CA Identity Manager r12

Option Pack 1 Administration Guide

CA Product References

This document references the following CA products:

- CA Identity Manager

Contact CA

Contact Technical Support

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

- 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

Provide Feedback

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

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.

Contents

Chapter 1: Introduction

This section contains the following topics:

Benefits of the Option Pack

The Option Pack is a separate add-on component that you can install with CA Identity Manager. The Option Pack enriches CA Identity Manager by offering the following enhancements:

Fine-Grained Account Management

Provides account management that controls the allocation, termination, and modification of endpoint account attributes, such as Active Directory groups, RACF groups, SAP roles, or SQL database access. The Option Pack can manage any endpoint, including dynamic endpoints generated by Connector Xpress.

Fine-Grained Workflow

Provides added flexibility, account management, and ease of configuration to CA Identity Manager's current workflow capabilities. Enhanced workflow supports fine-grained association of workflow processes and approvers to an attribute or an attribute's value. Also, the following functionality is added:

- Dynamic resolution of approvers according to the approver's profile
- Approval consolidation per approver
- Partial approval and provisioning
- Multi-valued attribute approval
- Group approval in one step
- Sequential and parallel approvers at the attribute-value level.

Fine-Grained Out of Office Delegation

Provides the ability to, at the attribute-level, delegate each approval task to a different person, delegate each approval task to a different user, and define start and end dates for each delegated task.

Scheduled Tasks

Provides the ability to perform time-based activities at all levels, including the attribute level. This feature allows a user to configure time-based task activation, define complex activation conditions, activate a task for a specific user population, and scheduled mass updates for users with a specific profile. For example, all employees working for Sales in New York need access to a new database. Rather than performing the same action multiple times for each sales person, a CA Identity Manager administrator can perform all these identical tasks with one step, and in a time-based way.

Reverse Synchronization

Ensures and validates that access entitlements that a user has in the user store are identical to the access entitlements the user has on endpoints. This is done at the account-level for orphan accounts, and at the attribute-level. Reverse Synchronization allows you to either accept a discrepancy, reject it, or send it to an approval workflow. Once a decision is made, the relevant attributes are forwarded to CA Identity Manager for provisioning or de-provisioning.

Policy Xpress

Provides the ability to create custom business logic (policies) quickly, without the need for custom code.

Fine-Grained Account Auditing

Provides historical audit information about any changes to a user's accounts. This audit information can be combined with CA Identity Manager's standard audit tables to create reports in the user's reporting tool.

Fine-Grained Preventive Segregation of Duties (SOD)

Detects predefined SOD violations. Violations are captured at run time and sent for approval or rejection based on the user's configuration.

Roles and Tasks

Option Pack features are embedded in CA Identity Manager as Admin tasks. You can add new tasks to any Admin role, or remove them from an existing Admin role.

The following Admin roles are included by default:

- Option Pack Administrator—opens configuration tasks
- Option Pack Approver—approves predefined approval tasks
- Option Pack Self-Manager—performs account self-service and workflow delegation assigned to all users

Samples

The Option Pack has a fully configured Active Directory (AD) endpoint by default. With this sample, you can cover a wide range of features such as detecting new Active Directory accounts, using Reverse Synchronization, or managing a complex workflow approval chain. Also, sample workflow and approval tasks which can be used as a basis for new processes and tasks are included by default.

Chapter 2: Customizing the Option Pack

This section contains the following topics:

Overview

You can customize the Option Pack in the following ways:

- Edit Option Pack Global Settings
- Localize the Option Pack
- Change the Look and Feel of the Option Pack

Global Settings

The Global Settings screen allows you to configure parameters that were set during installation, and default parameters such as the Reverse Synchronization action during rejection.

Global Settings are located under Option Pack tab, System, Manage Global Settings.

You can define the following parameters:

Audit

AUDIT_POLICY_XPRESS

Enables auditing for Policy Xpress. Set this parameter to 1 to enable auditing.

General

DB_LANGUAGE

Defines the locale for the database.

DB_DATE_FORMAT

Defines the database date format. Default is compatible with Microsoft SQL and Oracle. Only change this parameter if necessary.

TIME_FORMAT

Defines the time format used in the Option Pack.

SCHEDULED_TASK_RECOVERY

Enables the recovery of Scheduled Tasks that runs every 9 minutes. Set this parameter to 1 to enable recovery.

DATE_FORMAT

Defines the date format used in the Option Pack.

Note: For LDAP user stores, dates are stored as strings. Also, using 'mm' in the date string format indicates *minutes*, not months. If you want to indicate months, use 'MM'.

IDM

IDM_ENVIRONMENT

Defines the inbound provisioning environment specified in the Provisioning Manager.

IDM_APPLICATION_SERVER_PORT

Specifies the port where you access the environment.

WORKPOINT_DATABASE_NAME

Defines the name of the WorkPoint database.

Reverse

NEW_ACCOUNT_REJECTED_ACTION

Defines the action taken (suspend or delete an orphan account) when a Reverse Synchronization action is rejected. The default setting is Suspend.

Schema

Contains the well-known attribute names for attributes used by the Option Pack. If you change these attributes, be sure to reflect those changes here. The attributes included are as follows:

- WORKFLOW_DELEGATIONS_ATTRIBUTE
- POLICIES_ATTRIBUTE_NAME
- REVERSE_TRIGGER
- DB_KEY_PHYSICAL_ATTR
- DATA_ATTRIBUTE

Localize the Option Pack

By default, the Option Pack supports the following four additional languages:

- French
- Italian
- Spanish
- German

The bundle files for these languages are located in the following folder:

Option_Pack_1_home/config/bundles

To add additional languages to the Option Pack

1. Stop the application server.
2. Go to *Option_Pack_1_home*/config/bundles.
3. Create copies of the files.
4. Translate the files to the language you need and save them using the following naming convention:

   filename_language.properties

   for example, to save accManage.properties as a French file, use the name accManage_fr.properties.

   The list of two character language abbreviations can be found at the following location:

   http://www.loc.gov/standards/iso639-2/php/code_list.php
   http://www.loc.gov/standards/iso639-2/php/code_list.php
5. Restart the application server.

Change the Look and Feel

To change the look and feel of the Option Pack

1. Stop the application server.
2. Modify the idfocus.css file to change the look and feel. The ccs file depends on your application server, as follows:
   - JBoss: The css file is in the /deploy/ACEWeb.war/ folder.
   - WebLogic: The css file is in the IdentityMinder.ear/ACEWeb.war/ folder.
   - WebSphere: The css file is in the IdentityMinder.ear/ACEWeb.war/ folder.
3. Restart the application server.

Customize Option Pack Tasks

If you want to customize an Option Pack tasks in your environment, we recommend that you *copy* the Option Pack task and then modify the copy. This process will prevent future upgrades from overwriting your custom tasks.

Chapter 3: Auditing

This section contains the following topics:

Overview

The following tables store audit information for the Option Pack. These tables are open and can be used for reporting purposes using your preferred reporting tool.

Account Management

Stores the Option Pack account data. The content depends on the endpoint types that you are managing, and the attributes you have selected for this endpoint type. For example, if you are managing UNIX – etc endpoints and you want to manage the groupNames and description attributes, the account management table stores any changes to these attributes and includes a time stamp for the change.

The Option Pack audit table is IDF_AceDataAudit.

Note: You can use the sessionID to join with CA Identity Manager standard audit tables (event ID). The initiator depends on how the task was executed. It can be a user, the Provisioning Server (inbound events), Reverse Synchronization, or the Initialize Endpoint Accounts task.

Reverse Synchronization

Any execution of Reverse Synchronization generates audit entries in the IDF_ReverseAudit audit table. For example, an account automatically suspended through Reverse Synchronization is stored.

You can group all Reverse Synchronization audit events by the same Reverse Synchronization GUID.

Segregation of Duties (SOD)

All SOD information is stored in the following three audit tables, including the SOD item involved, the approver, the mitigating control, and a time stamp:

- IDF_SODAudit
- IDF_SODAuditEntitlements
- IDF_SODAuditItem

Policy Xpress

Policy Xpress stores all information on the actions it performs.

Note: The View Submitted Tasks task in the User Console displays information about user changes, which are reflected by events. The View Submitted Tasks task does not contain Policy Xpress actions that are not events.

The following tables hold information about all actions in CA Identity Manager, regardless of type. These audit tables are not restricted to users.

The policy Xpress audit tables are as follows:

- IDF_StateAuditPolicies
- IDF_StateAuditActions
- IDF_StateAuditActionParams

Note: To enable Policy Xpress event auditing, go to Option Pack, System, Manage Global Settings, Audit, and change the value of AUDIT_POLICY_XPRESS to 1.

View Account Management Events

This feature displays a list of the changes to a user's account attributes that may occur. This report is not a point-in-time snapshot, but rather an ongoing record of changes on a user's account. To access this list, go to Option Pack, Audit, View Account Management Events.

Note: You can also use the IDF_AUDIT table to generate a custom report.

The fields in the audit report are as follows:

- SessionID—for internal use.
- Initiator—the initiator of the change. This field can be the account owner (for self-service), another user, detection through Reverse Synchronization, or the Provisioning Server.
- User Id—the account owner.
- Endpoint Type - the endpoint type of the account, such as UNIX - etc.
- Endpoint—the endpoint the account belongs to.
- Account Id—the audited account ID.
- Attribute Name—the attribute changed.
- New Value—the value after the change. For multi-valued attributes, the values are separated by a "^" sign.
- Modification time—date and time that the change occurred.

View Reverse Synchronization Events

This feature displays a report of the discrepancies between Identity Manager accounts and accounts on endpoints that may occur. To access this report, go to Option Pack, Audit, View Reverse Synchronization Events.

Each execution of Reverse Synchronization generates a new ReverseGUID. All the actions and results are audited and have the same ReverseGUID.

Note: You can also use the IDF_REVERSE_AUDIT table to generate a custom report.

The fields in the Reverse Synchronization Event report are as follows:

- ReverseGUID—unique number for each Reverse Synchronization execution.
- Domain—the Provisioning Server domain.
- Endpoint Type - the endpoint type of the account.
- Endpoint—the endpoint the account belongs to.
- Message—the Reverse Synchronization event log. This log contains the information Reverse Synchronization detects and executes. For example, an orphan UNIX account "jsmith" was detected and automatically suspended.
- Modification time—date and time that the change occurred.

Chapter 4: Managing Accounts and Endpoints

This section contains the following topics:

Overview

This feature allows you to display and manage user accounts (and their attributes) on an endpoint from the User Console.

Account Management has the following uses:

- To eliminate the manual configuration of tasks when managing new endpoints. An administrator can now create new account management tasks (similar to the default Manage Active Directory Accounts task) without manually creating and importing XML files. This includes dynamic endpoints generated by Connector Xpress.
- To dynamically define the values of endpoint account attributes. An administrator can now select the source for the values of endpoint account attributes.

Note: This feature supports any endpoint accessible through JIAM and is not limited to the default endpoints provided. Also, all the attributes within these endpoints can be managed (except for passwords).

Default Account Management Tasks

The Option Pack allows you to modify user account attributes on a managed endpoint. While many endpoints and attributes are supported, several attributes are added by default.

By default, there are two Admin tasks related to endpoint account management. The first allows you to manage another user's accounts. These tasks are included in the admin role Option Pack Administrator. The second allows you to manage your own accounts. These tasks are included in the admin role Option Pack Self-Manager. The Self-Manager role is granted to all users by default.

The Option Pack Administrator role has the following default task:

- Manage Active Directory Accounts

The Option Pack Self-Manager role has the following default task:

- Manage My Active Directory Accounts

You can reorganize the default tasks, and add new tasks for other endpoints.

Acquire a New Endpoint Type

Every endpoint type managed by the Option Pack needs a corresponding attribute in the Identity Manager user store. All endpoint account data is stored in that attribute, and later used by the various Option Pack tasks.

Note: The Option Pack *only* supports Connector Xpress endpoints from CA eTrust Admin version SP2 CR13 or later.

To acquire an endpoint type

1. Go to Option Pack, Account Management, Acquire Endpoint Types.
2. Select the endpoint type you want to manage.
3. Set the schema attribute chosen to hold the endpoint type data.
4. Select the attribute you want to manage on the endpoint type. This attribute needs to be defined in the directory XML file. As an example, when installing the Option Pack, the Active Directory attribute is mapped.

   Note: This attribute must be able to store large values. If you are using an RDB user store, set the attribute to nText for a Microsoft SQL user store, or CLOB for an Oracle user store.
5. If the attribute is multi-valued, select the Multi-value check box.
6. Set the attribute name, or use the suggested default in the Attribute Name field. The attribute name must be unique across all endpoint types.
7. (Optional) Set the Provisioning Object associated with the attribute.
8. If available for the endpoint type, choosing an object class will provide an additional option when defining an account screen. This option will allow the list of objects to be the available values list. The values are taken from the Provisioning Server. For example, for ADGroups, the object is set to "ADGroup" by default, allowing the screen to show the groups known to the Provisioning Server.

9. Click Add.
10. Repeat Steps 4 through 6 for all attributes you want to manage on the endpoint type.

Note: If you want to manage an endpoint account attribute with Reverse Synchronization, you must also map those attributes (see page 58) to a custom attribute in the Provisioning Manager.

Create an Account Screen

After you acquire a new endpoint type, you can create an account screen to manage the endpoint accounts.

Editing the account screens is possible using the Identity Manager Modify Admin Task feature, but this only allows cosmetic changes to the screens, such as attribute display names, order, or HTML additions. To make other changes, such as adding a new value to an attribute, create an Option Pack account screen.

To create an account screen

1. Go to Option Pack, Account Management, Create Account Screen.
2. Create the task by filling in the following fields:

   Task Name

   Specifies the name that appears in the User Console on the left sidebar.

   Endpoint Type

   Defines the new endpoint type. This endpoint type must be acquired (see page 22).

3. Select the attributes you want to manage and fill in the following fields:

   Style

   Defines how the field appears in the account screen. Possible values are as follows:

   - Free text—the user can type any value. No predefined value available.
   - Dropdown—based on Value source, a drop-down list appears (only one value can be selected).
   - Filtered Dropdown—same as Dropdown, but the user can apply a selected filter to prevent multiple values from appearing in the drop-down (acts like a search).

- Single selection—same as Dropdown, but all values are visible.
- Filtered Single selection—same as Single selection, but the user can apply a selected filter to prevent multiple values from appearing in the drop-down (acts like a search).
- Multiple selection—a list of options appears, and the user can highlight more than one option using the Control key (Ctrl).
- Option selection—two boxes appear for available and current values. The user can move values between the two boxes for selection.
- Filtered option selection—same as option selection, but a filter field appears above the check box. For example, the ADGroups in the default Active Directory management screen.

Note: The options differ depending on if the attribute is single or multi-valued.

Value source

Defines how the selected value's attribute is populated in the account screen. Possible values are as follows:

- No list—no predefined values.
- Provisioning server—if a Provisioning Object was selected for the attribute when acquiring the endpoint type, the list of available values is taken directly from the endpoint. For example, Active Directory groups are selected from the Active Directory domain automatically.
- User defined—a static list of predefined values. You can define a display name and a stored name. The format is stored value;displayed value, such as cn=telnet,cn=users,dc=ca,dc=corp;Telnet Access

Note: The options differ depending on if the attribute is single or multi-valued.

4. Click Apply.
5. Repeat Steps 3 and 4 for each endpoint account attribute you want to manage.
6. When you have finished adding attributes to manage, click Save.

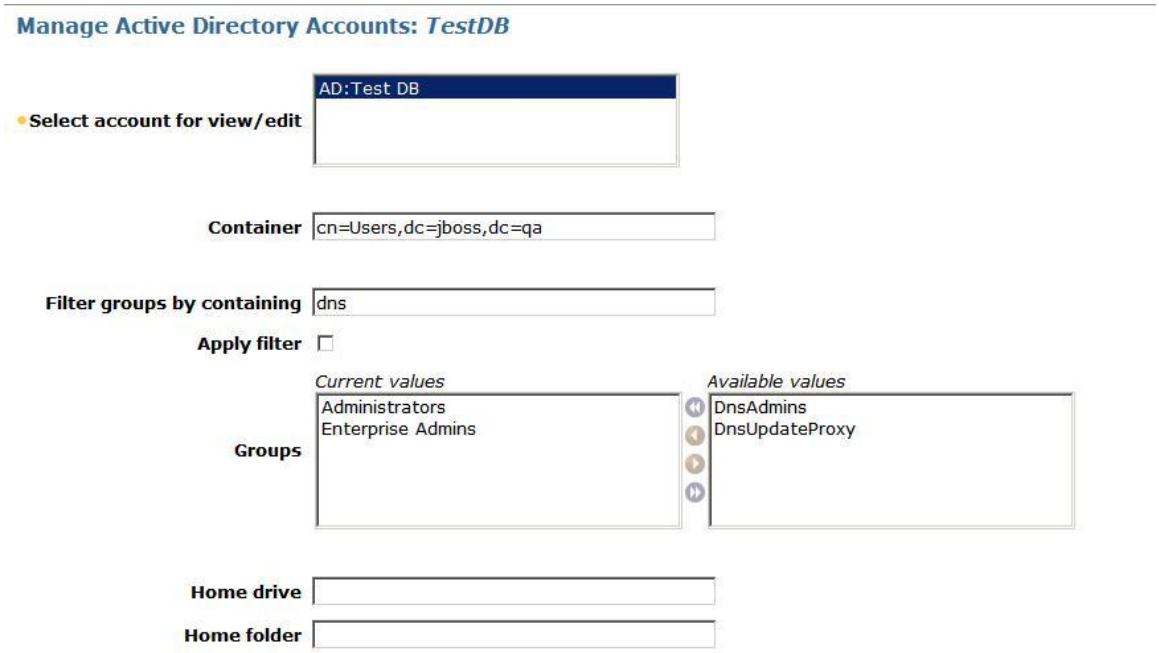
   Wait until Save finished successfully appears. This may take a few minutes.
7. Restart your application server.

   The new task is added to the Option Pack Administrator role.

Note: If you want to change an attribute definition, such as from multi-valued to single-valued, you must run the Initialize Endpoint Accounts task afterward for the changes to take effect.

Sample Active Directory Account Screen

The following graphic shows the Option Pack account self-service screen for Active Directory:



Select account for view/edit

Specifies the user's Active Directory accounts. If a user has multiple accounts in Active Directory, they all appear in this field. Selecting an account shows the Active Directory values associated with this particular account.

Container

Modifies the Active Directory account's container (OU). This is equivalent to a Move account and not to a Delete and Create account (the SID is kept). The container value is case sensitive. For example, to move the account from Users to Administrators, type ou=Administrators and the rest of the DN.

Filter groups by containing

Defines a filter to limit the number of groups shown. Use this filter option if you have many groups and want to restrain the groups shown.

Note: Wildcards are not necessary in the filter. For example, to search for Active Directory Groups containing "Administrator", type Administrator in the filter field and click Apply filter.

Groups

These selection boxes allow you to request membership in Active Directory groups. This membership may be subject to SOD interception and workflow approval. Each value can be added or removed independently. Current Values represent the Active Directory groups the user currently has and Available Values represent the list of all Active Directory groups available for the user to request.

Note: To configure the available list of Active Directory groups, use the Account Screen Configuration tool to specify the source for any attribute. In this case, you would select the Provisioning Server. The groups are then taken from the Active Directory domain.

Initialize Endpoint Accounts

Initialize Endpoint Accounts populates the user store endpoint account attribute, such as %ActiveDirectory%, for all users. No business logic is applied, but new values are audited by the Option Pack.

Note: This task may take a significant amount of time to complete, depending on the number of accounts and users.

Use this task in the following situations:

- You have acquired a new endpoint type using the Acquire Endpoint Types task.
- You have added or removed an attribute from the managed endpoint using the Acquire Endpoint Types task, for example, adding the UNIX description for all accounts.
- You have added a new endpoint to the endpoint type. For example, a new domain in Active Directory.

To initialize an endpoint

1. Go to Option Pack, Account Management, Initialize Endpoint Accounts.
2. Provide the following parameters:

Initial Load Type

Defines the mode to improve performance, as follows:

Users—the endpoint initialization needs User/Account relationship information. In Users mode, it scans the provisioning global users list and detects the associated accounts for each user.

Accounts—scans endpoint accounts and finds the associated user for each account.

If you know that you have many users and almost all of those users are being associated with accounts, select Users. If you have many users, but only a few users own accounts on the selected endpoint type, select Accounts. If you are unsure, select Users as the default.

Clean

Specifies whether the Option Pack data is deleted and then recreated from scratch. This option only deletes data on the selected endpoint and does not affect other endpoints or endpoint types.

Note: Use this check box *only* when you want to delete the endpoint data in the user store. For example, if you have already loaded data into an endpoint and then decide to delete the endpoint, use the Clean check box to delete the original data and start again. Clean does *not* affect accounts on the endpoint.

Recovery From a Previous Run

Specifies whether data is recovered from a previous initialization. If the initialization process was prematurely stopped, you can start a new initialization and recover from the previous run. The new initialization starts from the last point of your previous run. Select the desired run from the drop-down box.

Note: If you recover from a previous run, you are not able to select a different endpoint and endpoint type.

Identity Manager Domain Name

Defines the Provisioning Server domain.

Administrator Name and Password

Specifies the Provisioning Server administrator name (such as etaadmin) and password.

Endpoint Type

Specifies the endpoint type, such as Active Directory or CA-ACF2.

Endpoint

Specifies the system name where you want to get accounts from.

3. Click Submit.

   The endpoint is initialized and a log file is created under the Option Pack folder.

Chapter 5: Email Notifications

This section contains the following topics:

Overview

The Option Pack Email Notifications feature provides simplified, user-friendly email policy management, allowing non-technical users to configure email notifications without the need for code.

Email Notifications offer a list of commonly used items that are needed in an email, such as different types of recipients and different information that can be added into the body of an email.

How to Create a New Email Notification

To create an email notification

1. Under the Option Pack tab, go to Email Notifications, Manage Email Notifications, and select Create New.
2. Provide a name and description to identify the email.

   These fields are not displayed in the email sent, they are only used for managing the email. Both are displayed in the email list available through the main page.
3. Define when to send an email.

   There are several default selections for when to send the email. Some of the options require secondary selections, which narrow down the scope. For example, sending an email when a task starts requires selecting the task that triggers the email.
4. Specify the recipients of the email.

More Information:

When to Send (see page 30)

When to Send

One or more of the following When to send options are available to send an email on all relevant events:

User created

Specifies whether an email is sent when a user has been created. The email is sent when the CreateUserEvent reaches completion.

User modified

Specifies whether an email is sent when a user has been modified. The email is sent when the ModifyUserEvent reaches completion.

Workflow pending

Specifies whether an email is sent when workflow reaches a point where it requires approval. This requires you to select the relevant workflow process. To use this option, the workflow process must be connected to the Policy Xpress workflow agent. All Option Pack Workflow processes are connected to the Policy Xpress by default.

Event Starts

Specifies whether an email is sent when an event reaches the Before state. This option requires you to select the event.

Event approved

Specifies whether an email is sent when an event reaches the Approved state. This option requires you to select the event.

Event rejected

Specifies whether an email is sent when an event reaches the Rejected state. This option requires you to select the event.

Event Completes

Specifies whether an email is sent when an event reaches the After state. This option requires you to select the event.

Task submitted

Specifies whether an email is sent when the task starts processing. This option requires you to select the task.

More Information:

WorkPoint Workflow Integration (see page 49)

Recipients

You can configure multiple recipients for the To, CC, or BCC fields of an email. Select the required recipient and click the appropriate button next to the selection. The following common recipients are included by default:

Workflow approvers

Specifies that the email is sent to all approvers of the current workflow step. This option is only applicable if the email is sent for a workflow pending event.

Note: If an Option Pack Email Notification is configured with the recipient 'Workflow approvers', each recipient receives an email with only their email address in the To list. Other recipients (workflow approvers) do not show up in the To list, but the email is sent to all Workflow approvers.

Manager of user

Specifies that the email is sent to the manager of the user whom the task has been performed on.

Note: To set the manager attribute, go to the environment in the Management Console, under Advanced Settings, Miscellaneous, and set managerattribute to the well-known name of the manager attribute.

Group members

Specifies that the email is sent to all members of a group. Selecting this option opens a drop-down with available group names.

Role members

Specifies that the email is sent to all members of an Admin role. Selecting this option opens a drop-down with available role names.

Static address

Specifies that the email is sent to a selected email address. You can specify the email address in the additional text area available.

User

Specifies that the email is sent to the user whom the task was performed on.

Initiator of request

Specifies that the email is sent to the person who made the request.

Custom

This option creates a custom data element in Policy Xpress. Once this custom data element is created, you can then go to Policy Xpress and configure the data element with any recipient. A name is required for this custom option, which you will use to identify the custom element in Policy Xpress. (Do not change this name through Policy Xpress.)

To provide the data for this new custom data element, go to Policy Xpress, search under the Emails category for a policy with the same name as the email notification, then edit the custom data element that you created.

Note: The custom data element will be set to 'custom value' until updated by Policy Xpress. An email will *not* be sent to *any* recipient until all custom addresses are set using Policy Xpress.

Subject and Body

You can define the subject and body of an email as simple text, or add them with dynamic content that is calculated when the email is sent.

The subject line is a plain text field where you can write your message. This message is the subject of the email sent.

The body is displayed in an HTML editor. Any text can be inserted and formatted to form the email body. The editor offers the ability to edit the text in full screen or to edit using HTML tags, including logo URL.

In addition to text, each email can be populated with dynamic content. The dynamic content can be inserted into the main text using a special format (indicated by curly brackets and the word Dynamic in it). A value appropriate to the context replaces the text when the email is sent. Because this is a text replacement, all text formatting (such as using bold characters) apply to the dynamic content too.

The dynamic content includes the following:

Current date

Specifies today's date in the format defined under Option Pack tab, System, Manage Global Settings.

Task name

Specifies the task for which the email is sent.

Event's primary object name

Specifies the friendly name of the event where the email is sent from. If a user event, this field is the user's login name. The primary object can be something other than a user. For example, it can be any managed object such as a group, admin role, and so on. This option is more useful for role or group assignment events, where the name of the role or group is displayed.

User's attribute

Specifies the value of one of the user's attributes. The user is the subject of the task. This option requires selecting the attribute from a drop-down.

Manager's attribute

Specifies the value of one of the attributes of the user's manager. The user is the subject of the task. This option requires selecting the attribute from a drop-down.

Note: To set the manager attribute, go to the environment in the Management Console, under Advanced Settings, Miscellaneous, and set managerattribute to the well-known name of the manager attribute.

Custom

This option creates a custom data element in Policy Xpress. Once this custom data element is created, you can then go to Policy Xpress and configure the data element with any dynamic body content. The dynamic content is presented as a constant data element in Policy Xpress, which can be edited to any other type of data element that may rely on new data elements, but the name of the data element must stay the same.

To provide the data for this new data element, go to Policy Xpress, search under the Emails category for a policy with the same name as the email notification, then edit the custom data element that you created.

Note: Only modifications to custom fields should be handled through Policy Xpress. Any other email notification changes should be made through the Email Notifications interface.

Modify Email Notifications

When you create an email notification, it is added to the list of available email under Option Pack tab, Email Notifications, Manage Email Notifications. This screen displays all available email notifications in the system, including the name and description. The page also allows you to expand the events at which the email is sent.

Email notifications can also be deleted through this screen by selecting the email and clicking Delete Selected.

To modify an email notification, click the arrow icon next to it. The same page as the create email screen opens, but with the email's details. The email notification can then be modified and saved.

Note: Saving an email notification does not damage any custom setting used in the email, as long as the custom data element's name has not been modified.

Disable Email Notifications

You can enable or disable email notifications using the disable check box found for each email. When checked, the selected email policy is not active and no email is sent.

Configure SMTP

The Option Pack sends email using the CA Identity Manager SMTP configuration.

Note: For more information about CA Identity Manager SMTP settings, see the *CA Identity Manager Installation Guide*.

Chapter 6: Policy Xpress

This section contains the following topics:

Overview

Policy Xpress allows you to create complex business logic (policies) without the need to develop custom code. The Policy Xpress task is located in the User Console and is, by default, assigned to the Option Pack Administrator role, and to members of the System Manager role.

The main screen offers an option for creating a policy, or searching for an existing policy.

Searching a policy can be done based on several parameters that define a policy. By default, there is no filter and the search returns all policies. Mark the check box next to a policy to activate the filter.

How Policy Xpress Works

When a trigger (attributes, events, workflow, and Business Logic Task Handlers currently) occurs, Policy Xpress is activated and the following steps occur:

1. Policy Xpress checks activation times to see if there is a policy that should run at that particular time.
2. A list of policies is generated.
3. Policies are ordered based on priority, and Policy Xpress goes through them one by one, as follows:
   a. All required data elements are calculated.
   b. Entry rules are checked to see whether the policy should run.
   c. If the entry rules allow the policy to run, all action rules are checked for matches.
   d. If an action rule is matched, the Add Actions for that rule are executed. All other rules which previously matched execute their Remove Actions.
   e. Actions are performed in order of priority.
4. Once the policy completes, the data is saved in the user record.
5. The action commits where needed and the next policy is loaded.

Note: This flow may change based on some actions.

More Information:

Special Process Flow (see page 45)

How to Create a Policy

To create a policy with Policy Xpress, define the four basic elements of a policy.

Activation Times (Run At Events)

Defines when a policy should be run. Business logic must run at specific times to prevent data corruption and to increase performance. For example, setting a user as enabled should occur when the user is created. Running this logic at all times may cause users who should be disabled to become enabled again. Another example is giving the user a provisioning role that grants access to a certain system. This role should only be assigned to the user after a different role has been assigned and approved. Policy Xpress allows for the activation of its business logic during event and BLTH processing, much like custom adapters. Therefore, unlike identity policies, the logic can be triggered at any time, and not only at the beginning of a task.

Data Gathering (Data Elements)

Specifies the data used by the policy. Every type of business logic requires some data to work with. That data may be used to make decisions or it may be used to construct more complex data. Policy Xpress provides many individual components to gather data. These components are referred to as *Data Elements*. An example of a data element is a user's attribute value. For example, Policy Xpress can gather the user's first name and store it as a data element for later use.

Rules

Defines the rules of the policy. The core of any business logic is rules. Business logic provides the ability to decide what to do, based on information available. Using the information gathered at the data gathering phase, Policy Xpress has two types of rules:

Entry Rules

Defines the requirements met before execution. These rules allow the policy to be simple and more effective at the same time. An example of an entry rule is to run a 'Set Full Name' policy *only* if the first name or the last name has changed.

Action Rules

Defines the action taken based on the information gathered. For example, based on a user's department name we can assign the user to different roles or different account values.

Actions

Specifies the action to perform. At the end of the process, Policy Xpress performs the actions needed by the business logic. Policy Xpress works by having an action rule attached to multiple actions, so when the rule is met, the actions are performed. Actions can vary from the assignment of attribute values on a user or in an account, to executing a command line, running a SQL command, or generating a new event.

Create a Policy

Important! If you click Close while creating a policy, you will *not* be prompted for confirmation, and all your unsaved work will be lost.

You can create a policy by selecting New Policy on the main Policy Xpress screen, or by clicking New Policy after you search for policies.

In addition to the four main elements of a policy, there are other fields that help with managing policies and refining policy capabilities.

Note: A policy is only effective in the environment it is created in. For example, if you create a policy while logged into the neteauto environment, the policy triggers only for the neteauto environment.

Provide the following fields when creating a policy:

Policy name

Defines a friendly name for the policy. The name can be used to search for the policy, and is displayed in the log messages that describe the actions taken by the policy. This field requires value.

Policy Type

Defines the action that triggers the policy. Each policy type has a different configuration based on the type.

Note: You cannot change this field once the policy is saved.

Category

Defines a group of related policies. This field is optional and allows you to group policies for ease of management.

Description

Specifies a description of the policy.

Environment

Defines the environment that the policy is associated with. Different Identity Manager environments can have different policies associated with them. This value is automatically set to the environment you are creating the policy in. When you import policies, the environment is set to the target environment where the policy is imported.

Run Once

Specifies if the policy should run only once. Some policies may need to run every time they meet criteria, and others may need to run only once. This value determines if action rules that have already executed in the past should execute again. For example, adding an SAP role to a user based on department is an action that should only occur the first time the user matches that department. Adding it repeatedly, even though the user is still a member of the department, can cause significant issues. Alternately, a policy that sets the user's salary level based on title would *not* be set to run once, for enforcement purposes. If anyone tried to change the user's salary level, the policy would reset it.

Priority

Specifies when a policy should run, if there are multiple policies that need to run at a single event. Policies are checked and executed based on their priority. The lower the number, the higher the priority (priority 1 runs first, 10 runs second, 50 runs third, and so on).
Setting priority is useful for policies which have a dependency on one another, or breaking an otherwise complex policy into two simple ones running one after the other.
For example, there are three policies which should only run if there is a specific value in the database. Instead of having each of the policies verify the database for that value, create a policy that runs before the other three policies, and checks the value. If the new policy matches the required value, a variable is set. The other three policies are configured to run only if that variable is set, which prevents redundant access to the database.

More Information:

Variables (see page 44)

Run At Events

Run At Events (activation times) is similar to CA Identity Manager's native functionality. Depending on the policy type selected, time can be linked to a policy to make it run at different stages of a process.

For example, a policy of type Event can be set to run before CreateUserEvent or approved SynchroniseUserEvent. A policy of type Task can be set to run at Validation for Create User or at Set Subject for Disable User.

The following policy types require deploying listeners:

- Attribute
- Workflow

More Information:

On-Screen Attribute Validation (see page 46)
WorkPoint Workflow Integration (see page 49)

Data Elements

Data elements are the core of policy rules and are also used for creating other policy data. Data elements represent the information used when defining a policy. A policy can contain multiple data elements.

Policy Xpress uses flexible plug-ins for gathering the data element information. Each one of the plug-ins can do a small scale, dedicated task. However, several plug-ins can be used together to build more complex policies. An example of a data element plug-in is a user attribute element. The goal of the element is to gather information about a certain attribute which is a part of the user's profile.

Data elements are calculated when they are called, meaning either a rule is using the data element, or another element needing calculation is using the data element as a parameter.
For example, an SQL query data element can retrieve a value from a table, but it needs the user's department to build the query. In this case, the department data element must run before the SQL query data element, and then the value can be used as a parameter (see page 44).

The following fields define a data element:

Name

Defines a friendly name that describes the data element. Some data elements are complex (such as getting variables or retrieving information from the database). Be sure to select a meaningful name to simplify data element management.

Category

Provides a grouping of data elements. This field sorts the data elements and makes selection easier.

Type

Specifies the data element type, each with its own dedicated use. This field is based on the category selected.

Sub type

Defines possible variations of the same data. Most data elements only support the Get function.

For example, the user attribute data element has the following sub types:

- Get—returns the values of the attribute
- is multi valued—returns true if the value is multi-valued
- is logical—returns true if the value is logical

Explanation and Description

Provides a prepopulated description of the sub type. Each sub type option selected provides a different description to help in understanding its function and what the expected values are.

Parameters

Defines the parameters passed to the data element. Data elements are dynamic and can do different things based on the parameters. A user attribute data element returns different results based on the attribute selected. The sub type option also defines the number of parameters, their names, and the optional values when available.

You can add additional parameters if necessary. The SQL query example accepts two required parameters, the data source and the query itself. The query can use the "?" to be replaced with values (much like a prepared statement). Adding additional parameters allows you to set those values.

Use Dynamic Values in Data or Action Elements

Dynamic values are the result of calculated data elements, and their values are only decided at run time. The values can then be used as parameters to other data elements (that run after, based on priority) or in action elements.

To use a dynamic value as a parameter for a data or action element

1. Edit the data element (or action).
2. If the parameter is a drop-down box, it lists the dynamic values at the top. Select the dynamic value you want to use.
3. If the parameter is a text field, click the ellipses (...) button next to the field.

   A screen appears with the list of currently defined data elements.
4. Select the dynamic value and click Add.

   A symbolic reference to that data element is placed in the text field. The reference can be moved within the field, more text can be added before and after the reference, and additional dynamic values can be added too.

Entry Rules

Entry rules define the logical conditions for when a policy should run. The conditions use the values gathered by the data elements in the policy.

There can be multiple entry rules in a policy, and an entry rule can have multiple conditions. At least one entry rule must be matched, meaning that *all* conditions must be met, for a policy to move to the action rules.

The following fields define an entry rule:

Name

Defines the meaning of the entry rule.

Conditions

Specifies the criteria to match.

Note: Conditions in an entry rule always have an AND operator between them.

More Information:

Conditions (see page 42)

Conditions

A condition is used in entry and action rules and is comprised of the following components:

- Data Element
- Operator
- Value

For example, you want to create a condition that checks if a user's department was changed. First, define a Department Changed data element, then, in the condition, select the Department Changed data element, set the operator to Equals, and set the value to True.

More Information:

Entry Rules (see page 42)
Action Rules (see page 43)

Action Rules

Action rules are similar to entry rules in structure, but differ in functionality. Instead of having to match one entry rule, several action rules may be matched. The single action rule with the highest priority (1 being the highest) is the *only* one used.

Action rules also contain one or more actions, and the actions are divided into Add Actions and Remove Actions.

The following fields define an action rule:

Name

Defines the meaning of the action rule. This name must be unique.

Priority

Defines which action rule executes, in the case of several action rules matching. This field is useful for defining default actions. For example, if you have multiple rules, each for a department name. It is possible to set a default by adding an additional rule with no conditions but a lower priority (such as 10 if all others are 5). If none of the department rules are matched then the default is used.

Conditions

Specifies the criteria to match.

Add Actions

Defines a list of actions taken when the rule is matched. For example, if the user's department matches the one configured in the condition, add a specific Active Directory group. Action rules behave differently when the policy is set to run once or not. If the policy is set to run once, then after the first time the rule is matched and performs its actions, it will not run again while still matching. In the example above, the Active Directory group is added to the user only once. If run once is not set, then the actions run again as long as the rule is matched. This field is important for enforcing values.

Remove Actions

Defines a list of actions to perform when the rule matched in a previous run, but no longer matches. Remove actions are useful to balance add actions. For example, the previous example added an Active Directory group to the user, based on the department. If the department changed, then the remove action removes the Active Directory group.

More Information:

Conditions (see page 42)

Actions

Actions perform the business logic after all the decision-making is done.

An action works in a similar way to data elements except at the end. When it runs, it performs a task instead of returning a value.

The following fields define an action:

Name

Defines the purpose of the action.

Category

Provides a grouping of actions. This field sorts the actions and makes selection easier.

Type and Sub type

Defines the Type and Sub type of the action taken.

Note: For more information about Type and Sub type, see Data Elements.

Priority

Specifies which action to perform in ascending order of priority, when you have multiple actions in an action rule.

Parameters

Defines the parameters passed to the action.

Variables

Policy Xpress is able to use variables. Variables are shared across all policies that run at the same time, so a variable that has been set can be used by other policies of lower priority.

For example, a variable can contain a value calculated once by one policy, and then shared across other policies that no longer need to recalculate the value. A variable can also be a trigger for other policies, where the policies only run if the policy before them has run.

Variables are set with actions and saved as data elements. They are available in the Variables category of both actions and data elements.

Special Process Flow

Important! Use caution when changing process flows. Using these actions may result in an infinite loop.

By default, policies are sorted by priority and then executed one by one. While this flow is almost always the flow necessary, you can change the flow of the system.

This flow-changing functionality is represented by an action that can be attached to any action rule.

The following four flow-changing subtypes can be used:

Stop processing

Causes all policies after the current policy to be ignored, and Policy Xpress will exit.
Note: Only Policy Xpress exits. If you want to force CA Identity Manager to stop also, you can use the Exception type action plug-in.

Restart all policies

Stops processing the rest of the policies and goes back to the start of the list. This option is useful in cases where the action of one policy causes another policy, which ran before it and did not execute, to now met the entry criteria. That policy is now reevaluated.

Redo the current policy

Causes a policy to run again. This option is useful for iteration. For example, creating a unique username requires a policy to run over and over again until it finds a unique name.

Go to a specific policy

Should be used rarely and with caution. This action requires selecting an existing policy. If that policy is running at the same time as the current policy (can be before or after) then Policy Xpress jumps to the selected policy. If the new policy is of lower priority, all policies between the current policy and the selected policy are ignored. If the new policy priority is higher, the process goes back.

On-Screen Attribute Validation

In addition to the defined triggers (policy types), Policy Xpress can also listen to validation on attributes. To do this, use the Policy Xpress logical attribute handler. This allows you to create policies that can run when an on-screen attribute that has been flagged as "validate on change" is updated. However, task-level validation is not triggered when an attribute changes. The only way to use Policy Xpress in those instances is by setting up the Policy Xpress logical attribute handler.

Note: For more information about logical attribute handlers, see the *CA Identity Manager Programming Guide for Java*.

This functionality can be used for creating dependant drop-down boxes. For example, if there are two drop-down boxes on the screen, Policy Xpress runs when the first drop-down option is selected, then set the values for the second drop-down box based on the option selected in the first. An unlimited number of drop-down boxes and other screen refreshes can be done. This differs from CA Identity Manager's native functionality by allowing the drop-down options to be populated using any logic, rather than importing an XML file of static options.

Another use is populating other attributes based on the value of one attribute. For example, you can select department, and attributes such as department manager, department number, and HR Dept Code are automatically populated as suggested values. This replaces the need to write logical attribute handler custom code.

To use this functionality, at least one attribute on the screen must be created using the Policy Xpress attribute logical handler.

The handler is also an easy way for creating attributes that exist only during the current session and are not written to the user object (unless a policy copies the values to a physical attribute).

More Information:

Create a Policy Xpress Logical Attribute Handler (see page 47)
Example: Dependant Drop-Down Boxes (see page 48)

Create a Policy Xpress Logical Attribute Handler

For Policy Xpress to listen to validation on attributes, configure a Policy Xpress logical attribute handler.

To create a Policy Xpress logical attribute handler

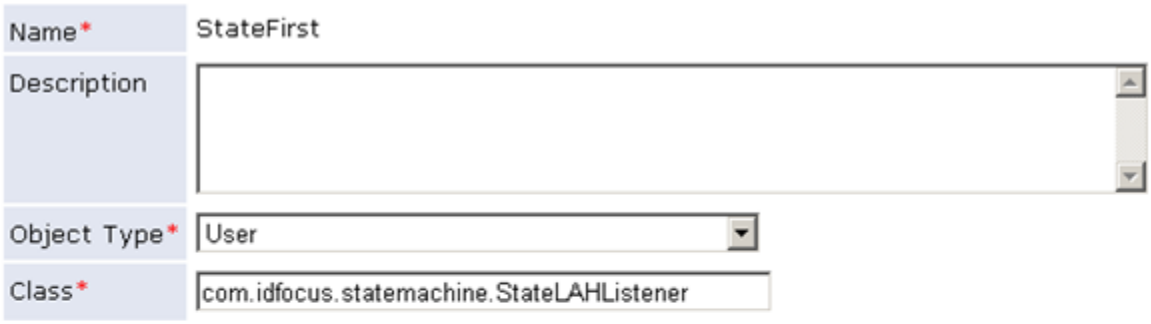
1. In the Management Console, and click Environments.
2. Select the environment and click Advanced Settings.
3. Click Logical Attribute Handlers and select New.
4. Create a new logical attribute handler and provide the following details:
   - Name
   - Description
   - Object type—Policy Xpress runs a policy for any of the object types. Some of the options (such as getting attribute values) are only relevant for users in Policy Xpress.
   - Class—Set to com.idfocus.statemachine.StateLAHListener.
5. Click Save.

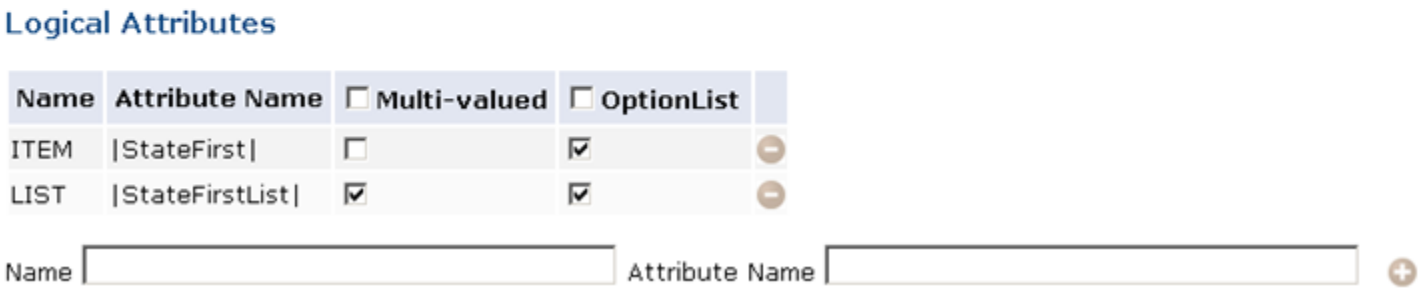
   In this handler, the actual attributes are created. No physical attributes or user properties are required.

Note: For more information about logical attribute handlers, see the *CA Identity Manager Programming Guide for Java*.

Example: Dependant Drop-Down Boxes

The following process is one way of creating an easy set of a dependant drop-down boxes.





1. In the Management Console, create two logical attribute handlers using the Policy Xpress class name. Both should contain an item and a list (a total of four attributes, two items and two lists).
2. Add the four new attributes to a screen.

   Note: The two lists should be hidden (automatically) and the two items should be set as drop-down boxes.
3. In the first drop-down (the item attribute), set the flag "validate on change". This flag will appear at the bottom of the attribute configuration after setting the type to drop-down.

4. In Policy Xpress, create a policy which populates the initial values of the first drop-down box.

   This policy is of type Task and runs at (Run at Event) Set Subject. An action in this policy sets values to the list attribute of the first handler. In the example, that would be |StateFirstList|. This policy can also assign an initial value to the item attribute, if a current value is available.

5. Create a second policy to update the values of the second drop-down box when the first drop-down box changes.

   This policy is of type Attribute and runs at Validation. The value of the first drop-down box is read as a normal attribute of the user, and is taken from the item attribute. In the example, that would be |StateFirst|. An action in this policy sets values to the list attribute of the second handler, based on the result from the first.

When using this screen, the first policy sets optional values to the first drop-down box. When a value is selected, the second policy updates the options in the second drop-down box. You can do various things with the results of the second drop-down box. For example, you can set up a third policy of type Task that runs at Validation (different from attribute validation) and copies the value in the item attribute of the second handler to a physical attribute.

WorkPoint Workflow Integration

Policy Xpress integrates with WorkPoint approval processes, generated by CA Identity Manager. This allows logic to be triggered when workflow processes are executed. For example, to print out the names of the approvers appointed by the workflow process.

Workflow integration requires deploying an agent on the WorkPoint activity that notifies Policy Xpress that the approval step is occurring.

All Option Pack default workflow processes and workflow processes created within the Option Pack include the agent automatically.

To add the agent:

1. Open WorkPoint Designer and edit the required process.
2. Open the relevant approval activity (displayed as an image of a running man).
3. Navigate to the agents tab.

4. Add the "StateWorkpointListener-Agent" to the Asynchronous section.
5. Save the process.

Note: Not all new workflow processes with the previous configuration trigger Policy Xpress. If a policy of type Workflow has this process name set as the trigger, it is evaluated.

Not all actions or data elements are applicable to workflow. Refer to the individual plug-in for restrictions.

Example

To get the list of approvers, you can use the Approvers list data element under the Workflow category. This retrieves either the login names of the approvers or their email addresses.
This information can have various uses, such as sending an email to the approvers to notify them that an approval is required.

Import a Policy

When importing a policy, note the following:

- When importing an older policy that does not support policy types, Policy Xpress checks the most significant activation time (Run At Events) entry and set the policy type appropriately.
- The environment of a policy is set to the environment where the policy is being imported to, not the environment from which it was exported.

Policy Xpress Examples

Set a user's full name

Run At Events—when the user is created or modified

Data Elements—get the values of the first name and last name

Entry Rules—if the first name or last name has changed based on the data gathered. It prevents the policy from running otherwise.

Action Rules—set the full name to be the value of the first name, space, and the value of the last name.

Assign different provisioning roles for employees versus contractors

Run At Events—at create user and modify user

Data Elements—get the value of the user's type

Entry Rules—none (action rules are always evaluated)

Action Rules—1) checks if the user type is an employee 2) checks if the user type is not an employee. Only one of the action rules can be met, and assigns the appropriate provisioning role.

Set the user's groups and OU in Active Directory, based on department

Run At Events— at the end of the assign provisioning role event. This ensure that an account is already created when setting the values.

Data Elements—get the user's department, and also the endpoint type and Active Directory domain to make things easier to manage later on

Entry Rules—if the department is not empty

Action Rules—multiple rules for each possible department. Each rule checks if department equals Sales or any other value. There is a default rule in case the department does not meet any requirements. Different actions are configured for each rule, assigning different values. This ensures that a user in a specific department gets the Active Directory groups and OU they need, while a user in a different department gets others, as appropriate.

Write all new users to a table. The table contains some of the user's HR data.

Run At Events—on create user, but only after the user has been created (after the create user event has completed)

Data Elements—gets the required HR information, such as user name, country, department, and any other values

Entry Rules—none (action rules are always evaluated)

Action Rules—execute an SQL query which accepts the values gathered as parameters. The result of activating the query is having a new record in the database for the new user.

Chapter 7: Scheduled Reverse Synchronization

This section contains the following topics:

Overview

Reverse Synchronization ensures control of the accounts a user has on each endpoint by identifying discrepancies between Identity Manager accounts stored in the Option Pack endpoint attribute and accounts on the endpoints.

Although it is CA Identity Manager's responsibility to create, delete and modify accounts, it is impossible to prevent an endpoint system administrator from performing these operations on their own. This can occur due to emergency reasons, or malicious reasons (a hacker, for instance).

As a result, CA Identity Manager must provide its administrators, managers, and users the ability to detect any changes performed on the endpoint systems. For example, if an account was created in the Active Directory domain using an external tool, CA Identity Manager must be aware of this potential security issue. In addition, bypassing CA Identity Manager causes a lack of approval processes, SOD prevention, and audit reports.

Two types of discrepancies between CA Identity Manager and managed endpoints are as follows:

- A new account detected
- A change within an existing account

You can treat both cases by defining account and attribute policies for these two types of discrepancies.

Note: To manage an endpoint account attribute with Reverse Synchronization, you must first map the account attribute (see page 58).

How Reverse Synchronization Works

The following table shows the Reverse Synchronization process, depending on the configuration of the Reverse Synchronization policies:

Reverse Synchronization Type	Action in policy	Result	Comments
Account detection	Reject changes	The account is deleted or suspended .	The account is deleted if NEW_ACCOUNT_REJECTED_ACTION =DELETE under Manage Global Settings. **Default:** The account is suspended if NEW_ACCOUNT_REJECTED_ACTION =SUSPEND under Manage Global Settings (for endpoint types that support account suspension).
Account detection	Send to business engine processing	A workflow process is initiated.	If the approver rejects the task, the account is rejected. If the account was not correlated and if the approver accepts the task, the account is assigned to the default user and is no longer detected as a new account. If the account was not correlated and the user selects another user to which he "assigns" the account, and the approver accepts the task, the account is assigned to the user manually selected in the task and is no longer detected as a new account. If the account was automatically correlated (suggested correlation that needs approval) and if the approver accept the task, the account is assigned to the automatically correlated user and is no longer detected as a new account.
Account Detection	Create User	A new corporate user and global user are created based on the	The new user's attribute values, such as first name, last name, and so on, are defined in the Provisioning Server configuration (attribute mapping).

		account detected.	
Attribute change detection	Reject changes	The value in the Identity Manager user store overrides the value in the endpoint.	This is true for any account attribute or HR attributes, such as department or site.
Attribute change detection	Send to business engine processing	A task, usually associated with workflow, is initiated.	The workflow process is the same as if the value was changed in the User Console.
Attribute change detection	Accept	The value is updated in the user store.	No task is initiated.

Account Policy Management

Account policy management allows you to define next steps if a new account is detected on an endpoint.

Assume that a user has created a few new Active Directory accounts in several OUs in the corporate domain. You can detect these accounts and decide how to handle them using Reverse Synchronization account policies.

You can do the following using Reverse Synchronization:

- Configure a policy to reject or send to workflow any new noncorrelated accounts.
- Configure a policy to reject or send to workflow any new correlated accounts.
- When an account is sent to workflow, you can reject it (delete/suspend it from the endpoint).

- When an account is sent to workflow, you can accept it (so that it will not be detected next time).
- When an account is sent to workflow, you can manually assign it to a selected user in User Console.

Note: When an account is sent to workflow, you can send an email to the approver.

Create Reverse Synchronization Account Policies

If you want to define a process for when a new account is detected on an endpoint, create an account policy.

To create an account policy

1. Under Reverse Synchronization, define a new account policy.
2. Enter the following parameters:
   - Endpoint Type
   - Endpoint
   - Is Correlated—if set to YES, this parameter specifies that a matching user was found in CA Identity Manager
   - Status—always set to New
   - Container—the container the detected account resides in (for hierarchical endpoints only)
   - Priority—the priority of selection. The most relevant policy is the one with the highest priority.

     Priority is important when you use a wildcard in the policy parameters, such as Endpoint=*. A Priority=2 policy is run instead of a policy with Priority=1.

     Note: Only *one* policy will run.
3. Select one of the following Actions:
   - Reject changes—the account is deleted or suspended, depending on what is specified in the Manage Global Settings task, under the NEW_ACCOUNT_REJECTED_ACTION parameter. Possible values are DELETE or SUSPEND.
   - Create User
   - Send to business engine processing—the account needs approval by the predefined approver, where the attribute is |ReverseNewAccountDefaultAnswer| and the value is the value of the account's endpoint (ActiveDirectory, RACF, Microsoft SQL Server).
4. Click Save.

Attribute Policy Management

Attribute policy management allows you to define next steps if a discrepancy is found between existing endpoint accounts and their known values in CA Identity Manager.

Unlike account policies, attribute policies do not have dedicated workflow. Instead, they use the native Option Pack Workflow processes.

Any account attribute in an endpoint account can be managed by Reverse Synchronization, as long as it is defined in the attribute mapping (see page 58) of the Provisioning Manager.

Create Reverse Synchronization Attribute Policies

To define a process for when a discrepancy is found between existing endpoint accounts and their known values in CA Identity Manager, create an attribute policy.

To create an attribute policy

1. Under Reverse Synchronization, define a new attribute policy.
2. Enter the following parameters:
   - Endpoint Type
   - Endpoint
   - Attribute—mandatory and case sensitive, must be physical name
   - Priority

   The values can be wildcards, such as Endpoint=*.

3. Select one of the following Actions:
   - Accept changes—updates the account information in the user store without creating a task.
   - Reject changes—the value stored in the user profile (as it is shown in the Manage User Account task in CA Identity Manager) overrides the value in the endpoint.
   - Send to business engine processing—(sent to CA Identity Manager) the value triggers a relevant workflow process, based on the defined process for this attribute for a regular (non-Reverse Synchronization) request. For example, Active Directory group grp1 is defined to be approved by the user's manager when a user requests this group from the Manage Active Directory Accounts task. If there is a discrepancy due to grp1 being added to the user manually, the Send to business engine processing option forces the user's manager to approve this value.
4. Click Save.

Map Endpoint Attributes

Every endpoint account attribute that you want to manage with Reverse Synchronization must be mapped to an available custom attribute. To identify which attributes to manage, go to Option Pack, Account Management, Acquire Endpoint Types, select the endpoint, and check the Current attributes table.

To map endpoint attributes for Reverse Synchronization

1. In the Provisioning Manager, do the following:
   a. Click Endpoints.
   b. Search on endpoint type and double-click the endpoint type you want to manage.
   c. Go to the Attribute Mapping tab.
   d. Check Use custom settings.
   e. Click Add to add a new custom attribute.
   f. Select an available custom attribute. For example, use CustomField 10 if it is not mapped to another user attribute in your environment.
   g. Map the custom attribute to the account attribute name that you want to manage.

      Note: To identify the account attribute name of the attribute you want to manage, go to Option Pack, Account Management, Acquire Endpoint Types, select the endpoint, and use the Account attribute name for the attribute under the Current attributes table. For example, the account attribute name for ADGroups is groupMembership.

h. Click Ok.

i. Repeat Steps e through g to add mappings between all account attributes required and the custom attribute selected.

   Use the same custom attribute (CustomField 10 in our example) for all attributes you want to manage.

j. Click OK.

k. Run Explore on the endpoints without Correlation.

2. Go to Option Pack, Account Management and run Initialize Endpoint Accounts.

   This repopulates the user store attributes with the new endpoint attribute data.

Search for Existing Account and Attribute Policies

You can search for existing policies by the following criteria:

- Endpoint Type/Namespace
- Endpoint
- Container—account policies only
- Attribute—attribute policies only
- Status—account policies only, such as new account
- Action—Send to business engine processing or Reject
- Priority—if you use the asterisk wildcard in your policy, the highest priority prevails over the lowest

Run a Reverse Synchronization

After creating Reverse Synchronization policies for account detection and attribute discrepancies, you can launch Reverse Synchronization.

Reverse Synchronization can be scheduled or submitted immediately.

To start a Reverse Synchronization

1. Under Option Pack, Reverse Synchronization, Schedule Reverse Synchronization, enter the following parameters:

   Provisioning Server Domain Name

   Defines the provisioning domain in CA Identity Manager. This parameter auto-populates.

   Administrator Name

   Specifies the provisioning administrator name.

   Administrator Password

   Specifies the provisioning administrator password.

   Endpoint Type

   Defines the endpoint you want to synchronize with.

   Directory

   Defines your directory. Alternatively, you can select ALL.

   (Optional) Organization Unit

   Defines the OU for hierarchical endpoints.

2. (Optional) Define a schedule for the task.

   Note: Reverse Synchronization is a resource-intensive operation. We recommend running Reverse Synchronization for a subset of directories and OUs during an inactive time of day.

3. Click Submit.

   Note: If you defined a schedule, the Reverse Synchronization occurs at the appointed time. If you do not define a schedule, the task runs immediately. In both cases, the task will appear as submitted, but this does not indicate that the task has completed.

After Reverse Synchronization is finished, you can inspect the log file to see any discrepancies found between Identity Manager accounts and attributes and the actual endpoints. The Reverse Synchronization log file is in the Option Pack folder under /logs/reverseXXX.log.

Any approvals generated by the Reverse Synchronization appear under Option Pack, Workflow, View My Work List. If an approver does not select a user in the Assign account to user field, the account is assigned to the default user. If the Assign account to user field is already populated in the approval task, the account was correlated with the user shown in this field.

Reverse Synchronization Recovery

Reverse Synchronization is subject to heavy load and must recover from sudden system outages. The following features prevent data loss and enhance performance:

- Reverse Synchronization recovery table

  When Reverse Synchronization runs, all the names of accounts modified in the target system are stored in the IDF_Reverse_Recovery table. If the system fails, the next Reverse Synchronization run continues the processing for all the accounts still left in the table.

- Additional attributes table

  Some attributes are likely to change every day, such as Windows Last Login. As a result, the Reverse Synchronization becomes heavily loaded with new data. If you declare these attributes in the IDF_Reverse_Additional_Attr table, they become optimized. The optimized attributes will not slow down the Reverse Synchronization, but the new data will be taken from the target system.

Chapter 8: Scheduled Tasks

This section contains the following topics:

Overview

Scheduled Tasks allow you to perform the following functions:

- Launch a task related to date-based attributes such as termination date, hire date, and so on.
- Launch a task that runs periodically, such as every Saturday.
- Bulk user changes, such as modifying all users within a selected department.

Schedule a Task

Note: If you have multiple Identity Manager environments, a scheduled task created in a specific environment, such as neteauto, only triggers for that environment.

To schedule a task, go to Scheduled Tasks, Submit Scheduled Task, and define the following components:

Scheduled Task Name

Defines the name of the scheduled task. This name can be any name.

Task to perform

Specifies the task to perform. This task list includes all tasks in your system, except the following:

- Tasks where the managed object is not a user (such as modify group)
- Self-service tasks (such as Change My Password)

- Tasks of type View or Create (such as View User and Create User)
- Approval tasks

Optional Attributes

Defines a list of attributes and their set values, for any user that matches the search criteria. These optional attributes are useful with tasks that involve attribute changes, such as Modify User. For example, you could select Department Name as the attribute and 'Sales' as the value, and for every user who matches the search criteria, their Department Name attribute is changed to Sales.

Note: Optional attributes selected must *not* be read-only.

Search Filter

Allows you to select the users for which the task applies. You can define multiple conditions to the filter by defining the following three fields:

- Attribute
- Operator
- Value

This filter can be used for date-based searches. The value acts as a date offset and all dates filtered against will be in the past. For example, if today is the 22nd of the month and you select the attribute Hire Date, set the operator to Before today (in days), and set the value to 5. This filter matches all users who were hired 5 days ago and before. Alternately, you can select Termination Date, set the operator to After today (in days), and set to the value to 20. The filter now matches all users whose termination date is the 12th of the next month or lower.

Also, for an RDB user store, the attribute can be defined as a "date" type for better performance.

Note: The date format is defined under Option Pack, System, Manage Global Settings, General.

Define Schedule

Defines the scheduled time, such as daily, monthly, or a specific date.

Note: Any scheduled task can be submitted immediately by clicking Submit.

Scheduled Task Recovery

The scheduled task process queues all users that meet the search criteria in the IDF_UserBatch table. Once the scheduled task is run against a user, the user is removed from the User_Batch table. This queue mechanism provides for a recovery feature that runs automatically every 9 minutes. If a scheduled task is prematurely stopped before it runs through all matched users, the recovery feature restarts the process where it left off in the table.

If you want to stop an existing batch sent by Scheduled Tasks, you can remove the relevant entries from the IDF_Batch table.

Note: Scheduled Task Recovery can be enabled and disabled in the Option Pack Global Settings. It is enabled by default.

Relate Tasks to Date-Based Attributes

CA Identity Manager treats all attributes as strings or multi-valued strings. The Option Pack allows you to treat an attribute as a date for use with scheduled tasks. Any attribute can be declared as a date. By doing so, the Scheduled Task engine no longer compares values as strings, but as dates.

Example

You must create an automated process to disable temporary users twenty days before their termination date.

1. Go to Scheduled Tasks and create the new scheduled task Disable Contractor.
2. Set Task to perform to Disable User.
3. Enter the following values in the search filter:
   - Attribute: Termination Date
   - Operator: Before Today (in days)
   - Value: 20

   You can add any other attribute in the search filter, such as Employee Type = Contractor. In this case, only contractors are affected.

Note: If your search filter includes date-based attributes, such as Termination Date, we recommend populating only users with relevant values. For example, do not populate users that have no Termination Date, as this can negatively impact performance.

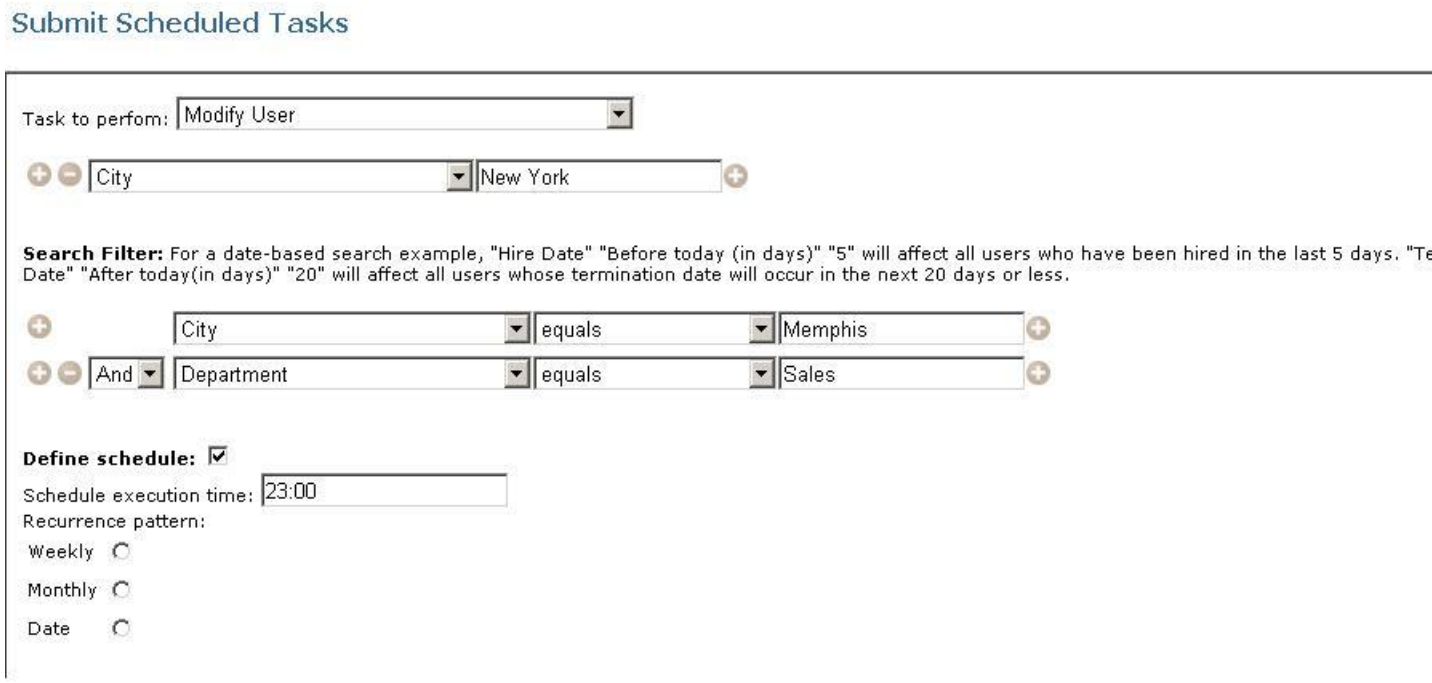
Batch User Changes

You can modify a population of users at once using a scheduled task. This bulk change task can run at a particular date and time, or it can reoccur periodically.

Example

An SAP job code name was modified from "VAX 2P2" to "V4X 1V5" in the SAP system. CA Identity Manager must update this change for a selected user population. The task is to be scheduled to run at 11 PM that same day for the user population in Los Angeles. To configure a bulk user change task, do the following:

1. Select Modify User or Modify User through Approval task.
2. Select the attribute or attributes you want to change for the selected population.
3. Build a search filter that corresponds to the user population you want to modify.
4. Schedule the task.



Chapter 9: Segregation Of Duties (SOD)

This section contains the following topics:

Overview

Segregation Of Duties (SOD) ensures that no user has access over two or more phases of a transaction, so that a deliberate fraud is less likely to occur.

Currently SOD works in a Detect mode. More advanced SOD works in a Detect & Remediate mode, however advanced SOD has the following limitations:

- It only identifies in-process SOD violations. Someone may have already misused the system and caused damage.
- Remediation requires costly manual configuration.

The Option Pack SOD feature prevents the violation from occurring at all, rather than allowing the violation to happen and then remediating it.

SOD provides the following features:

- Identifies and prevents a violation between two newly requested accounts
- Identifies and prevents a violation between a newly requested account and any existing accounts the user already has
- Holds a SOD rules or connects to an existing SOD rules table (if available)
- Analyzes across applications and systems
- Integrates SOD analysis and prevention with the approval and provisioning processes
- Provides a real-time view of current SODs
- Reports SOD audit information periodically
- Provides attribute-level SOD analysis, such as SAP role level, Active Directory group level, and so on

Important! SOD should be audited to regulate when it was approved, by whom, and for what purpose. The SOD process always occurs *before* workflow approval.

Create an SOD Rule

To use the SOD feature in the Option Pack, define SOD rules.

To create an SOD rule

1. Under Option Pack, Segregation of Duties, Manage Segregation of Duties, click Define New Sod.
2. Enter the title and description.
3. Select one of the following actions:

   Accept

   Writes the SOD event to the SOD audit tables, and continues to possible workflow approvals

   Reject

   Denies the SOD conflict and writes the event to SOD audit tables, *and continues* processing the task

   Workflow

   Sends the SOD event to a designated approver. If approved, it continues on to regular approval processes. If rejected, no further workflow processes are triggered.

   RejectAll

   Denies the SOD conflict and writes the event to SOD audit tables, *and stops* the task

   The difference between RejectAll and Reject is as follows: SOD works at the attribute level, meaning that it identifies a potential violation between two different attributes. However, an access entitlement request may include four different Active Directory groups and three RACF roles. It may be that only one RACF role generates a violation. If Reject is selected, only the RACF role generating the violation is rejected and the other four Active Directory groups and two RACF roles continue on to the normal approval process. If RejectAll is selected then all the requests, including all four Active Directory groups and the three RACF roles, are rejected and the task is stopped.
4. Add at least two SOD items by defining conflicting entitlement values.

   An SOD item is defined by its endpoint (such as Active Directory or HR_endpoint), the entitlement name, and value.
5. Click Save.

Search for Existing SOD Rules

You can search for existing SOD rules with the following criteria:

- SOD Id—identifier of the SOD object
- Message—short description of the object, which appears in the SOD audit
- Description—long text that fully describes the SOD object
- Item Id—embedded within the SOD object
- Endpoint Type—endpoint type such as RACF or HR_endpoint for non-system attributes
- System Name—a subsystem
- Entitlement name—attribute name

SOD Violations

The audit engine writes every SOD violation to its tables. Even if the SOD violation was approved, rejected, or partially rejected, it is audited for potential further analysis. You can search by any audit criteria, such as endpoint or user name approver.

Once your search criteria is submitted, you see all matching SOD entries, who approved them or rejected them, and the reason for approval or rejection. If you click the SOD Id, you see the entry's detailed information, including description, action, and conflicting items.

SOD Process Example

At run time, any request, such as a task or Reverse Synchronization, is checked for an SOD violation.

Example

According to the SOD rules, a person cannot be a member of the RACF group grp1 *and* a member of the Active Directory group Administrator at the same time.

Therefore, if the user requests RACF group grp1 and Active Directory group Administrator at the same time, a violation is triggered. The SOD engine looks up all the SOD rules, as defined, for the action taken, such as Reject or Workflow.

If the user is already a member of the Active Directory group Administrator, and their manager decides to add them to RACF group grp1, the same violation is triggered and the same action lookup takes place.

If the SOD rule action is Workflow, the SOD approver gets an approval task. Any SOD approval requires a reason for approval or rejection.

Chapter 10: Option Pack Workflow

This section contains the following topics:

Overview

Option Pack Workflow supplies more flexibility and fine-grained control of an approval process. This feature does not replace Identity Manager Workflow, but enhances it using the WorkPoint engine. Identity Manager workflow deals with approving events, while Option Pack Workflow deals with approving attribute values.

Option Pack Workflow is a bridge between CA Identity Manager and WorkPoint workflow. It serves as an interpreter for a request, and can work with WorkPoint in a more granular way than CA Identity Manager alone.

Option Pack Workflow provides the following features:

- Process Separation

  With Option Pack Workflow, a single approval task can be broken into multiple independent approval tasks, each with its own set of approval logic, screens, WorkPoint processes, and more. There is no dependency between the different processes, so each process can be approved or rejected without affecting the other processes.

- Value Separation

  Approval is defined at the value level so that each new entitlement a user gets, depending on if it is an account value (SAP roles) or a Human Resources value (pay grade), is sent to a different approver. Each approval task can be approved or rejected separately, resulting in the ability for partial approval.

- Aggregation of Approval Tasks

  While an approver can get several approval tasks to approve under the same process, all approval tasks are aggregated into a single approval action.

- Delegation

  Option Pack Workflow supports the following two types of delegation:

  - Out-of-Office Delegation—allows an approver to set a replacement while they are away
  - On-Task Delegation—a particular approval task is delegated to a different approver after it is assigned

- Time-based Escalations

  Approval tasks can be set to escalate after a certain period. An escalator is assigned to the approval tasks that the former approver should have approved.

How to Configure Workflow

Perform the following steps to configure Option Pack Workflow.

1. Configure a workflow process.
2. Define approvers for approval tasks.
3. Create an approval task that approvers can use to view their work items.
4. Create a WorkPoint process. The Option Pack Workflow uses a WorkPoint process to trigger the task for the approver's to do list.

Configure a Workflow Process

To configure a workflow process

1. Under the Option Pack tab, go to Workflow, Manage Workflow, and click Define new workflow config.
2. Define the Triggering Attribute and Target Attribute (see page 73) as appropriate.
   - Triggering Attribute—the attribute that is changed
   - Target Attribute—the attribute that receives the approved value
3. Select Yes if the Target Attribute is physical.

   The target attribute is usually a physical attribute. There are examples where a change in a certain attribute is only the trigger to a manual step required. In this case, there is no need to write the approved value to a physical attribute, and a logical attribute can be used instead.

4. Select Yes if the Target Attribute is multi-valued.

   Note: Resource attributes controlled by the Option Pack (such as Active Directory groups, SQL roles and more) are always multi-valued. This is because there may be multiple instances of the same value across several accounts. For example, the Active Directory home folder is a single value for an account, but because there may be more than one account, each account may have a different value, making the Active Directory home folder a multi-valued attribute.

5. Enter the unique name of the WorkPoint Process (see page 81) where the name of the approval task is configured.

Note: This configuration is environment-specific. The default configurations are shared across all environments, but new settings *only* affect the environment they were created in.

Example: Triggering Attribute and Target Attribute

The following use cases show examples of how to set the Trigger and Target Attributes when configuring an Option Pack Workflow process (see page 72).

Example:

A user needs to set up approval for any SAP roles requests. Whenever an SAP role changes, the changes must be approved. In this case, both the trigger attribute and the target attribute is the SAP roles attribute.

Example:

A user needs to set up approval for SAP roles requests, triggered from custom code. A logical attribute handler is set in place to manage the SAP role request, and is separated from the physical attribute. In this case, the logical attribute is the trigger and the SAP roles physical attribute is the target. New values are added to the logical attribute, and once approved, they are automatically copied over to the physical attribute.

Note: Throughout the configuration, the target attribute is used as the key for the process.

Default Check Boxes

These settings are used to define custom, advanced approval logics. These settings should only be changed after careful consideration.

Define Approvers for Approval Tasks

Define approvers to approve or reject work items.

To define approvers for approval tasks

1. Go to Option Pack, Workflow, Manage Workflow and click on Define new workflow approvers and escalators.
2. Fill in the following fields:

Attribute

Defines a list of target attributes pre-defined in the workflow configuration screen. The target attribute is the key to the process and approvers are assigned to it.

Note: If there are multiple processes pointing to the same target attribute, there is no need to copy the approvers' configuration for each process, since the approver is defined by the target attribute.

Attribute Value

Specifies a string with wildcards for deciding which value requires approval.

Sequence Order

Defines the step of the approval, starting from 1 and increasing. If the request needs to be approved in parallel by two approvers, set the sequence order to 1 for both approvers. For sequential approvals, set the sequence order to 1 and 2.

Note: Do not skip sequence numbers. For example, do not set the first approver to a sequence order of 1 and the second approver to a sequence order of 3. This will cause workflow to fail.

Approver type and Name

Defines the type of approver. Several default workflow resolvers are available, as follows:

- Name
- Manager
- Group
- AdminRole

- AccessRole
- Attribute

Escalator Type and Name

Define the escalators for the Attribute Value in case of a time-based escalation. The escalator resolvers are identical to the approvers' resolver, with one additional option:

ManagerOfApprover—Sets the approver to the current approver's manager. Since this is dynamic, this will result in the approval moving higher and higher in the hierarchy each time the previous approver fails to approve in time.

3. Click Save.

How Approval Tasks are Triggered

An Option Pack Workflow approver is defined at the value level. For a specific process, the new values added are checked against the approvers' configuration, and each results in an approver if necessary. New values are those that are now in the triggering attribute and do not yet exist in the target attribute (before the change).

A triggering attribute starts a workflow process and the target attribute starts the approver selection. For example, if attribute RACF group is defined as a triggering attribute and there is a change in RACF group for a selected user, a defined workflow process starts.

During the approval chain, an approver may reject some of the groups requested. The target attribute will hold the accumulated approved values until the chain of approval completes.

Note: Deleting a value from an attribute does *not* trigger a workflow process.

Example

There is an Active Directory group approval process configured. The ADGroups attribute is both the trigger and the target. Two new groups are added to the user. These groups are now in the trigger (ADGroups attribute) which starts the workflow process, but are not in the target (ADGroups again, before the change). Therefore, these two new groups are recognized as new values, and are checked against the approvers' configuration.

Example

There is a logical attribute to which new Active Directory group values are added. This is the trigger to the Active Directory workflow process. The target is the ADGroups attribute, which is synchronized with the endpoints. Adding two groups to the logical attribute will cause the workflow to trigger. Those groups may or may not already exist in the ADGroups physical attribute, so only those that did not exist are checked.

Attribute Value and Sequence Order

Both the Attribute Value field and the Sequence Order field are keys for the approval setting. The value can be either a specific value or a wildcard. Every new value added to the attribute is checked against all approvers' configurations to see if any match the pattern. If so, the approver is added to the list.

Attribute Value

Setting the Attribute Value to "Admin*" means that all new values starting with Admin require approval by the defined approver. Therefore, adding the three values “Administrator”, “Administration Officer”, and “Manager” results in the first two requiring approval.

A value may be defined in multiple settings. This results in several approvers having to approve the same value. A value is considered to be approved only if approved by all who were resolved for it, and rejected if any have rejected it.

In addition, a single approver may be resolved for more than one value, either by having to approve a range of values (like “*”) or by showing in multiple settings. All values which a single approver must approve is concatenated into a single approval task opened for that approver. They are then able to partially approve the request.

Note: Values that are requested and do not match any approver settings are considered to be approved and are updated automatically in the user's record.

Sequence Order

The sequence is used to define sequential approval steps. The order starts with 1, being the first approver that must approve the value. After a value is approved by all sequence 1 approvers, it is checked against sequence 2, and so on.

The approvers are recalculated every time a value is moved into a new sequence. This happens at the beginning of the request when entering sequence 1, or when a value is approved by all approvers needed at a specific level, and is now checked against the next level. Only approved values pass on to the next sequence.

Because the approvers list is dynamically calculated, changes to the setting while an approval is running may affect the flow of the approval.

Note: A value may require approval at sequence 1, but not at sequence 2. This would mean that the value is approved, even if the rest of the values continue in the process.

Example

There are two approvers defined in the system, one to approve all values for the attribute at sequence 1, and the other to approve a specific value at sequence 2. This means that the first approver (for example, the manager) must approve all values requested for the user. If the value for which the second approver is configured has been approved, then it must be approved again, this time by the second approver. All other values approved at sequence 1 that do not require further approval are updated in the user's record.

The combination of the value and the sequence is what defines parallel and sequential approval.

Approver Type and Name

The Option Pack has several default workflow resolvers. To define an approver, the type must be set first. The name field is context sensitive and changes according to the type which is selected. Also, all values provided in the name field are case sensitive.

Note: Settings in this configuration screen refer to usage of the default approval logic. Any change to the logic may lead to those values being ignored or treated differently.

Possible resolver types are as follows:

Name

Defines the user ID for the approver. For example, when selecting Name as the approver type, the "superAdmin" value can be set in the name field. This results in the superAdmin being the direct approver for the selected value.

Manager

Defines, automatically, the manager of the user who has changed to be the approver.

Group

Specifies that all members of the group get the approval notification, while only one must approve or reject the values. This field requires the name of a group defined in CA Identity Manager.

AdminRole

Specifies that members of the Admin role get the approval notification, while only one must approve or reject the values. This field requires the name of an admin role in the Identity Manager environment.

AccessRole

Specifies that all members of the role get the approval notification, while only one must approve or reject the values. This field requires the name of an access role in Identity Manager environment.

Attribute

Resolves the approver using a search. The search uses a single-valued attribute from the user (such as managerId) as the User's attribute and searches for all users who have the same value in the Approver's attribute (such as the %USER_ID%). Multiple users may be returned by the search, resulting in a behavior similar to a group.

Example

Approvers can be set as responsible for a particular department. The name of the department (or departments) is written to an attribute called approverForDepartment.
An attribute resolver setting defines the User's attribute as departmentNumber and the Approver's attribute as approverForDepartment. The result is that the approver becomes the person responsible for the user's department.

Set Time-Based Escalations

Every approval task using Option Pack Workflow is subjected to checks for timeouts. Once a task pending for an approver times out, all values under their approval are marked as escalated. New approvers are assigned according to the resolution. There can be more than one escalator resulting from the list of values, in which case multiple new processes are opened and the values are split between them.

Note: Calculating escalators is identical to calculating approvers. All rules that apply to the approvers apply here too (such as concatenation of values).

Option Pack Workflow has a default timeout setting of 15 minutes. This timeout can be changed for each process in particular, or for all approval tasks. All timeout settings are done using the WorkPoint designer.

Change the global escalation timeout

1. In WorkPoint Designer, open ACEDefaultProcess.
2. Click the first step, Approver ###.
3. On the Alerts tab, click ACE_triggerEscalation on the left side.

4. Go to the Evaluation Date tab and change the time setting to the necessary value.
5. Save all items, including the process.

Note: This change affects all Option Pack Workflow processes which were not assigned with a unique escalation timer. All escalation settings affect *only* Option Pack Workflow processes.

Set a specific time-based escalation

1. In WorkPoint Designer, open the appropriate process.
2. Click the first approval step.
3. On the Alerts tab, select New.
4. Provide a Name and click OK.
5. On the Evaluation Date tab, set the time by using a system calculated time, or by using your own script.
6. On the Condition tab, select Conditional and select the ACE_escalate script.

   The evaluation date is determined by the length of the escalation time. For minute intervals, a 1 minute evaluation time is recommended.
7. Save the new alert and move it to the right, in place of the ACE_triggerEscalation alert.
8. Save the process.

Create an Approval Task

For an approver to be able to view a work item and perform actions accordingly, define a task in CA Identity Manager. These tasks must include required elements that are used in Option Pack Workflow, but are otherwise free to be configured as desired.

Create an approval task

1. Log in to the User Console as a user with permission to create Admin tasks.
2. Go to Roles and Tasks, Admin Tasks, Create Admin Task and select Create a copy of an admin task.
3. Search for the Approve default task, select it and click OK.
4. Specify a unique task name.
5. Click Business Logic Task Handlers at the bottom of the page.
6. Select WorkflowGetApprovalValue.

7. In the Business Logic Task Handler, remove TARGET_ATTRIBUTE and re-add it using the new name of the target attribute you selected configuring an Option Pack Workflow process (see page 72).
8. Save the new task and verify that it was created successfully.

Optional: Add the new task to the approver role. This is a role given to all users, which allows them to perform Option Pack approval tasks. The task can also be added to other roles. Be sure the role to which the task is set has the appropriate scope for the delegation user search.

Create a WorkPoint Process

Option Pack Workflow triggers the WorkPoint process specified when it needs to send an work item to the desired approver.

Creating a WorkPoint process

1. In WorkPoint Designer, open the process named ACEDefaultProcess.
2. Save this process with a different name. This is the name you use when configuring the Option Pack Workflow process (see page 72).
   Note: Do not change the original process; it can be used for future process creation.
3. Click the first step, Approve ###.
4. Change the name of this step in the process. This is the name shown in the approver's To Do list, so it must be meaningful to the process.
5. Go to User Data and update the value of the TASK_TAG to the name of the approval task (see page 80) you created.
6. Save the process.
7. Restart the application server.

Note: If there are multiple environments, a single process can be used by two workflow configurations running from the different environments. However, because the approval task name is mentioned in the WorkPoint process, create the approval task in both environments, using the same name.

Chapter 11: Delegation

This section contains the following topics:

Overview

All Option Pack Workflow processes support the following two types of delegation:

- Out-of-office delegation—An approver can set a time period during which their approval tasks are routed to other approvers. This affects approvals assigned to the user in the time frame specified, and only approvals assigned to the user after the delegation setting has been activated.
- On-task delegation—Once the user is assigned an approval task, they can then choose to assign it to someone else in their place. This applies to a particular approval task which is already assigned to the approver.

Delegation is supported for Option Pack Workflow processes only.

Set an Out-of-Office Delegation

Out-of-Office delegation is a self-service task under Option Pack tab, Workflow. A user needs to have the approver role to use this functionality.

To set an out-of-office delegation, specify the process, name an approver, and define a data range.

Set an out-of-office delegation

1. Under the Option Pack tab, go to Workflow, Out of Office.
2. Fill in the following fields:

   Selected delegation

   Defines the process to delegate. The list of processes is taken from the workflow configuration.
   Note: By selecting All, all processes which are assigned to you and do not have a more specific setting are selected.

   Selected person to assign to

   Defines a user to whom you want to delegate.

Delegation start date

Defines the start date. The start date is automatically populated with today's date, but can be changed. A future start date is also possible, allowing the approver to set the date to a few days before going on vacation, for instance.

Delegation end date

Defines the end date. This date must be later than the start date.

3. Click the update check box.

   The delegation appears in the Your active delegations list.

Note: Out-of-Office delegation is recursive, meaning that if you are delegating to someone and that person is delegating to someone else, requests assigned to you are routed to the third approver instead of the one you specified. A checking mechanism prevents loops, so if an approver is delegated to an approver already on the list, the delegation stops and the request remains with the last person on the list. For example, user 1 is delegating to user 2 and user 2 is delegating to user 1. A request assigned to user 1 is routed to user 2, because they are delegating to an approver already on the list (user 1).

Perform On-task Delegation

On-task delegation is done in real time by the approver.

For an approver to delegate their approval task to another approver, they must open the approval task, select a person from the delegation search and click Approve or Reject. The result is that the task is routed to the person selected, pending a check on the selected person's out-of-office delegations.

If no users are returned by the search for delegation, then the task is probably not associated with a role that has a sufficient scope. Add the approval task to the Option Pack approver role.

Appendix A: Maintenance

We recommend periodically backing up and cleaning the following tables:

- IDF_AceDataAudit
- IDF_Reverse_Recovery
- IDF_ReverseAudit
- IDF_SODAudit
- IDF_SODAuditEntitlements
- IDF_SODAuditItem
- IDF_StateAuditActionParams
- IDF_StateAuditActions
- IDF_StateAuditPolicies
- IDF_UserBatch
- IDF_WorkpointJobs
- QRTZ_JOB_DETAILS

Appendix B: Troubleshooting

This section contains the following topics:

Account Management

The following section covers troubleshooting topics related to Account Management.

Nothing Appears in the Account Management Screen

Symptom:

When I open my account management screen, nothing shows up.

Solution:

Be sure that the selected user has at least one account in the selected endpoint type.

Only the Account Name Appears on my Account Management Screen

Symptom:

Only the account name appears on my account management screen.

Solution:

Try one of the following:

- Be sure to run Initialize Endpoint Accounts for the selected endpoint type. This populates the values of the endpoint attributes for all users.
- Be sure the program exits work and that inbound notifications are enabled. Also, verify that the method in the SOAP exit definition is InvokeExit.

Available Values in the Account Screen are Empty

Symptom:

Available values in my account screen are empty.

Solution:

Be sure to remove Set Filter and replace it with your own filter, then click the Apply filter check box. If no values appear, create a more general filter to return more values.

Not All Values in the Endpoint Appear in the Available Values

Symptom:

Not all values visible in the endpoint system appear in the available values.

Solution:

Be sure to explore the endpoint after creation of groups or roles in the endpoint system.

Email Notifications

The following section covers troubleshooting topics related to Email Notifications.

No Email was Sent

Symptom:

No email was sent after configuring email notifications.

Solution:

Try one of the following:

- Be sure that your SMTP settings are properly configures. For more information about CA Identity Manager SMTP settings, see the *CA Identity Manager Installation Guide*.
- Be sure that there is a value in either the TO or CC field. Also, be sure that the specified email, group, or role member exists.

Email not Sent to Approvers

Symptom:

An email was not sent to the approvers.

Solution:

Be sure that you set the When to Send field to Workflow Pending. Also, be sure that if the workflow process is not an Option Pack workflow process, that the Policy Xpress workflow listener is set.

Policy Xpress

The following section covers troubleshooting topics related to Policy Xpress.

Cannot Import Policies

Symptom:

I cannot import policies into Policy Xpress.

Solution:

Check the XML parser to find the line that is failing. Correct the XML file and restart the import.

Only One Action Rule Triggered

Symptom:

Only one of my action rules triggered, but more than one rule matches.

Solution:

This behavior is correct. Only one action rule executes, based on the matching rule with the lowest priority.

Reverse Synchronization

The following section covers troubleshooting topics related to Reverse Synchronization.

Reverse Synchronization is not Working

Symptom:

Reverse Synchronization is not working properly.

Solution:

Verify the following:

- Be sure that the accountforapproval user exists in both the user store and Provisioning Directory. Note the user ID is case sensitive.
- Be sure that your inbound synchronization is working properly. Go to the Provisioning Manager and change any user's mapped attribute, such as first name. Search for this user in CA Identity Manager and be sure that the first name was updated accordingly. If not, enable notifications and verify the configuration of the CA Identity Manager setup (ETAcallback).
- Be sure that the Provisioning Modify User task has run and is completed by checking View Submitted Tasks (VST). For orphan account detection, the user is accountforapproval. If the task is pending in VST, see who the current approver is and approve the task.
- Be sure that the ReverseSyncTrigger attribute is mapped to correctly (by default, custom field 09) in the Provisioning Manager, the Management Console, and in the Option Pack Global Settings.

A Defined Workflow Approval Process is Failing

Symptom:

A workflow approval process that you defined is not working.

Solution:

Be sure that the approver defined in the process exists. Check the application server log for exceptions.

Attribute Changes are not Detected

Symptom:

The Option Pack is not detecting attribute changes.

Solution:

Be sure that the attribute is mapped in all endpoint types. Also, be sure that the attribute is part of the endpoint acquisition (see page 22) process.

Business Logic Errors are Occurring

Symptom:

Business Logic errors are occurring.

Solution:

Try one of the following:

- Check the workflow settings related to the errors that are occurring. Also, be sure that Workflow is enabled.
- Be sure that no other inbound tasks are still being processed. Reverse Synchronization requests do not appear until all previous requests are finished.

Unable to Create a New User Based on New Account Detection

Symptom:

You are unable to create a user based on new account detection.

Solution:

Look at the Create User task and be sure that all mandatory field information is being supplied.

Scheduled Tasks

The following section covers troubleshooting topics related to Scheduled Tasks.

The Task Fails to Execute

Symptom:

The task fails to execute.

Solution:

Be sure the user who configured the scheduled task still has access to execute the task.

Time-Based Attributes Not Working

Symptom:

Time-based attributes do not work properly.

Solution:

Be sure the global date format (under Option Pack Global Settings) corresponds to the user store date format. If the global date format is MM/dd/yyyy and the user's date attribute is 02-27-99, the date will not match.

Segregation of Duties (SOD)

The following section covers troubleshooting topics related to Segregation of Duties.

SOD is not Triggered, but Workflow Approval Appears

Symptom:

SOD is not triggered, but regular workflow approval appears.

Solution:

Try one of the following:

- Check if the conflicting SOD rules match the new values. If they do not match, no SOD violations are triggered.
- Be sure to specify the *stored* values and not the displayed values in the SOD configuration.
- Be sure that the conflicting values belong to the correct endpoint type in the SOD rule configuration.
- Check that you specified Workflow as the action of the SOD rule.

No SOD Violations Detected in New Accounts

Symptom:

From a Reverse Synchronization, no SOD violations are detected in the new accounts.

Solution:

This works as designed. Reverse Synchronization automatically sends detected new accounts to approval, even if there is an SOD violation within the new account.

Not Able to Accept or Reject SOD Work Items

Symptom:

I am not able to accept or reject my Approve SOD work items.

Solution:

Be sure to enter a meaningful reason into the Mitigating Control field.

Work Item Appears After SOD Violation Approval

Symptom:

After approving an SOD violation, a work item for approval appears.

Solution:

This behavior is correct. Approving an SOD violation releases the task to workflow approval.

Workflow

The following section covers troubleshooting topics related to Option Pack Workflow.

Workflow is not Working

Symptom:

Option Pack Workflow is not working properly and no approval tasks appear.

Solution:

Try one of the following:

- Check View Submitted Tasks and see if the task is still pending, and to whom.
- Be sure that workflow is enabled for this environment.
- Be sure that you restart your application server after creating your WorkPoint process.
- Be sure that all multi-valued attributes are set correctly in the workflow configuration.
- Be sure the name you entered in the WorkPoint activity matches the workflow approval task created. This name is case sensitive.
- Be sure that the trigger attribute exists and that it was modified. If the attribute does not exist or was not modified, no workflow process is triggered.
- Check your workflow approvers configuration. If no approvers were resolved, something may be wrong with the configuration. Also, a delegation may be active, but the work item was assigned to another approver.
- Check that no sequence number was skipped in the workflow configuration. Check the server logs for more information.

- Check that the values you specified in your approvers and escalators matches the values set in the task.
- Be sure that the approvers do not belong to a different environment than the one you are in.

A Work Item is Created but does not Show the Value to Approve

Symptom:

A workflow work item is created, but it does not show the value to approve.

Solution:

In the approval task definition, be sure to set the TARGET_ATTRIBUTE to be the *physical* name of the attribute you want to trigger your workflow process.

Index

O

P

R

S

T

U

V

W