CA Identity Governance

Release Notes

12.6.02a

ca technologies

CA Technologies Product References

- This document references the following CA Technologies products:
- CA Identity Governance
- CA Identity Manager
- CA Single Sign On
- CA User Activity Reporting
- CA SDM
- CA IAM Connector Server

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Welcome

Welcome to CA Identity Governance 12.6.02a. This guide describes new platform certification, installation and general considerations, published solutions, and known issues for the product.

Chapter 2: New and Changed Features

This section contains the following topics:

Product Rebrand

The product has been rebranded as CA Identity Governance.

New Platform Certification

The following new platform is certified with CA Identity Governance 12.6.02a:

Application Server

- IBM WebSphere Application Server V8.5.5.0

Chapter 3: Install and Upgrade Considerations

This section contains the following topics:

Supported Installation Languages

When you install CA Identity Governance, you can specify the language in which the product is installed and displayed. The following are the supported languages that you can specify:

- Danish
- English
- Finnish
- French
- German
- Italian
- Japanese
- Korean
- Norwegian
- Portuguese (Brazilian)
- Spanish
- Swedish

JBoss EAP 6 Installation Script

If you want to deploy the product on a standalone JBoss Enterprise Application Platform 6 server, an installation script is provided. The JBoss EAP 6 installation script can be found in the following location in the core ZIP file:

`CA-RCM-12.6.`*`X`*`-Core.zip\CA-RCM-12.6.`*`X`*`-Core\Utils&Conf\Jboss6EAP`

View the readme file included with the script for instructions.

Prevent Deadlocks After Upgrading a Microsoft SQL Environment

When upgrading from CA Identity Governance 12.5 SP7 or an earlier release and using a Microsoft SQL database, if you make many updates at once, deadlock exceptions can occur. To improve performance while making many updates, run the following query on the SQL database while the CA Identity Governance server is down:

```
ALTER DATABASE eurekify_sdb
                SET READ_COMMITTED_SNAPSHOT ON;
GO
ALTER DATABASE eurekify_sdb
                SET ALLOW_SNAPSHOT_ISOLATION ON;
GO
```

When running the script on an existing database, it can take a very long time. If possible, we recommend the following procedure:

1. Stop the CA Identity Governance server.
2. Restart the Microsoft SQL service.
3. Run the query above.
4. Start the CA Identity Governance server.

Note: This query is done during installation for CA Identity Governance 12.6 and later.

Use Current JCS Password When Upgrading

If you have a Java Connector Server (JCS) installed in your current environment and you upgrade to this release, provide the same password for the new CA IAM Connector Server during installation as your current JCS password.

If you provide a different password during installation, update the existing JCS connectors with that password before you run them.

Upgrading CA Identity Governance on JBoss 4.2.2

The CA Identity Governance installer currently installs on JBoss 5.1.0.

During a CA Identity Governance upgrade running on a JBoss 4.2.2, the CA Identity Governance installer upgrades the application server to JBoss 5.1.0.

During this process, when the previous JBoss version is located, it is renamed to eurikify_jboss_backup.

As a result of the CA Identity Governance installer upgrade, all JBoss customizations must be reapplied for the JBoss 5.1.0 configuration.

For example:

- Web.xml — Manual editing of the web.xml file (to work with JMS, and so on) must be reapplied for the JBoss 5.1.0 folder.
- Server.xml file — The JBoss port number located in the server.xml file must be reapplied if different from the default port setting.

Note: We recommend that you create a backup JBoss configuration file for reference.

CA Identity Governance with IPv6

Internet Protocol version 6 (IPv6) is a new version of the Internet Protocol that supports 128-bit addresses.

Not all components of CA Identity Governance accept the extended IP addresses specified by IPv6. To implement CA Identity Governance in an environment that uses IPv6 addresses, use host names instead of explicit IP addresses.

Servers can be mapped to host names in the following two ways:

- On the DNS in the operating environment
- In the hosts file on each CA Identity Governance system

Chapter 4: General Considerations

This section contains the following topics:

Default Email Logo Update

The default email logo is updated to "GovernanceMinder".

PDI Performance Issue

Under certain circumstances, PDI experiences an infinite data loop.

CSV Import Failures

Sometimes, log warnings indicate that the maximum number of thread thresholds is high when there is no IM integration. This is normal activity, CA Identity Governance creates threads for all universes, and you can introduce optimization steps to reduce the number of threads for a universe that does not require continuous updates.

FIPS 256 Bit Key

To use CA Identity Governance FIPS algorithm with 256 bit size hard coded key (128 bit size is default setting), you must:

- Add a common property, **fips.key.size**, and set the **Property Value** to 256.
- Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 from the Oracle site http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html, and replace two JRE jar files according to the readme file instructions located in the downloaded zip.

Oracle Error Message

When a customer installs CA Identity Governance with Oracle RAC with OID (Oracle Internet Directory), an ORA-28030 troubleshoot error is a successful response.

Chapter 5: Known Issues

This section describes known functional or performance issues for this release.

This section contains the following topics:

Combined Multiple Attributes not Supported in BPRs Based on User Attribute Value

Symptom:

When I create a BPR using the User Attribute Value type with multiple attributes in the rule definition, the restrictions are only applied on “Any” of the attributes. If I select “All” restrictions, the rule produces incorrect results.

Solution:

To combine multiple attributes in a BPR, define several rules for each attribute. Within each rule, define one attribute with the restriction "Any".

Report Localization Issue

The **Certified Resources with Violations Highlighted** report is not fully translated for these languages: French, German, and Japanese.

Reports Data Access Driver Setting

Symptom:

When I use an Oracle database, the policy violation report displays an ‘illegal character’ error.

Solution:

For an Oracle database, when you define a new connection in the BusinessObjects XI 3.1 SP6 (CABI 3.3 SP1) Designer, set the Data Access driver to **JDBC Drivers**.

Check Boxes Cleared During a Certification

As an approver, sometimes you select and approve a certification task with comments. When you have to add comments to continue the certification, the previously selected tasks do not remain selected.

Purge Tasks Uses Large Amounts of Memory

When you purge certifications from a universe, or a universe with certifications from a system that uses Microsoft SQL Server, allow for an increased amount of time and disk space.

Pop Up Windows Open In Incorrect Location

Symptom:

When I click an entry in the certifications window the pop up window opens at the top left corner of the window.

Solution:

The issue occurs when the following properties are specified as follows:

```
tooltip.balloons.mouse.enabled = false
tooltip.balloons.onfocus.show.enabled = true
```

Set the tooltip.balloons.mouse.enabled property to true to workaround this issue.

Ignore Non Imported Failed Endpoints

Symptom:

When I import endpoints, offline endpoints without last known successful configurations cause the import process to fail.

Solution:

Modify an existing import process to ignore failed endpoints.

In the Workpoint Designer, alter the import process flow by creating a step that ignores failed endpoints. In the Portal, you associate the modified import process for endpoints.

Follow these steps:

1. In the Workpoint Designer, rename and modify a process.
    a. Go to Start, Programs, CA, Role & Compliance Manager, Server, Workpoint Designer.
    b. Navigate to File, Open, Open Processes.

       The Open Process tab displays.

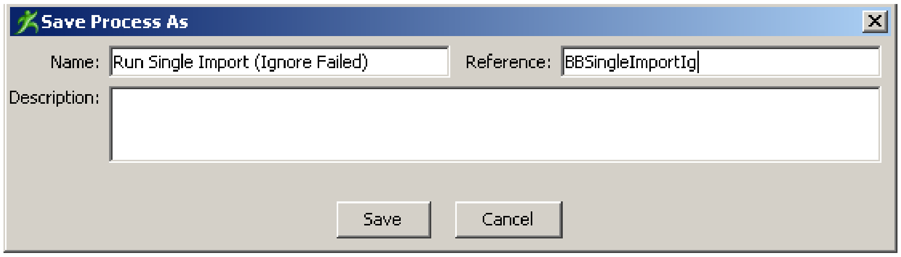
c. Locate and double-click the Run Single Import process (ID 46:WPDS).

   The 46:WPDS (BBSingleImport) Run Single Import process appears.

d. Save the process with a new name and reference name.

   Example:

   Run Single Import (Ignore Failed), BBSingleImportIg



Save Process As

Name: Run Single Import (Ignore Failed)

Reference: BBSingleImportIg

Description:

2. Duplicate the Run Connector? default building block (BB) and modify the Properties.

   a. Copy paste the Run Connector? BB.

   b. Right click the BB, select Properties, and in the Activity Properties (Process) window, select the General tab.

   c. In the Name field, rename the BB as Ignore Failed Connector, and click OK.

   d. Right click the BB, select Properties and in the Activity Properties (Process) window, select the User Data tab.

   e. In the Name field add the user data name as isRCMJobParameter, and in the Value field add the value as flow.import.boolean.ignoreFailedConnectors.

   f. Click Add, and OK.

      The user data is saved.

   g. Right click the BB, select Properties and in the Activity Properties (Process) window, select the RCM Parameters tab.

   h. Click Add.

      The New RCM Property window appears.

   i. Enter flow.import.boolean.ignoreFailedConnectors in the Property Name field, and click OK.

      The property is listed in the RCM Parameters tab.

   j. Set the value as false, click Apply and OK.

      The process window displays.

      You have duplicated and renamed the BB, and modified properties.

3. Add the BB to the process.

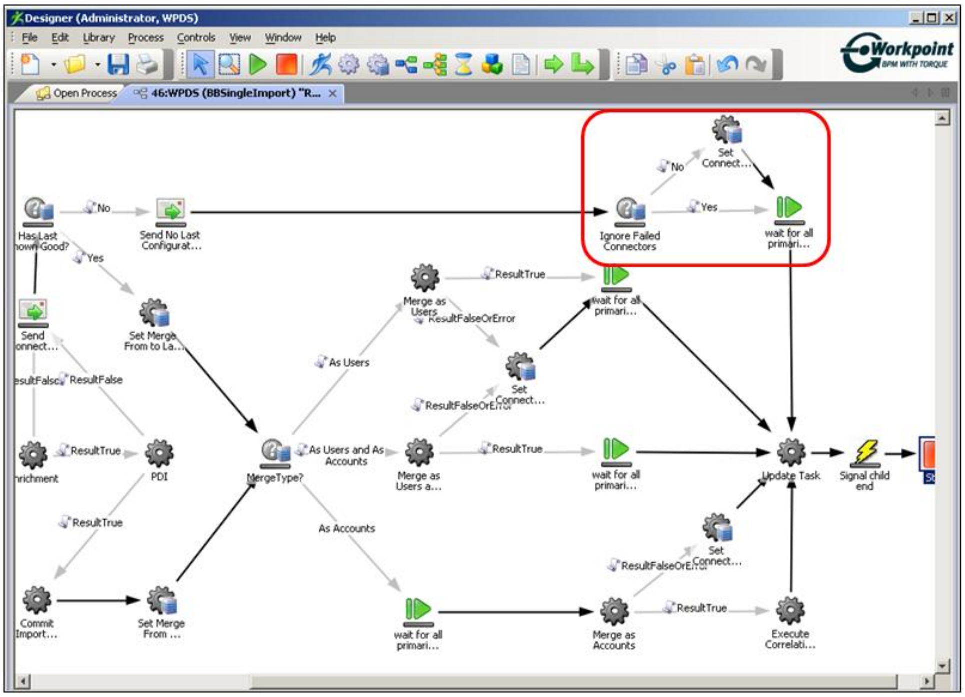
   a. Drag and drop the Ignore Failed Connector BB between the Send No Last Configuration Email and Set Connector Failed 3 BBs.

   b. Set the transition between Ignore Failed Connector and Set Connector Failed 3 steps as Conditional, select the Use an existing script option and in the Name field select No and click Finish.

   c. Set the transition between Ignore Failed Connector and wait for all primaries ended 4 as Conditional, select the Use an existing script option and in the Name field select Yes and click Finish.

   d. Save the process.

      You have added a BB and modified the process.



4. In the Portal, add a Process Mappings.

   a. In the Portal, navigate to Administration, Workflow Settings, Workflow Process Mapping, and add a Process Mappings.

   b. In the Add Process Mappings section, add a name, and description.

   c. In the Workflow Type section, select Import from the drop-down list.

   d. Click Add.

      The New Process Mapping screen appears.

   e. In the Import section, select BBSingleImport from the drop down menu and click Add.

5. Navigate to Administration, Universes, select a universe, and in the Default Process Mappings tab, in the Import section, set the mapping to the Process Mapping from Step 4, and click Save.
6. Select the universe and in the Connectivity tab, and in the Import Flow Properties area, select flow.import.boolean.ignoreFailedConnectors.
7. Run the import for endpoints.

   Nonimported failed endpoints are ignored.

Export Fails when Removing a Nested Provisioning Role in CA Identity Manager

When you integrate CA Identity Governance with CA Identity Manager, and you try to remove a child provisioning role from a parent provisioning role in CA Identity Governance, the export to CA Identity Manager fails.

Note: This issue is resolved in CA Identity Manager 12.6.1.

Data Warehouse Issues when using Two Universes

Symptom:

When I have different business policy rules (BPRs) in two separate universes, and the ETL process for both universes is running at the same time, the data in the database may be switched between universes.

Solution:

To work around this issue, run separate ETL processes for each universe at different times.

Entitlement Quality Report Performance Issues

Performance issues occur when running the Entitlement Quality report with a Microsoft SQL database. The report may take more than an hour to run.

Some Text in Reports Not Localized

Symptom:

Some text in the default reports appears in English when viewing the reports in other languages.

Solution:

Customize the reports and edit the text that appears in English.

Issue with Saving Reports in InfoView

Symptom:

When I log in to InfoView by going to Reports, Manage Reports, and I try to save a report, the system does not allow me to save.

Solution:

To work around this issue, start a new browser session before going to Manage Reports and logging in to InfoView.

Connection Errors After Identity Minder Server Upgrade

Symptom:

Connect error when accessing CA Identity Governance from CA Identity Manager after upgrade of an existing installation.

Solution:

After CA Identity Manager server upgrade more configuration is required.

Follow these steps:

1. In the CA Identity Manager User Console, go to System, Web Services, Delete Web Services Configuration, Search.
2. Delete the IMRCM configuration.
3. Log in to the CA Identity Governance web portal.
4. Go to Administration, Universes and select the universe configured to integrate with CA Identity Manager.
5. Go to Connectivity tab and select the CA Identity Manager connector.
6. Click Test and confirm that the connection is successful.

Disabling IPv4 on Windows 2008

If you remove the IPv4 stack from Windows 2008 by using "netsh interface ipv4 uninstall", the CA Identity Governance installer fails to connect to the database.

Workaround

Disable IPv4 by clearing the IPv4 layer check box in the network properties page (Internet Protocol Version 4 (TCP/IPv4).

BPR Fails When Assigning Roles During Violation Check

Symptom:

When I assign roles to a user while a Business Policy Rule (BPR) is running and checking for violations, the initial run is successful. When I repeat this action a second time, an exception occurs in the application server console, and no violation is returned.

Solution:

Clear the Portal browser cache before running the next BPR.

Client Tools Connector Configuration Files Removed During Upgrade

Symptom:

After I upgrade CA Identity Governance and run the migrated connector, the connector does not point to the specific endpoint and generates a log error.

Solution:

During the upgrade process, when you uninstall the Client Tools, you remove the connector configuration files. Before you start the CA Identity Governance upgrade process, backup the connector configuration files. After the upgrade is complete, reapply the backed-up connector configuration files.

The default connector configuration files are located in the following folder:

```
RCM_install\Program Files\CA\RCM\Client Tools\Software\Converters\CA\conf
```

Internet Explorer 7: Zoom Level Can Affect User Interface Component Appearance

When using Internet Explorer 7 browser, and zooming greater than 100 percent zoom level, CA Identity Governance UI components can appear distorted but are fully functional.

Degraded Performance on a JBoss Cluster

Symptom:

After an extended period of time, degraded user interface performance and high CPU usage results when using CA Identity Governance configured on a JBoss cluster.

Solution:

Edit the vfs.xml file on one JBoss node.

Follow these steps:

1. Stop all JBoss nodes.
2. Delete the tmp, temp, and work folders in the following location on all nodes:
   `JBoss Cluster Home\server\all`
3. Locate the vfs.xml file in the following folder:
   `JBoss_cluster\server\all\conf\bootstrap`
4. In the last entry under the map tag, add the following lines:

   ```
   <entry>
     <key>${jboss.server.home.url}farm</key>
     <value><inject bean="VfsNamesExceptionHandler"/></value>
   </entry>
   ```
5. Save the vfs.xml file and copy it to all other nodes in the cluster.
6. Restart all JBoss nodes.

Change Default Hostname on Linux Cluster

Symptom:

I am trying to deploy CA Identity Governance on a JBoss cluster on Linux and the cluster is not working.

Solution:

The Linux installer adds the hostname to the /etc/hosts file pointing to the localhost address (127.0.0.1) by default. Modify the /etc/hosts file and remove the hostname from the localhost address.

For example,

```
127.0.0.1            RCM-Server localhost.localdomain localhost
```

changes to:

```
127.0.0.1            localhost.localdomain localhost
```

Some Endpoint Data not Synchronized after CA Identity Governance Export

In some cases, when removing links between non-user entities in CA Identity Governance (such as between nested roles or a role and a resource), the change is exported to CA Identity Manager, but CA Identity Manager does not synchronize those changes with the endpoint. Therefore, CA Identity Governance thinks that some user privileges have been removed, but in CA Identity Manager, these user privileges still exist.

Workaround

In CA Identity Manager, manually synchronize the endpoint after completing an export from CA Identity Governance.

Accessing a New Role

Because approval of a new role is a manual process dependent on the approvers, it may take time for the new role to be added to the configuration. If you try to access a newly added role before it is approved and added to the configuration, you get an Entity not found error.

Renaming a Role that Represents a Provisioning Role is not Supported

In CA Identity Governance Client Tools, there are places where you can rename a role. However, exporting a rename operation to CA Identity Manager does not work, and renaming of a provisioning role is not supported.

Continuous Updates Not Supported for Explore and Correlate

Continuous Updates from CA Identity Manager to CA Identity Governance for the Explore and Correlation functionality is *not* supported.

If you Explore and Correlate an endpoint, do an import after the Explore and Correlate completes to add the new or updated endpoint data to CA Identity Governance.

Filtering Limitation When Importing from CA Identity Manager

When importing from CA Identity Manager, CA Identity Governance does not support filtering users by organization or retrieving user organization membership information from an LDAP user store.

(Optional) Increase File Handles

In Unix, increase CA User Activity Reporting default number server file handles when integrating with the product. The default file handles limit the opening of too many files that can exhaust system resources. The CA User Activity Reporting server is only supported on Linux.

Follow these steps:

1. On the CA User Activity Reporting server, navigate to the following location:

   /etc/security/

2. Edit the limits.conf file. Look for the following caelmservice settings:

   - caelmservice   soft   nofile   4096
   - caelmservice   hard   nofile   4096

3. Change both caelmservice settings to 8192.

   You have increased file handles on the CA User Activity Reporting server.

Using Secured Active Directory as a User Store for CA Identity Manager Requires a Certificate in CA Identity Governance

Symptom:

When integrating CA Identity Governance with CA Identity Manager using Active Directory (with SSL enabled) as a user store, the import feature fails.

Solution:

To work around this issue, do the following:

1. Configure CA Identity Governance for SSL.

   Note: For more information about configuring CA Identity Governance with SSL, see the **Installation Guide**.

2. If your certificate is not published by CA (Certificate Authority), perform the following steps:

   a. Import a certificate into a keystore in the default JDK JRE security directory.

   b. Reference the keystore in either the batchImport.properties file or the eurekify.bat file by adding JRE arguments, such as the following:

   ```
   -Djavax.net.ssl.keyStore="C:/Program
   Files/Java/jdk1.6.0_21/jre/lib/security/storename"
   -Djavax.net.ssl.keyStorePassword=changeit -
   Djavax.net.ssl.trustStore="C:/Program
   Files/Java/jdk1.6.0_21/jre/lib/security/storename"
   ```

Multi-valued Attribute Changes not Supported in Export

Multi-valued attribute changes made in CA Identity Governance cannot be exported to CA Identity Manager. Multi-valued attributes are supported in import, but not in export.

Unsupported Characters in Role Names that Correspond to CA Identity Manager Roles or Account Templates

When integrating CA Identity Governance and CA Identity Manager, CA Identity Governance role names for roles that correspond to provisioning roles or account templates in CA Identity Manager cannot contain the following characters:

- asterisk (*)
- comma (,)
- semicolon (;)

- forward slash (/)
- backslash (\)

Error When Opening a BPR File From the Audit Card

Symptom:

I receive the following error message when I try to open a BPR file (created in the portal) by right clicking on an alert and selecting the View or Edit BPR rule options:

```
The File is Not a Valid Business Policy Rules File
```

Solution:

Open the BPR file using the File, Open menu options.

Internet Explorer 8.0: Default Security Options May Affect Display

Symptom:

The default security settings in Internet Explorer 8.0 browsers may cause issues with search screens that are displayed as pop-up windows in CA Identity Governance.

Solution:

1. Open Tools, Internet Options from an Internet Explorer 8.0 browser.
2. Select the Security tab.
3. Select the Local Internet, then select Custom Level.

   A Settings window opens.
4. Select Enable under Scripting, Active Scripting.
5. Click OK.
6. Restart the browser for changes to take effect.

   You can view pop-up search screens correctly.

Mozilla Firefox 17: Truncated Tooltips

When using a Mozilla Firefox 17 browser, CA Identity Governance tooltip screen titles that contain more than 80 characters and no spaces appear truncated and unwrapped.

Wrong Error Code When SBT File Fails to Run

Symptom:

When my SBT file fails to run, the error level returned is zero.

Solution:

Run the SBT file with a /w flag, for example, use the following format:

```
start batch_file.sbt /w
```