

# CA GovernanceMinder

## Reference Guide

12.6.1



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

## CA Technologies Product References

This document references the following CA Technologies products:

- CA GovernanceMinder
- CA Identity Manager
- CA SiteMinder®
- CA User Activity Reporting Module
- CA SDM

## 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](mailto: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: CA GovernanceMinder System Properties 9

## Chapter 2: System Property Basics 11

Properties Settings .....	11
Create a Property Key .....	12
Customize Columns in My Task Tables .....	13

## Chapter 3: Utilities 15

Updating Existing Links .....	15
Encrypt Administrator Passwords .....	17
Workpoint Processes .....	19
System Properties for Emails .....	19

## Chapter 4: Help Desk Integration 21

Client Creation Events .....	21
Help Desk User Name .....	21
Help Desk Password .....	21
Help Desk Web Service URL .....	22
Help Desk System User Login .....	22
Help Desk Ticket Type Mapping .....	22
Help Desk Object Type .....	22
Number Ticket Attribute Definition .....	23

## Chapter 5: Implicit Accounts 25

implicit.accounts.enabled .....	25
implicit.accounts.field.name .....	25
implicit.accounts.field.nameuniverse_name .....	26
Traffic Limits for Usage Data .....	26

## Chapter 6: Process Parameters for Default Reviewers 27

flow.defaultManager .....	27
flow.userApproval.portalUser.defaultManager .....	27
flow.roleApproval.portalUser.defaultManager .....	28
flow.resourceApproval.portalUser.defaultManager .....	28

---

system.approval.defaultManager .....	28
Conceal Custom Configuration Option.....	28
FIPS Compliant Encryption .....	29

## Chapter 7: System Properties for Business Workflows 31

approvals.flowOwner .....	31
role.defaultOwner.enable.....	31
approval.role.defaultOwner.....	32

## Chapter 8: Certifications 33

Consult .....	33
Multiple Reveiwrs on Customized Workflows .....	34
Reassignment.....	34
Reassign Option User List.....	35
Certification Custom Workflow Processes .....	35
Delete Expired Alerts .....	36
Certification Processes Available in the Portal.....	36
Previous Review Decisions as Live Choices in Recertification Tasks .....	37
Customized Workflow Mappings in the Certification Creation Wizard .....	37
Specify Custom Process Mappings for Individual Certifications .....	38
Certify Indirect Links .....	38

## Chapter 9: Business Flows 39

Action Details Screen Action Management .....	39
My Details Actions .....	39
My Tasks Actions.....	40
User Details Popup Dialog.....	40
Resource Details Popup Dialog .....	40
Role Details Popup Dialog .....	40
Approve or Reject All Entity Actions .....	40
Reassign Entity Tasks.....	41
Escalate Property .....	41

## Chapter 10: Sage Security Parameters 43

sage.security.disable.optimizations .....	43
Single Sign-on (SSO) .....	44
Proxy ID Expiration.....	44
Regular Expression Role Filter .....	44
Returned HTTP Header UserID.....	44

---

Returned HTTP Header User Name.....	45
Specify the Session Cookie Name for Each Zone .....	45
Single Sign-on (SSO) User ID .....	45

## **Chapter 11: Business Policy Rules (BPR) Compliance Properties 47**

Segregation of Duties (SoD) .....	47
ALL Flag BPR Rules.....	48

## **Chapter 12: CA Business Intelligence Properties 49**

bo.boReportUserPassword .....	49
bo.host .....	49
bo.httpUrl.....	49
bo. password .....	50
bo.universeName .....	50
bo.user .....	50
Pre-approved Web Services .....	50
Do Not Remember Username at Login .....	50
Save Data Extraction .....	51
Custom Certification Workflow Processes .....	51

## **Chapter 13: Transaction Log Event Recording 53**

Portal User Login .....	53
Portal User Logout .....	53
Web Service Login.....	54
Record Transaction Log Events .....	54
Tracking User Navigation .....	54
Tracking Excluded Portal Pages.....	54
Record an Event for Web Service Login .....	55
Model Event Notification Properties.....	55
Enabled Event Notification.....	55
Enabled Event that Triggers a Notification .....	55
Specify LDAP Authentication .....	56
System, Workflow and Task Parameters.....	56
Special Characters for Member Lists Properties .....	57
Define CA Identity Manager Thread Pool Size .....	58
Logout URL .....	58
Date Display .....	59
Day, Month, and Year .....	59
Day, Month, Year, Hour and Minute .....	59
Define Workpoint Server Information .....	59

---

Certification Rows Displayed.....	59
Information Bubble Properties .....	60



# Chapter 1: CA GovernanceMinder System Properties

---



# Chapter 2: System Property Basics

---

This section contains the following topics:

[Properties Settings](#) (see page 11)

[Create a Property Key](#) (see page 12)

[Customize Columns in My Task Tables](#) (see page 13)

## Properties Settings

The Properties Settings utility provides access to the `eurekify.properties` file, where you create property keys and you edit existing property key values.

Common Properties are properties that other CA GovernanceMinder components use, such as Workpoint and the CA User Activity Reporting. These common properties are listed separately under Common Properties Settings. This utility functions in the same way as the general Properties Settings utility.

The Properties table contains the following columns:

### Type

The associated property file name.

### Property Key

The property key name.

### Property Value

The property key assigned value.

When creating or editing an existing property, the data is saved to the CA GovernanceMinder database. If the value of a database property key is different from the value listed in the `eurekify.properties` file, the system uses the value listed in the database.

**Note:** You can encrypt an existing property by editing the property and selecting the Encrypt Property check box.

The Portal provides you with the following property types to store your key values:

#### Home Directory Property

The value is taken from the eurekify.properties file. The value can be the default value, or the value if someone manually edited the eurekify.properties file.

#### Database Property

The value is taken from the database. Selecting this property type *overrides* the value of the property in the eurekify.properties file.

**Note:** You can change a property value *only* by saving the property as a Database Property. The Save button is not enabled otherwise. To revert to the default value (for a database property), click Remove from DB.

#### Follow these steps:

1. On the Administration menu click Settings.  
The list of available options appears.
2. Click Property Settings or Common Property Settings.  
The Property Settings Page screen opens.

## Create a Property Key

You define property keys as part of the product. You install property keys by default in CA GovernanceMinder. To add new property keys to the property file, use the Properties Settings utility.

To create a property key, enter the key before you click Add New.

#### Follow these steps:

1. In the Properties page, enter a name of a property key in the Properties text box.
2. Click Add New.

The Edit Property screen appears.

3. Enter a property value in the Property Value text box.
4. In the Type field, select a database type from the drop-down list.
5. (Optional) Select the Encrypt Property check box to encrypt a property.

**Note:** Some common properties (bootstrap) cannot be encrypted.

6. Click Save.

The new property key appears in the Property Settings screen.

## Customize Columns in My Task Tables

You can customize the tables that display workflow actions. Customize the information that is displayed for different types of actions to support your decision process.

Click Customize on a table header you want to modify. In the dialog, you can add or remove columns, and change their order.

*Mandatory columns* cannot be removed from table displays. Red text and a locked padlock icon indicate mandatory columns in customization screens and dialogs. Some mandatory columns are hard-coded defaults in CA GovernanceMinder. Administrators can define additional mandatory columns.



# Chapter 3: Utilities

---

This section contains the following topics:

[Updating Existing Links](#) (see page 15)

[Encrypt Administrator Passwords](#) (see page 17)

[Workpoint Processes](#) (see page 19)

[System Properties for Emails](#) (see page 19)

## Updating Existing Links

The following system properties enable RACI synchronization to update existing links:

### **raci.sync.override.accountable.roles**

Determines whether existing roles are updated in the Accountable configuration. When this property is true, CA GovernanceMinder updates the Accountable configuration when the accountable user of a role changes. To implement this property for a universe, create a property with the following name:

`universe.property.universe_name.raci.sync.override.accountable.roles`

**Note:** *universe\_name* is the name of the target universe.

**Default:** False

### **raci.sync.override.accountable.resources**

Determines whether existing resources are updated in the Accountable configuration. When this property is true, CA GovernanceMinder updates the Accountable configuration when the accountable user for the resource changes. To implement this property for a universe, create a property with the following name:

`universe.property.universe_name.raci.sync.override.accountable.resources`

**Note:** *universe\_name* is the name of the target universe.

**Default:** False

**continuousUpdates.shouldSyncRaci**

Determines whether to synchronize RACI in each CA GovernanceMinder notification from CA Identity Manager.

**Default:** True.

Valid values are as follows:

**True**

Users can specify if they want CA Identity Manager users included in CA GovernanceMinder RACI configuration.

**False**

Users can specify if they do not want CA Identity Manager users included in CA GovernanceMinder RACI configuration.

**continuousUpdtes.shouldUpdatePermissionsConfiguration**

Determines whether to synchronize RACI in each CA GovernanceMinder permission notification from CA Identity Manager.

**Default:** True.

Valid values are:

**True**

Users can specify if they want CA Identity Manager users included in CA GovernanceMinder RACI configuration.

**False**

Users can specify if they want CA Identity Manager users included in CA GovernanceMinder RACI configuration.



**raci.sync.override.accountable.roles**

RACI synchronization does not update links to users in the A configuration.

**Description:**

After synchronizing the RACI configuration through the portal, links to users in the A configuration that determines the managers to assign to tickets are not updated. As a result, tickets are assigned to the default administrator or to previous manager.

**Default:** False

**Solution:**

Follow these steps:

1. Set the following properties to True:

raci.sync.override.accountable.roles

raci.sync.override.accountable.resources

2. Perform the RACI synchronization.

The accountable configuration (A configuration) contains the link to the user that is written in the role/resource field marked as the owner in the universe definition.

## Encrypt Administrator Passwords

Use the following system properties to encrypt CA GovernanceMinder administrator passwords:

**sage.admin.password**

Defines the CA GovernanceMinder EAdmin user account password.

**Default:** eurekify

**sage.batch.password**

Defines the password of the EBatch user account.

**Default:** eurekify

**usage.import.logmanager.odbc.host**

Defines the hostname of the target CA User Activity Reporting server.

**Default:** elmhostname

**usage.import.logmanager.odbc.port**

Defines the default CA User Activity Reporting database port.

**Default:** 17002

**Note:** To verify the database port CA User Activity Reporting Module is listening on, open Administrative Tools in Windows, and select Services, ODBC Server. Click on the CA User Activity Reporting server and check the Server Listening Port field.

**usage.import.logmanager.odbc.user**

Defines the username of the CA User Activity Reporting account that CA GovernanceMinder uses to log in to CA User Activity Reporting. Must be an administrator account in CA User Activity Reporting or an account that has read access to everything.

**Default:** elmusername

**usage.import.logmanager.odbc.password**

Defines the password of the CA User Activity Reporting account that CA GovernanceMinder uses to log in to CA User Activity Reporting.

**Default:** apassword

**usage.online.logmanager.https.host**

Defines the hostname of the target CA User Activity Reporting server.

**usage.online.logmanager.https.port**

Defines the listening port on the target CA User Activity Reporting server portal.

**Default:** 5250

**usage.online.logmanager.https.certificate**

Specifies the CA User Activity Reporting security certificate name provided when registering CA GovernanceMinder on the CA User Activity Reporting server.

**Default:** CA\_RCM

## Workpoint Processes

System properties described in this section affect Workpoint processes.

The following system property controls progressive launch of Workpoint processes:

### **lazy.workflow.job.creation.enabled**

Specifies whether CA GovernanceMinder uses progressive launch. When this Boolean property is true, CA GovernanceMinder generates review actions based on the initial review node of Workpoint processes before it creates a Workpoint job instance.

**Default:** True.

Unilateral Cancel - During a workflow, a task can be canceled or become irrelevant. For example, a manager can terminate a request for several new privileges when only some of them are approved. CA GovernanceMinder marks these tasks internally as canceled, but does not continue to manage the corresponding Workpoint process. When a custom process includes conditions and nodes to handle a canceled process, CA GovernanceMinder does not return the cancellation status to the Workpoint process, and does not handle those nodes.

The following system property controls unilateral cancellation of Workpoint processes:

### **aggregated.workflow.job.cancel.enabled**

Specifies whether CA GovernanceMinder maintains Workpoint processes that correspond to canceled workflow tasks. When this Boolean property is true, CA GovernanceMinder continues to interact with Workpoint processes after their workflow tasks are canceled.

**Default:** False.

## System Properties for Emails

Use the following system properties to configure the CA GovernanceMinder connection to an SMTP server, and to define email behavior.

**Note:** Some of these properties are set automatically during CA GovernanceMinder installation.

### **mail.Server**

Defines the URL of the SMTP server.

### **mail.ServerPort**

Defines the port used for communication with the SMTP server.

**mail.user**

Defines the user account for CA GovernanceMinder on the SMTP server.

**Note:** If you enter a value in the mail.user property, an unauthenticated mail server may have issues when sending emails. When using an unauthenticated SMTP server, we recommend that you leave the mail.user and mail.password properties empty.

**mail.password**

Defines the password of the CA GovernanceMinder account on the SMTP server.

**mail.from**

Defines the originating e-mail address of the CA GovernanceMinder server. **Default:** RCM@ca.com

**mail.useSSL**

Determines whether communication with the SMTP server uses SSL encryption.

**mail.max.attempts**

Defines how many times CA GovernanceMinder attempts to send an email.

**mail.sending interval**

Defines the time, in seconds, between attempts by CA GovernanceMinder to send emails.

**mail.smtp.timeout**

Defines CA GovernanceMinder email timeout, in seconds, by attempts to send emails.

**Default:** 60 seconds

**portalExternalLink.certificationUrl**

Defines the value of the certification URL parameter in email templates.

**portalExternalLink.homeUrl**

Defines the value of the CA GovernanceMinder URL home page parameter in email templates.

# Chapter 4: Help Desk Integration

---

This section contains the following topics:

[Client Creation Events](#) (see page 21)

[Help Desk User Name](#) (see page 21)

[Help Desk Password](#) (see page 21)

[Help Desk Web Service URL](#) (see page 22)

[Help Desk System User Login](#) (see page 22)

[Help Desk Ticket Type Mapping](#) (see page 22)

[Help Desk Object Type](#) (see page 22)

[Number Ticket Attribute Definition](#) (see page 23)

## Client Creation Events

Defines whether to delegate CA GovernanceMinder ticket creation events to clients, such as a help desk application.

**tmsEvent.create.enable**

**Values:** True/False

## Help Desk User Name

Defines the help desk user name used to access the product, such as administrator.

**integration.unicenter.servicedesk.username**

**Default:** administrator

## Help Desk Password

Defines the password for the help desk user.

**integration.unicenter.servicedesk.password**

**Default:** capassword

## Help Desk Web Service URL

Defines the help desk Web Service URL.

**integration.unicenter.servicedesk.webservice.url**

**Note:** CA Help Desk r12 exposes a new web service, but the product only supports the r11 Web Service.

**Default:** http://HOSTNAME:8080/axis/services/USD\_WebServiceSoap

## Help Desk System User Login

Defines the field in the permission configuration user database (eurekify.udb) that states the login ID of the user in the help desk system.

**integration.unicenter.servicedesk.user.field**

**Note:** If not specified, PersonID is used.

**Default:** HelpDeskLogin

## Help Desk Ticket Type Mapping

Defines the mapping between CA GovernanceMinder ticket types and the help desk ticket types, using a key-value pair.

**integration.unicenter.servicedesk.type.mapping**

**Default:** TMS:TestTicket=1,SAGE:\*RoleTicket=2,FlowTicketForImport\_\_V0.8=2,...

**Example:** TMS:TestTicket=ChangeOrder,SAGE:\*RoleTicket=Bug, SAGE:ErrTicket=Issue

This example details the following:

Maps the CA GovernanceMinder test ticket to the help desk ChangeOrder:

- Maps the CA GovernanceMinder error ticket to the help desk 'Issue' ticket
- Maps any CA GovernanceMinder ticket with a type that ends in 'RoleTicket' to a help desk ticket of 'Bug' type. (SAGE:\*RoleTicket=Bug)

## Help Desk Object Type

Defines the help desk object type of the number ticket.

**integration.unicenter.servicedesk.object.type.[number 1-3]**

**Default:** chg

## Number Ticket Attribute Definition

Defines numberticket attributes. Use the velocity template language to set the values for this property. Predefined variables are available to set these values.

**integration.unicenter.servicedesk.attributes.number[1-3]**

**Default:** chg\_ref\_num,....

### Examples

```
chg_ref_num, RCM_1_${ticket.getTicketId()}_${currentTime},  
description, ${ticket.getDescription()},  
summary, ${ticket.getTitle()},  
affected_contact, ${ticketOwnerHandle},  
requestor, ${loginUserHandle} =
```

**Note:** For more information about the velocity template language, see the [Apache Velocity Project User Guide](#).





# Chapter 5: Implicit Accounts

---

When a CA GovernanceMinder universe does not have account configurations, or a user has no accounts on external endpoints, account information is unavailable. The product creates an implicit account to relate resources to users even when account information is unavailable from external endpoints.

Implicit accounts have the following structure:

- Account name - The account name is taken from the field specified in the `implicit.accounts.field.name` property.
- Mapped endpoint - The default mapped endpoint is taken from the Configuration resource application field that is specified for the universe.

This section contains the following topics:

[implicit.accounts.enabled](#) (see page 25)

[implicit.accounts.field.name](#) (see page 25)

[implicit.accounts.field.nameuniverse name](#) (see page 26)

## implicit.accounts.enabled

### **implicit.accounts.enabled**

Specifies if the product creates implicit accounts for users.

Valid values; True, False

**Default:** False

**Note:** We recommend using account correlation instead of enabling this feature.

## implicit.accounts.field.name

### **implicit.accounts.field.name**

Specifies the field of user records that is used to name implicit accounts. Typically this is the loginID field.

**Default:** personId

## implicit.accounts.field.nameuniverse\_name

### **implicit.accounts.field.nameuniverse\_name**

Specifies the user record field that is used to name implicit accounts in the specified universe. This value overrides the value of the implicit.accounts.field.name property for the specified universe.

**Note:** There is no period between name and universe\_name in this field.

### **universe**

Defines the universe that uses the field specified to name implicit accounts.

## Traffic Limits for Usage Data

This property defines the waiting period for data queries from CA GovernanceMinder to the CA User Activity Reporting . Increase this property value to support increased query volume. When the volume of traffic at the CA User Activity Reporting server is high, use values of an hour (3600 seconds) or more. If time periods are minimized, but timeouts persist, change the value of the following system property to suit the size of the CA GovernanceMinder data universe and your operating environment:

### **usage.import.logmanager.odbc.timeout.seconds**

# Chapter 6: Process Parameters for Default Reviewers

---

Standard Workpoint processes that include review nodes declare process-level parameters for default reviewers. When CA GovernanceMinder initiates a Workpoint job, it populates these parameters with names based on user settings (such as options in the certification creation wizard) or defaults. All nodes in the process can use these parameters to reference the specified default reviewer.

In processes that add or remove a link, a single default reviewer is specified.

In certification processes, one default reviewer is specified for initial certification, and two default reviewers are specified for change approvals, one for each entity in the link under review.

**Note:** In certification processes that manage links between parent and child roles, only one default reviewer is specified for approval of changes.

You can use any of these parameters to specify a default reviewer for any certification or change approval action. However, the default reviewer associated with one entity may not be knowledgeable or appropriate for other review actions.

This section contains the following topics:

[flow.defaultManager](#) (see page 27)

[flow.userApproval.portalUser.defaultManager](#) (see page 27)

[flow.roleApproval.portalUser.defaultManager](#) (see page 28)

[flow.resourceApproval.portalUser.defaultManager](#) (see page 28)

[system.approval.defaultManager](#) (see page 28)

## flow.defaultManager

### flow.defaultManager

Defines the default reviewer for initial certification in a certification. This parameter acquires its value from the Workflow.defaultManager CA GovernanceMinder system property.

## flow.userApproval.portalUser.defaultManager

### flow.userApproval.portalUser.defaultManager

Defines the default reviewer for approval of changes to a user in a certification.

## **flow.roleApproval.portalUser.defaultManager**

### **flow.roleApproval.portalUser.defaultManager**

Defines the default reviewer for approval of changes to a role in a certification.

## **flow.resourceApproval.portalUser.defaultManager**

### **flow.resourceApproval.portalUser.defaultManager**

Defines the default reviewer for approval of changes to a role in a certification.

## **system.approval.defaultManager**

### **system.approval.defaultManager**

Defines the default reviewer in general processes to add or remove links. This parameter acquires its value from the approval.defaultManager CA GovernanceMinder system property.

# **Conceal Custom Configuration Option**

You can conceal the Use custom configuration option in CA GovernanceMinder to discourage users from customizing endpoint mappings when defining a connector to CA Identity Manager or the IAM Connector Server.

The following property determines whether a user can access the custom configuration option when defining a connector to CA Identity Manager or the IAM Connector Server:

### **universe.property.universe\_name.endpointAssociations.enabled**

Defines whether the custom configuration option is displayed in the connector wizard. When true, the option to customize endpoint mappings appears. When false, the option to customize endpoint mappings is unavailable, and the user cannot configure associations for loaded endpoint templates.

**Default:** True

## FIPS Compliant Encryption

The following properties configure FIPS-compliant encryption:

### **pbe.fips.enabled**

Specifies if CA GovernanceMinder uses FIPS-compliant encryption algorithms.

**Default:** False

True—Use FIPS-compliant encryption.

False—Use non-compliant encryption.

### **pbe.provider**

Defines the FIPS-compliant algorithms provider. Leave this property blank to use the RSA JSafeJCE algorithms that CA provides. If you specify another provider, copy that algorithm set to all computers running the CA GovernanceMinder server.

### **passphrase.getter.class**

Defines the Java class that retrieves the encryption key.

Specify one of the previous options by setting the passphrase.getter.class parameter when you configure FIPS encryption.

**Default:** com.eurekify.security.SimplePassPhraseGetter

The CSM Password Tool enables you to use a FIPS key in an external file generated by the tool for encryption.



# Chapter 7: System Properties for Business Workflows

---

Administrators use CA GovernanceMinder Client Tools to analyze and directly edit CA GovernanceMinder data files. When the administrators change a configuration file, they can submit these changes to the CA GovernanceMinder server. The server initiates the appropriate workflow to approve and implement the changes.

Because no business user initiates these workflows, the system properties described in this section define default owners.

This section contains the following topics:

[approvals.flowOwner](#) (see page 31)

[role.defaultOwner.enable](#) (see page 31)

[approval.role.defaultOwner](#) (see page 32)

## approvals.flowOwner

### approvals.flowOwner

Defines the default owner of workflows submitted from CA GovernanceMinder client applications. By default the CA GovernanceMinder system administrator is the owner for these workflows. To implement this property for a universe, create a property with the following name:

`universe.property.universe_name.approvals.flowOwner`

**Note:** *universe\_name* is the name of the target universe.

**Default:** AD1\EAdmin

## role.defaultOwner.enable

### role.defaultOwner.enable

Determines whether the `approval.role.defaultOwner` system property defines the default owner for new role requests from CA GovernanceMinder client applications. When this Boolean property is false, the CA GovernanceMinder administrator is the owner of these roles, and the value of `approval.role.defaultOwner` is ignored.

**Default:** True

## approval.role.defaultOwner

### **approval.role.defaultOwner**

Defines the default owner of a proposed new role submitted from CA GovernanceMinder client applications. This user must be in the target universe for role creation. If this property is null, or if the specified user is not in the target universe, CA GovernanceMinder creates the role without an owner. In this case the user specified by the approval.defaultManager system property reviews the role request.

**Default:** AD1\EAdmin



# Chapter 8: Certifications

---

The review nodes of standard Workpoint processes declare parameters for default reviewers. The parameters populate with names based on the certification creation wizard user settings when CA GovernanceMinder initiates a Workpoint job. All nodes in the process can use these parameters to reference the default reviewer. A single default reviewer is specified in processes that add or remove a link.

One default reviewer is specified for the initial certification process. Two default reviewers are specified for change approvals with one reviewer for each entity in the link under review.

**Note:** Only one default reviewer is specified for changes approval in a certification process that manages links between parent and child roles.

Use these parameters to specify a default reviewer for a certification or change approval action. Remember that the default reviewer associated with one entity is not always the appropriate reviewer other actions.

This section contains the following topics:

[Consult](#) (see page 33)

[Multiple Reviewers on Customized Workflows](#) (see page 34)

[Reassignment](#) (see page 34)

[Reassign Option User List](#) (see page 35)

[Certification Custom Workflow Processes](#) (see page 35)

[Delete Expired Alerts](#) (see page 36)

[Certification Processes Available in the Portal](#) (see page 36)

[Previous Review Decisions as Live Choices in Recertification Tasks](#) (see page 37)

[Customized Workflow Mappings in the Certification Creation Wizard](#) (see page 37)

[Specify Custom Process Mappings for Individual Certifications](#) (see page 38)

[Certify Indirect Links](#) (see page 38)

## Consult

You can enable consultation with an additional reviewer about a certification item using the following property.

### **certification.more.consult.enabled**

Enables another reviewer to be asked for input about a certification item.

**Default:** True

## Multiple Reviewers on Customized Workflows

You can customize workflows to support multiple reviewers by adding a new property. This property exposes a new UI button that enables you to download a CSV/MS Excel file that details reviewer progress.

### **administration.workflows.progress.by.reviewers.csv.button.show**

Enables customized workflows for multiple reviewers.

**Default:** True

Set this property to true to enable this functionality.

## Reassignment

You can enable, disable, or configure reassign behavior with the following properties.

In the Portal go to Administration, Settings, Property Settings. Click Edit on the row with the property that you want to configure.

### **certification.reassign.enabled**

Enables a certification to be reassigned to another employee.

**Default:** True

### **certification.more.reassign.enabled**

Enables a certification to be assigned to more than one employee.

**Default:** True

### **email.onCertificationReassignCertifyUserAction.cc**

Enables email notification to be sent to the relevant employees when a certification item is reassigned.

**Example:** user@example.com or a Login ID such as AD1\EAdmin

You can enter two or more users by typing a semicolon between the email addresses: user1@example.com;user2@example.com.

## Reassign Option User List

Filters the reassign option user list.

**tms.campaign.[campaign-type].reassign.filter**

### Example:

```
tms.campaign.userCertification.reassign.filter=GFilter=(Organization=
$$owner.Organization$$)
```

```
tms.campaign.roleCertification.reassign.filter=GFilter=(Organization=
$$owner.Organization$$)
```

```
tms.campaign.resourceCertification.reassign.filter=GFilter=(Organization=
$$owner.Organization$$)
```

## Certification Custom Workflow Processes

CA GovernanceMinder uses a set of predefined processes to execute the certification tasks. Administrators can create alternative processes, which change how CA GovernanceMinder implements certification tasks. For example, administrators can define a set of processes that involve higher management levels in certification reviews. You create a certification and specify the set of processes that controls the certification tasks execution.

Before you can apply alternative processes to your certification, administrators must create and import the processes to CA GovernanceMinder, and map them to certification business workflow tasks.

Specify the process mapping for your certification in the certification creation wizard Execution screen. The following options are available under Processes:

- **System defaults** - Uses the default workflow processes installed with CA GovernanceMinder to implement the certification. Execute standard certification behaviors.

- Customized Processes - Uses the process mapping set you select from the drop-down list for the certification implementation.
- Processes - Displays the processes that CA GovernanceMinder invokes to execute the major tasks of the campaign, which is based on your selection.

Use the following system property in the process for the default user for approval and decision making:

**Workflow.defaultManager**

Use this property value as a default user for approval and decision-making activities.

**Value:** User login

**Default:** AD1\EAdmin

## Delete Expired Alerts

In CA GovernanceMinder, you can enable or disable a scheduled task to search through all universes that have an approved audit card, and delete all expired alerts. This scheduled task can be configured using the CA GovernanceMinder Portal.

**audit.delete.expired.alerts.enabled**

**Default:** True

**audit.delete.expired.alerts.intervals.seconds**

**Default:** 86400 (one day)

**Note:** To override the default behavior for a specific universe, create a universe-specific property. For example, you can create the `universe.property.Universe \ Name.audit.delete.expired.alerts.enabled` property, and set it appropriately for that universe. Spaces in a universe name are replaced with a backslash followed by a space (\ ).

## Certification Processes Available in the Portal

Specifies whether certification processes that bypass the approval task are available in the CA GovernanceMinder Portal.

**campaign.settings.allowModifiedCampaignProcesses**

**Default:** False

True - Makes review processes that bypass approval available during certification creation.

False - Hides review processes that bypass approval. Only standard review processes, which include approval tasks, can be selected during certification creation.

## Previous Review Decisions as Live Choices in Recertification Tasks

Determines if previous review decisions are presented as live choices in recertification tasks.

### **campaign.settings.recertification.allowOneClickResubmit**

**Default:** False

True - Previous Approve or Reject decisions are selected by default in recertification tasks. Reviewers in the recertification can accept these decisions by clicking Submit in the My Tasks screen. The certification creation wizard displays the Keep Approver's Selections option.

False - Previous Approve or Reject decisions are indicated by grayed icons in recertification tasks, but these decisions are not selected by default. Reviewers in the recertification must select a review decision for each link under review. The certification creation wizard displays the Show Approver's Selections option.

## Customized Workflow Mappings in the Certification Creation Wizard

Controls the availability of customized workflow mappings in the certification creation wizard. It determines whether users can specify custom process mappings for individual certifications.

### **campaign.settings.allowModifiedCampaignProcesses**

**Default:** False

True - Users can specify a custom process mapping when they create a certification . The Processes section and its options are displayed in the Execution tab of the certification creation wizard.

False - Users cannot specify a custom process mapping when they create a certification . The Process section is not displayed in the certification creation wizard.

## Specify Custom Process Mappings for Individual Certifications

Determines whether users can specify custom process mappings for individual certifications.

### **IsAggregatedExportEnabled**

**Default:** False

True - Users can specify a custom process mapping when they create a certification. The Processes section and its options are displayed in the Execution tab of the certification creation wizard.

False - Users cannot specify a custom process mapping when they create a certification. The Process section is not displayed in the certifications creation wizard

## Certify Indirect Links

You can verify indirect links for a certification.

Determines whether users can include indirect links for a certification.

### **campaign.allowIndirectTasksActions**

Enable certification actions for indirect links through the Portal.

**Default:** False

True - The Indirect links option in the certification template (Filter step) is active.

False - The Indirect links option in the certification template (Filter step) is inactive. When a certification uses this template, it creates tasks only for direct links in the certification in the Portal.

**Note:** This property is informative and only applies on the Universe level.

# Chapter 9: Business Flows

---

This section contains the following topics:

[Action Details Screen Action Management](#) (see page 39)

[My Details Actions](#) (see page 39)

[My Tasks Actions](#) (see page 40)

[User Details Popup Dialog](#) (see page 40)

[Resource Details Popup Dialog](#) (see page 40)

[Role Details Popup Dialog](#) (see page 40)

[Approve or Reject All Entity Actions](#) (see page 40)

[Reassign Entity Tasks](#) (see page 41)

[Escalate Property](#) (see page 41)

## Action Details Screen Action Management

Defines group handling of actions in the Action Details screens.

### **businessflows.reviewers.default.allowSelectAll**

This property determines whether reviewers can manage all actions in a table as a group. When set to true, action detail tables display checkboxes in the Approve, Reject, and Reassign column headers. Reviewers select these check boxes to apply a decision to all the links in the table. This property also determines the default behavior for certifications. When this property is true, the Enable managers to select an entire column option in the Reviewers screen of the Add Certification wizard is selected by default.

**Default:** True

## My Details Actions

Defines users to control groups of actions from the My Tasks overview screen.

### **businessflows.inbox.approveRejectAll.enabled**

Determines whether reviewers can approve or reject groups of actions in the My Tasks overview screen. When set to true, the My Tasks overview screen displays Assign and Reject columns. Users can approve or reject groups of actions listed in the screen. They can also select checkboxes in the Approve and Reject column headers to apply a decision to the entire contents of a table.

**Default:** False

## My Tasks Actions

Defines whether reviewers can reassign groups of actions in the My Tasks overview screen.

### **businessflows.inbox.reassignAll.enabled**

When this property is set to true, the My Tasks overview screen displays the Reassign column. Users can reassign groups of actions listed in the screen. They can also select check boxes in the Reassign column headers to reassign the entire contents of a table.

**Default:** False

## User Details Popup Dialog

Enables you to set the user data column linked to the Details popup dialog.

### **businessflows.inbox.display.field.USER**

**Default:** UserName

## Resource Details Popup Dialog

Enables you to set the resource data column linked to the Details popup dialog.

### **businessflows.inbox.display.field.RESOURCE**

**Default:** Resname1

## Role Details Popup Dialog

Enables you to set the role data column linked to the Details popup dialog.

### **businessflows.inbox.display.field.ROLE**

**Default:** Rolename

## Approve or Reject All Entity Actions

Enables reviewers to approve or reject all the actions for an entity without having to address each action individually.

### **businessflows.inbox.approveRejectAll.enabled**

**Default:** False



## Reassign Entity Tasks

Enables reviewers to reassign all the tasks for an entity without having to address each action individually.

### **businessflows.inbox.reassignAll.enabled**

Set the value of this property to true to enable this functionality

**Default:** False

## Escalate Property

This property is used for filtering the escalate option user list, and contains the following options:

### **tms.escalate.filter**

Default escalate filter.

Example:

```
tms.escalate.filter=GFilter=(Organization=$$owner.Organization$$)
```

### **tms.escalate.filter.TicketType.SAGE.ChangeApprovalParentTicket**

Ticket type filter.

Example:

```
tms.escalate.filter.TicketType.SAGE.ChangeApprovalParentTicket=GFilter=(Organization=cookingdept)
```

### **tms.escalate.filter.LinkUser-Role**

Ticket name filter.

Example:

```
tms.escalate.filter.LinkUser-Role=GFilter=(Email=ssimhi@eurekify.com)
```



# Chapter 10: Sage Security Parameters

---

These properties determine various performance features and header and cookie details.

This section contains the following topics:

[sage.security.disable.optimizations](#) (see page 43)

[Single Sign-on \(SSO\)](#) (see page 44)

[Proxy ID Expiration](#) (see page 44)

[Regular Expression Role Filter](#) (see page 44)

[Returned HTTP Header UserID](#) (see page 44)

[Returned HTTP Header User Name](#) (see page 45)

[Specify the Session Cookie Name for Each Zone](#) (see page 45)

## sage.security.disable.optimizations

Enables you to set the security filter calculation optimization. This setting improves performance for all the components that use security filters.

### sage.security.disable.optimizations

**Default:** False

These values preserve the old security filter calculation if we do not want to use this new feature.

**Example:** We can see that security filter 1 already contains security filter 2, and therefore filter 2 is redundant.

If we have the following security filters:

- 1. Role=a\*
- 2. Role=ab\*

Available settings for this property are Boolean (true,false).

Where sage.security.disable.optimizations = true:

CA GovernanceMinder does not do security filter optimization when it calculate it s filter result.

sage.security.disable.optimizations=false:

CA GovernanceMinder does security filter optimization before calculating the filter result (default).

## Single Sign-on (SSO)

Enables SSO on the CA GovernanceMinder server by setting the following system property to True.

**sage.security.SiteMinder.enabled**

Specifies whether you implement SSO using CA SiteMinder.

**Default:** False

**Valid values:** True, False.

## Proxy ID Expiration

Defines the lifetime of a proxy ID, in minutes. CA GovernanceMinder creates temporary proxy user IDs to support user authentication by CA SiteMinder®.

**sage.security.GUID.expiration.minutes**

**Default:** 360 minutes (6 hours).

## Regular Expression Role Filter

Defines whether regular expression characters in the filter are escaped.

**sage.security.filter.escapeRegex**

**Default:** False

When set to false, you can create a role filter such as 'rolename=Org.\*' that enables you to see all roles that start with 'Org'. The asterisk (\*) is read as a wildcard.

When set to true, you can create a role filter that includes a regular expression character in the role name. To filter for a role with a regular expression character, the character must be escaped in the permission configuration, for example, 'rolename=Org\\.\\\*'.

## Returned HTTP Header UserID

Defines the attribute label in the returned HTTP header that contains the username or the value of the UserID field. The field defined in this property must be present in the HTTP header.

**sage.security.CA SiteMinder.username.attribute**

**Default:** sm\_user

## Returned HTTP Header User Name

Defines the attribute label in the returned HTTP header that contains the user domain.

**sage.security.CA SiteMinder.domain.attribute**

**Default:** rcm\_domain

## Specify the Session Cookie Name for Each Zone

Configure this system property to specify the session cookie name for each zone.

Replace *zone\_name* with the name of the SiteMinder zone. Specify the session cookie name as the value for the system property.

**sage.security.siteminder.cookie.zone\_name**

## Single Sign-on (SSO) User ID

This property controls CA GovernanceMinder SSO operations.

**sage.security.GUID.expiration.delta.seconds**

CA GovernanceMinder creates temporary proxy user IDs to support user authentication by CA SiteMinder®. This property defines a cutoff time before the proxy ID expires, beyond which no new requests are sent using the ID.

**Default:** 60 seconds.



# Chapter 11: Business Policy Rules (BPR) Compliance Properties

---

This section describes BPR compliance properties.

This section contains the following topics:

[Segregation of Duties \(SoD\)](#) (see page 47)

[ALL Flag BPR Rules](#) (see page 48)

## Segregation of Duties (SoD)

Current Segregation of Duties (SoD) rules only consider users that are assigned to one or more of the specified resources. This property considers all users, even those users that are not assigned to resources.

This property enables you to create a Segregation of Duties (SoD) rule that counts users that do not have any of the specified entities as violators.

### **bpr.sod.ignore.zero**

**Default:** True

#### **True**

Specifies that users who have no defined roles or resources on the left side of the SoD rule are not considered violators.

#### **False**

Specifies that users who have no defined roles or resources on the left side of the SoD are considered violators. The system detects users who have none of the specified entities.

**Note:** This functionality only exists in the CA GovernanceMinder Portal Client. Tools behavior is unchanged and ignores users with zero specified resources.

## ALL Flag BPR Rules

Controls the behavior of the ALL flag for BPR rules that specify their entities as regular expressions.

### **bpr.all.representative**

#### **True**

Specifies that a representative entity for each rule is present.

**Default:** False

#### **False**

Specifies that all of the entities that satisfy all of the rules are present.

### **Example:**

If there are two rules on the left with the following statements:

- Roles that begin with A
- Roles that begin with B

If the property is set to false, ALL is satisfied only if the user has all of the roles that begin with A and all of the roles that begin with B.

If the property is set to true, ALL is satisfied if the user has at least one role that begins with A (a representative that satisfies the first rule) AND at least one role that begins with B (a representative that satisfies the second rule).



# Chapter 12: CA Business Intelligence Properties

---

This section describes CA Business Intelligence properties.

This section contains the following topics:

[bo.boReportUserPassword](#) (see page 49)

[bo.host](#) (see page 49)

[bo.httpUrl](#) (see page 49)

[bo.password](#) (see page 50)

[bo.universeName](#) (see page 50)

[bo.user](#) (see page 50)

## bo.boReportUserPassword

Describes the CA Business Intelligence password that is provided to generated users to view reports.

**bo.password**

## bo.host

Contains the SAP BusinessObject host name and port.

**bo.host**

**Default:** localhost:6400

## bo.httpUrl

Describes the CA Business Intelligence URL for report viewing.

**bo.httpUrl**

**Default:** http://localhost:8080/OpenDocument/opendoc/openDocument.jsp

**Example: CA Business Intelligence report URL**

http://mybomachine:8081/OpenDocument/opendoc/openDocument.jsp

## bo.password

Describes the CA Business Intelligence password.

**bo.password**

## bo.universeName

Describes the CA Business Intelligence universe name.

**bo.universeName**

**Default:** CA GovernanceMinder

## bo.user

Describes the CA Business Intelligence user with administrator permissions.

**bo.user**

**Default:** Administrator

## Pre-approved Web Services

By default, web services do not include pre-approved violations.

**audit.approved.alerts.webservices.include**

**Default:** False

To include pre-approved violations, set this property to true.

## Do Not Remember Username at Login

The CA GovernanceMinder login screen now remembers usernames by default with a property. If you do not want the login screen to remember usernames, set the following property to false.

**security.login.cookies.enable**

**Default:** True

## Save Data Extraction

Enables data extraction by specifying whether the product saves data snapshots to the external report database.

**reportdb.enabled**

**Default:** False

Valid values: True, False

**Note:** The product resets this property to false when it cannot export a scheduled data snapshot to the database. If the connection to the database server is interrupted, reset the property to true when the connection is restored.

## Custom Certification Workflow Processes

The product uses a set of predefined processes to execute certification tasks. Administrators can create alternative processes, which change how CA GovernanceMinder implements certification tasks. For example, administrators can define a set of processes that involve higher management levels in certification reviews. When you create a certification, you can specify which set of processes controls the execution of certification tasks.

Before you can apply alternative processes to your certification, administrators must create the processes, import them to the product, and map them to a certification business workflow.

The following system property is used in the process for the default user for approval and decision making:

**Workflow.defaultManager**

Use this property value as a default user for approval and decision making activities.

**Default:** AD1\EAdmin

**Value:** User login



# Chapter 13: Transaction Log Event Recording

---

These properties specify whether to record an event in the transaction log for a specific purpose.

This section contains the following topics:

[Portal User Login](#) (see page 53)

[Portal User Logout](#) (see page 53)

[Web Service Login](#) (see page 54)

[Record Transaction Log Events](#) (see page 54)

[Tracking User Navigation](#) (see page 54)

[Tracking Excluded Portal Pages](#) (see page 54)

[Record an Event for Web Service Login](#) (see page 55)

## Portal User Login

Specifies whether to record an event in the transaction log when a user logs in to the CA GovernanceMinder Portal.

**txlog.portal.login.enable**

**Default:** False

Values: True, False

## Portal User Logout

Specifies whether to record an event in the transaction log when a user logs out of the CA GovernanceMinder Portal.

**txlog.portal.logout.enable**

**Default:** False

Values: True, False

## Web Service Login

Specifies whether to record an event in the transaction log when a web service logs out of the CA GovernanceMinder Portal.

**txlog.webservice.login.enable**

**Default:** False

Values: True, False

## Record Transaction Log Events

Specifies whether to record events in the transaction log when users navigate in the CA GovernanceMinder Portal.

**txlog.portal.pageaccess.enable**

**Default:** False

Values: True, False

## Tracking User Navigation

Specifies the portal pages to include when tracking user navigation in the CA GovernanceMinder portal. Identify pages of the portal by their class names, and format the list as comma-separated values.

**txlog.portal.pageaccess.include.pageclasses**

**Default:** \*

**Example: Tracking user navigation to the CA GovernanceMinder Portal home page**

The following string enables you to track user navigation to the portal home page and the top-level dashboard and entity browser pages:

```
com.eurekify.web.portal.homepage.HomePage,com.eurekify.web.dashboards.ConfigurationDashboardPage,com.eurekify.web.entitybrowser.EurekifyBrowserPage
```

## Tracking Excluded Portal Pages

Specifies the CA GovernanceMinder Portal pages exclude when tracking user navigation in the CA CA GovernanceMinder Portal. Identify CA GovernanceMinder Portal pages by their class names, and format the list as comma-separated values.

**txlog.portal.pageaccess.exclude.pageclasses**

**Default:** com.eurekify.web.portal.EmptyPage

## Record an Event for Web Service Login

Specifies whether to record an event in the transaction log when a web service logs in to the CA GovernanceMinder Portal.

**txlog.webservice.login.enable**

**Default:** False

Values: True, False

## Model Event Notification Properties

Workflows can result in universe model configuration changes. You can export these changes to provisioning endpoints by using the Model Event Notification API. This API provides a JMS topic for all model changes. You can then write custom code on external clients that manages this model event information.

**This section contains the following topics:**

[Enabled Event Notification](#) (see page 55)

[Enabled Event that Triggers a Notification](#) (see page 55)

### Enabled Event Notification

Indicates whether model event notification is enabled. This parameter signals the availability of the Model Event Notification API to CA GovernanceMinder Workpoint processes that contain the Notify Model Change and Notify Aggregated Model Change building blocks.

**approval.isModelChangeNotificationOn**

**Default:** False

### Enabled Event that Triggers a Notification

Specifies what events trigger a change notification.

**modelEvent.producer.fireEvent**

**Values:** Valid values include:

**Atomic**

Triggers an event after every approval during a workflow.

**Aggregate**

Triggers an event when all approvals complete for a workflow.

## Specify LDAP Authentication

When you enable LDAP authentication, the system authenticates users logging in to the Portal using the LDAP directory.

### **sage.security.disable.ADAuthentication**

**Default:** True

For LDAP authentication, set to false.

### **security.ldap.server**

Identifies the LDAP server name in your network.

**Default:** adserver

### **security.manager.dn**

The LDAP administrator username in your network.

**Default:** AD1\EAdmin

### **security.manager.password**

The LDAP administrator password in your network.

**Default:** eurekify

## System, Workflow and Task Parameters

The product exposes several types of parameters to Workpoint processes. Typically the product populates these parameters with values when it creates a Workpoint job.

- System parameters receive static values based on CA GovernanceMinder server system properties. These values are not unique to the workflow context. The `system.` prefix identifies these parameters.
- Workflow parameters receive unique local values based on the data set and other options in the business workflow context. For example, many settings in the certification creation wizard pass to Workpoint processes as workflow parameters. The `flow.` prefix identifies these parameters.



- Task parameters receive unique local values based on the workflow context. These values are necessary to complete the task associated with the Workpoint process. For example, the attributes that identify entities under review are necessary and specific to a link review task, and depend on the source configuration and data filters in the workflow context. The `task.` prefix identifies these parameters.

#### Examples: System, Workflow, and Task Parameters

The `RoleSuggestRole` process suggests new roles during a role certification campaign. This process declares the following parameters:

##### **certification.useApprovers**

Specifies which entities in a link under review generate reviewers. The value comes from the `certification.useApprovers` CA GovernanceMinder system property.

This value is not unique to the workflow, but applies to review tasks in all business workflows.

**Default:** 1,2

##### **flow.userApproval.userMembersList**

Specifies the member list that is used to assign reviewers for user entities.

This parameter reflects settings made by the user in the campaign creation wizard, and stored by the product in the workflow context. The *flow.* prefix indicates that it applies to *all* tasks of *this* workflow that review a user entity.

##### **task.personID**

Specifies the user in the link under review.

##### **task.roleName**

Specifies the role in the link under review.

These task parameters contain information *unique to this workflow task*. Other Workpoint jobs of the workflow reference other links in the campaign.

## Special Characters for Member Lists Properties

These system properties define special characters used to parse comma-separated values (CSV) files for member lists.

##### **memberlist.csv.reader.separator**

Defines the character that separates fields in each line of the file. The comma (,) character is used by default.

##### **memberlist.csv.reader.escape**

Defines the escape sequence used in the file. The backslash (\) character is used by default.

**memberlist.csv.reader.quotechar**

Defines the character that encloses field values that have spaces or other special characters. The double-quote (") character is used by default.

**Example: Backslash Characters in CSV Input**

Often CSV input for a member list contains backslash characters in pathnames, as in the following example:

```
Login, Category, Value
DOMAIN\Hector_Torres, ResName3, Solaris\HTorres
DOMAIN\Alex_Patrick, Location, Atlanta
```

By default, the CSV parser treats the backslash character as an escape character. The resulting member list omits backslashes, as follows:

```
Login, Category, Value
DOMAINHector_Torres, ResName3, SolarisHTorres
DOMAINAlex_Patrick, Location, Atlanta
```

To include the backslash character in field values, edit the `memberlist.csv.reader.escape` system property to define a different escape character.

**Note:** Select an escape character that does not appear in your data. Do not use the double quote character as an escape character.

## Define CA Identity Manager Thread Pool Size

Defines the thread pool size for an export to CA Identity Manager.

**connectors.im.export.thread.pool.size**

Default: 15

## Logout URL

Defines the web page to which users are sent when they log out of the CA GovernanceMinder Portal. For a page external to the CA GovernanceMinder Portal, specify the full URL of the page. For a page in the CA GovernanceMinder Portal, specify only the page name, and omit the host, port, and pathname of the portal.

**logout.landingPageUrl**

**Default:** loginForm

## Date Display

These properties define day, month, year, hour and minute display.

### Day, Month, and Year

Defines the CA GovernanceMinder format for the day, month, and year.

**format.onlyDate.display**

**Default:** dd/MM/yyyy

### Day, Month, Year, Hour and Minute

Defines the CA GovernanceMinder format for the day, month, year, hour and minute.

**format.date.display**

**Default:** dd/MM/yyyy HH:mm

## Define Workpoint Server Information

Defines the DNS and port information for Workpoint servers.

**java.naming.provider.url**

When there is a single server in your cluster, use the following:

**java.naming.provider.url=iiop://server:port**

If you have more than one server use:

**java.naming.provider.url=corbaloc:iiop: server1:port,; server2:port,; server3:port,; server4:port**

**Note:** *Port* is typically the application server Bootstrap port.

## Certification Rows Displayed

These properties describe the default displayed number of rows of a certification in a CA GovernanceMinder Home Portal page for an administrator and a business user.

**dashboard.officer.currentCertifications.visibleItems**

**Default:** Six

**dashboard.bu.currentCertifications.visibleItems**

**Default:** Six

## Information Bubble Properties

The following system properties have been added for information bubbles:

**tooltip.balloons.mouse.enabled**

When you focus on an object using the mouse or another input device, an information bubble automatically appears.

**Default:** True

**tooltip.balloons.onfocus.show.enabled**

When you focus on an object using the keyboard as a primary input device, an information bubble automatically appears.

**Default:** True

**tooltip.balloons.onfocus.show.delay**

Time delay for keyboard focus. The unit of measure is in milliseconds.

**Default:** 3000

**tooltip.balloons.onfocus.triggerKey**

Assign a keyboard trigger key for the keyboard information bubble.