EVIDEN

Identity and Access Management

DirX Identity

Certification Campaigns

Version 8.10.13, Edition October 2025

Table of Contents

Copyright ii
Preface 1
DirX Identity Documentation Set 2
Notation Conventions 3
1. Overview 5
1.1. Use Cases 5
1.1.1. User Certification Campaigns 5
1.1.2. Privilege Certification Campaigns 5
1.1.3. Certification Campaigns with Risk Governance 6
1.1.4. Continuous Access Certification via Re-approval Workflows 6
1.1.5. Scheduled Access Certification Campaigns via Re-approval Workflows 6
1.2. How a Certification Campaign Works 6
1.2.1. Certification Campaign Pre-Requisites 7
1.2.2. Creating a Certification Campaign 7
1.2.3. Certification Campaign Notifications 7
1.2.4. Starting a Certification Campaign 8
1.2.5. Certifying Users or Privileges 9
1.2.6. Finishing a Certification Campaign 10
1.2.7. Recurring Certification Campaign 10
1.2.8. Generating Reports 11
2. Configuring the Pre-Requisites 12
3. Creating a Certification Campaign 13
4. Starting a Certification Campaign 15
5. Monitoring and Finishing a Campaign 16
6. Customizing with User Hooks 19
6.1. Documentation and Sample Source Code 19
6.2. Select Approvers with a “Find Approvers” User Hook 19
6.2.1. Before – Creating the Certification Task in the User Hook 20
6.2.2. After – Changing Default Attributes 20
6.2.3. Find Approvers – Adding Additional Approvers 20
6.3. Select Campaign Subjects with a “Find Subjects” User Hook 21
6.4. Limit Resources with a “Limit Resources” User Hook 22
6.5. Send emails with the “Send Email” User Hook 23
6.6. Override Campaign Creation with “Campaign Creator” 23
7. Generating Certification Campaign Reports 25
7.1. About the Default Report Templates 25
7.2. Producing a Report 25
7.3. Adding or Extending Reports 25
8. Continuous Certification by Re-Approval 27

8.1. About this Use Case . . . 27
8.2. Setup and Configuration . . . 28
8.2.1. Setting up the Domain Object . . . 28
8.2.2. Setting up the Privileges . . . 29
8.2.3. Setting up the Workflows . . . 29
8.2.3.1. InitializeReapproval . . . 29
8.2.3.2. StartReapproval . . . 30
8.3. Running the Use Case . . . 31
8.4. Alternative or Extended Configurations . . . 31
8.4.1. Certifying Other Privilege Types . . . 31
8.4.2. Running Separate Campaigns . . . 31
9. Scheduled Certification by Re-Approval . . . 32
9.1. About this Use Case . . . 32
9.2. Setup and Configuration . . . 33
9.2.1. Setting up the Domain Object . . . 33
9.2.2. Setting up the Privileges . . . 34
9.2.3. Setting up the Workflows . . . 34
9.2.3.1. InitializeReapproval . . . 34
9.2.3.2. StartReapproval . . . 35
9.3. Running the Use Case . . . 35
9.4. Alternative or Extended Configurations . . . 36
9.4.1. Certifying Other Privilege Types . . . 36
9.4.2. Setting Individual Re-Approval Dates or Re-Approval Periods . . . 36
10. Hints and Limitations . . . 37
10.1. Manual and Automatic Assignments . . . 37
10.2. Certification Campaign Logging . . . 37
10.3. Java-based Server Workflow Load . . . 37
Legal Remarks . . . 39

Preface

This document describes how to set up and run certification campaigns for **users** and **privileges**.

A user or privilege certification campaign does not use request workflows. In the current DirX Identity version, this functionality is visible in configuration settings for **users** and **privileges**. The request workflow-based campaign technique is deprecated and will be removed with the next DirX Identity version.

This document consists of the following chapters.

- Chapter 1 provides an overview of the use cases.
- Chapter 2 describes how to prepare for user/privilege certification campaigns.
- Chapter 3 describes how to create a user/privilege certification campaign.
- Chapter 4 describes how to start a user/privilege certification campaign.
- Chapter 5 describes how to monitor and finish a user/privilege certification campaign.
- Chapter 6 describes how to customize user/privilege certification campaigns with user hooks.
- Chapter 7 describes how to create reports for a user/privilege certification campaign.
- Chapter 8 describes continuous certification via re-approval workflows.
- Chapter 9 describes scheduled certification via re-approval workflows.
- Chapter 10 provides information about hints and limitations.

DirX Identity Documentation Set

The DirX Identity document set consists of the following manuals:

- *DirX Identity Introduction*. Use this book to obtain a description of DirX Identity architecture and components.
- *DirX Identity Release Notes*. Use this book to understand the features and limitations of the current release. This document is shipped with the DirX Identity installation as the file **release-notes.pdf**.
- *DirX Identity History of Changes*. Use this book to understand the features of previous releases. This document is shipped with the DirX Identity installation as the file **history-of-changes.pdf**.
- *DirX Identity Tutorial*. Use this book to get familiar quickly with your DirX Identity installation.
- *DirX Identity Provisioning Administration Guide*. Use this book to obtain a description of DirX Identity provisioning architecture and components and to understand the basic tasks of DirX Identity provisioning administration using DirX Identity Manager.
- *DirX Identity Connectivity Administration Guide*. Use this book to obtain a description of DirX Identity connectivity architecture and components and to understand the basic tasks of DirX Identity connectivity administration using DirX Identity Manager.
- *DirX Identity User Interfaces Guide*. Use this book to obtain a description of the user interfaces provided with DirX Identity.
- *DirX Identity Application Development Guide*. Use this book to obtain information how to extend DirX Identity and to use the default applications.
- *DirX Identity Customization Guide*. Use this book to customize your DirX Identity environment.
- *DirX Identity Integration Framework*. Use this book to understand the DirX Identity framework and to obtain a description how to extend DirX Identity.
- *DirX Identity Web Center Reference*. Use this book to obtain reference information about the DirX Identity Web Center.
- *DirX Identity Web Center Customization Guide*. Use this book to obtain information how to customize the DirX Identity Web Center.
- *DirX Identity Meta Controller Reference*. Use this book to obtain reference information about the DirX Identity meta controller and its associated command-line programs and files.
- *DirX Identity Connectivity Reference*. Use this book to obtain reference information about the DirX Identity agent programs, scripts, and files.
- *DirX Identity Troubleshooting Guide*. Use this book to track down and solve problems in your DirX Identity installation.
- *DirX Identity Installation Guide*. Use this book to install DirX Identity.
- *DirX Identity Migration Guide*. Use this book to migrate from previous versions.

Notation Conventions

Boldface type
In command syntax, bold words and characters represent commands or keywords that must be entered exactly as shown.

In examples, bold words and characters represent user input.

Italic type
In command syntax, italic words and characters represent placeholders for information that you must supply.

[ ]
In command syntax, square braces enclose optional items.

{ }
In command syntax, braces enclose a list from which you must choose one item.

In Tcl syntax, you must actually type in the braces, which will appear in boldface type.

|
In command syntax, the vertical bar separates items in a list of choices.

...
In command syntax, ellipses indicate that the previous item can be repeated.

userID_home_directory
The exact name of the home directory. The default home directory is the home directory of the specified UNIX user, who is logged in on UNIX systems. In this manual, the home pathname is represented by the notation *userID_home_directory*.

install_path
The exact name of the root of the directory where DirX Identity programs and files are installed. The default installation directory is *userID_home_directory*/**DirX Identity** on UNIX systems and **C:\Program Files\DirX\Identity** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathnames is represented by the notation *install_path*.

dirx_install_path
The exact name of the root of the directory where DirX programs and files are installed. The default installation directory is *userID_home_directory*/**DirX** on UNIX systems and **C:\Program Files\DirX** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathname is represented by the notation *dirx_install_path*.

dxi_java_home
The exact name of the root directory of the Java environment for DirX Identity. This location is specified while installing the product. For details see the sections "Installation" and "The Java for DirX Identity".

tmp_path

The exact name of the tmp directory. The default tmp directory is /tmp on UNIX systems. In this manual, the tmp pathname is represented by the notation *tmp_path*.

tomcat_install_path
The exact name of the root of the directory where Apache Tomcat programs and files are installed. This location is defined during product installation.

mount_point
The mount point for DVD device (for example, **/cdrom/cdrom0**).

1. Overview

DirX Identity provides a comprehensive role model to control user access rights to resources in connected systems.Features such as access policies, segregation of duties (SoD) and approval workflows help to secure the assignment of access rights.Compliance requirements require regular certification or re-certification of these assignments.DirX Identity provides several mechanisms to support these compliance processes.

Be aware that certification can only be applied to manually-assigned privileges.Rule-based assignments and the assignments made from business object inheritance are not subject to user/privilege certification campaigns because DirX Identity assumes that a rule or an inheritance definition is designed to make the correct assignments.It is not possible to "adjust" the rule or the inheritance definition later on by manually removing specific assignments.

1.1. Use Cases

This document describes several use cases in detail.Be aware that other use cases are possible that are not described in this document.

1.1.1. User Certification Campaigns

This use case performs a certification campaign for a subset of users, referred to as the **subjects** of the campaign.

The users are selected by applying an LDAP search filter configured for the campaign. By default, all manual privilege assignments must be certified. By implementing a “Find Subject” user hook, customers can implement their own method of finding users for the campaign. The set of privileges to be certified (called the **resources**) can be reduced by configuring an LDAP filter or by implementing a “Limit Resources” user hook.

For each user, one or more approvers are automatically defined. The default implementation selects the user’s manager. A “Find Approvers” user hook can override this setting and select a custom set of approvers per user.

1.1.2. Privilege Certification Campaigns

This use case performs a certification campaign for a subset of privileges, typically roles. In this case, the privileges are the certification **subjects**.

The privileges are selected by applying an LDAP search filter configured for the campaign. By default, all manual user-privilege assignments must be certified. By implementing a “Find Subject” user hook, customers can implement their own method of finding privileges for the campaign. The set of users to be certified (called the resources) can be reduced by configuring an LDAP filter or by implementing a “Limit Resources” user hook.

For each privilege, one or more approvers are automatically defined. The default implementation selects the privilege’s owner. A “Find Approvers” user hook can override this setting and select a custom set of approvers per privilege.

1.1.3. Certification Campaigns with Risk Governance

In addition to certification campaigns above, customers can create certification campaigns for **subjects** with a high risk. If the **Risk Governance** feature is enabled, the customer can extend the LDAP search filter for adding users based on risk values; for example a user certification campaign for the finance department, for users with a high risk, or a privilege certification campaign for the role finance administrator only for users with a medium risk or above.

1.1.4. Continuous Access Certification via Re-approval Workflows

This use case works with DirX Identity's built-in re-approval feature. In this scenario, the approval for selected and critical privileges is repeated at the specified time. You can either run the same workflow that was run to approve the privilege or a specific workflow for re-approval. If the approvers reject the assignment, the privilege is removed from the user. This method works individually per assignment.

You can combine the re-approval of selected privileges with timing conditions. If you run the **InitializeReapproval** and the **StartReapproval** workflows on a daily basis, these workflows check the timing conditions and then start re-approval workflows as necessary.

1.1.5. Scheduled Access Certification Campaigns via Re-approval Workflows

This use case works with the built-in re-approval feature. In this scenario, the approval of all critical privileges is scheduled for a specific time. You can either run the same workflow that was run to approve the privilege or a specific workflow for re-approval. If the approvers reject the assignment, the privilege is removed from the user. This method works individually per assignment. The difference from the previous use case is that the parameters are set to run all re-approvals at the same time. Flag the critical privileges for re-approval and then set the re-approval date at the domain.

In this case, it makes sense to run the **InitializeReapproval** and the **StartReapproval** workflows only once at the correct time to start all re-approval workflows in parallel.

1.2. How a Certification Campaign Works

This section describes some technical details that help to understand the certification campaign use cases. First we describe how the feature works and which components are involved. Next, we explain how all these components are integrated in the system and how to calculate the certification campaign end date.

You can skip this section and read it later on if you need deeper understanding of this fairly complex feature.

Several processes are necessary to perform a certification campaign in DirX Identity. They are described in the following sections.

1.2.1. Certification Campaign Pre-Requisites

A certification campaign has the following DirX Identity configuration pre-requisites:

- **Certification Campaign Controller workflow** (called the campaign controller) – this workflow needs to be active, needs a schedule so that it runs at least once per day and must be deployed on exactly one Java-based Server (resource family Certification Campaign).
- **Email service** – the campaign controller sends various notifications during the campaign and relies on the general email service to be configured correctly.

1.2.2. Creating a Certification Campaign

A certification campaign administrator creates a campaign entry in state **Campaign is in preparation (PREPARING)** and then:

- Select the certification type (user/privilege)
- Sets the start and approval period.
- Sets the filter for the subjects (the users or privileges) or alternatively a “Find Subjects” user hook.
- Sets a resource (privilege or user) filter or a “Limit Resources” user hook if some privileges of a user or some users assigned a privilege shall be excluded.
- Sets a “Find Approvers” user hook if the approver is not the default.
- (Optional) Sets “Recurring Certification Campaign” to indicate that the campaign is to be run periodically and sets the time period after which the campaign will be run again in “Interval”.

Next, the administrator must enable the notifications to be used and adapt their templates, especially subject and body.

1.2.3. Certification Campaign Notifications

From the campaign’s start until its end, the Certification Campaign Controller can send different mail notification for each campaign phase. When a campaign is created, the mail notification templates are copied from **Certification Campaigns** → **_Default** → **Notifications** container to the newly created campaign **Notifications** container. The administrator can enable or disable these notifications (**General** → **Is Active**), and adjust the notification content (for example, subject, body).

The following mail notification templates are available (listed here in alphabetical order):

- **Approval Remind** – Send a notification to approvers to remind them about their tasks. This notification is configurable with **Remainder** notification values available in the Certification Campaign entry (**Days before due date** and **Interval between remainders (hours)**).
- **Approval Start** – Send a notification to approvers when they get new certification tasks.
- **Approval Timeout** – Send a notification to approvers when one of their certification

tasks has expired.

- **Assignment Reject** – Send a notification to certified users when at least one of their privilege assignments has been rejected.
- **Campaign End** – Send a notification to the campaign owner when a campaign ends.
- **Campaign Start** – Send a notification to the campaign owner when a campaign starts.
- **No Approver** – Send a notification to the campaign owner when no approver was found for a user or privilege to be certified.
- **Prepare Error** – Send a notification to the campaign owner when starting a campaign failed.

When the certification campaign is restarted (manually or as part of the recurring certifications) the Notifications container and its content are not modified.

1.2.4. Starting a Certification Campaign

When the start date of the campaign in state **Campaign is in preparation (PREPARING)** is reached, the Certification Campaign Controller workflow starts the campaign.

The following figure provides an overview of the campaign phases and notifications to be sent:

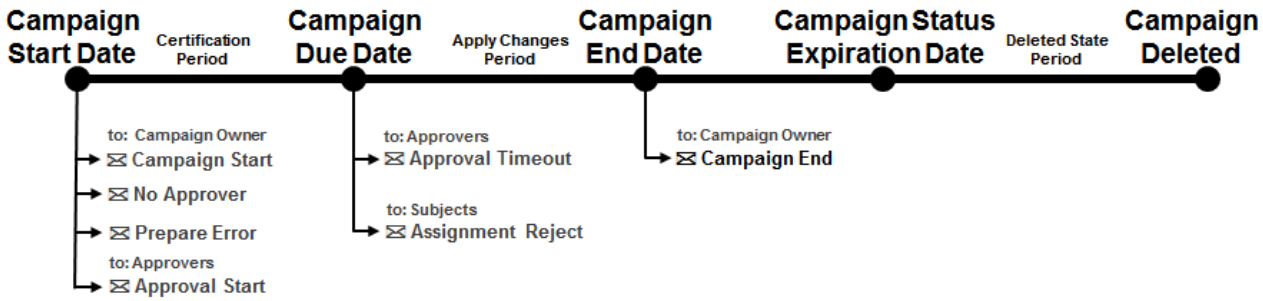

Figure 1. Certification Campaign Phases and Notifications

At start-time, the campaign controller validates the parameters of the campaign. Any warnings or errors are stored in the **Logs** field of the campaign entry.

- **Approval Period.**
- **Due Date**: can be empty and it will be calculated at the start of the campaign: **Start Date** plus **Approval Period**. If **Due Date** is set, this value is used for the current campaign run. If it is a recurring certification campaign, the value will be set to the default value: **Start Date** plus **Approval Period** - on the next start of the campaign
- **Status Expiration Date**: if available, must be after the **Due Date**. If not available, the controller logs a warning. At the end of the campaign, it will calculate a default value **End Date** plus 30 days.
- **User Filter** and **Privilege Filter**:

For a user campaign, both a **User Base** and a **User Filter** must be set or a “Find Subjects” user hook must be specified.

For a privilege campaign, both a **Privilege Base** and a **Privilege Filter** must be set or a “Find Subjects” user hook must be specified.

If the validation fails, the controller sets the campaign state to **Campaign failed to start (FAILED.PREPARED)** and sends a notification “**Prepare Error**” to the campaign owner. The administrator - who should be the campaign owner - can then fix the problems, set the state to **PREPARING** and then start the Certification Campaign Controller workflow.

If the start settings are correct, the campaign controller searches the users (subjects of the campaign), collects their manual privilege assignments (the resources of the certification), potentially removes them according the privilege filter or the “Limit Resources” user hook and sets the approver(s) per user. For each user, it stores the result in a certification entry underneath the campaign entry in a child container **User Certification**. If a “Find Approvers” user hook provides more than one approver for the user, it creates a sub-tree of certification entries. For more details, see the section “Select Approvers with a “Find Approvers” User Hook”.

For a privilege campaign, the certification entries are stored in a child container **Privilege Certification**. Each certification entry represents a privilege to be certified and its assignments are the users of this privilege. The approver is responsible for certifying the privilege.

For each certification entry (that is, for each user or privilege to be certified), the campaign controller sends an **Approval Start** notification if available.

If a certification entry does not have at least one approver, its state is set to **FAILED.PREPARE** and the campaign controller sends a notification **Prepare Error** to the campaign owner. If a certification entry does not have any manual assignments, the state will be directly set to **RUNNING** and certification entry will be automatically closed at the end of the approval period. The campaign controller also sends a **No Approver** notification to the campaign owner.

When all certification entries have been created, the campaign controller sets the campaign state to **Campaign is running (RUNNING)** and then sends a **Campaign Start** notification to the campaign owner.

1.2.5. Certifying Users or Privileges

Approvers are notified by an **Approval Start** notification. When they open DirX Identity Web Center, they can see the certification campaigns in which they are involved in their start page and can immediately navigate to their certification tasks or they can use DirX Identity Business User Interface Certification Campaign feature to approve or reject certification tasks. For each entry to be certified (user or privilege), they can see all manual assignments and can decide whether to accept or reject each individual assignment. If an assignment has an end date or a role parameter (for example, the manager for a project), the approver can delete or modify the end date or the parameter. These changes are stored underneath the certification entry and are applied at the end of the campaign. Approvers can store their decisions at any time and then continue with the open tasks later on. When

the approver saves the decisions for all assignments of a certification entry, DirX Identity Web Center or DirX Identity Business User Interface sets the state of the entry to **APPROVAL.FINISHED**.

The Certification Campaign Controller workflow should be scheduled to run regularly. In addition to starting campaigns, it also monitors running campaigns.

When it detects a finished certification entry, the campaign controller starts downstream approvals for that entry when available. When a certification task is approaching the due date, it sends reminder notifications (type **Approval Timeout**). When a certification task has reached the due date, the campaign controller sets its state to **FAILED.EXPIRED**. If a downstream approval exists, it is started.

The administrator can change the due date or state of single certification entries or the entire campaign at any time, as necessary. So they can react in a flexible way to any errors.

1.2.6. Finishing a Certification Campaign

When the **Due Date** of the certification campaign is reached (manually set by the campaign administrator or automatically calculated at the start of the campaign)**,** the campaign controller starts to apply the changes. The actions depend on the "revoke privileges" settings made in the campaign entry. Rejected, changed and ignored (uncertified) assignments can simply be left as they are, removed from the users or evaluated by an approval workflow (only when set accordingly per privilege). When an assignment is removed, the campaign controller sends an **Assignment reject** notification to the users.

If an error occurs during the apply change process, the campaign controller sets the state of the certification entry to **FAILED.APPLIED.CHANGES**. Otherwise, the controller sets the state to **FINISHED** and sets the **End Date**.

At the end, the campaign controller sets the campaign state to **Campaign finished successfully (SUCCEEDED)**, sets the **End Date**, calculates the **Status Expiration Date** if required (the date at which the campaign will be moved to state **DELETED**), and sends a **Campaign End** notification.

When the **Status Expiration Date** is reached, the campaign controller sets the campaign state to **Campaign is marked for deletion (DELETED)**. A subsequent "Cleanup Objects" workflow will physically delete the entire sub-tree for the campaign later on.

1.2.7. Recurring Certification Campaign

When values are set for **Recurring Certification Campaign**, the certification campaign will be restarted after the time period specified in **Interval**.This option applies only to campaigns that have finished with success.The campaign controller will check if the new start date is reached (**Start Date** from previous campaign plus **Interval**) and will move the current closed campaign to the **_Archive** container in a folder with the campaign name and start date (for example, Finance High Risk Users Certification 2016-07-01) and will start the new campaign.The **Due Date** for the new campaign is calculated based on **Start Date** and **Approval Period** from the initial campaign.Any eventual manual modification of the

Due Date during the previous campaign will be ignored.

To stop a recurring certification campaign, the administrator must clear all values from **Interval**.

1.2.8. Generating Reports

DirX Identity provides default reports on certification campaigns.You can generate a report on a campaign at any time, especially after the campaign has finished.

To generate a report, in DirX Identity Manager, right click a campaign entry, select **Report** and then select one of the available reports from the list provided.See their descriptions to get more information on their content.

2. Configuring the Pre-Requisites

Before you can start a certification campaign, you need to ensure that the workflow for creating and monitoring certification campaigns is active and can run on exactly one Java-based Server and that the general email service is configured.

To satisfy these requirements, perform the following configuration tasks:

- **Make sure that the email service is configured**.The Certification Campaign Controller workflow uses the central **SendMail** workflow to send emails via **SMTP.** Browse to **Provisioning** → **Workflows** → **Services** → **SMTP**.To enable this service, you need to provide values for **SMTP host** and **Port** fields with correct values for an external SMTP server.Also check the value in the **Map mail address** field.For production, make sure the field is blank and does not contain the text **dummy**, which disables the SMTP workflow.If you plan to send encrypted emails then turn on the flag **Encrypt Email** and decide about the flag **Send on Encryption Failure.** Please consult the context-sensitive help for more details on how to configure this service.
- **Configure the Certificate Service** (that is used to get the certificate for a given email address) if you plan to send encrypted emails by the SendMail workflow.Define the **IP Address** and **Port** if you want the to get the user certificates from an external LDAP directory.If the certificates are available in the user tree of the Provisioning View then simply leave the field **IP address** empty.Furthermore provide the **Search Parameter** fields and the **Refresh Interval** of the internal certificate table.Please consult the context-sensitive help for more details on how to configure this service.
- **Configure the resource family for the Certification Campaign workflow**.The Certification Campaign Controller workflow requires the resource family **CertificationCampaign** to run on a Java-based Server.By default, it is not configured.Select a Java-based Server by navigating to **Connectivity** → **Expert View** → **Configuration** → **Java Servers** → *yourdomain* → *yourdomain*-**yourhost***.**In the *Resource Families** tab, move the **CertificationCampaign** item from the **Available** list down to **Selected**.Set the value for **Thread number** to **1**.Click **Save** to commit the changes.
- **Create a schedule for the Certification Campaign workflow**.The Certification Campaign Controller workflow is started by a schedule, not by events.The workflow performs actions like starting campaigns, monitoring campaigns, applying changes from campaigns, finishing campaigns, deleting campaigns and sending notifications.

  To create a schedule, navigate to **Connectivity** → **Expert View** → **Schedules** and create a schedule for the workflow **Workflows** → **Default** → **Identity Store** → **CertificationCampaignController**.

  For more details about how to create a schedule, consult the context-sensitive help and DirX Identity documentation.

- **Enable the Certification Campaign Controller workflow**. The Certification Campaign Controller workflow is disabled by default and must be enabled. To enable it, navigate to **Connectivity** → **Workflows** → **Default** → **Identity Store** → **CertificationCampaignController**. In the **General** tab, enter edit mode and then check **Is Active**.

3. Creating a Certification Campaign

A certification campaign is represented by a campaign entry in the Provisioning domain. To set up a new user certification campaign, you need to create a new entry: In the sub-view **Certification Campaigns** of the view group **Provisioning**, right click an appropriate parent container and select **New** → **CertificationCampaign** and then supply values for the following mandatory fields:

- **Name** – the name of the campaign to be displayed to approvers and stated in emails.
- **Type** – the campaign type. Set it to **User Certification** or **Privilege Certification.**
- **Owner** – a user in the domain who is to be considered the owner of the campaign.
- **Reminder Notifications** – the period before the campaign due date at which reminders are to be sent to approvers about their certification tasks and the interval at which these reminders are to be sent.
- **Apply Changes** – whether rejected assignments are ignored, revoked or need additional approval at the end of the campaign. The options are:
  - **Do not revoke any rejected privileges** – no assignments are removed.
  - **Revoke all manually rejected privileges that are rejected or left uncertified** – both assignments that are explicitly rejected, and assignments that have been ignored by the approver are removed.
  - **Revoke only rejected Privileges that were manually assigned** – only the assignments that are explicitly rejected by the approver are removed. The ignored ones are left untouched.
  - **Review the revocation of all manually assigned privileges that are rejected or left uncertified** – starts an approval workflow for all of the manual assignments that the approver did not explicitly accept and where the concerned privilege needs approval during assignment. Assignments which the approver did not explicitly accept are removed.
- **Status** – the certification campaign status. This field must be set to **Campaign is in preparation (PREPARING)**.
- **Start Date** – the date at which the campaign should start. If you want to start the campaign immediately, set this date somewhere in the past.
- **Approval Period** – the duration of the approval period. This value will be used to calculate the **Due Date** and should provide sufficient time for the approvers to certify all assignments.
- **Due Date** – the date at which the campaign should end. This date is calculated at the start of campaign from **Start Date** plus **Approval Period**. The administrator can change this value later on during the campaign.
- **Status Expiration Date** – the time at which certification LDAP entries should be physically deleted (optional). When this field is blank at the end of the campaign, the campaign workflow will set a default expiration date of the current date plus 30 days.
- **User Base** and **User Filter** – the subjects of the certification.

It is possible to create a Certification Campaign for users with a specific risk, if the **Risk Governance** feature is enabled in the **Domain Configuration** tab. **User Filter** may contain an additional search parameter for the LDAP attribute: **dxrRskLevel** (**0** – normal risk, **1** – low risk, **2** – medium risk, **3** – high risk), for example

```
(&(objectClass=dxrUser)(|(ou=Finances))(dxrRskLevel>=2))
```

The query above retriever all users for a Cerification Campaign from the organization unit **Finance** withthe risk level medium risk.

- **Privilege Filter Base and Filter** – the privileges to be certified.Leave these fields blank when you want all manual assignments of the subjects to be certified.Specify values for these fields when you want to restrict the privileges to be certified: the privileges to be certified must match this filter.

These fields are mandatory to start a certification campaign.

4. Starting a Certification Campaign

When the start date of the campaign in state **Campaign is in preparation (PREPARING)** is reached, the Certification Campaign Controller workflow starts the campaign.The workflow is normally started according the schedule.But you can also start it manually using DirX Identity Manager: in the Connectivity view, navigate to the workflow entry and then select **Run Workflow** from the context menu.

The Campaign Controller workflow collects the users to be certified along with their privilege assignments, finds approver(s) for each user, stores their certification tasks in the campaign subtree and notifies the approvers.

If something fails – for example, an approver cannot be found for a user to be certified – the workflow creates the certification task, but sets its state to **FAILED.PREPARE** and notifies the campaign owner.The campaign owner can then manually fix the problem and change the state to **PREPARED** or **RETRY.PREPARE**.When the Certification Campaign workflow runs again, it re-evaluates this certification task and – if successful – changes the state to **RUNNING**.

Approvers can then work on their tasks and certify the user assignments using DirX Identity Web Center or DirX Identity Business User Interface.

5. Monitoring and Finishing a Campaign

The following diagram gives an overview on the states of a campaign:

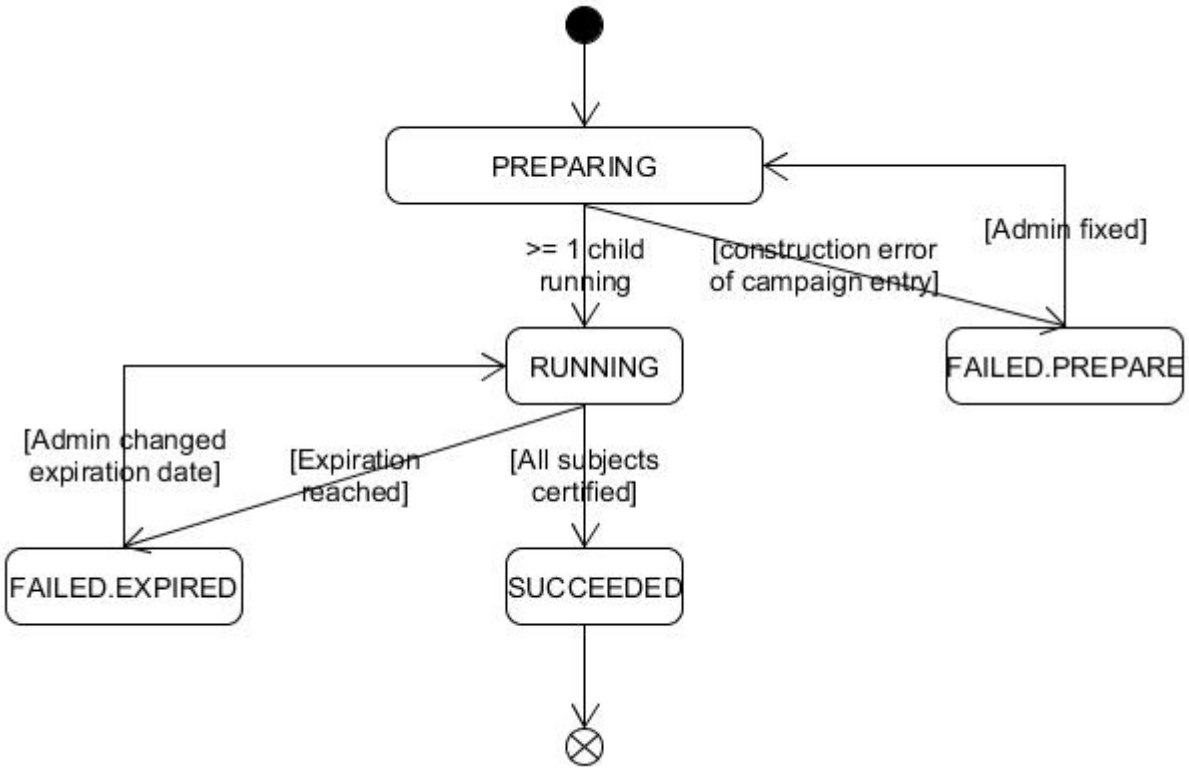

Figure 2. Certification Campaign States

When the Certification Campaign workflow has successfully created at least one certification task, it considers the campaign to be running.Otherwise, it sets the state to **FAILED.PREPARE**.The administrator (campaign owner) can then fix any problems and set the state manually to **PREPARING**.When it runs again, the workflow tries to start the campaign.

When the due date of the campaign is reached, the workflow applies the changes of all finished certification tasks of the campaign.If no certification task has been finished, the campaign is set to **SUCCEEDED**.In both cases, the administrator can extend the campaign by pushing the due date into the future and setting the campaign state back to **Campaign is running (RUNNING)**.

The following diagram gives an overview of the states of a single certification task:

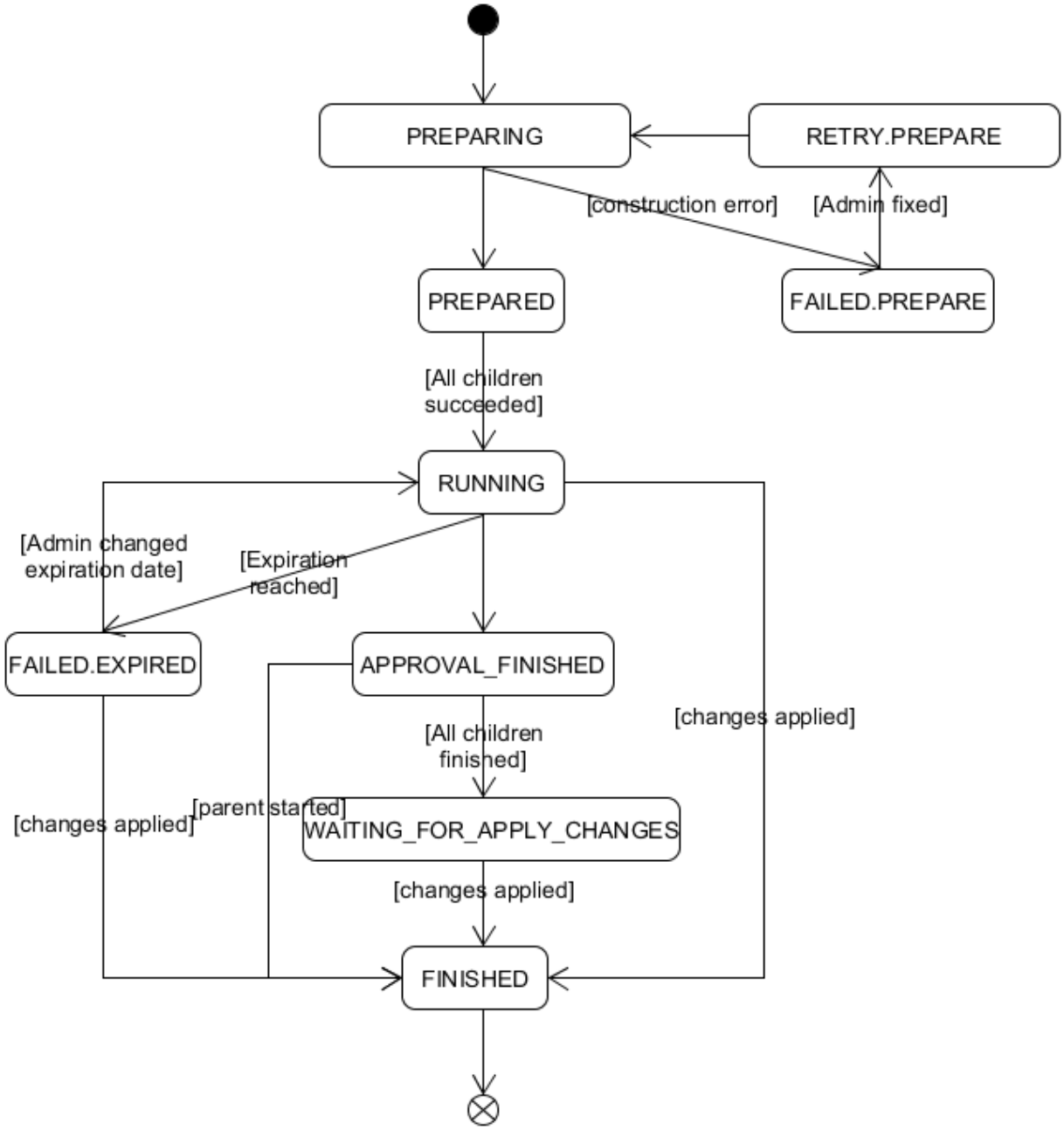

Figure 3. Certification Task States

When the task cannot be created successfully, the workflow sets it to the **FAILED.PREPARE** state.The administrator can then fix any issues and set the state to **RETRY.PREPARE**.When on the next run the starting the task succeeds, the workflow sets the state to **RUNNING**.The **PREPARED** state is a temporary state that is relevant when there are several approvers and extra tasks need to be created for them.

When the approver has certified all assignments, the certification task changes to the **APPROVAL.FINISHED** state.When the **Due Date** of the task is reached, the Certification Campaign workflow sets the state to **FAILED.EXPIRED**.The administrator can move the due date to the future, set the state back to **RUNNING** and thus give the approver the opportunity to finish the task.

When the **Due Date** of the campaign is reached, the Certification Campaign workflow stops all running certification tasks with the **FAILED.EXPIRED** state and starts to apply changes according to the settings in the **Apply Changes** field of the campaign.After all changes are applied, the certifications are moved to state **FINISHED**.The state A**WAITING.FOR.APPLY.CHANGES** is a transient state and is currently not used.

If a certification contains uncertified assignments when the **Due Date** is reached, this certification is moved to the state **FINISHED**.

If there are changes that cannot be applied for a certification, this certification is moved to the state **FAILED.APPLY.CHANGES**.

6. Customizing with User Hooks

This section gives hints for customizations with user hook implementations.

if you configure user hooks, you must provide their implementation in Java ***.jar** libraries and deploy them to the relevant IdS-J Server into the sub-folder **confdb/jobs/ CertificationCampaign/lib**.After you complete these tasks, make sure you re-start the IdS-J Server.

6.1. Documentation and Sample Source Code

You can find the Java documentation of the user hooks interfaces and samples on the DirX Identity DVD in the folder:

Documentation/DirXIdentity/CertificationCampaign

The sample source code is delivered in the folder:

Additions/CertificationCampaign

6.2. Select Approvers with a “Find Approvers” User Hook

The **Find Approvers** user hook allows you to change the default approvers for certifications. For a user certification campaign, the default approver is the **manager** of the user, and for a privilege certification campaign, the default approver is the **owner** of the privilege. You can override this default implementation with a custom **Find Approvers** user hook.

The **FindApprovers** user hook must implement the **FindApproversUserhook** Java interface. This interface contains the following methods:

```
void setContext(FindApproversContext context);
```

```
FindApproversContext getContext();
```

```
boolean before();
```

```
boolean after();
```

```
TreeNode<StorageObject> findApprover(FindApproversContext context)
```

```
throws NoApproverException;
```

The method setContext is used by the campaign controller to give the user hook access to some DirX Identity context objects:

`GlobalContext` object – an object that can be used to access different attributes from the IdS-J Server.

`Campaign` object - a `StorageObject` that contains details about the current campaign.

`Certification` object - a `StorageObject` that contains details about the current certification task.

`Subject` object - a `StorageObject` that contains details about the current subject to be certified (for example, in a user certification campaign, it is a `SvcUser` object).

Inside the user hook, you can change objects, especially the Certification (task). For example, you can store the due date in the attribute `dxrEndDate`. If you do so, you must store your changes to LDAP on your own.

6.2.1. Before – Creating the Certification Task in the User Hook

The method `before()` is executed before all controller actions and the method `after()` is called after the controller finishes all the actions for the current certification object. If these methods return false, the default implementation of the Certification Campaign controller will not be executed.

This is especially important for the method `before()`. If it returns false, the controller assumes that the complete certification task object has been created by the user hook. In this case, the user hook must find the approvers, the assignments to certify per subject (user), set the state and the start and end dates, and at the end save the certification task object(s).

6.2.2. After – Changing Default Attributes

When the method `after()` is called, the certification object has already been created and saved to LDAP. The user hook can then override some attribute values and must store its changes in LDAP.

6.2.3. Find Approvers – Adding Additional Approvers

You can also use the **Find Approvers** user hook to add more approval tasks (called **sub-certifications**) for the given subject. In this way, you can even create a hierarchy of approval tasks by several approvers, as illustrated in the following diagram:

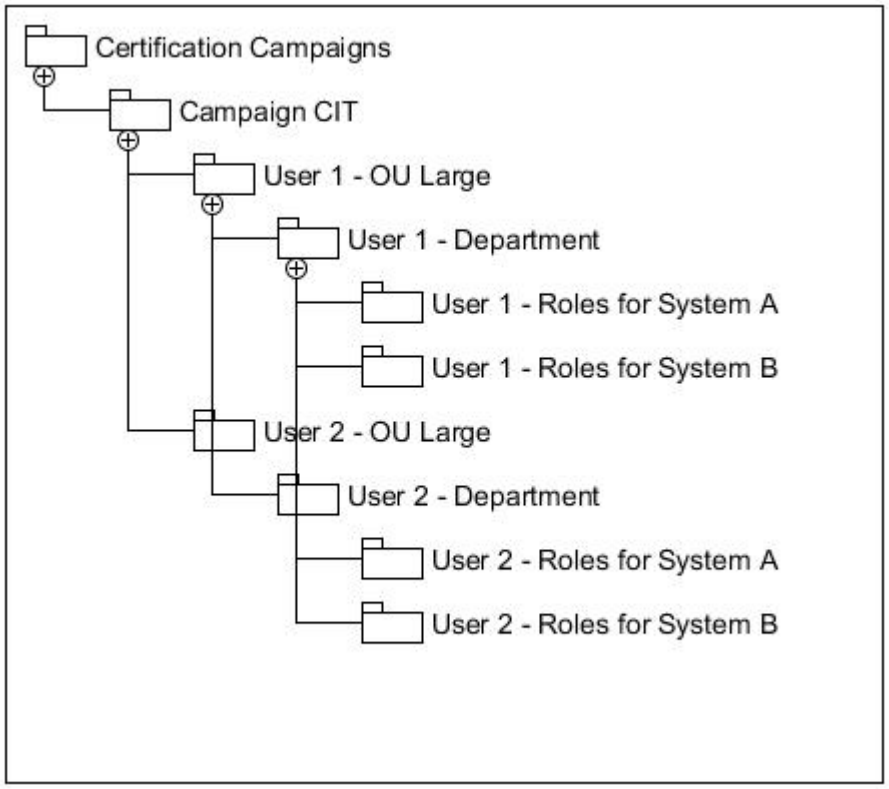

Figure 4. Certification Campaign Sub-certification Structure

To create this kind of structure for a certification, you must implement the following method inside the **FindApprovers** user hook:

`TreeNode`*`StorageObject`* `findApprover(FindApproversContext context)`

This method returns a tree structure of `StorageObjects`. The controller creates a certification object (which reflects one approval task) for each approver in the tree structure. The tasks are processed according the campaign field **Approver Sequence** top down or bottom up. Each sub-certification follows the same states as a normal certification. The last approval task determines the state of the whole subject certification.

6.3. Select Campaign Subjects with a “Find Subjects” User Hook

A user hook that implements the `FindSubjectsUserhook` Java interface can select the subjects. The subjects are users for a user certification and privileges for a privilege certification. This action is helpful when an LDAP filter is not sufficient to identify the subjects of the campaign.

You need to implement the following methods:

```
FindSubjectsContext getContext()
```

```
setContext(FindSubjectsContext context)
```

```
List<String> findSubjects(FindSubjectsContext context)
```

The first two methods have the same functionality as in the **FindApprovers** user hook. You can use setContext method to store the FindSubjectContext object.

The method `findSubjects` is called before the controller starts to find the subjects for the certification campaign. You can use this user hook method to override this functionality and return your own list of subjects (a list of DNs) instead. The `FindSubjectContext` provides access to a `GlobalContext` object and to the `Campaign` object.

6.4. Limit Resources with a “Limit Resources” User Hook

A user hook that implements the `LimitResourcesUserhook` Java interface can reduce the list of resources to be certified. The resources are privileges for a user certification and users for a privilege certification.

The default implementation considers the resource base and filter. If they are empty, all resources must be certified. If they have values, the resources must be descendants of the resource base (including the resource base itself), and their attributes must match the LDAP filter.

If the LDAP filter is not sufficient, you can implement this user hook. If you do, both resource base and resource filter are ignored.

You need to implement the following methods:

```
LimitResourcesContext getContext()
```

```
setContext(LimitResourcesContext context)
```

```
List<String> limitResources(LimitResourcesContext context)
```

The first two methods have the same functionality as the **FindApprovers** user hook. You can use the setContext method to store the LimitResourcesContext object.

The method `limitResources` is called before the controller starts to find resources for the certification campaign. You can use this user hook method to override this functionality and return your own list of resources (a list of DNs) instead. The `LimitResourcesContext`

provides access to the `GlobalContext` object and to the `Campaign` object.

6.5. Send emails with the “Send Email” User Hook

With a user hook that implements the `SendEmailUserhook` Java interface, you can send notifications your own way.

The user hook needs to implement the following methods:

```
SendEmailContext getContext()
```

```
setContext(SendEmailContext context)
```

```
boolean onSendEmail (SendEmailContext context)
```

```
boolean before()
```

```
boolean after()
```

The first two methods have the same functionality as the **FindApprovers** user hook. You can use `setContext` method to store the `SendEmailContext` object.

The `SendEmailContext` method contains the following objects: GlobalContext object, Campaign object, a list with Certification objects used for sending emails, a list with NotificationProcessor objects which can be used to process the email templates.

The `before()` and `after()` methods are called before and after sending emails. If these methods return false, the default implementation from the Certification Controller will not be executed.

With the `onSendEmail` method, you can override the default implementation of the Certification Campaign controller. If you don’t want to execute the default sendEmail implementation, the user hook method must return false.

6.6. Override Campaign Creation with “Campaign Creator”

With an implementation of the `CampaignCreatorUserhook` Java interface, you can completely override the creation of a campaign: find the subjects, select the assignments and calculate the approvers.

You need to implement the following methods:

```
CampaignContext getContext()
```

```
setContext(CampaignContext context)
```

```
boolean before()
```

```
boolean after()
```

The first two methods have the same functionality as the **FindApprovers** user hook. You can use the setContext method to store the CampaignContext object.

The method `before()` is called by the controller when it is ready to start creation of the certifications task entries. If it returns false, the controller skips the default implementation and assumes that all the certification tasks have been created and stored by the user hook.

If the method `after()` returns false, the default implementation is skipped, which means that the notification about the started campaign will not be sent.

7. Generating Certification Campaign Reports

This chapter describes how to create reports for a certification campaign.

7.1. About the Default Report Templates

DirX Identity provides some default reports that you can use immediately. They are located in **Provisioning** → **Domain Configuration** → **Reports** → **Default** → **CertificationCampaigns**. Each report contains the following files (for example, see **Campaign with all properties**):

- **Campaign with all properties** – this file contains the search base and search filter for the report and a list with all attributes to be retrieved from the LDAP directory. This file contains the export formats for reports, by default: HTML, XML and RAW (to be passed to a XSLT transformer).
- **Settings for Producer/Selector** – this file contains values for search filter, sort criteria, name of the report, search level, and attributes to be retrieved from LDAP.
- **Settings for Templates** – this file contains flags to display or hide different fields from reports.
- **Templates** – this file in XSLT format is the markup for the report.

7.2. Producing a Report

To run a report, right click on a certification campaign entry and then select **Report**. The dialog **Run report** pops up and lists the available reports for certification campaigns. Select one of them from the list.

Near the bottom of the dialog there is a description for the report and some parameter fields. Leave the search base and the scope: they refer to the folder for the selected campaign. Switch the type to **HTML** for a nice output format. Change the name of the output file or check **Output to viewer** if you want to check the report output in the dialog window.

Select **XML** as the output format if you want to check all available attributes and their values or if you want to process the file later on with an XML tool. In HTML format, some attributes and values are sometimes hidden during the XLST transformation depending on the settings in the report template.

7.3. Adding or Extending Reports

You can create a new report definition by starting with an existing report. For example, you can copy **Campaign with Failed.Prepare certificates** and then modify it to generate a report which contains certifications where applying the changes failed; that is, with the state **FAILED.APPLY.CHANGES**.

To adjust the search filter, change the following line in the entry **Settings for Producer/Selector**:

```
<var name="SearchFilter" value="(|(objectClass=
dxrCertificationCampaign)(&amp;(objectClass=dxrCertificationEntry)(|(
dxrState=FAILED.PREPARE)(dxrState=FINISHED))))"/>
```

to

```
<var name="SearchFilter" value="(|(objectClass=
dxrCertificationCampaign)(&amp;(objectClass=dxrCertificationEntry)(dx
rState=FAILED.APPLY.CHANGES))))"/>
```

Now this report will contain only the certification tasks where the changes could not be applied successfully.

8. Continuous Certification by Re-Approval

This chapter describes continuous certification via re-approval workflows. This is a highly effective method that distributes load with regard to your employees and your DirX Identity system and that works with maximum efficiency.

8.1. About this Use Case

This use case leverages DirX Identity's re-approval feature. Privileges are flagged for re-approval and - depending on the timing conditions in place - a re-approval workflow is started for a specific assignment before the assignment's end date is reached. The following figure illustrates this use case.

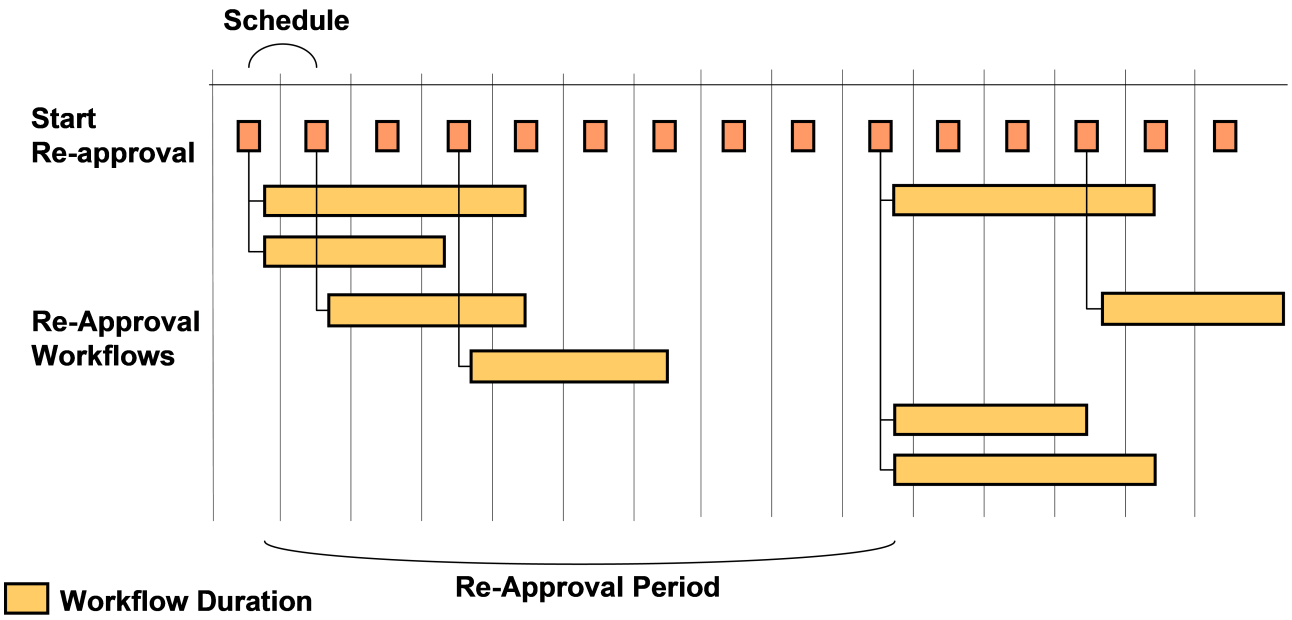

Figure 5. Certification by Re-Approval

The approvers of these workflows receive an e-mail notification informing them that they need to re-approve a specific assignment. They must decide whether the user keeps the privilege or whether the privilege should be removed.

The workflows are continuously started from a daily **StartReapproval** workflow. It checks for privilege assignments that are to be re-approved. To ensure that all assignments are correctly flagged, an **InitializeReapproval** workflow should be started in advance. The following figure illustrates the timing conditions.

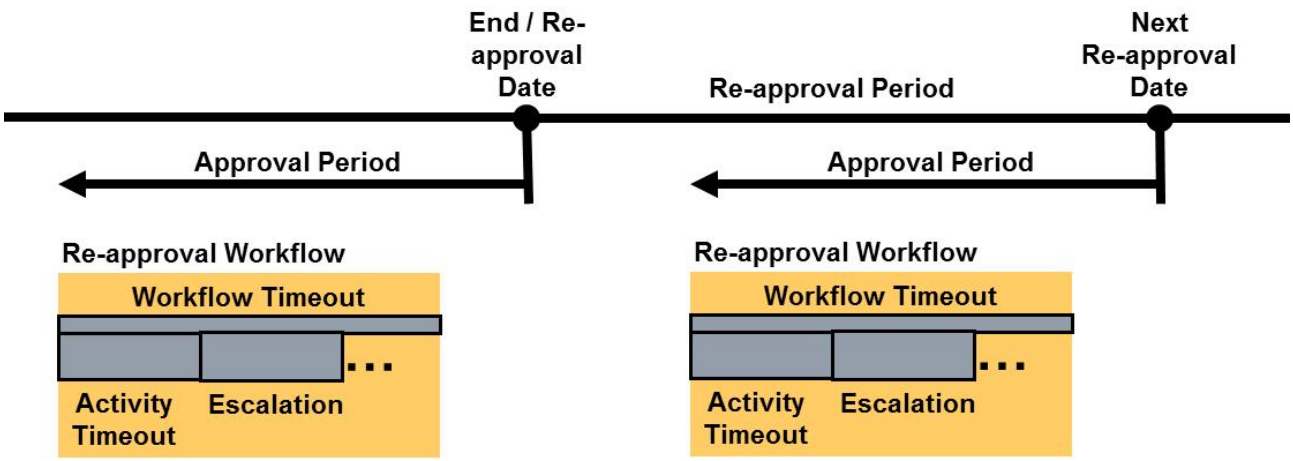

Figure 6. Certification by Re-Approval Timing

In the figure:

- The **end date** at the assignment marks the date where the next re-approval has to be finished. If this date is reached and the approval was accepted, the user keeps the assignment. If the approval was rejected or not performed in time, the user will lose the assignment at this date.
- The next re-approval date is calculated from the current end date of the assignment plus the **Re-approval Period** value at the privilege (if this value is not available, the default value is taken from the domain object) or according to the **Re-approval Date** set at the privilege (if this value is not available, the default value is taken from the domain object). For a complete definition of the calculation, see the section "About Re-Approval" in Chapter 1.
- The timeout of the approval activity is individual per re-approval workflow. When this time expires, one or more escalations can occur depending on the workflow's configuration.
- The workflow has its own individual **Workflow Timeout**, which should be longer than the sum of all possible activity timeouts including the escalations.

8.2. Setup and Configuration

This use case requires you to set up the following items:

- The relevant flags at the domain object
- The re-approval properties at the privileges
- The workflows

8.2.1. Setting up the Domain Object

Select the **Domain Configuration** view, click the top-level node and then select the **Timing** tab.

In the **Approval** area, you should set three attributes that are relevant for re-approval:

- Set the **Approval period** to four (4) weeks to give the approvers enough time to react to the re-approval request. The re-approval workflow is started at the time at which the re-approval must occur minus this approval period value. For example, if the re-approval is set to the end of May and you select a four-week period, the re-approval workflow is started at the beginning of May. If no approval period is configured at the domain, a default value of 14 days applies.
- The **Re-approval period** is a default value that takes effect when the corresponding field at the privilege is not set. Typical values for re-approval periods are from three (3) months to two (2) years. The default value is three months.
- Leave the **Re-approval date** empty because we want to run individual re-approvals for each assignment.

See the online help for an explanation of these settings.

8.2.2. Setting up the Privileges

To keep it simple, we only set up role re-approval here. You can configure privileges of any other type if that is what's required.

For each role requiring re-approval, set its **Requires re-approval** flag and then set the other parameters in one of the following ways:

- If you want to have the same behavior for all privileges, leave the **Re-approval date** and **Re-approval period** empty. In this case, the domain settings apply.
- If you have privileges requiring a shorter or longer re-approval period, set an individual **Re-approval period** at the privilege.

If you want to use different re-approval workflows, set a link to the appropriate one in the **Workflow** field for each role. Make sure that the activity, escalation and workflow timeouts match the approval period.

Perform this procedure for all roles you want to be re-approved.

8.2.3. Setting up the Workflows

You need to set up two workflows for re-approval. The next sections describe these tasks.

8.2.3.1. InitializeReapproval

The **InitializeReapproval** workflow sets for all existing privilege assignments whether an end date is set according to the defined conditions at the privilege and the domain object. You should run this workflow either manually if you changed the re-approval conditions at privileges or - and we recommend this method - regularly each night to be sure that all assignments are correctly set up for re-approval.

Open the workflow's wizard in the **Connectivity** view group:

- In the **Rule Search Parameters** tab, you can see that the **InitializePrivilegeForReapproval** consistency rule is run.

- Check this rule in the **Provisioning** → **Policies** → **Rules** → **Default** → **Consistency Rules** → **Reapproval** folder.
- With the flag **updateConfiguredReapprovalDates** in the **General** tab set, you can automatically shift the re-approval dates configured at the domain and/or the considered privileges: If the re-approval date lies in the past or within the approval period, it is shifted to the future by one re-approval period.
- Check the filter conditions in the **Filter** tab. The **Search Base** works on the entire domain and the **Search Filter** is set to:
  (dxrneedsreapproval="TRUE" and (objectclass="dxrRole" or objectclass="dxrPermission" or objectclass="dxrTargetSystemGroup"))
  which means that it searches for all privileges that have the dxrNeedsReapproval flag set.

Don't forget to copy the rule and the workflow to be sure that changes in the configuration remain and are not overwritten by the next DirX Identity product update.

This workflow is set up as a separate workflow that runs exactly one consistency rule (InitializePrivilegeForReapproval). Alternatively, you can run it together with other consistency rules in your custom policy execution workflow.

8.2.3.2. StartReapproval

The **StartReapproval** workflow should run regularly once per night. It checks whether an assignment is flagged for re-approval and whether the end date is reached. Then it starts the defined re-approval workflow.

Open the workflow's wizard in the **Connectivity** view group:

- In the **Rule Search Parameters** tab, you can see that the **StartWorkflowsForReapproval** consistency rule is run.
- Check this rule in the **Provisioning** → **Policies** → **Rules** → **Default** → **Consistency Rules** → **Reapproval** folder.
- Check the filter conditions in the **Filter** tab. The **Search Base** works on the entire domain and the **Search Filter** is set to:
  (objectclass="dxrAssignment" and dxrneedsreapproval="TRUE"
  and dxrEndDate<="$(approvaldate)" and (not (dxrInApproval="TRUE") or not (dxrInApproval=*)))
  which means that it searches for all assignments that have the dxrNeedsReapproval flag set and whose end date is reached and where no re-approval workflow is already started.

Don't forget to copy the rule and the workflow to be sure that changes in the configuration remain and are not overwritten by the next product update.

This workflow is set up as a separate workflow that runs exactly one consistency rule (StartWorkflowsForReapproval). Alternatively, you can run it together with other consistency rules in your custom policy execution workflow.

8.3. Running the Use Case

Run the configured workflows once and test the result. Be sure to run it in the sequence InitializeReapproval and then StartReapprovalWorkflows.

After completion, view the status of the workflow and check the trace file for errors.

View the Request Workflow Monitor area to check for the newly created re-approval workflows.

If everything works well, set up schedules to run the two workflows regularly. We recommend that you set up a hierarchical workflow that defines the sequence and then run this workflow daily.

8.4. Alternative or Extended Configurations

This section gives hints for alternative or extended configuration of the use case.

8.4.1. Certifying Other Privilege Types

In this use case, we ran re-approval only on roles. If required, you also can run re-approval at permission or group level. Set the corresponding flags and fields at these types of privileges.

You can also run a certification on any mix of roles, permissions and groups.

8.4.2. Running Separate Campaigns

If you need to re-approve a huge number of privileges, think about setting up multiple workflows. Set up InitializeReapproval and StartReapprovalWorkflows workflows with different search bases and filters.

If you run separate campaigns, set up the corresponding schedules and try to distribute the load.

9. Scheduled Certification by Re-Approval

This chapter describes scheduled certification via re-approval workflows. This is another use case that you can perform using the re-approval feature.

9.1. About this Use Case

This use case leverages DirX Identity's re-approval feature. Privileges are flagged for re-approval and a central definition of the re-approval date is set at the domain. This use case defines a campaign that is run at the same time for all flagged privileges. The following figure illustrates this use case.

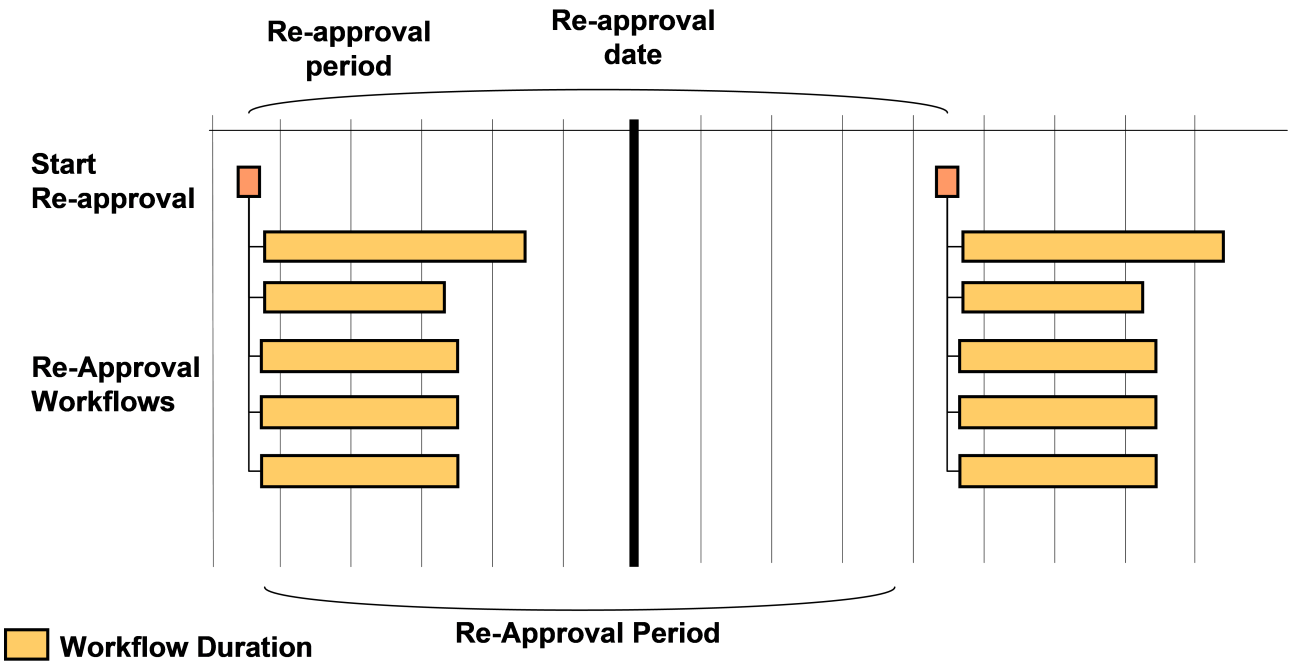

Figure 7. Certification by Re-Approval

The approvers of these workflows receive an e-mail notification informing them that they must re-approve a specific assignment. They need to decide whether the user keeps the privilege or whether the privilege shall be removed.

It makes sense to run the **InitializeReapproval** and **StartReapproval** workflows only once at the beginning of the campaign. This action starts all necessary workflows for the campaign. The following figure shows the timing condition details.

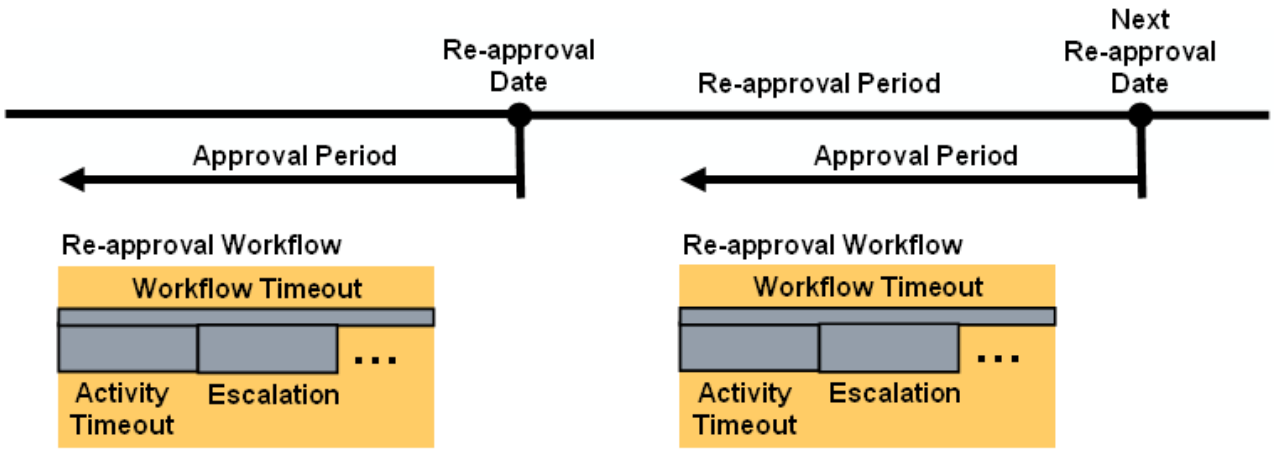

Figure 8. Certification by Re-Approval Timing

In the figure:

- We assume that the **Re-approval Date** is only set at the domain, which means that it is used for all privilege assignments that are flagged for re-approval. All re-approval workflows are started at the same time. If the re-approval date is reached and the approval was accepted, the user keeps the assignment. If the approval was rejected or no decision was taken, the user will lose the assignment on this date.
- We also assume that there is only a central definition of the **Re-approval Period** at the domain. This setting defines when the next re-approval will take place.
- The timeout of the approval activity is individual per re-approval workflow. When this time expires, one or more escalations can occur depending on the workflow's configuration.
- The workflow has its own individual **Workflow Timeout**, which should be longer than the sum of all possible activity timeouts including the escalations.

9.2. Setup and Configuration

This use case requires you to set up the following items:

- The relevant flags at the domain object
- The re-approval properties at the privileges
- The workflows

9.2.1. Setting up the Domain Object

Select the **Domain Configuration** view, click the top level node and then select the **Timing** tab.

In the **Approval** area, you should set three attributes that are relevant for re-approval:

- The **Reapproval period** is a default value that takes effect when the corresponding fields at the privileges are not set. Because we want to run a certification campaign each year, we set the value to one (1) year. The default value is 3 months.

- Because we intend to run a campaign at the end of March each year, we set the **Reapproval date** to the 31st of March.
- Set the **Approval period** to four (4) weeks to give the approvers enough time to react to the re-approval request. The re-approval workflow is started at the time when the re-approval must occur minus this approval period value. If the re-approval is set to end of March and you select a four-week period, the re-approval workflow is started at the beginning of March. If no approval period is configured at the domain, a default value of 14 days applies.

See the online help for an explanation of these settings.

9.2.2. Setting up the Privileges

To keep it simple, we only set up role re-approval for this use case. You can configure privileges of any other type if that is required.

Perform these steps for each privilege that requires re-approval:

- Set the **Requires re-approval** flag.
- If you want to use different re-approval workflows, set a link to the appropriate one in the **Workflow** field for each role. Make sure that the activity, escalation and workflow timeouts match the approval period.

All other parameters are taken from the domain definitions, so no further configuration is necessary.

9.2.3. Setting up the Workflows

You need to set up two workflows for re-approval. The next sections describe these tasks.

9.2.3.1. InitializeReapproval

The **InitializeReapproval** workflow sets, for all existing privilege assignments, whether an end date is set according to the defined conditions at the privilege and the domain object. You should run this workflow only once - in this case, at the beginning of March. The start of the workflow must be slightly later than the intended **Re-approval date** (31st of March) minus the **Approval period** (4 weeks).

Open the workflow's wizard in the **Connectivity** view group:

- In the **Rule Search Parameters** tab, you can see that the **InitializePrivilegeForReapproval** consistency rule is run.
- Check this rule in the **Provisioning** → **Policies** → **Rules** → **Default** → **Consistency Rules** → **Reapproval** folder. You can use the flag **updateConfiguredReapprovalDates** in the **General** tab to automatically shift the re-approval date that is configured at the domain: If the re-approval date lies in the past or within the approval period, it is shifted to the future by one re-approval period.
- Check the filter conditions in the **Filter** tab. The **Search Base** works on the entire domain and the **Search Filter** is set to:

(dxrneedsreapproval="TRUE" and (objectclass="dxrRole" or objectclass="dxrPermission" or objectclass="dxrTargetSystemGroup"))
which means that it searches for all privileges that have the dxrNeedsReapproval flag set.

We recommend that you copy the rule and the workflow to be sure that changes in the configuration remain and are not overwritten by the next product update.

This workflow is set up as a separate workflow that runs exactly one consistency rule (InitializePrivilegeForReapproval). You could also run it with other consistency rules in your custom policy execution workflow.

9.2.3.2. StartReapproval

The **StartReapproval** workflow should run only once directly after the **InitializeReapproval** workflow. It checks whether an assignment is flagged for re-approval and whether the end date is reached, which is the case for all assignments. Then it starts the defined re-approval workflow.

Open the workflow's wizard in the **Connectivity** view group:

- In the **Rule Search Parameters** tab, you can see that the **StartWorkflowsForReapproval** consistency rule is run.
- Check this rule in the **Provisioning** → **Policies** → **Rules** → **Default** → **Consistency Rules** → **Reapproval** folder. You can use the flag **updateConfiguredReapprovalDates** to automatically shift the re-approval date configured at the domain and/or the considered privileges: If the re-approval date lies in the past or within the approval period, it is shifted to the future by one re-approval period. Because the **InitializeReapproval** workflow performed this task, there is nothing to do.
- Check the filter conditions in the **Filter** tab. The **Search Base** works on the entire domain and the **Search Filter** is set to:
(objectclass="dxrAssignment" and dxrneedsreapproval="TRUE"
and dxrEndDate<="$(approvaldate)" and (not (dxrInApproval="TRUE") or not (dxrInApproval=*)))
which means that it searches for all assignments that have the dxrNeedsReapproval flag set and whose end date is reached and where no re-approval workflow is already started.

We recommend that you copy the rule and the workflow to be sure that changes in the configuration remain and are not overwritten by the next product update.

This workflow is set up as a separate workflow that runs exactly one consistency rule (InitializePrivilegeForReapproval). You could also run it with other consistency rules in your custom policy execution workflow.

9.3. Running the Use Case

Run the configured workflows at the defined time (the beginning of March). Be sure to run **InitializeReapproval** first and then run **StartReapprovalWorkflows**. We recommend that

you build a combined workflow that starts both workflows in sequence.

After completion, view the status of the workflow and check the trace file for errors.

View the Request Workflow Monitor area to check for the newly created re-approval workflows.

9.4. Alternative or Extended Configurations

This section gives hints for alternative or extended configuration of this use case.

9.4.1. Certifying Other Privilege Types

In this use case, we only ran re-approval on roles. If required, you can also run re-approval at the permission or group level. Set the corresponding flags and fields at these types of privileges.

You can also run a certification on any mix of roles, permissions and groups.

9.4.2. Setting Individual Re-Approval Dates or Re-Approval Periods

You may want to set individual timing parameters for specific privileges.

For example, you could set an individual re-approval date at the privilege to perform re-approval on that date. If you do not set the re-approval period at the privilege, the value from the domain is taken.

You could also set the re-approval period at the privilege to enforce shorter or longer re-approval cycles.

If you set these individual parameters at the privileges, you should schedule the **InitializeReapproval** and **StartReapproval** workflows to run on a daily basis. Otherwise, re-approvals are set but the execution is not performed.

10. Hints and Limitations

This chapter provides additional information on certification campaigns.

10.1. Manual and Automatic Assignments

A certification campaign requires certification only on manually-assigned privileges. Rejecting an automatically-assigned privilege does not make sense, because it will be assigned again as soon as the Provisioning rules for the user are evaluated or the access rights of the user are resolved for any reason. Consequently, rule-based assignments and assignments inherited from business objects cannot be certified.

However, an approver might be interested in seeing all assignments, including these automatically assigned ones, during the certification. As a result, these assignments are presented in Web Center or Business User Interface. An approver cannot really revoke them, but he can indicate that they should be revoked and give a reason. This information is stored with the certification task and can then be evaluated by the certification administrator and included into reports. It is their responsibility to bring this information to the attention of the relevant people in order to effect any improvements of automatic rules.

10.2. Certification Campaign Logging

You can increase the log level to obtain more details about campaign execution. Use the **Admin** Web application to add the following Java packages in **Java Server** → **Logging** → **Set log levels**:

- `com.siemens.idm.jobs.campaign (set value to ALL for all debug information)`
- `com.dirxcloud.dxi.campaign (set value to ALL for all debug information)`

10.3. Java-based Server Workflow Load

When a certification campaign is started and finished, a lot of tasks are performed:

At the start: creating a certification task for each certification subject along with finding approvers for them and sending start notifications.

At the end: checking all certification tasks, finding revoked assignments and resolving the new access rights of the affected users along with sending notifications.

These tasks will generate a high load on the affected IdS-J Server and may affect parallel provisioning or approval processes. As a result, consider allocating enough CPU and memory to the affected servers and reduce other processes in those periods.

DirX Product Suite

The DirX product suite provides the basis for fully integrated identity and access management; it includes the following products, which can be ordered separately.

DirX Identity

DirX Identity provides a comprehensive, process-driven, customizable, cloud-enabled, scalable, and highly available identity management solution for businesses and organizations. It provides overarching, risk-based identity and access governance functionality seamlessly integrated with automated provisioning. Functionality includes lifecycle management for users and roles, cross-platform and rule-based real-time provisioning, web-based self-service functions for users, delegated administration, request workflows, access certification, password management, metadirectory as well as auditing and reporting functionality.

DirX Directory

DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable, highly scalable, and secure LDAP and X.500 Directory Server and LDAP Proxy with very high linear scalability. DirX Directory can serve as an identity store for employees, customers, partners, subscribers, and other IoT entities. It can also serve as a provisioning, access management and metadirectory repository, to provide a single point of access to the information within disparate and heterogeneous directories available in an enterprise network or cloud environment for user management and provisioning.

DirX Access

DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy- and risk-based authentication, authorization based on XACML and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication including FIDO, identity federation based on SAML, OAuth and OpenID Connect, just-in-time provisioning, entitlement management and policy enforcement for applications and services in the cloud or on-premises.

DirX Audit

DirX Audit provides auditors, security compliance officers and audit administrators with analytical insight and transparency for identity and access. Based on historical identity data and recorded events from the identity and access management processes, DirX Audit allows answering the “what, when, where, who and why” questions of user access and entitlements. DirX Audit features historical views and reports on identity data, a graphical dashboard with drill-down into individual events, an analysis view for filtering, evaluating, correlating, and reviewing of identity-related events and job management for report generation.

For more information: support.dirx.solutions/about

Legal remarks

On the account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this document are available through the Eviden sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available locally. The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases. Eviden reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Eviden sales representative for the most current information. Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.