CA Identity Portal

Administration Guide

1.5.1

CA Technologies Product References

This document references the following CA Technologies products:

- CA Identity Governance
- CA Identity Manager
- CA Single Sign On
- CA User Activity Reporting
- CA Service Desk Manager
- CA IAM Connector Server

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

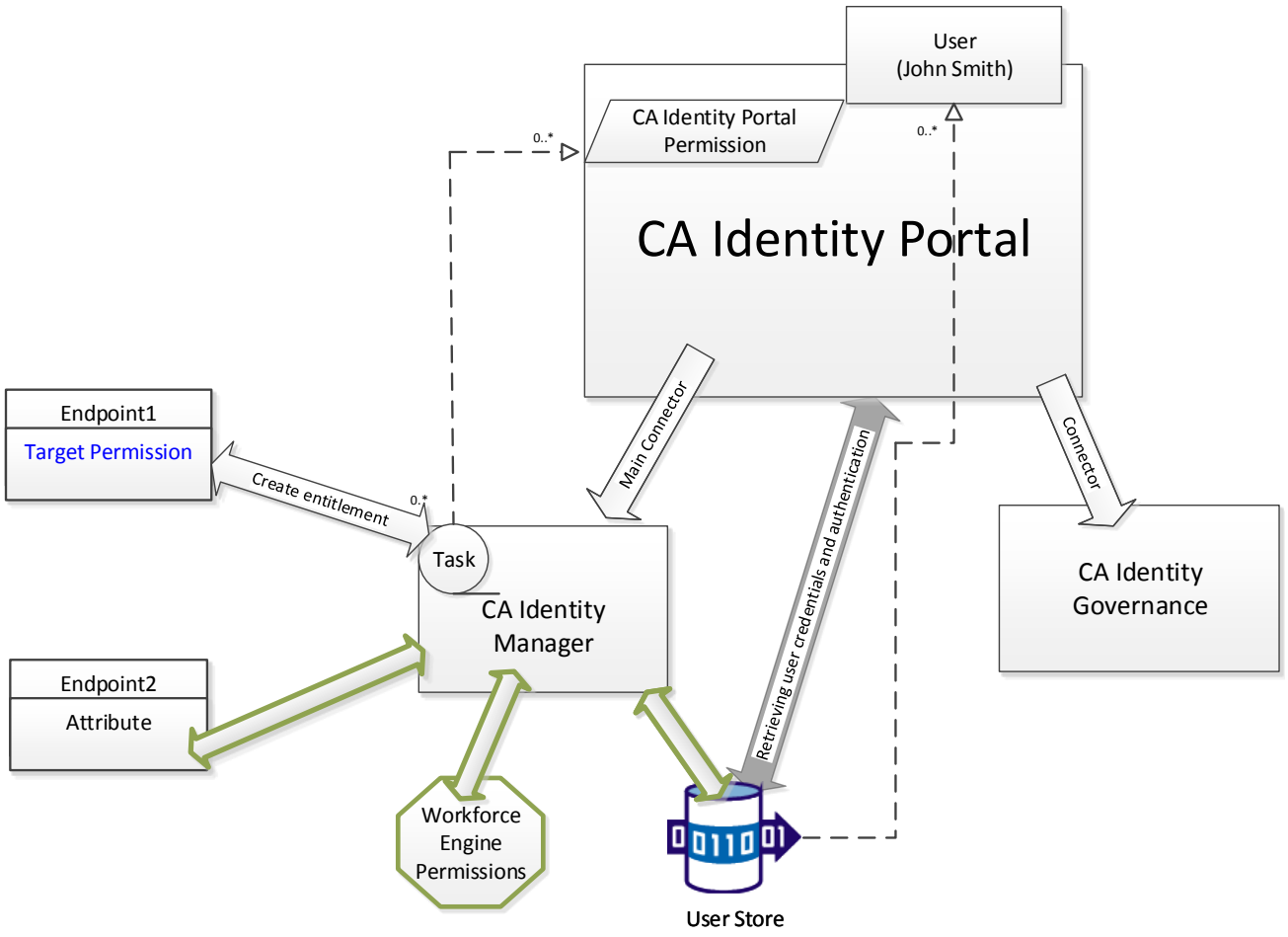
To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Introduction

CA Identity Portal is a web-based business-ready identity and access management application, which serves as a business logic layer that leverages and aggregates functionality from existing identity management products, such as CA Identity Manager (IM) and CA Identity Governance (IG). CA Identity Portal is designed for the non-technical business end-user and delivers an intuitive, all-inclusive interface in the form of a single page web application.

CA Identity Portal interfaces with the organization's existing IDM platforms (such as CA Identity Manager) through CA Identity Portal's backend connectors, and communicates with the IDM backend platforms using the exposed public APIs of these backend systems (for example, Web Services (TEWS) & Workpoint APIs for IM, and web services API for IG).

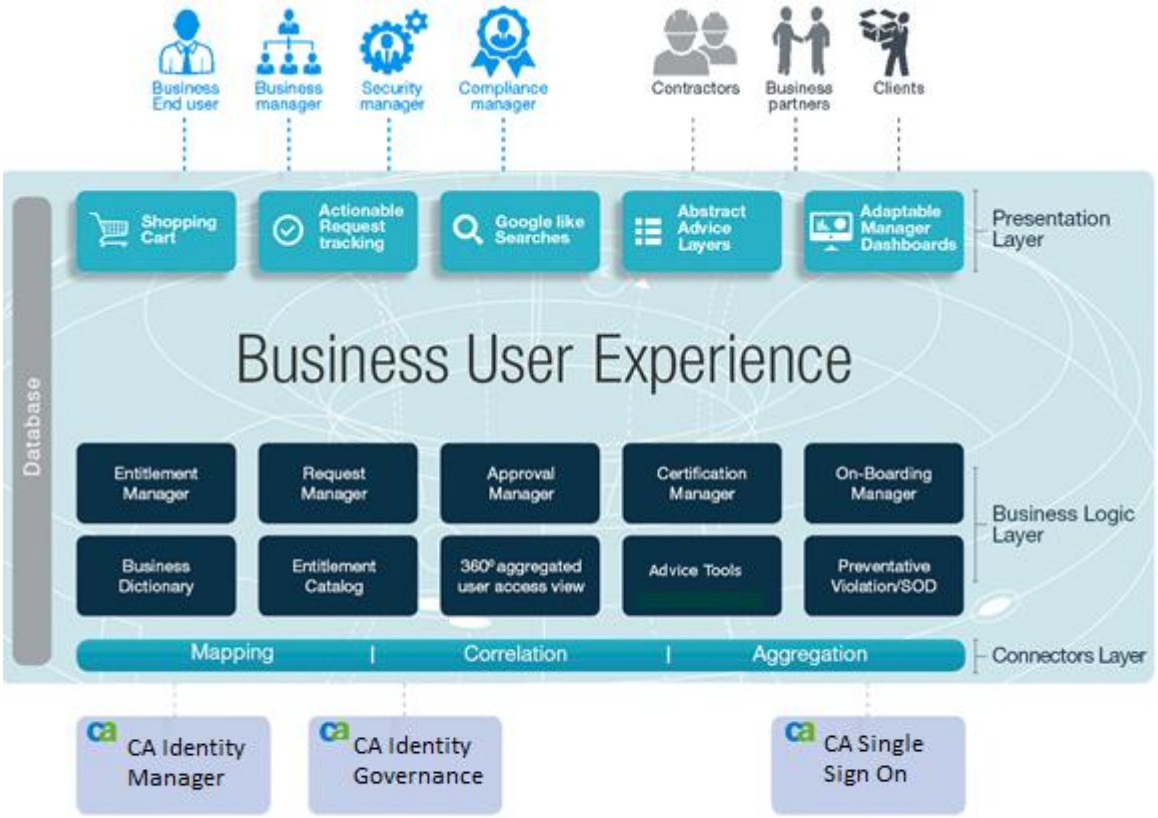


Architecture

CA Identity Portal's architecture is based on a layered approach:

- Presentation Layer – single page web application that runs on the client side. It makes Ajax/REST calls to the CA Identity Portal BL tier. This layer is written in angular.js which is Google's framework for client applications.
- Business Logic Layer – JAVA application server implementing the CA Identity Portal BL language. Business level language of IAM (access, entitlements, certifications etc.). The BL layer uses functionality that the connector layer provides.
- Connectors Layer – another layer in the application server that pulls, aggregates data and invoke operations on CA Identity Portal endpoints. The CA Identity Portal endpoints are the IAM platforms currently supported. Today these are: CA Identity Manager and CA Identity Governance. CA Identity Portal is not a provisioning engine, it inherits that logic and functionality from IM.

CA Identity Portal can integrate with CA Single Sign On for authentication only (SSO integration is optional, not a prerequisite).



System Administration

CA Identity Portal's administration application allows system administrators to perform the following administrative tasks:

- Configuring CA Identity Portal in the organizational environment and linking it to various organizational applications (IAM - Identity and Access Management / IAG - Identity and Access Governance); refer to Connectors for more information on connecting to CA Identity Portal connectors.
- Defining the business logic of the CA Identity Portal system, and workflows derived from that logic.
- Configuring the end-user interface based on these business logic definitions

Refer to CA Identity Portal Administration for more information on CA Identity Portal administration and configuration.

Note: In order to perform administrator tasks in CA Identity Portal you must be logged in with a CA Identity Portal system admin account.

Functionality Overview

CA Identity Portal enables you to expose a user-friendly business-oriented interface which performs a translation of technical IDM terms to business user terms. It allows the end user to perform the following functions:

- Access Request
- Create Objects
    - Create User (for example: Onboarding and Self-registration)
    - Create Group
- Manage Objects
    - Modify User (for example: User Management)
    - Modify Group
- Passwords Management
- Certify Existing Entitlements

Each action the user performs (access request, user management etc.) is treated in CA Identity Portal as a request. The end user will be provided a REQUEST ID and with that he is able to track his requests in "My Requests" section. The actions can also result in an approval process that is dependent on the backend configuration of the task that is triggered. If the task triggered has an approval workflow configured then when a user logs into CA Identity Portal, the user can see the approval and implementation items that require attention in the "Tasks" section.

By deploying CA Identity Portal in a client environment you will improve the efficiency and usage of the IAM solution and reduce security risks by providing the end users with advisory tools.

CA Identity Portal Functionality

The following section describes the functionalities that are exposed to the CA Identity Portal end user. It will help the administrator understand the features that are available to the end user and it provides quick links to the relevant administration sections so the administrator can make the required configurations.

My Requests

Any request or action the end user performs in CA Identity Portal results in a request. When a user submits such a request he is displayed a REQUEST ID. That request ID can be used to track his submitted actions. "My Requests" is available from the landing page ("Home"), from the top navigation menu or from the "Dashboard".

The "My Requests" page is divided into the following panes:

- Left pane – displays the list of requests submitted by the user and their status. The list can be filtered by any of the displayed fields. The user can select a different "Profile" to view the requests by, this will allow him to get an administrative view of requests that he did not submit. The available profiles are configurable; refer to "Profiles" configuration section for more information.
- Middle pane – displays the details of the selected request. The details contain the original request only. Modifications to a request are not visible here. One CA Identity Portal request can contain multiple request items in it (for example: multiple applications and permissions). Each one of the permissions can be selected.
- Right pane – displays the timeline of the request or the specific permission selected in the request details (in the middle pane). The timeline details the flow of the requested item – submitter, approver, implementer etc. and the status of each step of the workflow. The user can hover over the name of the approvers and view additional information about the user (or group of users). That information is configurable; refer to "GUI Configuration" section for more information.

Tasks

This section will display any pending tasks the user has on the supported systems that were configured in CA Identity Portal. For example: pending certification campaigns in CA Identity Governance or pending work items in CA Identity Manager. "Tasks" is available from the landing page ("Home"), from the top navigation menu or from the "Dashboard". The following task types are available in CA Identity Portal:

- Approvals
- Implementations
- Certification Campaigns

Approvals

Any request or action the end user performs in CA Identity Portal can potentially result in an approval workflow, this is dependent on backend configuration in the supporting system (for example: CA Identity Manager Workflow). If a workflow work item exists in the connected system CA Identity Portal will automatically display it in "Tasks". Any work item is displayed here even if it was not generated in CA Identity Portal. Work items generated in CA Identity Portal will have a request ID, whereas work items generated directly in the backend system will not have a CA Identity Portal request ID. Work items can be approved/rejected or any other action that was defined in the backend system. Once in action is taken on an approval item it is removed from the list.

The "Approvals" tab is divided into the following panes:

- Left pane – displays the list of pending work items. The list can be filtered by any of the displayed fields.
- Middle pane – displays the details of the selected request.
    - Request Information – this tab contains the original request only and only the requested item that is relevant to the approver reviewing the request.
    - Process Information – this tab is optional and it depends on the configuration of an approval task; refer to "Tasks" section for more information. This tab can be editable in case an original request needs to be modified or approvers are required to provide additional input.
    - Advanced Information – this tab displays the entire information in the approval task in an unedited able/raw form.
- Right pane – displays the request history similarly to the timeline view of "My Requests". The timeline details the flow of the requested item – submitter, approver, implementer etc. and the status of each step of the workflow. The user can hover over the name of the approvers and view additional information about the user (or group of users). That information is configurable; refer to "GUI Configuration" section for more information. The approver can leave a comment and then click a button to perform the desired action. The default actions are approve/reject but more actions are available based on the button configuration of the connected task; refer to "Tasks" section for more information.

Implementations

Implementation tasks are approval tasks that have some configuration on them telling CA Identity Portal this is actually an implementation. In CA Identity Manager this is done by setting a user data on the Workpoint activity node; refer to "Tasks" section for more information.

When a work item is interpreted in CA Identity Portal as an implementation task instead of an approval task all CA Identity Portal does is display the item under "Implementations" tab instead of "Approvals" and display "Implement" action button instead of the "Approve/Reject" actions; refer to "Approvals" section for more information on what is displayed here.

Certification Campaigns

Any certification campaign pending tasks in the connected backend system will be automatically displayed here for the end user to review. For example: if a campaign was triggered in CA Identity Governance and the connected user has pending approval items in that campaign he will be able to approve/reject in this tab. Pending campaign alerts are also available from the top menu which will display the remaining days of a campaign.

The "Certification Campaigns" tab is divided into two panes:

- Left pane – displays the list of pending campaigns.
- Right pane – displays the list of pending approval for that campaign. The view can be switched between: by user, by role and by resource. Decisions can be saved or submitted. The approver can automatically populate decisions in the campaign by clicking on "Previous Decisions". This will only work if the user had approved/rejected the same item in a previous campaign (for example: approve John's network access)

Access

Users can request access for themselves, other users or even a request in bulk using a file upload. Access request can be for real access to connected systems, manually provisioned access to disconnected systems or non-system access such as hardware request.

When a user(s) is selected (self, other or bulk) there are two tabs:

- Current – displays the current access the user has. When the request is for more than one user the current access will always be blank.
- Add Systems – display the current access plus all the available items the user can request access for. The available access is dependent on permissions defined in the backend IDM system and also in an additional layer of scoping provided by CA Identity Portal.

Add Systems

Available systems for request can be viewed in the following ways:

- All Available Systems – this gives the requester a full view of everything he can request access for based on the defined scoping.
- By Role – administrators can define suggestive roles in CA Identity Portal and link them to various permissions. The requester can then view a role and select permissions from that role.
- By Similar Users – requesters can view the access of other users and based on that decide what access they want to request. The view of the similar users section is configurable; refer to "GUI Configuration" section for more information.
- Favorites – requester can save items such as applications, roles and requests as favorites in order to save time when navigating to them in the future.

"Add Systems" tab is divided into the following panes:

- Left pane – displays the list of available applications. Applications can be grouped into different sections. The applications and group of applications can be searched. The list of applications is configurable; refer to "Permission Model" section for more information.
- Middle pane – displays the list of available permissions for the selected application. The user can select to Add/Modify/Remove permission. The available actions are configurable for the specific permission; refer to "Target Permissions" section for more information. For each action there can be additional information for the user to fill out; refer to "Forms" section for more information.
- Right pane – displays the CA Identity Portal cart which is the selections the requester made in the permissions section in the middle pane. Request to "Add" permission is automatically added to the "Added Permissions" section in the cart and so on.

Risk Meter

If risks is enabled, while adding permissions to the cart the risk will be calculated and be reflected using the cart icon on the risk meter. Clicking on the risk meter will display what constructed the risk. When entering the request summery view the violations that exist due the permissions in the cart will be displayed on top of their corresponding permission.

The user itself will be displayed in the color of his current risk.

Dynamic Modules

Administrators can configure CA Identity Portal to manage two types of objects: users and groups. The dynamic configuration though allows the administrators to reflect those objects to the end user as custom objects as well. The administrator can name the module in any name they like to reflect the type of actions that can be performed there; refer to "Modules" section for more information.

The next sections describe the available actions.

Create

This module template allows for creation of user and group objects. For example this can be used to configure a module called: Onboarding.

In this module the user can select create actions as defined by the administrator; refer to "Tasks" and "Forms" sections for more information.

Manage

This module template allows for modification of user and group objects. For example this can be used to configure a module called: User Management.

In this module the user can search and select an object (user or group) and then select modification actions as defined by the administrator; refer to "Tasks" and "Forms" sections for more information.

Registration

This module template allows for creation of user and group objects. For example this can be used to configure a module called: Self-Registration.

In this module the user can perform public tasks (that do not require him to log into the system) as defined by the administrator; refer to "Tasks" and "Forms" sections for more information.

Passwords

Forgotten Password

This feature is provided out of the box with CA Identity Portal. The end user will be able to perform the public task of forgotten password reset as long as the basic connector configuration to the Identity Management system has been performed. No need for additional admin configuration unless changes from the default behavior are required; refer to "Password Management" section for more information.

Expired Password

This feature is provided out of the box with CA Identity Portal. The end user will be able to perform the public task of change password when it is expired as long as the basic connector configuration to the Identity Management system has been performed. No need for additional admin configuration unless changes from the default behavior are required; refer to "Password Management" section for more information.

Dashboard

The dashboard view aims to bring the various information that exist in different modules to one place. In the dashboard view a user can perform actions on tasks, campaigns and track requests.

CA Identity Portal Administration

This section describes the configuration and administration capabilities of CA Identity Portal's administrative UI. It also contains explanations for CA Identity Portal features that do not require additional configuration.

To login to the administrative UI follow this link:

http://<CA Identity Portal App Server>:<Port>/sigma/admin/

You will be prompted for username and password, use the credentials entered during the installation process.

Understanding Scoping

Before diving into specific configurations in CA Identity Portal it's important to understand CA Identity Portal's scoping mechanism.

Administrative roles are used in identity management for managing individual business requirements. A role defines what operations can be performed by a user.

These operations define the ability of a user to acquire access (or requesting one) for different entitlement or business flows in the organization.

When a user logs in to CA Identity Portal, this information is pulled by CA Identity Portal connectors. CA Identity Portal then calculates and translates this information and allows the user to request access or trigger flows only to what he's allowed to.

This calculation is performed in several scenarios:

- After selecting a user in the access module - CA Identity Portal calculates which permissions the logged in user is allowed to request for the selected user.
- In dynamic modules – CA Identity Portal calculates what invocations operations (operations of type USER and GROUP) are within the logged-in user scope on the selected user.

CA Identity Portal offers an additional layer of scoping in the access module which can be configured in the target permission's rule. Refer to Target permission Rules for more information.

Connectors

Configuring CA Identity Portal in the organizational environment consists of creating interfaces to the organization's IAM/IAG's by configuring CA Identity Portal's connectors.

CA Identity Portal uses connectors to communicate with IAM/IAG's.

The connectors enable CA Identity Portal to perform the following tasks:

- Authenticate/authorize users to CA Identity Portal's interface.
- Fetch exiting entitlements and expose them to end user.
- Request entitlements.
- Update statuses or ongoing activities.

CA Identity Portal's factory settings support the following connectors:

- IM Connector – supports connectivity to the various IM versions.
- IG Connector – supports connectivity to various IG versions.

Note: For supported versions, please refer to the CA Identity Portal's Platform Support Matrix.

- DB Connector – A connector to a custom database which allows you to define your own entities and save their current state.

CA Identity Portal also supplies an SDK for implementing your own custom connector. For more information please see the CA Identity Portal's Programming Guide.

Note: Configuring connectors is the first task that has to be completed in CA Identity Portal's setup process. Complete all required connectors before proceeding with the rest of the configuration.

Main Connector

The Main Connector identifies a connector as the authoritative source that will be used by CA Identity Portal for user authentication.

It is recommended that the Main Connector will be connected to the IAM/IAG system which contains the most extensive information of users in the organization.

Creating a Connector

To create a connector you must have the IAM/IAG set-up. You will need to collect basic connectivity information on the endpoint to which you would like to connect before creating the connector. This information is typically available in the endpoint administrative management console.

To create a connector:

- Select the ***Connectors*** tab.
- Choose the ***New Connector*** button.
- Fill in a name that will identify the connector.
- Tag will be auto-populated based on the name, it can be modified.
- Select the type of connector from the list.
    - For CA Identity Manager connector select: com.idmlogic.sigma.connector.ca.CaimAdapter
    - For CA Identity Governance connector select: com.idmlogic.sigma.connector.ca.GmAdapter
- If no Main Connector is defined in the system, an option to configure this connector as the main connector will be available.
- Fill in all the information required by the connector. An explanation of the purpose and samples of values is available next to each field.
- Once completed click ***Save***.

Upon saving the connector for the first time, the connector will not attempt to load automatically. The connector can be started manually by clicking on ***Start***. If an error occurs you will receive an error message in the log and the connector status will be displayed as ***Down***. If the connector is created successfully the connector status will be displayed as ***Up*** and no error message is displayed in the log.

To modify the connector settings, click the connector.

Editing an existing Connector

1. Switch to the Connectors tab.
2. Click the connector you wish to edit.
3. Edit the connector's settings.
4. Click ***Save***.

Upon saving the connector, the configuration will be saved but the connector will not attempt to load with the new configuration. To start the connector with the new configuration, click the ***Restart*** button to restart the connector with the new configuration.

Note: Restarting the connector will cause it to be unavailable for the duration of the restart.

CA IM Connector configuration

CA IM connectors are defined per environment. The following parameters are used when defining a connector:

CA IM

CA IM UserId – the identifying attribute of a user in the CA IM endpoint, which can be found in the User directory mappings in the management console.

Group name attribute – the identifying attribute of a group in the CA IM endpoint, which can be found in the Group directory mappings in the management console.

CA IM Admin User – service admin user for identity management.

CA IM Admin Password – service admin user password for identity management.

Environment Id – environment id number; can be found in the environment configuration in the management console.

Environment Name - environment name, can be found in the environment configuration in the management console.

Generate Binding File – determine whether to create a binding file that tries to correct the errors in the compilation of the WSDL.

Management console password – password to be uses for authentication to the management console, if defined.

Management console URL – environment management console URL. Usually http://<server_name>/iam/immange/ (make sure to include the closing "/")

Management console user id – username to authenticate to the management console, if defined.

No compile list – the list contains task tag names from IM (comma-separated) that will not be compiled when the connector starts (black list).

Roles and task converter – define the version of IM for the connector. For IM supported versions up to 12.6 SP1 (including) select – com.idmlogic.caim.Converter1259. For IM supported versions from 12.6 SP2 (including) select – com.idmlogic.caim.Converter1262.

Static roles and tasks XML – used as a static override for environment roles and tasks xml file, should be used only in debug mode.

TEWS client dir – directory for saving compiled classes used for TEWS.

TEWS wsdl URL – this is a mandatory attribute which contains the URL for the WSDL, which is generated for the connector environment. This parameter is case sensitive in CA IM. Typically http://<server_address>/iam/im/TEWS6/<environment_public_name>?WSDL

Forgotten Password

Forgotten password answer attribute – prefix for the answer attribute as defined in IM (usually this is the forgotten password LAH attribute).

Forgotten password attribute – the password attribute as defined in the forgotten password task.

Forgotten password confirm attribute – the confirm password attribute as defined in the forgotten password task.

Forgotten password question attribute – prefix for the question attribute as defined in IM (usually this is the forgotten password LAH attribute).

Forgotten password task – the task (tag) used to reset forgotten password in IM (by default there are two different forgotten password tasks in IM that can be used in CA Identity Portal as well).

Reset Password

Reset password confirm password attribute name – the password confirm attribute as defined in the reset password task.

Reset password password attribute name – the password attribute as defined in the reset password task.

Reset password task tag – the task (tag) being used to reset users' expired password. By default this is configured to a CA Identity Portal service task.

Reset password to another confirm password attribute name – the password confirm attribute as defined in the reset password task. Reserved for future use.

Reset password to another password attribute name – the password attribute as defined in the reset password task. Reserved for future use.

Reset password to another task tag – the task (tag) being used to reset users' expired password. By default this is configured to a CA Identity Portal service task. Reserved for future use.

Tasks

Admin task task – CA Identity Portal service task (tag) for reading information about other tasks.

Approval task search task – CA Identity Portal service task (tag) used to search for approval tasks

Default search task – CA Identity Portal service task (tag) used to search for users who must be in scope.

Group search task – CA Identity Portal service task (tag) used to search for groups who must be in scope.

Login task – CA Identity Portal service task (tag) used to verify login.

Scope task – CA Identity Portal service task (tag) used to fetch the tasks in the authorized scope for this user in the system:

Scope task execution field - used to describe *Scope task* task field.

Scope task group field - used to describe *Scope task* group association field.

Scope task roles field - used to describe *Scope task* role field.

Task status task – IM default task (tag) used to read information about task state.

Task statuses batch size – Limits the task statuses batch size (as configured in *Task statuses task*)

Task statuses task – CA Identity Portal service task (tag) used to read information about multiple tasks state (unlike the default IM task that only allows one task).

User Status attribute – the IM user attribute that contains the user status for login purpose.

Worklist task – CA Identity Portal service task (tag) used to read information about a logged in user's pending work list

Workpoint

Worklist date format – date format of a work list item. i.e: EEE MMM d HH:m:s z yyyy

Workpoint application server – application server brand on which workpoint is installed, JBoss and WebLogic are supported.

Workpoint client directory – location of the workpoint client jars specific for the application server

Workpoint context class – used to define Workpoint client context class. This information is relevant for defining the Application Server on which the workpoint resides. Information can be fetched from the workpoint designer configuration file.

Workpoint DB – workpoint DB name, by default WPDS.

Workpoint fetch work items strategy – the method in which CA Identity Portal will fetch work items. Either from TEWS task "View My Worklist" (default configuration) or directly from workpoint client API (which allows you to limit the number of work items retrieved)

Workpoint service method – agent connection type, usually EJB.

Workpoint service URL – used to define the URL used by the workpoint client to connect to the workpoint server. When workpoint is installed on JBoss, this is usually the hostname of the server. On WebLogic this is usually t3://<server address>

Note: It's important to configure FQDN resolution between the servers before defining this parameter.

Workpoint service user id – application server administrative user, if defined. Usually WebLogic application server is protected by a service user.

Workpoint service user password – application server administrative user password, if defined.

Workpoint user id – user for workpoint access (any name is valid here, does not need to be an actual system user)

Workpoint user password – password for the workpoint user. This is for future use, today workpoint API does not support this feature.

Workpoint work item client limit – when fetching work items directly from workpoint it has a limit on the number of work items to get.

CA IG Connector Configuration

Admin Name– service admin username for CA Identity Governance

Admin password – service admin for CA Identity Governance

Certification resource display field – the display field that is used in the IG universe to describe the resource. By default the display attribute will be the IG configuration. To control the display attribute refer to the customization option in certification campaigns

Certification role display field - the display field that is used in the IG universe to describe the role. By default the display attribute will be the IG configuration. To control the display attribute refer to the customization option in certification campaigns.

Certification user display field - the display field that is used in the IG universe to describe the user. By default the display attribute will be the IG configuration. To control the display attribute refer to the customization option in certification campaigns.

IG server version – version of the connector, should match the version of IG. Versions supported: 12.5.7, 12.6.0, 12.6.1

Master configuration – master configuration under the universe.

Model configuration – model configuration under the universe.

Reassign Search attribute – IG attribute used to identify users for reassign feature in a certification campaign.

Server name – IG server IP address or FQDN.

Server port – IG server port.

Universe name – Universe name to which the connector will connect.

Managed Objects

The ***user*** is the most fundamental entity in the CA Identity Portal application. The user entity is a representation of an organizational entity as it exists in the various IAM/IAG systems connected to CA Identity Portal.

The group entity has been introduced in CA Identity Portal 1.5 and now allows the management of group objects as well. The group entity like the user entity is a representation of an organizational entity as it exists in the various IAM/IAG systems connected to CA Identity Portal.

CA Identity Portal does not save organizational users and groups' information. Instead, it fetches the information from the connected systems on demand.

The representation of the CA Identity Portal user and group is defined by mapping of attributes in CA Identity Portal to attributes in the IAM/IAG systems. To configure that mapping, use the User Info and Group Info sections in the admin UI.

User Info

The user information is derived from mapping the CA Identity Portal user attributes to the IAM/IAG attributes.

You need to map all the user attributes that you intend to use in the CA Identity Portal UI configuration and in CA Identity Portal's business logic. Search attributes availability varies depending on the connector from which the attributes are being fetched.

For example:

If a CA IM type connector exists in the system, the “First Name” attribute of the CA Identity Portal user can be connected to the %FIRST_NAME% attribute in the CA IM connector. This means that once a user entity is used in CA Identity Portal, the First Name will be fetched from the %FIRST_NAME% attribute of the CA IM connector from. The CA IM service task that is used to fetch attributes is configured in the connector as the ***Default search task*** parameter. The default service task is SigmaViewUser. The user attributes are fetched from the search screen of this service task and not from the profile screen. If you’d like to search on this user attribute in CA Identity Portal you also need to make this attribute searchable in the IM search screen.

Configuring User Info

- Switch to the Managed Objects → User Info tab. The configured attributes will be displayed.
- To create a new attribute, click the ***New*** button. For each attribute you’ll need to supply a name for that attribute (the CA Identity Portal attribute name), select the connector (from the list of system defined connectors) from which to fetch the information, and select the attribute in the connector to map the attribute to.
- If the attribute is configured is searchable in the connected system then CA Identity Portal will allow you to check the box and make the attribute “Searchable” in CA Identity Portal as well. Refer to User Search for additional information.
- Click ***Save*** to commit the changes made.

In order to change the existing configuration, simply modify the attributes displayed on the screen and save.

Note: For additional attributes in the user info you must first expose those attributes in the connected task on the endpoint then restart that connector.

User Search

CA Identity Portal allows searching for users in the CA Identity Portal system. This option is available in various modules such as:

- Searching for a user to request access for.
- Searching for another user when filling a form.
- Searching for a similar user in order to compare entitlements.

The CA Identity Portal search is a free text search. The search will look in a set of defined attributes for the keyword(s) entered by the user. To define these attributes check the “Searchable” checkbox next to the attribute in the User Info tab.

Group Info

The group information is derived from mapping the CA Identity Portal group attributes to the IAM/IAG attributes.

Group information is optional and need to be configured only if group objects are managed in CA Identity Portal.

You need to map all the group attributes that you intend to use in the CA Identity Portal UI configuration and in CA Identity Portal's business logic.

For example:

If a CA IM type connector exists in the system, the “Group Name” attribute of the CA Identity Portal group can be connected to the %GROUP_NAME% attribute in the CA IM connector. This means that once a group entity is used in CA Identity Portal, the Group Name will be fetched from the % GROUP_NAME% attribute of the CA IM connector from. The CA IM service task that is used to fetch attributes is configured in the connector as the ***Group search task*** parameter. The default service task is SigmaViewGroup. The group attributes are fetched from the search screen of this service task and not from the profile screen. If you’d like to search on this group attribute in CA Identity Portal you also need to make this attribute searchable in the IM search screen.

Configuring Group Info

1. Switch to the Managed Objects → Group Info tab.

   The configured attributes appear.

2. To create a new attribute, click the ***New*** button. For each attribute you’ll need to supply a name for that attribute (the CA Identity Portal attribute name), select the connector (from the list of system defined connectors) from which to fetch the information, and select the attribute in the connector to map the attribute to.

3. If the attribute is configured is searchable in the connected system then CA Identity Portal will allow you to check the box and make the attribute “Searchable” in CA Identity Portal as well.

4. Click ***Save*** to commit the changes made.

In order to change the existing configuration, simply modify the attributes displayed on the screen and save.

Note: For additional attributes in the group info you must first expose those attributes in the connected task on the endpoint then restart that connector.

GUI Configuration

The GUI Configuration tab allows you to define the information displayed in various places throughout the CA Identity Portal application. The following is configurable:

- The presentation of user information in various places in the application. For example: display the “First Name” and “Last Name” in the search results of the Access Rights search.
- The messages displayed to users in case no items are available. For example: in the Tasks module, if no pending approvals are awaiting, the user can be prompted with a configured message such as “No pending approval, have a nice day”
- Implementation specific information, such as:
  - System unique identifiers – used to instruct users to search bulk files.
  - Predefined search – For example, how to search for the user’s (organizational) subordinates.

GUI Configuration

Switch to the GUI Configuration tab.

Configure each of the parameters as desired or click ***Use default*** for CA Identity Portal to set the parameter to its default configuration. For first time use a ***Reset to default*** button is available at the bottom of the screen, this will reset all parameters to CA Identity Portal defaults.

The configurable parameters are displayed on the screen. The available User attributes are listed to the right under ***User Info***. By hovering over each of the fields the application context, which this parameter refers to, will be displayed.

To simplify the configuration you can type the “{“ key and the system will display the available user attributes that are defined in the system.

To save the GUI configuration click ***Save***.

Note: In case you supplied a user attribute which is not defined, the system will display it in the list on the right under ***Not configured.*** In addition, you’ll be promoted with a message of undefined attributes in the user Info tab.

User Related

Search_result - – When clicking on access -> User search -> Searching for a user. The upper part of each search result will be the parameters configured in this attribute.

Search_result_bottom – When clicking on access -> User search -> Searching for a user. The bottom part of each search result will be the parameters configured in this attribute.

Approval_details – In tasks -> approval or implementation table the requester display attributes.

Approval_table - In tasks -> approval or implementation table the target user display attributes.

User_selector_displayname – when using a user selector prop, after the user is selected, the display name that displayed on the form.

Dashboard_approvals – the approvals target user display name in the dashboard view.

User_dialog_info1/2/3– these attributes control the display of the user in multiple places:

- In access -> search a user -> hover on a user from the search result, when clicking on the more info link a user tooltip will be displayed, these parameters control that.
- In User selector prop -> when selecting a user from the results, the user details will be displayed on the right.
- On My requests and approval timeline when hovering on a user -> a tooltip with the user details will be displayed.

approval_details_requester – in tasks/implementation, in the middle pane the requester information.

User_displayname – the default parameter to control what to display when showing a user. Used in:

- Hello message in the upper dashboard
- When displaying the user in the access rights (after selecting the user to request access for).
- Right panel display when selecting multiple users in access search
- The selected user in the similar user table in the top of the middle pane
- Display of the user in the risk summery dialog
- Display of the users in the bulk dialog in approvals.

no_current – message to be displayed in access rights module when user has no current permissions

no_campaigns – message to be displayed in campaigns view when there are no campaigns.

No_requests – message to be displayed to the user when there are no requests.

No_implementation – message to be displayed to the user when he has no implementation pending.

No_penders – in dashboard when clicking on request in the right pane, if the request is not pending to anyone, this message will be displayed.

Namedquery_<subordinates> - defined the predefined search that is performed when the user enters the access search. Structure should be <logged_in_user_attribute>,<attribute to search in>. So for example if we define UserId,Manager then it will search the userId at all users Manager attribute which will return all the user subordinates.

Risk_max_level – the max value to be displayed in the risk meter.

Similar_user_table – in access view, click add systems, switch to similar user view, the search results will be displayed in a table defined in this parameter.

Users_info_table – in modules that are defined to be operate on object type USER. When searching for a user a more info link will be displayed on each search result, when hovering on that link a tooltip with this configuration will be displayed ONLY if nothing is configured in the more info configuration in the module configuration.

Strict_cart_mode – This parameter controls the behavior of the cart in the access rights module.

Note: Other attributes might appear in admin UI configuration. These attributes are deprecated and are saved for backward compatibility.

Group Related

group_displayname – the default display of the group object.

approval_table – the display in the tasks approval/implementation table in a case the approval is for a group object.

approval_details – the display of the target object in the middle pane in the tasks if the approval is for a group object.

group_info_table – in modules that are defined to be operate on object type GROUP. When searching for a group a more info link will be displayed on each search result, when hovering on that link a tooltip with this configuration will be displayed ONLY if nothing is configured in the more info configuration in the module configuration.

Access Catalog

When an identity management solution grows, organizing the structure of the entitlements becomes a challenge. To address that process, a flexible structure needs to be deployed, which will enable users to quickly and easily locate the entitlements they need.

The CA Identity Portal Permission Model consists of the following entities:

- Application groups
- Applications
- Permissions
- Role Groups
- Roles

Permission Tree

The basic entity is the permission entity. A permission is the business representation of the entitlement the user requests. Once permission is requested, CA Identity Portal translates this business representation to the technical entitlements – the target permissions (refer to Target Permissions section for more information on creating target permissions).

The following rules define the permission model:

- A permission can be linked to many target permissions. Example: The permission “Internet Access” can consist of several technical entitlements, such as DMZ access, Soft Token account and corporate LAN access.
- A target permission can be linked to many permissions. Example: Active Directory Group membership, which can be a provisioning role in an IM solution and can be linked to several business permissions such as Network Access, Security Admins etc.

- Permission can be linked under another permission. In this case the permission will have a parent-child relationship. This relationship will ensure that a child permission cannot be granted without requesting/having the parent permission. This situation is common in profile-based applications. The basic access to the application is defined as the parent permission, while the specific profile/role in the application is defined as child permissions or sub-permissions. This behavior is enforced when defining the cart to behave in strict mode (refer to strict_mode in GUI configuration).
- Every permission must be linked to an application. A permission cannot be linked to more than one application.
- Application can contain multiple permissions.
- A group of applications contains one or more applications.
- There is no limit to the number of son permissions nesting in the permission model. In essence every son permission of a permission can have its own son permission and so on.
- Permission can be grouped in a group of permissions. Grouping permissions together means they are mutually exclusive (only one can be selected during access request).

Managing the permissions model

CA Identity Portal allows the administrator to draw the permission model in the way it will be presented to user.

- Switch to Permissions Tree in the Access Catalog tab.
- The left panel contains the Group of Applications and Applications.
- To create a new group of applications click ***Create Group***. A new group will be displayed. Double-click it to rename.
- To create an application under the group of application, select the group and click ***Create Application***.
- To create permission, select the application in the left panel and click ***Create Permission*** in the middle panel.
- To create a group of permission click the application and click ***Create Group*** in the middle panel.
- To add permissions to a group click and select the group name to add a permission under it.
- To create nested permissions, either create a permission while selecting the parent permission, or create the permission and drag and drop it under the parent permission.
- Click ***Save*** to commit these changes (unsaved changes will be displayed in red).

Connecting Permission to Target Permission

- Switch to Permissions Tree in the Access Catalog tab.
- Select the permission you wish to connect.
- Once a permission is selected the right panel will display the list of available target permission in the system (refer to Target Permissions section for more information on creating target permissions). Check the target permission you wish to connect the permission to.
- Click ***Save*** to commit these changes.

Configuring Entity Properties

CA Identity Portal enables administrators to enrich the permission tree with additional information in order to provide end-users more information about the permissions. This is used to help end-users finding the correct entitlement they wish. The information will be displayed with a small Info icon next to the entity.

To configure this additional information:

- Select the permission and click the Properties tab in the right panel.
- Enter property key and value, for example: Key=Description, Value=This permission requires a security administrator to approve.
- Click ***Save*** to commit these changes.

Roles

A CA Identity Portal role is a group of permissions which defines an organizational role.

CA Identity Portal roles are suggestive roles that will be displayed to the end user during access request → add systems → by role.

A group of roles contain one or more roles.

Managing the roles model

The roles model tree is managed in a very similar way to the permissions model.

- Switch to Roles in the Access Catalog tab.
- The left panel contains the Group of Roles and Roles.
- To create a new group of roles click ***Create Group***. A new group will be displayed. Double-click it to rename.
- To create a role under the group of roles, select the group and click ***Create Role***.
- Click ***Save*** to commit these changes (unsaved changes will be displayed in red).

Connecting roles to permissions

- Switch to Roles in the Access Catalog tab.
- Select the role you wish to connect.
- Once a role is selected the right panel will display the list of available permissions from the permission tree (refer to Permission Tree section for more information on creating permissions). Check the box next to the permissions you wish to connect to the role.
- Click ***Save*** to commit these changes.

Backend Management

This section covers the basic components of CA Identity Portal that have a direct link to its connectors.

In CA Identity Manager for example the core components are: attributes, screens, tasks, groups and provisioning roles. CA Identity Portal triggers, assigns and sets those components and in the backend management the administrator can configure the representation of those objects in CA Identity Portal.

The backend management objects should be configured in the following order as they are referencing each other:

1. Tasks (CA Identity Portal tasks link to connector tasks)
2. Forms (CA Identity Portal forms link to CA Identity Portal tasks)
3. Target Permissions (CA Identity Portal Target Permissions link to CA Identity Portal Forms)

Note: Target Permissions are only required to be configured for access requests and not for other modules (such as onboarding and registration)

Tasks

In essence, tasks are IAM/IAG procedures, accessible through the connector's API. Each connector interacts with an external system using a public API. The API procedures are the way to execute business logic in that system. CA Identity Portal defines the tasks as the repository of API calls that can be used in order to define the business logic. The task name will define the API function that needs to be triggered.

When building the implementation the administrator needs to define the various API procedures, which must to be defined in CA Identity Portal in order to request various target permissions or perform other actions in the system.

Configuring Tasks

- Switch to the Backend Management → Tasks Tab. The configured Tasks will be displayed.
- Click ***New*** to add a new task.
- Select the ***Connector*** which is associated with the target permission. The exposed tasks for that connection will be available in the ***Name*** parameter.

Note: In order for a CA IM task to be available for CA Identity Portal it needs to be exposed to TEWS (Web Service). Refer to CA IM bookshelf for additional information on exposing tasks to TEWS.

- To select a task start typing in the name of the task tag as it is configured on the selected connector endpoint.

Note: If this task is intended to be triggered in bulk it will need to be a bulk loader task in the connector endpoint.

- Upon selection the tag will be auto populated.
- Description is optional but is recommended to use in order to identify what the tasks functionality is.
- Complete the task configuration
- **additionOperation/removalOperation** – for details see Assigning a target permission.
    - Select ***directChange*** to use a direct action (CA Identity Portal will perform the assignment/removal of the permission).

Note: When using directChange in a task to assign a target Permission of type Provisioning role or Group, the provisioning role/Group tab cannot be configured to manage administrators. To remove administrators' management in a tab, click the tab edit button and uncheck "manage administrators" and uncheck "display administrators" option.

    - Select ***execute Task*** for indirect action (CA Identity Portal will trigger a task that will be responsible for the assignment/removal of the permission).

Refer to *Target Permission* for more information.

- **IsBulkTask**: select true if the task is a bulk task.

Note: If a task is configured to be a bulk task it can still be used for single users but it will always run in the backend it will run in bulk mode.

- **BulkConf** – defines the configuration used to create the bulk file to be executed. This configuration holds the mappings between the actions and the task names to be executed in the IM Connector so that CA Identity Portal can build the correct bulk load file. BulkConf requires:
- **Action name** – the name of the action that will be set in the bulk loader file (for example: add_role). Important: start this parameter with a lower case.
- **Task name** – the name of the task that IM will trigger for the above action (for example: Modify User).
- **Operations** – Select the target permission and the action allowed for it (Add, Modify or Delete).
- **Mappings** – type in any additional attributes you would like to send in the bulk loader file. First parameter is the attribute in the triggered task that will accept the attribute and the second parameter

is the value to be sent. Use well known values or physical values in this field.
Second Parameter is the value that can be one of the following options:

- Static value - for example “IT”.
- Form Attribute value – a value that is fetched from one of the request forms, use the “{“ to encapsulate the attribute such as “{Department}” for fetching the value from the Department form attribute.
- Target Permission value – use one of the following: {{TP_NAME}} for target permission name, {{TP_VALUE}} for target permission value, {{TP_TYPE}} for target permission type.

Note: BulkConf are applicable to bulk tasks only (if **IsBulkTask** is set to true).

- Click ***Save*** to finish the configuration.

Understanding Bulk Configuration

A bulk request can be submitted in two different ways, either by selecting access module and searching for users and selecting more than one user or by using the bulk file to select users. Both of these methods will cause the user to enter the access rights module in a bulk mode.

After the user completes the add/modify/remove permissions to his cart and fill the necessary form information associated with these permissions, he can proceed to submit the request.

In case one (or more) of the permissions are linked to a task which is defined as bulk, a bulk file will be generated using the bulk configuration in the task.

Bulk configuration works as following:

1. Each target permission and action (Add/Remove/Modify) that exist in the cart will be searched in the BulkConf configuration.
2. For each match found, a line in the bulk file will be created for each user in the request. The line will contains the following information:
    a. The action name – the corresponding action the user and attributes to be set in the task.
    b. The userId – a line per action per user in the request.
    c. Action Mappings – these are the attributes that will be passed to the executed task the first parameter is the attribute name and the second parameter is the value. As mentioned above the value can be fetched either from one of the forms in request, either be static value or it could be the name/value/type of the target permission that triggered this action.

Example – ACCESS REQUEST

This is a snapshot of an existing configuration

1. *Permission A* is linked to *Target Permission A*.
   Target Permission A has only one rule and in its rule an Add Form is mapped to *Form A*.
   Form A has no attributes and is linked to task called *BulkTask.*
2. *Permission B* is linked to *Target Permission B*.
   Target Permission B has only one rule and in its rule an Add Form is mapped to *Form B*.
   Form B has one attribute in it and it mapped to backend screen attribute called *ScreenAttributeB* through a task called *BulkTask.*
3. *Permission A* is linked to *Target Permission A*.
   Target Permission A has only one rule and in its rule an Modify Form is mapped to *Form C*.
   Form C has no attributes and is linked to task called *BulkTask.*

Since the two permissions are linked to the same bulk task, they will only trigger this task once.

Let's assume this is the *BulkTask* bulkconf configuration:

#	Action Name	Task	Operation		Mappings	
			Target Permission	Action	Key	Value
1	add_tp1	Assign Target Permission A to user	Target Permission A	ADD	Department	IT
2	modify_tp	modify User	Target Permission A	MODIFY	%END_DATE%	{ScreenAttributeB}
3	add_tp2	Generic assign Role task	Target Permission B	ADD	%ROLE%	{{TP_NAME}}

In case a user logs in and request access for *userA and userB* and in the access request he selects to add *Permission A* and add *Permission B.* the bulk file will look as follows:

action,%USER_ID%,Department,%ROLE%

add_tp1,userA,IT,

add_tp1,userB,IT,

add_tp2,userA,,Target Permission B

add_tp2,userB,,Target Permission B

If a user logs in and requests access for *userC* and *userD* and in the access request he selects to modify *permission A* and in the form he enters the value "12/31/2014" and also selects to add *permission B* the bulk file will looks as follows:

action,%USER_ID%,%END_DATE%,%ROLE%

modify_tp,userC,12/31/2014,

modify_tp,userD,12/31/2014,

add_tp2,userC,,Target Permission B

add_tp2,userD,,Target Permission B

HOW TO CONFIGURE BULK ONBOARDING

In order to perform bulk onboarding, perform the following configuration:

1. Create a task in CA Identity Portal and map it to a bulk loader task.
2. Configure the bulfconf with only action name and task name. For example:
    a. Action name: create_user
    b. Task Name: Create User
3. Create a form mapped to the task above. In the form create one prop of type “CSV” and map it to a backend Name called “FileContent” (Note: this prop should not be available in a list, you’ll need to type it yourself).
4. You can configure on the CSV prop the mandatory header fields this file should have, for example in bulk onboarding you might want to put: action, %USER_ID%, %FIRST_NAME%, %LAST_NAME%, %FULL_NAME% this will make sure that when the user loads the file it gets validated that it has all of these fields.
5. Create a new Module (or use and existing one) of type Create, and map this form to a new create action.
6. Make sure the bulk task is in scope for your requester.

For the above configuration the following file could be used if the user uploads:

action,%USER_ID%,%FIRST_NAME%,%LAST_NAME%,%FULL_NAME%
create_user,John.S,John,Smith,John Smith
create_user,Kim.L,Kim,Larry,Kim Larry

Forms

CA Identity Portal Forms contain attributes which map from CA Identity Portal to the executed task. For example: if the task is of the CA IM type, each property will be a representation of a field in the IM task that you want to display in the access request screen of CA Identity Portal or a module action.

Forms are what the end user sees when they either select an action or an access request type (add/modify/remove), they can either contain various types of data or remain empty so they just trigger tasks.

CA Identity Portal Forms must be linked to a CA Identity Portal task for the following reasons:

- The form will eventually trigger that task on the selected connector.
- The form can display data and allow the user to edit data, that data is retrieved and set using the linked task.

Once a form is created it can be used in the following ways:

- Linked to module actions. For example: a “create contractor” form which is linked to a “create user” task can be linked to an onboarding module.
  Refer to Modules section for more information on linking forms to module actions.
- Linked to target permissions rules. For example: an “add permission X” form which is linked to an “assign permission” task can be linked to the Add action of the target permission’s rule. Refer to Configuring Target Permissions section for more information on linking forms to target permissions.

Configuring Forms

1. Switch to the Backend Management → Forms Tab. The configured Forms will be displayed.
2. Click ***New*** to add a new form.
3. Enter ***Form Name*** which is a descriptive name of the form and will be used as a reference from other locations in CA Identity Portal.
4. ***Form Tag*** will be auto populated based on the name and can be modified.
5. Select the ***Task*** which will be associated with the form. The selected task will control:
   - The fields that can be displayed on this form. For example in IM the available fields are retrieved from the profile screen in the IM linked admin task.
   - The backend task that will be triggered once this form is submitted in CA Identity Portal. For example in IM if the linked task is the “Modify User” task then it will be triggered with all the workflows, PXs and other backend operations defined on it.
6. Add properties and tabs as needed (refer to Configuring Form Properties for more information).
7. Click ***Save*** to finish the configuration.

Note: CA Identity Portal’s form generator offers a preview that gets updated in real time while editing the form, including results of handler scripts when available.

Configuring Form Properties

Form properties are mapped to attributes on the profile screens of the linked task to this form.

Managing form properties and tabs:

1. Click ***Add Prop*** to add a new property.
2. Click the X on the right side of the form property to delete an existing property.
3. Click anywhere on the property header to edit an existing property.
4. Click the three lines symbol on the left side of the form property to drag an existing property and drop anywhere on the form to change its order.
5. For properties can only be organized vertically.
6. Form properties can be organized in tabs.
7. Click ***Add tab*** to add a new tab.
8. Double click a tab name to edit its name.
9. Click the X on the right side of the form tab to delete a tab.

Form Property Options

- **Property Name** is also its label and is defined in the header line of a property. When first created the property is unnamed yet a name is mandatory.
- **Property Type** – defines the behavior and display of the property. Options in this type include: text, checkbox, radio buttons, drop down list, single select list, multi select list, CSV, File Attachment, Date Picker, user selector etc.
- **Server Type** – used to define the logic of the property. String is the default behavior, which means the selected value will be passed as is. Different types include: File (used for attachments), List, Date etc.
    - **Hidden** is a special Server Type, if Hidden is selected another parameter called “Type” becomes available.
    - The available types are: User IDs (value of the user id's associated with the request), Sigma Payload (value of the content of the request), Request ID and Custom.
    - Each selection populates a default value for it. When Custom is selected the default value is left for the administrator to configure.
- **Options** – next to server type there are some options the administrator can select if this is a mandatory, hidden, or a read-only property.
- **Target Name** – name of the property on the endpoint into which to pass this information or read information from.
- **Default Value** – enter default values for this property.
- **Reference** – give the parameter a reference name in order to access is from scripts on the form (optional).

Note: Each property type has its own additional options and configurations to perform. For example: drop downs have an options list, date pickers have a date format to enter etc.

Form Handlers

Each property configured in the form has three types of handlers available. Those handlers allow the administrator to write Javascripts that will be triggered depending on the type of handler. For handler scripts can be used to trigger service actions (refer to Service Actions for more information) or plugins (refer to Plugins for more information).

The available handler types are:

- Change Handler – trigger at any change happening to the property in run time. For example when a user types in text in a text box or when a user uploads a file to a file attachment property.
- Validate Handler – trigger at the at the submission of a form
- Initialization Handler – trigger on load of the property in the form. For example when a user opens a form a drop down can be populated by dynamic data at initialization of the property.

In a handler script for a specific property you can refer to other properties in the form by configuring a "Reference" parameter for them and using it in the script.

Refer to CA Identity Portal developers guide for more information on form handlers and scripts. Also refer to Form Handler Examples for some sample usage of form handlers.

Form Handler Examples

- Change Handler – in this example we set the full name of a user based on the first and last names as they are entered by the user. This is the Change Handler script of the first name property and in it the last name property is read then if not null it is concatenated with the current property and set in the full name property. The access to other properties is done by calling their Reference parameter in the following way: api.getProp("<ref name of a prop>"). The last name property has a similar script in it and it has a reference set to be "lastName".

```
function onChange(api, prop) {
var last = api.getProp("lastName").value;
if (last == null) {
    last = "";
}
api.getProp("fullName").value = prop.value + " " + last;
}
```

- Validate Handler – in this example a regular expression is used to validate the name of the object provided by the user. Standard Javascript RegEx functions are used to define the regular expression and test it. The CA Identity Portal elements to note in this script are the usage of the prop variable that holds the information of the prop being validated. In this script the prop.value is being tested. In order to display the error message to the user the prop.error is being used. Note the Validate function must have a return value of true or false.

```
function validate (api, prop) {
var ptn = /^[-\s&\(\)A-Za-z0-9]+$/;
if (true === ptn.test(prop.value)) {
    return true;
}
prop.error = "Invalid object name: " + prop.value;
return false;
}
```

- Initialization Handler – in this example plugin is being used to fetch data that will be used to initialize a drop down property. The call to get the data from the plugin is: api.server(['<plugin name>']). This

specific prop is a drop down so it has options name and value. The script if using a forEach loop to push the name and value to the drop down options.

```
function initialize (api, prop) {
api.server(['initAppList']).then(
    function(success) {
        success.returnValue.forEach(function(entry) {
            prop.options.push({“name”:entry,”value”:entry})
            });
        }, function(error) {
            });
}
```

Target Permissions

The target permissions are the corner stones on which the CA Identity Portal permission model is constructed. It is the technical permission that the user requests, over-layered and simplified by the CA Identity Portal permission model.

A Target Permission is the entitlement representation in the systems (i.e. IM, IG) that are connected to CA Identity Portal. Use target permission either for fetching the entitlements the user currently has, or for granting new entitlements to the user. The supported entitlements are:

- Provisioning Role (IM)
- Group Membership (IM)
- Attribute (IM)
- Role (IG)
- Resource (IG)

When designing a CA Identity Portal setup and implementation, one needs to plan and configure the relevant target permissions as detailed below.

Assigning a target permission

Target permissions can be assigned in 2 ways:

- Directly through the native implementation of the connector:
  - **IG** – Through the API native method.
  - **IM** – triggering the corresponding event (similar to assigning a provisioning role in the Provisioning Roles tab)
- Indirectly through a dedicated API.
  - **IM** – through executing a task which will be responsible to assigning that task.

Configuring Target Permissions

1. Switch to the Target Permission Tab. The configured target permissions will be displayed.
2. Click ***New*** to add new target permission.
3. Select the ***Connector*** which is associated with the target permission. The relevant target permissions for that connection will be available in the ***Name*** parameter.
4. To select a target permission start typing in the name of the target permission as it is configured on the selected connector endpoint.
5. Upon selection, the ***Type*** of the target permission will be automatically indicated and the tag will be auto populated.

Note: If a target permission is of attribute type, a value needs to be supplied.

6. Set the required compliance settings (optional). Refer to Compliance for more information.
7. Set the required rules for this target permission. Refer to Target Permission Rules for more information.
8. Click ***Save*** to finish the configuration.

Target permission Rules

Target permissions rules define a few things:

- The type of access request that can be performed on permissions. The options are: Add, Modify and Remove.
- The form that will be displayed for the end user when clicking on Add, Modify or Remove.

Note: Forms are linked to a task, which means the selected form both controls the screen that the user will see and also the backend task/workflow that will be triggered.

- The scenario in which the configured options and forms will be displayed. Meaning multiple rules can be configured for the same target permission. For example: one rule that applies to all users from a specific department and they are allowed to request for add or remove with a specific form and with manager approval. Second rule that applies to all managers and they are allowed to request for add only with a specific form that does not require approval.

Note: Target permissions must have rules configured in order to be displayed to the end user.

Target permission Rules Example

Example: A manager can add and remove “Network access” permissions for his employee using the “Add Network Access by manager” and “Remove Network access by manager” tasks respectively. His employee can request to add the Network Access permission using the “Request your manager network access” task.

To implement this logic two rules have to be defined on the target permission which provides the network access.

Rule 1 – Manager acting on his employee. For this rule, the relationship between the requester (manager) and the target user (the employee) has to be defined. Usually these relationships are defined by an attribute in the subordinate's user profile indicating the manager. The resulting rule will look like this: *"user.getValue(“Manager”) = requester.getValue("userId”)* should be created.

Once the population of the rule is configured, the next step is to define which task to execute when the Add/Modify/Delete actions are selected. In this example the “Add Network Access by manager” task will be linked to the ***Add*** action, and “Remove Network access by manager” will be linked on the ***Remove*** action.

Rule 2 – Every employee can request the permission for himself. This is useful when the executed task is configured with a workflow, requiring an approval of a supervisor. To configure this rule define an expression which identifies the employee such as Requester[‘User Type’] = ‘Employee’. Then configure the ***Add*** operation with the “Request your manager network access” task.

Configuring Rules

1. Switch to the Backend Management → Target Permissions Tab. Click a target permission to edit it.
2. Click ***Add Rule*** to add new rule for the selected target permission.
3. Give the rule a descriptive name.
4. Provide a priority for the evaluation of this rule (lower number has a higher priority).
5. Select the mode for this rule. Available modes are:
    - **Access Rights** – the selected forms will be displayed during access rights request for a single user
    - **Bulk Access Rights** – the selected forms will be displayed during access rights request for multiple users (either multi-select or bulk upload)
    - **Onboarding Access Rights** – the selected forms will be displayed during access rights request for a single user which happens during onboarding request.
    - **Bulk Onboarding Access Rights** – the selected forms will be displayed during access rights request for multiple users which happens during onboarding request.

6. Click Edit Expression to select the condition for which this rule will apply. The options are:
   - **True** – this rule will apply to all users (requesters and subjects of a request).
   - **Use Wizard** – this rule will apply to the users matching the condition defined using the wizard. For example: users from a specific department, managers of users etc.
   - **Custom** – this rule will apply to the users matching the condition defined using a custom JavaScript. For example: manager of a user
     `user.getValue("Manager").equals(requester.getValue("userId"))`

     Refer to the CA Identity Portal Developer Guide for more information about building complex customer expressions
7. Select a form for each one of the actions that need to be available to the end user in this specific rule scenario. Only actions that have a form applied to them will be displayed in the access request. Not all actions need to be linked to forms. For example some scenarios might only require the Add action for permission.

Compliance

We use the compliance configuration to indicate which target permission should be used when evaluating compliance for the subject target permission. In some cases the target permission itself does not reside in the system which evaluates the compliance check, but a representation of it exist and should be used instead. For example: when using a target permission which is a provisioning role in CA Identity Manager, but we would like to perform a compliance check when requesting that provisioning role (the permission that is linked to that provisioning role) using the IG role that was created using the CA Identity Manager and CA Identity Governance integration.

To perform that configuration we would need a connector to IDM and a connector to IG. We would then configure a target permission from the IM connector and another target permission (with the same name) that exist in IG. Then we would configure the compliance on the IM connector to point to the IG target permission.

For the compliance evolution to be executed we would need to define an external condition in a risk. *Refer to Risks section for more information.*

Modules

Modules are used to enable users' request activities which are not related to access requests (entitlements assignment). Activities of this type may include:

1. Profile changes – changing an object's name and attributes (such as: user name, user's manager, group name etc.)
2. Onboarding entities – used usually to onboard users, create groups.
3. Service actions – used to fetch information from an IAM/IAG systems for enriching form capabilities.
4. Execute generic requests – these are usually requests that are used to trigger a business process flow.

Modules names and objects are flexible and therefore they are referred to as Dynamic Modules.

Note: CA Identity Portal's pre 1.5 versions had onboarding and user management features which have been deprecated in version 1.5. Instead those features are optional and configurable as Dynamic Modules.

Creating a Module

1. Switch to the Modules tab
2. Click the ***New Module*** button.
3. Enter the following parameters:
    a. General
        i. Name – the new module descriptive name as it will appear at the top navigation bar for the end user. Tag is automatically populated based on the name and be modified.
        ii. Template – select the type of module to be created. Once a template is selected, other tabs become available in the configuration of a module with parameters specific for that module template. The following module templates are available:
            1. Create Only – only expose create actions to the end user without going through search screen to search for the object. For example: Onboarding.
            2. Manage Only – only expose management actions to the end user which requires going through search screen to search for the object first. For example: User Management.
            3. Create and Manage – expose both create and management actions to the end user. This will require search for the object for the manage actions or clicking the ***Create New*** button for the create actions. For example: Vendor Management
            4. Multi Onboard (Bulk and Single)
            5. Registration
        iii. Object Type – select the type of object that will be the subject of requests in this module. The available object types are:

1. USER
2. GROUP

b. **Template Info** – template specific information, the options may change between the different templates.

   i. Allow user to save draft – even if the draft feature is turned on in the profile management you can still control the draft option per module.

   ii. Header – the module header that will appear within the module once a module is selected.

   iii. Search text box place holder – text to be displayed within the search box. This is only applicable for templates that include object management (such as "Manage Only").

   iv. Enable "Continue to Access Rights" – allow the requester to continue to access request as part of the onboarding request. This feature is only applicable in the ***Multi Onboard*** template.

   v. Allow the user to submit action (without request access rights) – allow the requester to Submit an onboarding request without continuing to access request. This feature is only applicable in the ***Multi Onboard*** template.

c. **Actions** – the actions that will appear for the end user within this module

   i. Click ***Add*** to add a new action

   ii. Enter a display name as it will appear for the end user. Tag will be auto-populated and can be modified.

   iii. Category – a name to identify the category on which the task runs. For multi onboarding action this is either SINGLE or BULK which identifies to where this task will be displayed. For other templates the category is free text.

   iv. Form – select the form to be displayed for this action. The form is linked to a task so this is also the task that will be triggered upon request.

Note: When the template is for create and manage you first need to select which action is being created – "Actions for Create" or "Actions for Manage"

d. **Search** – search parameters, this tab is only applicable for templates that include object management (such as "Manage Only")

   i. **Results Text** – add text and/or User/Group info parameters that you would like to be displayed in the Upper and Lower search results.

   ii. **Search Condition** – filter the search results based on an object attribute

   iii. **More Info** – when search results are displayed each object has an option for a "More Info" tooltip. The tooltip content is configurable here based on user/group info.

e. **Landing page icon** – new modules will automatically appear in the top navigation bar but by default they do not have a landing page icon. Select a landing page icon if you'd like this module to be available from the home page.

4. Click ***Save*** to commit.

Note: In order for a new module to be visible to user it needs to be added to at least one profile. Refer to Profiles section for additional information.

Service Actions

Service actions can be referred to as internal service tasks in CA Identity Portal. They are configured almost the same way as module actions are configured but they are not visible to end users. Instead they are referred to from scripts within other forms and are mainly used to retrieve data using service tasks on the connectors. For example: on the CA IM connected system build a service task that calculates and returns information then link it to a service action and call it from a script on one of the forms.

Configuring Service Actions

Before configuring a service action, the task and form need to be configured so they can be linked to the service action.

1. Switch to the Modules tab
2. Click ***Manage Service Action*** button, the existing Service Actions are displayed
3. Click ***Add***
4. Enter the required parameters:
   4.1. Display Name, Tag is auto populated based on the display name
   4.2. Category is optional
   4.3. Select the managed object type for the task (user, group or none)
   4.4. Select the form that is linked to the service task
5. Click ***Save***

Risks

CA Identity Portal provides a real-time context-based RISK ANALYZER & SIMULATOR. It's based on an advanced, robust rules engine that calculates user risk score in real time.

It offers an easy-to-use, configurable user-centric Risk Model that identifies areas of risk within the organization caused by users with high risk scores. It also enables organizations to strategically prioritize security and compliance activities to focus proactive controls on the areas of higher risk, as follows:

1. Calculates and displays users' risk scores and Alerts whenever it detects a risky user
2. Updates risk scores continually based on changes to user access privileges, user attributes and other relevant compensating factors

3. Simulates in real time the user's risk score changes in the context of access requests, including permissions requested in the cart
4. Implements three levels of preventive controls across IAM processes, based on risk and violation types and levels, when high-risk users or violating transactions are detected:
    - First level - Informative – alert on violation
    - Second level – collect justification from the user in order to continue request
    - Third level – prevent the user from continuing with his action
5. Displays violations (and justifications) to approver to support approver's decision
6. Audits violations and tracks them throughout the end-to-end process

Enabling Risks

In order to start using risks it first needs to be enabled in CA Identity Portal:

1. Go to ***General*** tab
2. Check the box for ***Enable Risk*** to enable it or uncheck to disable it
3. Click ***Save***

The maximum risk level is configured as part of the GUI configurations:

1. Go to ***GUI Configuration*** tab
2. Set the parameter "**risk_max_level**" (default is 1000)
3. Click ***Save***

Configuring Risks

1. Go to ***Risks*** tab
2. Existing risks are displayed and can be edited/deleted
3. Click Configure New Risk
4. Define base parameters for the risk
    a. Name – logical name of the risk
    b. Tag is automatically filled out based on the name
    c. Score – define the risk score for this risk (take into consideration the maximum risk level defined in the GUI configuration)
    d. Risk Behavior – define the behavior of CA Identity Portal when a risk is identified. There are three different types of available behaviors:
        i. Informative – a notification will be displayed for the user but he will be allowed to continue with the request
        ii. Requires justification – a notification will be displayed for the and if he wants to continue with the request he will be required to enter a justification for the request

iii. Enforcive – a notification will be displayed and the user will not be allowed to continue with the request

e. Message – the message that will be displayed for the user when the risk is identified

5. Define the conditions(s) for the risk

a. Select if all of the rules or any of the rules bellow must apply for the risk to be identified

b. To add another rule click ***Add Condition***

c. Select the parameter to evaluate for the rule, based on the parameter the rule configuration changes

d. Group – Use group to define another layer of nesting in the condition. For example (GROUP: Condition A AND Condition B) OR Condition C.

e. User's permissions

i. Select the condition for the permissions

ii. Select the permissions

f. User's attribute

i. Select the attribute

ii. Select the condition for the attribute

iii. Enter a string for the condition

g. Violations from external source

i. When using this type of condition CA Identity Portal will transform the permissions in the cart, to the target permissions that they are linked, then transform them to a list of compliance target permissions and send them to evaluation in the external systems.

ii. The external systems are all systems that are able to perform compliance check that CA Identity Portal has connector to (i.e. CA Identity Governance).

iii. These systems will return violation if they exist.

iv. This rule will then filter the violations according to the definition in the condition filter. For example if we defined to only show violations that are related to Permission X, all violation that do not include Permission X will be discarded.

v. If "include violations with external entitlements" is checked then violation that include items that CA Identity Portal is not familiar with (not mapped as target permission) will not be ignored.

vi. Only violations that are related to permissions in the Cart will be used.

vii. If a violation is fetched it will be displayed under this rule. So in turn, the user will be displayed with this risk message, and all the violations fetched from the external system underneath it.

viii. The violations fetched from external source will inherit the behavior from the risk fetching them. The score they receive is the risk that fetched them.

Tools

Cache

CA Identity Portal has multiple types of caches for various elements used to improve performance and reduce the load on the database. On regular system operation these cache should not be changed or cleared. You can use this section to clear the various caches that are used in CA Identity Portal.

Search Request

Search request tool allows the administrator to enter a CA Identity Portal request ID and get the backend details of the request including the task session ID of the connector task triggered by CA Identity Portal.

This is mainly useful for debugging purposes, for example if there was an issue during a provisioning process for a request and the administrator needs to identify which task triggered on the connector.

Searching for a request

1. Go to ***Tools*** → ***Search request*** tab
2. Enter the Request ID and click Search.
3. If exists the details of the request are displayed.
4. The “backendRequestId” holds the task session ID on the connector, select it and it will be displayed next to the search button.
5. The task session ID can now be copied and searched for in the backend system.

Export

The export tool allows the administrator to export the objects configured in CA Identity Portal to text files in JSON format. The administrator can either select to export all objects or check specific objects to be exported.

This tool is useful for backup and migration purposes. A solution can be developed in a low environment then exported so it can be imported to a higher environment.

Exporting objects

1. Go to ***Tools*** → ***Export*** tab
2. To export all available objects click ***Select All*** on the bottom left side of the screen
3. To selectively export objects select the object type on the left and then select the specific object(s) in the middle section
4. The "Export Cart" on the right shows the list of selected objects to be exported
5. Click ***Export***

Import

The import tool allows the administrator to import CA Identity Portal objects from text files in JSON format. The administrator can import files exactly as they were exported from another environment or he can modify the files or even create his own files and import them.

This tool is useful for restore and migration purposes. A solution can be developed in a low environment then exported so it can be imported to a higher environment.

This is also useful for development purposes, for example if a large amount of target permissions need to be configured you can configure just one, export it to get a good understanding of the expected format, then write some automation to generate a file with all the new target permissions. Then use the import tool to import them into the development environment.

Importing objects

1. Go to ***Tools*** → ***Import*** tab
2. Click ***Choose File*** and select a file in the correct format from your file system
3. CA Identity Portal will show the list of identified objects to be imported
4. Click ***Import***
5. If the object(s) already exist in CA Identity Portal it will display a warning message. At this stage you can either close to discard the import or click "Approve all and try again"

Notify Release

This tool is used to release notifications to CA Identity Portal from external systems that were not successful (for example if there was a network issue at the time and now the CA Identity Portal request is pending).

This is useful in the scenarios that combine onboarding and access request which require a step to notify CA Identity Portal that the first step completed and it can continue with the second one.

Note: Use this tool with extra caution so that you do not accidentally release and notify the wrong request!

Performing a Notify Release

1. Go to ***Tools → Notify Release*** tab
2. Enter the following parameters:
    a. Username - Enter username for CA Identity Portal notifications, username can be found under General tab -> IM USER
    b. Password - Enter password for CA Identity Portal notifications user
    c. Request Id - Enter the backend Request ID of the onboarding task and not the CA Identity Portal request ID. Backend request ID (task session ID) can be found using the search request tool.
    d. Request status for release – enter the expected request status after the release
    e. User Ids – Fill in user(s) id(s) separated by commas. These are the users that the access request will continue for them.
    f. File Upload – if the notification should include a file (for example with users that were created during the onboarding) then upload a file here.
3. Click ***Submit***

Profiles

CA Identity Portal Profiles define what modules and features are exposed to the user when they log into CA Identity Portal. If no profiles are defined (default settings) the user that logs in will not see any module.

It is recommended to create a default profile for all users with basic functionality exposed.

Profiles also control what type of requests can be seen under “My Requests” section. The default view is the requests that user himself submitted but additional views can be defined using Profiles which allows the user to see track requests made by other people. This is a useful administrative view for application owners, managers etc.

Configuring Profiles

1. Go to ***Profiles*** tab
2. The existing profiles are displayed, they can be edited or deleted
3. Click ***New Profile***
4. Enter the following parameters:
    a. **Name** – the profiles display name (if this profile is used for request tracking then this will be the name displayed for the user under “My Requests”)
    b. **Tag** will be auto populated based on the name
5. Members scope
    a. **Apply to all users** – this profile configuration will apply to all users in the system
    b. **Configure members rule** – this profile will apply only to the users defined in this rule
        i. Click ***Add Rule***
        ii. Select if ***All*** or ***Any*** of the rules will apply
        iii. Select the type of condition:
            1. Target Permission Condition
            2. **Group** – this will allow to define a sub group of rules
        iv. Select the condition (***Contains All*** or ***Contains***)
        v. Select the target permission(s)
6. **Features** – select the features that will be available to the users that the member scope applies for.
7. **Modules** – select the modules that will be available to the users that the member scope applies for

Note: If you create a dynamic module it will appear here on the list, In order to expose it to users you will need to identify or create the right profile and check the box for the newly created dynamic module

8. Request Tracking Scope – use this section if you want this profile to be added to the users’ “My Requests” module to allow them to view other people’s requests
    a. Click ***Add Rule***
    b. Select if All or Any of the rules will apply
    c. Select the type of condition:
        i. Object
        ii. **Group** – this will allow to define a sub group of rules
    d. Select the condition (***Contains All*** or ***Contains***)
    e. Select the type of objects in scope:
        i. Permission
        ii. Target Permission

iii. Application

iv. Module Action

f. Select the specific object(s)

Plugins

Plugins are either Java or RhinoJS (server-side JavaScript) code executed on the CA Identity Portal server that can be used to enrich the business logic configured in CA Identity Portal.

Samples usages of plugins:

1. Fetching available form prop values from external database.
2. Validating a file's content.
3. Performing complex validation logic.

Refer to the CA Identity Portal Developer Guide for more information about using Plugins.

General

General configuration attributes for CA Identity Portal's infrastructure:

1. **Enable Risk** – Is Risk feature enabled for CA Identity Portal. True/False.
2. **Enable SSO** – Is CA Single Sign On protected. True/False.

Note: Changing this parameter requires a restart to all cluster servers.

3. **FileUpload Root** – The Directory to where files will be uploaded.
4. **IM USER** – set a user name that can used by IM in external calls to CA Identity Portal (this is not an actual user in IM)
5. **IM USER Password** – set a password for the IM user to be used in external calls from IM to CA Identity Portal
6. Client Logging
    a. **Logging interval** – the interval in seconds which the client sends the logs.
    b. **Logging level** – the Log level from 1 to 4 on which the client should work.
    c. **Logging users** – the userids which require to send logging. The client will only log if his userid matches this.
7. **Logout URL** – the URL to be used when users logout of CA Identity Portal. Default CA Identity Portal page is: ../app/login.html but it can be configurable
8. **MAX Requests to Fetch** – maximum requests that CA Identity Portal will fetch when users go to My Requests or Tasks

9. **Max Upload Size** – Max size for file attachments in CA Identity Portal.

Note: Changing this parameter requires a restart to all cluster servers.

10. **Plugin Dir** – The Directory where CA Identity Portal will look for custom code plugins.
11. Risk Rule Thresholds – Reserved for future use.
12. Risk Rule Thresholds Names - Reserved for future use.
13. **SSO User ID header** – the CA Single Sign On header which contains the universeId used to authenticate to CA Identity Portal.
14. Temp file lifetime – the duration to which CA Identity Portal will saved temporary files. Temporary files are defined as file that have been uploaded in a form but not submitted.

Branding

CA Identity Portal allows for administrators to brand and change the look and feel of CA Identity Portal. There's a friendly interface in the admin UI which enables the administrator to pick elements in the CA Identity Portal page and edit their look.

To use this interface, go to the Branding section in the CA Identity Portal admin UI. Click any element on the screen and edit its properties on the right side of the screen.

You can also edit the background and the logo by uploading your own images.

Other functionalities available:

- Choose OOTB Skin which will define a predefined color scheme.
- Use custom CSS for complete control over each element in CA Identity Portal.
- Text Size
- Landin page Icons rounded corners

CA Identity Portal Additional Features

CA Identity Portal comes with some additional features that work out of the box and do not require configuration (though some can be modified/configured).

Password Management

CA Identity Portal comes out of the box with some password related tasks pre-configured. The tasks are: Forgotten Password Reset and Expired Password

Forgotten Password

In CA Identity Portal's login the end user has the option of clicking the link "Forgot password?", this will take the user through a public interface (meaning the user does not login) of challenge questions in which at the end of successful responses the user will be provided with a new temporary password. CA Identity Portal's forgotten password reset is based on the IM default configuration.

The configuration can be modified in the IM connector configuration. Refer to the Forgotten Password section for more information.

Expired Password

When a user's password expires he is required to replace it at the login screen to CA Identity Portal. As part of the CA Identity Portal Core roles and tasks there's a service task (Sigma Change My Password) that is being used by default in this scenario.

The configuration can be modified in the IM connector configuration. Refer to the Reset Password section for more information.

Drafts

CA Identity Portal allows the end user to save his request as draft before actually submitting it. This feature is available out of the box and does not require any configuration; it just needs to be included in the features of the profile.

Currently Drafts are only available in dynamic module actions and not in access requests.

Using Drafts

When Drafts is enabled for the user and module action the user will see a button called ***Draft*** as part of the request.

1. Click ***Draft***
2. Enter a name for the draft, if the name already exists you can override it
3. To return to a saved draft go to Drafts icon on the right next to the localization menu, the number of existing drafts will be noted in parenthesis. For example: Drafts (0)
4. The list of drafts will be displayed
5. A draft can be deleted or edited
6. Click a draft to open it
7. Edit the request and ***Submit***

Mobile

CA Identity Portal comes with an OOTB Mobile Web application. No configuration is required to enable and configure this mobile application.

The application can be browsed through any mobile browser and is available at <sigma_base_url>/sigma/mobile/login.html. You could also browse to the CA Identity Portal desktop application URL at <sigma_base_url>/sigma and CA Identity Portal will automatically detect that you are browsing from a mobile device and redirect you to the mobile application.

Tablet devices are directed to the mobile application. To view the full application from your tablet device, open the navigation panel and click the link directing to the Desktop site. The desktop site will be automatically adjusted to the tablet screen resolution.

The mobile web application has the following features enabled:

- Work on pending work items.
- Track Requests.
- Complete certification campaigns.
- Forgotten Password Reset
- Reset expired password.

Certification Campaigns

Unlike other CA Identity Portal features Certification Campaigns are available to end users by default without any additional configurations. All it requires is a connector to the CA Identity Governance system. Once a connector is configured and an end user has a campaign pending his attention it will be displayed in the "Tasks" section.

Supported Campaigns

CA Identity Portal supports the following campaign types:

- Users
- Roles
- Resources
- Accounts

CA Identity Portal also supports the various types of workflows including custom workflows attached to the certification process.

Certification Features

CA Identity Portal supports the following features and behaviors in a certification campaign:

- Different views of a campaign (By role, resource or user)
- Save selection
- Submit selection
- Reassign
- Add comments – this feature can be enforced on violations on campaign definition.
- Select all – this feature can be controlled on the campaign definition.
- Display violations
- Display entity attributes including link attributes
- Display task history (if task was reassigned).
- Previous decisions – this is an internal CA Identity Portal feature which searches previous decisions made for the specific approval required in this campaign. If previous decisions were made they will override any current decisions.

Campaign Customization Options

The following customization options are available in the certification campaign:

- Control the display of an entity – each entity in the campaign can be displayed using the attributes in the campaign. For example an administrator would like to display the user full name and title as the entity display and on hover would like to see all the other attributes. This configuration can be achieved in the connector configuration

  Use the "{" and "}" to encapsulate a user attribute of the entity, static text can be used for example: {UserId}, Title: {Title}

- Control reassign search attribute – define the reassign search attribute to be used to search users when performing a task reassign. This definition is done using the "reassign search attribute" in the connector properties.

