CA Identity Governance

Client Tools Guide

12.6.02a

CA Technologies Product References

- This document references the following CA Technologies products:
- CA Identity Governance
- CA Identity Manager
- CA SiteMinder®
- CA User Activity Reporting
- CA SDM
- [assign the value for iamcs in your book]

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: Introduction

Implementing role-based systems on an enterprise level is a significant undertaking. Creating a role specification from scratch is complex. Porting various legacy specifications from existing systems is difficult due to different and incompatible environments and conventions. Dynamic corporate environments replete with periodic restructuring, mergers, relocation and flexible employee mobility all contribute to the problematic nature of maintaining a coherent role model.

This section contains the following topics:

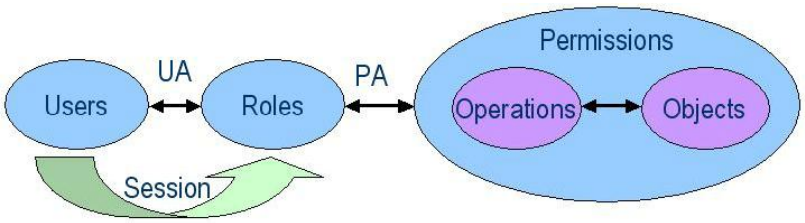
Audience

This guide is intended for Role Engineers who are responsible for the installation of CA Identity Governance software, downloading and uploading of users and resources databases, and role discovery and audit operations. Role Engineers are typically well-trained professionals who are familiar with the target organization. This guide assumes that the Role Engineer has had professional training on a CA Identity Governance system and is familiar with the CA Identity Governance documentation that accompanied the CA Identity Governance installation package.

Role Based Access Control (RBAC)

Role Based Access Control (RBAC) is a project of the National Institute of Standards and Technology (NIST) and is intended to create a comprehensive access security model for the structure and operation of enterprise-level organizations in a high technology environment. RBAC has now reached maturity and has been mandated or recommended for implementation by industry regulations worldwide.

In RBAC, users have roles that provide them with permissions to perform defined operations, such as read/write, and on objects, such as computer files. RBAC incorporates the principles of separation of duties and organizational hierarchy into its model. Separation of duties prohibits a user with a certain job function to serve in another job function at the same time. Hierarchy reflects the layered role structure of large organizations but also facilitates administration and role creation by allowing rights to flow down from senior to junior roles. The following diagram describes the RBAC model:



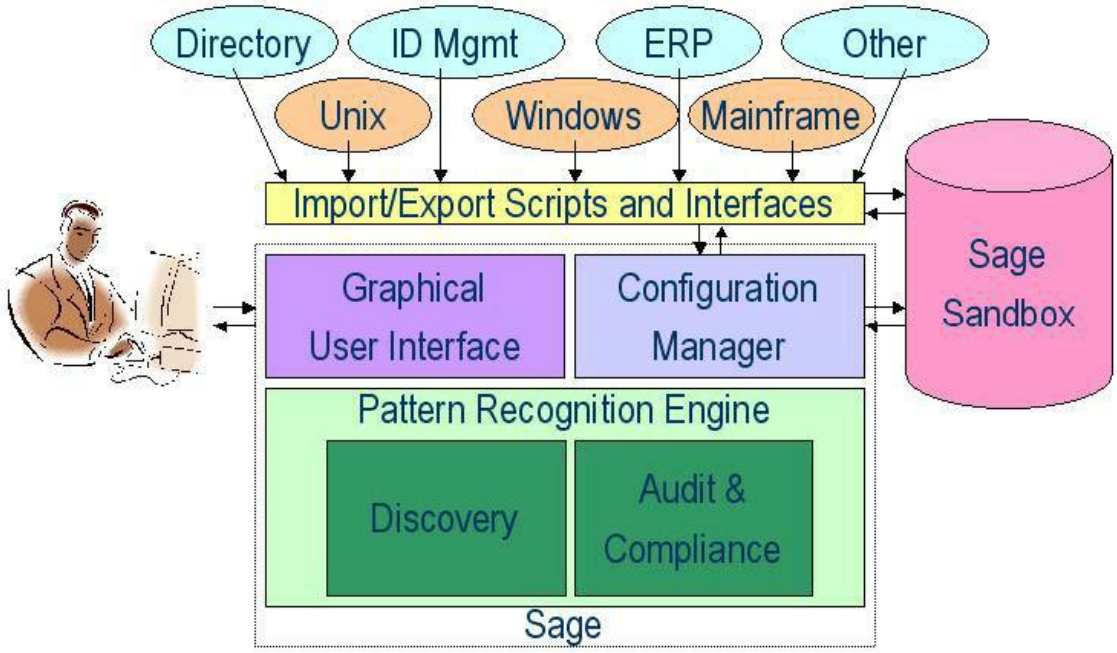
Basic Concepts and Architecture

CA Identity Governance implements RBAC standards without affecting an organization's on-going operation. CA Identity Governance implements the concept of a *sandbox* to separate CA Identity Governance's operation from the organization's on-going security environment (production server). The assumption is that when working with CA Identity Governance, existing access definitions must first be imported into a sandbox. A sandbox is an offline PC computer on which CA Identity Governance is installed where role discovery and audit activities are performed without affecting current operations of the organization. All work on discovering new or refining existing access definitions is performed in the CA Identity Governance environment.

CA Identity Governance defines *roles* as a group of users that have a common set of privileges. By *users*, CA Identity Governance refers to people or functions: employees, customers, suppliers, representatives, and so on. A *resource* is a specific right of access that may be an operation or object in formal RBAC terms. Thus, a resource can be as specific as a particular access right (Read/Write/Execute) to a specific file in a specific file system on a specific system, and it can also be used to provide a model for access to a computer system (such as, a user group on that system). A *privilege* is a connection between a user and a resource, indicating that this user possesses a specific access right. A role can include a set of users and a set of resources, with the semantics being that all users in the user set are allowed access to all resources in the resource set.

Most of CA Identity Governance's work is performed within a CA Identity Governance *configuration* that is automatically created when access data is imported into CA Identity Governance. By configuration, CA Identity Governance means a data structure that holds a snapshot of the definition of users, resources and roles (if already defined) and the relevant relationships (privileges) between them.

The following shows the CA Identity Governance architecture and how it relates to existing systems in your enterprise:



CA Identity Governance Technology

CA Identity Governance is based on advanced pattern recognition technology. CA Identity Governance provides a comprehensive set of highly sophisticated solutions to the challenges that organizations face when implementing and maintaining role-based management.

Core Technology

An important innovation of CA Identity Governance lies in the observation that role-based management revolves around patterns of privileges and access. As such, even in an organization where privileges are not currently managed by roles, the actual assignment of privileges roughly follows role-based patterns. Similarly, deviations and exceptions must be detectable when they do not follow the same patterns.

CA Identity Governance's technology is designed to uncover the patterns that are hidden in existing sets of privileges. These patterns are not trivial, because the number of excessive privileges can sometimes reach 50 percent of the total number of privileges. Many users can also be under-privileged or wrongly-privileged. Furthermore, the problem is complex due to the sheer number of user accounts typical of large enterprises. CA Identity Governance combines a set of pattern recognition techniques and other advanced algorithms and applies them to the special challenges of roles management.

Other Technology Components

In addition to this core technology, CA has developed substantial additional technology that is required to deploy a full solution:

- CA Identity Governance products use sophisticated algorithms that help the user make intelligent decisions, while hiding most of the complexity of the problems they address.
- CA Identity Governance products use sophisticated data structures and algorithms to reduce the CPU and memory load to the point where a CA Identity Governance project can be fully implemented on a single system.
- CA Identity Governance architecture is designed to allow easy mapping of privileges data from virtually any ACL-based platform/application, including most operating systems, databases, directories, applications, and identity management and provisioning systems.
- CA Identity Governance's user-friendly interface facilitates importing privilege data from a common or proprietary operating environment and exporting processed data and role definitions to this or another target operating environment.

Typical Processes

The following are the main processes when working with CA Identity Governance:

Import

In a typical implementation, the Role Engineer first imports current access data from the security administration server. Source documents would include a users database file, resources database file, roles file (if existing) and possibly one or more files describing the relationship between one or more entities (users, resources, roles). Using a direct communications link to the production server, CA Identity Governance enables the importing of data from many formats including: CSV, SQL, and RACF. CA Identity Governance creates its own CA Identity Governance “configuration” document, which contains the known user, role, and resource information.

Role Discovery

The role discovery process enables the discovery of roles that were not explicitly defined in the source data and the refining of existing roles. CA Identity Governance's role discovery tools include searching for and proposing basic roles, obvious roles, roles that are almost perfect matches of other roles, and identifying role hierarchy. These options contain sub-menus that enable fine-tuning CA Identity Governance's discovery algorithm to adapt it to the specific configuration that is being analyzed. The results of running these CA Identity Governance options are CA Identity Governance's proposals for role definitions. These roles are individually examined to determine their appropriateness and validity for the organization.

Audit

CA Identity Governance's basic auditing tools apply CA Identity Governance's internal logic and built-in algorithms to an existing configuration to analyze and identify many types of non-conformities or suspicions related to users, roles, and resources. The Role Engineer can apply individual tools to analyze a configuration or can run a comprehensive audit. The output of an audit is the AuditCard, which contains a list of all suspicious records and the type of suspicion involved (currently about 50 different types). The AuditCard also contains a built-in mechanism for tracking progress until resolution is achieved.

CA Identity Governance Policy Compliance

The CA Identity Governance Policy Compliance module is an additional audit tool that enables formulating a unique set of Business Process Rules (BPR) that represent various constraints on privileges. These rules are formulated independently of a specific CA Identity Governance configuration and can then be applied to different configurations.

Export

Before uploading a processed CA Identity Governance configuration to the organization's production server, the differences between the original source data and processed CA Identity Governance configuration are examined using a built-in CA Identity Governance option. After verifying the differences and making any necessary changes, the configuration data is directly exported from the CA Identity Governance interface to the production computer's format. The export eliminates cross-platform conversion problems.

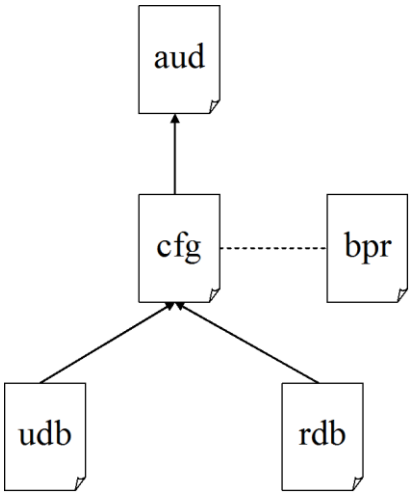
Chapter 2: CA Identity Governance Client Tools

This chapter provides an overview of the CA Identity Governance client tool interface.

This section contains the following topics:

File Types in CA Identity Governance

CA Identity Governance uses the following file types, as illustrated in the following diagram:



Users database file (udb)

Contains one entry for each user that participates in any of our analyses. This entry usually contains such information as the user name, organizational unit (possibly in various levels), job description/code, status (internal/external, current/past employee), and so on), reporting structure, location (also possibly hierarchical, and so on). Typically, much of this information is brought from an HR system of some sort. Each user is identified by a unique ID called PersonID. The users database does not contain information about the user's privileges - this is the subject of our analyses and possible restructuring, and is therefore part of the configuration.

Resources database file (rdb)

Complements the udb file, and contains one entry for each resource. A resource can be anything that a user may need access to, for example, a user group on a specific operating environment or application, access level to a certain file or share, permission to perform a transaction, and so on. The granularity in which resources are analyzed is up to the role engineer, and may vary. Furthermore, it is possible to perform different levels of analysis on the same set of systems.

The udb and rdb are relatively static and serve as the basis for possibly many configurations.

Configuration file (cfg)

Represents a snapshot of privileges and role definitions. As such, the configuration includes information about roles – the third type of CA Identity Governance entity, and also about the four types of CA Identity Governance connections:

user to resource

Represents a direct privilege of a user on a resource

user to role

Represents a user's membership in the role

role to resource

Represents the permission of all of the role's users to the given resources

role to role

Represents a role hierarchy relationship, whereby users who are members of a parent role are automatically members of the sub-role, and therefore privileged to all of the sub-role's privileges.

Note: A configuration depends on its udb and rdb, but not all users/resources in the udb/rdb are necessarily included in a given configuration. Configurations that contain only a portion of the users/resources, for example, only the users of a certain organizational unit, are called partial configurations. There can be many configurations, representing various views, and using same udb and rdb.

AuditCard file (aud)

Contains a set of alerts that were generated for a specific configuration at a specific time. The alerts can be generated using any of the CA Identity Governance auditing mechanisms. The AuditCard can then be updated and modified as part of the alert tracking process.

Policy file (bpr)

Contains a set of business process rules that can be used to audit one or more configurations. Each rule is typically a business constraint, such as "people that do X cannot do Y", or "only people that have a skill A can do B". Another common example of business process rules is segregation of duty principles, which restrict the ability of users to perform sensitive and critical tasks on their own without the involvement of other users. Policies are loosely tied to configurations, because same policy can be applied to multiple configurations and multiple policies can be applied to a single configuration. The result of applying one or more policies to a configuration is an AuditCard with the relevant violations as alerts.

User Interface

Use Client Tools to perform discovery and analysis operations on CA Identity Governance data. To view the sample data files in Client Tools, open the sample configuration file included with your installation.

Follow these steps:

1. Start the CA Identity Governance Client Tools by clicking the Client Tools icon on your desktop.
2. Go to File, Open from File.
3. Browse to the **\Sage Demo** folder under the installation directory. Select the **ConfigWithRoles.cfg** file.

   The program opens the.cfg file in the configuration window. When a configuration file is open, three panels are displayed. Each panel shows a different part of the data that comprises a configuration: Users (left panel), Roles (middle panel), and Resources (right panel).

   Note: By default, the configuration window displays three vertical panels. You can change the display mode to vertical panels, tabs, or horizontal panels using the View menu.
4. You can open several files simultaneously in the main window: configuration files (.cfg), users database (.udb), resources database (.rdb), auditing cards (.aud) and policies (.bpr). The menu bar and toolbar expand to include available options relevant to the type of data files that is active.

Menu Bar

The menu bar provides access to most client tools options. The menu bar is functionally organized and includes the following main items:

- File
- View
- Import
- Export
- Management
- Help

Some menu bar items contain submenus with additional options. To avoid navigating complex menu systems, the most commonly-used options are represented by icons on the toolbar. However, not all options are included on the menu bar or toolbar. Some options can only be accessed by activating the right-click menu controls.

More information:

Tool Bar and Shortcut Key Combinations (see page 23)
Context Menus (see page 25)

File Menu

The File menu contains the options for file handling as well as connecting to external systems and peripheral equipment.

View Menu

The View menu provides the following functions:

- Determine how data is displayed in the active document window
- Review the log file generated by the client tools, to look for possible errors that were encountered during operation
- Review properties and statistics for the active document window
- Switch view to a related document, such as, the udb of the current configuration
- Explore connections of a select set of entities

Management Menu

The Management menu provides the main role engineering options. This menu is available only when the active document is a configuration. Role discovery and refining are the main tasks that the Role Engineer performs once the configuration is ready for analysis. The main functions available here are:

- Various methodologies for bottom-up and top-down role engineering
- Functions for refinement of new role definitions and/or of existing ones

Audit

The Audit menu provides review and auditing functions:

- Pattern-based auditing
- Compliance auditing, based on policies (BPR)
- Review of current roles
- Search for suspected users, resources, and role definitions

Tool Bar and Shortcut Key Combinations

Toolbar icons and shortcut key combinations are available for performing frequently-used activities. Their option is the same as their corresponding menu bar counterparts.

Icon	Description	Shortcut
	New file	Ctrl + N
	Open file	Ctrl + O
	Save current file	Ctrl + S
	Copy	Ctrl + C
	Paste	Ctrl + V
	Print file	Ctrl + P
	Print Preview	-
	Audit Cards	-
	Users Database	Ctrl + U

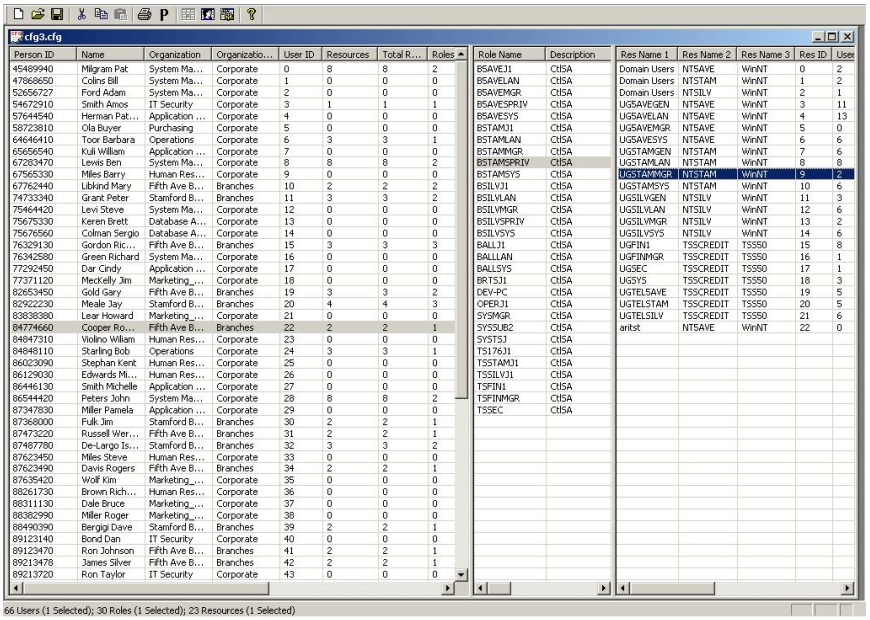
Icon	Description	Shortcut
	Resources Database	Ctrl + R
	About Discovery	-
-	Compare Configurations	Ctrl + D
-	Undo	Ctrl + Z
-	Audit Card Generation and Management	Ctrl + T
-	Policy Compliance Check	Ctrl + B
-	Select All	Ctrl + A

Configuration Window

When a configuration is opened, a three-panel window appears containing individual user data in the Users Panel, physical resources data in the Resources Panel and roles data; that is, the link between users and resources, in the Roles Panel.

Users, Resources, Roles Panels

The following graphic shows a typical Configuration window.



The data displayed in the User and Resources Panels are taken from the respective users and resources databases. The type of data (fields) displayed are determined by the Role Engineer. Similarly, roles data in the Roles Panel are also determined by the Role Engineer. Each panel enables scrolling horizontally to view attributes and counters, which are used in the role engineering and role audit process. Some attributes are self-configured by the user. Each column can be used to sort the panel.

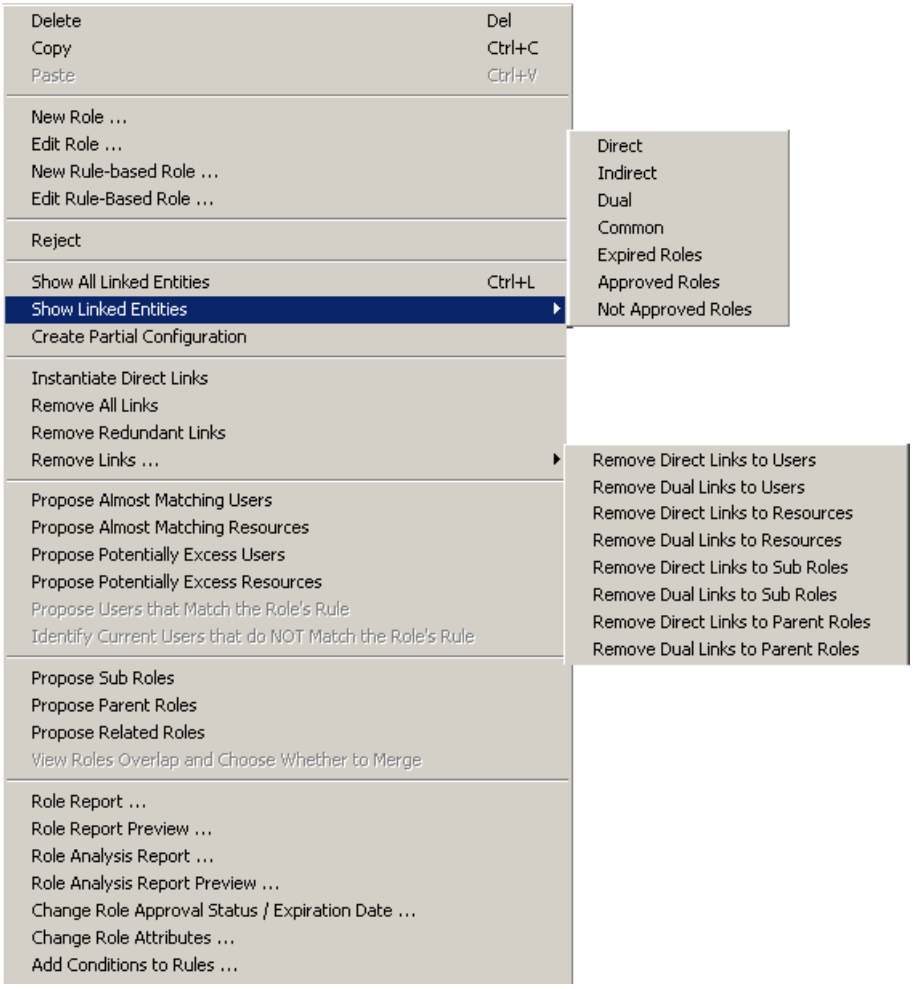
Context Menus

To access role engineering controls quickly in the configuration windows, each of the panels has its own context menu that shows the most most common options relevant to that panel.

To view a context menu, use the right-click mouse operation.

Roles Panel

The following Roles Panel context menu controls are available:



The following table provides a brief description of each control as well as a reference to a more detailed discussion below in this guide. Note that some items do not have menu bar counterparts.

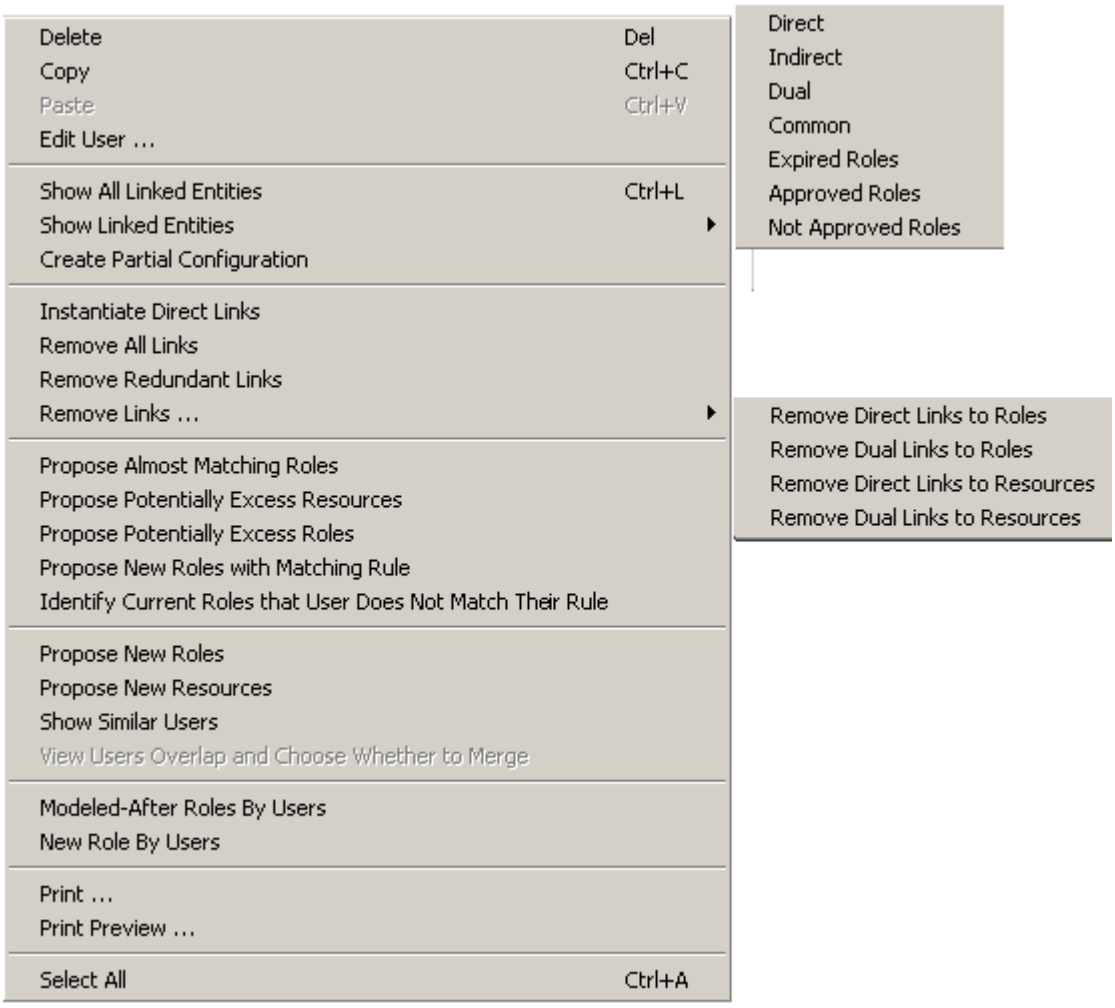
Roles Panel Context Menu	Menu Bar Location	Shortcut	Description in Section
Delete	Edit	Del	Delete (see page 61)
Copy	Edit	Ctrl + C	Copy (see page 63)
Paste	Edit	Ctrl + V	Paste (see page 63)
New Role...	Edit		New Role (Configuration Only) (see page 69)

Roles Panel Context Menu	Menu Bar Location	Shortcut	Description in Section
Edit Role…	Edit		Edit Role (see page 76)
New Rule-based Role…	Edit		New Rule-Based Role (see page 73)
Edit Rule-based Role…	Edit	-	Edit Rule-Based Role (see page 74)
Reject	Discovery	-	Rejecting Discovered Roles (see page 119)
Show All Linked Entries	View	Ctrl + L	
Show Linked Entries: Direct, Indirect, Dual, Common, Expired Roles, Approved Roles, Not Approved Roles.	View	-	Show Linked Entities (see page 97)
Create Partial Configuration	Edit	-	Create Partial Configuration (see page 64)
Instantiate Direct Links	Edit, Manage Links	-	Instantiate Direct Links (see page 80)
Remove All Links	Edit, Manage Links	-	Remove All Links (see page 81)
Remove Redundant Links	Edit, Manage Links	-	Remove Redundant Links (see page 80)
Remove Links… Remove Direct Links to Users Remove Dual Links to Users Remove Direct Links to Resources Remove Dual Links to Resources Remove Direct Links to Sub Roles Remove Dual Links to Sub Roles Remove Direct Links to Parent Roles Remove Dual Links to Parent Roles	Edit>Manage Links	-	Manage Links (Configuration Only) (see page 80)
Propose Almost Matching Users	Discovery, Identify Almost Perfect Matches	-	Propose Closely Matching Users (see page 112)
Propose Almost Matching Resources	Discovery, Identify Almost Perfect Matches	-	Propose Closely Matching Resources (see page 113)
Propose Potentially Excess Users	Audit, Identify Excess Privileges	-	Propose Potentially Excess Users (see page 130)

Roles Panel Context Menu	Menu Bar Location	Shortcut	Description in Section
Propose Potentially Excess Resources	Audit, Identify Excess Privileges	-	Propose Potentially Excess Resources (see page 132)
Propose Users that Match the Role's Rule	-		
Identify Current Users that do Not Match the Role's Rule	-		
Propose Sub Roles	Discovery, Identify Role Hierarchy	-	Propose Sub Roles (see page 117)
Propose Parent Roles	Discovery, Identify Role Hierarchy	-	Propose Parent Roles (see page 99)
Propose Related Roles	Discovery, Identify Role Hierarchy	-	Propose Related Roles (see page 119)
View Roles Overlap and Choose Whether to Merge	-	-	View Roles Overlap (Configuration Only) (see page 98)
Role Report	Entity Report	-	Role Analysis Report (see page 122)
Role Report Preview	Entity Report Preview	-	
Role Analysis Report	Role Analysis Report	-	
Role Analysis Report Preview	Role Analysis Report Preview	-	
Change Role Approval Status/Expiration Date…	-		
Change Role Attributes	-		
Add Conditions to Rules	-		
Select All	-	Ctrl + A	Select All (see page 35)

Users Panel

The following Users Panel context menu controls are available.



The following table provides a brief description of each control as well as a reference to a more detailed discussion later in this guide. Some items do not have menu bar counterparts.

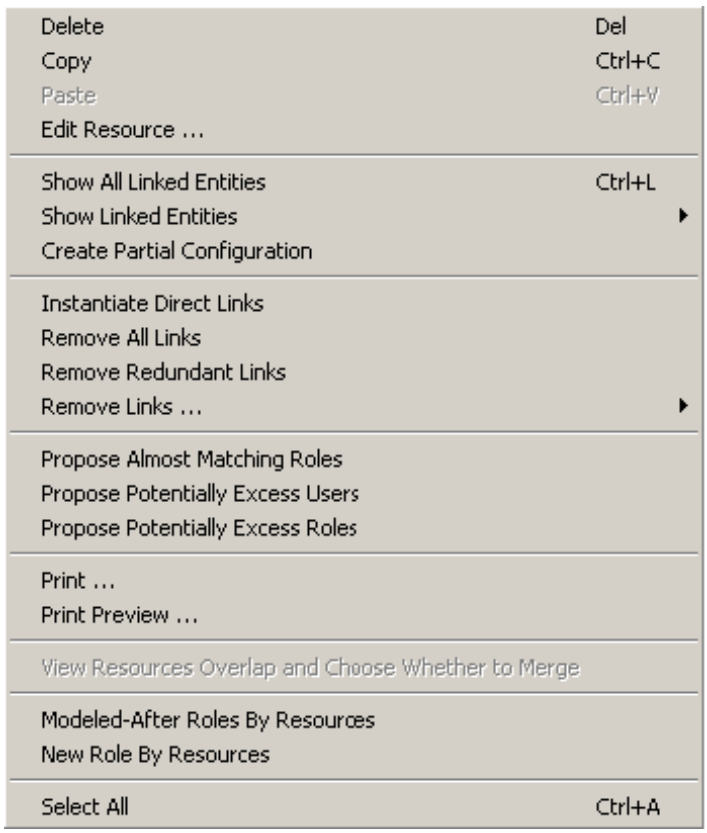
Users Panel Context Menu Option	Menu Bar Location	Shortcut	Refer to
Delete	Edit	Del	Delete (see page 61)
Copy	Edit	Ctrl + C	Copy (see page 63)
Paste	Edit	Ctrl + V	Paste (see page 63)
Edit User	Edit	-	Edit User (see page 75)

Users Panel Context Menu Option	Menu Bar Location	Shortcut	Refer to
Show All Linked Entries	View		Show Linked Entities (see page 97)
Show Linked Entries: Direct, Indirect, Dual, Common, Expired Roles, Approved Roles, Not Approved Roles.	View	-	View Roles Overlap (Configuration Only) (see page 98)
Create Partial Configuration	Edit	-	Create Partial Configuration (see page 64)
Instantiate Direct Links	Edit, Manage Links		Instantiate Direct Links (see page 80)
Remove All Links	Edit, Manage Links		Remove All Links (see page 81)
Remove Redundant Links	Edit, Manage Links	-	Remove Redundant Links (see page 80)
Remove Links: Remove Direct Links to Roles Remove Dual Links to Roles Remove Direct Links to Resources Remove Dual Links to Resources.	Edit, Manage Links	-	Manage Links (Configuration Only) (see page 80)
Propose Almost Matching Roles	Discovery, Identify Almost Perfect Matches	-	Identify Almost Perfect Matches (see page 111)
Propose Potentially Excess Resources	Audit, Identify Excess Privileges	-	Propose Potentially Excess Resources (see page 132)
Propose Potentially Excess Roles	Audit, Identify Excess Privileges	-	Propose Potentially Excess Roles (see page 131)
Propose New Roles with Matching Rule	Discovery		
Identify Current Roles that User Does Not Match Their Rule	Discovery		
Propose New Roles	-	-	Propose New Roles (see page 132)
Propose New Resources	-	-	Propose New Resources (see page 133)
Show Similar Users	-	-	Show Similar Users (see page 133)

Users Panel Context Menu Option	Menu Bar Location	Shortcut	Refer to
View Users Overlap and Choose Whether to Merge	-	-	View Resources Overlap – Choose Whether to Merge (see page 101)
Modeled After Roles by Users	Discovery	-	Discovering Characteristic Roles (see page 106)
New Role by Users			
Print	File	-	Printing Reports (see page 120)
Print Preview	File	-	Print Preview (see page 121)
Select All	-	Ctrl + A	Select All (see page 35)

Resources Panel

The following Resources Panel context menu controls are available.



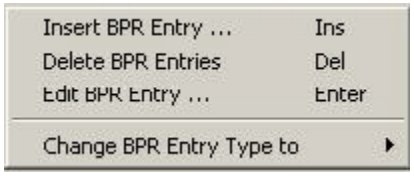
The following table provides a brief description of each control as well as a reference to a more detailed discussion below in this guide.

Resources Panel Context Menu Option	Menu Bar Location	Shortcut	Description in Section
Delete	Edit	Ctrl + X	Delete (see page 61)
Copy	Edit	Ctrl + C	Copy (see page 63)
Paste	Edit	Ctrl + V	Paste (see page 63)
Edit Resource…	Edit	-	Edit Resource (see page 79)
Show All Linked Entities		Ctrl + L	
Show Linked Entries	View	-	Show Linked Entities (see page 97)
Create Partial Configuration	Edit	-	Create Partial Configuration (see page 64)
Instantiate Direct Links	Edit, Manage Links	-	Instantiate Direct Links (see page 80)
Remove All Links	Edit, Manage Links	-	Remove All Links (see page 81)
Remove Redundant Links	Edit, Manage Links	-	Remove Redundant Links (see page 80)
Remove Links	Edit, Manage Links	-	Manage Links (Configuration Only) (see page 80)
Propose Almost Matching Roles	Discovery, Identify Almost Perfect Matches	-	
Propose Potentially Excess Users	Audit, Identify Excess Privileges	-	Propose Potentially Excess Users (see page 130)
Propose Potentially Excess Roles	Audit, Identify Excess Privileges	-	Propose Potentially Excess Roles (see page 131)
Print	-	-	Printing Reports (see page 120)
Print Preview	-	-	Print Preview (see page 121)

Resources Panel Context Menu Option	Menu Bar Location	Shortcut	Description in Section
View Resources Overlap and Choose Whether to Merge	-	-	View Resources Overlap – Choose Whether to Merge (see page 101)
Modeled-After Roles By Resources	Discovery	-	Discovering Modeled-After Roles (see page 110)
New Role By Resources			
Select All	-	Ctrl + A	Select All (see page 79)

Business Policy Rules - Context Menu

The following is a sample of the context menu in the business Policy document window (working with Policy windows is described in chapter 10).

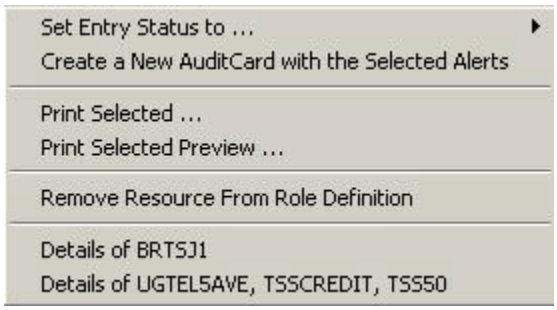


The following right-click controls enable you to edit BPR entries:

BPR Panel Context Menu Options	Menu Bar Location	Shortcut	Description in Section
Insert BPR Entry	Edit	Ins	Add BPR Entry (BPR Only) (see page 89)
Delete BPR Entry	Edit	Del	Delete BPR Entry (BPR Only) (see page 89)
Edit BPR Entry	Edit	Enter	Edit BPR Entry (BPR Only) (see page 89)
Change BPR Entry Type to	-	-	

AuditCard - Context Menu

The following is a sample AuditCard with the context menu open. The displayed options may vary slightly depending on the highlighted AuditCard record.



The following context menu options enable you to edit AuditCard records and print selected records:

AuditCard Context Menu Options	Menu Bar Location	Shortcut	Description in Section
Set Entry Status To	-	-	Set Entry Status To (see page 145)
Create a New AuditCard with the Selected Alerts	-	-	Create a New AuditCard with the Selected Alerts (see page 145)
Print Selected	-	-	Print Selected (see page 123)
Print Selected Preview	-	-	Print Selected Preview (see page 123)

Drag and Drop Cursor Symbols

When moving records between windows, the cursor changes shape to indicate the type of activity being performed. For example, when a configuration record is being dragged from one configuration window to another, the cursor changes from ⊖ (indicating the record is being moved) to LINK (indicating the record has left its location) to ADD (before the record is actually dropped in its new location).

You are prompted for user confirmation to complete the action.

Select All

The configuration panels contain long lists of entities, users, roles and resources. When it is necessary to perform an activity that involves all records in the panel, the Select All option is useful for selecting the entire panel. This option is activated by right-clicking the mouse on the desired panel and selecting Select All or by using the Ctrl+A shortcut key combination.

Chapter 3: Working with Privileges Data

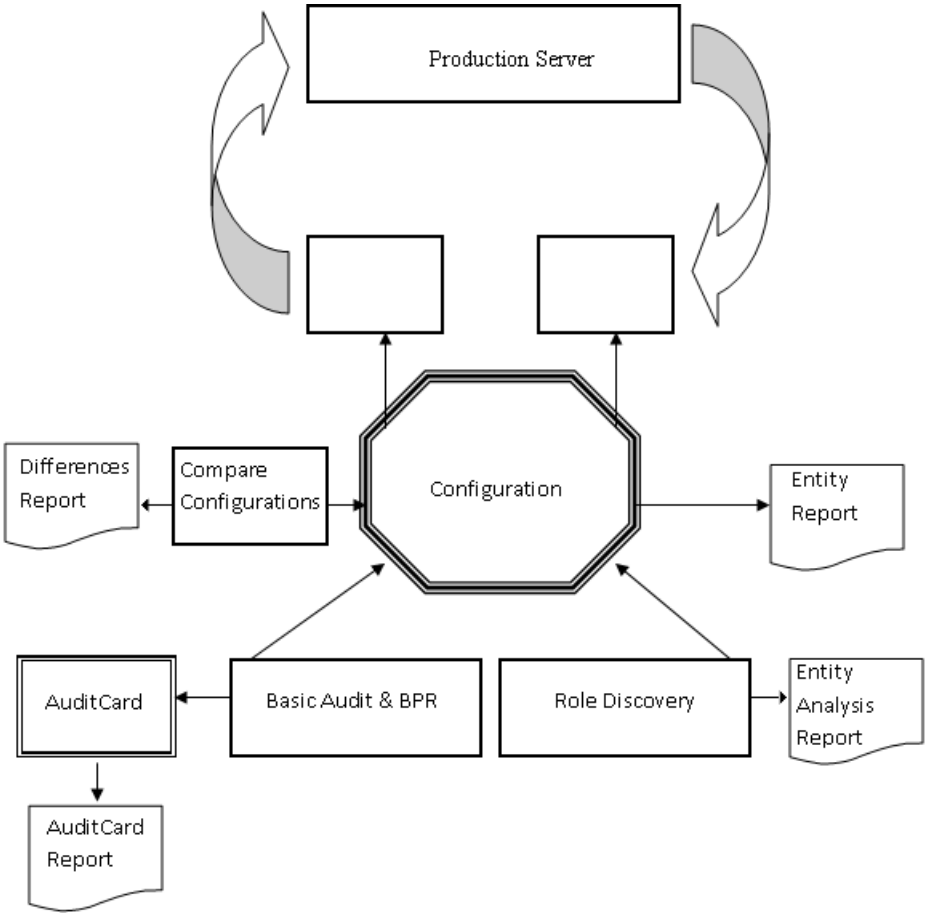
You can generate comprehensive printed reports at each stage of the workflow. Options are functionally organized on the menu bar, and right-click control menus enable the selection of context-sensitive options.

This is an overview of the typical workflow processes, with a description of the entire process, from importing data, through role discovery and audit to exporting processed data back to the production server. Appropriate reference is provided, where necessary, to more detailed descriptions of key processes in this guide. For example, the import and export processes is described here in a general way, but these procedures are described in detail in the appendixes, depending on specific production servers.

This section contains the following topics:

Workflow

The following diagram describes a typical installation:



Importing Source Data

You can import production files using the Import option on the menu bar. This option enables you to import Active Directory, CSV, RACF, or SQL files by creating a communication link to the downloading (production) server. CA Identity Governance database files are simple text files. Converters verify that imported files adhere to CA Identity Governance file format rules.

Typically, source documents include a users database file, a resources database file, a roles file (if existing), and possibly one or more files describing the relationship between one or more entities (users, resources, roles). These relationships can be any or all of the following: user-resource, role-resource, user-role, role-role. Sometimes, it is necessary for the Role Engineer to manipulate or extend the source files using a tool such as Excel.

The output of the conversion process is a CA Identity Governance configuration document (CFG file), which is the basis for the role discovery process.

Discovery of Roles

When user, resource, and roles data (if available) is imported into CA Identity Governance, it is converted into a configuration document. Then, CA Identity Governance can analyze the data and implied relationships (connections) in the downloaded data to determine roles. A role defines a relationship that exists between users, resources, or other roles. Certain roles can imply access to resources that are not immediately apparent. For example, a hierarchical relationship can mean that a user possessing a certain role can access resources that are not defined as belonging to them, or not even in their own physical area of operation. In addition, because of employment circumstances, some employees (users) may acquire too many resources, or some resources may be improperly allocated to them. The client tools analyze and propose roles identify both a specific role phenomenon or many role phenomena at the same time.

These role discovery tools are contained in the Discovery menu option on the menu bar.

Role discovery options include searching for and proposing basic roles, obvious roles, roles that are almost perfect matches of other roles, and identifying role hierarchy. These options contain sub-menus that enable fine-tuning the discovery algorithm to adapt it to the specific configuration that is being analyzed. The user should experiment with these tools and the thresholds that they contain to determine the best tools for the particular configuration. The results of running these options are only proposals for role definitions. These roles must be examined by the Role Engineer to determine their appropriateness and validity for the organization.

An Entity Report is generated from the Management menu when a configuration window is active. It shows basic data including direct resources, sub-roles and parent roles. A report of any single or several highlighted entities can be printed in report form. These printed reports can be sent to other company officials to obtain their comments on the discovered roles or as part of on-going organizational activities.

More information:

Entity Report (see page 121)

Pattern-based Auditing

Auditing is a process performed on an existing configuration to locate erroneous privileges and other deviations from policies. The client tools contains two auditing modules: a basic role-based auditing module and a policy compliance module. This section discussed basic role-based auditing; policy compliance is discussed afterward.

Basic auditing tools apply internal logic and in-built algorithms to an existing configuration to analyze and identify many types of non-conformities or suspicions related to users, roles, and resources (currently about 50 different types). These tools can be individually applied to produce a limited number of suspicion types such as: collectors (users with too many resources), collectibles (resources with too many users), suspect roles, excess privileges for an individual entity. After identifying problematic entities, the Role Engineer can correct them and run the tool again to verify that the problem has been solved. In this manner, individual tools can be used “interactively” during the audit process.

In addition, an audit can be comprehensive and include many types of suspicions for many configuration records. In this case, an AuditCard is generated listing all suspicious records and the type of suspicion involved. The AuditCard contains a built-in mechanism for tracking progress in resolving the suspicion until resolution is achieved. In addition, this AuditCard can be printed.

Note: Role discovery tools can also be used as auditing tools and role discovery results can be the basis for determining comprehensive audits. Auditing tools can be run immediately after role discovery and verification has been performed to double-check, or periodically after inevitable changes on the production server (after downloading updated data), or as part of a comprehensive audit of the organization.

More information:

Audit Menu (see page 125)
AuditCard Report (see page 123)

Policy Compliance Check

The Policy Compliance module enables system administrators, business managers, and auditors to formulate sets of business constraints and segregation of duty principles using Business Policy Rules (BPRs). These rules are formulated independently of a specific configuration and can then be applied to different configurations. Thus, the Policy Compliance module augments the Pattern-Based Auditing capabilities with a new and powerful compliance verification and documentation tool.

The BPR Compliance module is accessed from the Audit menu option on the menu bar.

More information:

Check Policy Compliance (see page 149)

Exporting Configuration Data

After applying role discovery and auditing tools to users, roles and resources data and verification and correction where necessary, the data is almost ready for uploading (export) to the production server.

As mentioned, a typical process involves downloading resource, role, and user data from the external computer of an organization and performing role discovery and audit on those files using the client tools. The Compare Configurations option in the Management menu compares the original configuration imported from the external computer to the post-role discovery and audit configuration. The Role Engineer then examines the differences to verify that any changes to the databases are indeed correct and meet requirements. The Compare Configurations option is located in File, Compare Configurations on the menu bar.

Finally, the new users and resources databases are uploaded to the external computer and the original databases of the external computer are updated.

Chapter 4: File Menu

The File menu includes basic file handling options as well as options for connectivity with external systems and peripherals (printers). Connection with external systems is important for downloading and uploading access data and for backup purposes.

This section contains the following topics:

New

You can create a new file of one of the following types: configuration (.cfg), user database (.udb), resource database (.rdb), AuditCard (.aud), Business Policy (.bpr).

To create a new file, click File, New, select the appropriate radio button, and click OK.

New Configuration

It is customary to import external users and resources information, from which CA Identity Governance builds a configuration file, by downloading it from an external computer. However, you can also open a new configuration file from scratch. This option creates a new configuration containing users and resources (all users and resources, if the option is selected) without the links between them.

Note: To build a new configuration file, it is first necessary to prepare a Users Database and Resources Database in the appropriate formats.

To create a new configuration

1. Activate the appropriate radio button in the Choose Open File Type window, and click OK.

   The New Configuration window appears.

2. Insert the following data in the fields:

   Users Database File

   Defines the pathname of the users database file. Use the Browse button to locate the file.

Resources Database File

Defines the pathname of the resources database file. Use the Browse button to locate the file.

Include All Users

Check this option to insert all records in the users database into the new configuration. Uncheck this option to create the configuration without any users, and add a selected subset of users to the configuration later.

Include All Resources

Check this option to insert all records in the resources database into the new configuration. Uncheck this option to create the configuration without any resources, and add a selected subset of resources to the configuration later.

The Open button becomes active after the path to the Users Database and Resources Database files are filled in.

3. Click Open to create the configuration file.

   A new configuration is generated in a new window. The Roles panel of the configuration is empty.

   CA Identity Governance designates the new configuration with a new default name. Note that the Users Panel and the Resources Panel contain data, and the columns contain the appropriate titles. The Roles Panel is empty. The Role Engineer can implement discovery and audit procedures to generate roles.

More information:

Role Discovery (see page 103)
Audit Menu (see page 125)
New Users Database (see page 44)
New Resources Database (see page 45)

New Users Database

This option enables the Role Engineer to create a new users database from scratch. To create a new users database, activate the appropriate radio button in the Choose Open File Type window, and click OK.

CA Identity Governance creates the new users database with default field names. Note that the typical Users Database contains one key field (Person ID) and a User ID field which is generated by CA Identity Governance. The other fields are optional and the names of the fields can be changed by the Role Engineer.

New Resources Database

This option enables the Role Engineer to create a new resources database from scratch. To create a new resources database, activate the appropriate radio button in the Choose Open File Type window, and click OK.

CA Identity Governance creates the new resources database with default field names. Note that the typical Resources Database contains three key fields (Res Name 1, 2, 3), which together comprise a unique key of the specific resource. The Res ID field is generated by CA Identity Governance. The other fields are optional, and the names of the fields can be changed by the Role Engineer.

New AuditCard

This option enables the Role Engineer to create a new resources database from scratch. Since AuditCards are based on configurations, it is necessary for a configuration to be open before a new (blank) AuditCard can be created.

To create a new AuditCard

1. Open the configuration on which to base the AuditCard.
2. Activate the appropriate radio button in the Choose Open File Type window.
3. Click OK.

   An audit card window appears.

More information:

Generate and Manage AuditCards (see page 134)

New Business Policy

This option opens a new blank Business Policy document, which is the first step in creating a Business Policy document, consisting of Business Policy Rules (BPR). The Business Policy Compliance module enables running a defined set of business constraints and segregation of duty rules against one or more configurations. This feature contrasts with the Audit engine, which runs pre-determined rules on the current configuration.

More information:

Audit Menu (see page 125)
Check Policy Compliance (see page 149)

Open From File

You may often need to open a configuration file (.cfg) for discovery and audit purposes. In addition, you can open other file types: user database files (.udb), resource database files (.rdb), AuditCards (.aud) and policy files (.bpr).

Click File, Open from File and specify the file type you want to open. By default, files of that type that are located in the default (installation) folder appear. Select the file you want to open (file name will be displayed in the File Name field). Click Open to continue.

Open from Database

This option enables modification of database files directly on the production server without the need to create intermediary files or to import database files, which would otherwise involve the stages of import, processing, and export back to the production computer. This option is useful for implementing simple changes on the production server.

It can be used only *after* files had been imported and exported back to the production server. It is only after export of files to the production server that required files are created on the target server.

By working on the production server, the Role Engineer has essentially waived the inherent protection of the sandbox principle. Extreme care should be taken when working directly on a production server. Only minor changes should be performed using this option.

Note: Before attempting to run the CA Identity Governance Database Wizard, verify that your connection to the remote computer is working.

To open from a database

1. Select Open from Database on the menu bar.

   The Database Wizard appears.

2. Fill in the following information in the Database Wizard window.

   Type

   Specifies the type of database data that you are downloading.

   Server

   Defines the remote server's IP address.

   Database

   Defines the database file name on the remote computer

Windows Authentication

Select this option to access the MS SQL server using the current user's Username and Password that is associated with Windows operating system.

User Name, Password

Defines credentials to access the database host

3. Click Next to continue to the next screen in the wizard.
4. Choose the file type from the list and file name from the list of files. If you have saved a configuration on the production server, you can work directly in that configuration.
5. Click Next to finish the procedure and begin working.

More information:

File Formats in CA Identity Governance (see page 241)

Review a Database

Each CA Identity Governance data Universe can contain various files that include: Configuration files, User Database files, Resource Database files, Audit Card files, and Business Policy files.

To review and manage the database files

1. Click File, Review Database.

   The Database wizard opens.
2. Click Source Database and fill in the fields as described in section Open from Database (see page 46).
3. Click Next.

   The Choose a Document to Open window appears.
4. Select a Database file type from the Document Type drop-down list.

   Database files of the selected type are listed in the file list.
5. Select the file that you want to review.
6. (Optional) Check the Logged checkbox.

   Changes to data entities in the file are recorded in the Transaction log on the CA Identity Governance server.

7. (Optional) Check the Write Protected checkbox.

   You cannot make changes to the file using CA Identity Governance client applications.

   Note: The file can still be modified by CA Identity Governance web services and by processes of the CA Identity Governance portal.

8. Click Open, Rename, or Delete.

Execute Batch File

When importing a large volume of data (which could involve several gigabytes in several source files), processing can take many hours. Therefore, a batch processing option enables processing during off-hours in accordance with a predetermined order defined by the Role Engineer.

The following list shows the typical order of commands in a batch file:

1. IMPORT RACF
2. IMPORT CSV
3. MERGE CFG
4. ENRICH UDB
5. ENRICH RDB
6. FILTER CFG

The format for batch file executions is an XML file format, which must follow XML file rules. The file extension must be .sbt.

To run the batch file from a Microsoft Windows command prompt, execute the file using the following format:

`EurekifySageDNA-V32.exe` *`SBT_file_name`*

For example, EurekifySageDNA-V32.exe merge.sbt.

Alternatively, you can run the batch file by selecting Execute Batch File from the File menu.

Note: For more information about running batch files, see the *Programming Guide*.

Print Setup

The File menu contains a number of Print and Printer Options.

More information:

Print Reports (see page 120)

General Settings

At the beginning of your project, you can set a variety of general settings.

Click File, General Settings to open a pane with the following tabs:

- Logging
- SQL Connectivity
- Presentation
- Print Fonts
- Files
- Discovery & Audit

Logging

Parameters set on the Logging tab allow you to assign the destination in which to save the log files. You choose to save the log files to a specific folder, the SQL Database or both. If you do not specify any destination for saving the log files then CA Identity Governance does not save the log file data at all.

To set logging options

1. Click File, General Settings.

   The Discover and Audit Settings window opens.
2. Select the Logging tab.
3. In the Logging Options section, specify the events that are logged.
4. In the Logging Directory section, browse to specify the pathname for log files.
5. (Optional) Select the Remove Logs Older Than option and specify a time period.

   Older log files are automatically purged.

Configure Database Connection Details

Use the SQL Connectivity tab to configure the connection to the CA Identity Governance databases. You must connect to these databases to use the Open from Database and Save to Database functions.

Note: Use this tab even when an Oracle server hosts CA Identity Governance databases.

To configure database connection details

1. From the main menu, click File, General Settings.

   The Settings dialog appears.

2. Click the SQL Connectivity tab.

3. Select a connectivity mode:

   - In implementations that include a CA Identity Governance server that also interacts with the CA Identity Governance databases, select the Request SQL Credentials from a server option.

     Note: When a CA Identity Governance server instance is in your environment, you *must* select this option.

   - In implementations without a CA Identity Governance server, select the Use static SQL credentials (see page 50) option.

4. Enter values in the fields as indicated.

5. (Optional) Select the Bulk Insert option (see page 52) to write data to a temporary SQL file. This option speeds the save process.

6. Click Apply.

Configure Direct Client Connection to Databases

In implementations that **do not** include a CA Identity Governance server, configure your client applications to work directly with the database server.

Follow these steps:

1. Verify that the database server is running.

2. Run the Data Management application.

   The Enter Server Credentials dialog appears.

3. Click Cancel. Then click File, General Settings from the main menu.

   The Data Management Settings dialog appears.

4. Click the SQL Connectivity tab.

5. Select the Use Static SQL Credentials option.
6. Configure the following fields and options:

   SQL Server Type

   Specifies whether a Microsoft SQL Server or Oracle Server hosts CA Identity Governance databases.

   Server

   Defines the target on the database server:

   - For a Microsoft SQL Server, this field specifies the host name of the database server instance.
   - For an Oracle database server, this field specifies the Oracle service name, as defined in the tnsnames.ora file in the Oracle service directory.

   Database

   (Microsoft SQL Server only) Defines the main CA Identity Governance database.

   Username, Password

   Define the login credentials of the database user or schema owner.

   Windows Authentication

   (Microsoft SQL Server only) When the database user is mapped to a general Windows user account in the environment, specifies whether the Windows user is used to log in to the database server.

7. Click Apply.

   A message confirming SQL connectivity appears. The application is now connected to the database.

8. Close the dialog.
9. Repeat this procedure in the DNA application.

   The client applications are configured and ready for use.

Configure Bulk Insertion of SQL Data

The Bulk Insert option writes data to a temporary SQL file. This option speeds the process of saving data, and allows you to continue working while the SQL database reads data from the file.

The SQL Server must have read access to the shared folder in which the temporary file is stored during the save process.

Note the following:

- To use bulk import when Microsoft SQL Server hosts CA Identity Governance databases, assign bulkadmin or sysadmin privileges to the CA Identity Governance database user.
- The CA Identity Governance server and the Microsoft SQL Server must be in the same domain.

To configure bulk insertion of SQL data

1. In a CA Identity Governance client application window, click File, General Settings.

   The Settings dialog appears.

2. Click the SQL Connectivity tab.

   Select the Bulk Insert option.

3. Select one of the following options:

   - When the SQL Server is located on a local computer, select the Create local share for temporary files option and define the pathname of the shared file on the local computer.

     Note: When you specify this option, the SQL database looks for the shared file locally on its own server under the specified pathname.

   - When the SQL Server is located on a remote computer, select the Use Remote Share directory option and define the full network address of the shared file, including the hostname of the target computer.

4. Specify values for the following fields to define the file structure of the CA Identity Governance databases:

   Field Delimiter

   Specifies the character that separates field values in the shared folder.

   Line Delimiter

   Specifies the end-of-line character in the shared folder.

   Note: The characters you specify cannot appear in the data content of the folder. When these characters appear in data fields, the file is parsed incorrectly and bulk insert fails. Similarly, when data strings are longer than their legal length, bulk insert fails.

Configuration Presentation

Use the Presentation tab to set how data is treated when it is being loaded from files into CA Identity Governance, and how the data is presented when displayed.

To set presentation parameters

1. Click File, General Settings.

   The Discover and Audit Settings window opens.

2. Select the Presentation tab.

3. In the Configuration View section, specify how the user, role, and resource sections are displayed in a configuration file window.

4. (Optional) To display the user panel of configuration files in a hierarchical tree:

   a. Select the Show User Tree View option in the Configuration View section.

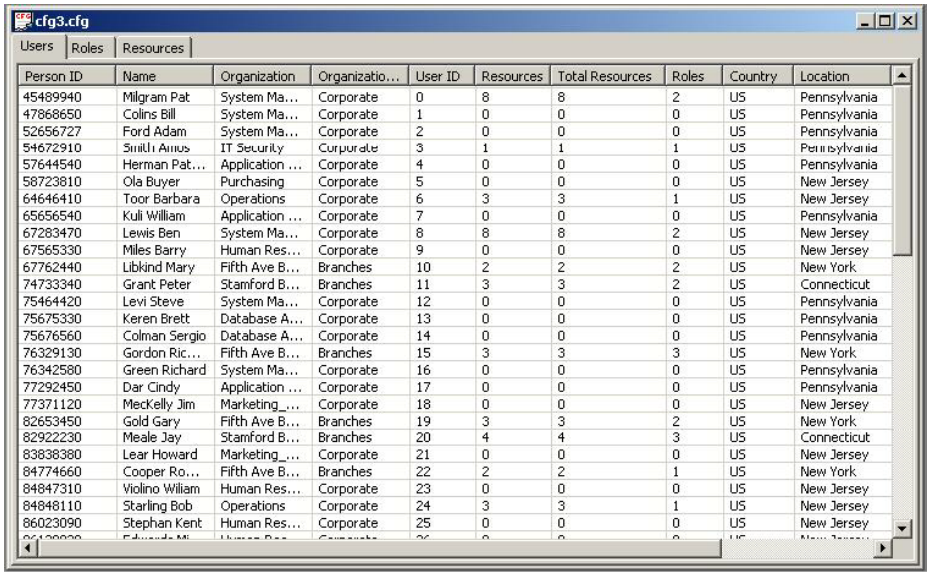
   b. In the User Hierarchy Order section, click and drag user attributes to define the structure of the user tree.

5. In the Fields to Show section, select the default attribute fields to display for each section of a configuration file.

Configuration View (Configuration Only)

View Mode enables the display of configuration data in three types of Configuration windows: horizontal panels, tabbed panels, vertical panels. Panels can be sorted by any column by clicking on the column name. Clicking the column toggles between ascending/descending sorts. Scrolling through records in the panel is performed by dragging the scroll bars.

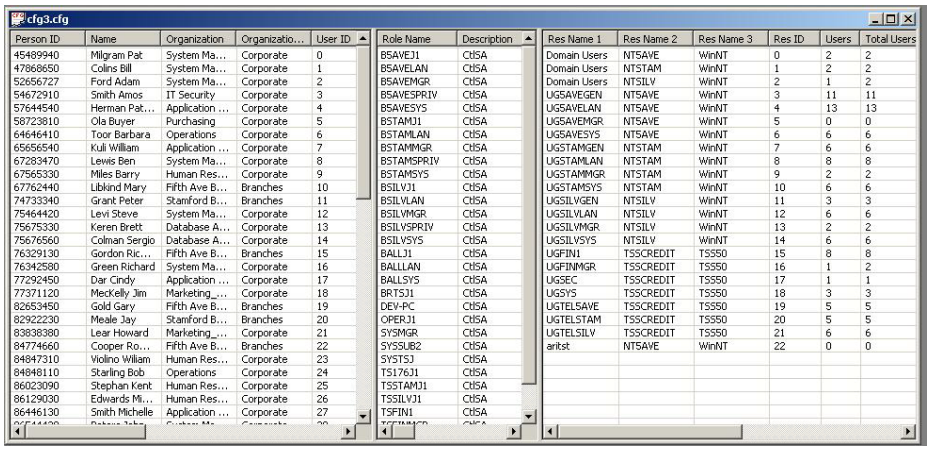
When Tab Mode is selected, a typical Configuration window will look like this:



Person ID	Name	Organization	Organizatio...	User ID	Resources	Total Resources	Roles	Country	Location
45489940	Milgram Pat	System Ma...	Corporate	0	8	8	2	US	Pennsylvania
47868650	Colins Bill	System Ma...	Corporate	1	0	0	0	US	Pennsylvania
52656727	Ford Adam	System Ma...	Corporate	2	0	0	0	US	Pennsylvania
54672910	Smith Amos	IT Security	Corporate	3	1	1	1	US	Pennsylvania
57644540	Herman Pat...	Application ...	Corporate	4	0	0	0	US	Pennsylvania
58723810	Ola Buyer	Purchasing	Corporate	5	0	0	0	US	New Jersey
64646410	Toor Barbara	Operations	Corporate	6	3	3	1	US	New Jersey
65656540	Kuli William	Application ...	Corporate	7	0	0	0	US	Pennsylvania
67283470	Lewis Ben	System Ma...	Corporate	8	8	8	2	US	New Jersey
67565330	Miles Barry	Human Res...	Corporate	9	0	0	0	US	New Jersey
67762440	Libkind Mary	Fifth Ave B...	Branches	10	2	2	2	US	New York
74733340	Grant Peter	Stamford B...	Branches	11	3	3	2	US	Connecticut
75464420	Levi Steve	System Ma...	Corporate	12	0	0	0	US	Pennsylvania
75675330	Keren Brett	Database A...	Corporate	13	0	0	0	US	Pennsylvania
75676560	Colman Sergio	Database A...	Corporate	14	0	0	0	US	Pennsylvania
76329130	Gordon Ric...	Fifth Ave B...	Branches	15	3	3	3	US	New York
76342580	Green Richard	System Ma...	Corporate	16	0	0	0	US	Pennsylvania
77292450	Dar Cindy	Application ...	Corporate	17	0	0	0	US	Pennsylvania
77371120	MecKelly Jim	Marketing_...	Corporate	18	0	0	0	US	New Jersey
82653450	Gold Gary	Fifth Ave B...	Branches	19	3	3	2	US	New York
82922230	Meale Jay	Stamford B...	Branches	20	4	4	3	US	Connecticut
83838380	Lear Howard	Marketing_...	Corporate	21	0	0	0	US	New Jersey
84774660	Cooper Ro...	Fifth Ave B...	Branches	22	2	2	1	US	New York
84847310	Violino Wiliam	Human Res...	Corporate	23	0	0	0	US	New Jersey
84848110	Starling Bob	Operations	Corporate	24	3	3	1	US	New Jersey
86023090	Stephan Kent	Human Res...	Corporate	25	0	0	0	US	New Jersey

Click on column headers to sort the column.

When Vertical Mode is selected, a typical Configuration window will look like this:



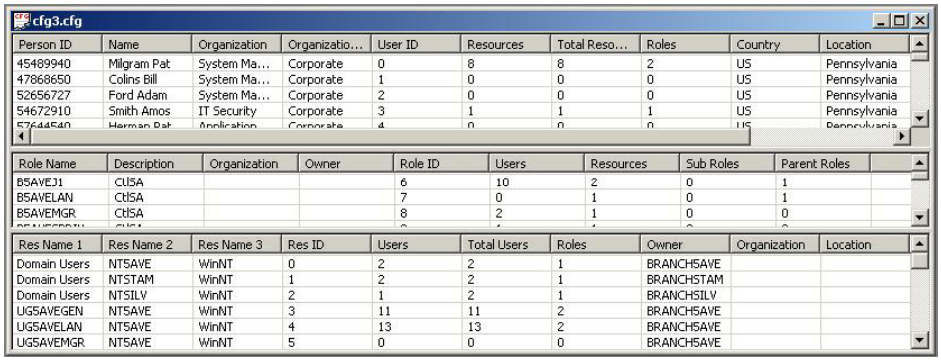
Person ID	Name	Organization	Organizatio...	User ID
45489940	Milgram Pat	System Ma...	Corporate	0
47868650	Colins Bill	System Ma...	Corporate	1
52656727	Ford Adam	System Ma...	Corporate	2
54672910	Smith Amos	IT Security	Corporate	3
57644540	Herman Pat...	Application ...	Corporate	4
58723810	Ola Buyer	Purchasing	Corporate	5
64646410	Toor Barbara	Operations	Corporate	6
65656540	Kuli William	Application ...	Corporate	7
67283470	Lewis Ben	System Ma...	Corporate	8
67565330	Miles Barry	Human Res...	Corporate	9
67762440	Libkind Mary	Fifth Ave B...	Branches	10
74733340	Grant Peter	Stamford B...	Branches	11
75464420	Levi Steve	System Ma...	Corporate	12
75675330	Keren Brett	Database A...	Corporate	13
75676560	Colman Sergio	Database A...	Corporate	14
76329130	Gordon Ric...	Fifth Ave B...	Branches	15
76342580	Green Richard	System Ma...	Corporate	16
77292450	Dar Cindy	Application ...	Corporate	17
77371120	MecKelly Jim	Marketing_...	Corporate	18
82653450	Gold Gary	Fifth Ave B...	Branches	19
82922230	Meale Jay	Stamford B...	Branches	20
83838380	Lear Howard	Marketing_...	Corporate	21
84774660	Cooper Ro...	Fifth Ave B...	Branches	22
84847310	Violino Wiliam	Human Res...	Corporate	23
84848110	Starling Bob	Operations	Corporate	24
86023090	Stephan Kent	Human Res...	Corporate	25
86129030	Edwards Mi...	Human Res...	Corporate	26
86446130	Smith Michelle	Application ...	Corporate	27

Role Name	Description
BSAVEJ1	CtlSA
BSAVELAN	CtlSA
BSAVEMGR	CtlSA
BSAVESPRIV	CtlSA
BSAVESYS	CtlSA
BSTAMJ1	CtlSA
BSTAMLAN	CtlSA
BSTAMMGR	CtlSA
BSTAMSPRIV	CtlSA
BSTAMSYS	CtlSA
BSILVJ1	CtlSA
BSILVLAN	CtlSA
BSILVMGR	CtlSA
BSILVSPRIV	CtlSA
BSILVSYS	CtlSA
BALLJ1	CtlSA
BALLLAN	CtlSA
BALLSYS	CtlSA
BRTSJ1	CtlSA
DEV-PC	CtlSA
OPERJ1	CtlSA
SYSMGR	CtlSA
SYSSUB2	CtlSA
SYSTSJ	CtlSA
TS176J1	CtlSA
TSSTAMJ1	CtlSA
TSSILVJ1	CtlSA
TSFIN1	CtlSA

Res Name 1	Res Name 2	Res Name 3	Res ID	Users	Total Users
Domain Users	NT5AVE	WinNT	0	2	2
Domain Users	NTSTAM	WinNT	1	2	2
Domain Users	NTSILV	WinNT	2	1	2
UGSAVEGEN	NT5AVE	WinNT	3	11	11
UGSAVELAN	NT5AVE	WinNT	4	13	13
UGSAVEMGR	NT5AVE	WinNT	5	0	0
UGSAVESYS	NT5AVE	WinNT	6	6	6
UGSTAMGEN	NTSTAM	WinNT	7	6	6
UGSTAMLAN	NTSTAM	WinNT	8	8	8
UGSTAMMGR	NTSTAM	WinNT	9	2	2
UGSTAMSYS	NTSTAM	WinNT	10	6	6
UGSILVGEN	NTSILV	WinNT	11	3	3
UGSILVLAN	NTSILV	WinNT	12	6	6
UGSILVMGR	NTSILV	WinNT	13	2	2
UGSILVSYS	NTSILV	WinNT	14	6	6
UGFIN1	TSSCREDIT	TS550	15	8	8
UGFINMGR	TSSCREDIT	TS550	16	1	2
UGSEC	TSSCREDIT	TS550	17	1	1
UGSYS	TSSCREDIT	TS550	18	3	3
UGTELSAVE	TSSCREDIT	TS550	19	5	5
UGTELSTAM	TSSCREDIT	TS550	20	5	5
UGTELSILV	TSSCREDIT	TS550	21	6	6
aritst	NT5AVE	WinNT	22	0	0

In Vertical Mode, Users will always be in the left panel, Roles in the middle panel and Resources in the right panel.

When Horizontal Mode is selected, a typical Configuration window will look like this:



In Horizontal Mode, the Users Panel will always be on top, the Roles Panel in the middle and the Resources Panel on bottom.

Note: The view mode can only be changed if an AuditCard window is not open. If the Role Engineer tries to change the view mode when an AuditCard window is open on the desktop, the client tools prompts to close the window.

More information:

Assign Users using Rule-based Roles (see page 73)

Print Fonts

At various points throughout the lifecycle of a project you may find it useful to generate and print reports such as Entity Reports, Role Analysis Reports and AuditCard Reports that contain details such as Users, Roles and Resources. While the content of the reports may vary according to the type of report that you generate, the Font format used for various report elements is maintained across all report types. The elements include report *titles*, *text*, *headers*, and *footers*. Once the report font characteristics are set you only need to deal with generating reports. This section deals with setting the font format and characteristics used in the reports.

To set the fonts used in reports

1. Click File, General Settings.

   The Discover and Audit Settings window opens

2. Select the Print Fonts tab.

   A window opens previewing the font formatting used for the Header, Footer, Title and Text report elements.

3. For each print font element click Set.

   The Font window opens.

4. Make your font selections.

5. Click OK and your choices are shown in the Set Print Fonts window.

Note that four types of fonts can be determined for different parts of the report: header, footer, title and text.

Note: These font choices become the print default used in all subsequent print jobs until they are changed.

More information:

Print Reports (see page 120)
Print Preview (see page 121)

Discovery & Audit

The following section describes the Discovery & Audit tab.

Rejected File

As a result of performing the Discovery process, the client tools identify and lists roles as part of a configuration file. The process may identify roles that you decide are redundant, old or that already exist. To prevent the configuration file from displaying roles that are no longer needed you can select such roles and reject them from your active configuration.

By default, rejected roles are removed from the working configuration and saved to a special configuration file called Rejected.cfg. The rejected.cfg file is stored in a predefined path and folder.

The Rejected File option in the General Settings *Discovery* tab gives you the capability to assign a specific configuration file to collect and house Roles that are rejected from the active configuration file.

To assign a specific configuration to act as the Rejected.cfg file

1. Click File, General Settings.

   The Discover and Audit Settings window opens.
2. Select the Discovery tab.
3. In the Rejected File section click Browse and navigate to the directory that houses your configuration files.
4. Enter a name for your specific file, such as <MyRejected>.cfg, in the File Name edit field.
5. Click Save.

   The Path and File name are listed in the Rejected File edit field.
6. Click Apply.

   The new <rejected>.cfg file is created.

More information:

Reject Discovered Roles (see page 119)

Search Advanced Options

During the Discovery process, the client tools use the values set in the Search Advanced Options window to fine tune the process. The option values are set by default and should not be modified.

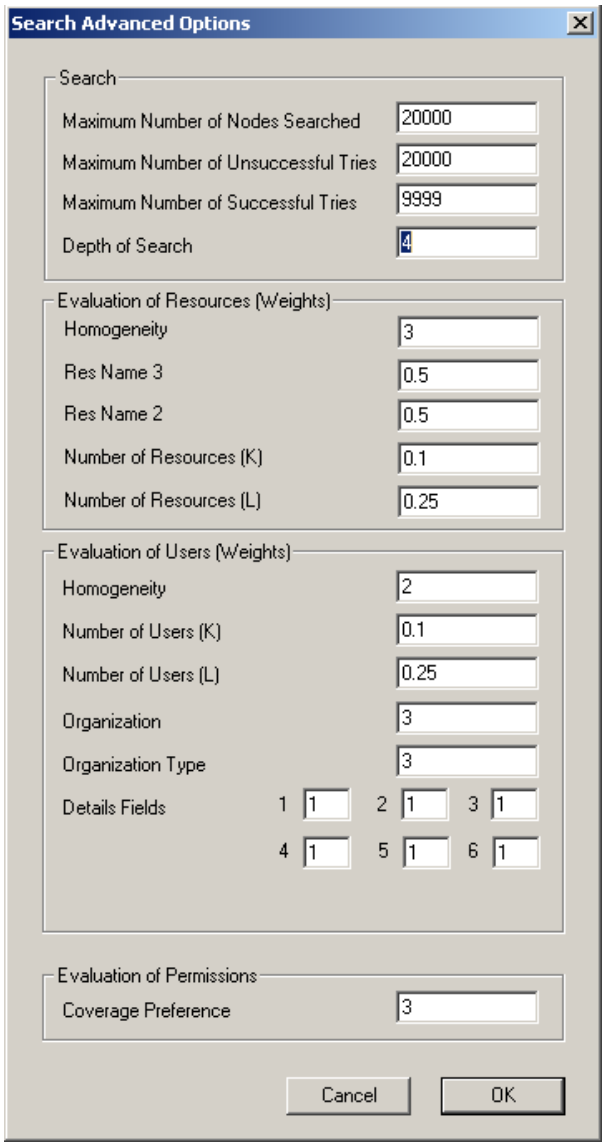
To view the default search advanced options

1. Click File, General Settings.

   The Discover and Audit Settings window opens.

2. Select the Discovery tab and click the Advanced Options.

   The Search Advanced Options window opens and displays the default settings.



Chapter 5: Edit

The Edit menu includes options to edit all the types of files used by CA Identity Governance: configuration files, databases (users and resources), audit (AuditCard), BPR. When a document is active, only edit options that apply to that type of document are displayed in the Edit menu.

This section contains the following topics:

Delete

The Delete operation can only be performed on records in a Configuration file or in an Audit Card. As such the Delete option only appears in the Edit menu within the context of a Configuration file and Audit Card.

Deleting Records from a Configuration

This feature enables deleting one or more users, roles or resources records (depending how many are highlighted) from the Users Panel, Roles Panel or Resources Panel of a configuration. A message such as the following is displayed for each record:

If more than one record is highlighted, CA Identity Governance requests individual confirmation for each record to be removed from the original configuration. Note that all direct and indirect links to the highlighted record are removed along with the record. The Role Engineer can choose whether or not to delete the highlighted records all at once by clicking Yes to All.

Note: A deletion is not saved to memory. To perform a “Cut and Paste” action, first copy the desired item to its intended location and then delete it from its original location.

Note: Modifications to a configuration document are only final after a configuration file has been saved. If exited without saving, the configuration document reverts to its original state as before the deletion.

Deleting Records from an AuditCard

When an AuditCard is open, you can delete highlighted records from the list of suspicious records. Use this option with care as no confirmation message is displayed before deletion.

Copy

The Copy operation can only be performed on records listed in either Configuration files or Databases. As such the Copy option only appears in the Edit menu within the context of Configuration files and Databases.

This feature enables you to copy any number of highlighted (into memory) users, roles or resource records from the Users Panel, Roles Panel or Resources Panel of a configuration file into memory. You Copy records to memory in preparation for pasting them into another configuration file.

When a users database (*.udb) document is active or when a resources (.rdb) document is active, then those records can be copied into a Users Panel or Resources Panel of a configuration. Pasting such records into a different resources or users database, or into a configuration file that is not related to the databases from which the records were copied is prohibited.

All direct and indirect links to the highlighted record are copied along with the record.

Paste

The Paste operation can only be performed on records listed in Configuration files. As such the Paste option only appears in the Edit menu within the context of Configuration files.

This feature enables one or more users, roles or resources records, which were copied from one configuration using the copy option, to be pasted into another configuration's Users Panel, Roles Panel or Resources Panel, respectively.

In addition, when a users database (.udb) document is active or when a resources (.rdb) document is active, then those records can be copied and pasted into a Users Panel or Resources Panel of a configuration. Pasting records into a different resources or users database or into a configuration that is not related to the databases from which the records were copied is prohibited.

When a paste operation is performed, a confirmation message appears. If more than one record is highlighted, CA Identity Governance requests confirmation for each record to be pasted. Note that for each pasted record a prompt appears to confirm establishing linkage (direct and indirect) to other records in the target configuration, if applicable. The Role Engineer can choose to confirm linkage of all the highlighted records by clicking Yes or Yes to All.

Note: Modifications to a configuration document are final only after the configuration file is saved. If you exit the file without saving, the configuration document reverts to its original state as before performing the copy and paste action.

More information:

Copy (see page 63)

Create Partial Configuration

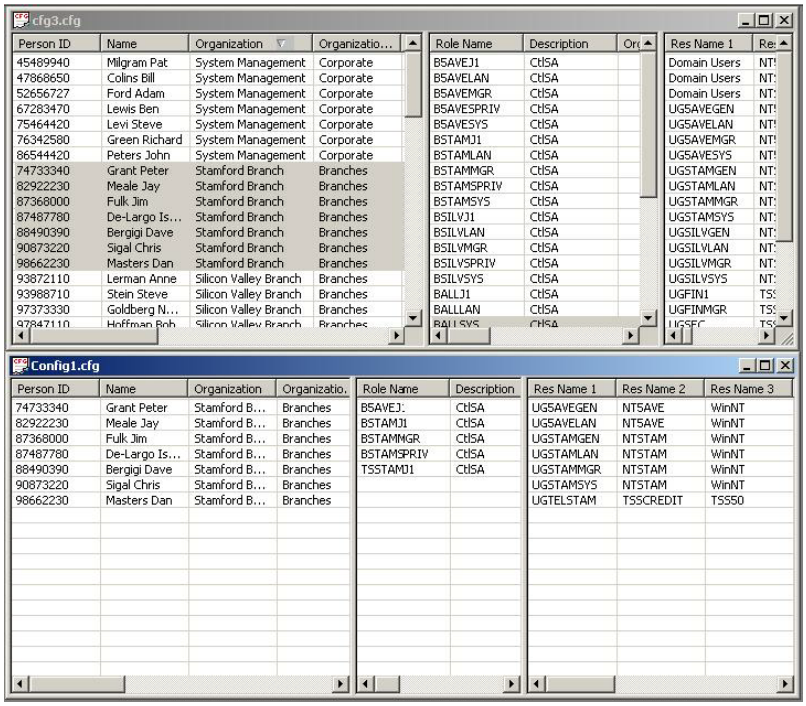
This option creates a new, “partial” configuration from highlighted records of a current configuration. This option is useful when a Role Engineer designates a particular segment of the current configuration for further operations such as verification of those records by other officials of the organization or to handle certain criteria from the current configuration

The Create Partial Configuration operation can only be performed on records listed in Configuration files. As such the option only appears in the Edit menu within the context of Configuration documents.

To create a partial configuration

1. Place the focus on the configuration document from which the partial configuration is to be extracted.
2. From within the current configuration select the records to include in the partial configuration.
3. Click Edit, Create Partial Configuration or right-mouse click in the selection and choose Create Partial Configuration from the menu. A new configuration document is displayed that only contains the previously selected records and all their links.
4. Save the newly created configuration document under an appropriate name.

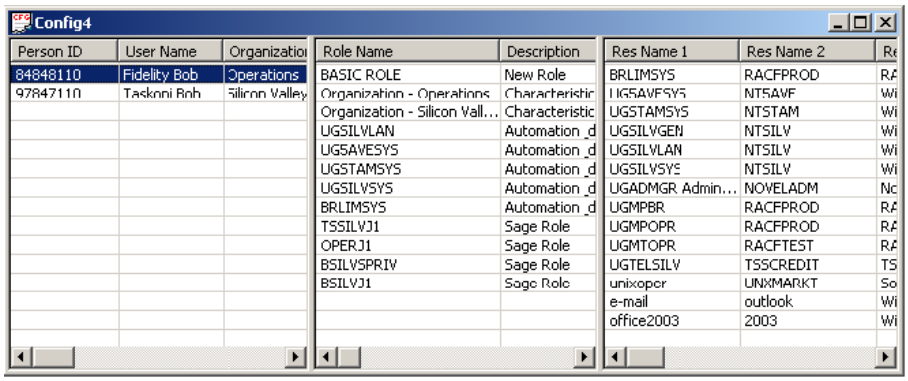
The first window is the current configuration. The second window is a partial configuration:



Create Filtered Configuration

You can apply one or more filters to the User, Role or Resource entities of a configuration. Filters are expressions that select entities based on the content of attribute fields. When you define several filters, they are applied with a logical AND operation, and the result is a set of entities that satisfy all the filters.

For example, you can define a filter that selects user entities with the string "Bob" in their UserName field. The following screen displays the resulting configuration file after the applying this filter. Two users are identified that contain the string "Bob" as part of their User Names.



CA Identity Governance saves the results in a new configuration file, which is automatically given a name. You can save the configuration under another name.

You can only apply filters to one entity at a time. You can filter the resulting configuration by another entity to refine the results.

The following table lists the Filter Criteria and their descriptions.

Filter Criteria	Description
Entity	Sets the entity to filter.
Field	Displays the available Fields for the selected entity that can be used as a filter.
From	Sets the upper limit of the filter range for the selected Field.
To	Sets the lower limit of the filter range for the selected Field.
Pattern	Any alphanumeric string that can be used to fine-tune the filter operation. For example, the first name of any User, such as Bob.
Regular Expression	Select this option to indicate that the Pattern contains recognized regular expression (see page 67) characters.

Filter Criteria	Description
Filter Only Specified Entity	Select to retain entities of other types, even if they are not linked to the entities selected by the filter. For example, when a filter selects a subset of users, the roles and resources are unaffected. Unselect to retain only entities that link to the filtered entities. For example, when a filter selects a subset of users, the results contains only roles and resources linked to those users.

To filter a configuration:

1. In the client tools, open the configuration document you want to filter.
2. Click Edit, Create Filtered Configuration.

   The Filter window appears.
3. Set the range for any or all of the filter options in the Criteria section of the window.
4. Click Add.

   The filter ranges are listed in the Filter list on the right side of the Filter window.
5. Click OK to filter the configuration using the select filter ranges.

   A new configuration document is displayed.
6. Save the newly created configuration document under an appropriate name.

Regular Expressions in CA Identity Governance

CA Identity Governance uses regular expressions to define patterns for various match or filter operations, such as business process rules (BPRs). CA Identity Governance supports most standard regular expression syntax. The following table lists commonly used special characters.

Character	Usage
*	Matches any string of zero or more characters. For example, the following pattern matches both Maureen and Green: *reen
.	Matches any single character. For example, the following pattern finds the names Dean, Sean, and Jean: .ean

Character	Usage
[ ]	Matches any single character within the specified range. For example, the following pattern matches Larsen and Karsen but not Carsen: [K-P]arsen
|	Matches any one of the concatenated regular expressions. For example, the following pattern matches Jerrold, Jorge, or Jurgenson. (Jer*)|(Jor*)|(Jur*)
[^]	Matches any single character *not* within the specified range. For example the following pattern finds Delano but not Desiree. De[^s]

Flatten Role Hierarchy

If the hierarchic relationship between roles in an organization reaches a level of complication that prevents you from assigning roles and providing access permissions to resources in a clear and manageable fashion you may want to reassess the role relationships. You can flatten the role hierarchy in a configuration file, by removing the links between roles. The result is that all roles that previously had access to a resource via an intermediate role are given direct access to those resources. The configuration file that results from this treatment can then be reassessed. Using the flattened configuration file as base platform, you can then streamline the role hierarchy in your organization, remove redundant roles, and establish new relationships between subordinate and parental roles that accurately reflect the current use of resources in your organization.

To flatten a configurations role hierarchy

1. From the client tools, open or select the configuration file to be flattened.
2. Click Edit, Flatten Role Hierarchy.

   The client tools scan the configuration file and opens a new configuration file that reflects the role hierarchy treatment. The previous configuration file is maintained without any changes.
3. Save the new configuration file under a new name.

Create a Role (Configuration Only)

In the course of the Discovery process, new relationships may be discovered, which were previously unknown, and you may need to create new roles to support these relationships.

Follow these steps:

1. Click Edit, New Role.

   The Role window opens. CA Identity Governance automatically provides a numeric Role ID.

2. Use the options in the drop-down lists to set the values for Owner, Type, Organization, Organization 2 and Organization 3 fields.

3. Enter descriptive text in each of the Rule and Description edit fields.

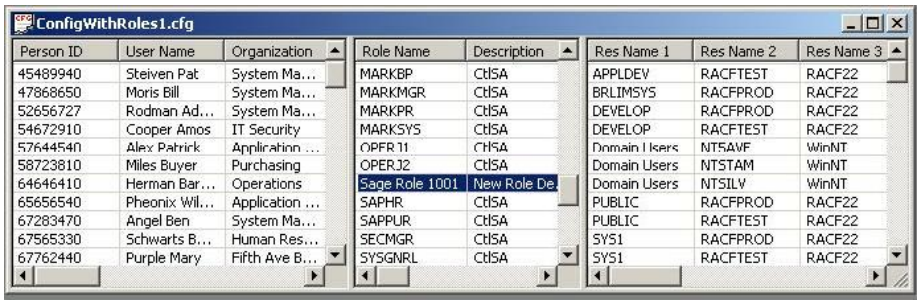
4. The New Role window contains the following fields:

Field	Description
Role ID	By default, CA Identity Governance increments the role ID by 1 digit each time a new role is added. This field is a key field and is non-modifiable by the Role Engineer.
Name	By default, CA Identity Governance inserts the name “Role nnnn”, where “nnnn” is an incremented number. This is a text field intended for a relevant mnemonic name of the new role. The default data can be modified by the Role Engineer.
Owner	Owner of the role. The default data can be modified by the Role Engineer.
Type	Type of role. An arbitrary description that can be modified by the Role Engineer.
Organization	Text field for naming the organization to which the role belongs. This field is especially useful for large organizations. The default data can be modified by Role Engineer .
Rule	Text field is supplied for descriptive purposes only.
Description	Text description of the role. The default data can be modified by the Role Engineer.

These data contain the identifying details of the new role. However, none or the user or resources data have, as yet, been associated with the new role.

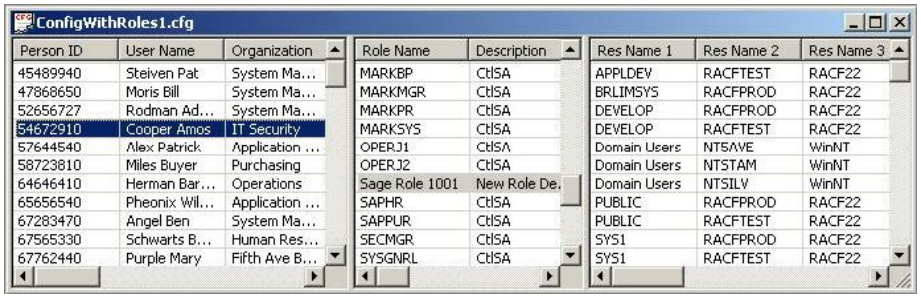
5. Click Save to include the new role in the configuration. A new configuration window opens and the new role is listed in the Roles Panel.

   New role added to Roles panel are highlighted:



6. Add users, roles, and resources to the new role by dragging and dropping them on the new role.

   The following screen displays the link between the two highlighted fields using drag and drop:



Note: When an item is dragged and dropped, the cursor changes from ⊖ to LINK before it is dropped.

Examining a New Role

The Role window is divided into an upper section listing the role fields as entered when the role was created. The lower section is divided into tabs that list additional information relating to Users, Resources, Parent Roles, Sub Roles and the Role Status.

Upper Section

Displays the field information as entered for the new role

Lower Section

Is divided into tabs displaying specific data relating to the subject of each tab

The following table describes the fields and information included on the tabs in the lower section of the Role window. The content of these fields is taken from the records that were dragged and dropped on the new role:

Field	Description
Users tab fields	The default fields are: Person ID, Organization, Organization Type, Country, Location, Title, and Cost Center. The field names can be changed by the Role Engineer.
Users - Show	The drop-down menu includes the options to show the following: Direct Links Only, Covered by Parent-Roles only, Covered by Both Parent-Roles and Direct Links, and All.
Resources tab fields	The default fields are: Resource Name 1, Resource Name 2, Resource Name 3, Owner, Organization, and Location. The field names can be changed by the Role Engineer.
Resources - Show	The drop-down menu includes options to show the following: Direct Links Only, Covered by Sub-Roles only, Covered by Both Sub-Roles and Direct Links, and All.
Parent Roles tab fields	The proposed role is a parent of the indicated roles. The default fields are: Role Name, Description, Organization, Owner, Role ID, Type, Create Date, Reviewer, Approval Code, Approval Date, Rule, Organization 2, and Organization 3. The field names can be changed by the Role Engineer.
Parent Roles - Show	The drop-down menu includes options to show the following: Parent Roles Linked Directly, Parent Roles Linked Indirectly, Parent Roles Linked Both Directly & Indirectly, and All.
Sub-Roles fields	The proposed role is a sub-role of the indicated roles. The default fields are: Role Name, Description, Organization, Owner, Role ID, Type, Create Date, Reviewer, Approval Code, Approval Date, Rule, Organization 2, and Organization 3. The fields names can be changed by the Role Engineer .

Field	Description
Sub-Roles - Show	The drop-down menu includes the options to show following: Sub Roles Linked Directly, Sub Roles Linked Indirectly, Sub-Roles linked Both Directly and Indirectly, and All.
Status	The Status tab includes fields that can be used to track the role development. These fields include Create Date, Approve Role. Set Approve Role to set the Approval Date and activate the Reviewer and Approval Status drop-down menu. Set the Expiration Date check box to activate a calendar and define the date beyond which the Role is no longer valid.

To examine a new role

1. From within the configuration window double-click the new role in the Roles Panel. The Role window opens listing the Role field information in the upper section of the window, and displaying a series of tabs in the lower section of the window.
2. After verifying the correctness of a new role, click Apply. Changes to the configuration are only permanently saved after the configuration is saved.

To remove items from a role

1. From within the Role window select the tab that contains data that you want to remove.
2. Select the item you want to remove from the list.
3. Click Remove.

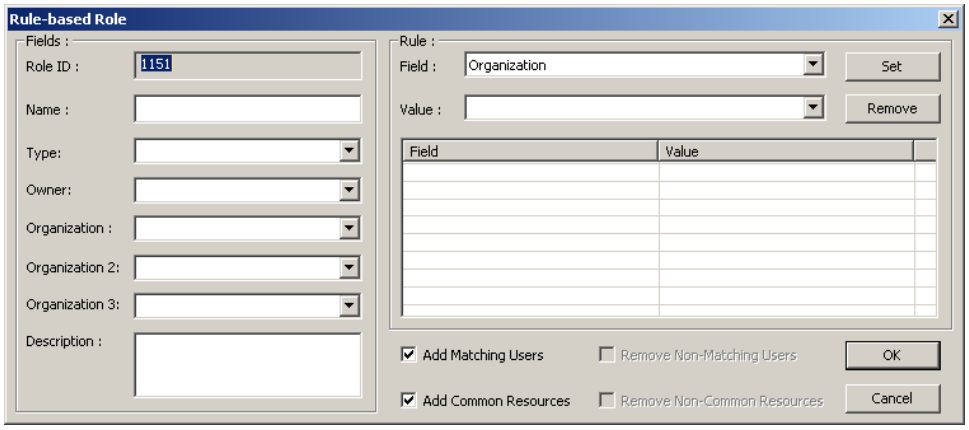
   The item is removed from the list.
4. Click Apply.

   Changes to the configuration are only permanently saved after the configuration is saved.

Assign Users using Rule-based Roles

Rule-Based roles employ a set of organizational, functional, and hierarchical based characteristics to define a rule that is then used to assign users with matching characteristics to the role. Using a rule-based role, you can scan the entire configuration and identify all users that conform to the role in one single action. Rules-based roles are constructed and added to the configuration through the Rule-based Role window.

Rules are made up of a series of Field and Value pairs, selected and then set in the Rule group box in the right side of the Rule-based Role window.



Follow these steps:

1. Click Edit, New Rule-based Role.

   The Rule-based Role window appears. The Role ID appears and is incremented by a value of 1 from the ID given to the previously created role.

2. Enter a Name for the role in the Name text field.

3. Populate the remaining edit fields in the Fields group box in the left part of the window. The operation is identical to that described for creating a regular role.

4. In the Rule group box, select a field type from the Field drop-down.

5. Select a corresponding value from the Value drop-down.

6. Click Set.

   The Field and Value pair are placed in the Rule list.

7. Repeat steps 4-6 to add another Field/Value pair to the rule.

8. Select the Add Matching Users check box to populate the role with all users that match the rule. The check box is selected by default.

9. Select the Add Common Resources to populate the role with all resources that match the rule.

   The check box is selected by default.

10. Click OK to save the Rule-based role.

    The role is added to the configuration file and is listed at the bottom of the configuration file Role Panel.

Edit Rule-Based Role

The rules that are assigned to a Rule-Based Role can be edited from within the Rule-Based Role window. You may need to append or remove Field/Value pairs to or from a rule. Reset the accompanying role information, or add or remove users and resources that match the role.

To edit a rule-based role

1. Select a rule-based role from the role panel in the active configuration window.
2. Either from the Edit menu, or from the right mouse button menu, select Edit Rule-Based Role.

   The Rule-based Role window opens, displaying the content of the selected rule.

3. Make changes to the rule as required. Operations within the window are performed the same as described for creating a new rule-based role.
4. Click OK to save changes and return to the configuration window.

More information:

Assign Users using Rule-based Roles (see page 73)

Edit Users, Roles, or Resources in a Configuration

You can edit a User, Role or Resource record from within the active configuration by removing direct links that are assigned to the record. The links that can be removed depend on the type of record selected The Edit Item menu item is context sensitive depending whether a User, Role or Resource record is selected in the configuration window. Access to this functionality is provided either via the right mouse menu, or from the Edit menu.

The content of the Edit User, Edit Role and Edit Resource windows are reviewed in the following sections.

Edit User

This option enables removal of direct links to resources and roles from a user record. There are three types of data in a typical User Edit window: users, resources, roles.

The following is a typical User Edit window:

Note: Double-clicking on a role area record opens the Role Edit window for that record, which enables the removal of direct links of roles. Double-clicking on a resources area record opens the Resources Edit window for that record, which enables the removal of direct links of resources.

User fields include the default fields: Person ID, User Name, Organization, Organization Type, User ID, Country, Location, Title, Cost Center. These fields are grayed out and cannot be changed in the Edit Item window. However, they can be changed when the users database (.udb file) is open.

The Resources Tab of the User Edit window includes statistical data on the user's resources (direct, indirect and both together) as well as the following fields: Resource Name 1, Resource Name 2, Resource Name 3, Owner, Organization, Location.

The Show drop-down menu enables display of the following combinations: Direct Links Only, Covered by Roles Only, Covered by Both Roles and Direct Links, All. All is the default.

The Role Tab of the User Edit window includes statistical data on the user's roles (direct, indirect and both together) as well as the following: Role Name, Description, Organization, Owner, Role ID, Type, Create Date, Reviewer, Approval Code, Approval Date, Rule, Organization 2, Organization 3, Expiration Date.

The Show drop-down menu enables display of the following combinations: Roles Linked Directly, Roles Linked Indirectly, Roles Linked Both Directly and Indirectly, All. All is the default.

To remove a direct link

1. Highlight the users, resources or sub-roles from which to remove a direct link.
2. Click Remove. The row disappears from the list.
3. Click Apply to confirm the changes and return to the configuration window.

Note: No confirmation message appears before removing the link. Indirect links cannot be removed directly. An attempt to remove indirect links generates an error message. An indirect link is removed automatically after removing its direct link.

More information:

Add User (Users Database Only) (see page 81)

Edit Role

This option enables editing role fields as well as removal of direct links to users, resources parent roles and sub-roles. The following types of data appear in a typical Role Edit window: Roles, Users, Resources, Parent Roles Sub-Roles and Status and is divided between various tabs by the same name.

Note: Double-clicking on a users area record opens the Users Edit window for that record. Double-clicking on a role area record (parent role or sub-role) opens the Role Edit window for that record. Double-clicking on a resources area record opens the Resources Edit window for that record.

Role data includes the following fields:

Field	Description
Role ID	The role ID is assigned by the system when the role is originally created. It is a non-modifiable field and is grayed out.
Name	Role name is set when the role is first created. The name can be modified.
Owner	To edit the role owner, select a new owner from the Owner drop-down.
Type	To edit the role Type, select a new type from the Type drop-down.
Organization	To edit the role Organization value, select a new organization value from the Organization drop-down.
Organization 2	To edit the role Organization 2 value, select a new organization 2 value from the Organization drop-down.
Organization 3	To edit the role Organization 3 value, select a new organization 3 value from the Organization drop-down.
Rule	The rule edit field displays a rule when the role is a rule-based role.
Description	Displays a textual description of the role. The description can be modified.

The Users Tab

Includes statistical data about the user's roles (direct, indirect and both together) as well as the following fields: Person ID, User Name, Organization, Organization Type, Country, Location, Title, Cost Center.

The Show drop-down menu enables showing the following combinations: Direct Links Only, Covered by Sub-roles Only, Covered by Both Sub-roles and Direct Links, All. All is the default.

The Resources Tab

Includes statistical data on the user's resources (direct, indirect and both together) as well as the following fields: Resource Name 1, Resource Name 2, Resource Name 3, Owner, Organization, Location.

The Show drop-down menu enables showing the following combinations: Direct Links Only, Covered by Sub-roles Only, Covered by Both Sub-roles and Direct Links, All. All is the default.

The Parent Roles Tab

Includes statistical data (direct, indirect and both together) as well as the following fields: Role Name, Description, Organization, Owner, Role ID, Type, Create Date, Reviewer, Approval Code, Approval Date, Rule, Organization 2, Organization 3. These fields cannot be removed and are included for information purposes only.

The Show drop-down menu enables showing the following combinations: Parent Roles Linked Directly, Parent Roles Linked Indirectly, Parent Roles Linked Both Directly And Indirectly, All. All is the default.

The Sub Roles Tab

Includes statistical data on the user's roles (direct, indirect and both together) as well as the following: Role Name, Description, Organization, Owner, Role ID Type, Create Date, Reviewer, Approval Code, Approval Date, Rule, Organization 2, Organization 3.

The Show drop-down menu enables showing the following combinations: Sub-role Linked Directly, Sub-role Linked Indirectly, Sub-role Linked Both Directly and Indirectly, All. All is the default.

The Status Tab

Provides a location to view the role creation date, role approval date, view and edit approval status, set an expiration date for the role.

To remove a direct link

1. Select the Users, Resources Parent Roles, or Sub-Roles tab from which to remove a direct link.
2. Select the record in the list that you want to remove.
3. Click Remove. The row disappears from the list.
4. Click Apply to confirm the changes and return to the configuration window.

Note: No confirmation message appears before removing the link. Indirect links cannot be removed directly. An attempt to remove indirect links generates an error message. An indirect link is automatically removed after removing its direct link.

Edit Resource

This option enables removal of direct links to users and roles. There are three types of data in a typical Resources Edit window: resources, users, roles.

Note: Double-clicking on a users area record opens the Users Edit window for that record. Double-clicking on a role area record opens the Role Edit window for that record.

Resource fields

Include the default fields: Res ID, Res Name 1, Res Name 2, Res Name 3, Owner, Organization, Location. These fields are grayed out and cannot be changed in the Edit Item window. However, they can be changed when the resources database (.rdb file) is open.

The Users Tab

Includes statistical data about the user's roles (direct, indirect and both together) as well as the following fields: Person ID, User Name, Organization, Organization Type, Country, Location, Business Unit, Special Field.

The Show drop-down menu enables showing the following combinations: Direct Links Only, Covered by Roles Only, Covered by Both Roles and Direct Links, All. All is the default.

The Roles Tab

Includes statistical data on the user's roles (direct, indirect and both together) as well as typical resource database fields: Role Name, Description, Organization, Owner, Role ID.

The Show drop-down menu enables showing the following combinations: Roles Linked Directly, Roles Linked Indirectly, Roles Linked Both Directly and Indirectly, All. All is the default.

To remove a direct link

1. Select the Users or Roles tab from which to remove a direct link.
2. Select the record in the list that you want to remove.
3. Click Remove.

   The row disappears from the list.
4. Click Apply to confirm the changes and return to the configuration window.

Note: No confirmation message appears before removing the link. Indirect links cannot be removed directly. An attempt to remove indirect links generates an error message. An indirect link is removed automatically after removing its direct link.

More information:

New Resource (Resources Database Only) (see page 85)
Edit Resource (Resources Database Only) (see page 87)

Manage Links

This option performs cleanup of direct and indirect links associated with users, roles and resources typically resulting from the Role Discovery process. To activate this option, highlight a record or group of records in the Users, Roles or Resources Panel. Go to Edit, Manage Links on the menu bar and choose the appropriate option. You are prompted to confirm with each record. Choose Yes for All to avoid confirming separate records.

More information:

Role Discovery (see page 103)

Remove Redundant Links

Redundant links are direct relationships between a users and resources that exist in addition to indirect links such as through a role. Typically, Role Engineers prefer to remove redundant links, so that user access to a resource depends on continued membership in a role.

To remove redundant links, select the relevant entities and run this option.

Instantiate Direct Links

This option establishes direct user-resource links. Links that were removed due to the introduction of a role or were added to a role but not to the individual users (indirect links) can be established as direct links using this option.

Remove Remaining Direct Links

This option removes any user links, which are not associated with any of that user's roles. This option is useful for cleanup purposes after all roles have been defined.

Remove All Links

This option enables removing all links (direct and indirect) associated with a user, role or resource.

Add User (Users Database Only)

On some occasions you may need to add a new user to the User Database but do not want to import data using the import process provided by the client tools. This may arise in the case where you want to add a single user only. The client tools provide you with the means to manually add users and their details to the Users database.

User details include the following mandatory and default fields:

Field	Description
User ID	CA Identity Governance automatically assigns the new usera User ID. This is a key field. It is a non-modifiable field and is grayed out.
Person ID	Person ID should correspond to the format of other users in the User Database. Person ID is a key field together with the User ID. Its length can be a maximum of 128 characters. Subsequently, if the user record has to be edited in the Edit User - User Database window, this record will be grayed out.
User Name	An optional 128 character text field. This field is provided by default and includes critical data.
Organization	An optional 128 character text field. This field is provided by default and includes critical data.
Organization Type	This field is provided by default and includes critical data.

All other fields are optional 128 character text fields and appear as a consequence of the Database definitions that were set when the Database was first created.

To manually add a user to the UsersDB database

1. Open or make active the configuration file that is associated with the Users database to which you want to add a user.
2. From the Configuration files toolbar click the UsersDB icon. The Users window opens.

3. Click Edit Add User.

   The User Details window opens.

   The User ID field is updated automatically when the newly added user is included in the configuration file.

4. Enter a unique ID number in the Person ID field. This is mandatory. The Person ID is converted into an additional and non-modifiable key field in the User Database.
5. For each Field, click in the associated Value edit box and enter a suitable value.
6. Click OK.

   The new user is added to the User database and appears in the UsersDB window.

7. Add the new user to a configuration file by dragging it onto a configuration window.

Edit User (Users Database Only)

This option enables you to manually modify user data in the User Database. This feature is only available when a User Database is active.

To manually edit user details in the users database

1. Open or make active the configuration file that is associated with the Users database for which you want to edit user details.
2. From the Configuration files toolbar click the UsersDB icon.
3. The Users database window opens.
4. Select a User from within the Database.
5. Click Edit, Edit User.

   The User Details window opens.

6. Edit the details in the Value edit boxes as required.
7. Click OK to save the changes and return to the Users Database window.

The changes to the User Details are reflected in the Users Database and the Configuration window.

Link Attributes

You can create attributes and attribute values between linked entities in the CA Identity Governance Discovery & Audit client tool. This is useful when you manage relationship links and assign descriptive labels, such as listing and recording resource expiration dates.

Entities must be listed in a specific order. For example, in a User-Res declaration, the first entity is a user record, and the second entity is a resource record. In a Role-Role link, the first entity is the role ID of the parent role, and the second entity is the role ID of the child role.

To create and manage these links, you must edit the configuration file (*.cfg) header field to enable the Attributes button option where it appears when editing a resource (see page 79).

You can edit the following attribute type declarations for link attributes:

- **User-Resource**: User-resource link.

  For user-resource link attributes, consider the following header:

  ```
  User-Res-Field-Names,"<Att1>","<Att2>"
  ```

  Where "<Att1>" is "Expiration Date" and "<Att2>" is "Printer".

- **User-Role**: User-role link.

  For user-role resource link attributes, consider the following header:

  ```
  User-Role-Field-Names,"<Att3>"
  ```

  Where "<Att3>" is "Manager".

- **Role-Role**: Role-role link.

  For role-role resource link attributes, consider the following header:

  ```
  Role-Role-Field-Names,"<Att4>","<Att5>"
  ```

  Where "<Att4>" is "Address" and "<Att5>" is "Email".

- **Role-Resource**: Role-resource link.

  For role-resource link attributes, consider the following header:

  ```
  Role-Res-Field-Names "<Att6>", "<Att7>", "<Att8>"
  ```

  Where "<Att6>" is "Site Manager", "<Att7>" is "Printer" and "<Att8>" is "Scanner".

More information:

Define Link Attributes (see page 84)
Assign Link Attribute Values (see page 85)

Define Link Attributes

Define link attributes by adding headers to the CA Identity Governance Discovery and Audit configuration file for linking members, roles and resources.

Important: The initial three lines in the configuration file are reserved for user and resource database files. Do not insert headers in these areas.

Note: You must edit the configuration file (*.cfg) header field to enable the Attributes button option where it appears when editing a resource (see page 79).

To edit the configuration file

1. Locate and open the applicable configuration file and add an attribute type declaration.

   Configuration files are usually located in the Sage Demo folder in the installation directory (C:\Program Files\CA\RCM\Client Tools\Sage Demo).

2. Insert and edit headers for the desired link attributes.

   For example, for a user-resource link use the following header:

   ```
   User-Res-Field-Names,"Att1","Att2"
   ```

   Where "Att1" is the expiration date, and "Att2" is printer.

   For example, for a user-role link, use the following header:

   ```
   User-Role-Field-Names,"Att3"
   ```

   Where "<Att3>" is "Manager".

3. Save and close the configuration file.

Assign Link Attribute Values

Assign link attribute values between the selected entities once you edit a configuration file and add the applicable headers.

To assign and view attributes

1. Navigate to and open the configuration file.

   The filename.cfg window appears.

2. Select an entity and select Edit, Edit entity.

   The entity window appears.

3. In the entity Resources, Users or Roles tab, select a resource, user or role and click Attributes.

   The Link Attributes window appears listing the entity, the linked entity resource, and attributes linking them.

4. Assign a value to the attribute in the Value column and click OK.

   The attributes are assigned to the selected values.

New Resource (Resources Database Only)

On some occasions you may need to add a new resource to the Resource Database but do not want to import data using the import process provided by the client tools. This may arise in the case where you want to add a single resource only. The client tools provide you with the means to manually add resources and their details to the Resources database.

The Resources Database contains several fields, the exact number and name of those fields depends on the mapping that was performed when the data base was first imported and created. Three of the fields, Res Name 1, Res Name 2 and Res Name 3 will appear by default. When adding a new resource, a value must be supplied for at least one of those three fields. In any case the combination of values provided for the three Res Name fields must be unique amongst all the resources present in the database. The Res ID field is a key field and is non-modifiable in this window. The remaining fields can contain data filled in by the Role Engineer.

Resource details include the following fields:

Field	Description
Res ID	CA Identity Governance automatically designates the new resource with a Res ID. This is a key field. It is a non-modifiable field and is grayed out.

Field	Description
Res Name 1	Res (resource) Name 1 should correspond to the format of other resources in the Resources Database. Res Name 1, Res 2 and Res Name 3 become key fields together with Res ID. Its length can be a maximum of 128 characters. Subsequently, it is grayed out in the Edit Resource window.
Res Name 2	Res (resource) Name 2 should correspond to the format of other resources in the Resources Database. Res Name 1, Res Name 2 and Res Name 3 become key fields together with Res ID. Its length can be a maximum of 128 characters. Subsequently, it is grayed out in the Edit Resource window.
Res Name 3	Res (resource) Name 3 should correspond to the format of other resources in the Resources Database. Res Name 1, Res Name 2 and Res Name 3 become key fields together with Res ID. The length can be a maximum of 128 characters. Subsequently, it is grayed out in the Edit Resource window.
Owner	An optional 128 character text field.
Organization	An optional 128 character text field.
Location	An optional 128 character text field.

All other fields are optional 128 character text fields and appear as a consequence of the Database definitions that were set when the Database was first created.

To manually add a resource to the resource database

1. Open or make active the configuration file that is associated with the Resource database to which you want to add a resource.
2. From the Configuration files toolbar click the Resource Database icon.

   The Resource Database window opens.
3. Click Edit, New Resource.

   The Resource Details window opens.

   The Res ID field is updated automatically when the newly added resource is included in the configuration file.

4. Enter a value for at least one of the three Res Name fields. This is mandatory.
5. For each of the remaining fields, select a suitable value from the drop-down list boxes as required.
6. Click OK.

   The new resource is added to the Resource database and appears in the Resources Database window.
7. Add the new resource to the configuration file by dragging it onto resource panel in the configuration window.

   Modifiable fields are equipped with drop-down menus that include all current database definitions for the field.

   To change a field definition, choose the new definition, and click OK.

Edit Resource (Resources Database Only)

This option enables you to modify resource data in the Resources Database for a single record. It is only available when a Resources Database is active.

To manually edit user details in the users database

1. Open or make active the configuration file that is associated with the Resource database for which you want to edit resource details.
2. From the Configuration files toolbar click the Resource Database icon.

   The Resource database window opens.
3. Select a Resource from within the Database.
4. Click Edit, Edit Resource.

   The Resource Details window opens.

   The Res ID, Res Name 1, Res Name 2 and Res Name 3 are key fields and are cannot be modified.
5. Select a new value for any of the modifiable fields from the drop-down lists. These include all current database definitions for the field.
6. Click OK to save the changes and return to the Resource Database window.

   The changes to the Resource Details are reflected in the Resource Database and the Configuration window.

Change Resource Attributes (Resources Database Only)

This option enables you to modify resource data in the Resources Database for a selection of records. It is only available when a Resources Database is active. Functionally it is similar to Editing Resource data.

To change resource attributes for several records

1. Open or make active the configuration file that is associated with the Resource database for which you want to change resource attributes.
2. From the Configuration file's toolbar click the Resource Database icon. The Resource database window opens.
3. Select several Resources from within the Database.
4. Click Edit, Change Resource Attributes.

   The Resource Details window opens.

   The Res ID, Res Name 1, Res Name 2 and Res Name 3 are key fields and are cannot be modified.
5. Select a new value for any of the modifiable fields from the drop-down lists. These include all current database definitions for the field.
6. Click OK to save the changes and return to the Resource Database window.

The changes to the Resource Details are reflected in each of the previously selected records in the Resource Database and the Configuration window.

More information:

Edit Resource (Resources Database Only) (see page 87)

AuditCard Properties (AuditCard Only)

This menu includes one auditing option: deleting a record designated as suspicious from the AuditCard.

Delete

You can delete records designated as suspicious when an AuditCard is open. To remove a record simply press the Delete key. No confirmation message is displayed, so caution is recommended before doing this.

AuditCard Properties

To view a statistical report on the suspicion types and progress in handling the suspicion, click View, AuditCard Properties when an AuditCard is open.

For each suspicion type, the following statistics are displayed:

Field	Description
Suspected	The number of suspected records for the specific type of suspicion.
OK	The number of suspected records of the specific type of suspicion that have been found to be OK after the suspicion was examined.
Addressed	The number of suspected records of the specific type of suspicion that have already been handled.
In Progress	The number of suspected records of the specific type that are currently being handled.
Total	The total number of suspected records of the specific type that are being handled plus those whose handling has been completed.

More information:

Audit Codes (see page 143)

Add BPR Entry (BPR Only)

See Modify Existing Business Process Rules (see page 157).

Delete BPR Entry (BPR Only)

See Modify Existing Business Process Rules (see page 157).

Edit BPR Entry (BPR Only)

See Modify Existing Business Process Rules (see page 157).

Chapter 6: View Menu

The View menu includes options that enable setting the display of information for the Role Engineer's convenience.

This section contains the following topics:

Toolbar

When this option is marked, the toolbar is displayed in the main window. When the option is not marked, the toolbar is not displayed in the main window. Some Role Engineers may prefer to turn off the toolbar to enable more screen space to perform complex activities with many windows.

More information:

Tool Bar and Shortcut Key Combinations (see page 23)

Status Bar

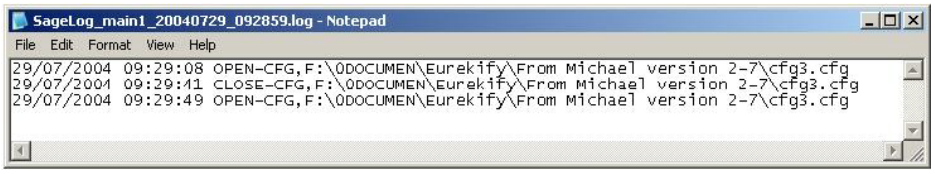
The status bar is located at the bottom of the main window and provides general information regarding the currently active window. As with the menu bar, some Role Engineers may prefer to turn off the status bar to enable more screen space to perform complex activities with many windows.

The following table shows typical information that is displayed on the status bar for each type of window:

Window	Sample Displayed Data
Configuration	“66 users (1 selected); 30 roles (1 selected); 23 resources (0 selected)”
Users database	“66 users”
Resource database	“23 resources”
Audit card	“766 Suspected; 0 OK; 0 Addressed; 0 In Progress”
Policy	“Ready”

View Log

To activate the Log window, choose View, Log on the menu bar. A window such as the following opens:



The log is opened in a Microsoft Windows Notepad document. The log records CA Identity Governance events and provides the following data:

- Date
- Time
- Type of activity
- Activity’s path.

In addition, if unusual events or errors occur, these too are listed. This window is generally used for performing software troubleshooting activities.

Sort

Use the Sort operation to arrange the way a configuration file's data is presented on screen in a configuration document. You can arrange the presentation for the Users panel, Roles panel and Resources panel independently of each other. Information can be arranged sequentially in either Ascending or Descending order for any three parameters listed in the configuration file.

The Sort operation can only be performed on records listed in Configuration files. As such the Sort option only appears in the Edit menu within the context of Configuration files.

To sort information in a configuration window

1. Select a Configuration window and place the focus on any one of the panels.
2. Click Edit, Sort.

   The Sort dialog opens.
3. From the Sort List drop-down list select the configuration panel on which to perform the sort operation. You can choose from either, Users, Roles, or Resources.
4. From the Sort By drop-down list select the parameter to function as the primary sort parameter.
5. Select the associated Ascending or Descending option to indicate the vertical order in which to display the data.
6. From the remaining two Then By secondary sort lists select additional parameters by which to sort the display.
7. For each secondary Then By sort parameter chosen select whether to display the information either in Ascending or Descending order.
8. Click OK to run the sort process. Information in the configuration window is rearranged according to your selections.

Find

This option enables searching a configuration document to locate any record in a specific panel. The Role Engineer specifies the column name in the Search Column field of the Find window. The desired text is specified in the Search Text field. Any combination of alphanumeric characters can be specified (maximum 32 characters). However, Boolean or logical searches (for example, “>n” where n is any number) cannot be performed.

Records that corresponds to the search string, it is highlighted in gray. A search for more records containing the same string can be performed by clicking Find Next.

Drag scroll bar to view all the data types of a specific panel.

Users Database (Configuration Only)

To view the Users Database choose View, Users Database from the menu bar or use the Ctrl + U keystroke shortcut. A description of each field is provided in the following table:

Field	Description
Person ID	Required field.
User Name	Required field.
Organization ID	Required field.
Organization type	Required field.
User ID	Required field.
Field 1	Optional field.
Field 2	Optional field.
Field 3	Optional field.
Field 4	Optional field.
Field 5	Optional field.
Field 6	Optional field.

Double-clicking a user record opens the User Details window for editing.

Resources Database (Configuration Only)

To view the Resources Database choose View, Resources Database from the menu bar or use the Ctrl+R keystroke shortcut. A description of each field is provided in the following table:

Field	Description
Res Name 1	Res Name 1, 2, 3 comprise a unique resources key. Mandatory.
Res Name 2	Res Name 1, 2, 3 comprise a unique resources key. Mandatory.
Res Name 3	Res Name 1, 2, 3 comprise a unique resources key. Mandatory.
Res ID	Automatically-generated unique ID.
Users	Automatically-generated unique ID.
Total Users	Number of direct links counted by CA Identity Governance.

Field	Description
Roles	Number of direct and indirect links counted by CA Identity Governance.
Owner	Number of links to roles.
Field 1	Intended for country. Field name is user configurable.
Field 2	Intended for location. Field name is user configurable.
Field 3	Intended to indicate business unit. Field name is user configurable.
Field 4	Optional for free text.
Field 5	Optional for free text.
Field 6	Optional for free text.

Double-clicking a resource record opens the Resources Details window for editing .

Configuration Properties (Configuration Only)

Configuration Properties displays general statistics regarding the active configuration. This includes information that refers to the following:

- Users Database
- Resource Database
- Configuration File
- Statistics
- Properties

To view the configuration properties window, click View, Configuration Properties from the menu bar.

The Configuration Properties window appears.

The Properties group box in the Configuration Properties window contains a number of fields that are either updated by the system or for which the contents can be edited and saved for your own purposes. The following table lists the fields and provides a brief description as of their use.

Field	Description
Create Date	The date and time when the configuration file was created.
Modify Date	The date and time when the configuration file was last modified.

Field	Description
Owner 1	By default this field displays the login name for the machine on which the configuration file was created.
Owner 2	Optional field for free text.
Organization 1	Optional field for free text.
Organization 2	Optional field for free text.
Operation 1	If the file was created as a partial configuration of a pre-existing file, then the field indicates the operation used to create the current configuration file.
Operation 2	Optional field for free text.
Operation 3	Optional field for free text.
Status	Optional field for free text.
Status Date	List the date and time when the Status field was last updated.
Parent Configuration	List the name of the configuration file from which the current configuration file was extracted.

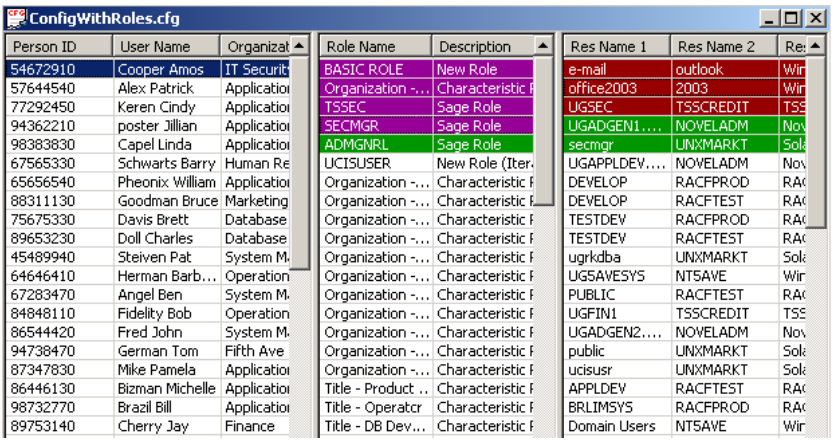
Show Linked Entities

This option shows all directly and indirectly linked entities. The entity types that you can view include:

- Direct links
- Indirect links
- Dual links
- Common links
- Expired roles
- Approved roles
- Not approved roles

To view linked entities

1. Select an entity from the Users Panel.
2. Click View, Show Linked Entities or right-click the selected panel and choose Show Linked Entities from the right-click menu.
3. A window similar to the following appears.



Links are displayed using the following color coding:

Green

Indirect Links

Purple

Direct links

Red

Dual links

Blue

Expired roles, Approved roles, Not Approved Roles

This option also works for a selected group of entities. For example, if several entities are selected, Show Linked Entities will display all of a group's directly and indirectly linked entities.

Refresh Current Window

Refresh the current window after performing operations that may have affected the display. For example, to eliminate highlights or grayed rows that remain on-screen from a previous activity.

View Overlaps in a Configuration

CA Identity Governance provides a special tool for handling situations in which two very similar roles or resources have been discovered that is available when a configuration file is open.

Roles Overlap – Choose Whether to Merge

Two roles that are presumed to be very similar can be examined using the View Roles Overlap option and, if judged to be worthy of being designated as the same role, can be automatically merged. This option is only available from the right-click menu.

To activate the View Roles Overlap option

1. Highlight the two roles in a configuration menu.
2. Right-click on the highlighted roles.
3. Select View Roles Overlap and Choose Whether to Merge from the right-click controls menu.

   The Merge Role Definitions window opens.

   The Merge Roles Definition window provides statistics on the users, resources, sub-roles and parent roles of each of the two roles and shows statistics on the degree to which they are the same.

   The following options are available:

   Merge Into

   Merges one role into the other.

   Empty

   Deletes selected items from the role.

   Make Alias (Parent)

   Makes the selected role a parent.

   Leave As-Is

   Does not make any changes to the roles.

   Merge Users

   Select this option to merge users.

   Merge Resources

   Select this option to merge resources.

   Merge Sub-roles

   Select this option to merge sub-roles.

   Merge Parent Roles

   Select this option to merge parent roles.

   Select the options you want.
4. Click OK to make the selected changes.

Users Overlap – Choose Whether to Merge

Two users that are presumed to be very similar can be examined using the View Users Overlap option. The Merge Users window provides statistics on roles and resources for each of the two highlighted users and shows statistics on the degree of overlap. This option is only available from the right-click menu.

To activate the view users overlap option

1. Highlight the relevant users in a configuration menu.
2. Right-click on the highlighted users.
3. Click View Users Overlap and Choose Whether to Merge from the right-click menu.

   The Merge User Definitions window opens.

   The following options are available:

   Merge Into

   Merges one user into the other.

   Empty

   Deletes all roles and resources of the selected users.

   Leave As-Is

   Does not make any changes to the users.

   Merge Resources

   Select this option to merge resources.

   Merge Roles

   Select this option to merge roles.

   Select the options you want.
4. Click OK to make the selected changes.

View Resources Overlap – Choose Whether to Merge

Two resources that are presumed to be very similar can be examined using the View Resources Overlap option and, if judged to be worthy of being designated as the same resource, can be automatically merged.

To activate the View Resources Overlap option

1. Highlight the relevant resources in a configuration menu.
2. Right-click on the highlighted resources.
3. Select View Resources Overlap, Choose Whether to Merge from the right-click menu.

   The Merge Resources window opens.

   The Merge Resources window provides statistics on users' roles for each of the two highlighted entities and shows statistics on the degree of overlap.

   The following options are available:

   Merge Into

   Merges one user into the other.

   Empty Users

   Deletes all roles and resources of the selected users.

   Leave As-Is

   Does not make any changes to the users.

   Merge Users

   Select this option to merge users.

   Merge Roles

   Select this option to merge roles.

   Select the options you want.
4. Click OK to make the selected changes.

Business Policy Properties (Policy Only)

When a Business Policy (BPR) window is open, basic policy statistics are displayed using this option.

More information:

Check Policy Compliance (see page 149)

Set Print Fonts (AuditCard Only)

When an AuditCard window is open, this option appears in the View menu.

More information:

Print Reports (see page 120)

Chapter 7: Role Discovery

A role is a common set of privileges shared by a group of users within an organization. These privileges usually include resources that are integral to users' performance of their role. The Discovery menu provides a set of tools for examining imported user and resources data in order to distinguish roles embedded in long lists of users and resources data. Client tools implement internal algorithms to "discover" and "propose" role candidates. The Role Engineer provides input during the discovery process by determining criteria and thresholds.

These discovery tools represent different strategies that can be implemented in the role discovery process. The Role Engineer can use one, some or all the strategies in the course of the role discovery process, depending on the nature of the specific organization under examination.

Users can have different sets of privileges that are presumably related to several different roles that they perform. Therefore, roles proposed must be carefully examined and refined to establish conformance with the existing situation within the organization.

This section contains the following topics:

Basic Roles

This option applies to the currently selected CA Identity Governance configuration and identifies possible roles that do not seem to fit into previously defined roles. It is generally recommended to generate a limited set of 3 – 5 candidates, review and select a single candidate, and refine the role. The first set that meet the search criteria will be identified and displayed. The run time to discover roles depends mainly on the parameters specified. If necessary, Basic Roles can be run again with the new role (refer to Iterated Search in the following section).

The following table describes the available fields:

Field	Description
Default Description	A textual description used for your own purposes that later appears as the role's description in the configuration file. This description is different from the actual name of the role candidate, which is assigned by CA Identity Governance. The user can rename each candidate and change its description later. Sometimes it is convenient to fill in a name and/or date in this field. However, do not leave it blank.
Role Name Prefix	Set a prefix that is added to the role name for each role that is discovered.
Minimum number of users	Minimum number of users that should be included in a role candidate
Minimum number of resources	Minimum number of resources that should be included in role candidate
Maximum number of role candidates to propose	Maximum number of role candidates to be proposed in this run. We recommend generating no more than 10 new role candidates in each session. Roles proposed in a single session may have significant overlap with one another thereby increasing the work load on the Role Engineer to distinguish among them.
Minimum newly covered connections	Minimum number of Users, Resources, and User-Resource connections that must be covered by a role candidate and that were not covered by existing and previously discovered roles. This feature is useful to discover roles that are as disjointed from previously discovered roles as possible. If not relevant, use 0. Values can be entered as whole numbers or as a percentage of newly covered connections.

Field	Description
Minimum Users not Covered	Sets the minimum number of Users or the minimum percentage of Users that are not previously discovered by a role.
Minimum Resources not Covered	Sets the minimum number of Resources or the minimum percentage of Resources that are not previously discovered by a role.

The results of a typical Basic Role Discovery run are displayed in a new configuration.

The role name is automatically incremented with each run and is viewable in the Person ID column.

The Default role description is viewable in the User Name column.

Iterated Search

This option repeatedly invokes the Basic Roles search function (refer to previous section). However, to implement different search strategies, e.g., search for roles with maximal number of users, the iterated search may require tens and even hundreds of iterations of Basic Search. In each iteration, search parameters are adjusted according to the results of the previous search. If the search is successful, CA Identity Governance retains the top role candidate, and proceeds to the next search.

Note: Since iterated searches are extensive and can take a long time, we recommend using the Basic search for interactive analysis and schedule iterated searches to run during periods of low activity such as over night.

One of three types of maximizing strategies can be selected in the Preferred Search Mode drop-down menu:

Prefer many users

Many users will be proposed who have the same set of resources.

Prefer many resources

Many resources will be proposed that have the same users associated with them.

Prefer many user-resource connections

Each discovered role will have many users and resources associated with it.

More information:

Basic Roles (see page 104)

Discovering Characteristic Roles

It is often preferable to create roles around organizational units, functions, locations, reporting structure, etc. The characteristic roles function help automate this process.

You can seek roles that are characteristic to each organizational unit by selecting the organizational unit attribute of a user, and running a search with the preferred parameters.

The following table describes the specific fields of the characteristic search:

Field	Description
Role Name Prefix	Set a prefix to be included as part of each role discovered.
User Attribute	You set one of the users attributes to serve as the basis for the characteristic role search. CA Identity Governance will create roles for each group of users that have same value in the selected attribute. Thus, if you select the organization field, CA Identity Governance will create organizational roles.
Resource Attribute	You set one of the resource attributes to serve as the basis for the characteristic role search. CA Identity Governance will create roles for each group of resources that have same value in the selected attribute. Thus, if you select the Res Name 1 field, CA Identity Governance creates roles based on values belonging to Res Name 1.
From/To Attribute Value	Specify the range of values for which roles will be searched. This is useful in case you wish to search for a single role, or for a part of a hierarchy.
Minimum Percent of Sub-Group Users	Specify the threshold for creating a characteristic role. For example, you may require a role that characterizes at least 90% of the users in each of the sub-groups. If you specify a high value, CA Identity Governance may not find a role for all selected groups. In any case, CA Identity Governance will only associate with the role users that have the role's resources. Use "almost matching" search to identify users that almost match.
Preferred Search Mode	Indicates whether to make the Users, Resources or User-Resource Connections the focus of the roles created by the rule.

The rest of the parameters of the Characteristic Roles Search are similar to the ones that you have already seen in the Basic and Iterated Searches.

More information:

Iterated Search (see page 105)

Discovering Rule-Based Roles

Client tools provide you with the capability to establish Rule-Based Roles during the discovery process. By assigning a set of User attributes that defines a rule. Client tools search the configuration to identify and establish roles that include users that match the rule. Roles that are created using this mechanism are identified as rule based roles and the roles are added to configuration. You can set several parameters to refine the process by which rule based roles are identified.

To assign rules for the discovery process

1. From the Discovery menu, select Rule-Based Roles.

   The Discover Rule-Based Roles window opens.

2. Set the Search Parameters as described for Basic Roles.

3. In the Rules Parameters group, specify Rule Parameters to create rule-based roles during discovery. The following options are available:

   Role Name Prefix

   Defines a prefix to be included as part of each role discovered.

   User Attributes to Search

   You can set several Users Attributes to serve as the basis for the rules-based role search. CA Identity Governance creates roles for each group of users that match the attributes added to the Attributes to Search list. Thus, if you select the Organization and organization Type attributes, client tools create roles for groups of Users that match the selection and that have common resources.

   Ignore Null Value

   Select this option to prevent rules being created where an attribute does not contain any values.

   Min. Percent within Group

   Specify the range of values for which roles will be searched. This is useful in case you wish to search for a single role, or for a part of a hierarchy.

Max. Rules per Group

Specify the threshold for creating a characteristic role. For example, you may require a role that characterizes at least 90% of the users in each of the sub-groups. If you specify a high value, CA Identity Governance may not find a role for all selected groups. In any case, CA Identity Governance will only associate with the role users that have the role's resources. Use "almost matching" search to identify users that almost match.

Preferred Search Mode

Indicates whether to discover roles with a preference to Users, Resources or User-Resource Connections as the focus of the roles created by the rule.

4. Click Search to start the discovery process.

   Newly created roles are listed in a new configuration file.

More information:

Basic Roles (see page 104)

Discovery – Structured Search

The Structured Search supported by the Discovery process that the client tools provide extends the Rule-Based search process. The rule-based role search process finds roles that match each attribute chosen in a flat manner. The Structured Search creates roles that reflect the hierarchic structure of the search attributes that you choose. Roles that are created using this mechanism are provided with the text Structured at the beginning of the role name. Roles discovered via a Structured Search are provided with a rule that reflects the hierarchic path of the search, and are added to the configuration. You can set several parameters to refine the process by which rule based roles are identified.

To assign attributes for the Structured Search process

1. From the Discovery menu, select Structured Search.

   The Structured Search window opens.

2. Set the Search Parameters as described for Basic Roles.

3. In the Rules Parameters group, specify Rule Parameters to create rule-based roles during discovery. The following options are available:

   Role Name Prefix

   Defines a prefix to be included as part of each role discovered.

User Attributes to Search

You can set several Users Attributes to serve as the basis for the rules-based role search. CA Identity Governance creates roles for each group of users that match the attributes added to the Attributes to Search list. Thus, if you select the Organization and organization Type attributes, the client tools create roles for groups of Users that match the selection and that have common resources.

Select All Attributes

When selected, the client tools override all previously selected user attributes and takes all the configuration's User Attributes into consideration when conducting the search.

Let DNA Order Attributes

When selected, Client Tools override the Search order as listed in the User Attributes list.

Ignore Null Value

Select this option to prevent rules being created where an attribute does not contain any values.

Min. Percent within Group

Specify the range of values for which roles will be searched. This is useful in case you wish to search for a single role, or for a part of a hierarchy.

Max. Rules per Group

Specify the threshold for creating a characteristic role. For example, you may require a role that characterizes at least 90% of the users in each of the sub-groups. If you specify a high value, CA Identity Governance may not find a role for all selected groups. In any case, CA Identity Governance will only associate with the role users that have the role's resources. Use "almost matching" search to identify users that almost match.

Preferred Search Mode

Indicates whether to discover roles with a preference to Users, Resources or User-Resource Connections as the focus of the roles created by the rule.

4. Click Search, to start the discovery process.

   Newly created roles are listed in a new configuration file.

More information:

Basic Roles (see page 104)

Obvious Roles

Obvious role candidates are a group of users that share *exactly* the same resources or a set of resources that have *exactly* the same users.

One of two strategies can be selected in the Preferred Search Mode menu:

Users with exactly the same resources

Roles will be proposed, the members of which are users that possess links to exactly the same resources.

Resources with exactly the same users

Roles will be proposed, the members of which are resources that possess links to exactly the same users.

Discovering Modeled-After Roles

CA Identity Governancesupports two types of modeled-after roles:

By users

In this type, CA Identity Governancecreates a role that is exemplified by a select group of users. CA Identity Governance will complete the role with the relevant resource, and other users that have not been explicitly selected but that share the role's resources. Use this form to create a role for the organizational unit, function, or any other feature that is common to the selected group of users.

By resources

In this type, CA Identity Governance creates a role that is exemplified by a select group of resources. CA Identity Governance will complete the role with the relevant users, and will add other resources that have not been explicitly selected but that are shared by the role's users. Use this form to create a role for a project or application.

When searching for roles that are modeled after a group of users, CA Identity Governance identifies the resources that are common to the selected users, and then completes the role with additional users. The result of running Define Modeled-After Roles by Users is a new CA Identity Governance configuration that includes the “model” users and any other users that possess the same resources as the “modeled-after” users.

To activate modeled-after search by users, select the model users, then use either the Discovery menu or the context menu (right click).

When searching for roles that are modeled after a group of resources, the client tools identify the users that are common to the selected resources, and then completes the role with additional resources. The result of running Define Modeled-After Roles by Resources is a new CA Identity Governance configuration that includes the “model” resources and any other resources that are accessible to the same users as the “modeled-after” resources.

To activate modeled-after search by resources, select the model resources, then use either the Discovery menu or the context menu (right-click).

Defining Roles Manually and for a Select Group of Users/Resources

You can define roles manually, as well as for a selected set of users or resources.

To create a role manually, select the New Role feature from the Edit Menu. Roles created that way are initially not associated with any users or resources. To add those, you drag and drop within the configuration.

You can also create roles for a select set of users or alternatively for a select group of resources. To do so, select the resources and choose New Role By Users/Resources from the context menu (right click). A new role will be created in the configuration with the selected users/resources and all resources/users that are common to all of them.

More information:

Create a Role (Configuration Only) (see page 69)

Identify Almost Perfect Matches

This option enables finding almost perfect matches based on users, resources or roles criteria determined by the Role Engineer. The intention here is to find matches that differ slightly from one another for the purpose of verifying the appropriateness of their qualifications (users, roles or resources) to the role that they possess. This option is useful to identify situations in which slight differences have resulted, for example, due to shifting job functions.

Propose Closely Matching Users

To find closely matching users

1. Choose a single role from the Roles Panel.

   Click Discovery, Identify Almost Perfect Matches, Closely Matching Users or right-click the Roles Panel and select Closely Matching Users.

   It is now necessary to determine the extent of matching resources; the client tools display default values. The following variables can be set when searching for closely matching users:

   Minimum Number of Matching Resources

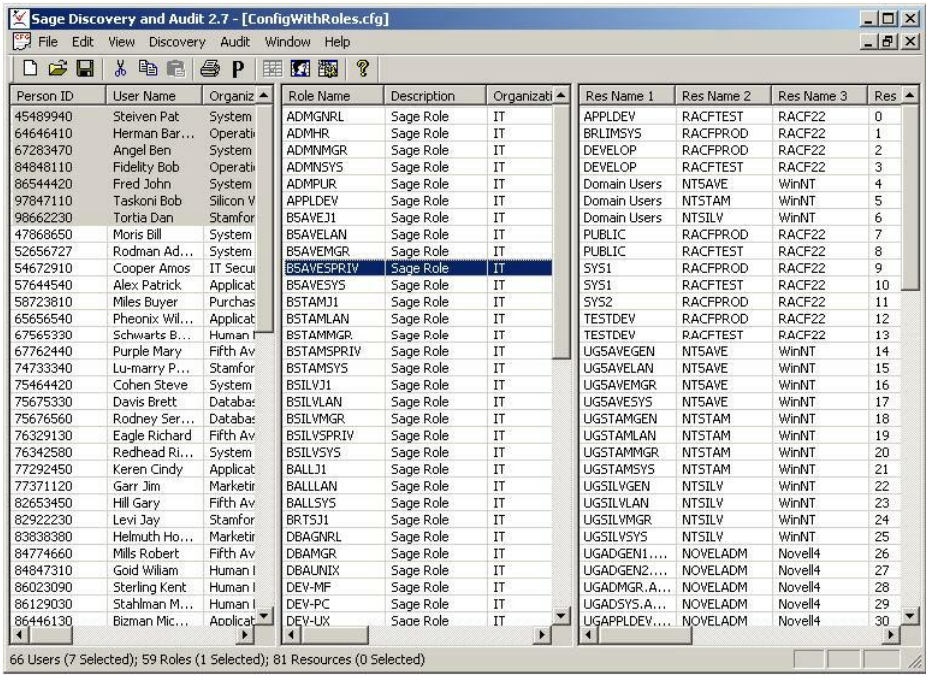
   An absolute number of resources that match that of the role to match.

   Minimum Percent of Matching Resources

   On a scale of 1 to 100 percent. The result is determined by an internal algorithm.

2. After filling in the values, click OK to generate the results.

The following is a typical results window. Closely matching user are marked in Gray. Selected role on which results are based is highlighted.



The role to which users are to be matched remains highlighted. The closely matching users that meet the search criteria are marked in gray in the Users Panel.

Propose Closely Matching Resources

To find closely matching resources

1. Choose a single role from the Roles Panel.
2. Go to Discovery, Identify Almost Perfect Matches on the menu bar and select Closely Matching Resources, or right-click on the Roles Panel and select Closely Matching Resources.

   At this point, it is necessary to determine the extent of matching users; CA Identity Governance will display default values. The following variables can be set when searching for closely matching resources:

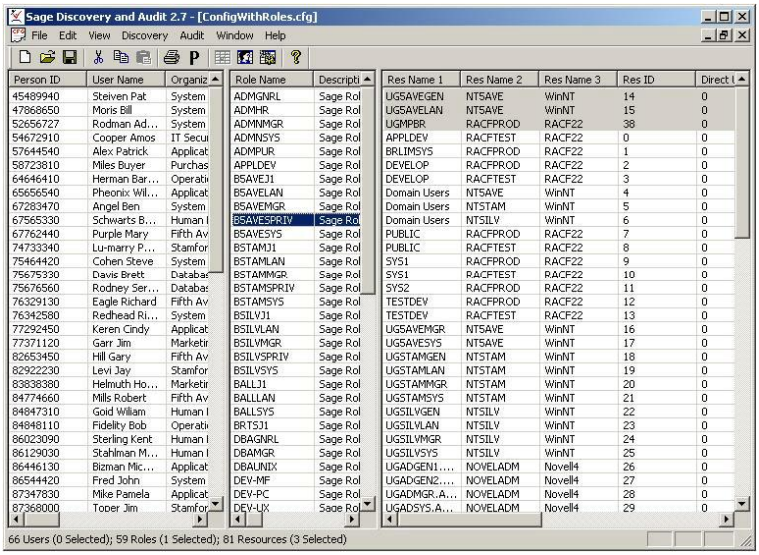
   Minimum Number of Matching Users

   An absolute number of users that match that of the role to match.

   Minimum Percent of Matching Users

   On a scale of 1 to 100 percent. The result is determined by an internal algorithm.
3. After filling in the values, click OK to generate the results.

The following is a typical results window: Selected role on which results are based are highlighted. Closely matching resources are marked in Gray.



The role to which resources are to be matched remains highlighted. The closely matching resources that meet the search criteria are marked in gray in the Resources Panel.

Propose Closely Matching Roles

CA Identity Governance enables finding closely matching roles based on either a user or resource.

More information:

Propose Closely Matching Users (see page 112)
Propose Closely Matching Resources (see page 113)

Based on User

To find closely matching roles based on a user

1. Select the user in the Users Panel.
2. Go to Discovery, Identify Almost Perfect Matches on the menu bar and select Closely Matching Roles, or right-click on the users record in the Users Panel and select Almost Matching Roles from the right-click controls menu.
3. The Almost Matching Roles window opens .

   At this point, it is necessary to determine the extent of matching resources; CA Identity Governance will display default values. The following variables can be set when searching for closely matching users:

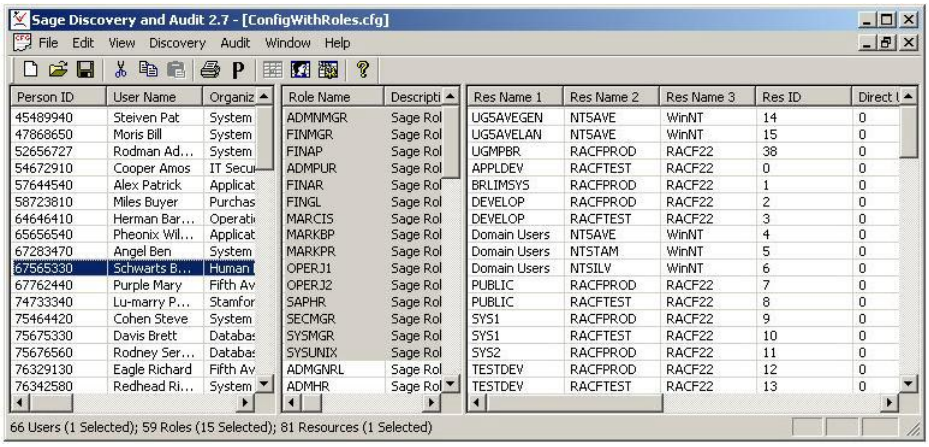
   Minimum Number of Matching Resources

   An absolute number of resources that match that of the role to match.

   Minimum Percent of Matching Resources

   On a scale of 1 to 100 percent. The result is determined by an internal algorithm.
4. After filling in the values, click OK to generate the results.

The following is a typical results window. User on which results are based are highlighted. Closely matching roles are in gray.



Based on Resource

To find closely matching roles based on a resource

1. Select the resource in the Resources Panel.
2. Go to Discovery, Identify Almost Perfect Matches on the menu bar and select Closely Matching Roles, or right-click on the resources record in the Resources Panel and select Almost Matching Roles from the right-click controls menu. The Almost Matching Roles window opens.

   At this point, it is necessary to determine the extent of matching users. CA Identity Governance will display default values. The following variables can be set when searching for closely matching resources:

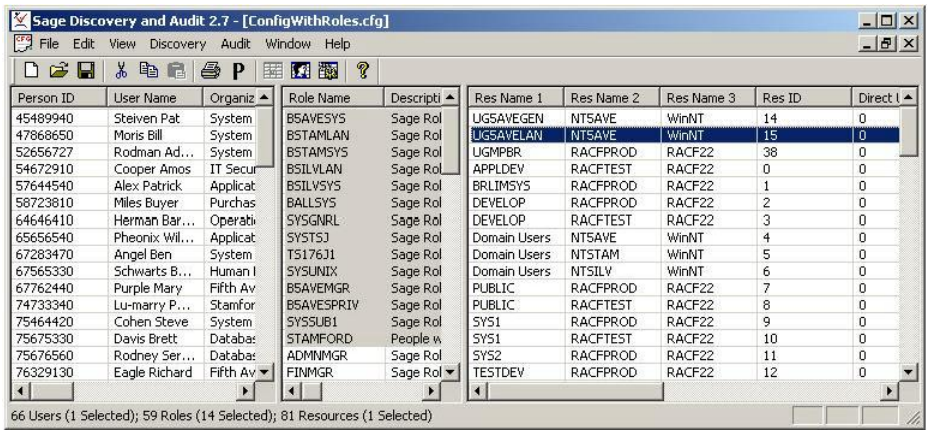
   Minimum Number of Matching Users

   An absolute number of users that match that of the role to match.

   Minimum Percent of Matching Users

   On a scale of 1 to 100 percent. The result is determined by an internal algorithm.
3. After filling in the values, click OK to generate the results.

The following is a typical results window. Selected resource on which results are highlighted. Closely matching roles are marked in Gray.



Identify Role Hierarchy

This option identifies possible family relationships between roles: sub-roles (children) or parent roles (parents) or other possibly related roles This option is activated by highlighting a role and going to Discovery, Identify Role Hierarchy on the menu bar and choosing one of the following options: propose sub-role, propose parent role, propose related role. The proposed roles will be highlighted. Drag and drop the highlighted roles onto the role in question to confirm the relationship.

Note: Role hierarchy can only be determined after roles have been determined for a given configuration. If only users and resources data were imported and no possible roles have yet been discovered and confirmed, the strategies in earlier in this chapter before hierarchy can be discovered.

More information:

Basic Roles (see page 104)
Defining Roles Manually and for a Select Group of Users/Resources (see page 111)

Propose Sub Roles

This option displays roles that can possibly be sub-roles (children) of a highlighted role. CA Identity Governance finds possible sub-roles by examining other existing roles in the configuration to determine whether the highlighted role includes resources of other roles in the configuration. If so, those roles are designated as sub-roles of the highlighted role.

Highlight the role for which sub-roles are to be identified. The option will highlight the possible sub-roles of the indicated role.

Note: Original role jumps to top of Roles Panel and sub-role is highlighted under it.

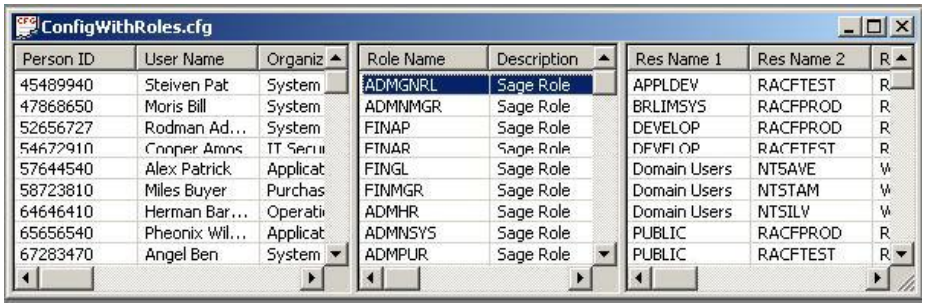
The Role Engineer would then individually examine each proposed sub-role. If a parent-sub-role (child) relationship exists, then the sub-roles would be dragged to the parent role, which would then show the new roles as sub-roles of the original role (parent).

Propose Parent Roles

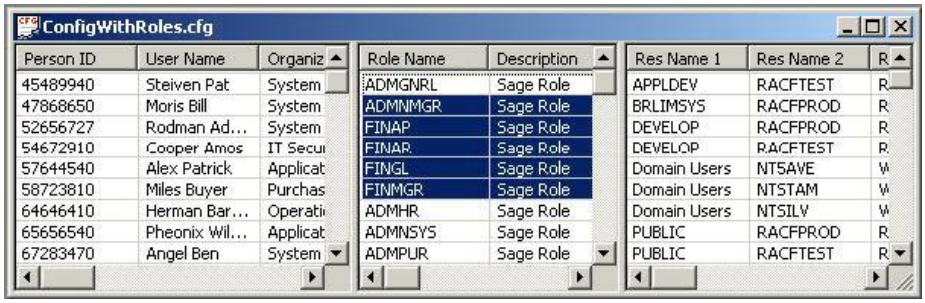
This option displays roles that can possibly be parents of a highlighted role. CA Identity Governance finds possible parent roles by examining other existing roles in the configuration to determine whether the resources of the highlighted role are already **included** as resources in other roles. If so, they are designated as possible parent roles.

Highlight the role for which parent roles are to be identified. The option will highlight the possible parent roles of the indicated role.

Original highlighted role is highlighted.



Possible parent- roles of the original role are highlighted as follows:



The Role Engineer would then individually examine each proposed parent role. If a parent-sub-role (child) relationship exists, then the sub role would be dragged to the parent role, which would then show the original role as one of its sub-roles.

Propose Related Roles

A related role is a role that shares users and/or resources with a selected role but is neither its parent role nor its sub-role. To run this option, it is necessary to provide a minimum number of users and resources.

Highlight the role for which related roles are to be identified. Go to Discovery, Identify Role Hierarchy on the menu bar and choose Propose Related Role.

Modify the default values as necessary and click OK. Related roles appear. The Role Engineer then individually examines each proposed related role.

Reject Discovered Roles

The Reject option is useful in order to prevent display of roles that were discovered but are no longer needed. Roles that are outdated or that are unused can be rejected from the configuration file. Rejected roles are collected and stored in a special configuration file called Rejected.cfg. The file, Rejected.cfg, is automatically created when the first role candidate is rejected and is usually located in the same folder as the other *.cfg files.

To reject a role, highlight the role to be rejected, go to Discovery on the menu bar and choose Reject. A confirmation prompt is displayed before the reject activity is performed.

This configuration can be opened for viewing. The configuration can be manipulated as for any other CA Identity Governance configuration, including dragging roles to and from it. At any point roles that need to returned to general use can be returned to the active configuration file by simply removing them from the Rejected configuration file. In this way they are returned to general use.

Selecting a Specific *.cfg file to House Rejected Roles

You can create a new configuration file or select any pre-existing *.cfg file to function as the Rejected roles configuration file. Once this is done then the newly assigned file assumes the function of collecting rejected roles instead of the default Rejected.cfg file.

To select a specific configuration file to house Rejected roles

1. Click File, Select Rejected Roles File.

   The Save As dialog box opens to the directory that houses the projects pre-existing configuration files.

2. Select a file from the list or type a new name into the File name field.

3. Click Save.

   The newly selected file functions to house rejected roles from that point on.

Print Reports

You can make basic font and format changes to reports before publishing. This avoids the problems inherent in exporting report data to another application for formatting and printing purposes.

An Entity Report and Role Analysis Report are generated when a configuration document is open. An AuditCard Report is generated when an AuditCard is open.

Note: In addition to the Entity Report and Role Analysis Report, CA Identity Governance enables printing the Users Database and the Resources Database. Printing these documents is performed by the standard Windows method using the File, Print option on the menu bar.

More information:

Entity Report (see page 121)
Role Analysis Report (see page 122)

Entity Report

An Entity Report is generated when a configuration window is active. This feature enables printing a report of any single or several highlighted entities in report format. Entity types are users, roles and resources. Only one type of entity report can be printed at a time. For example, a role report would include unique data of the role as well as direct users, direct resources, sub-roles and parent roles.

This section will describe how Role Engineers can adjust the print parameters to obtain a printed report that is suitable to their needs.

To print an Entity Analysis Report

1. Open the configuration that contains the desired entities.
2. Highlight the entity (or entities) to be printed. If a report that includes more than one entity of a certain type is being generated, the Ctrl + mouse click or Shift + mouse combination can be used to highlight them.

Print Preview

Go to Discovery, Entity Analysis Report on the menu bar and choose Print Preview.

The following options are available from the Preview Print button bar:

Button	Description
Print	Prints the document as it appears on screen.
Next Page	Displays the next page of the report.
Prev Page	Displays the previous page of the report.
One Page / Two Page	Toggles between displaying one page or two pages of the document.
Zoom In	When the pointing device is held on a page of the report, the pointer changes from its normal appearance (usually an arrowhead) to a magnifying glass icon. This signifies that by clicking on the document zoom-in will be performed. Usually, it is possible to zoom in two orders of magnitude (clicking each time to do so). Clicking a third time will return the document image to its original size.
Zoom Out	After zoom-in is performed (by clicking on the document image), the Zoom Out button becomes active. Click the Zoom Out button to return the document image to its original size.
Close	Closes the Preview window and returns to the previous window.

Print Fonts

The report fonts can be set from inside the Set Print Fonts window.

To set the report print fonts

1. From the menu bar select Print, Set Print Fonts.
2. For each print font element click the Set button. The Font window opens.
3. Make your font selections.
4. Click OK and your choices are shown in the Set Print Fonts window

Note that four types of fonts can be determined for different parts of the report: header, footer, title and text.

Note: These font choices become the print default for all subsequent print jobs until they are changed.

Print Setup

To print, choose Print Setup from the menu bar. Verify that the printer is connected and in proper working order. Verify that the name of the printer in the print setup window matches the printer to which you are printing, size of the paper is correct and portrait or landscape printing has been chosen, as appropriate for the print job.

Role Analysis Report

A Role Analysis Report is generated when a configuration window is active. This feature enables printing a report of any single or several roles plus an analysis.

A Role Analysis Report includes the data in a Role Entity Report as well as almost matching users, almost matching resources, potential sub-roles, potential parent roles, and related roles. The thresholds of these parameters are determined in the Discovery menu.

More information:

Role Discovery (see page 103)
Print Reports (see page 120)

AuditCard Report

CA Identity Governance enables printing an entire AuditCard or selected records as designated by the Role Engineer. An AuditCard report is generated when an AuditCard is active. Large systems may generate long and unwieldy lists of alerts, so it may be advisable to print only selected parts for further examination. This subject is covered below.

Print Selected Preview

To print selected parts of an AuditCard, highlight those specific alerts in the AuditCard. Use the Windows Ctrl + Mouse click and Shift + Mouse click to mark the desired alerts. This option opens the preview window where the print job can be reviewed before printing.

Print Selected

Opens the Microsoft Windows Print Setup window to print the selected alerts. The report can be printed directly without previewing.

Chapter 8: Audit Menu

The Audit menu provides review and auditing functions:

- Pattern-based auditing
- Compliance auditing, based on policies (BPR)
- Review of current roles
- Search for suspected users, resources, and role definitions

Some audit options, which focus on specific types of problems, can be run separately from dedicated windows: identify potential collectors, suspected resources, suspect role definitions or excess privileges (see below). Alternatively, a comprehensive audit can be performed, which includes a wide variety of variables. Output is displayed in the AuditCard window as a list of suspicious records showing the type of problem detected for each record and other relevant data.

Suspicions are handled and managed from the Edit menu.

In addition to in-built pattern-based audit tools, CA Identity Governance enables the creation of policies using sets of Business Process Rules (BPR).

This section contains the following topics:

Identify Potential Collectors

This option identifies users that have apparently accumulated excessive privileges (access to resources), i.e., they are potential collectors. This phenomenon often occurs when veteran employees move from job to job within an organization and accumulate privileges without relinquishing their previous ones.

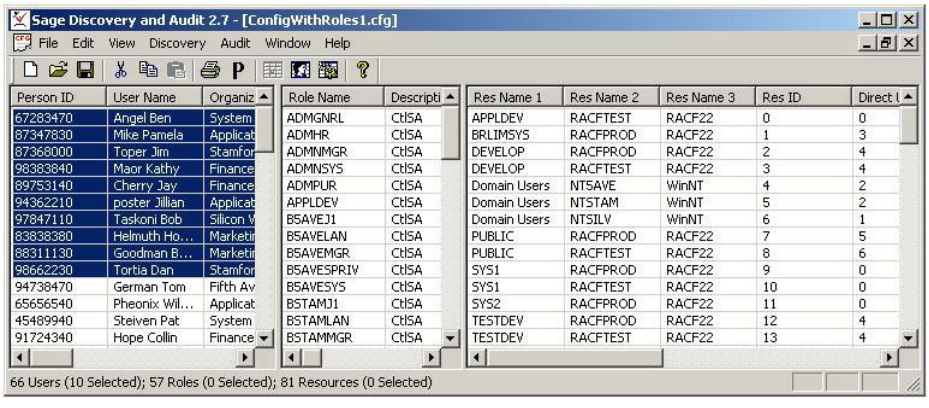
Proprietary algorithms identify the suspected users based on the criteria and weighted values that the Role Engineer enters in the Identify Potential Collectors window. Generally, identification is based on a user who seems to be an exception among similar users who also possess many resources. Note that this option can be used even before any roles are defined, for example, to clean up an imported database.

Use the Details toggle button to show the whole Identify Potential Collectors window.

The following table describes the fields in the window:

	Criteria	Description
Criteria	Maximum number of users to propose	Limits the maximum number of users displayed to no more than the indicated absolute number thereby preventing display of an unmanageable number of suspects.
	Maximum percent of users to propose	The percentage of users to display out of all those who meet the criteria.
	Minimum number of resources per user	Each displayed user will have at least the indicated number of resources.
Evaluation Weights	Organization	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Organization Type	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Country	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Location	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Title	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Cost Center	Enter a value on a scale of 1 to 10 where 10 is the greatest value.

The following is a typical configuration window showing results after running this option.



The Role Engineer can now examine each user one-by-one to determine if in fact any users are collectors of privileges (resources).

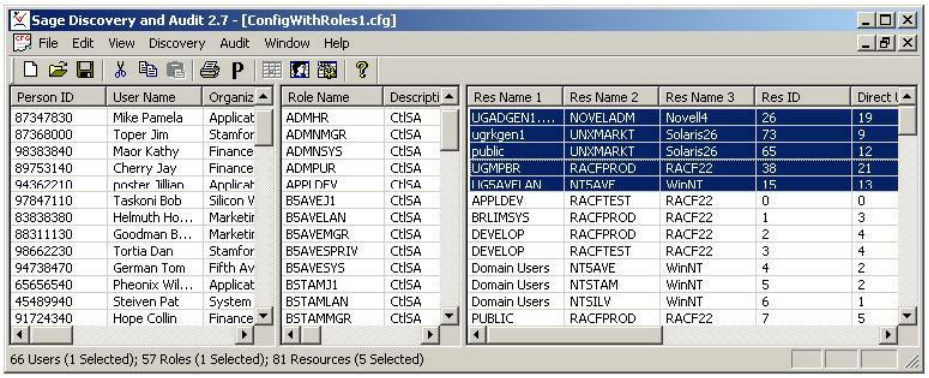
Identify Suspected Resources

This option identifies resources that are owned by many types of users.

The following table describes the fields in the window:

	Criteria	Description
Criteria	Maximum number of resources to propose	Limits the maximum number of resources displayed to no more than the indicated absolute number thereby preventing display of an unmanageable number of suspects.
	Maximum percent of resources to propose	The percentage of resources to display out of all those who meet the criteria.
	Minimum number of users per resource	Each resource will have at least the indicated number of users.
Evaluation Weights	Organization	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Organization Type	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Country	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Location	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Title	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Cost Center	Enter a value on a scale of 1 to 10 where 10 is the greatest value.

The following is a typical configuration window showing results window after running this option.



The Role Engineer can now examine each resource one-by-one to determine if in fact any suspected resource is not in compliance.

Identify Suspect Role Definitions

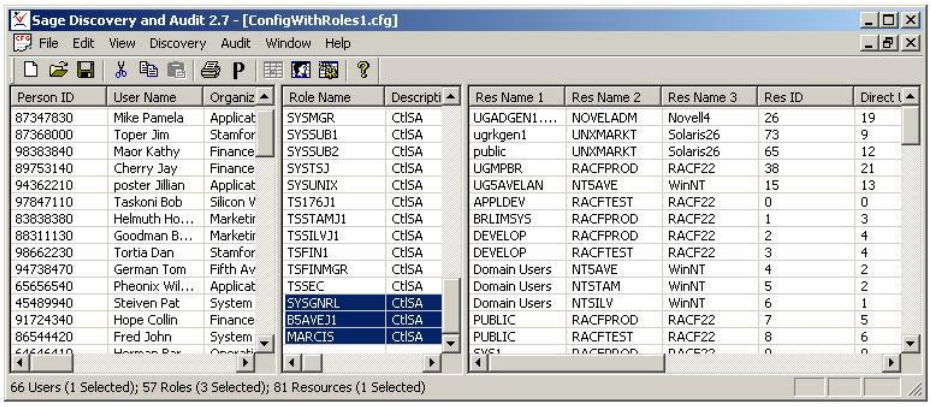
This option identifies roles that are owned by many types of users or suspected users; that is, users possess roles but do not seem to comprise a homogeneous group.

The following table describes the fields in the window:

	Criteria	Description
Criteria	Maximum number of roles to propose	Limits the maximum number of roles displayed to no more than the absolute indicated number, preventing display of an unmanageable number of suspects.
	Maximum percent of roles to propose	The percentage of roles to display out of all that meet the criteria.
	Minimum number of users per role	Indicates the minimum number of users for each suspect role.
	Minimum number of resources per role	Each role has at least the indicated number of resources.
Evaluation Weights	Organization	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Organization Type	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
	Country	Enter a value on a scale of 1 to 10 where 10 is the greatest value.

Criteria	Description
Location	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
Title	Enter a value on a scale of 1 to 10 where 10 is the greatest value.
Cost Center	Enter a value on a scale of 1 to 10 where 10 is the greatest value.

The following is a typical configuration window showing results after running this option.



The Role Engineer can now examine each role one-by-one to determine if in fact any suspected role is not in compliance.

Identify Excess Privileges

These options identify potentially excessive links for individual users, resources and roles.

This section contains the following topics:

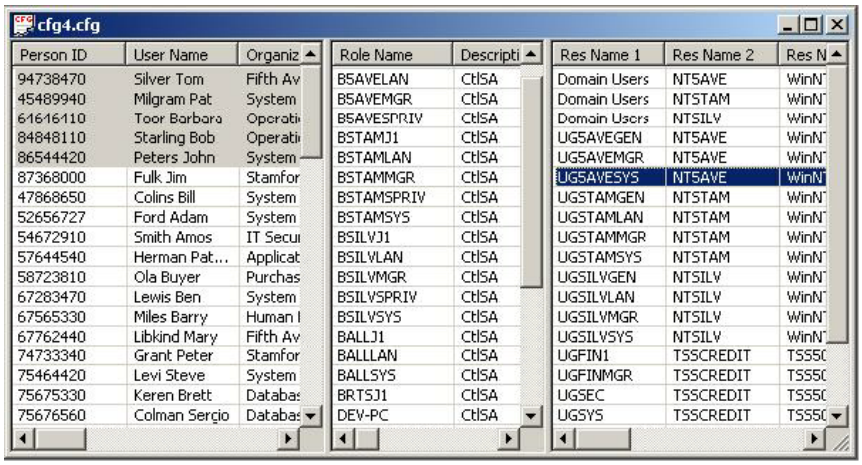
Propose Potentially Excess Users

This option proposes roles or resources that seem to have too many users.

To activate this option, highlight a role or resource in a configuration. Then on the menu bar, go to Audit, Identify Excess Privileges, and select Propose Potentially Excess Users.

The criteria (Minimum Degree of Mismatch) is determined by the Role Engineer on a scale of 0 to 100. If too many or too few users are identified then the scale should be changed appropriately. The evaluation weights are similar to those described earlier in this chapter.

Refer to the following window. Excess users proposed are highlighted in gray. The resource is highlighted.



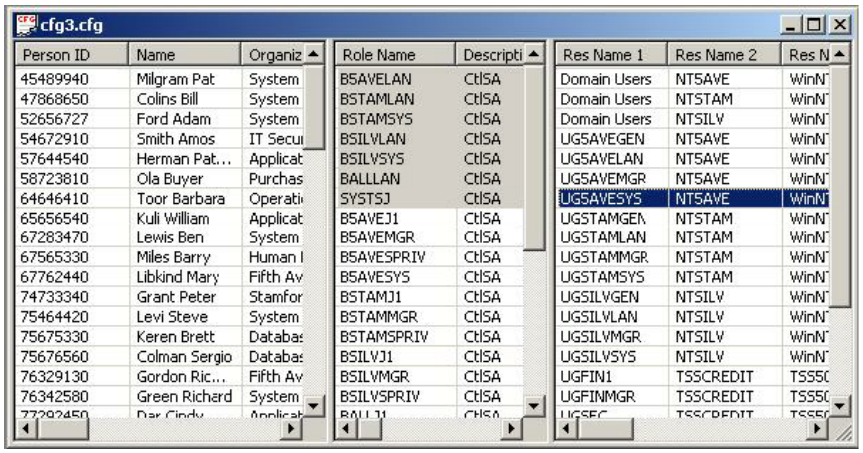
Propose Potentially Excess Roles

This option proposes users or resources that seem to have too many roles.

To activate this option, highlight a user or resource in a configuration. Then on the menu bar, go to Audit, Identify Excess Privileges, and select Propose Potentially Excess Roles.

The criteria (Minimum Degree of Mismatch) is determined by the Role Engineer on a scale of 0 to 100. If too many or too few users are identified then the scale should be changed appropriately. The evaluation weights are similar to those described earlier in this chapter.

Refer to the following window. Excess roles proposed are highlighted in gray for the highlighted resource.



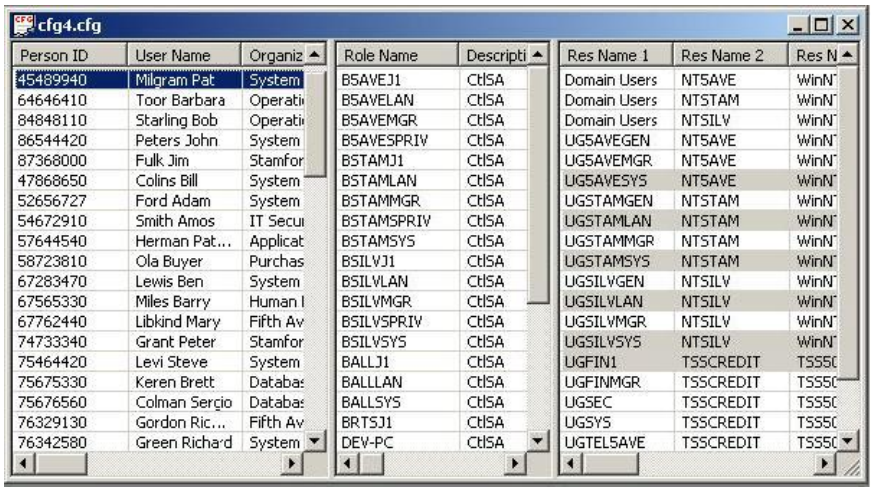
Propose Potentially Excess Resources

This option proposes users or roles that seem to have too many resources.

To activate this option, highlight a user or role in a configuration. Then on the menu bar, go to Audit, Identify Excess Privileges, and select Propose Potentially Excess Resources.

The criterion (Minimum Degree of Mismatch) is determined by the Role Engineer on a scale of 0 to 100. If too many or too few resources are identified then the scale should be changed appropriately. The evaluation weights are similar to those described in earlier in this chapter.

Excess resources are displayed in the Resources Panel. Refer to the following window. User is highlighted and the excess resources proposed are highlighted in gray.



Propose New Roles

This option identifies roles of which a user is not part, but which may be relevant to this user.

To activate this option, highlight a user in a configuration. Note that new roles can be proposed for only one user at a time. Right-click with the mouse to open the right-click controls menu, and select Propose New Roles.

The Propose New Roles window opens.

Click Details to open the whole window. Set the thresholds. CA Identity Governance searches for roles that include other users that are “similar” to the selected user. Proposed roles are highlighted in the Roles Panel.

More information:

Propose Potentially Excess Resources (see page 132)

Propose New Resources

This option identifies resources of which a user is not part, but which may be relevant to the highlighted user.

To activate this option, highlight a user in a configuration. Note that new resources can be proposed for only one user at a time. Right-click with the mouse to open the right-click controls menu, and select Propose New Resources.

The Propose New Resources window opens.

Click Details to open the whole window. Set the thresholds. CA Identity Governance searches for resources that are accessible to users similar to the current user. Proposed resources will be highlighted in the Resources Panel.

More information:

Propose Potentially Excess Resources (see page 132)

Show Similar Users

The Show Similar Users option identifies users that are similar to the highlighted user.

To activate this option, highlight a user in a configuration. Right-click with the mouse to open the right-click controls menu, and select Show Similar Users. Note that this option can also be applied to a set of users (all users in the set have to be highlighted).

The Show Similar Users window opens.

Click Details to open the whole window. Set the thresholds. Proposed similar users are highlighted in the Users Panel.

Generate and Manage AuditCards

CA Identity Governance provides a mechanism to identify and list suspicious users, roles, and resources in the following categories:

- Suspect Entities
- Suspect Connections
- Similar Roles and Role Hierarchy
- Similar Resources
- In/Out Of Pattern Entities
- Entities with Many/Few Connections

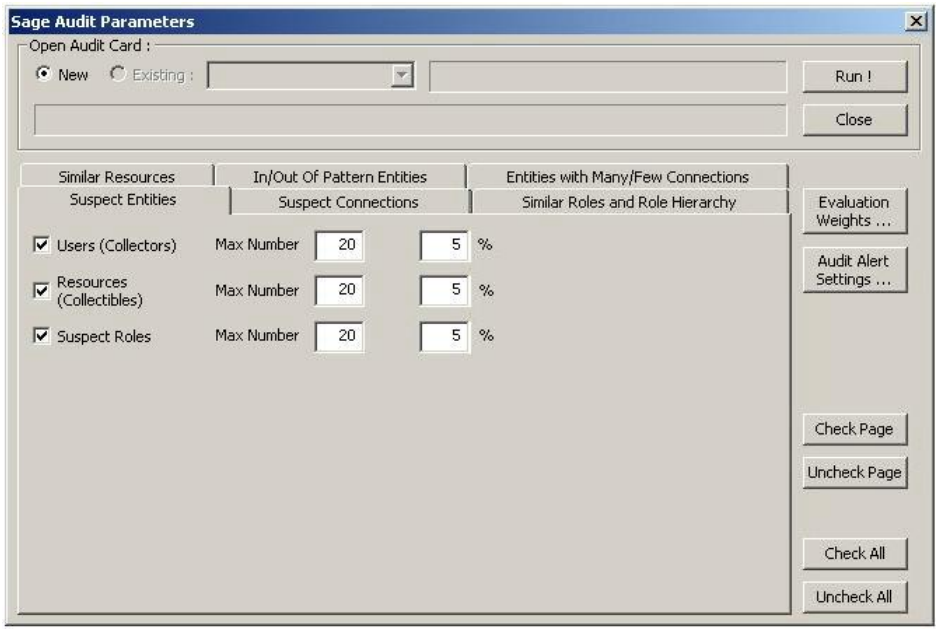
Parameters are selected in the Audit Parameters window using tabs, one tab for each category. Within each tab, you can set various parameters (refer to the following sections). After processing the selections listed in the Audit Parameters window, the Client Tools produce an AuditCard that lists an alert for each suspected entity. You can then review each alert to determine if it warrants attention. Each alert or suspected entity is listed as a separate record in the generated AuditCard.

In addition to providing a comprehensive list of suspected entities (see more below), handling of suspicious records can be tracked until they are properly addressed and comments can be added to each record of the AuditCard for reference.

Pattern-Based Audit

To open the Audit Parameters window, click Audit, Pattern-Based Audit.

The Audit Parameters window appears:



The following options are available from the main Audit Parameters window.

Option	Description
Run!	Runs the AuditCard generation module and produces an AuditCard based on the marked parameters.
Close	Closes the Audit Parameters window.
Evaluation Weights	Opens the Evaluation Weights window for setting the relative weight of the following parameters: organization, organization type country, location, title, and cost center. Other fields in this window are currently reserved for system use only.
Audit Alert Settings	Opens the Audit Card Alert Settings window to set the following parameters: Total number of alerts of the same category, Limit number of alerts of same category, Limit total number of alerts for same entity, and Limit number of alerts of same category and for same entity. In general, these numbers should be kept low in order to facilitate analysis of a suspicious record. Oftentimes, one alert can be responsible for many other alerts. Solving one alert can significantly reduce the number of generated alerts on subsequent runs.
Check Page	Marks all the check boxes in the current tab.

Option	Description
Uncheck Page	Clears all the check boxes in the current tab.
Check All	Marks all the check boxes in all the six tabs. This option produces the full range of suspicious records.
Uncheck all	Clears all the check boxes in all the six tabs. This option is used when the Role Engineer wants to start marking parameters without any default parameters already marked.
Open AuditCard radio button	New - opens a new Audit Card with the indicated parameters. Existing - opens an existing Audit Card, usually for continued work or follow up. A pull-down menu lists all existing Audit Cards. An existing Audit Card can be only opened if a configuration to which it is attached is already active. Otherwise, this option will be grayed out.

Suspect Entities

This tab is used to set the client tools to identify suspect entities. In the case of users these are users that have an extraordinarily different access to resources relative to their peers. In the case of resources or roles, these are resources or roles for which there is no clear pattern by which they are connected to users. To identify such exceptions to the rule you must enter a value for the conditions used to list the exceptions.

Using the minimum standard deviation (Min STD) condition on the tab you set a boundary that is used as the minimum threshold for identifying the exceptional cases. Any entity that lies above the threshold is considered as an exception.

Using the Max % condition you set a boundary that is used to set an upper threshold that lists to upper X% of all exceptions identified.

You can use each condition exclusively or in combination. In any case the client tools list the alerts in the audit card according to the condition that provides the fewest alerts.

The fields are described in the following table:

Option	Description
Users (Collectors)	Mark users to include users in the output. Unmark users not to include users in the output. Min STD - Limits the maximum number of users displayed to no more than the indicated absolute number thereby preventing the display of an unmanageable number of suspects. Max % - The maximum percentage of users to display out of all those who meet the criteria.

Option	Description
Resources (Collectibles)	Mark resources to include users in the output. Unmark resources not to include users in the output. Min STD - Limits the maximum number of resources displayed to no more than the indicated absolute number thereby preventing the display of an unmanageable number of suspects. Max % - The maximum percentage of resources to display out of all those who meet the criteria.
Suspect Roles	Mark roles to include users in the output. Unmark roles not to include users in the output. Min STD - Limits the maximum number of roles displayed to no more than the indicated absolute number thereby preventing the display of an unmanageable number of suspects. Max % - The maximum percentage of suspect roles to display out of all those who meet the criteria.

Suspect Connections

This tab enables you to identify suspect connections. These are connections between entities that are most suspect of being exceptions, compared to all other connections.

Note that dual (redundant) links includes instances in which the user and resource are connected both directly and indirectly through a role.

The fields are described in the following table:

Option	Description
User-Resource Connections by HR	User-Resource connections based on Human Resource attributes. Mark to include user-resource connections in the output. Unmark not to include user-resource connections in the output. Min mismatch - Set the minimum mismatch threshold to trigger an alert. Direct-Only Connections - Mark to only include connections for which the User-Resource relationship is described by a direct connection.
User-Resource Connections by Privileges	User-Resource connections based on access privilege attributes. Mark to include user-resource connections in the output. Unmark not to include user-resource connections in the output. Min mismatch - Set the minimum mismatch threshold to trigger an alert. Direct-Only Connections - Mark to only include connections for which the User-Resource relationship is described by a direct connection.

Option	Description
User-Role Connections by HR	User-Role connections based on Human Resource attributes. Mark to include user-role connections in the output. Unmark not to include user- role connections in the output. Min mismatch - Set the minimum mismatch threshold to trigger an alert.
User-Role Connections by Privileges	User-Role connections based on access privilege attributes. Mark to include user-role connections in the output. Unmark not to include user- role connections in the output. Min mismatch - Set the minimum mismatch threshold to trigger an alert.
Role-Resource Connections	Mark to include role-resource connections in the output. Unmark not to include role-resource connections in the output. Min mismatch - Set the minimum mismatch threshold to trigger an alert.
User-Resource Dual Links	Mark to include user-resource dual links in the output. Unmark not to include user-resource dual links in the output.
User-Role Dual Links	Mark to include user-resource dual links in the output. Unmark not to include user-resource dual links in the output.
Role-Resource Dual Links	Mark to include role-resource dual links in the output. Unmark not to include role resource dual links in the output.
Role- Role Dual Links	Mark to include role-role dual links in the output. Unmark not to include role-role dual links in the output.

Similar Roles and Role Hierarchy

This tab identifies related roles/resources and hierarchy opportunities. In this tab, the intention is to identify role definitions that are related (very close to one another indicating that perhaps they should be unified), as well as opportunities for role hierarchies (simplifying the definition of a role if it is a superset of another role). Similarly, resources can be identified that contain a high degree of overlap.

The fields are described in the following table:

Option	Description
Roles Covering Same Users	% of Each Role Users Covered by Other Role. Insert a percentage. Mark to include roles covering same users in the output. Unmark not to include roles covering same users in the output.

Option	Description
Roles Covering Same Resources	% of Each Role Resources Covered by Other Role. Insert a percentage. Mark to include roles covering same resource in the output. Unmark not to include roles covering same resource in the output.
Role with	% of Users Covered by Another Role. Insert a percentage. Mark to include in the output. Unmark not to include in the output.
Role with	% of Resources Covered by Another Role. Insert a percentage. Mark to include in the output. Unmark not to include in the output.
Roles Potentially Subsumed	% of Users and All Resources Covered. Insert a percentage. Mark to include in the output. Unmark not to include in the output.
Roles Potentially Subsumed	% of Resources and All Users Covered. Insert a percentage. Mark to include in the output. Unmark not to include in the output.
Roles with At Least	% of Users and % of Resource overlap. Insert a percentage for Users and for Resource overlap. Mark to include in the output. Unmark not to include in the output.
Roles Hierarchy Opportunities	Mark to include roles hierarchy opportunities in the output. Unmark not to include roles hierarchy opportunities in the output.

Similar Resources

This tab identifies almost matching users and resources and then identifies users/resources that almost match a role according to the threshold percentage. For each user, this option also identifies other roles that are populated by users with similar attributes.

The fields are described in the following table:

Option	Description
Resources with >=	% of Common Users. Insert a percentage. Mark to include in the output. Unmark not to include in the output.

Option	Description
Resources Hierarchy Opportunities	% of Common Users. Insert a percentage. Mark to include in the output. Unmark not to include in the output.

In/Out of Pattern Entities

This tab checks whether entities are within or outside the designated pattern, depending on which check boxes are marked.

The fields are described in the following table:

Option	Description
Users Matching	% of a Role's Resources. Insert threshold. Mark to include users matching in the output. Unmark not to include users matching in the output.
Resources Matching	% of Role's Users. Insert threshold. Mark to include resources matching in the output. Unmark not to include resources matching in the output.
Propose New Roles for Users	Mismatch level. Insert threshold. Mark to propose new roles for users in the output. Unmark not to propose new roles for users in the output.
Propose New Resources for Users	Mismatch level. Insert threshold. Mark to propose new resources for users in the output. Unmark not to propose new resources for users in the output.
Identify Users Matching Rule Based Roles	Mark to propose new resources for users in the output. Unmark not to propose new resources for users in the output.
Identify Users Not Matching Rule Based Roles	Mark to propose new resources for users in the output. Unmark not to propose new resources for users in the output.

Entities with Many/Few Connections

This tab identifies users and resources with very few or very many connections, depending on which check boxes are marked.

The fields are described in the following table:

Option	Description
Users with	>= Direct Resources, Total Resources, Roles. Insert threshold. <= Direct Resources, Total Resources, Roles. Insert threshold. Mark to include in the output. Unmark not to include in the output.
Resources with	>= Direct Users, Total Users, Roles. Insert threshold. <= Direct Users, Total Users, Roles. Insert threshold. Mark to include in the output. Unmark not to include in the output.
Roles with	>= Direct Resources, Total Resources, Sub-roles. Insert threshold. >= Direct Users, Total Users, Parent Roles. Insert threshold. <= Direct Resources, Total Resources, Sub-roles. Insert threshold. <= Direct Users, Total Users, Parent Roles. Insert threshold. Mark to include in the output. Unmark not to include in the output.

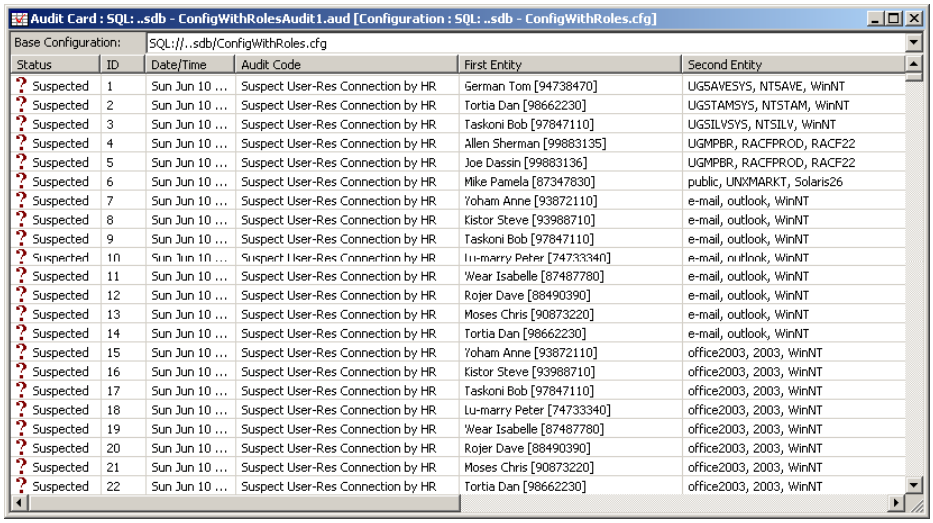
Generating an AuditCard

After parameters have been filled in, click Run! in the Audit Parameters window. A progress bar will be displayed during the generation process. If many parameters were selected, then generating the AuditCard may take a long time. In this circumstance, consider whether to perform the run during off-peak hours. For large and complex configurations, consider running the AuditCard option in separate parts. The run can be stopped at any time without losing work. The accumulated records will be displayed in a new AuditCard.

Each record in the audit card reflects a separate alert and all records contain a date/time stamp and their tracking status (new records are marked as suspected). An existing AuditCard can be re-run to check the status of alerts that have already been addressed. The AuditCard's description field can be used to annotate alerts with clarifications or explanations for reference purposes at a later date (for example, if the record needs to be re-checked in the future or if it was found to be OK even though it continues to be generated).

AuditCards are saved as special documents (.aud files) and enable subsequent tracking of alert status. It is also possible to add new alerts to existing alerts by activating the Open AuditCard radio button and performing a new run (Run!). The following window shows a typical AuditCard generated from an existing configuration.

Comments can be added in the Description field.



The fields are described in the following table:

Name	Description
Base Configuration	Displays the Configuration file path and name on which the AuditCard is built.

Name	Description
Status	The AuditCard provides a list of “suspected” violations of internal logic as applied to the specific configuration.
ID	An incremented number showing the number of suspected records within the “suspected” list generated in the AuditCard.
Date/Time	Date and time that record was generated.
Audit Code	Lists a text description of the type of the suspicion detected.
First Entity	First entity involved in the alert.
Second Entity	Second entity involved in the alert.
Third Entity	Third entity involved in the alert.
Score	Not relevant for AuditCard.
Description	Comments can be inserted by the Role Engineer.

More information:

Pattern-Based Audit (see page 135)

Audit Codes

Audit codes explain the reason that the system has designated the record as suspicious. The following are the audit codes that currently exist in CA Identity Governance:

Audit Code Text	Audit Code No.	Audit Code Text	Audit Code No.
"Suspect Role Definition"	101	"User with Few Direct Resources"	804
"Suspect Role Def (User)"	102	"User with Few Total Resources"	805
"Suspected Collector"	201	"User is Member of Few Roles"	806
"Suspected Collector (Res)"	202	"Resource with Many Direct Users"	807
"Suspected Collectible"	301	"Resource with Many Total Users"	809
"Suspected Collectible (User)"	302	"Resource Used by Many Roles"	810
"Suspect User-Res Connection"	401	"Resource with Few Direct Users"	811
"Suspect User-Role Connection"	402	"Role with Many Users"	814
"Suspect Role-Res Connection"	403	"Role with Many Total Users"	815
"Roles For Almost Same Resources"	501	"Role with Many Resources"	816

Audit Code Text	Audit Code No.	Audit Code Text	Audit Code No.
"Roles For Almost Same Users"	502	"Role with Many Total Resources"	817
"Role Resources Covered By Another"	503	"Role with Many Sub Roles"	818
"Role Users Covered By Another"	504	"Role with Many Parent Roles"	819
"Role Subsumed By Another (Same Resources)"	505	"Role with Few Users"	820
"Role Subsumed By Another (Same Users)"	506	"Role with Few Total Users"	821
"Hierarchy Opportunity (Parent Child)"	507	"Role with Few Resources"	822
"Overlapping Resources (Users)"	508	"Role with Few Total Resources"	823
"Resources Hierarchy Opportunity (Fuller Partial)"	509	"Role with Few Sub Roles"	824
"User Almost Matches a Role"	601	"Role with Few Parent Roles"	825
"Resource Almost Matches a Role"	602	"Dual User-Resource Link"	826
"User with Many Direct Resources"	801	"Dual Role-Resource Link"	827
"User with Many Total Resources"	802	"Dual Role-Role Link"	828
"User is Member of Many Roles"	803		

Set AuditCard Alert Options

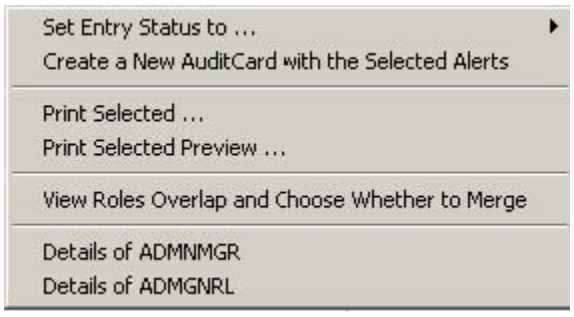
The primary audit alerts management options are accessed by highlighting one or more AuditCard records and activating the right-click control menu.

View Roles Overlap and Choose Whether to Merge

Activate entity window for more details about problematic entity.

Details of ADMNMGR

The CA Identity Governance suggestion for handling specific alert.



Set Entry Status To

This is the main tool for tracking progress of alert handling. Four options are available:

Status Name	Icon	Description
Suspected		Initial designation of a record as suspicious.
OK		The alert was examined and found to be in compliance.
Addressed		The problem detected has been handled by audit personnel and is no longer a problem.
In Progress		The problem is in the process of being handled by audit personnel.

Audit status appears in the far left-hand column of the AuditCard. If status has been changed by the Role Engineer , then the status name and icon in the left-hand column will also change.

Create a New AuditCard with the Selected Alerts

To use this option, highlight alerts in the AuditCard. Then, right-click on the highlighted records, and choose Create a New AuditCard with the Selected Alerts. A new AuditCard window will open containing the selected alerts only.

Alert Handling Suggestions

CA Identity Governance generally offers “intelligent” suggestions for handling an alert based on its analysis of each generated alert. The range of suggestions is very wide and corresponds to the type of alert. If the Role Engineer clicks on the suggestion, a relevant follow-up window often opens to continue handling the problem as suggested. In some cases, CA Identity Governance does not make any suggestions for handling the alert but does give direct access to the entity details window (refer to the following section).

The following are some examples of suggestions from an actual AuditCard:

Audit Code	Suggestion	Action
Suspected Collector	Review User Definition	Opens User window
Suspected Collectible	Review Resource Definition	Opens Resource window
Suspect Role Definition	Review Role Definition	Opens Role window

Audit Code	Suggestion	Action
Suspect Role-Res Connection	Remove privilege to “SYS1, RACFPROD, RACF22” from Role “ADMHR”	Privilege will be removed and alert will be marked as “Addressed”.
Suspect User-Role Connection	Remove privilege to “SYS1, RACFPROD, RACF22” from User “John Doe [ID NO. NNN]”	Privilege will be removed and alert will be marked as “Addressed”.
Suspect User-Resource Connection	Remove privilege to “BRLIMSYS, RACFPROD, RACF22” from user “John Doe [ID NO. NNN]”	Privilege will be removed and alert will be marked as “Addressed”.
Roles for Almost Same Users	View overlap and choose whether to merge	Merge Role Definitions window will open. If OK is pressed a merge occurs, and the alert is marked as “addressed”.
Roles Users Covered by Another	View overlap and choose whether to merge	Merge Role Definitions window will open. If OK is pressed a merge occurs, and the alert is marked as “addressed”.
Roles Resources Covered by Another	View overlap and choose whether to merge	Merge Role Definitions window will open. If OK is pressed a merge occurs, and the alert is marked as “addressed”.
User Almost Matches a Role	Add privilege to “FINAR” for User “John Smith [ID NO. NNN]”	Privilege will be added and alert will be marked as “Addressed”.
New Role Proposal	Add privilege to “FINAR” for User “Jim Jones [ID NO. NNN]”	Privilege will be added and alert will be marked as “Addressed”.
User with Few total Resources	Review User Definition	Opens User window.

Details

This option appears among the options listed for the AuditCard right-click menu. It is a sort of short cut that directly accesses the indicated entity window and is provided to facilitate examination of the relevant problematic entity.

More information:

Edit User (see page 75)
Edit Role (see page 76)
Edit Resource (see page 79)

Print Selected

Opens the Microsoft Windows Print window to print the selected alerts.

More information:

Print Reports (see page 120)

Print Selected Preview

This option shows a print preview of the selected alerts.

More information:

AuditCard Report (see page 123)

Chapter 9: Check Policy Compliance

Unlike the role-based auditing options, which involve the application of internal logic to a specific configuration, this chapter introduces CA Identity Governance's Compliance module. The Compliance module enables a system administrator, business manager, auditor, or any other actor to formulate a unique set of Business Process Rules (BPRs), which represent various constraints on privileges. These rules are formulated independently of a specific CA Identity Governance configuration and can then be applied to different configurations. Thus, the Compliance module augments CA Identity Governance auditing capabilities with a new and powerful compliance verification and documentation tool.

This section contains the following topics:

Manage Business Policy Rules

A Business Policy Rule (BPR) expresses business, provisioning, or security constraints as a logical condition that can be applied to the entities and links in a CA Identity Governance configuration. For example:

```
<Purchasing> forbidden to be <Subcontractor Payments>
```

You can apply this rule to a CA Identity Governance configuration to ensure that workers who have privileges to order stock from subcontractors do not have privileges to authorize payments to those subcontractors.

Typically a BPR is defined by specifying the following information:

- The type of rule—CA Identity Governance provides a broad range of rules that let you examine and compare various entity values. The rule type that is used in the previous example is Restrict access of users to roles by role access. This type of rule restricts the roles that a user can have based on other roles they already have.
- The logical condition—in our example, users with certain roles are forbidden from having other roles. You can also use this type of rule to allow or require users with certain roles to have other roles.
- Data sets and limit values—in our example, we specify a set of roles that are related to purchasing functions, and another set of roles that grant payment privileges.

A Business Policy is a set of BPRs. This policy (saved as a BPR file) exists independently of any specific configuration. The rules that comprise the policy can be adapted and applied to any CA Identity Governance configuration to verify its logic, integrity, and compliance with policy.

Rule Restrictions

Most rules describe a relationship between two groups of entities. You specify the members of these groups when you create a rule. These groups are identified as Left and Right in BPR editing screens. The following table lists the rule types and the restrictions available for each rule type.

Role – Role (by Users)

Only <L> May Have <R>

Only users that have roles on the left may have roles on the right side.

<L> Must Have <R>

Users that have roles on the left must have roles on the right.

<L> Forbidden to Have <R>

Users that have roles on the left must not have roles on the right.

<L> Only Allowed to Have <R>

Users that have roles on the left can only have roles on the right, and no others.

Role – Role (by Roles)

Only <L> May Have <R>

Only roles that have child roles on the left may have roles on the right as children

<L> Must Have <R>

Roles that have child roles on the left must have roles on the right as children.

<L> Forbidden to Have <R>

Roles that have child roles on the left must not have roles on the right as children.

<L> Only Allowed to Have <R>

Roles that have child roles on the left can only have roles on the right as children, and no others.

Role – Resource (by Users)

Only <L> May Have <R>

Only users that have roles on the left may access resources on the right.

<L> Must Have <R>

Users that have roles on the left must access resources on the right.

<L> Forbidden to Have <R>

Users that have roles on the left are must not access resources on the right.

<L> Only Allowed to Have <R>

Users that have roles on the left can only access resources on the right, and no others.

Role – Resource (by Roles)

Only <L> May Have <R>

Only roles that are parents of roles on the left may access resources on the right.

<L> Must Have <R>

Roles that are parents of roles on the left must access resources on the right.

<L> Forbidden to Have <R>

Roles that are parents of roles on the left must not access resources on the right.

<L> Only Allowed to Have <R>

Roles that are parents of roles on the left can access only resources on the right, and no others.

Resource – Resource (by Users)

Only <L> May Have <R>

Only users that can access resources on the left may access resources on the right.

<L> Must Have <R>

Users that can access resources on the left must access resources on the right.

<L> Forbidden to Have <R>

Users that can access resources on the left must not access resources on the right.

<L> Only Allowed to Have <R>

Users that can access resources on the left can access only resources on the right, and no others.

Resource – Resource (by Roles)

Only <L> May have <R>

Only roles that include resources on the left may include resources on the right.

<L> Must have <R>

Roles that include resources on the left must include resources on the right.

<L> Forbidden to have <R>

Roles that include resources on the left must not include resources on the right.

<L> Only allowed to have <R>

Roles that include resources on the left can include only resources on the right, and no others.

User Attribute - Role

Only <L> May have <R>

Only users with user attributes on the left may have roles on the right.

<L> Must have <R>

Users with user attributes on the left must have roles on the right.

<L> Forbidden to have <R>

Users with user attributes on the left are forbidden to have roles on the right.

<L> Only allowed to have <R>

Users with user attributes on the left can have only roles on the right, and no others.

User Attribute - Role Attribute

Only <L> May have <R>

Only users with attributes on the left may have roles with attributes on the right.

<L> Must have <R>

Users with attributes on the left must have roles with attributes on the right.

<L> Forbidden to have <R>

Users with attributes on the left are forbidden to have roles with attributes on the right.

<L> Only allowed to have <R>

Users with attributes on the left can have only roles with attributes on the right, and no others.

User Attribute - Resource

Only <L> May have <R>

Only users with user attributes on the left may access resources on the right.

<L> Must have <R>

Users with user attributes on the left must access resources on the right.

<L> Forbidden to have <R>

Users with user attributes on the left are forbidden to access resources on the right.

<L> Only allowed to have <R>

Users with attributes on the left can access only resources on the right, and no others.

Segregation of Duty Roles

Should have no more than <R> of <L>

Users should have no more than *number* (on right) of the roles on the left.

Should have at least <R> of <L>

Users should have at least *number* (on right) of the roles on the left.

Should have exactly <R> of <L>

Users must have exactly *number* (on right) of the roles on the left.

Segregation of Duty Resources

Should have no more than <R> of <L>

Users should have no more than *number* (on right) of the resources on the left.

Should have at least <R> of <L>

Users should have at least *number* (on right) of the resources on the left.

Should have exactly <R> of <L>

Users must have exactly *number* (on right) of the resources on the left.

User Counter of Roles

Should have no more than <R> Users

Roles on the left should have no more than *number* (on right) users.

Should have at least <R> Users

Roles on the left should have at least *number* (on right) users.

Should have exactly <R> Users

Roles on the left must have exactly *number* (on right) users.

User Counter of Resources

Should have no more than <R> Users

Resources on the left should have no more than *number* (on right) users.

Should have at least <R> Users

Resources on the left should have at least *number* (on right) users.

Should have exactly <R> Users

Resources on the left must have exactly *number* (on right) users.

User Attribute Value

Number <L> must be greater than <R>

The numeric value of the user attribute on the left must have a greater value than the numeric value on the right.

Number <L> must be less than <R>

The numeric value of the user attribute on the left must be less than the numeric value on the right.

Number <L> must be equal to <R>

The numeric value of the user attribute on the left must be equal to the numeric value on the right.

Date <L> must be earlier than <R>

The date for the user attribute on the left must be earlier than the date on the right.

Date <L> must be later than <R>

The date for the user attribute on the left must be later than the date listed on the right.

<L> Must match regular expression (see page 67) <R>

The value for the user attribute on the left must match the value defined by the regular expression on the right.

<L> Must not match regular expression (see page 67) <R>

The value for the user attribute on the left must not match the value defined by the regular expression on the right.

<L> Should be empty

The value for the user attribute on the left should be empty.

<L> Should not be empty

The value for the user attribute selected on the left should not be empty.

Create a Business Policy File with New Business Process Rules

Business Policy documents are constructed either manually by entering text directly into the Edit Business Policy Business Process Rule window one entry a time, or in a group wise manner by selecting a group of entities and dragging them onto the BPR window.

Entering Entities - Manual Method

You can add roles and resources for new or complex BPR rules by manually typing using the Edit window.

Follow these steps:

1. Open the Configuration and Business Policy documents.
2. Right-click in the BPR window, and select Add Business Process Rule (or click the Insert shortcut key).

   The Edit Business Policy Business Process Rule window opens.
3. Enter identifying text in the Rule ID field.
4. Select a Rule Type from the Rule Type drop-down list.
5. Select a Restriction for the rule from the Restriction drop-down list.
6. Enter values for the Left and Right entities in the Left and Right Entities edit boxes.

   This method is acceptable when editing or adding occasional records to an existing policy document. If you have selected a Default Configuration then you can select entities from the drop-down list.
7. Click Add to add the Entity values to their respective lists.
8. Click OK.

   The rule is added to the Business Policy Document.

Entering Entities - Group Method

When adding roles and resources for new or complex BPR rules, manual typing can be tedious and prone to errors. In this case, it is preferable to use the drag-and-drop copy method and add entities as a group. When adding the entities as a group you select them from a pre-existing configuration file and drag them to the respective left or right entities for a rule you have set up in a Business Policy document.

Follow these steps:

1. Open the Configuration and Business Policy documents.
2. Right-click in the Business Policy document and select Add Business Process Rule.

   The Edit Business Process Rule window opens.
3. In the Edit Business Process Rule window enter values for the Rule ID, Rule Type and Restriction.
4. Click OK, and the rule is added the Business Policy document. The rule is only partially complete as it is missing values for the Left and Right entities.
5. Select the Configuration file that is open on the desktop and that functions as the source of the rule entities.

   According to the rule created, select a group of values from the configuration that match the Left entity for the rule that was only created. Assuming the rule was of type Role-Resource select a group of roles from the Role Name column in the configuration file.
6. Drag-and-drop the group into the Left Entities field of the new rule in the Business Policy window. A name now appears in the Left Entities field for the rule.
7. Select a group of values from the column in the configuration file that matches the Right entity of the rule.
8. Drag-and-drop the group into the Right Entities field of the new rule in the Business Policy window.

   A name now appears in the Right Entities field for the rule.
9. Click the rule in the Business Policy window and the Edit Business Process Rule window opens. The values selected for the entities now appear in the Left and Right Entities list.
10. Edit the contents of the list by removing entries as required. Add more entries as required.
11. Save your changes.
12. Select a configuration file from the Default configuration drop-down.

As the entities are being dragged, the cursor pointer symbol changes from LINK (indicating the record is in memory) to ⊖ (indicating the record is being dragged) to ADD, before actually being “dropped” into the appropriate column.

Note: Roles and resources cannot be dropped on an empty record. The record must first be created before performing drag-and-drop of roles and resources.

Open an Existing Business Policy File (.bpr)

To open an Existing Business Policy File, click File, Open and select the existing business policy document and click Open.

Modify Existing Business Policy Rules

To edit an existing BPR rule, highlight the intended record and right-click the mouse.

Select an option from the menu.

Menu Option	Description
Add BPR	Right click on the first empty BPR line in the open policy document, and select Add BPR Entries, an empty Edit Business Process Rule window. Create the new rule and click OK. The new rule is added t the Policy document.
Delete BPR	Highlight a BPR record, and select Delete BPR Entries. A delete confirmation message will be generated. Press Yes to delete or No to cancel the delete operation.
Edit BPR	The Edit Business Process Rule window opens displaying the values for the selected rule. Make changes and save the edited rule.
Change BPR Type	

Running Business Policy Compliance Checks

To run a Compliance check

1. Open the relevant configuration file and choose Audit, Business Policy Compliance Check from the menu bar or use the Ctrl + B keyboard shortcut.

   The Business Policy Compliance Check window opens.

2. The following options can be implemented from this window:

BPR Files check box

Mark only the Business Policy file(s) that will be run in the BPR Files list.

Test BPR Consistency

Tests the BPR rules of the policy file for errors before performing the run. However, even if a policy file is run without first performing this check, verification will be performed during the run process (when the Test for Violations button is pressed), and any errors will be displayed for handling.

Add Policy

Enables adding a policy file not already on the list.

Remove Policy

Enables removing a policy file currently on the list.

Test for Violations

Runs the marked policy file(s) on the currently selected CA Identity Governance configuration. Verification is performed before the actual run, and any errors are displayed for handling.

Maximum number of alerts generated for each Rule

Limits the number of alerts generated per BPR rule. An “alert” is a record that is designated as “suspected” in the resulting AuditCard (Figure 146). Sometimes, an alert generates other alerts that are dependent on it. Putting a limit on the number of alerts restricts the number of total alerts generated and enables the Role Engineer to focus on basic alerts or suspected records.

Maximum number of alerts generated for each Entity

Limits the number of alerts generated for each entity.

Generate an AuditCard with the Compliance Module

Compliance BPR rules are written to find exceptions, which can then be examined by the relevant administrator or auditor to determine their validity in the context of the audited system. After determining and verifying Business Process rules in the selected Business policy files, click Test for Violations in the Business Policy Compliance Check window.

An AuditCard is generated.

The AuditCard provides a list of “suspected” violations of the policy-defined rules as applied to the specific configuration. The format of the Compliance AuditCard is similar to the format of the AuditCard generated by running pattern-based audit functions. However, there are differences.

Refer to the following table:

Name	Description
Status	The AuditCard provides a list of “suspected” violations of the Role Engineer -defined rules as applied to the specific configuration.
ID	An incremented number that shows the number of the suspected records within the “suspected” list generated in the Compliance AuditCard.
Date/Time	Date and time that the record was generated.
Audit Code	The Audit Code column lists the group and specific restriction of the record.
First Entity	The user detected by the Compliance module to whom the rule applies.
Second Entity	The left entity as recorded in the Compliance window.
Third Entity	The right entity as recorded in the Compliance window.
Score	Not relevant for Compliance AuditCard.
Description	Description of rule as recorded by the Role Engineer when rule was created.

More information:

Running Business Policy Compliance Checks (see page 157)

Chapter 10: Import and Export

The import process transfers user information into CA Identity Governance from the native systems on which it resides. The export process returns the information to the native systems after creating and modifying roles with CA Identity Governance.

Data Management provides a number of converters through which user information is processed. These import and export facilities represent the most common operating systems used on the native security systems.

The converters are located in the Import and Export menus.

This section contains the following topics:

Supported Import and Export Platforms

The Import and Export menus provide support for importing and exporting user and user privilege information to and from CA Identity Governance.

To access either the CA Identity Governance Import or Export converters

1. From the menu bar, select either Import or Export.

   The menu opens and lists the Import/Export converters.

2. Select the converter that you want to use.

   The selected converter opens.

The Import menu provides support for importing from the following file types and platforms:

- CSV files
- LDIF files

- Active Directory
- RACF
- TSS
- Unix
- SAP
- Windows Shared Folder
- ITIM V4.5 and V4.6
- Control SA

The Export menu provides support for exporting to the following file types and platforms:

- Active Directory
- RACF
- SQL Database
- CSV files
- ITIM V4.5 and V4.6
- Control SA

CSV Files Converter

Import from CSV Files

It is often convenient to convert information about users and privileges from native security systems into simple CSV files. The CSV (Comma Separated Values) format is the most common import and export format for spreadsheets and databases. CSV files can then be manipulated and extended using simple tools such as Excel, if necessary. CA Identity Governance has its own converter that takes several CSV files as input and creates a CA Identity Governance configuration.

Typically, the CA Identity Governance CSV converter uses several CSV files as input, with each individual file representing one entity type (such as users and resources databases) or one relation between two entity types (roles). Some of the files are optional and if not specified at the time of import will be assumed to be empty. The converter produces one output file, which is the CA Identity Governance configuration file.

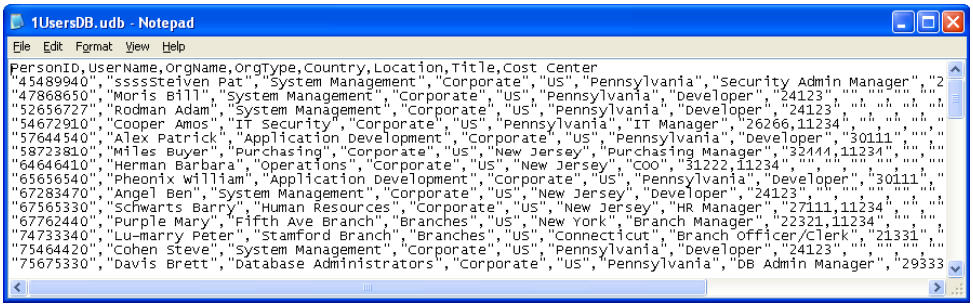
Note: The UsersDB and ResDB files are not created and are assumed to be provided in the same CSV format as used in a CA Identity Governance configuration.

Entity Files

Users database

The first row in the entity file must be a header row. Each subsequent row represents a single user, where the row contains the following fields:

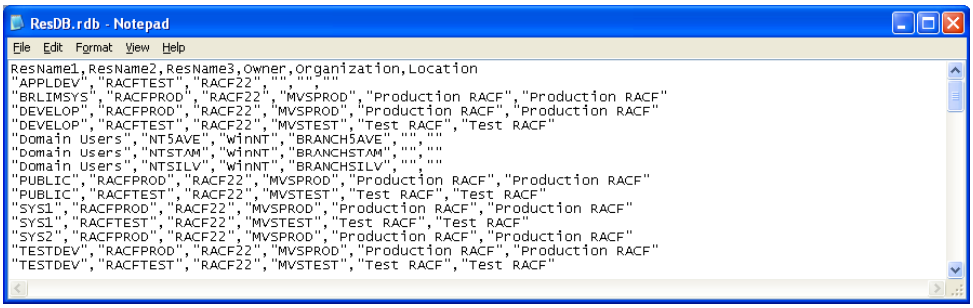
- PersonID—the key, and must be unique
- UserName
- Organization
- Organization Type
- Field 1 to Field n (optional)



Resources database

The first row in the entity file must be a header row. Each subsequent row represents a single resource and contains the following fields, where a combination of Resource Name 1, 2, and 3 is the key and is assumed to be unique:

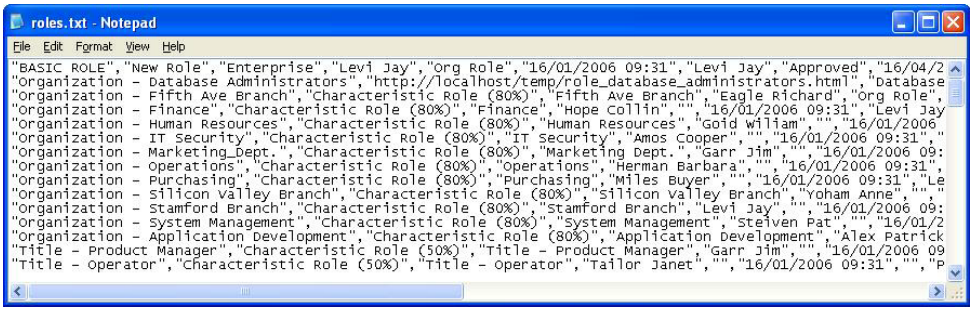
- Resource Name 1
- Resource Name 2
- Resource Name 3
- Field 1 to Field n (optional)



Roles

The Roles entity file does not require a header row. The file has one row per role definition, each with the following fields:

- Role Name - must be unique
- Description
- Organization
- Owner
- Type
- Creation Date
- Reviewer
- Approval Status
- Approval Date
- Rule
- Organization 2
- Organization 3
- Expiration Date



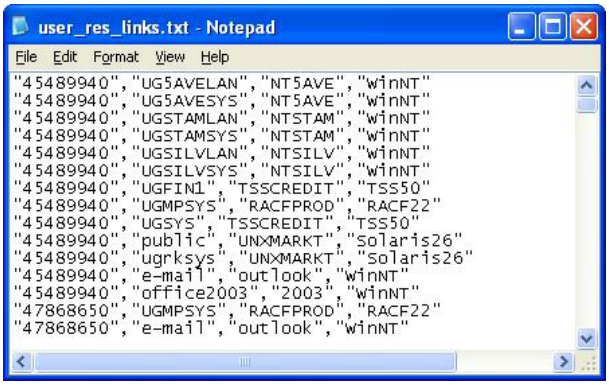
Relations Files

User-Resource Connections

The User-Resource Connections entity file does not require a header row. The file requires one row per connection, each with the following fields:

- PersonID
- Resource Name 1

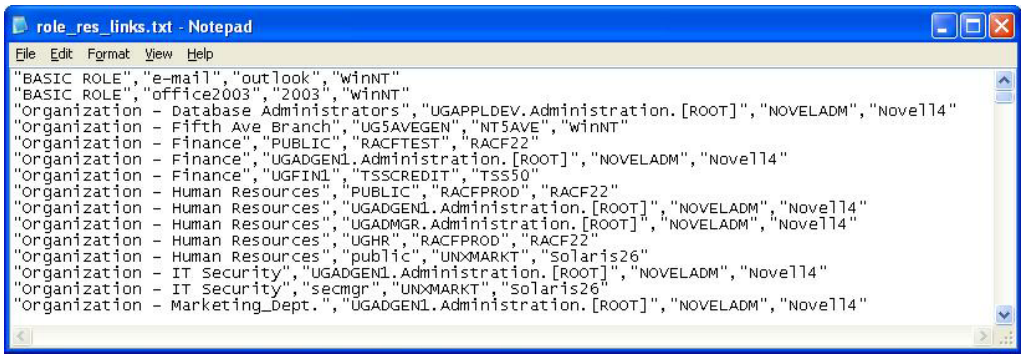
- Resource Name 2
- Resource Name 3



Role-Resource Connections

The Role-Resource Connections entity file does not require a header row. The file requires one row per connection, each with the following fields:

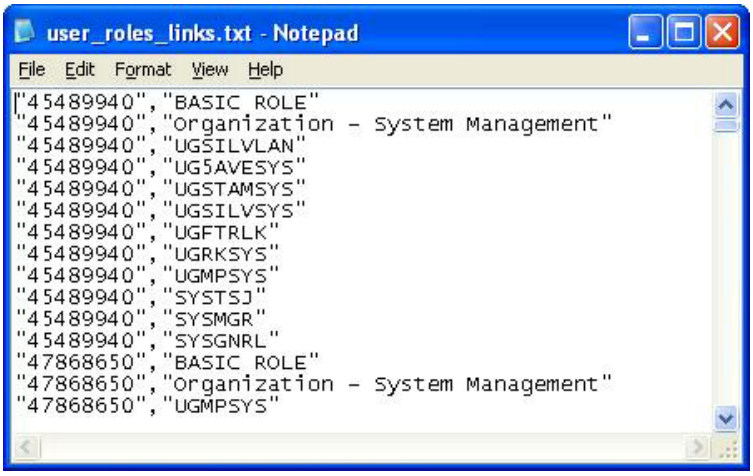
- RoleID
- Resource Name 1
- Resource Name 2
- Resource Name 3



User-Role Connections

The User-Role Connections entity file does not require a header row. The file requires one row per connection, each with the following fields:

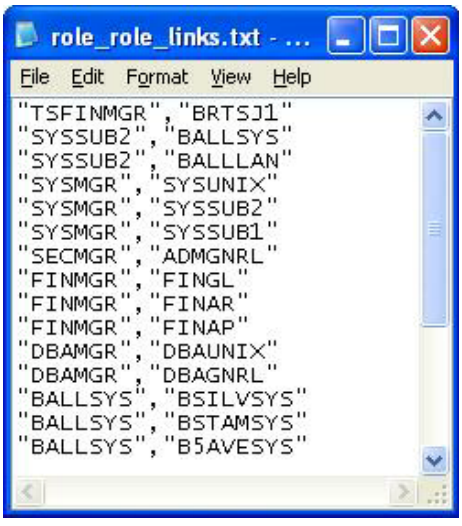
- PersonID
- Role Name



Role-Role Connections

The Role-Role Connections entity file does not require a header row. The file requires one row per connection, each with the following fields:

- Role Name (parent)
- Role Name (child)



Import a CSV File

To import a CA Identity Governance Configuration from a CSV file

1. Click Import, Import from CSV file from the main menu.

   The Importing to CA Identity Governance Configuration from CSV Files dialog appears.

2. Specify the pathname of the configuration file that receives imported data.

3. Specify the pathnames of the CSV files containing entity and link information.

4. Specify the character used to separate values in the CSV file set.

   Note: Some of the inputs may remain empty. For example, if you import from a system that does not yet have roles, then you leave the roles file and all the role connections files fields clear. The output is a CA Identity Governance configuration file that can then be opened to perform role discovery and audit activities.

   During the import process, CA Identity Governance creates a log file in the CA Identity Governance Logs folder. This log file is separate from the CA Identity Governance main log file, and is named according to CA Identity Governance's naming convention, which follows: eurekifyCSVConverter_<username>_<date>_<time>.log. This log file contains all the errors and misconfigurations that CA Identity Governance has encountered. CA Identity Governance will prompt you to view this log file when the import is finished.

   At the end of the conversion process, a message is displayed that indicates whether errors were detected.

   Important! In case of errors, review the log file to ensure that it does not contain material warnings. The configuration file does not automatically open.

5. To open the configuration file from the File menu select Open from File, and navigate to the target folder to open it.

Prevent Role-Role Cyclical Dependencies in CSV File Import

Symptom:

I tried to run an import in the portal using CSV files with cyclical links. After the import completes, I cannot open the Model or Master configurations.

Solution:

When importing data into CA Identity Governance using CSV file format, CA Identity Governance can detect and prevent role-role cyclic dependencies.

Set the following properties:

- import.csv.shouldCheckRoleRoleCyclicLinks=true
- import.csv.shouldCheckRoleRoleCyclicLinks.shouldFailOnRoleCyclic=true

Note: The second property is relevant only if the first property is set to true.

CSV File Import Generation

Symptom:

When I import data in a CSV file from Microsoft Excel, the file is corrupted after porting to CA Identity Governance. Upon looking at the resultant CSV file, it is seen that the backslash ("\") character is removed under certain circumstances.

Solution:

When importing CSV files into CA Identity Governance, use the following property setting:

import.csv.reader.escape

Description: Changes the escape character to a specific character not included in the CSV font set when the backslash character ("\") is included.

Export to CSV Files

CA Identity Governance can convert a configuration file to CSV files for uploading to an external security system.

To export a configuration to CSV files

1. Click Export, Export to CSV Files.

   The Exporting from CA Identity Governance Configuration to CSV Files window opens.

2. Specify the pathname of the source configuration file.
3. Specify the pathnames of the exported data files.

   The following field is not self-explanatory:

   Role ID as Number

   This option is available for compatibility with previous versions of CA Identity Governance where a role was identified by a Role ID (number). Otherwise, it should be unchecked.

4. Click Export.

   During the export process, CA Identity Governance creates a log file in the CA Identity Governance Logs folder. This log file is separate from the CA Identity Governance main log file, and is named according to CA Identity Governance's naming convention eurekfiyCSVConverter_<username>_<date>_<time>.log. This log file contains all the errors and mis-configurations that CA Identity Governance has encountered. CA Identity Governance prompts you to view this log file when the export is finished.

   At the end of the conversion process, a message is displayed that indicates whether errors were detected.

   Important! Review the log file to ensure that it does not contain material warnings.

CSV Mapper Utility

The CSV Mapper Utility allows you to extract user and resource data from any CSV file and map that data to create CA Identity Governance Configuration files, and User and Resource databases. The utility does not identify any role relationship that may exist between the Users and Resources in CSV file.

To map a CSV file to CA Identity Governance entities

1. Click Import, CSV Mapper Utility.

   The CSV Mapper window opens.

2. In the Files section, specify the pathnames of source and target data files, and specify the character used to separate data values in the source CSV file.
3. In the Source CSV to DNA Mapping section, specify the columns in the source CSV file that correspond to mandatory user and resource fields.
4. Click Convert.

   The CSV Mapper Utility creates each of the CFG, UDB, RDB files and locates them as indicated in the CSV Mapper Utility.

Generic LDIF to CA Identity Governance Converter

This converter is provided by CA Identity Governance, and retrieves data from a given LDIF file. The converter allows mapping different attributes of LDIF objects to CA Identity Governance fields. Once a map was designed it can be easily rerun on the same file or on other LDIF files to produce CA Identity Governance configurations.

To start an LDIF conversion

1. Click File, Import From External Sources, Import from LDIF File.

   The Import LDIF dialog appears.

2. Specify the LDIF file to convert and the target CA Identity Governance configuration files to be created.

   If you have an LDIF-CA Identity Governance map xml file you may specify it and continue with Step 6.

3. Click Edit Mapping.

   The SET LDIF Mapping dialog appears.

4. The mapping allows 3 views of LDIF objects.

   Map an LDIF object to a CA Identity Governance entity

   The object may either be a user, a role or a resource. In order to perform the mapping, choose both object and entity and click “Add”. After choosing a CA Identity Governance entity for a specific object an attribute mapping is required. Select attributes for the relevant CA Identity Governance fields and click “Set” to add them to the mapping list. You may also map CA Identity Governance fields to an OU of the object or to a constant text.

   Link CA Identity Governance entities based on LDIF object attributes

   When an LDIF object has an attribute pointing to another object this link may be reflected in the CA Identity Governance configuration. Select the source and destination objects and choose the attributes of the objects that should match. Click “Add / Set” to add the selected mapping to the list.

   Link CA Identity Governance entities based on attributes of an LDIF object

   When an LDIF object represents a link between two other objects this link may be reflected in the CA Identity Governance configuration. Choose the object representing the link and select the source and destination attributes from the object attributes. For both source and destination attributes select which field of which entity they should match. Click “Add / Set” to add the selected mapping to the list.

   In any stage of the mapping click Show Example to view an example of the attributes of the selected object. This is designed to assist you when choosing attribute mappings.

5. After you finish mapping all relevant data click Save to save the mapping to an xml file and return to the conversion window. This mapping may be edited in the future.
6. When you are pleased with the mapping click Start to perform the actual data conversion and open the generated CA Identity Governance configuration.

Active Directory Converter

Active Directory (AD) is a Microsoft directory service for storing information about network-based entities, such as users, groups, applications, files, and printers. It is the central authority that manages the identities and brokers the relationships between these distributed resources, thereby enabling them to work together. It is a mechanism for managing the identities and relationships of the distributed resources that make up network environments. Since Active Directory is the central authority for network security, enabling the operating system to verify a user's identity and control access to network resources, it is the natural point from which to download users, groups and resources information into CA Identity Governance.

After performing role discovery, analysis, definition and audit in CA Identity Governance, you can export the new roles, and other changes that were made in the configuration, back into Active Directory.

Import from Active Directory

The product enables import from one or more AD servers. Importing from multiple servers is useful when there are frequent cross-links between them. Currently, the product can export to only a single AD server.

Follow these steps:

1. Click Import, Import from Active Directory.

   The Active Directory Wizard - Step 1 dialog appears.

2. In the Credentials section, specify the servers from which data is imported. For each AD server from which you want to import, provide the IP/Domain Name, and port and login credentials.

   The following option is available:

   Secure Authentication

   Specifies that the Windows login is used to access target servers.

   Note: Passwords are not saved in the registry, so when returning to an AD import page, most values are kept, but not the password. Reset passwords each time you run the connector.

3. In the Output Files section, browse to set the pathnames of the data files that receive imported data.
4. Specify the pathname of the mapping file–an XML file that describes the mapping of AD attributes to CA Identity Governance entities. This file is saved after the first time a new mapping is provided.
5. Click Next to continue.

   The Active Directory Wizard - Step 2 dialog appears.
6. Under Search Area, select the points in the directory from which information is imported (the bases), in this case the respective “DC”. You can import specific containers from each of the imported AD servers.
7. Specify what to import. The following options are not self-explanatory:

   Identify Roles By

   Specifies how Active Directory entities are mapped to CA Identity Governance roles. You can select more than one option. Valid values include:

   CA Identity Governance Roles

   Native CA Identity Governance roles are marked as such during a preceding export.

   Nested Groups

   Primitive groups (meaninig that they are not the parent of other groups), are imported as resources, and parent groups are imported as CA Identity Governance roles.

   Distribution Groups/Security Groups/Universal Groups/Global Groups/domain Local Groups/Local Groups

   Specified types of Active Directory groups are imported as roles.
8. Click Next to continue.

   The Active Directory Wizard - Step 3 dialog appears.
9. A mapping window for Users attributes appears. Similar windows for Roles and Resources appear in subsequent steps.

   In these windows, fields of each entity type (users, roles and resources) may be associated with their corresponding Active Directory attribute. The result of each mapping operation is displayed in the mapping window.

   To activate the mapping, select the line that is associated with the CA Identity Governance attribute in the mapping table on the right.

   When you map AD attributes to CA Identity Governance entities, take special care to import unique values into CA Identity Governance keys, including users' PersonID, roles' Role Name, and resources' combination of ResName1, 2, and 3.

To enable proper mapping of imported attributes back into AD in an export process, import the CN and DN. Use the Object Name attributes.

Note: CA Identity Governance imports up to 127 characters for each field, and logs alerts for objects that exceed such limitation.

The following fields are not self-explanatory:

Object Name

Chooses specific predesignated schema attributes ad/or combinations thereof.

CN and DN map to the respective schema attributes.

CNi maps to the i-th part of the object's DN, from right to left (meaniing that it is based on the hierarchy), and beginning from the first container after the DC values.

DNi maps to the i-th part of the object's DCs.

Constant Field

You can map a constant field into a CA Identity Governance field. For example, it is often preferred to map the string "Active Directory" to Res Name 3.

Empty Field

This field enables you to leave a CA Identity Governance field blank.

Configuration Entity Field Name

Specifies a name for a CA Identity Governance attribute field

10. After you have mapped the fields of all entities, the product prompts you to save the mapping into a reusable XML file.

    A similar window displays to enable you to map roles.

    When completed, the product starts the import, and displays the import process progress. The following are steps to the import process:

    - **Import of objects** – in this pass, the product imports all users, roles, and resources objects
    - **Import of links** – in this pass, the product imports all links between objects
    - **Verify links** – in this pass, the product complements the configuration with external objects that are linked to configuration objects. the product creates a "stub" for each external object.

    When the import process is completed, a message appears that provides statistics on the imported data.

11. Click OK.

    During the import process, the product creates a log file in the CA Identity Governance Logs folder. This log file is separate from the product main log file, and is named according to CA Identity Governance's naming convention eurekifyADConverter_<username>_<date>_<time>.log. This log file contains all the errors and mis-configurations that the product has encountered. The product prompts you to view this log file when the import is finished.

    Important! Review the log file to ensure that it does not contain material warnings.

Export Active Directory

The process for exporting your modified CA Identity Governance configuration data to your Active Directory server is similar to the process for importing Active Directory information into CA Identity Governance. The process differs in the following ways:

- Only the differences between the imported configuration and the modified configuration are exported to the Active Directory server. Compare the two configurations and generate a Differences Report file. You use the Differences Log file as input for the Export process.
- You can export to only a single Active Directory server at a time.

To export data to an Active Directory server

1. Click Management, Compare Configurations.

   The Compare Configurations window opens.

2. Compare your original configuration file to your updated configuration file and generate a Differences Log file.

3. From the Export menu select Export to Active Directory.

   The Active Directory Wizard Step 1 dialog appears.

4. Fill in the Credentials as described for the Import from Active Directory process.

   Note: The export process only supports exporting to a single Active Directory server at a time.

5. In the Input Files group field, enter the path and file name of the Differences Log File containing the data to export to the Active Directory server.

6. Click Next.

   The Active Directory Wizard Step 2 dialog appears.

7. In the Options area, select the options that are relevant to your configuration, and click Next.

   The Active Directory Wizard Step 4 dialog appears.

8. On each of the Users, Roles and Resources tabs, map the CA Identity Governance Entities to the appropriate Active Directory Attributes.
9. On each of the Users, Roles, and Resources tabs select the location in the Active Directory to house new Users, Roles and Resources.
10. When appropriate, select the correct DN and CN values for the target Active Directory from the DN and CN drop-down lists.
11. Click Finish to export the modified data to the Active Directory server.

    Data is exported to an Active Directory server.

More information:

Import from Active Directory (see page 171)

RACF Converter

The Resource Access Control Facility (RACF) is a security component for IBM mainframe computers that works together with the existing operating system to provide system security, resource access control, auditability, accountability and administrative control. As such, it is the main repository for users, roles and resources data on mainframe computers.

The main input to the RACF import option requires downloading access data from RACF using the IRRDBU00 unload utility. This generated text file should then be segmented according to various line types, each representing a different type of entity and/or connections. You can add enriched data about users attributes (for example, from the human resources department database).

The output is a CA Identity Governance configuration, with RACF groups appearing as CA Identity Governance roles and with RACF profiles as CA Identity Governance resources.

Import from RACF

To import data from RACF into CA Identity Governance

1. Click Import, Import from RACF.

   The Importing from RACF Files window appears.
2. In the Resulting Configuration section, browse to set the pathnames of the data files that receive imported data.

3. In the Options section, specify import options. The following fields are not self-explanatory:

   Add ACL Entities

   Specifies if CA Identity Governance processes Application Control Language (ACL) scripts during import.

   Input HR file

   Specifies the pathname of the file containing supplementary user data, if any.

   Input RACF Download File

   Specifies the text file that is generated by running the IRRDBU00 Unload utility. The file contains lines that refer to the Users, Groups, Data Set Profiles and General Resource Profiles. These lines are converted into CA Identity Governance users, roles, and resources. All input types can be located in the same file name, or input can be divided into separate files depending on line types. This is done mainly for performance purposes.

4. Click Convert to import.

   The configuration is created in the target folder but is not automatically opened by CA Identity Governance.

5. To open the file, on the menu bar, select File, Open From File.

   If any errors result from the import process, a CA Identity Governance message appears. Check any errors in the eurekifyRACFConverterXXX.log file located in the CA Identity Governance Logs folder.

Export to RACF

Exporting involves the reverse process of importing.

To export data from CA Identity Governance into RACF

1. Click Export, Export to RACF.

   The Export to RACF window opens.

2. In the Files section, specify the pathnames of output files.

   Note: If a differences file is being used when exporting to RACF, then it will first have to be generated.

3. In the Options section, specify the entities and links to export.

   Note: Either the Add or Remove check box must selected for each entity or link type, but not both.

4. Click Convert to export.

   Note: In some cases the Export to RACF process only creates partial commands. This occurs primarily for commands that require the creation of new accounts. The output cannot be used as is and you must then complete the missing details in the exported file.

Import from TSS

CA Top Secret (TSS) is a security component for IBM mainframe computers that works together with the existing operating system to provide system security, resource access control, auditability, accountability and administrative control. As such, it is the main repository for users, roles and resources data on mainframe computers.

The main input to the CA Identity Governance TSS import option requires downloading access data from TSS using the by generating a TSS List File, and transferring the generated text file to a location on the Windows system to which CA Identity Governance has access. There is also a possibility to add enriched data about users attributes (for example, from the human resources department database).

The output is a CA Identity Governance configuration, with TSS profiles appearing as CA Identity Governance roles and with TSS groups appearing as CA Identity Governance resources.

To import data from TSS into CA Identity Governance

1. Create a TSS List File on the mainframe and transfer the file to a location that can be accessed by your Windows system.
2. Click Import, Import from TSS.
3. In the Files section, browse to set the pathnames of the data files that receive imported data.
4. In the Options section, specify import options. The following fields are not self-explanatory:

   Add ACL Entities

   Specifies if CA Identity Governance processes Application Control Language (ACL) scripts during import.

   Input HR file

   Specifies the pathname of the file containing supplementary user data, if any.

5. Click Convert to import.

   If any errors result from the import process, then a CA Identity Governance message appears.

6. Check any errors in the SageTSSConverterXXX.log file located in the CA Identity Governance Logs folder.

   The configuration is created in the target folder but is not automatically opened by CA Identity Governance.

Import from UNIX

The UNIX to CA Identity Governance converter accepts UNIX IDM files and converts them into CA Identity Governance formatted CSV files which can then be transformed into or incorporated in a CA Identity Governance configuration. The UNIX Group and Password files serve as input for the conversion process. You must transfer these source files to a location on your Windows system that can be accessed by CA Identity Governance.

To import data from UNIX into CA Identity Governance

1. Transfer the UNIX Group and Password files to a location on the Windows system.
2. Click Import, Import from UNIX.

   The Unix Converter window opens.

3. In the Source Unix Files section, enter the location of the UNIX password and group files.
4. In the Target Files section click Browse to select the target CA Identity Governance files to be generated. You must generate a Configuration file, Users file and Resources file.
5. To treat the UNIX groups as CA Identity Governance resources select the Groups as Resources check box.
6. Click Convert to initiate the conversion process and create the CA Identity Governance configuration files.

The configuration is created in the target folder but is not automatically opened by CA Identity Governance.

SAP to CA Identity Governance Converter

The SAP to CA Identity Governance converter extracts data that is housed in SAP tables and deposits the data in the various CA Identity Governance Databases according to the Mapping scheme that you select in the SAP to CA Identity Governance Converter.

Note: This data connector is not included with the standard Role & Compliance Manager package. Contact CA Technical Support to install this connector.

Mapping SAP Data to CA Identity Governance

The SAP tables and fields used by the *SAP to* CA Identity Governance converter are listed:

SAP Table	SAP Fields
USR02	mandt, bname
AGR_AGRS	mandt, agr_name, agr_child
AGR_USERS	mandt, agr_name, bname, to_dat, col_flag
AGR_1251	mandt, agr_name, object, auth, field, low, high, deleted
AGR_1252	mandt, agr_name, varbl, low, high

Note: Low values in the AGR_1251 table can be represented by variables. In such instances the variable references Low and High values that are contained in the AGR_1252 table.

We recommend that you do not trim the tables to remove fields that are not necessary, since additional fields may be needed in future versions.

The current converter supports several mapping schemes. These are:

- Map roles to resources
- Map field values to resources
- Map authorization objects as resources
- Map object as roles, field values as resources

Map Roles to Resources

The Map Roles to Resources mapping scheme takes SAP Roles and maps them to CA Identity Governance resources. The SAP role information is taken from the following SAP tables:

- USR02 - holds a list of system users
- AGR_AGRS - links composite roles to their child simple roles
- AGR_USERS - links users to roles (both composite and simple)

This table shows the relationship between CA Identity Governance Database entities and their respective source Table and Fields in a generic SAP database.

CA Identity Governance Entities and Links	SAP Table	SAP Fields
Users	USR02	bname
Resources	AGR_AGRS	agr_child
Roles	AGR_AGRS	agr_name
User-Role links	AGR_USERS	bname, agr_name
Role-Resource links	AGR_AGRS	agr_name, agr_child
User-Resource links	AGR_USERS	bname, agr_name (only simple roles)

Map Field Values to Resources

The Map Field Values to Resources mapping scheme takes SAP Objects and Fields and maps them to CA Identity Governance resources. The SAP role information is taken from the following SAP tables.

CA Identity Governance Entities and Links	SAP Table	SAP Fields
Users	USR02	bname
Resources	AGR_1251	object, field, low, high
Roles	AGR_AGRS	agr_name
User-Role links	AGR_USERS	bname, agr_name
Role-Resource links	AGR_1251	agr_name, object, field, low, high
Role-Role links (Hierarchy)	AGR_AGRS	agr_name, agr_child

Map Authorizaton Objects as Resources

The Map Authorization Objects as Resources mapping scheme takes SAP Authorization Objects and maps them to CA Identity Governance resources. The Mapping scheme only imports to fields that are selected in the FieldsForm window in the SAP to CA Identity Governance converter.

CA Identity Governance Entities and Links	SAP Table	SAP Fields
Users	USR02	bname
Resources	AGR_1251	auth, object, field, low, high
Roles	AGR_AGRS	agr_name
User-Role links	AGR_USERS	bname, agr_name
Role-Resource links	AGR_1251	agr_name, auth, object, field, low, high
Role-Role links (Hierarchy)	AGR_AGRS	agr_name, agr_child

AGR_1251 specifies role Authorization Objects with fields and values.

Map Object as Roles and Fields as Resources

The Map Object as Roles and Fields as Resources mapping scheme maps SAP Objects to CA Identity Governance Roles, and maps SAP fields as CA Identity Governance Resources.

CA Identity Governance Entities and Links	SAP Table	SAP Fields
Users	USR02	bname
Resources	AGR_1251	Combinations of field, low, high values
Roles	AGR_1251	object
User-Role links	AGR_USERS, AGR_1251	bname, object
Role-Resource links	AGR_1251	object, mixed field, low, high

AGR_1251 specifies role Authorization Objects with fields and values.

Running the SAP to CA Identity Governance Converter

Note: This data connector is not included with the standard Role & Compliance Manager package. Contact CA Technical Support to install this connector.

To load SAP privileges data into a CA Identity Governance configuration

1. Create a new database in your MS-SQL Server for the purpose of importing SAP authorization information into CA Identity Governance.
2. Import the SAP tables into the new database.

   The relevant tables are: USR02, AGR_AGRS, AGR_USERS, AGR_1251, AGR_1252 and their names must be identical to those written here.
3. Click Import, Import from SAP.

   The Importing from SAP dialog appears.
4. In the Server Name Text field Insert the name of the MS-SQL server you are using.
5. In the DataBase Name text field, insert the name of the database you are using for the SAP data.
6. Click Test Connection to verify that the connection details are valid.
7. In the MANDT Value text field, enter the MANDT identifier value for the SAP environment that you wish to convert. If you do not know the value contact your SAP administrator.
8. Choose the type of Mapping to use from the available mapping scheme options.
9. If you select Map authorization objects as resources click Choose Fields.

   The FieldsForm window opens.
10. Select which fields should be used to generate CA Identity Governance resources.
11. If you have separate tables in the database that contain the lists of simple and/or composite roles then enter their names in the respective Simple Role Table and Composite Role Table text fields. The table must only contain the role name as its data.
12. Select the respective check box if you have roles linked to either Users or Authorization Objects (AO) that do not appear in the role hierarchy.

    In these cases, the converter will not be able to tell whether they are simple or composite. You may choose how to treat them. The default is to treat them as simple roles.
13. In the Target Configuration field enter the Path and Filename to be used for the Target CA Identity Governance configuration file. Click Browse locate the Path.

14. In the Target Users DB field enter the Path and Filename to be used for the Target CA Identity Governance Users Database file. Click Browse to locate the Path.
15. In the Target Resource DB field enter the Path and Filename to be used for the Target CA Identity Governance Resource Database file. Click Browse to locate the Path.
16. Click “Convert” and wait for the completion message (it may take a while).

Import Windows Shared Folder

CA Identity Governance's customers are often interested in mapping privileges at a finer level of granularity than that provided by most IdM tools. That is below the level of groups and or profiles. This converter provides this granularity for Windows environments by scanning Windows servers for shared folders, and mapping access rights for those shares to the relevant domain groups and users.

The converter relies on CA Identity Governance's Active Directory (AD) converter to bring in AD groups, possibly from multiple AD servers and domains, and users. The converter uses agent-less Windows WMI technology to scan a range of Windows computers and import their shares as resources. It then links them to the above AD users and AD groups (imported as CA Identity Governance roles).

Mapping Windows Share Data to CA Identity Governance

The scanner connects with each of the machines defined by the user and queries it for shares. All the acquired shares are translated to CA Identity Governance resources, detailing computer name, share name, and access level. For each share, all permissions are obtained and are translated to CA Identity Governance user and role links with resources (the resources being shares). Different access levels of different users are reflected as separate resources.

To import data from Windows Shared Directories into CA Identity Governance

1. Click Import, Import from Active Directory.

   The Connect Active Directory window opens.
2. Set the Credentials and Output Files fields.
3. Click Next to advance to the next step in the wizard.
4. In the Search Active Directory Objects step, select the All Groups as Roles option from the Groups as Roles section.
5. Complete the Wizard and generate an Active Directory configuration. This will serve as CA Identity Governance Configuration input in the Windows to CA Identity Governance converter.

6. From the Import menu select Import Windows Shared Directory.

   The Windows to Sage Converter opens.

7. In the Original Sage AD Configuration section enter the Path and File name for the Active Directory configuration that you created.

8. From the Windows Share Scan section, click Scan Shares.

   The Scan Windows Shares window opens.

9. In the Credentials section enter domain administrator User Name and Password. You can enter the credentials for any other user that have permissions to use WMI on the target systems.

10. In the Machines to Scan section, enter the IP ranges to be scanned, by entering the IP address range and clicking Add. Alternatively you can add pattern based computer names by selecting the Computer Name by AD filter checkbox and entering a filter and an AD Server in the respective text boxes.

11. In the Target Share Files section, enter file names for the Shares Resource File and Shares Links File text boxes.

12. Click Scan to perform the scan.

    A progress bar appears, wait for it to reach finish.

13. Click Close and return to the Windows to CA Identity Governance Converter window.

14. In the Target Configuration section, enter the Path and File name for the Target Configuration file.

15. Click Merge and wait until the Done message appears.

    The new CA Identity Governance configuration is then ready for use.

More information:

Export Active Directory (see page 174)

TIM2CA Identity Governance Converter

This converter is provided by CA Identity Governance, and uses the TIM Java-based API to convert TIM privileges data into CA Identity Governance configurations. The converter maps TIM users, roles, accounts, provisioning policies, services, and groups, into CA Identity Governance. It allows mapping different TIM fields to CA Identity Governance fields. Once the initial mapping setup is complete, re-running this interface requires only a few clicks.

Note: This data connector is not included with the standard Role & Compliance Manager package. Contact CA Technical Support to install this connector.

Prerequisites

This converter supports the following:

- IBM TIM versions 4.5 and 4.6
- WebSphere application server version 5.1 and Java version 1.4.2
- Run on Windows OS

Importing from ITIM

Note: This data connector is not included with the standard Role & Compliance Manager package. Contact CA Technical Support to install this connector.

Importing from ITIM to CA Identity Governance requires the following steps:

1. Provide information about the TIM and WebSphere environments (kept in TIM configuration format)
2. Map TIM fields to CA Identity Governance fields (kept in XML configuration format)
3. Convert to CA Identity Governance's standard CSV format and then to a CA Identity Governance configuration

The process for importing from ITIM V4.5 and ITIM V4.6 is identical. However you must use the import option that is suitable for each version. The following description uses ITIM V4.5. You may also use ready connection and mapping xml files, and run a conversion by clicking the “Convert” button.

To import from ITIM V4.5

1. Click Import, Import from ITIM V4.5.

   The ITIM to CA Identity Governance Converter window opens.
2. In the Connection group box, click “Edit” to set the ITIM connection details.
3. Provide TIM credentials.
4. Provide the application server home directory (for example “C:\IBM\WebSphere\AppServer”).
5. Provide the TIM home directory (for example “C:\IBM\itim”).
6. Provide the location of the file called “jaas_login_was.conf” which is located under “%itim home%\extensions\examples\apps\bin”.
7. Provide the location of the java executable files (the jar and batch files received with the converter).
8. Save these parameters in an XML file for reuse.
9. Click Done, then save changes to return to the converter window.

10. Click Test Connection to test the TIM connection.
11. Map fields.
    - In the Mapping group box click Edit to set the mapping details.
    - The Field Mapping window appears.
    - In the Properties file filed, specify the xml properties file.
    - Map TIM attributes to CA Identity Governance fields. Save these settings for reuse.
12. Provide the location of the CA Identity Governance executable file and a directory for temporary files.
13. Click Done to return the converter window, and then click Convert to create CA Identity Governance configuration.

Load Previously Stored ITIM Credentials

To load previously stored ITIM Credentials

1. Click Itim Connection file, Open.
2. Select the XML file that contains the previously stored ITIM credentials information:

   All Credentials information is reloaded.
3. Click Done, then Save to return to the converter window.

Exporting to ITIM

Note: This data connector is not included with the standard Role & Compliance Manager package. Contact CA Technical Support to install this connector.

The client tools support exporting to ITIM Versions 4.5 and 4.6. Input for the export process is similar to that described for Importing from ITIM. Exporting to V4.5 and V4.6 is identical other than choosing the appropriate item from the Export to ITIM menu item. This section uses ITIM V4.5 to illustrate the export process.

Exporting to ITIM requires the following:

- Provide information about the TIM and WebSphere environments (kept in TIM configuration format)
- Map TIM fields into CA Identity Governance fields (kept in XML configuration format)
- Create a CA Identity Governance Differences file by comparing configuration original to the modified configuration.

To export to ITIM V4.5

1. Compare the original configuration created from the import ITIM to CA Identity Governance process, to the modified configuration and created a Differences file. You will need the Differences file lists the differences in a form that can be accepted by ITIM.
2. Click Export, Export to ITIM V4.5.

   The CA Identity Governance to ITIM converter opens.

   A Connection Details File was created as part of the Import from ITIM process. In the ITIM Connection section of the window, enter the Path and Name of the Connection Details File if it exists.
3. If the Connection Details File is missing then click Edit.

   The ITIM to CA Identity Governance Converter window opens.
4. Enter the ITIM Login Details and Java Configuration details.

   In the Field Mapping section, enter the Path and Name of the Mapping Details file if it exists. If you do not have a current Mapping Details File, click Edit.

   The Attribute Mapping window opens.

   The Entities Mapping section contains several tabs; Person, Role, Service and Policy. On each tab map the CA Identity Governance User Fields to the appropriate TIM Person Attribute by selecting entries from the TIM Person Attribute and CA Identity Governance User Field drop down lists.
5. Click Add to add the selections to the list.
6. On the Policy tab, do the following:
   a. Set the Scope from the Scope drop down list
   b. Set the Priority level in the Priority edit field.
   c. Select the Policy Enabled check box to indicate that the Policy is enabled.
7. From the Actions to Perform section select the check box for each action you want to perform during the export process.
8. In the Addition Options section select the checkboxes for any of the options you want to perform. These include:
   - Force service removal from policies
   - Force removal of linked entities
   - Map app-roles to provisioning policies.
9. In the Map XML File section provide a name for the mapping file and save the file for future use.
10. Click Done.

    You return to the CA Identity Governance to ITIM converter.

11. In the Source CA Identity Governance Difference Log section enter the Path and Name of the Differences Log file created as a result of Compare Configurations process.
12. Click Convert.

    A command line window opens and provides information on the converters progress.

BMC Identity Manager Open Services

This converter maps ESS Persons, Profiles (job codes), Groups and Accounts, into CA Identity Governance Users, Roles, Resources and Links.

Note: This data connector is not included with the standard Role & Compliance Manager package. Contact CA Technical Support to install this connector.

Importing from BMC Identity Management

Note: This data connector is not included with the standard Role & Compliance Manager package. Contact CA Technical Support to install this connector.

To import from BMC Identity Management to CA Identity Governance

1. Click Import, Import from BMC Identity Manager(OpenServices).
2. Fill in the BMC Identity Management convert (Import) Window.
   - If the files: defaultConnection.xml, defaultMapping.xml exist in the CA Identity Governance home directory, Form values will automatically be loaded from the xml file.
   - XML files must be saved before the import process can be performed.
3. In the Input Details group provide the JBoss Input Detail connection parameters.
4. Click Test Connection to test the connection parameters.
5. Pre saved parameters can be loaded from an XML file. If file defaultConnection.xml exists in the CA Identity Governance home directory, connection values will automatically be loaded from the xml file.
6. In the Map Fields group enter the map xml file path and directory if it exists, in the Map XML File text field.

   Pre-saved parameters can be loaded from an XML file. If file defaultMapping.xml exists in the CA Identity Governance home directory, mapping values will automatically be loaded from the xml file.
7. If the file does not exist click Edit in the Map Fields group.

   The Field Mapping window opens.

8. Fill in the Field Mapping window as indicated.

   If the Input details were inserted correctly then the drop down list values is available.

9. Save your changes and click Done.

   The window closes and you return to the BMC Identity Manager window.

10. In the Output Files group enter the target address for the CA Identity Governance output configuration files. These include the configuration, Users Database and Resources Database (cfg, udb and rdb).

11. In the Executable group enter the directory and path to the client tool executable file.

12. Click Start Import to initiate the import process.

Exporting to BMC Identity Management

The client tools support exporting to BMC Identity Management.

Note: This data connector is not included with the standard Role & Compliance Manager package. Contact CA Technical Support to install this connector.

Exporting to BMC Identity Management requires the following:

- Generate a CA Identity Governance diff log file by comparing two CA Identity Governance configurations. This diff log should contain all the operations which will be reflected in ESS.
- Use the BMC Identity Manager convert (Export) application to perform the changes.

To export to BMC Identity Management

1. Compare the original configuration created from the import BMC Identity Management to CA Identity Governance process, to the modified configuration and create a Differences file.

2. Click Export, Export to BMC Identity Manager (OpenServices).

   The BMC Identity Management Convert (Export) window opens:

3. In the Input Details group enter the connection details. We recommend that you use the connection XML file that was used during the import process.

4. In the Map Fields group enter the mapping field details. If you use the Map XML File that was used for the import process the details will be extracted from the file and the relevant fields in the Map Fields window will be automatically populated. Otherwise click Edit button and enter the details manually.

5. In the Diff Log group enter the directory and path to the CA Identity Governance Diff log file that you created.
6. Click Start Export to start the export process.

   A Done message appears to report the completion of the convert process.

Chapter 11: Management Menu

Changes to users data occur in an ongoing manner on the HR system and to maintain the Users, Roles and Resources relationship you can enrich the CA Identity Governance User and Resource databases by incorporating the latest HR Users and Resource data.The HR data is used as input for CA Identity Governance pattern-based audits, role engineering, and compliance review certifications.

This section contains the following topics:

Enrich Users Database

The client tools expect to receive the supplementary HR data to be merged with the existing users database as a CSV formatted file. The first column of the Supplementary HR data file must contain the unique Person ID. This type of Person ID used in the HR file must match the type of Person ID used in the CA Identity Governance users.UDB file. For example if the value for the Person ID in the UDB file is taken from the Users Login Account then the HR file should also take the Person ID from the Users Login Account.

- For every Person ID in the CA Identity Governance UDB file that has a matching Person ID in the HR file, CA Identity Governance replaces the record in the UDB file with the record taken from the HR file.
- The resulting Output Users Database contains the same number of records, arranged in the same order, as that for the original CA Identity Governance UDB file.

To enrich a users database

1. Click Management, Enrich Users DB.

   The HR Data Merge Converter window opens.

2. In the Users Database text field, enter the path and name of the CA Identity Governance Users database that is to receive the supplementary HR data.

3. In the Supplementary HR File text field, enter the path and name of the file containing the supplementary HR data.

4. In the Output Users Database text field , enter the path and name of the resulting database file that contains the merged output.
5. From the Options group box, select any of the options that are relevant.

   The following options are not self-explanatory:

   Clear Fields that are empty in the HR file

   Select this option to omit imported data for a field if the corresopnding entry in the enrichment file is blank. Clear the option to disregard empty fields in the HR file and keep the existing content in the UDB.

   Clear Fields of the UDB users that were not found in the HR file

   Select this option to omit user data if no corresponding user record is found in the enrichment file. Clear the option keep user information in the UDB even if the User does not exist in the HR file
6. Click Enrich.

   A new CA Identity Governance users database is generated and saved in the specified location.

Enrich Resource Database

For each set of resources, R1, R2, R3 in the CA Identity Governance RDB file that has a matching set of resources in the supplementary resource database file, CA Identity Governance replaces the record in the RDB file with the record taken from the supplementary resource database file.

To enrich a resource database

1. Click Management, Enrich Resource DB.

   The Resource Data Merge Converter window opens.
2. In the Resource Database text field, enter the path and name of the CA Identity Governance Users database that is to receive the supplementary HR data.
3. In the Supplementary Resource DB File text field, enter the path and name of the file containing the supplementary HR data.
4. In the Output Resource Database text field , enter the path and name of the resulting database file that contains the merged output.
5. Click Enrich.

   A new CA Identity Governance Resource database is generated and saved in the specified location.

Preserving Columns During Enrichment

During the enrichment process, the original records in both the CA Identity Governance Users databases and Resource databases are overwritten with the data from the Supplementary HR files. The order in which data is arranged in the CA Identity Governance databases is lost if the order of data arrangement in the supplementary HR files differs from those in CA Identity Governance database.

Important! CA Identity Governance Users and Resource database headers are location-based and must have the same number of characters to verify correct database structure.

If need be, you can preserve the arrangement and content of any column in the source file by modifying the supplementary HR file before performing the enrichment process. To prevent any column from being overwritten, you must place an empty column in the parallel position in the supplementary HR file.

The following illustration represents the arrangement and content of a CA Identity Governance Users Database:

	A	B	C
1	PersonID	UserName	Title
2	45489940	Steiven Pat	Security Admin Manage
3	47868650	Moris Bill	Developer
4	52656727	Rodman Adam	Developer

The following illustration represents the arrangement and content of the Supplementary HR File.

```
PersonID,UserName,OrgName,OrgType,Country,Location,
"45489940","Steiven Pat","System Management","Corpo
"47868650","Moris Bill","System Management","Corpor
"52656727","Rodman Adam","System Management","Corpo
"54672910","Cooper Amos","IT Security","Corporate",
```

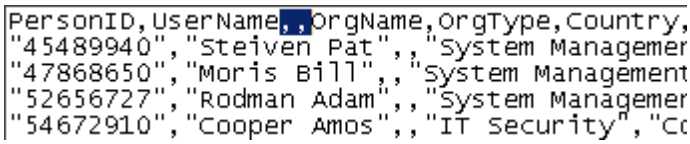
Notice the following:

- The column order in the CA Identity Governance User Database is Person ID, UserName, and Title.
- The column order in the supplementary file is Person ID, UserName, OrgName, OrgType, …

In this scenario when the two files are merged, the Title entry for each record in the CA Identity Governance User Database would be overwritten by the OrgName entry from each record in the Supplementary HR File. The Title column is the 3rd column in the CA Identity Governance Users Database.

To prevent the Title column from being overwritten, a empty column must be placed in the 3rd position in the Supplementary HR file. This is done by placing an additional comma as a place holder in each record of the supplementary file at the position you want to preserve in the CA Identity Governance Users Database.

The following illustrates how the Supplementary HR File in the above scenario is modified to prevent the entries in 3rd column of the CA Identity Governance Users Database from being overwritten.



In the figure two commas signifying and empty column now appear in each record between the original 2nd and 3rd columns, UserName and OrgName respectively.

Configuration Management Operations

Configuration management operations are used when you must combine configurations and their underlying databases. Such a need may occur when you want to combine configuration files that were created for different database systems or platforms. The various operations that you can perform include

- Evaluate Users Database
- Merge Configurations
- Merge Users Databases
- Merge Resource Databases
- Merge Audit Cards
- Trim Configuration

Evaluate Users Database

Evaluating Users Database provides a report detailing the number of values associated with each User Attribute and their distribution amongst all the users listed in the database.

To evaluate the users database

1. Click File, Configuration Management Operations, Evaluate Users DB.

   The Open file dialog box displays the Users Database files included in the project.

2. Select the Users Database from the list that you want to evaluate.
3. Click Open.

   A message box appears asking if you want to view the comments and statistics.

4. Click Yes to view the report. The report is displayed as a text file.

Merge Configurations

This option merges two configurations, including their underlying users and resources databases. The resulting configuration collects all users and resources that appear in either of the input configurations and integrates all privileges of the two configurations. This option is especially useful to merge configurations that result from importing data from different platforms.

Merging more than two configurations repeats the process for merging two configurations and is performed in several steps, each time adding one more configuration to the resulting configuration.

To merge configurations

1. Click File, Configuration Preparation Operations, Merge Configurations.

   The Configuration Data Merge Converter dialog appears.

2. Browse to select the configuration files you wan to merge, and to specify the pathname of the files that contain output of the merge operation.

   Note: merge overwrites the output configuration and database files you specify.

The following optional field is available:

Case-Sensitive Person ID

Select this option to apply case-sensitive matching of personID fields during merge. For example, when this option is selected, the user record JohnSmith in one input configuration will not be merged with the record johnsmith in the other input configuration.

When all files have been specified, the Merge button becomes active.

3. Click Merge to finish.

Merge Users Databases

This option is used to merge information contained in two Users Databases.

To merge two databases

1. Click File, Configuration and Management Operations, Merge Users Databases.

   The Merge Database window opens.

2. Fill out the fields in the window:

   First Users DB

   Fill in the name and path of the first Users Database to be merged. Click Browse to choose the file.

   Second Users DB

   Fill in the name and path of the second Users Database to be merged. Click Browse to choose the file.

   Output Users Database

   Enter the file name and path of the new users database to be created. Click Browse to choose the file.

3. Click Merge to produce the new Users Database.

Merge Resource Databases

This option is used to merge information contained in two Resource Databases.

To merge two resource databases

1. Click File, Configuration and Management Operations, Merge Resource Databases.

   The Merge Database window opens.

2. Fill out the fields in the window as follows:

   First Resource DB

   Fill in the name and path of the first Resource Database to be merged. Click Browse to choose the file.

   Second Resource DB

   Fill in the name and path of the second Resource Database to be merged. Click Browse to choose the file.

   Output Resource Database

   Enter the file name and path of the new Resource Database to be created.

3. Click Merge to produce the new Resource Database.

Merge Audit Cards

This option is used to merge information contained in two Audit Cards.

To merge audit cards:

1. Click File, Configuration and Management Operations, Merge Audit Cards.

   The Merge Audit Cards window opens.

2. Browse to select the files you wan to merge, and to specify the pathname of the output file of the merge operation.

   Note: merge overwrites the output file you specify.

3. The following fields of the dialog are not self-explanatory:

   Choose the First/Second Configuration for new Audit Card

   Specifies on which configuration file format to base the output audit card. Each audit card can be based on the attribute fields and other details of a different reference configuration. Specify which reference configuration is used in the merged audit card.

4. Click OK.

Trim Configuration

Use Trim Configuration when you have a configuration file that refers to a relatively small number of users than those that are contained in the associated Users Database and Resource Database. This situation may arise when a Partial Configuration is created from a much larger configuration. The Partial Configuration only contains a fraction of the Users of the original Configuration, but still refers to the entire Users Database and Resources Database. By trimming the configuration file you produce new Users Database and Resources Database files, which then only contains information that is linked to the Users listed in the Configuration file. The result is a smaller and more manageable configuration that uses fewer computing resources to load and manipulate.

To trim a configuration

1. Click File, Configuration and Management Operations, Trim Configuration.

   The Trim Configuration window opens.

2. Enter values for the fields as follows:

   Source Configuration

   Fill in the name and path of the Source Configuration to be trimmed. Click Browse to choose the file.

   Output Configuration

   Fill in the name and path of the Output Configuration to be created. Click Browse button to choose the file.

   Output Users Database

   Fill in the name and path of the Output Users Database to be created. Click Browse to choose the file.

   Output Resources Database

   Enter the file name and path of the Output Resources Database to be created. Click Browse to choose the file.

3. Click Trim.

Compare Configurations

A Role Engineer may examine the differences between two configurations to verify that the changes are correct before exporting.

The Compare Configurations option is a comparison that is made after discovery and audit processes are performed. The Master configuration from an endpoint is compared to the Model configuration, which is created while applying discovery and audit processes. In the final stage of the process, the Model configuration is exported to the endpoint, and the Master configuration is updated.

The Role Engineer has the option to display or not display the output, which is a Differences Report (DIFF file) or Updates Log.

Note: The Updates Log file and Differences Reports file, named DiffLog.txt and Diffreport.txt, can be opened at any time in a text editor for consultation or editing purposes.

Follow these steps:

1. In the Client Tools, click File, Compare Configurations.

   The Compare Configurations dialog appears.

2. Specify pathnames to input and output files.
3. Specify which differences to include in output files.
4. Specify report options as follows:

   View Report File

   Select this option to display a user-friendly report (Differences Report).

   View Updates Log

   Select this option to display the Updates Log.

5. Click Compare.

More information:

Evaluate Users Database (see page 195)
Merge Users Databases (see page 196)

Differences Report

The Differences Report is a user-friendly report that shows the differences that were recorded after Compare Configurations runs. It is based on and has the same content as the Updates Log. The Differences Report has a more readable format that the Updates Log.

Note: The **Role Engineer should verify the correctness of the differences before exporting the file to the external computer.**

Regardless of whether the Role Engineer chooses to display a Differences Report when Compare Configurations is run. The file that contains the Differences Report is saved to the path and file name as entered in the Compare Configurations window.

The Differences Report file is overwritten each time that Compare Configurations is run; that is, the file name is not automatically incremented. Therefore, if the Role Engineer is interested in preserving back copies of this file, it is recommended that the file name be manually changed each time Compare Configurations is performed.

The following is an extract from a differences report that shows the main components of the report.

Section	Sample Report Content
Title	Differences Report
Compared Configurations	
Original Configuration	F:\0DOCUMEN\CA RCM\Ver 2-7 of 1 Sept 2008\cfg3.cfg
Updated Configuration	F:\0DOCUMEN\CA RCM\Ver 2-7 of 1 Sept 2008\cfg4.cfg
Discovered differences in roles, users, and resources	
Role	(10,B5AVESYS,CtlSA) appears only in original configuration
User	(65656540, Kuli William, Application Development) appears only in the original configuration
Res	(UG5AVELAN,NT5AVE,WinNT) appears only in the original configuration

More information:

Merge Configurations (see page 195)

Updates Log

The Updates Log is a file generated in a format that can be exported to the production server in order to update its databases. It shows the differences that were recorded when the Compare Configurations process was run and has the same content and is generated at the same time as Differences Report. The Differences Report has a more readable format than the Updates Log.

Note: The **Role Engineer should verify the correctness of the differences before exporting the file to the external computer.**

Regardless of whether the Role Engineer chooses to display the Updates Log when Compare Configurations is run, a file that contains the Updates Log is generated. The file that contains the Updates Log is saved to the path and file name as entered in the Compare Configurations window.

Note: The Updates Log file is overwritten each time that Compare Configurations is run; that is, the file name is not automatically incremented. Therefore, if the Role Engineer is interested in preserving back copies of this file, it is recommended that the file name be manually changed each time Compare Configurations is performed.

The following is an extract from an Updates Log that shows the main components of the log.

```
DIFF,ORIGCFG,F:\0DOCUMEN\Eurekify\Ver 2-7 of 1 Sept 2004\cfg3.cfg
DIFF,UPDCFG,F:\0DOCUMEN\Eurekify\Ver 2-7 of 1 Sept 2004\cfg4.cfg
DIFF,REMOVEDROLE,"B5AVESYS"
DIFF,REMOVEDROLERES,"B5AVESYS","UG5AVESYS","NT5AVE","WinNT"
DIFF,COMMONROLEREMOVEDRES,"B5AVEJ1","UG5AVELAN","NT5AVE","WinNT"
DIFF,COMMONROLEREMOVEDRES,"B5AVELAN","UG5AVELAN","NT5AVE","WinNT"
DIFF,COMMONROLEREMOVEDROLE,"BALLSYS","B5AVESYS"
DIFF,REMOVEDUSER,"65656540"
DIFF,COMMONUSERREMOVEDRES,"45489940","UG5AVELAN","NT5AVE","WinNT"
DIFF,COMMONUSERREMOVEDRES,"67283470","UG5AVELAN","NT5AVE","WinNT"
DIFF,COMMONUSERREMOVEDRES,"76329130","UG5AVELAN","NT5AVE","WinNT"
DIFF,REMOVEDRES,"UG5AVELAN","NT5AVE","WinNT"
```

More information:

Evaluate Users Database (see page 195)

Analyzing Differences

The purpose of a differences file is to identify only the changes that were made to a given configuration. Each line in a differences file identifies one difference. The following table shows some examples of changes recorded in a differences file with an explanation of each change:

Change	Descriptions
1	Removing a role definition
	DIFF,REMOVEDROLE,"Branch Clerks"
2	Removing a user definition
	DIFF,REMOVEDUSER,"52656727"
3	Removing a resource definition
	DIFF,REMOVEDRES,"users","UNXMARKT","Solaris"
4	Removing a resource connection from an existing user
	DIFF,COMMONUSERREMOVEDRES,"88311130","users","UNXMARKT","Solaris"
5	Removing a user connection from an existing role
	DIFF,COMMONROLEREMOVEDUSER,"Branch Clerks","52656727"
6	Removing a role connection from an existing role
	DIFF,COMMONROLEREMOVEDROLE," Branch Clerks ","Clerks"
7	Removing a resource connection from an existing role
	DIFF,COMMONROLEREMOVEDRES," Branch Clerks ","users","UNXMARKT","Solaris"
8	Removing the sub-roles of a removed role
	DIFF,REMOVEDROLEROLE,"Branch Clerks","Clerks"
9	Removing the resources of a removed role
	DIFF,REMOVEDROLERES,"Clerks","administrators","RACFPROD","RACF"
10	Removing the users of a removed role
	DIFF,REMOVEDROLEUSER,"Clerks","45489940"
11	Removing a removed role from all user members
	DIFF,COMMONUSERREMOVEDROLE,"45489940","Clerks"
12	Adding a new user
	DIFF,NEWUSER,"45489940"
13	Adding a new resource connection to a new user

Change	Descriptions
	DIFF,NEWUSERNEWRES,"45489940","administrators","RACFPROD","RACF"
14	Adding a new role connection to a new user
	DIFF,NEWUSERNEWROLE,"45489940","Clerks"
15	Adding a new resource
	DIFF,NEWRES,"administrators","NT176","WinNT"
16	Adding a new role
	DIFF,NEWROLE,"San Francisco Clerks","General Needs of SF Clerks"
17	Adding a new role connection to an existing user
	DIFF,COMMONUSERNEWROLE,"45489940","San Francisco Clerks"
18	Adding a new resource connection to an existing user
	DIFF,COMMONUSERNEWRES,"45489940","administrators","NT176","WinNT"
19	Adding a user to a new role
	DIFF,NEWROLEUSER,"San Francisco Clerks","45489940"
20	Adding a role to an existing role
	DIFF,COMMONROLENEWROLE,"San Francisco Clerks","San Francisco Junior Clerks"
21	Adding a role to a new role
	DIFF,NEWROLEROLE,"San Francisco Clerks","San Francisco Junior Clerks"
22	Adding a new resource to a new user
	DIFF,NEWROLERES,"San Francisco Clerks","administrators","NT176","WinNT"

Compare Users Databases

The Compare User Databases option enables you to compare two different databases and identify their differences. The function can be used to compare various databases stored on the original production server, or to conduct a comparison between the original database and the database that contains the results of discovery and audit processes. The Role Engineer then examines the differences to verify that the changes are correct.

The Role Engineer has the option to display or not display the Compare User Databases output. This includes a Differences Report and a Differences Log. The feature can be used to produce a Differences Audit file also. Both the Differences Report and the Updates Log are displayed as text files in a Windows Notepad window. This enables you to edit and save the file on-the-spot.

To compare user databases

1. Click File, Compare User Database.

   The Compare User Databases dialog appears.

2. Specify pathnames to input and output files.
3. Specify which differences to include in output files.
4. Specify report options as follows:

   View Report File

   Select this option to display a user-friendly report (Differences Report).

   View Updates Log

   Select this option to display the Updates Log.

5. Click Compare.

   The Differences report, log and audit files are generated.

Users Database Differences Report and Log Files

The Users database report and log files list the results found after comparing the content of the Original Users Database and the Updated Users Database. The files are formatted in the same way as the report and log files that are generated when comparing two configuration databases.

The Report is presented in a user-readable format, whereas the Log is presented in a form that can be uploaded to the production machine. The following samples are extracts of both file types after comparing the same two User databases: the first sample shows the User Database Report, the second sample shows the User Database Log.

The following is a sample Users Database Differences Report:

```
Differences Report
Original User Database: C:\Documents and Settings\User\Desktop\Compare\UsersD.udb
Updated User Database: C:\Documents and Settings\User\Desktop\Compare\UsersDNew.udb
User: (97774230, More Cathrine) Different Field (Field=USERNAME, Previous=More
Cathrine, Updated=Wing Caryn)
User: (97774230, More Cathrine) Different Field (Field=ORGNAME, Previous=Finance,
Updated=Purchasing)
User: (99883134,Ron Mark,Human Resources) appears only in the original configuration
User: (99883434,Garcia Sandy,Human Resources) is new
```

The following is a sample Users Database Differences Log:

```
DIFF,ORIGUDB,C:\Documents and Settings\User\Desktop\Compare\UsersD.udb
DIFF,UPDUDB,C:\Documents and Settings\User\Desktop\Compare\UsersDNew.udb
DIFF,COMMONUSERDIFFFIELD,"97774230",USERNAME,More Cathrine,Wing Caryn
DIFF,COMMONUSERDIFFFIELD,"97774230",ORGNAME,Finance,Purchasing
DIFF,REMOVEDUSER,"99883134"
DIFF,NEWUSER,"99883434"
```

More information:

Evaluate Users Database (see page 195)
Merge Configurations (see page 195)

Compare Resources Databases

The Compare Resource Databases option enables you to compare two different resource databases and identify their differences. The function can be used to compare various databases stored on the original production server, or to conduct a comparison between the original database and the database that contains the results of discovery and audit processes. The Role Engineer can then examine the differences to verify that the changes are correct.

The Role Engineer has the option to display or not display the Compare Resource Databases output. This includes a Differences Report and a Differences Log. The feature can be used to produce a Differences Audit file also. Both the Differences Report and the Updates Log are displayed as text files in a Windows Notepad window. This enables you to edit and save the file on-the-spot.

To compare resource databases

1. Click File, Compare Resource Database.

   The Compare Resource Databases dialog appears.

2. Specify pathnames to input and output files.

3. Specify which differences to include in output files.

4. Specify report options as follows:

   View Report File

   Select this option to display a user-friendly report (Differences Report).

   View Updates Log

   Select this option to display the Updates Log.

5. Click Compare.

   The Differences report, log and audit files are generated.

Resource Database Report and Log Files

The Resource database report and log files list the results found after comparing the content of the Original Resource Database and the Updated Resource Database. The files are formatted in the same way as the report and log files that are generated when comparing two configuration databases.

The Report is presented in a user-readable format, whereas the Log is presented in a form that can be uploaded to the production machine. The following samples show an extract of both file types after comparing the same two resource databases.

The following is a sample Resource Database Report:

```
Differences Report
Original Resource Database: C:\Documents and
Settings\User\Desktop\Compare\ResDB.rdb
Updated Resource Database: C:\Documents and
Settings\User\Desktop\Compare\ResDBNew.rdb
Resource: (APPLDEV,RACFTEST,RACF22) Different Field (Field=Owner, Previous=,
Updated=ADMNLAN)
Resource: (APPLDEV,RACFTEST,RACF22) Different Field (Field=Organization, Previous=,
Updated=Production RACF)
Resource: (APPLDEV,RACFTEST,RACF22) Different Field (Field=Location, Previous=,
Updated=SAP R/3 Sun Server)
Resource: (appldev,NOVELADM,Novell4) appears only in the original configuration
Resource: (appldev,RACFTEST,WinNT) is new
```

The following is a sample shows the Resource Database Log:

```
DIFF,ORIGRDB,C:\Documents and Settings\User\Desktop\Compare\ResDB.rdb
DIFF,UPDRDB,C:\Documents and Settings\User\Desktop\Compare\ResDBNew.rdb
DIFF,COMMONRESDIFFFIELD,"APPLDEV","RACFTEST","RACF22",Owner,,ADMNLAN
DIFF,COMMONRESDIFFFIELD,"APPLDEV","RACFTEST","RACF22",Organization,,Production
RACF
DIFF,COMMONRESDIFFFIELD,"APPLDEV","RACFTEST","RACF22",Location,,SAP R/3 Sun Server
DIFF,REMOVEDRES,"appldev","NOVELADM","Novell4"
DIFF,NEWRES,"appldev","RACFTEST","WinNT"
```

More information:

Evaluate Users Database (see page 195)
Merge Configurations (see page 195)

Chapter 12: Unique User ID (UUID) Menu

The UUID menu lets you access the Unique User ID utility. Use this utility to consolidate related or duplicate user accounts from the different directories in your environment.

This section contains the following topics:

The UUID Tool

To access the UUID interface, click UUID, Launch UUID Tool.

The UUID user interface is divided into several sections that reflect the work process that you undertake in consolidating the access rights and privileges on your system. The following table describes the sections:

Section	Description
Java Package Directory	The path in which the UUID package is located. (this is where the CA Identity GovernanceMatcher.jar is located)
UUID Mapping File	The main settings file that refers to all other definitions.
UUID Working Directories	Defines the locations in which the tool can find source data and deposit temporary output files that contain consolidated output data. (all directories here must be on same drive, for example, C:\)
User Databases	Provide mappings that map each of the accounts sources (CA Identity Governance user databases).
Match Process	Provides the file name and directory of the configuration that results from the matching process, as well as a few general parameters for the matching. Also runs the process that performs the matching process.

Section	Description
Merge Process	Provides the file name and directory of the resulting configuration file that contains the consolidated access rights based on the above matching. Also runs the process that performs the merging process.

UUID Work Process

This section describes the general work flow that you perform when using the UUID tool.

The general work process is as follows:

1. For each of your company systems you must extract or export the user data and save it in the form of a CSV file in the same format as a CA Identity Governance Users DB (UDB). Each of the csv files should be renamed so that they use a *.udb extension. If you have imported the full access rights from those systems in a CA Identity Governance configuration, you can use the UDB from these configurations. You must create a data directory and then place the *.udb, or *.cfg files in the data directory.
2. Specify the path for the UUID Working Directories: Data Directory, Index Directory and Output Directory. (note that all directories must be on same logical drive, e.g., C:\).
3. Define the mapping definitions for matching users to their resources and accounts across available systems and save the mapping definitions file.
4. Run the Index.
5. Enter the path and name of the configuration file that contains the matched data in the Match Process section and run the Match process.
6. If desired enter the path and name of the configuration file that contains the merged data in the Merge Process section and run the Merge process.

Prepare Company HR and Systems Data

Using proprietary pattern recognition technology the UUID tool identifies and matches users to their accounts across all of your company systems. The source data used by the UUID tool is the user and account data for each system saved in the form of a CSV file. The format for this file is exactly the same as any other CA Identity Governance UDB. If you have imported a full configuration from a certain system, you can simply use its UDB here.

For each of your company systems:

Copy the *.udb files (or full set of .cfg, .udb, and .rdb) to the data directory.

The Data Directory is referenced as one of the Working Directories. The UDB files are used by the UUID tool during the matching and merging process.

Set Java Package Directory

The Java Package section in the UUID Tool references the installation directory that contains the CA Identity GovernanceMatcher.jar file.

To set the Java Package Directory

1. In the Java Package Directory section click *Browse*.

   A Browse dialog opens.

2. Browse to select the directory:
   Install_dir\Client Tools\Software\UUID\

   Note: *Install_dir* is the CA Identity Governance installation directory.

3. Click OK.

   The selected directory appears in the text field in the Java Package Directory section.

Working Directories

The Working Directories are a set of directories on your local machine that are used to house data and deposit output files that contain consolidated output data. The Data Directory is used to store your *.udb files that contain data extracted from your various company systems.

Note: All working directories must be placed on same logical drive, such as C:\.

Working Directory	Description
Data Directory	Stores data files containing user and account data extracted from the various company systems.
Index Directory	Stores internal UUID files generated as part of the Indexing process. **Note:** Erasing or editing these files causes the UUID tool to malfunction.
Output Directory	Provides a container to house temporary output files that are for internal use by the UUID tool only. **Note:** Erasing or editing these files will cause the UUID tool to malfunction.

Create and Assign Working Directories

You need to create each of the working directories on your database server and then assign their path in the UUID tool.

To create and assign work directories

1. On your local machine, create three directories, one each for your Data Directory, Index Directory, and Output Directory.

   For example using the directory path C:\testdemo\uuid_demo, create the following directories:

   Data Directory

   C:\test\uuid_demo\demodata

   Index Directory

   C:\test\uuid_demo\demoindex

   Output Directory

   C:\test\uuid_demo\demooutput

2. In the UUID Working Directory section of the UUID tool (highlighted in the following screen), enter the directory path in the text field for each of the directories that you created. To search for the directory click Browse.

3. Select the directory, click OK.

   The directory path is displayed in the selected Working Directory text field.

User Databases in the UUID Tool

The User Databases section of the UUID Tool is where you define the parameters and settings, and identify data that is used to consolidate the user access rights and privileges across all systems in your organization. Your goal is to identify each person in your organization with the accounts they have access to on each of the systems in your organization.

In some cases this is straight forward, for example, if the organization's personnel use the same account ID on all systems. In other cases, it may be possible to identify the owner of an account because accounts are based on some naming convention, for example, jdoe for John Doe. In the more difficult cases, it may be possible to recognize the account owner based on cues in some of the other account fields, for example, name (free text), address, phone number, email address, and so on. This information is contained in the database files, *.udb files, that you extracted from each of the systems.

Master vs. Other Databases

The Master database is usually the database that you extracted from the system that supports your Human Resources department. Using the User Databases window you create virtual connections between each User Database file and a Master Database file based on common information contained in the Master Database and any of the other databases.

Databases extracted from Human Resources generally contain a broad set of data on the personnel in your organization and generally reference each person by a unique employee ID. This ID is the single piece of information that must be included in a Master Database. In most cases, more information will allow you to match more accounts more accurately. Thus, any other information that is available is important to be included in the Master Database: name, department, title, location, manager, and so on.

Connecting Master and Other Databases

To correlate between users in different databases, definitions are required that describe and "canonize" the user-related information contained in the databases. Those definitions are called UUID-Fields. Specifically, the NAME, GROUP and FUNCTION attributes of the UUID-Fields defined for each database provide a means to correlate the data.

Using these UUID-Field attributes you create a virtual bridge between each User Database and the Master Database. When the UUID tool processes the data in each of the databases, it uses the information in these virtual bridges to identify each person in the organization with the accounts on each system to which they have access.

In practice the virtual bridge is referred to as the Group attribute of the UUID-Field, and the Name and Function attributes define the actions that are performed on each field in the databases to correlate data between the Master Database and the other User Databases. To successfully match organization personnel with their accounts, you must examine each of the User Databases and create as many UUID-Fields as are needed to link each person listed in the Master Database to the accounts that are referenced in the User Databases.

Example Database Usage and UUID-Field Construction

This example shows two separate databases that treat data for a single employee in an organization. In Database 1 the employee is referenced by Person Name and the employee Telephone number is provided in the form <Area Code-Number>. In Database 2 the employee is referenced by a Person ID and the employee phone number is provided as two separate fields, Area Code and Phone Number.

Database 1

Fields in Database 1	Person Name	Telephone
Data	John Smith	09-7693219

Database 2

Fields in Database 2	Person ID	Area Code	Phone Number
Data	1234567	09	7693219

By looking at the phone number in each database you can see that the Phone Numbers are identical even though they are referred to in slightly different forms. We can therefore extrapolate from that, that the employee John Smith in Database 1 is the same individual that is referred to by the Person ID of 1234567 in Database 2. Essentially we have used the data provided by the phone numbers to build a virtual bridge between the two databases.

UUID-Field Construction in the UUID Tool

In the UUID tool, the Group attribute of the UUID-Fields forms the virtual bridge. You create UUID-Fields with given Group attributes in the Master Database for each type of information that you want to use. You then create UUID-Fields with identical Group attributes in the User Databases that contain the same type of information that you want to relate to the information in the Master Database. The functions may vary in structure for the identical Groups in each database, but the goal is to construct the same data set using the available fields in the databases. In our simple example, the databases looks as follows:

Database 1 UUID-Fields

Name	Group	Function
Database 1_Ex	Phone	Telephone

Database 2 UUID-Fields

Name	Group	Function
Database 2_Ex	Phone	<Area Code>-<Phone Number>

Each database contains a UUID-Field with a Group called Phone. The Functions for each Group vary in structure but the outcome is identical. In the case of the example a phone number that is in the form <Area Code>-<Phone Number>.

UUID-Field Elements

Each database can contain several UUID-Fields. Each UUID-Fields has the following elements: Name, Group, Function, and Weight. The following list describes these elements:

Name

Specifies a name that is provided for each UUID-Field that is extracted from the database. The name does not have to be identical across each database.

Group

Specifies a name that is used for each common data type. The name for each common data type must be identical in each database.

Function

Specifies the action to be performed on the database fields. This might be to extract the data contained in a database field, or it might be to extract a combination of data contained in several fields in the database.

For help on the protocol used to construct combinations click the ? button in the Fields section of the User Database window. See the "UUID Indexing Functions" (see page 224) section for a complete list of the functions available to manipulate database fields and create UUID-Fields.

Weight

Provides a numeric measure to indicate the internal priority given to each group within a database. The greater the value the higher the priority. The UUID tool processes the groups according to their order of priority.

A value of 0 means that this group is not taken into consideration in the matching process.

Naming UUID-Fields

Each database must contain at least one UUID-Field that references the field in the database that contains the user-account information (Login). The name provided for that UUID-Field must be provided in the following form: <Database Name>_ID. The Name provided for any other UUID-Field can take any form.

For example, for a database called RACF.udb the Name provided for the UUID-Field relating to the user-account field is RACF_ID.

The purpose of this special UUID-Field is to support the Merge operation (post matching). It is used to compare to the Person ID field in the merged configuration.

Note: The ID UUID-Field *is not* used for the correlation process. It should be associated with a group of its own, and given a weight of 0.

Adding New Databases

You need to include a database for each system in your organization that you are referencing. These are files that were extracted from each system and renamed as *.UDB files.

To add a new database

1. Click Add New in the User Databases section of the UUID Tool.

   The User Database window opens.

2. Click Browse next to the UDB/CFG File Name text field and from the Open dialog box select the database file that you want to include.

   Note: If you later plan to run the Merge Process, you need to select a CA Identity Governance configuration file (.cfg file) originating from the referenced systems. Configuration files automatically direct the tool to their User Database (.udb file). Otherwise, you can select the User Database (.udb file) directly.

3. Click Open and the selected file name is displayed in the UDB/CFG File Name text field.

4. Click Save and provide a name for an XML file in the Save As dialog box. The XML file is the UUID Mapping file and stores all the mapping parameters associated with the database.

5. Repeat this procedure to add a reference for each User Database that was extracted from the organization.

6. Select the Database that contains the HR data and click Set Master. This sets the selected database as the Master database.

   The database that you select as the Master database must contain an explicit reference to each of your personnel by name. For this reason it is usually the database that contains the HR data.

Adding Databases from XML Files

If you already have an XML file from a previous implementation, you can refer to that XML directly. You do so by using the Add from XML feature in the User Databases section of the UUID tool.

To add a database from an XML file

1. From the User Databases section click Add from XML.

   The Save As window opens.

2. Navigate to the folder that contains your databases saved as XML files and select the database to add to the mapping file.

3. Click Save.

   The database is added to the list of User Databases referenced in the mapping file.

4. Click Save in the UUID Mapping File section to save the modified list of databases as part of the mapping file.

Editing Database UUID-Fields

At times you may need to modify existing matching UUID-Fields in a database, add UUID-Fields to a database, or remove UUID-Fields from a database. You do so by using the Edit feature in the User Databases section of the UUID tool.

To edit a database UUID-Field

1. Select an XML file from the User Databases list.

2. From the User Databases section click Edit.

   The User Database window opens displaying the list of UUID-Fields.

3. Select the UUID-Field that you want to edit.

   The selected row is highlighted.

4. Double-click in any field and the field becomes editable. You now can manually edit the value for the selected field.

5. When you are satisfied with your changes, click Save to confirm your changes in the database.

To add a UUID-Field to a database

1. Select an XML file from the User Databases list.

2. From the User Databases section click Edit.

   The User Database window opens displaying the list of UUID-Fields.

3. Enter values in the Name, Group and Function fields.

4. Enter a numeric value in the Weight text field.
5. Click Add.

   The new UUID-Field is added to the list of groups in the database.
6. Click Save to confirm your changes in the database.

To remove a UUID-Field from a database

1. Select an XML file from the User Databases list.
2. From the User Databases section click Edit.

   The User Database window opens displaying the list of groups.
3. Select the UUID-Field that you want to remove.

   The selected row is highlighted.
4. Click Remove and the selected group is deleted from the list of groups.
5. Click Save to confirm your changes in the database.

Note: You can define several UUID-Fields having the same Group name. For example, if the Master Database contains a value for US State (such as, NY), but it does not exist in a given User Database, you can still use some of the information that is available in the User Database to match to it. For example, suppose that the User Database contains telephone number and zip code. In that case, you can create two fields in the User Database: one will try to “guess” the state by mapping (lookup function) the telephone area code, and one will do the same but with the zip. Hopefully at least one of the matches will succeed and you will get a match.

Removing Databases

For any number of reasons you may no longer need to deal with data that is included in a particular system in your organization. In such cases you need to remove references in your mapping file to the database. You do so by using the Remove feature in the User Databases section of the UUID tool.

To remove a database from a mapping file

1. In the UUID tool, load the mapping file that contains the databases to be removed.

   The User Databases referenced in the mapping file are displayed in the User Databases list.

2. Select the User Database to be removed from the mapping file.

   The selected row is highlighted.

3. Click Remove.

   The selected row is deleted from the list.

4. In the UUID Mapping File section click Save to confirm the changes made to the mapping file.

Indexing the Databases

Index the databases referenced in a Mapping file you run the Match or Merge processes. While indexing the databases the UUID tool scans the data in each of the databases and loads the data into temporary files that are recorded in the Index Directory. If any changes are made to the database files or the Mapping file, then perform the index process again before you perform the Match or Merge process.

To index the databases

1. After setting the Working Directories, and defining the User Databases in the UUID tool, save the definitions as a Mapping file. If a Mapping file already exists click Load and load the mapping file into the UUID tool.

2. In the User Databases section of the UUID tool click Run Index.

   The UUID Index window opens and displays a progress bar for the index process. Depending on the size of your databases this process may take a couple of minutes.

   If an error occurs during the index process, an error message is issued as part of the progress report displayed in the lower part of the UUID Index window, and the cause of the error is indicated in the log file.

   If you neglected to Save the mapping file prior to trying to Run Index, a Save As window opens for you to save the file. After saving the file the UUID Index process begins automatically.

3. (Optional) To view a log of the index process click View Log to open the log. The log contains a line for each record that was scanned in each of the databases included in the mapping file.

   At the end of the progress display, the message Finished building Index files is displayed when the index is successfully built.

4. Click Done when the Index process is complete.

UUID Mapping File

The UUID Mapping File is an XML file that stores the parameters that are set in the UUID Working Directories, User Database, Match Process and Merge Process sections of the UUID tool. Once the parameters are saved, you can use the Mapping file to quickly populate the UUID Tool with the saved parameters instead of manually entering the data each time that you want to run the Match or Merge process. Alternately you can load mapping file and use it as the base for editing and saving a new mapping file under a new name.

To use a UUID Mapping File

1. Click Load in the UUID Mapping File section of the UUID tool.

   An Open dialog appears in which you can navigate to the location that contains the mapping files on your local machine. For organizational purposes we suggest that the UUID Mapping Files be saved in the same directory that contains the Working Directories.

2. Select an XML and click Open.

   The parameters stored in the XML file are loaded into the UUID tool.

Match Process

The Match process reads the User Database files referenced in the User Databases section of the UUID tool and correlates the Users with the account details in each of the systems. The results of the Match Process are stored in a configuration file.

Follow these steps:

1. Click Load in the UUID Mapping file section and load a Mapping XML file.

   The UUID Tool is populated with the parameters stored in the selected UUID file.

2. Click Run Index in the Users Databases section.

   The listed User Databases are indexed. Depending on the size of the Databases the indexing process may take a few minutes.

3. Click Run Match in the Match Process section.

The UUID tool processes the databases and tries to correlate every account in each User Database to one or more potential owners in the Master Database. The correlation is based on the fields defined for matching, weighted accordingly. The result is a Matching Configuration, where each of the users in the Master Database appears In the configuration's User Pane, and each of the users in the other User Databases (representing accounts) appear in the configuration's Resource. Res Name 1 is the account ID, taken from the <Database Name>_ID field in the User Database The name of the source system appears as Res Name 2. The degree of match is represented in the score (0-100) and appears as Res Name 3.This information is saved in the configuration file listed in the Output Config field of the Match Process section. You can now open the Output Configuration file in the client tools and view each person in the organization and the accounts on each system to which they have access.

Because the matches are represented as a regular CA Identity Governance configuration, you can also:

- Review and add/remove/change correlations manually, using the client tools Workstation
- Report all correlations, using the CA Identity Governance Reporting facilities
- Run a certification to confirm the correlations, using the CA Identity Governance Portal

See the respective user manuals for more details.

When reviewing and correcting correlation in the client tools Workstation, pay special attention to:

- Accounts that were not matched at all (Res Name 3 will be empty for these)
- Accounts that were matched but with a low probability (low score in Res Name 3) and thus represent more of a guess than a deterministic matching
- Accounts that were matched to multiple people (first note accounts with Total Number of Users greater than 1; note also that same account may be matched with different scores, so look out for those as well).

Merge Process

After you run the Match Process, inspect the results, and perform needed corrections, you now have a finalized configuration file, matching each person in the organization with their respective accounts on the referenced systems. You can now proceed to the final stage of creating a final configuration that links each person in the organization with all their resources in the referenced systems. This phase is called the Merge Process.

The Merge process reads the configuration files referenced in the User Databases section of the UUID tool and correlates the Users with the resource details in each of the systems that are referred to in the tool.

Note: To run the Merge Process, the UUID tool needs to have access to the configuration files of the referenced systems (.cfg files), and not to the Users Databases (.udb files).

To run the Merge Process

1. Click Load in the UUID Mapping file section and load a Mapping XML file.

   The UUID Tool is populated with the parameters stored in the selected UUID file.

   We assume that you have previously run a Match Process and that the configuration specified in the Output Config field of the Match Process section exists and represents the correct matching.

2. Click Run Merge in the Merge Process section.

   CA Identity Governance processes the databases and matches each person in the organization with the resources to which they have access rights and privileges across each system in the organization. This information is saved in the configuration file listed in the Output Config field of the Merge Section.

3. You can now open the Output Configuration file in the client tools and view the each person in the organization and the resources on each system to which they have access.

UUID Indexing Functions

UDB Fields Referencing

UDB fields can be referenced directly, for example *FirstName*, or with the Field Function, such as Field *('FirstName')*.

If the UDB field contains a space (' ') character, it can only be referenced with the FIELD function. for example *Field('User Name')*.

Field Referencing

Function Name Example	Parameters Results
<Direct>	Param1 - field name
FirstName	'John'
Field(fieldname)	fieldname -name of a field from the UDB
Field('First Name')	'John'

Lookup Functions

Translating using a CSV file

Function Name Example	Parameters Results
CsvLookup(csvFilename, value)	csvFilename - the CSV file containing the translation map value - the value to look-up
CsvLookup('areas.csv', City)	

String Functions

String Concatenation

Function Name Example	Parameters Results
+operator	str1 - string str2 - string
FirstName + LastName	'John Smith'

String Concatenation

Function Name Example	Parameters Results
Concat(str1, str2, separator)	str1 - string str2 - string separator - string
Concat('Hello','world',', ')	'Hello, world'

Sub String

Function Name Example	Parameters Results
Substr(str,from,to)	str - the string from - starting offset of requested substring to - ending offset of requested substring
Substr('John Smith',5,6)	'Sm'

String Trimming

Function Name Example	Parameters Results
Trim(str)	str - string with leading/ending spaces
Trim(' sentence between many spaces ')	'sentence between many spaces'

String Last Characters

Function Name Example	Parameters Results
LastChars(str,len)	str - string len - integer value specifying the required length of the tail
LastChars('where is the end',7)	'the end'

String Length

Function Name Example	Parameters Results
Strlen(str)	str - string
Strlen('hello world')	11

String Searching

Function Name Example	Parameters Results
StrFind(str,substr)	str - string substr - the string which we need offset of
StrFind('My favorite color is red','color')	12

Convert from Integer to String

Function Name Example	Parameters Results
StrOf(int)	int - integer value
StrOf(5)	'5'

Finding Digits in a String

Function Name Example	Parameters Results
DigitsOf(str)	str - string
DigitsOf('john12smith34')	'1234'

Replacing Strings

Function Name Example	Parameters Results
StrReplace(strSource,substr,replacing)	strSource - source string substr - the substring to be replaced replacing - the new sub-string
StrReplace('firstname1lastname1','1','2')	'firstname2lastname2'

Finding Alphabetic Characters

Function Name Example	Parameters Results
AlphaOf(str)	str - string
AlphaOf('a1!@b2#$A1%^B2')	'abAB'

Finding Alpha-Numeric Characters

Function Name Example	Parameters Results
AlphaAndDigitsOf(str)	str - string

Function Name Example	Parameters Results
AlphaAndDigitsOf('a1!@b2#$A1%^B2')	'a1b2A1B2'

Lower Case Conversion

Function Name Example	Parameters Results
ToLower(str)	str - string
ToLower('RRYMON')	'rrymon'

Upper Case Conversion

Function Name Example	Parameters Results
ToUpper(str)	str - string
ToUpper('rrymon')	'RRYMON'

Two-way Case Conversion

Function Name Example	Parameters Results
SwapCases(str)	str - string
SwapCases('RRymon')	'rrYMON'

Removing Vowels from a String

Function Name Example	Parameters Results
RemoveVowels(str)	str - string
RemoveVowels('johnSMITH')	'jhnSMTH'

Left-to-Right Reversing

Function Name Example	Parameters Results
Reverse(str)	str - string
Reverse('john SMITH')	'HTIMS nhoj'

Telephone Number Functions

Finding Country Code

Function Name Example	Parameters Results
TelCountryCode(phone)	phone - full phone number
TelCountryCode('+972-8-7654321')	'972'

Finding Area Code

Function Name Example	Parameters Results
TelAreaCode(phone)	phone - full phone number
TelAreaCode('+972-8-7654321')	'8'

Finding last 7 Digits of a Phone Number

Function Name Example	Parameters Results
Tel7Digits(phone)	phone - full phone number
Tel7Digits('+972-9-7467346')	'7467346'

Name Functions

Getting First Name

Function Name Example	Parameters Results
FirstName(name)	name - full name
FirstName('Ron Rymon')	'Ron'

Getting Last Name

Function Name Example	Parameters Results
LastName(name)	Name - full name
LastName('Ron Rymon')	'Rymon'

Getting Middle Name

Function Name Example	Parameters Results
MiddleName(name)	Name - full name
MiddleName('Ron Rymon')	'' (empty string)
MiddleName('John Ferdinand Smith')	'Ferdinand'

Getting Middle Initial

Function Name Example	Parameters Results
MiddleInitial(name)	Name - full name
MiddleInitial('John Ferdinand Smith')	'F'

Getting Name Suffix

Function Name Example	Parameters Results
NameSuffix(name)	Name - full name, including suffix
NameSuffix ('John Smith, Jr.')	'Jr.'

Email Address Functions

Getting User ID from Email Address

Function Name Example	Parameters Results
EmailUserID(emailAddress)	emailAddress - full email address
emailAddress - full email address	'rrymon'

Getting Email Domain From Email Address

Function Name Example	Parameters Results
EmailDomain(emailAddress)	emailAddress - full email address
EmailDomain('rrymon@ca.com')	'ca.com'

Formatting Email Address

Function Name Example	Parameters Results
EmailConvention(format, first, last, domain)	Create a convention formatted string of email address format - one of: ■ Flast ■ Lastf ■ First.last ■ Last.first ■ Last ■ First first - first name last - last name domain - the email domain
EmailConvention('flast','John', 'Smith', 'ca.com')	'jsmith@ca.com'
EmailConvention('lastf','John', 'Smith', 'ca.com')	'smithj@ca.com'
EmailConvention('first.last','John', 'Smith', 'ca.com')	'john.smith@ca.com'
EmailConvention('last','John', 'Smith', 'ca.com')	'smith@ca.com'

Function Name Example	Parameters Results
EmailConvention('first','John', 'Smith', 'ca.com')	'john@ca.com'

Address Functions

Getting Country Name from Address

Function name Function name	Parameters Results
AddressCountry(fullAddress)	fullAddress - string of full address
AddressCountry('CA Technologies, One CA Plaza, Islandia, NY 11749 USA')	

Getting City From Address

Function name Example	Parameters Results
AddressCity(fullAddress)	fullAddress - string of full address
AddressCity('CA Technologies, One CA Plaza, Islandia, NY 11749 USA')	

Getting Street Name from Address

Function name Example	Parameters Results
AddressStreet(fullAddress)	fullAddress - string of full address
AddressStreet('CA Technologies, One CA Plaza, Islandia, NY 11749 USA')	

Getting State from Address

Function name Example	Parameters Rsults
AddressState(fullAddress)	fullAddress - string of full address
AddressState('CA Technologies, One CA Plaza, Islandia, NY 11749 USA')	

String

Function name Example	Parameters Results
AddressZipCode(fullAddress)	fullAddress - string of full address
AddressZipCode('CA Technologies, One CA Plaza, Islandia, NY 11749 USA')	'46345'

Getting All Digits from an Address

Function name Example	Parameters Results
AddressDigits(fullAddress)	fullAddress - string of full address
AddressDigits('CA Technologies, One CA Plaza, Islandia, NY 11749 USA')	'82 1 46345'

Combining Functions

It is possible to nest functions, for example: ToLower(AlphaOf('A1B2C3')) => 'abc'

User-Defined Functions

It is possible for users to define and implement their own functions.

The declaration of such functions is done in an XML file named “userJarsDef.xml”. The format of the file is:

```
[set the jars variable for your book]
 <indexFunction
jarFilename="c:\dev\uuid\userJar.jar"
implClass="EvalSubstring"
function="UserPrivateSubstring" />
</jars>
```

The function implementation is expected to be found in the specified JAR file. The specified class should extend the class:

com.eurekify.matcher.indexer.evalfunctions. EvalFunc

The default-constructor of the class should define the number parameters this function accepts:

```
numberOfParameters = 1;
```

The class should implement the method:

```
public void run(Stack<Object> stack) throws eurekifyEvaluationException
```

First the stack needs to be checked with the function

```
checkTheStack(stack);
```

The parameters passed to the function are retrieved from the stack using:

```
String strParam = getStringParam(stack);
```

Or:

```
int intParam = getIntParam(stack);
```

The result of the function should be pushed back to the stack using

```
stack.push(result);
```

Example implementation class:

```
import java.util.Stack;
import com.eurekify.matcher.indexer.evalfunctions.*;
public classEvalSubstring extends EvalFunc {
```

```
public EvalSubstring() {
numberOfParameters = 3;
}
public void run(Stack<Object> inStack) throws eurekifyEvaluationException
{
// check the stack
checkTheStack(inStack);
// get the parameter from the stack
int to = getIntParam(inStack);
int from = getIntParam(inStack);
String str = getStringParam(inStack);

String result = str.substring(from, to);
// push the result on the stack
inStack.push(result);
}
}
```

Chapter 13: Troubleshooting

This chapter considers the following topics:

- Restoring/instantiating role links
- Copying roles from one configuration to another
- Error messages

This section contains the following topics:

Restoring/Instantiating Role Links

To remove a role but keep the links between the users and resources, do the following:

- Right-click on a role and select “Instantiate Direct Links” (and click Yes For All).
- Now the role can be deleted.

Copying Roles from One Configuration to Another

This example assumes that two configurations share almost the same users and resources.

In this case, it would be necessary to export the two configurations to CSV file format. Then, import the new configuration again with its roles and the roles-related text file.

The following example is a Perl template script to be used for copying roles:

```
#!/cygdrive/c/Perl/bin/perl

$cfg1=$ARGV[0];
$cfg2=$ARGV[1];
$cfgnew=$ARGV[2];

if ("$cfgnew" eq "")
{
print("Missing parameters\n");
printf("\n");
printf("Syntax:  copy_roles <CFG with source roles>\n");
printf("                    <TARGET CFG to copy the roles to>\n");
printf("                    <CFG New file Name>\n");
printf("\n");
printf("Example\n");
printf("copy_roles   old.cfg    new.cfg   new_cfg.cfg\n");

exit(1);
}

 if (!(-e $cfg1))
{
print "File $cfg1 does not exist";
exit(1);
}

 if (!(-e $cfg2))
{
print "File $cfg1 does not exist";
exit(1);
}
  print "Copy ALL roles from $cfg1.cfg to $cfg2.cfg\n";

open(A, $cfg2);

@b=split(',',Action:);
$udb2=$b[1];
chop($udb2);
print "udb=$udb2\n";
@b=split(',',Action:);
```

```
$rdb2=$b[1];
chop($rdb2);
print "rdb=$rdb2\n";
close(A);

 print "\n";
open(A, ">a.sbt");
print A "<BATCH> \n";
print A " <COMMAND \n";
print A " ACTION=\"EXPORT CSV\"\n";
print A " CONFIG=\"$cfg1\"\n";
print A " ROLE=\"roles1.txt\"\n";
print A " USER_RES=\"user_res1.txt\"\n";
print A " USER_ROLE=\"user_role1.txt\"\n";
print A " ROLE_RES=\"role_res1.txt\"\n";
print A " ROLE_ROLE=\"role_role1.txt\"/>\n";
print A "</BATCH>\n";
close(A);

print "Exporting $cfg1 started at ", `date`;
system("sage.exe a.sbt");

open(A, ">b.sbt");
print A "<BATCH> \n";
print A " <COMMAND \n";
print A " ACTION=\"EXPORT CSV\"\n";
print A " CONFIG=\"$cfg2\"\n";
print A " ROLE=\"roles2.txt\"\n";
print A " USER_RES=\"user_res2.txt\"\n";
print A " USER_ROLE=\"user_role2.txt\"\n";
print A " ROLE_RES=\"role_res2.txt\"\n";
print A " ROLE_ROLE=\"role_role2.txt\"/>\n";
print A "</BATCH>\n";
close(A);

print "Exporting $cfg2 started at ", `date`;
system("sage.exe b.sbt");
system("cp  roles1.txt roles3.txt");
system("cat roles2.txt >> roles3.txt");

system("cp  user_role1.txt user_role3.txt");
system("cat user_role2.txt >> user_role3.txt");

system("cp  role_res1.txt role_res3.txt");
system("cat role_res2.txt >> role_res3.txt");

system("cp  role_role1.txt role_role3.txt");
system("cat role_role2.txt >> role_role3.txt");
```

```
open(A, ">c.sbt");
print A "<BATCH>\n";
print A " <COMMAND\n";
print A " ACTION=\"IMPORT CSV\"\n";
print A " CONFIG=\"$cfgnew\"\n";
print A " USERS_DB=\"$udb2\"\n";
print A " RES_DB=\"$rdb2\"\n";
print A " ROLE=\"roles3.txt\"\n";
print A " USER_RES=\"user_res2.txt\"\n";
print A " USER_ROLE=\"user_role3.txt\"\n";
print A " ROLE_RES=\"role_res3.txt\"\n";
print A " ROLE_ROLE=\"role_role3.txt\"\n";
print A " ROLEID_AS_NUM=\"FALSE\"/>\n";
print A "</BATCH>\n";
close(A);

print "Importing $cfgnew started at ", `date`;
system("sage.exe c.sbt");

print "Importing $cfgnew ended at ", `date`;
exit(0);
```

Error Messages

The following table shows typical messages and the type of action to perform:

Message	Description
CSV Export Generated Some Errors. Please see log.	Refer to the log for details of the generated errors. This message can appear if the source and target files were not properly designated. The CSV converter has a special log named “CSVConverterLogxxx.log”.
Please enter an integer between 1 and 9999999	You are trying to enter non-numeric characters in a field that is numeric only.
Resource [name of resources] Has Links. remove anyway?	Confirmation message appearing before performing a deletion of a resource.
One or more parameters missing	Verify that you have filled in all the required parameters.
Cannot remove indirectly linked users. None were removed.	CA Identity Governance does not permit the removal of indirectly linked users since this would change the parameters of other users. Try going to the directly linked users first and performing the removal there.
No New Role Candidates Were Discovered	CA Identity Governance did not find any new role candidates within the parameters that you chose. Reset the threshold and try again.

Message	Description
Could Not Find Any Related Roles	CA Identity Governance did not find any related roles within the parameters that you chose. Reset the threshold and try again.
No Potential Collectible Resources Were Discovered	CA Identity Governance did not find any collectible resources within the parameters that you chose. Reset the threshold and try again.
AuditCard belongs to configuration file <file name and path>. Do you want to open the file? Yes. No.	You are attempting to open an existing AuditCard without first opening the related configuration file. Choose Yes to open the relevant configuration file. The AuditCard will open immediately afterward.
Failed to Connect Database Server	A communication error exists while trying to perform File, Save to Database. Check communications to the remote server.
To copy, source and target configurations must have same Users and Resources databases.	Copying from databases to a configuration that has different databases is not allowed. The only way to do this is to add the database item as a new record.
Server is down	Communication with the CA Identity Governance server has failed. This message may indicate a hardware failure. This message will also appear if attempting to download data from an active directory without first installing the CA Identity Governance AD interface.
Failed to Read User's Database. Do you want to view the Log file	You probably tried to open a configuration file whose database is not in the correct folder. View the log file, and try again after copying the file to the appropriate folder.
Encountered Errors Registering Configuration	Errors were detected when opening the configuration. It is usually followed by a prompt to open the log file.
Unknown error when opening the configuration file. Do you want to open the log file.	Click Yes to open the log file and determine the type of error.

Chapter 14: File Formats in CA Identity Governance

CA Identity Governance uses three separate but related files in text-based comma-separated format to represent a configuration. These files are:

- Users database file
- Resources database file
- Configuration file

The users and resources database files contain the basic features of users and resources. The configuration file contains the dynamic parts of a configuration, such as the roles and relationships/connections.

This section contains the following topics:

Users Database File

Each user is represented in this file by one line, which includes comma-separated values for the following fields (in this order):

- PersonID (the key)
- User name
- Organization name
- Organization type
- Additional fields (optional)
- Up to 6 additional fields per user

Example:

```
234A745,Tony O Smith,Sales US West Coast,Sales,San Francisco,234A111,5
```

373B234,Mark W Johnson,San Jose Wireless Research,R&D,San Jose,123B546,1

In the above example, the data imported for Role building includes the following data in the optional fields: the employee's geographic location in the first additional field; the direct supervisor's ID in the second field; and the number of years with the company in the third field.

In addition, it is possible to specify the names of the optional fields, using the following instructions:

- NumFields,<nfields> is used to specify the number of optional fields
- FieldName,<i>,<name of field i> is used to specify the name of the optional i-th field

For example, for the above set of users, the following text may be used at the beginning of the users database:

```
NumFields,3
```

FieldName,1,Location

FieldName,2,Supervisor

FieldName,3,Seniority

Resource Database File

Each resource is represented in this file by one line, which includes comma-separated values for the following fields (in this order):

- Resource Name 1
- Resource Name 2
- Resource Name 3
- Additional fields (optional)
- Up to 6 additional fields

Example:

```
System Administrator,Unix-348,Unix,AIX,ControlSA ESS
```

Marketing Managers,NT-720,NT,Windows,PR Planning

In the above example, resources are imported at the user group level (generally, any granularity for resources can be determined). The optional fields include information about the platform and specific application on this platform. Resources are differentiated from one another by the combination of the first three fields, which is the key.

As with users, here too one can specify the number and titles of each of the optional fields. The following is an example:

```
NumFields,2
```

FieldName,1,OS

FieldName,2,Application

Configuration File

Each line in this file represents one entity and/or one relationship.

Reference to Static Users and Resource Databases

This section comprises the first two lines in the file, and it provides a reference to the users and resource database files. These lines have the following formats:

```
UsersDB,<Users Database File Name>
```

ResDB,<Resource Database File Name>

Multiple configurations may share the same users and resource database files, even if only a small number of users and/or resources actually participate in each configuration.

Entities

This section immediately follows the database reference section, and it describes the entities that participate in this configuration. The first set of lines identifies the users, one line per user, in the following format:

```
User,<UserID>,<SA User ID>
```

The User ID is used to describe the rank of the user in the users database file with the first number being “0” (thus, the fourth user in the database will have a User ID of 3).

The second set of lines identifies resources, one line per resource, in the following format:

```
Res,<Resource ID>,<User Group Name>,<Resource Name>,<Resource Type>
```

The Resource ID is the rank of the resource in the resources database file (with the first number being “0”).

The third set of lines in this section identifies roles (if existing), one line per role, in the following format:

```
Role,<Role ID>,<Role Name>,<Description>, <Organization>,<Owner>
```

CA Identity Governance provides automatic serial numbering of roles. If a configuration is created from an EUA and roles are being imported, the Role Engineer can choose a specific numbering scheme, as long as the numbers are unique and the Role Name is unique.

Relationships

This section follows the entities section and consists of the following types of line formats:

User - Resource Permission

```
User-Res,<User ID>,<Resource ID>
```

User - Role Permission

```
User-Role,<User ID>,<Role ID>
```

Role - Resource Permission

```
Role-Res,<Role ID>,<Resource ID>
```

Role Hierarchy Permission

```
Role-Role,<Role ID of parent role>,<Role ID of child role>
```