EVIDEN

Identity and Access Management

DirX Identity

Configuring the Maintenance Workflows for User Facets

Version 8.10.12, Edition August 2025

Table of Contents

Preface

This document presents a use case that describes how to configure and use the DirX Identity maintenance workflows for user facets. It consists of the following chapters:

- Chapter 1 provides an overview of the use case.
- Chapter 2 explains how to configure and run the use case.

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

Customers deploying the user facets feature available in DirX Identity V8.5 need to create new maintenance workflows for handling these objects. These workflows are needed to support status changes for users and user facets (startTime, endTime, DisableEndTime, deleteTime). The set of workflows to be configured for user facet maintenance depends on whether you run the Tcl-based maintenance workflows or the Java-based ones. The affected Tcl-based workflows are Consistency Check, Privilege Resolution and Policy Execution. The affected Java-based workflow is Check Consistency.

This use case document describes how to create and configure these workflows. It also describes how to configure complete database maintenance. The first part covers the Tcl-based workflows, while the second part covers the Java-based consistency workflows.

The following documents provide additional details about the concepts and procedures referenced in this use case document. We recommend that you become familiar with the information in these documents before proceeding with the tasks described in this use case document:

- For details on user facets, see the *DirX Identity Provisioning Administration Guide* → "Managing User Facets".
- For details on users, see the *DirX Identity Provisioning Administration Guide* → "Managing Users".
- For details on the Tcl-based DirX Identity maintenance workflows discussed in this use case, see the *DirX Identity Application Development Guide* → "Using the Maintenance Workflows" → "Understanding the Tcl-Based Workflows" → information about the Consistency Check, Privilege Resolution and Policy Execution workflows.
- For details on the Java-based consistency management workflows discussed in this use case, see the *DirX Identity Application Development Guide* → "Using the Maintenance Workflows" → "Understanding the Java-Based Workflows" → "Consistency Management Workflows" and the *DirX Identity Provisioning Administration Guide* → "Managing the Provisioning System" → "Managing Consistency".
- For details on how to define a nested workflow, see the *DirX Identity Tutorial* → "Follow-on Tutorials" → "Creating a Nested Workflow".
- For details on how to configure Tcl-based Provisioning workflows with DirX Identity Manager, see the *DirX Identity Connectivity Administration Guide* → "Managing Tcl-based Workflows" → "Copying Tcl-based Provisioning Workflows". This section describes the DirX Identity Manager Global View → Configure method.

You can also consult the online help provided with DirX Identity Manager (click **Help** in a dialog or topic to access the online help).

2. Use Cases

When working with user facets, the DirX Identity maintenance workflows need to be configured in a special way: The user facet must be processed first. The corresponding user may inherit privileges from the user facet, which may flag this user with "To Be Analyzed" (TBA). In a second step, these users need to be resolved. This chapter describes how to configure these workflows. The first section describes the configuration steps for the Tcl-based workflows. The second section describes the steps for the Java-based consistency workflow.

2.1. Configuring the Tcl-based Maintenance Workflows

This section describes the steps to set up and run the following use cases for maintaining user facets with the Tcl-based maintenance workflows:

- Consistency checking for user facets
- Privilege resolution for user facets
- Policy execution for user facets
- Maintenance of the entire database

2.1.1. Configuring Consistency Checking for User Facets

The Consistency Check workflow performs the following operations:

1. Checks the consistency of target system groups and accounts.
2. Checks the consistency of start and end dates and the state of the user or user facet.
3. Checks the consistency of start and end dates of assignments.
4. Performs privilege resolution of those users flagged with TBA (**dxrTBA=true**)

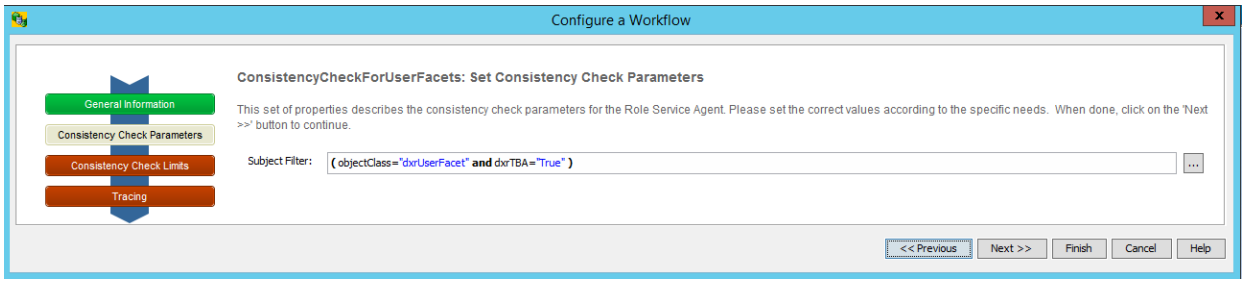
If the workflow finds inconsistencies in step 2 or 3, it flags the corresponding user with **dxrTBA=true**. It resolves these inconsistencies in Step 4. For user facets, privilege resolution does not take place; the corresponding user is simply flagged with **dxrTBA=true**. Because some additional users may be flagged with **dxrTBA=true** here, we need to use two workflows: the first workflow handles user facets and then flags the corresponding users in step 4. The second workflow performs the privilege resolution step for the previously flagged users.

2.1.2. Workflow 1: ConsistencyCheckForUserFacets

To configure the first workflow ConsistencyCheckForUserFacets:

- Log in to DirX Identity Manager and select the Connectivity view. You can use the Global View or the Expert View to perform the rest of these steps.
- Run the Workflow Configuration wizard (option **Configure** in the context menu) and select the Consistency Check workflow as a template.

- In the **Set Consistency Check Parameters** step, set the subject filter to user facets with **dxrTBA=true**:

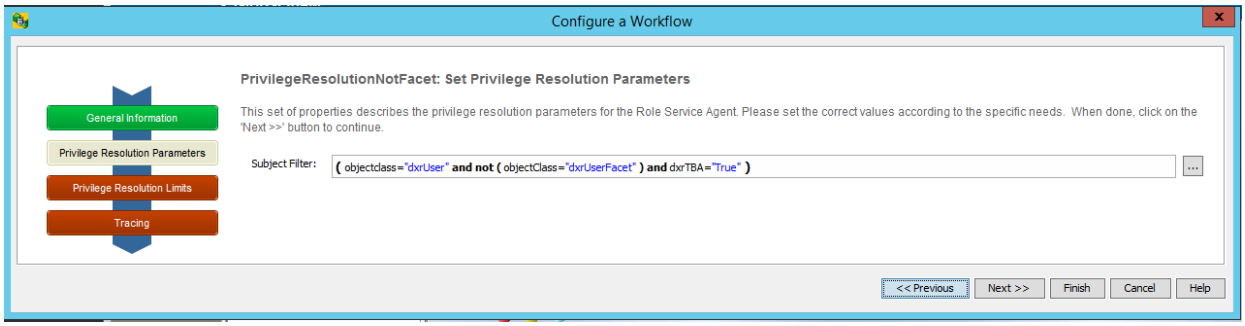


The filter is applied for step 4. Only user facets are handled here. Changes of the user facet state or assignment lead to flagging the corresponding user with **dxrTBA=true**.

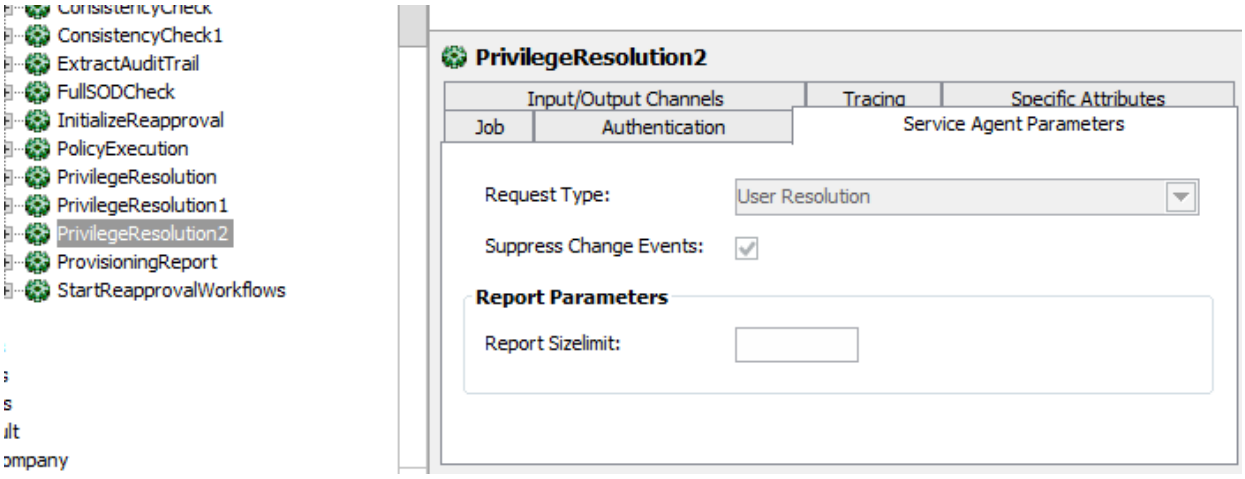
2.1.3. Workflow 2: PrivilegeResolutionNotFacet

To configure the second workflow PrivilegeResolutionNotFacet:

- Log in to DirX Identity Manager and select the Connectivity view.
- Run the Workflow Configuration wizard (option **Configure** in the context menu) and select the Consistency Check workflow as a template.
- In the Set Privilege Resolution Parameters step, set the subject filter to handle users and disallow any handling of user facets, since we've already done this in workflow 1:



- In the **Connectivity** → **Expert View** → **Jobs** tree, select the job **PrivilegeResolution2** and open it for editing.
- Select the Service Agent Parameters tab. In this tab:
- Set **Request Type** to **User Resolution**, which selects to resolve just the given users.
- Check **Suppress Change Events** to prevent change events from being initiated for user changes.



- Create a nested workflow that contains workflow 1 and workflow 2. See the *DirX Identity Tutorial* follow-on exercise "Creating a Nested Workflow" for an example.
- Create a schedule for this nested workflow which runs our Workflow 1 first and then runs Workflow 2. Go to **Connectivity** → **Expert View**→ **Schedules** → **Default** to see some example schedules. Click **Help** to get information about how to set the schedule configuration object's time controls and the rules for creating schedules.

2.1.4. Configuring Privilege Resolution for User Facets

Configuring privilege resolution for user facets is analogous to configuring for consistency checking:

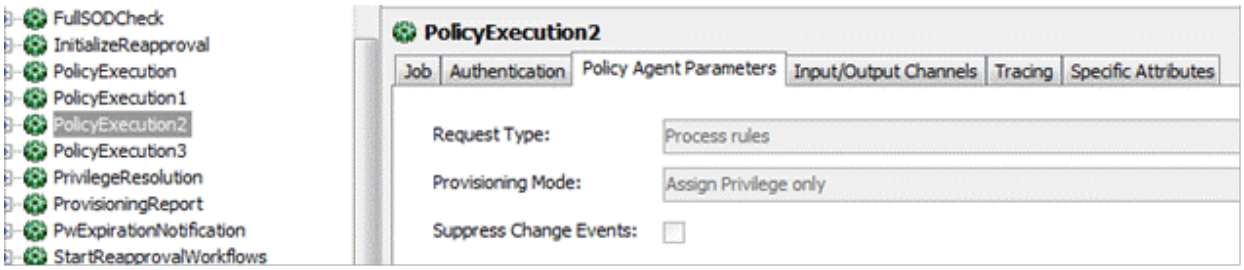
- Configure Workflow 1 with the subject filter: **(&(objectClass=dxrUserFacet)(dxrTBA=true))**.
- Configure Workflow 2 with the subject filter: **(&(objectClass=dxrUser)(!(objectClass=dxrUserFacet)) (dxrTBA=true))**.
- For Workflow 1, set **Request Type** to **Resolution**.
- For Workflow 2, set **Request Type** to **User Resolution**.
- Create a nested workflow that runs Workflow 1 first and then Workflow 2.

2.1.5. Configuring Policy Execution for User Facets

If rules for user facets should be applied, we recommend using the following configuration:

Workflow 1: Policy Agent

- In the **Connectivity** → **Expert View** → **Jobs** tree, select the job **PolicyExecution2** and open it for editing.
- In the Policy Agent Parameters tab, configure the Provisioning Mode to **Assign privilege only**.



Workflow 2: Privilege Resolution for User Facets

- Configure the subject filter: **(&(objectClass=dxrUserFacet)(dxrTBA=true))**.
- Configure **Request Type** to **User Resolution**.

Workflow 3: Privilege Resolution for other User Types

- Configure the subject filter: **(&(objectClass=dxrUser)(!(objectClass=dxrUserFacet))(dxrTBA=true))**.
- Configure **Request Type** to **User Resolution**.

We recommend building a nested workflow that runs workflow 1 > workflow 2 > workflow3 in the given sequence.

2.1.6. Maintaining the Entire Database

To maintain the entire database, use the workflow structure described in the previous sections of this use case, omitting **(dxrTBA=true)** in the subject filters. This process resolves all the users in the database, not just the ones with **dxrTBA=true**.

2.2. Configuring the Java-based Consistency Workflows

This section describes how to integrate consistency for user facets into the Java-based maintenance workflows. The only affected workflow in this case is the Check Consistency workflow.

2.2.1. Configuring Check Consistency

The Check Consistency workflow performs some checks on the entries that match the selection criteria. In particular, it applies consistency rules.

Unlike the Tcl-based Consistency Check workflow, the Java-based Check Consistency workflow does not check start and end dates of users and assignments or perform privilege resolution. These tasks are performed by the Mark Affected Users and User Resolution workflows.

As a result, you only need to duplicate the Check Consistency workflow: the first instance needs to handle user facets, while the second instance handles the other user types. The non-user object types (roles, permissions, groups, accounts) can be processed in either of the two workflows.

Let’s assume here that the first workflow handles only the user facets and the second workflow handles all other users and object types.

To create a Check Consistency workflow for user facets only:

- In Identity Manager’s Connectivity view group, open the Global View. Select the workflow line between the two Identity stores, and then select **New** from the context menu. Select the **CheckConsistency** workflow from the presented template list.
- In the wizard step on Consistency Check Attributes, change the user filter so that it matches only user facet objects: **&(objectClass=dxrUserFacet)**
- Disable the flags for check roles and permissions and check accounts and groups.
- Enable the flag for applying consistency rules.

Change the existing Check Consistency workflow to include users, but not user facets:

- In the Global View of Identity Manager’s Connectivity view group, select the **CheckConsistency** workflow and then run the configuration wizard.
- In the wizard step on Consistency Check Attributes, change the user filter so that it excludes user facet objects: **(&(objectClass=dxrUser)(!(objectClass=dxrUserFacet)))**

Now define schedules for both workflows so that the user facet workflow runs before the other one.

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.