Available for Windows NT 4.0

View products that this article applies to. (http://support.microsoft.com/kb/284996/en-us#appliesto)

Article ID:284996

Last Review: November 21, 2006

Revision: 4.4

This article was previously published under Q284996

SUMMARY

Applications can use Performance Data Helper (PDH) APIs to collect performance data on Windows NT 4.0 and Windows 2000. The Windows 2000 operating system comes with PDH.dll. For Windows NT 4.0, a redistributable version of PDH.dll is available. This article provides access to this redistributable version of PDH.dll.

MORE INFORMATION

Performance Data Helper DLL (PDH.dll) for Windows NT 4.0

Note: For Windows 2000-based systems, use the system-supplied Pdh.dll file. Do not install a new version of Pdh.dll over the system-supplied version. This will fail because of Windows File Protection.

For Windows NT 4.0, install Pdh.dll into the private directory of the application (not into the system directory).

You have the following nonexclusive, royalty-free rights subject to the Distribution Requirements:

You may distribute PDH.dll on Windows NT 4.0.

The latest redistributable PDH.dll for Windows NT 4.0 that can be used by applications can be downloaded by clicking on the link below.

NT4Pdhdll.exe
(http://download.microsoft.com/download/winntsrv40/update/5.0.2195.2668/nt4/en-us/nt4pdhdll.exe)

Release Date: NOV-7-2000

For additional information about how to download Microsoft Support files, click the following article number to view the article in the Microsoft Knowledge Base:

119591 (http://support.microsoft.com/kb/119591/EN-US/) How to Obtain Microsoft Support Files from Online Services

Microsoft scanned this file for viruses. Microsoft used the most current virus-detection software that was available on the date that the file was posted. The file is stored on security-enhanced servers that help to prevent any unauthorized changes to the file. The NT4PDHDLL.exe file contains the following files:

File nameSize

PDH.dll151,312

PDH.dbg8,392

PDH.pdb140,288

Redist.txt612

A redistributable version of PDH.dll can also be directly downloaded from the Microsoft Platform SDK Web site.

MIBBLE 2.8

Mibble

Software License Agreement

Document No: DOC:2007:03

Author: Per Cederberg, sales@percederberg.net

Last Updated: 2007-12-05

Software License Agreement

IMPORTANT NOTICE -- READ CAREFULLY: This Software License Agreement ("License") for Customer use of Mibble Software is the agreement which governs use of the software of Firma Per Cederberg ("Seller"), including source code and associated printed materials ("Software"). By downloading, installing, copying, or otherwise using the Software, you agree to be bound by the terms of this License. If you do not agree to the terms of this License, delete all copies of the Software and contact the place of purchase for a full refund.

1. Definitions

Whenever used in this Contract, unless inconsistent with the subject matter or context of their use, the following words and terms shall have the respective meanings ascribed to them as follows:

a. "Seller" means Firma Per Cederberg includes its successors and permitted assigns.

b. "License" or "Agreement" means this nontransferable Software License Agreement including the Terms and Conditions provided herein.

c. "Buyer" or "Customer", means the entity or individual that downloads the Software, and includes its successors and permitted assigns.

d. "Parties", means Seller and Buyer, collectively, and "Party" means any one of them.

e. "Software", means the Mibble software in both object and source code.

2. License Grant

Upon Seller's receipt of the full purchase price, Seller grants to Buyer a non-exclusive license to:

a. use or modify the Software in source or object code to create derived works including the Software or any portion or element thereof,

b. process or permit to be processed any data associated with the Software,

c. release, distribute or make available, either generally or to any specific third-party, the Software in source or object code format.

Email: sales@percederberg.net

Web: http://www.percederberg.net/software

3. License Conditions

The grant of the License under section 2 hereof will remain subject to the following terms and conditions, as well as to the other provisions hereof:

a. Buyer acknowledges that the copyright and title to the Software and any trademarks or service marks relating thereto remain with Seller. Neither Buyer nor any third party shall have right, title or interest in the Software except as expressly set forth in this Agreement.

b. Buyer may not remove or obscure any copyright or other notices included in the Software source code.

c. The names "Mibble" or "Per Cederberg" may not be used to endorse or promote products derived from this software without specific prior written permission.

d. The Software is only distributed bundled with or integrated into Buyer programs that add significant functionality to the Software.

4. Delivery & Risk of Loss

Copies of the Software will be provided to the Buyer through electronic transfer (by means of HTTP or otherwise). Risk of loss for Software delivered under this License shall pass to Buyer at time of delivery.

5. Early Termination

In the event that either party believes that the other materially has breached any obligations under this Agreement, or if Seller believes that Buyer has exceeded the scope of the License, such party shall so notify the breaching party in writing. The

breaching party shall have 30 days from the receipt of notice to cure the alleged breach and to notify the non-breaching party in writing that cure has been effected. If the breach is not cured within 30 days, the non-breaching party shall have the right to terminate the Agreement without further notice. Upon Termination of this Agreement the Buyer must stop any further distribution of the Software or any modified or derived works within 5 days. Any copies of the Software distributed prior to such termination of this Agreement may remain in use according to the terms specifically provided elsewhere in this Agreement.

6. Perpetual License

   Except for termination for cause, Seller hereby grants to Buyer a nonexclusive, royalty-free, perpetual license to use the Software. Such use shall be in accordance with the provisions of this Agreement, which provisions shall survive any termination of this Agreement.

7. "As Is" Warranty

   SELLER PROVIDES THE SOFTWARE "AS IS" AND IS IN LIEU OF ANY OR ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY, ANY IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE OR ANY WARRANTY ARISING OUT OF PERFORMANCE OR CUSTOM OR USAGE OF TRADE INCLUDING BUT NOT LIMITED TO A WARRANTY AGAINST PATENT, COPYRIGHT OR TRADE SECRET INFRINGEMENT.

   Email: sales@percederberg.net

   Web: http://www.percederberg.net/software

8. Limitation Of Liability

   IN NO EVENT, WHETHER AS A RESULT OF BREACH OF CONTRACT, WARRANTY, TORT, STRICT LIABILITY OR OTHERWISE, SHALL BUYER OR SELLER BE LIABLE FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, INDIRECT OR EXEMPLARY DAMASELLER, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUES, LOSS OF USE OF THE HARDWARE OR ANY OTHER EQUIPMENT, COST OF CAPITAL, COST OF SUBSTITUTE GOODS, FACILITIES, SERVICES OR DOWNTIME COSTS.

   The provisions of this Article, Limitations Of Liability, shall apply notwithstanding any other provisions of these terms or of any other agreement.

9. Assignment

   Neither this License nor any interest in it shall be assigned directly or indirectly by Buyer without the prior written consent of Seller.

10. Enforceability

    If any provision of this License is held invalid, illegal or unenforceable, the validity, legality or enforceability of the remaining provisions will, to the extent of such invalidity, illegality, or unenforceability, be severed, but without in any way affecting the remainder of such provision or any other provision contained herein, all of which shall continue in full force and effect.

11. Entire Agreement

    This License supercedes all previous proposals, negotiations, conversations, and understandings, whether oral or written, and constitutes the sole and entire agreement between the parties with respect to the purchase by Buyer of the Software. No modification or deletion of, or addition to these terms will be

binding unless made in writing and signed by duly authorized representatives of both parties.

Email: sales@percederberg.net

Web: http://www.percederberg.net/software

Robohelp 5.0

MACROMEDIA SOFTWARE END USER LICENSE AGREEMENT

ATTENTION: YOU MAY NEED TO SCROLL DOWN TO THE END OF THIS EULA BEFORE YOU CAN AGREE TO THE EULA AND CONTINUE WITH THE SOFTWARE INSTALLATION.

IMPORTANT: THIS SOFTWARE END USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR, IF PURCHASED OR OTHERWISE ACQUIRED BY OR FOR AN ENTITY, AN ENTITY) AND MACROMEDIA. READ IT CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AND USING THE SOFTWARE. IT PROVIDES A LICENSE TO USE THE SOFTWARE AND CONTAINS WARRANTY INFORMATION AND LIABILITY DISCLAIMERS. BY INSTALLING AND USING THE SOFTWARE, YOU ARE CONFIRMING YOUR ACCEPTANCE OF THE SOFTWARE AND AGREEING TO BECOME BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS OF THIS EULA THEN MACROMEDIA IS UNWILLING TO GRANT YOU THIS LICENSE, YOU MUST NOT INSTALL OR USE THE SOFTWARE, AND (1) IF YOU RECEIVED THIS SOFTWARE ON CD-ROM, YOU MAY RETURN THE UNUSED SOFTWARE TO THE LOCATION WHERE YOU OBTAINED IT FOR A REFUND, IN ACCORDANCE WITH THE REFUND POLICY OF SUCH LOCATION; OR (2) IF YOU RECEIVED THIS SOFTWARE VIA DOWNLOAD FROM AN INTERNET WEB SITE, THEN YOU MUST DELETE ALL OF THE DOWNLOADED FILES AND YOU MAY OBTAIN A REFUND IN ACCORDANCE WITH THE REFUND POLICY OF SUCH INTERNET WEB SITE.

THIS EULA SHALL APPLY ONLY TO THE SOFTWARE SUPPLIED BY MACROMEDIA HEREWITH REGARDLESS OF WHETHER OTHER SOFTWARE IS REFERRED TO OR DESCRIBED HEREIN.

1. Definitions

   a. "Education Version" means a version of the Software, so identified, for use by students and faculty of educational institutions, only.

   b. "Not For Resale (NFR) Version" means a version, so identified, of the Software to be used to review and evaluate the Software, only.

   c. "Macromedia" means Macromedia, Inc., its subsidiary eHelp Corporation, and their licensors, if any.

   d. "Software" means only the Macromedia software program(s) and third party software programs, in each case, supplied by Macromedia herewith, and corresponding documentation, associated media, printed materials, and online or electronic documentation.

   e. "Trial Version" means a version of the Software, so identified, to be used only to review, demonstrate and evaluate the Software for a limited time period. The Trial Version may have limited features, may lack the ability for the end-user to save the end product, and will cease operating after a predetermined amount of time due to an internal mechanism within the Trial Version.

2. License Grants

The licenses granted in this Section 2 are subject to the terms and conditions set forth in this EULA:

a. Subject to Section 2(b), you may install and use the Software on a single computer; OR install and store the Software on a storage device, such as a network server, used only to install the Software on your other computers over an internal network, provided you have a license for each separate computer on which the Software is installed and run. Except as otherwise provided in Section 2(b), a license for the Software may not be shared, installed or used concurrently on different computers.

b. Portable or Home Computer Use for Software Requiring Mandatory Product Activation. For Software requiring Mandatory Production Activation, in addition to the single copy of the Software permitted in Section 2(a), the primary user of the computer on which the Software is installed may make a second copy of the Software and install it on either a portable computer or a computer located at his or her home for his or her exclusive use, provided that: (A) the second copy of the Software on the portable or home computer (i) is not used at the same time as the copy of the Software on the primary computer and (ii) is used by the primary user solely as allowed for such version or edition (such as for educational use only), (B) the second copy of the Software is not installed or used after the time such user is no longer the primary user of the primary computer on which the Software is installed, and (C) the Software was not licensed under a volume discount.

c. In the event the Software is distributed along with other Macromedia software products as part of a suite of products (collectively, the "Studio"), the license of the Studio is licensed as a single product and none of the products in the Studio, including the Software, may be separated for installation or use on more than one computer.

d. You may make one copy of the Software in machine-readable form solely for backup purposes. You must reproduce on any such copy all copyright notices and any other proprietary legends on the original copy of the Software. You may not sell or transfer any copy of the Software made for backup purposes.

e. You agree that Macromedia may audit your use of the Software for compliance with these terms at any time, upon reasonable notice. In the event that such audit reveals any use of the Software by you other than in full compliance with the terms of this Agreement, you shall reimburse Macromedia for all reasonable expenses related to such audit in addition to any other liabilities you may incur as a result of such non-compliance.

f. Unless otherwise set forth in the documentation relating to such code and/or the Software or in a separate agreement between you and Macromedia, you may modify the source code form of those portions of such software programs that are identified as sample code, sample application code, or components (each, "Sample Application Code") in the accompanying documentation solely for the purposes of designing, developing and testing websites and website applications developed using Macromedia software programs; provided, however, you are permitted to copy and distribute the Sample Application Code (modified or unmodified) only if all of the following conditions are met: (1) you distribute the compiled object Sample Application Code with your application; (2) you do not include the Sample Application Code in any product or application designed for website development; and (3) you do not use Macromedia's name, logos or other Macromedia trademarks to market your application. You agree to indemnify, hold harmless and defend

Macromedia from and against any loss, damage, claims or lawsuits, including attorney's fees, that arise or result from the use or distribution of your application.

g. Macromedia Redistributables. Subject to the terms and conditions of this EULA, Macromedia grants you the non-exclusive, royalty-free right to reproduce and distribute, in object code form only, any Macromedia Redistributables identified in the REDISTRB.TXT file located i) on the Software CD-ROM, ii) if the Software was downloaded, in the unpacked installation folder or iii) in the Software folder on the computer hard drive, provided, that you (I) do not distribute the Redistributables as a stand-alone product, except however, that you may distribute updates of the Redistributables separately for purposes of updating an existing end user of your previously-distributed product that uses the Redistributables; (II) include Macromedia's copyright notice for the Redistributables on the title page of any documentation, on the product CD, and/or in the About box for any software product that incorporates the Redistributables; (III) except as required above, do not use Macromedia's name, logo, or trademarks in connection with any product that incorporates the Redistributables; (IV) agree to indemnify, defend and hold Macromedia harmless from any and all liabilities (including attorney's fees) arising from any claims, lawsuits, or other legal proceedings that arise from or are related to the use or distribution of any software application product that you reproduced and/or distributed that incorporates the Redistributables; and (V) do not incorporate the Redistributables into any software product which would compete with the Software.

h. MS-Redistributables. Subject to the terms and conditions of this EULA, Macromedia grants you the non-exclusive, royalty-free right to reproduce and distribute, in object code form only, any MS-Redistributables identified in the REDISTRB.TXT located i) on the Software CD-ROM, ii) if the Software was downloaded, in the unpacked installation folder or iii) in the Software folder on the computer hard drive, provided that you (I) do not distribute the MS-Redistributables as a stand-alone product, provided, however, that you may distribute updates of the MS-Redistributables separately for purposes of updating an existing end user of your previously-distributed product that uses MS-Redistributables; (II) include the following copyright notice for the MS-Redistributables "Portions copyright (c) Microsoft Corporation. All rights reserved." on the product CD, disk label, the title page of the documentation, and/or the About box for any software application product that incorporates the MS-Redistributables; (III) except as required above, do not use Microsoft's name, logo, or trademarks to market any Help system that incorporates the MS-Redistributables; (IV) agree to indemnify, defend and hold Macromedia and Microsoft harmless from any and all liabilities (including attorney's fees) arising from any claims, lawsuits, or other legal proceedings that arise from or are related to the use or distribution of any software application product that you reproduced and/or distributed that incorporates the MS-Redistributables; (V) do not incorporate the MS-Redistributables into any software product which would compete with the Software, and (VI) if Microsoft makes a new release of the MS-Redistributables (other than an Update release), use all reasonable efforts to cease distribution of the older version and commence distribution of the new release. You may continue to distribute existing inventory that contains the older release for up to 3 months following such new release.

i. Distribution of any Software code, other than the Sample Application Code, the Macromedia Redistributables, and the MS-Redistributables, is specifically prohibited.

j. Mandatory Product Activation. The license rights granted under this Agreement may be limited to a specified number ofthe first thirty (30) days after you first install the Software unless you supply information required to activate your licensed copy within the time and the manner described during the Software setup sequence and/or the dialog boxes appearing during use of the Software. You may need to activate the Software through the use of the Internet or telephone; toll charges may apply. You may need to reactivate the Software if you modify your computer hardware or alter the Software. Product activation is based on the exchange of information between your computer and Macromedia. None of this information contains personally identifiable information nor can they be used to identify any personal information about you or any characteristics of your computer configuration. YOU ACKNOWLEDGE AND UNDERSTAND THAT THERE ARE TECHNOLOGICAL MEASURES IN THE SOFTWARE THAT ARE DESIGNED TO PREVENT UNLICENSED OR ILLEGAL USE OF THE SOFTWARE. YOU AGREE THAT MACROMEDIA MAY USE SUCH MEASURES AND YOU AGREE TO FOLLOW ANY REQUIREMENTS REGARDING SUCH TECHNOLOGICAL MEASURES. YOU ACKNOWLEDGE AND AGREE THAT THE SOFTWARE WILL CEASE TO FUNCTION UNLESS AND UNTIL YOU ACTIVATE THE APPLICABLE SOFTWARE ACTIVATION KEY.

k. Non-Exclusivity. Your license rights under this EULA are non-exclusive.

l. Separation of Components. The Software is licensed as a single product. You may not separate the Software's component parts for use on more than one computer.

3. License Restrictions

a. Other than as set forth in Section 2, you may not make or distribute copies of the Software, or electronically transfer the Software from one computer to another or over a network.

b. You may not alter, merge, modify, adapt or translate the Software, or decompile, reverse engineer, disassemble, or otherwise reduce the Software to a human-perceivable form.

c. Unless otherwise provided herein, you may not rent, lease, or sublicense the Software.

d. Other than with respect to a Trial Version or a Not For Resale Version of the Software, you may permanently transfer all of your rights under this EULA only as part of a sale or transfer, provided you retain no copies, you transfer all of the Software (including all component parts, the media and printed materials, any upgrades, this EULA, the serial numbers, and, if applicable, all other software products provided together with the Software), and the recipient agrees to the terms of this EULA. If the Software is an upgrade, any transfer must include all prior versions of the Software from which you are upgrading. If the copy of the Software is licensed as part of the whole Studio (as defined above), the Software shall be transferred only with and as part of the sale or transfer of the whole Studio, and not separately. You may retain no copies of the Software. You may not sell or transfer any Software purchased under a volume discount. You may not sell or transfer any Trial Version or Not For Resale Version of the Software.

e. Unless otherwise provided herein, you may not modify the Software or create derivative works based upon the Software.

f. Education Versions may not be used for, or distributed to any party for, any commercial purpose.

g. Unless otherwise provided herein, you shall not (A) in the aggregate, install or use more than one copy of the Trial Version of the Software, (B) download the Trial Version of the Software under more than one username, (C) alter the contents of a hard drive or computer system to enable the use of the Trial Version of the Software for an aggregate period in excess of the trial period for one license to such Trial Version, (D) disclose the results of software performance benchmarks obtained using the Trial Version to any third party without Macromedia?s prior written consent, or (E) use the Trial Version of the Software for a purpose other than the sole purpose of determining whether to purchase a license to a commercial or education version of the software; provided, however, notwithstanding the foregoing, you are strictly prohibited from installing or using the Trial Version of the Software for any commercial training purpose.

h. You may only use the Not for Resale Version of the Software to review and evaluate the Software.

i. You may not export the Software into any country prohibited by the United States Export Administration Act and the regulations thereunder.

j. You may receive the Software in more than one medium but you shall only install or use one medium. Regardless of the number of media you receive, you may use only the medium that is appropriate for the server or computer on which the Software is to be installed.

k. You may receive the Software in more than one platform but you shall only install or use one platform. If the Software is delivered in multiple versions or languages, you may only run one version or language of the Software, and you may not run the additional versions in any other language on any other computer.

l. You shall not use the Software to develop any application having the same primary function as the Software.

m. In the event that you fail to comply with this EULA, Macromedia may terminate the license and you must destroy all copies of the Software (with all other rights of both parties and all other provisions of this EULA surviving any such termination).

4. Upgrades

If this copy of the Software is an upgrade from an earlier version of the Software, it is provided to you on a license exchange basis. You agree by your installation and use of such copy of the Software to voluntarily terminate your earlier EULA and that you will not continue to use the earlier version of the Software or transfer it to another person or entity unless such transfer is pursuant to Section 3.

5. Prior Same Version License

If this copy of the Software is licensed as part of the Studio (as defined above), and you have a prior license to the same version of the Software, and the Studio was licensed to you with a discount based, in whole or in part, on your prior license to the same version, the Software is provided to you on a license exchange basis. You agree by your installation and use of this copy of the Software to voluntarily terminate your EULA with respect to such prior license and that you will not continue to install or use such prior license of the Software or transfer it to another person or entity.

6. Ownership

The foregoing license gives you limited license to use the Software. Macromedia and its suppliers retain all right, title and interest, including all copyright and intellectual property rights, in and to, the Software (as an independent work and as an underlying work serving as a basis for any application you may develop), and all copies thereof. All rights not specifically granted in this EULA, including Federal and International Copyrights, are reserved by Macromedia and its suppliers.

7. LIMITED WARRANTY AND DISCLAIMER

   a. Except with respect to any Sample Application Code, Macromedia Redistributables, MS Redistributables, Trial Version and Not For Resale Version of the Software, Macromedia warrants that, for a period of ninety (90) days from the date of delivery (as evidenced by a copy of your receipt): (i) when used with a recommended hardware configuration, the Software will perform in substantial conformance with the documentation supplied with the Software; and (ii) the physical media on which the Software is furnished, if provided by Macromedia, will be free from defects in materials and workmanship under normal use.

   b. MACROMEDIA PROVIDES NO REMEDIES OR WARRANTIES, WHETHER EXPRESS OR IMPLIED, FOR ANY SAMPLE APPLICATION CODE, MACROMEDIA REDISTRIBUTABLE, MS REDISTRIBUTABLE, TRIAL VERSION AND THE NOT FOR RESALE VERSION OF THE SOFTWARE. ANY SAMPLE APPLICATION CODE, TRIAL VERSION AND THE NOT FOR RESALE VERSION OF THE SOFTWARE ARE PROVIDED "AS IS".

   c. EXCEPT AS SET FORTH IN THE FOREGOING LIMITED WARRANTY WITH RESPECT TO SOFTWARE OTHER THAN ANY SAMPLE APPLICATION CODE, MACROMEDIA REDISTRIBUTABLE, MS REDISTRIBUTABLE, TRIAL VERSION AND NOT FOR RESALE VERSION, MACROMEDIA AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESS, IMPLIED, OR OTHERWISE, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ALSO, THERE IS NO WARRANTY OF NON-INFRINGEMENT AND TITLE OR QUIET ENJOYMENT. MACROMEDIA DOES NOT WARRANT THAT THE SOFTWARE IS ERROR-FREE OR WILL OPERATE WITHOUT INTERRUPTION. NO RIGHTS OR REMEDIES REFERRED TO IN ARTICLE 2A OF THE UCC WILL BE CONFERRED ON YOU UNLESS EXPRESSLY GRANTED HEREIN. THE SOFTWARE IS NOT DESIGNED, INTENDED OR LICENSED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE CONTROLS, INCLUDING WITHOUT LIMITATION, THE DESIGN, CONSTRUCTION, MAINTENANCE OR OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, AND LIFE SUPPORT OR WEAPONS SYSTEMS. MACROMEDIA SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCH PURPOSES.

   d. IF APPLICABLE LAW REQUIRES ANY WARRANTIES WITH RESPECT TO THE SOFTWARE, ALL SUCH WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY.

   e. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY MACROMEDIA, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF ANY WARRANTY PROVIDED HEREIN.

f. (USA only) SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATE TO STATE.

8. Exclusive Remedy

Your exclusive remedy under the preceding is to return the Software to the place you acquired it, with a copy of your receipt and a description of the problem. Provided that any non-compliance with the above warranty is reported in writing to Macromedia no more than ninety (90) days following delivery to you, Macromedia will use reasonable commercial efforts to supply you with a replacement copy of the Software that substantially conforms to the documentation, provide a replacement for defective media, or refund to you your purchase price for the Software, at its option. Macromedia shall have no responsibility if the Software has been altered in any way, if the media has been damaged by misuse, accident, abuse, modification or misapplication, or if the failure arises out of use of the Software with other than a recommended hardware configuration. Any such misuse, accident, abuse, modification or misapplication of the Software will void the warranty above. THIS REMEDY IS THE SOLE AND EXCLUSIVE REMEDY AVAILABLE TO YOU FOR BREACH OF EXPRESS OR IMPLIED WARRANTIES WITH RESPECT TO THE SOFTWARE AND RELATED DOCUMENTATION.

9. LIMITATION OF LIABILITY

a. NEITHER MACROMEDIA NOR ITS SUPPLIERS SHALL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, COVER OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR THE INABILITY TO USE EQUIPMENT OR ACCESS DATA, LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION OR THE LIKE), ARISING OUT OF THE USE OF, OR INABILITY TO USE, THE SOFTWARE AND BASED ON ANY THEORY OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF MACROMEDIA OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

b. MACROMEDIA'S TOTAL LIABILITY TO YOU FOR ACTUAL DAMAGES FOR ANY CAUSE WHATSOEVER WILL BE LIMITED TO THE GREATER OF $500 OR THE AMOUNT PAID BY YOU FOR THE SOFTWARE THAT CAUSED SUCH DAMAGE.

c. (USA only) SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU AND YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATE TO STATE.

d. THE FOREGOING LIMITATIONS ON LIABILITY ARE INTENDED TO APPLY TO THE WARRANTIES AND DISCLAIMERS ABOVE AND ALL OTHER ASPECTS OF THIS EULA.

10. Basis of Bargain

The Limited Warranty and Disclaimer, Exclusive Remedies and Limited Liability set forth above are fundamental elements of the basis of the agreement between Macromedia and you. Macromedia would not be able to provide the Software on

an economic basis without such limitations. Such Limited Warranty and Disclaimer, Exclusive Remedies and Limited Liability inure to the benefit of Macromedia?s licensors.

11. U.S. GOVERNMENT RESTRICTED RIGHTS LEGEND

This Software and the documentation are provided with "RESTRICTED RIGHTS" applicable to private and public licenses alike. The Software is a "commercial item," as that term is defined at 48 C.F.R. 2.101 (Oct 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sep 1995) and is provided to the U.S. Government only as a commercial end item. Any technical data provided with such Software is commercial technical data as defined in 48 C.F.R. 12.211 (Sep 1995). Consistent with 48 C.F.R. 12.211 through 12.212, 48 C.F.R. 227.7202-1 through 227.7202-4 (Jun 1995), and 48 C.F.R. 252.227-7015 (Nov 1995), all U.S. Government End Users acquire the Software with only those rights expressly set forth in this EULA.

Without limiting the foregoing, use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in this EULA and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013 (c)(1)(ii)(OCT 1988), FAR 12.212(a)(1995), FAR 52.227-19, or FAR 52.227-14, as applicable. For purposes of these regulations the Manufacturer of the Software is Macromedia, Inc., 600 Townsend, San Francisco, CA 94103.

12. (Outside of the USA) Consumer End Users Only

The limitations or exclusions of warranties and liability contained in this EULA do not affect or prejudice the statutory rights of a consumer, i.e., a person acquiring goods otherwise than in the course of a business.

The limitations or exclusions of warranties, remedies or liability contained in this EULA shall apply to you only to the extent such limitations or exclusions are permitted under the laws of the jurisdiction where you are located.

13. Third Party Software

The Software may contain third party software which requires notices and/or additional terms and conditions. Such required third party software notices and/or additional terms and conditions are located at http://www.macromedia.com/go/thirdparty/ and are made a part of and incorporated by reference into this EULA. By accepting this EULA, you are also accepting the additional terms and conditions, if any, set forth therein.

14. General

a. This EULA shall be governed by the internal laws of the State of California, without giving effect to principles of conflict of laws. You hereby consent to the exclusive jurisdiction and venue of the state courts sitting in San Francisco County, California or the federal courts in the Northern District of California to resolve any disputes arising under this EULA. In each case this EULA shall be construed and enforced without regard to the United Nations Convention on the International Sale of Goods.

b. This EULA contains the complete agreement between the parties with respect to the subject matter hereof, and supersedes all prior or contemporaneous agreements or understandings, whether oral or written. You agree that any varying or additional terms contained in any purchase order or other written notification or document issued by you in relation to the Software licensed hereunder shall be of no effect. The failure or delay of Macromedia to exercise

any of its rights under this EULA or upon any breach of this EULA shall not be deemed a waiver of those rights or of the breach.

c. No Macromedia dealer, agent or employee is authorized to make any amendment to this EULA.

d. If any provision of this EULA shall be held by a court of competent jurisdiction to be contrary to law, that provision will be enforced to the maximum extent permissible, and the remaining provisions of this EULA will remain in full force and effect.

e. All questions concerning this EULA shall be directed to: Macromedia, Inc., 600 Townsend, San Francisco, CA 94103, Attention: General Counsel.

f. Macromedia and other trademarks contained in the Software are trademarks or registered trademarks of Macromedia, Inc. in the United States and/or other countries. Third party trademarks, trade names, product names and logos may be the trademarks or registered trademarks of their respective owners. You may not remove or alter any trademark, trade names, product names, logo, copyright or other proprietary notices, legends, symbols or labels in the Software. Except for the rights granted in Section 2 above relating to Sample Application code, Macromedia Redistributables, and MS Redistributables, his EULA does not authorize you to use Macromedia?s or its licensors? names or any of their respective trademarks.

Microsoft SQL SERVER DRIVER 2005, 1.2

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2005 JDBC DRIVER

October 2007

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft:

- updates
- supplements
- Internet-based services
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

By using the software, you accept these terms. If you do not accept them, do not use the software.

If you comply with these license terms, you have the rights below.

1. INSTALLATION AND USE RIGHTS. You may install and use any number of copies of the software on your devices.

2. SCOPE OF LICENSE. The software is licensed, not sold. This agreement only gives you some rights to use the software. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not:

- disclose the results of any benchmark tests of the software to any third party without Microsoft's prior written approval;
- reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
- publish the software for others to copy; or
- rent, lease or lend the software.

3. TRANSFER TO A THIRD PARTY. The first user of the software may transfer it and this agreement directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the software. The first user must uninstall the software before transferring it separately from the device. The first user may not retain any copies.
4. EXPORT RESTRICTIONS. The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
5. SUPPORT SERVICES. Because this software is "as is," we may not provide support services for it.
6. ENTIRE AGREEMENT. This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.
7. APPLICABLE LAW
   a. United States. If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
   b. Outside the United States. If you acquired the software in any other country, the laws of that country apply.
8. LEGAL EFFECT. This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
9. DISCLAIMER OF WARRANTY. The software is licensed "as-is." You bear the risk of using it. Microsoft gives no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this agreement cannot change. To the extent permitted under your local laws, Microsoft excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.
10. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. You can recover from Microsoft and its suppliers only direct damages up to U.S. $5.00. You cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages. This limitation applies to:
    - anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and
    - claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

Please note: As this software is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque: Ce logiciel étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le logiciel visé par une licence est offert " tel quel ". Toute utilisation de ce logiciel est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au logiciel, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers ; et
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Install Anywhere

END-USER LICENSE AGREEMENT

InstallAnywhere®

IMPORTANT-READ CAREFULLY: This End-User License Agreement ("Agreement") is a legal contract between you (either (a) an individual user or (b) a business organization ("you")) and Licensor (as designated below) for the InstallAnywhere software, including any associated media, printed materials and electronic documentation (the "Software").

By clicking on the "I ACCEPT" button, by opening the package that contains the Software, or by copying, downloading, accessing or otherwise using the Software, you agree to be bound by the terms of this Agreement and you represent that you are

authorized to enter into this Agreement on behalf of your corporate entity (if applicable). If you do not wish to be bound by the terms of this Agreement, click the "I DO NOT ACCEPT" button, and do not install, access or use the Software.

As used herein, "Licensor" means Macrovision Corporation or its subsidiaries.

EVALUATION SOFTWARE

If you have received the Software for purposes of evaluation, regardless of how labeled, the use of the Software is limited to a specified period of time, as detailed in the email accompanying the download instructions (the "Evaluation Period") and all use will be governed by the terms set forth below.

1. Grant of License. Licensor grants you a limited, personal, internal use, non-exclusive, non-transferable license to use the Software solely to evaluate its suitability for your internal business requirements during the Evaluation Period. Without limiting the foregoing, you may not use the Software during the Evaluation Period to create publicly distributed computer software or for any other commercial purpose. This license may be terminated by Licensor at any time upon notice to you and will automatically terminate, without notice, upon the first to occur of the following: (a) the completion of your evaluation of the Software or (b) the expiration of the Evaluation Period.
2. Limited Use Software. Portions of the full-use version of the Software may be withheld or unusable and use of the Software may require accessing portions of the Software remotely through the Internet. Full use of the Software may be restricted by technological protections.
3. Disclaimer of Warranty. THE SOFTWARE IS PROVIDED ONLY FOR EVALUATION PURPOSES ON AN "AS IS" BASIS. LICENSOR EXPRESSLY DISCLAIMS ALL WARRANTIES, REPRESENTATIONS AND CONDITIONS INCLUDING THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.
4. Limitation of Liability. IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY DAMAGES, INCLUDING LOST PROFITS OR DATA, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE OR ANY DATA SUPPLIED THEREWITH, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY. In no case will Licensor's liability for damages hereunder exceed fifty dollars (US $50).

For Users Outside of the United States, Canada or Mexico LICENSOR DOES NOT LIMIT OR EXCLUDE ITS LIABILITY FOR DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE.

SOFTWARE LICENSE

1. Grant of License. Upon your payment of the fees shown on the invoice and acceptance of this Agreement, Licensor grants you a limited, personal, non-exclusive license to install and use the Software on the terms and conditions set forth herein. You may install and use one copy of the Software on a single computer only for your internal business purposes. You may make one back up and/or archival copy of the Software.

   If you have licensed under the node locked model, you may install and use one copy of the Software on a single computer only for your internal business purposes. You may make one back up and/or archival copy of the Software.

If you have licensed under the concurrent licensing model, you may install the Software on any machine used only for your internal business purposes. The number of machines that may use the Software concurrently at any time will be governed by the number of concurrent licenses specified on the original invoice. All machines using the Software must have the ability to communicate with a license server to be authorized to use the Software. You may make one back up and/or archival copy of the Software.

2. Restrictions on Use of Software. You may not (a) make the Software available for use by others in any service bureau or similar arrangement; (b) distribute, sublicense, transfer, or lend the Software to any third party; or (c) disassemble or reverse engineer (except in European Union countries, to the extent allowed by law) the Software or (d) copy or adapt the Software for the purpose of error correction or making derivative works.. You may copy the Software solely for backup/archival purposes, provided that you include all copyright and similar rights notices. Licensor (or its licensor) retains all right, title, and interest in the Software (and in all copies). Unauthorized copying and modification of the Software is not permitted.

   If you have a license to the InstallAnywhere Collaboration or InstallAnywhere Enterprise, you may use the Software for the purposes of creating unit test installations for your own exclusive use. You may use the software as a plug-in to the Eclipse Open Source IDE. Licensor is not licensing to you any right, title, and interest with respect to the Eclipse Open Source IDE; your use of the Eclipse Open Source IDE is subject to your acceptance of the terms and conditions of the end-user license agreement from Eclipse Foundation for that product.

3. Shared Use on a Single Computer. Subject to the exceptions set forth herein, a copy of the Software installed on a single common machine may be shared for internal use by your employees, provided that a license has been purchased for each individual user.

4. Redistributable Files. The Software component parts may not be separated for use on more than one computer, except as set forth in this Agreement. You may copy the files specifically identified in the documentation as "redistributables" and redistribute such files to your end users of your products, provided that: (a) all such distribution is done solely with the redistributables as an integral part of your software installations; (b) all copies of the redistributables must be exact and unmodified; and (c) you grant your end users a limited, personal, non-exclusive and non-transferable license to use the redistributables only to the extent required for the permitted operation of your products and not to distribute them further. You will reproduce with the redistributables all applicable trademark and copyright notices that accompany the Software, but you may not use Licensor's name, logos or trademarks to market your products.

5. Limited Warranty and Disclaimer of Warranty. Licensor warrants that: a. it has the right and authority to grant the rights described in this Agreement, and; the Software, as provided, will substantially perform the functions described in the documentation when operated in the intended environment for a period of ninety (90) days from the date of delivery (the "Warranty Period").

   b. THE WARRANTIES ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, REPRESENTATIONS OR CONDITIONS EXPRESS OR IMPLIED. LICENSOR EXPRESSLY DISCLAIMS ANY WARRANTIES AND/OR CONDITIONS OF NON-INFRINGEMENT, MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. Licensor does not warrant that the Software will (a) achieve specific results, (b) operate without interruption, or (c) be error free.

6. Ownership. This Agreement does not convey to you any rights of ownership in the Software. All right, title, and interest in the Software and in any ideas, know-how, and programs which are developed by Licensor in the course of providing any technical services, including any enhancements or modifications made to the Software, shall at all times remain the property of Licensor or its licensor. You acknowledge and agree that the Software is licensed, not sold. You shall not permit the Software to be accessed or used by anyone other than your employees whose duties require such access or use.

   You will not remove, modify or alter any of Licensor's copyright, trademark or proprietary rights notices from any part of the Software, including but not limited to any such notices contained in the physical and/or electronic media or documentation, in the Setup Wizard dialogue or 'about' boxes, in any of the runtime resources and/or in any web-presence or web-enabled notices, code or other embodiments originally contained in or otherwise created by the Software, or in any archival or back-up copies, if applicable.

7. Transfer of Software. You may not, by operation of law or otherwise, transfer any license rights or other interests in Evaluation Software, or Software labeled "Not for Resale" or "NFR." You may not transfer any license rights or other interests in any other Software, unless (a) you permanently and wholly transfer all your rights under this Agreement; (b) you retain no copies (whole or partial); (c) you permanently and wholly transfer all of the Software (including component parts, media, printed materials, upgrades, prior versions, and authenticity certificates); and (d) the transferee agrees to abide by all the terms of this Agreement.

8. Limitation of Remedy and Liability. During the Warranty Period, in the event of any breach of the warranty outlined in Section 5b above, Licensor's (and its suppliers), entire liability and your exclusive remedy will be, at Licensor's option, to either, repair or replace the defective Software. NEITHER LICENSOR NOR ITS LICENSOR, IF ANY, SHALL BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OR FOR DAMAGE TO SYSTEMS OR DATA, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. LICENSOR'S LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED THE AMOUNT OF LICENSE FEES THAT YOU HAVE PAID.

   For Users Outside of the United States, Canada or Mexico: No person who is not a party to this Agreement shall be entitled to enforce any terms of the same under the Contracts (Rights of Third Parties) Act 1999.

   For Users Outside of the United States, Canada or Mexico LICENSOR DOES NOT LIMIT OR EXCLUDE ITS LIABILITY FOR DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE.

9. Maintenance Services. If ordered by you and upon payment of the applicable fee, you are entitled to receive technical support services, including corrections, fixes and enhancements to the Software as such are made generally available (the "maintenance services") from Licensor in accordance with Licensor's then-current maintenance terms for the applicable maintenance level purchased by you. Maintenance services will not include any releases of the Software which Licensor determines to be a separate product or for which Licensor charges its customers extra or separately.

10. Upgrades and Subscription. If you purchased a license for the Software which is identified as an "upgrade" or "subscription", you must have a valid license for the version of the Software which the "upgrade" or "subscription" supplements.

11. Unauthorized Use and Validation of Use. IN ORDER TO PROTECT THE SOFTWARE FROM UNAUTHORIZED USE AND IN ORDER TO CONFIRM YOUR COMPLIANCE WITH THE LICENSE GRANTS AND RESTRICTIONS SET FORTH IN THIS AGREEMENT, THE SOFTWARE CONTAINS A VALIDATION PROCEDURE WHICH MAY TRANSMIT YOUR IP ADDRESS AND/OR APPLICABLE LICENSE KEY RELATING TO THE SOFTWARE TO LICENSOR. IF THE SOFTWARE DETECTS ANY VIOLATION OF THE TERMS OF THIS AGREEMENT, YOU MAY BE CONTACTED BY LICENSOR REGARDING YOUR USE OF THE SOFTWARE AND/OR YOU MAY BE UNABLE TO USE THE SOFTWARE AND/OR CREATE UNRESTRICTED INSTALLER PRODUCTS UNTIL THE PROBLEM IS CORRECTED. IF YOU ARE UNABLE TO USE THE SOFTWARE AND/OR CREATE UNRESTRICTED INSTALLER PRODUCTS, YOU SHOULD IMMEDIATELY CONTACT LICENSOR.

12. Reports. Within thirty (30) days following Licensor's written request, and no more frequently than twice in any twelve (12) month period, you shall provide Licensor with a written statement certifying that you are not using copies of the Software in violation of this Agreement.

13. Audit. During the term of this Agreement and for a period of twelve (12) months thereafter, you shall permit, no more than once in any twelve (12) month period, a third party auditor, upon thirty (30) days prior written notice from Licensor and during normal business hours, to examine and audit your records to determine your compliance with this Agreement and report such findings to Licensor. Licensor shall bear the expense of the audit unless the audit uncovers that you have used the Software in violation of the terms of this Agreement or have unpaid the license fees rightfully owed to Licensor, in which event you shall bear the expenses for such audit. In the event such audit is the result of your failure to provide reports as set forth in Section 12, then you shall bear the expense of such audit.

14. Dual-Media Software. You may receive the Software in more than one medium (electronic and on a CD, for example). Receipt of the Software in more than a single manner (electronic or on a CD, for example) does not expand the license rights granted to you hereunder. Your use of the Software is limited to the number of licenses that you have acquired overall, regardless of number or type of medium on which it has been provided.

15. U.S. Government Restricted Rights. The Software and Documentation are provided as "Commercial Computer Software" or "restricted computer software". Use, duplication, or disclosure by the U.S. Government or a U.S. Government subcontractor is subject to the restrictions set forth in 48.C.F.R. Section 12.212 or 48 C.F.R 227.2702, as applicable or successor provisions. The manufacturer is Macrovision Corporation, 2830 De La Cruz Boulevard, Santa Clara, CA 95050 USA.

16. U. S. Export Restrictions. You will fully comply with all relevant export laws and regulations, including but not limited to the U.S. Export Administration Regulations and Executive Orders ("Export Controls"). You warrant that you are not a person, company or destination restricted or prohibited by Export Controls ("Restricted Person"). You will not, directly or indirectly, export, re-export, divert, or transfer the Software, any portion thereof or any materials, items or technology relating to Licensor's business or related technical data or any direct product thereof to any Restricted Person.

17. Termination. Your license may be terminated by Licensor if (a) you fail to make payment and/or (b) you fail to comply with the terms of this Agreement within ten (10) days after receipt of written notice of such failure. In the event of

termination, you must cease using the Software, destroy all copies of the Software (including copies in storage media) and certify such destruction to Licensor. This requirement applies to all copies in any form, partial or complete. Upon the effective date of any termination, you relinquish all rights granted under this Agreement.

18. Relationship of Parties. You and Licensor are independent parties. Nothing in this Agreement shall be construed as making you an employee, agent or legal representative of Licensor.
19. No Third-Party Beneficiaries. There are no third-party beneficiaries of this Agreement.
20. Controlling Law. This Agreement will be governed by the laws of California, USA, excluding conflicts of law, except that, for Users Outside of the United States, Canada or Mexico, this Agreement will be governed by the laws of England and Wales and you submit to the jurisdiction of the courts of England and Wales. This Agreement is not subject to the United Nations Convention on Contracts for the Sale of Goods.
21. Company Name. Licensor may include your company name in a list of Licensor customers.
22. Payment Terms/Shipments. All fees are in US Dollars and are non-refundable. For Users Outside of the United States, Canada or Mexico: All fees are in the currency outlined in the quote/invoice and are non-refundable. Fees are due within 30-days of the date of the invoice. Maintenance services purchased may be renewed for the next annual period for the amount specified on the original invoice for the Software. All shipments of any media will be FOB Origin.
23. Taxes. All fees do not include taxes. If Licensor is required to pay any sales, use, GST, VAT, or other taxes in connection with your order, other than taxes based on Licensor's income, such taxes will be billed to and paid by you.
24. Entire Agreement. This Agreement constitutes the complete and entire understanding and agreement of all terms, conditions and representations between you and Licensor with respect to the Software and may be modified only in writing by both parties. No term or condition contained in your purchase order will apply unless expressly accepted by Licensor in writing. Failure to prosecute a party's rights will not constitute a waiver of any other breach. If any provision of this Agreement is found to be invalid, it will be enforced to the extent permissible and the remainder of this Agreement will remain in full effect. This Agreement has been written in the English language and you waive any rights you may have under the law of your country or province to have this Agreement written in any other language. InstallAnywhere EULA (012008).

Additional Licensing Information

Additional licensing information about other third party products included with Oracle Database 10g R1, which is distributed with Enterprise Manager can be found at:

http://download-west.oracle.com/docs/cd/B14117_01/server.101/b12255/license.htm#638238

Additional licensing information about other third party products included with Oracle Database 10g R2, which is distributed with Enterprise Manager can be found at:

http://web51-01.oracle.com/archive/html_ns/B14199_10/toc.htm

Additional licensing information about other third party products included with Oracle Application Server 10g R2, which is distributed with Enterprise Manager can be found at:

http://iasdocs/iasdl/101202fulldoc/index.htm

Glossary

Acknowledge

An option available to a notification recipient to approve and take responsibility for a pending notification.

Active Session

A currently logged in Person configured within the Configuration Change Console.

Agent

Installed on individual monitored devices, the agent collects change event data, such as information about specific files, processes or user accounts, as well as inventory information (CPU usage, memory capacity, etc.), and reports it to the Configuration Change Console server.

Agent Module

An actual module that is part of the agent that is responsible for a specific type of monitoring. For instance, file monitoring is done by a specific File Watch agent module.

Alerts

See Notifications

Application

A mapping of component instances that relates and should be named after your business applications; ie: the "Finance" application.

Asset Tag

Alpha-Numeric identification number physically associated with a hardware device, used for inventory purposes within your organization.

Audit Action

A configuration of what actions to take when certain events occur that are tied to a component or component instance.

Authorized Event

An event that has been reconciled with a Change Management server and a ticket has been found that indicates this change should happen. There are many factors that are considered during reconciliation.

Baseline

In terms of the dashboards, a baseline is a calculated expected value for the given time period based only on change rates. For instance, in the past month if you expect X changes per day, then the baseline for today's change count would be X.

Categorization

Hierarchical classification system used in change management servers. See also CTI. For Change management systems that have a two level hierarchy, the levels are typically called Category and Sub-Category.

Change Event

A file deletion, creation, modification, rename; A process start or stop; A user login or logoff; etc.

Component

A user defined blueprint of an important elements (both internal and external) that makes up an application used in the monitored environment. An an example, the Finance application may have a database component, an application server component, a firewall component, one or more patch components that define changes that will occur in a patch. A component can be very granular describing a single rule in an application, or can be very broad to cover many rules across every application.

Component Internal

Elements associated with a component's internal capabilities, for example Registry key values, database tables, LDAP configuration items, etc.

Control

A granular element of a policy definition for an industry standard such as COBIT, PCI, or ITIL.

CTI

A categorization specifically for the BMC Remedy Change Management Server. The category indicates the overall classification of a ticket, the type indicates the individual subset of the classification, and the item denotes the individual object. For example, you could have a CTI that listed the category, Software, the type Finance, and the item Application Server. See Categorization.

Database Purging

A feature that deletes historic captured data that has reached an expiration time.

Detected User

A user that has been detected by an agent over the course of monitoring. The user may have been detected because the user logged in or out of a device. The user could also be detected if a file change was made by the user.

Deviation Time

The difference in minutes between a time displayed on a managed device and the time displayed on the server if the two clocks are not synchronized. If a discrepancy exists, all generated notifications will factor the deviation time into the time stamp.

Device

A computer or server within your infrastructure. This can be a physical device or a single virtual operating system instance.

Device Group

An administrator defined grouping of devices with similar applications, operating systems, and/or purposes.

Emergency Ticket

A ticket that is created in a Change Management server that does not typically require all of the normal approvals because the IT operations staff is trying to solve a critical problem and there is no time to wait for approvals.

Environment

All People, users, devices in your organization and the associated rule sets and rules used for monitoring within the Configuration Change Console.

Escalate

In terms of pending notifications, an option available to a notification's recipient to forward the notification to the next person in the Escalation path.

Escalation

The forwarding path a notification follows when its recipient is unable to respond within a specific time frame. Notifications are usually forwarded to the next highest manager within the organizational hierarchy until a manager is reached that has no higher manager.

Event

A file deletion, creation, modification, rename; A process start or stop; A user login or logoff; a database table change, read, etc.

External Monitoring

The monitoring of files, processes, or users related to, but outside of an application. These could also be referred to OS monitoring.

File

In terms of the Configuration Change Console an individual file to be monitored for change events.

File System

In terms of the Configuration Change Console, information pertaining to storage capacity and available disk space for a specified device.

Filter

A region near the top of most screens that let you choose various options to limit the details shown in the window.

Framework

An industry standard compliance structure such as COBIT, PCI, ITIL. These frameworks define policies and controls to ensure your IT organization is adhering to the standard.

Hold

A probe module state where the probe collects and queues data but does not report it to the Configuration Change Console.

IMAP

Internet Message Access Protocol. Used in IMAP servers for receiving and storing emails.

Infrastructure

The managed devices within your organization which are monitored by the Configuration Change Console.

Instance

An instance of an object; The most common instance is the component instance. You can define a component then assign that component to more or one device. Each of these assignments results in a single component instance.

Internal Monitoring

The monitoring of elements intrinsic to the internal operation of an application, such as registry keys, database tables, or LDAP configuration items.

Login Name

The username used by a Person to log into the Configuration Change Console.

Managed Device

See Device

Manager

A person configured within the Configuration Change Console that is ranked above another within the organizational hierarchy.

MIB

A definition of the content of an SNMP message. For SNMP monitoring, a MIB can be imported into the server so that object IDs that are represented as a series of numbers can be converted to human readable descriptions of the events.

Module

See Agent Module

Notification

A message generated by the Configuration Change Console to alert an administrator of a change event, resource consumption threshold, user login/logoff, or error occurrence.

Notification History

A log of all notifications sent by the system.

Owning Team

The team responsible for a specific device or device group.

Override

An option within the Configuration Change Console to change an authorization status, or create an exception to a predefined time window.

Parent

A group that contains another group. For example a group named Computers that contained another group named Production would be the parent group. While

multiple groups can be assigned to a single parent group, each group can have only one parent.

Path

The complete directory tree location for a stored file, starting from the individual device drive and ending at the directory in which the file is stored. Applicable for file names and process names.

Pause

A probe module state where the probe does not collect or report data.

Pending

A notification status indicating the notification has not yet been sent.

People

The persons, roles, and teams that interact with the Configuration Change Console user interface.

Person

Someone who can log in and view data within the Configuration Change Console using their configured user name and password.

Peer

A person configured within the Configuration Change Console who shares the same rank as another person within the organizational hierarchy.

Planned Changes

For Change Management integration, a planned change is ticket that has its planned start or planned end time in the future. This means that the ticket is set up to define a change to happen in the future.

Policy

A policy is a structure that maps directly to an industry standard such as PCI, Cobit, ITIL. A policy has controls to ensure your IT organization is adhering to the standard.

POP3

Post Office Protocol 3. Used in a POP server for receiving and storing emails.

Predefined

A set of objects that come with the Configuration Change Console. You can save a copy of a predefined object to use it your configuration. Examples include components, frameworks, policies, components.

Primary Email Address

Main email address for a Person. The primary email address is used by the Configuration Change Console for notification purposes.

Priority Level

An indicator as to the importance of an event or notification defined in an Audit Action. For notifications, a notification can follow a more direct, or more roundabout escalation pattern depending on its priority.

Processes

A resource used by a running software application that performs a single task. The Configuration Change Console monitors processes to verify what programs are being run, and what changes are occurring while they are in use.

Purging

The deletion of information once it has reached a predefined expiration date. For example, Database Purging.

Reassign

In terms of Pending Notifications, an option available to a notification recipient to assign responsibility for a notification to another person within the organization.

Recipient

The person whom a notification is sent to.

Recurrence

The frequency at which an operation is applied.

Regular

A Person configured within the Configuration Change Console who can view all screens except for Configuration and Administration screens.

Remote Host

A machine used to connect to the Configuration Change Console server. In broader terms any machine used to access a central machine.

Rule

A single monitoring definition inside of a component rule set. For instance, specifying to monitor c:\windows\system32 would be a single rule.

Rule Set

A type of rules to add to a component for monitoring. Rule Sets are tied directly to the agent modules available on the given device. For instance, one rule set is the File Rule Set. You can add the File Rule Set to a component, then define rules for that Rule Set.

Run

In terms of reports, a report generation.

Role

A skill-set classification defined by an administrator and applied to a Person.

SMTP

Simple Mail Transfer Protocol. Used in SMTP servers to send outgoing email.

Snapshot Monitoring

A monitoring capability where events are detected by taking snapshots at set intervals and comparing the output from two successive snapshots.

SNMP

Simple Network Management Protocol. Used in SNMP servers for SNMP notifications. The Configuration Change Console can be configured to generate

notifications of change events through SNMP. The Agents can also monitor traps from any system that can send traps.

Super Administrator

A configured person within the Configuration Change Console suite who has access to all configuration and visualization screens, as well as additional advanced administrative screens.

Team

An administrator defined grouping of configured persons sharing similar responsibilities within the monitored environment.

Team Membership

An assignment of a Person to a Team. Team assignment is important for Team Device Limiting features.

Team Device Limiting

A option within the Configuration Change Console that allows an administrator to prevent users from viewing information for devices they are not assigned through their defined team membership.

Threshold

Used in the to define an percentage limit for items ranging from unauthorized events to database table space.

Time Scale

When reviewing change event data, the time period for the data set. The Configuration Change Console provides Yearly, Monthly, Weekly, Daily, Hourly, and 15 Minute, Last 7 days, Last 30 days Time scale options. Not all screens always have all scale options available.

Time Window

A defined time window for some activity.

Unaudited Event

An event that was not reconciled with a Change Management server because no audit action or category component assignment was configured.

Unauthorized Event

An event that was reconciled with a Change Management Server, but no open ticket was found indicating this change should have happened.

Update

The process of pushing a new monitoring configuration to one or more agents. If you change component definitions and many other configurations, you must perform an Update Agents action.

Upgrade

The process of upgrading the agent remotely from the server.

User

A user on a monitored device (OS user) or inside an application (Component Internal User). Users can be associated with a configured Person in the Configuration Change Console through person to user assignments.

User Activity

CPU usage of an individual user reported by the agent.

User Assignments

An association between a configured Person and a detected User.