

Oracle® Enterprise Manager
Configuration Change Console Quick Start Guide
10g Version 10.2.0.5
E16464-01

December 2009

Oracle Enterprise Manager Configuration Change Console Quick Start Guide, 10g Version 10.2.0.5

E16464-01

Copyright © 2003, 2009, Oracle and/or its affiliates. All rights reserved.

Primary Author: Dan Hynes

Contributing Author: Leo Cloutier

Contributor: Jerry Russell

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	v
Audience	v
Documentation Accessibility	v
Conventions	viii
1 Configuration Change Console Quick Start Guide	
1.1 Creating the CCC Repository	1-1
1.1.1 Create the Database	1-1
1.1.2 Create the Tablespaces	1-2
1.1.3 Create the Database User	1-2
1.1.4 Load the Database Objects	1-2
1.2 Installing the Server	1-3
1.3 Installing the Agent	1-3
1.4 Getting Started with Common Usage Scenarios	1-4
1.4.1 Creating a New Account	1-4
1.4.2 Creating a CCC Server Component for Change Monitoring	1-5
1.4.2.1 Add Component Type	1-5
1.4.2.2 Add a Custom Component	1-5
1.4.2.3 Add Component Rule Sets (File and Process Event Rule Sets)	1-5
1.4.3 Creating a CCC Agent Component for Change Monitoring	1-6
1.4.3.1 Add Component Type	1-6
1.4.3.2 Add a Custom Component	1-6
1.4.3.3 Add Component Rule Sets (File and Process Event Rule Sets)	1-6
1.4.4 Assigning Devices to Components	1-7
1.4.5 Updating the CCC Agent	1-8
1.4.6 Creating the CCC Application	1-8
1.4.7 Viewing Events by Application	1-8
1.4.8 Viewing Events by Server	1-8
1.4.9 Viewing Events by User	1-9
1.4.10 Enabling Change Auditing on Windows	1-9
1.4.10.1 Configure Change Management Server	1-9
1.4.10.2 Create Audit Action for CCC Application	1-10
1.4.11 Creating Custom Frameworks, Policies and Controls	1-10
1.4.12 Managing Change Compliance for Policies	1-11
1.5 Advanced Examples	1-11
1.5.1 How to monitor changes made by a specific user	1-11
1.5.2 How to monitor file changes in a file share environment	1-12



Preface

This guide describes the basic features and functionality of the Oracle Enterprise Manager Configuration Change Console. The book is meant to provide a rapid understanding of the features and capabilities of the product in a short period of time.

Audience

The overview describes a quick overview of the user interface components. It is applicable to all users of the Configuration Change Console.

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 timeout 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
```

Note: You must locate the server executable file that matches the platform on which you are installing Configuration Change Console. For example, the server executable for Microsoft Windows is *server-win32.exe* and for Linux it is *server-linux-x86-32bit.bin*.

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\activerreasoning.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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Configuration Change Console Quick Start Guide

Configuration Change Console (CCC) 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.

This guide will walk you through the installation and configuration of a test environment for the Configuration Change Console product. This guide is meant to give you a rapid understanding of the features and capabilities of the product in a short period of time.

1.1 Creating the CCC Repository

The first step of installation is creating a database for the Configuration Change Console repository. You can use an existing Oracle supported database installation by adding a new database or you can install the software on a new system. This guide assumes you already have a supported Oracle database installed in your environment.

See the *Configuration Change Console Installation Guide* for special issues regarding supported database configuration.

1.1.1 Create the Database

Start the Oracle Database Configuration Assistant and select the option to create a new database. Set the following for the new database you will create for this guide:

Table 1–1 Database Settings

Setting	Value
Type	General Purpose
SID	gateway
Character Set	Unicode (AL32UTF8)

You can use the default settings for all other settings, or set memory usage according to what is available on your server.

1.1.2 Create the Tablespaces

The Configuration Change Console requires three tablespaces be created in the new database. The following are the tablespaces and suggested size of each for evaluation purposes.

Table 1–2 Tablespaces

Tablespace	Size	Description
GATEWAY	1000 MB	Stores configuration data
GATEWAY_LGDATA	2000 MB	Stores raw collected data
GATEWAY_INDEX	4000 MB	Stores database indexes

You may create the tablespaces smaller and set them to auto resize to the above limits. Alternatively, if you know your evaluation will involve a lot of data, you may want to make the maximum size of these tablespaces larger.

If you do not want to create the tablespaces manually, there is a script available with the product. Locate the *oracle-install.zip* file that comes with the Configuration Change Console media. Unzip this file and locate the file *oracle-install\scripts\dbstructure\tablespaces.sql*.

You can modify this script and run it to create the tablespaces. Note that this script will not work without customization for your environment.

1.1.3 Create the Database User

Find the *oracle-install.zip* file that came with the Configuration Change Console media. Unzip this file into the *oracle-install* directory. Open a command prompt and change the directory to the following folder:

```
{ORACLE-INSTALL}/scripts/dbstructure
```

Follow these steps to log into the database as the sys user.

```
Prompt> sqlplus /nolog
SQL> connect sys@gateway as sysdba
Enter password: Enter the password used when creating the DB
```

Once connected, execute the following script and follow the prompts. Note that you need to enter values at each prompt; hitting return will not work. You can use the example values shown in each prompt for this step.

```
@users.sql
```

Ensure that you did not receive any errors during this script execution.

1.1.4 Load the Database Objects

Change your directory back to the *oracle-install* directory that you created in the previous step, then run the following batch file which will populate all database tables and will output the result to the *out.log* file.

```
DBCreateEE.bat gateway gateway gateway > out.log
```

The fields after the batch file are the user name, the password for gateway user in the database and the service name of the database to use.

Review the *out.log* file to make sure there are no errors at all. This is a very important step as it could break features later on in the evaluation of the product.

1.2 Installing the Server

Locate the *server.exe* that was part of the Configuration Change Console media. Double click on this icon to start the server installation.

Note: You must locate the server executable file that matches the platform on which you are installing Configuration Change Console. For example, the server executable for Microsoft Windows is *server-win32.exe* and for Linux it is *server-linux-x86-32bit.bin*.

1. Specify where you want to install the server software
2. Select Non-Clustered Installation (without cluster support) for the server type.
3. Provide the database IP, port and credentials provided during the database installation. If the installer cannot reach the database, the installation will not continue.
4. Enter a name for your organization, for example, *Corporate IT*.
5. Enter passphrases for the two keystore keys we use.
6. Provide a password to use for the Oracle WebLogic management console. The username will be *weblogic*.
7. Provide a password to use for the Configuration Change Console's default administrator account. This will be the password you need to log into the CCC UI.
8. Specify the ports that will be used both for browser based UI access as well as for the agents to talk to the server. Agents are configured to only use the HTTPS port, you can specify an HTTP and HTTPS port for the browser-based UI access.
9. Choose the option to start the server when the installation is finished.
10. Set your memory usage. Without using advanced memory configuration of the OS. The most memory you will be able to assign will be around 1400MB.

After you have gone through the installer and it has finished, it will either start automatically, or you can start the *Oracle Configuration Change Console Server* service in the Windows Services utility.

Once the service has started (may take a few minutes depending on load on your machine), you can log into the CCC UI at the following URL:

http(s)://<servername>:<port>/

1.3 Installing the Agent

Locate the agent installer that you want to install. For Windows, the agent installer will be called *agent-win.exe*. Double click on this icon to start the agent installation.

If you are installing from a command line, start the installation by typing:

```
Prompt> agent-win.exe -i console
```

You will then be guided through the following steps to install the agent.

1. Select the location where you want to install the agent software.
2. Enter the host server connection URL to the primary server. If the primary server is on a host called HOST1 and the HTTPS port is 443, then enter the following:

```
t3s://HOST1:443
```

3. To secure communications between the agent and server, you must authenticate with the server at installation time. To do this, enter a Configuration Change Console administrator user name (such as *administrator*) and the corresponding password.
4. You will be asked to set Audit Enabled on some platforms. If you have auditing enabled as specified in the installation guide (such as using BSM on Solaris), then choose **Yes**. If you do not, then file monitoring will not be in real time, but will be using the snapshot module.

It is always best to choose Yes unless you know that you will never use OS auditing for file changes on this agent.

After installation finishes, the agent may start automatically, or you can start it manually via one of the following options:

- On Windows, there is a new service called *Oracle Configuration Change Console Agent*.
- On Unix, a new daemon will be added under */etc/init.d*. To start this daemon, type the following at the command prompt:

```
cd /etc/init.d/  
./arprobe start
```

After the agent starts, you can verify that it is communicating properly with the server by logging into the server UI and going to *Administration > Devices > Devices* and looking for an entry in the list of registered devices for this machine that the agent is installed on.

1.4 Getting Started with Common Usage Scenarios

This section outlines some of the basic usage scenarios of the Configuration Change Console. The walk throughs here are meant to help you learn how to develop your own configurations and use the product for your own environment.

1.4.1 Creating a New Account

New accounts in Configuration Change Console can be created by using the *Add or Update a Person* page. An individual who can log in to CCC is called a *person*. Note that CCC also has the concept of a 'user', which refers to an actual account on a managed device. A person may or may not be associated to certain user(s).

1. Navigate to *Administrator -> People -> People*.
2. Select **Add Person**.
3. Enter all required fields, such as Login Name, First Name, Last Name, Password, Password (verify), Email Address, and so on
4. Optionally configure preference settings for the new account, such as Organization and Product Settings
5. Click **Save** when finished.

Make sure that each account is associated to an existing Team by using the checkboxes in Teams section under Organization Settings, in the *Add or Update a Person* screen.

1.4.2 Creating a CCC Server Component for Change Monitoring

The first step of change monitoring and auditing is to configure the components and applications. In this guide we use CCC server component as an example, you can create the components that match the change monitoring requirements in your specific environment.

1.4.2.1 Add Component Type

1. Navigate to *Policy -> Operations Management -> Components*.
2. Select **Custom Components** from the View filter.
3. Click the **Add Component Type** link to the right of Component Type filter.
4. Click **Add Component Type** to add the type for CCC server component.
5. Enter Application Server as the Component Type Name. Optionally enter a description.
6. Save the component type and click **Done** on the component types page.

1.4.2.2 Add a Custom Component

1. Click **Add Custom Component** on the Component page.
2. Enter the following values:
 - Component Type: Application Server
 - OS: WINNT
 - Name: CCC Server
 - Version: 1.0
 - Enter an optional description
3. Save and verify that *CCC Server* is displayed in the component list.

1.4.2.3 Add Component Rule Sets (File and Process Event Rule Sets)

1. Click the Rule Sets link **(0)** on the CCC Server row.
2. Click **Go** to add File Event rule set.
3. Click the **Edit Rules** link on File Rule Set header.
4. Provide the following:
 - Files: *<CCC server install directory>\deploy*
 - Pattern Type: write
 - Description: Include main CCC server directory
 - Version: 1.0
 - Enter an optional description
5. Click **Save** when finished.
6. Click **Add Instance**, then select the **Exclude** radio button.
7. Provide the following:
 - Files: *<CCC server install directory>deploy\activereasoning.ear\gateway.war\temp*
 - Description: Exclude temp director

8. Click **Go** to add the Process Event rule set.
9. Click the **Edit Rules** link in the Process Rule Set header.
10. Provide the following:
 - Include processes: arocc.exe
 - Pattern Type: event
 - Description: Include main CCC server process
11. Click **Save** when finished.

If you only want to monitor file and process changes made by specific users, Add a User Event Rule Set, and include those users, and check **Filter change data by Users defined in Component** check box in the File and Process Event rule sets.

After returning to *Add or Update Component Rule Sets* page, clicking **Done** should complete the configuration of the 'EMCCC Server' component rule sets.

1.4.3 Creating a CCC Agent Component for Change Monitoring

The first step of change monitoring and auditing is to configure the components and applications. In this guide we use CCC server component as an example. You can create the components that match the change monitoring requirements in your specific environment.

1.4.3.1 Add Component Type

1. Navigate to *Policy -> Operations Management -> Components*.
2. Select **Custom Components** from the View filter on the top.
3. Click the **Add Component Type** link to the right of Component Type filter.
4. Click **Add Component Type** to add the type for CCC agent component.
5. Enter Agent as the Component Type Name. Optionally enter a description.
6. Save the component type, then click **Done** on the Component Types page.

1.4.3.2 Add a Custom Component

1. Click **Add Custom Component** on the Component page.
2. Provide the following:
 - Component Type: Agent
 - OS: WINNT
 - Name: CCC Agent
 - Version: 1.0
 - Enter an optional description
3. Save and verify that *CCC Agent* is displayed in component list.

1.4.3.3 Add Component Rule Sets (File and Process Event Rule Sets)

1. Click the **Rule Sets link** (0) on the CCC Agent row.
2. Click **Go** to add the File Event rule set.
3. Click the **Edit Rules** link on File Rule Set header

4. Enter the following values:
 - Files: <CCC agent install directory>\bin
 - Pattern Type: write
 - Description as 'Include main CCC server directory'.

Note the Include radio button is selected by default.
5. Click **Add Instance**.
6. Click **Save** when finished.
7. Click **Go** to add the Process Event rule set.
8. Click the **Edit Rules** link on the Process Rule Set header.
9. Enter the following values:
 - Include Processes:
 - Pattern Type: event
 - Description as 'Include main CCC server process'.
10. Click **Save** when finished
11. Click the Edit Rules link on the Process Rule Set header
12. Enter the following values:
 - Include Processes: arocc.exe
 - Pattern Type: event
 - Description as 'Include main CCC server process'.
13. Click **Save** when finished.

If you only want to monitor file and process changes made by specific users, Add a User Event Rule Set, and include those users, and check 'Filter change data by Users defined in Component' check box in the File and Process Event rule sets.

After returning to *Add or Update Component Rule Sets* page, click **Done**. This should complete the configuration of the 'EMCCC Server' component rule sets.

1.4.4 Assigning Devices to Components

After components are created, the devices that need to be monitored should be assigned to the components. The components that have devices assigned to them are called Component Instances.

1. On the Components page, click the **Component Instances** link within the CCC Server row.
2. Click **Modify Device Assingment**.
3. Expand **Device Groups** and select the host the CCC server is running on.
4. Click **Save**, then **Done**.

Repeat these steps for the CCC Agent.

1.4.5 Updating the CCC Agent

After Components are created and devices are assigned to them, the component definitions need to be propagated to the monitoring agents running on the component instance devices.

1. Click **Update Agents**.
2. Select the devices that are assigned to the components.
3. Click either **Update Selected** or **Update All** to update all agents in the console.

1.4.6 Creating the CCC Application

If your application is made up of more than one component, you must create a new application that includes all components. You will create 'CCC Application' as an example.

1. Navigate to *Policy -> Operations Management -> Applications*.
2. Click **Add Application**.
3. Enter CCC Application as the Application Name. Optionally enter a description.
4. Click **Save**.
5. Click the **# of Component Instances** link on the CCC Application row.
6. Click on **Modify Component Instance Assignments**.
7. Expand the check boxes and select **CCC Server 1.0 WINNT** and **CCC Agent 1.0 WINNT**.
8. Click **Save**. Verify that the # of Component Instances value is updated to "2" for CCC Application.

1.4.7 Viewing Events by Application

Once an application has been created, you can view events happening within it.

1. Navigate to *Visualization -> Event Visualization -> Application Events*.
2. Select the **CCC Application** checkbox. The *CCC Server 1.0 WINNT on device ...* and *CCC Agent 1.0 WINNT on device ...* options are also selected.
3. Click **Generate Report**.
4. Drill down to the *CCC Application* link.
5. Click the **Device** links to see changes on the components CCC Server on WINNT and CCC Agent on WINNT components.
6. Drill down to the **File** or **Process** links to view event details such as Timestamp, File/Process names, Event (created, deleted, or modified for files), etc.

Note that you can filter event data even further by select start date/time, and scale (by Month, Day, Hour etc)

1.4.8 Viewing Events by Server

You can also view events occurring on a specific monitored device.

1. Navigate to *Visualization -> Event Visualization -> Server Events*.
2. Expand all device groups and select the **CCC Server** and **CCC Agent** host devices.

3. Click **Generate Report**.
4. Drill down to the device name link.
5. Drill down to File or Process links to view event details such as Timestamp, File/Process names, event (created, deleted, or modified for files) etc.

Note that you can filter event data even further by select start date/time, and scale (by Month, Day, Hour etc)

1.4.9 Viewing Events by User

You can also view events initiated by a specific user.

1. Navigate to *Visualization -> Event Visualization -> User Events*.
2. Select **Operating System Users** from the User Type drop list.
3. Enter a user name or * for all users in the in the Search for user by name starts with field.
4. Click the user account you want to view.
5. Click the name of the monitored device where the user account exists.
6. Browse to see user events that are one of following types: Login/Logout; Process Activity (process events initiated by the user); File Activity (file events initiated by the user); and CPU Usage % (CPU resource consumed by the user processes).

1.4.10 Enabling Change Auditing on Windows

Change events detected by the Configuration Change Console can be audited through Change Management system such as Remedy. Unauthorized changes are captured and compliance can be measured directly based on the policies and controls defined for the monitored environment.

The following steps use Remedy ARS 6.3.0 as an example.

1.4.10.1 Configure Change Management Server

1. Navigate to *Administration -> Server Configuration -> Change Management Server*.
2. Pick **Remedy ARS 6.3.0 WINNT** as Ticket Management Type.
3. Enter the host (device) name the Ticket Server is running on.
4. Enter the following connection parameters:
 - Server IP: the IP address ticket server running on
 - Username/Password: the account that CCC should use to connect to CM server
 - Consolidate CTI: CT+D, so that tickets are consolidated by category and device
5. Check all check-boxes for Enter Ticket Correlation Criteria. This ensures that the change events are correlated with the time window, device(s), user, and approval timeout (status for emergency ticket) of the tickets.
6. Select the following for Configure Outbound Ticket:
Unauthorized/Unauthorized/Unauthorized for Category, Type and Item.
7. Enter Supervisor and Group names that the ticket should be assigned to in the Change Management Server.

8. Configure Ticket Expiry and Emergency Ticket similarly, but change Item to Expiry and Emergency.
9. Click **Save** when finished.

The Change Management Server is only configured once after installation. You can export the configuration and reuse it by importing to another Configuration Change Console if needed.

1.4.10.2 Create Audit Action for CCC Application

1. Navigate to *Policy -> Policy Management -> Audit Actions*.
2. Click **Add New Audit Action**.
3. Enter **CCC Application Audit Action** as the Audit Action Name.
4. Click the **Application** radio button in Component Assignment, then select CCC Application.
5. Check the **File, Process, User** and **Component Internal** check boxes in the Events to Detect section.
6. Check the **Update Ticket** and **Create Ticket** check boxes in the Actions section.
7. Click **Save** when finished.

At this point, the CCC Application has been configured so that all events detected within CCC Server and CCC Agent component instances will be audited by correlating events with tickets in Remedy. All changes events on the device where CCC Server and Agent are running will cause an Unauthorized event to be created in CM server, and corresponding administrator will be assigned.

Once change events are detected by the Configuration Change Console, it can also send email notifications, or generate reports and send those to administrators.

To do this, in Audit Action configuration, configure CCC using Email Administration, and select *Send Notification and Generate Report* and *Send* accordingly on *Audit Action* configuration page.

1.4.11 Creating Custom Frameworks, Policies and Controls

Configuration Change Console allows you to manage and audit configuration changes in the context of frameworks, policies and controls. Policy compliance can be easily managed and controlled by monitoring what changes are happening and whether they are authorized changes or not.

You can create custom frameworks and policies that are made up of specific controls that are mapped with application components. CCC also provides a set of predefined frameworks, policies, and controls that serve as starting points to create custom policies.

1. Navigate to *Policy -> Policy Management -> Frameworks*
2. Select **Create Custom Framework**.
3. Enter **Application Change Management FW** as the Framework Name.
4. Click **Save**.
5. Navigate to *Policy -> Policy Management -> Policies*
6. Click **Create Custom Policy**.
7. Enter **Application Change Management** as the Policy Name.

8. Select **Application Change Management FW** as the framework.
9. Enter **Critical changes to application should be monitored** as the description.
10. Optionally enter values for policy text, Reference URL, and Owner, then **Save**.
11. Verify Application Change Management is in the Custom Policies list.
12. Click on '0' under the Control column for Application Change Management, then click **Modify Control Assignment**.
13. Select the **Application Change** and **Application Availability** check boxes.
14. Click **Save** when finished.
15. You now need to map application components with the appropriate policies so that policy compliance can be associated with change events. Select *Policy -> Operations Management -> Components*.
16. In the CCC Agent and CCC Server component rows, click on the 0 link under the Controls column.
17. Expand **Frameworks** and select **Application Change Management** policy for both components. You should now see '2' under Controls for both components.

1.4.12 Managing Change Compliance for Policies

Once you have defined your environment using components and applications, and created policies and controls, you can now easily manage policy compliances.

The compliance status of each policy in the framework is displayed in the Dashboard. If a change management system is used, the percentage of unauthorized events is used to measure compliance. If no change management system is used, the deviation of change events from baseline is used to measure compliance.

Now drill down to each policy. You will see a detailed view of how many changes were captured, and what controls and applications are affected. You will also see the users who made the changes, and devices on which these changes occurred.

1.5 Advanced Examples

The following are advanced example use cases.

1.5.1 How to monitor changes made by a specific user

Configuration Change Console allows you to monitor changes that were made by a specific user.

1. Add a User Rule Set in the same component that has the file event rule set.
2. Include 'X' as Patterns and 'user' as Pattern Type.
3. Select the **User for filtering other types only, not for inclusion/exclusion of user login/logout events** checkbox to filter event changes by user.

Note that login/logout events for the users will not be detected if this option is selected. If you want to capture these events, do not select this option.

4. Click **Save**.
5. Click **Edit Rules** in the File Rule Set header.
6. Select the **Filter change data by Users defined in the Component** checkbox.

1.5.2 How to monitor file changes in a file share environment

In a shared file system environment, file change monitoring can be done depending on the way file system is shared.

- Mounting a share from another host

Install an agent on the source machine. This will be real-time monitoring of file changes on the source machine. This is no different from normal file change monitoring on non-fileshare systems.

- Mounting NFS share/NAS/Network Storage

Switch agent to 'snapshot' agent and monitor one machine where the share is mounted. This only works on Unix, and some event details such as users who made the changes will not be provided. This needs to be done manually post installation.

As an example, assume that one Windows XP folder X:/ is shared to a Linux host L. In order to monitor file changes in X:/ use following steps:

1. Install the Linux agent on host L as documented in the Installation Guide.
2. Change the symbolic link for *{agent_install_dir}\bin\filwatch* from *{agent_install_dir}\bin\filewatcha* to *{agent_install_dir}\bin\filewatchp*.

Alternatively, you can rename *filewatch* to *filewatch.renamed*, and then rename *filewatchp* to *filewatch*.

3. Restart the agent.

Once this is done, you can configure components on the server the same way you did as before, but now file monitoring on this agent will be done using the snapshot method instead of the real time method.