EVIDEN

Identity and Access Management

DirX Identity

Using Segregation of Duties

Version 8.10.10, Edition June 2025

Table of Contents

Preface

This document describes a set of use cases that explain how to use specific features of DirX Identity. It helps users to model their use case with DirX Identity and to set up and run their DirX Identity system.

The goal of this document is to explain how to use segregation of duties (SoD).

It consists of the following chapters.

- Chapter 1 provides an overview of the described use cases.
- Chapter 2 explains how to use the built-in segregation of duties feature.

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 for controlling access rights to resources in connected systems. A set of features like access policies or approval workflows allows securing the assignment of access rights. DirX Identity also allows using segregation of duties (SoD) policies to detect conflicting assignments as early as possible. Mitigation workflows can be started to approve exceptions to these rules.

1.1. Use Cases

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

Using DirX Identity SoD Policies

This use case works with DirX Identity's built-in SoD policies. It allows configuring rules for any type of privilege. If you define rules at the permission or role level, you can control SoD over many different target systems.

1.2. Use Case Comparison

The following table compares the two use cases described in this document to help you with your decision process.

Table 1. Use Case Comparison

Criteria	**DirX Identity SoD Policies**	**Using SAP GRC (Access Control)**
Complexity of solution setup	Low	High
Pre-configured SoD policies	Few	Comprehensive
SoD policies on role / permission level	Yes	No
SoD policies on group level	Yes	Yes
Hierarchical SoD policies	Yes	No

The table presents the following evaluation criteria:

Complexity of solution setup – the effort and complexity involved in setting up the initial solution.

Pre-configured SoD policies – the availability of pre-configured SoD policies that can be directly used in compliance processes.

SoD policies for role / permission level – whether the use case offers the option of setting up SoD policies at the role or permission level.

SoD policies for group level - whether the use case offers the option of setting up SoD policies at the group level.

Hierarchical SoD policies - whether the use case offers the option of setting up SoD policies at different levels, for example between a role and a group.

1.3. General Hints and Guidelines

Segregation of duties (SoD) policies can help to fulfill compliance regulations. However, additional checks require additional time, and that will slow down your company processes. Therefore, we recommend that you:

- Set up only those SoD policies that are truly necessary.
- Configure only the minimum number of necessary SoD checks in your request workflows.

2. Using DirX Identity SoD Policies

This chapter describes how to set up SoD policies with DirX Identity's built-in policy mechanism.

2.1. About this Use Case

You can set up SoD policies within DirX Identity at any privilege level: roles, permissions and groups. You can even set up policies at different levels; for example. between a role and a group. The following figure illustrates the options for setting up SoD policies, except for the option to set up a policy between a role and a group (which means that you can define hierarchical SoD).

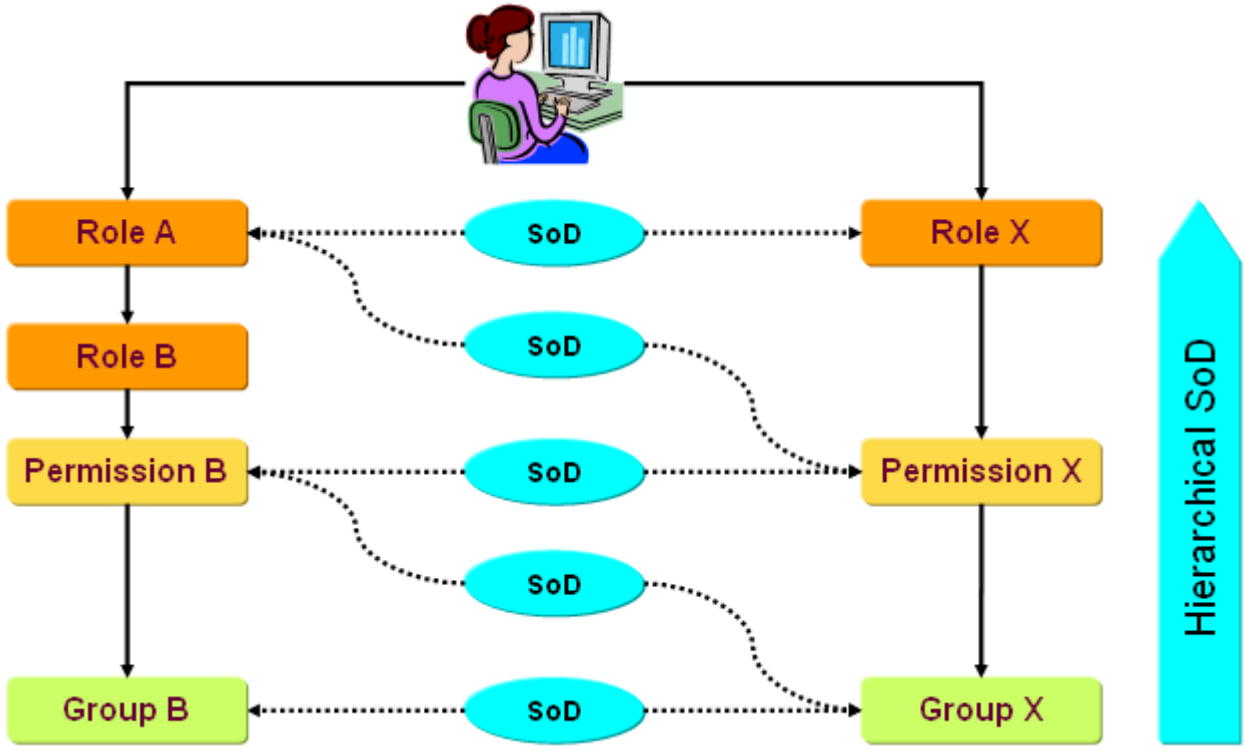

Figure 1. Setup of SoD Policies

The disadvantage of the SoD mechanism is that the policy engine must resolve users multiple times during rule execution if SoD checking is enabled, which lowers performance.

2.1.1. Documentation Hints

You can find additional information related to this use case in the following documents:

2.1.1.1. Application Development Guide

- **Understanding Request Workflows → Request Workflow Architecture → Selecting Request Workflows → Assignment Workflow Selection → Workflow Selection Mechanism for SoD** - describes how SoD request workflow selection works.

- **Understanding Tcl-based Workflows → Full SoD Check Workflow** - explains and gives hints for configuring the SoD full check workflow.
- **Understanding Tcl-based Workflows → Policy Execution Workflow** - explains how the policy execution is influenced when SoD is enabled.

2.1.1.2. Customization Guide

Customizing Status Reports → Customizing Provisioning Status Reports → Virtual Objects and Attributes – explains how to use the described attributes to add SoD information to your status reports.

2.1.1.3. Provisioning Administration Guide

Use the context-sensitive help when working with SoD policies, SoD tabs at users or SoD activities of request workflows. Alternatively, you can access these parts of the documentation directly through the online help.

This guide contains two other sections that give additional insight into the topic:

- **Managing Policies → Managing SoD** - general hints how to manage SoD policy objects and folders.
- **Managing Auditing → Managing SoD** – provides an overview of the SoD topic.
- **Managing Users → Working With Links at User Entries** - explains the meaning of the dxrPrivilegesGrantedLink attribute for SoD.

2.1.1.4. User Interface Guide

- **Using DirX Identity Web Center → Using the Self Service Menu / Using the Users Menu → Show SoD Violations** - explains how to view SoD violations.

2.1.1.5. Tutorial

Follow on Tutorials → Applying SoD policies - demonstrates (self training) how SoD works.

2.1.2. Specific Hints and Guidelines

Segregation of duties policies can help to fulfill compliance regulations. However, we recommend the following:

- Keep the number of SoD policies you create to the necessary minimum. Defining too many SoD policies may initiate a large number of approval workflows, which will slow down your assignment processes. Having too many policies also affects the overall performance of the privilege resolution mechanism even though the algorithms are optimized for performance.
- Activating SoD policies forces the policy execution workflow to perform immediate privilege resolution during rule-based processing even if you have configured it not to do so (that is, you did not set the **Assign Privilege and Resolve** option in the workflow wizard). The reason for this is that DirX Identity SoD checking works hierarchically and so the resolved privileges must be known. Performing this operation decreases the

policy execution service performance. To avoid too much loss of performance, try to define rules that assign multiple privileges instead of defining multiple rules with one privilege each. This recommendation comes from the fact that a resolution is performed once per rule.

- If you define an SoD workflow for a privilege that requires approval and the approval workflow is different from the SoD workflow, the SoD workflow has precedence, so the normal approval workflow is not started! We recommend keeping SoD workflows and normal approval workflows the same: you should include SoD approvers into your normal workflows and then use them as SoD workflows.

2.2. Setup and Configuration

Using DirX Identity's SoD feature requires you to set up:

- The central SoD flag at the domain object
- SoD policies for each conflicting pair of privileges
- SoD request workflows
- A regularly running full SoD check
- Reports and queries
- Access policies

2.2.1. Set Up the Domain-Wide SoD Flag

Set the **Segregation of duty (SOD) checks** flag at the domain object. Note: restart DirX Identity Manager if you intend to test the policies within the Manager.

2.2.2. Set Up SoD Policies

Define SoD policies for each conflicting pair of privileges. Set the **Is Active** flag at each policy.

If the related privilege combination is already assigned to a user, an SoD workflow is started immediately to request approval for this SoD violation. As a result, you should be careful when activating SoD policies because the SoD process can generate a large number of SoD workflows within seconds.

2.2.3. Set Up Request Workflows for SoD

Ensure that assignment approval workflows are correctly configured. The workflow engine uses these workflows if an SoD approval is required.

2.2.4. Set Up a Full SoD Check

Run a FullSODCheck workflow regularly to detect SoD violations that are not currently approved. Note that this workflow automatically creates SoD approval workflows for all unresolved conflicts. It also reports all discovered SoD conflicts that have not yet been approved in its log files.

2.2.5. Set Up SoD Reports and Queries

DirX Identity comes with the following pre-configured SoD reports:

SoD policies with all properties - a report on all configured SoD policies.

SoD exceptions with all properties - a report on all approved and existing SoD exceptions.

Both reports are ready to use.

If you want to modify the reports, copy them to the folder **Status Reports** → **Customer Specific**.

You can also use or set up queries. DirX Identity comes with two default queries in the folder **Policies** → **Queries**:

All Active SoD Policies - displays all active SoD policies. This is the most important query for productive use.

All Inactive SoD Policies - displays all inactive SoD policies.

Copy these query folders to a project-specific folder (use the domain name as folder name) and refine them accordingly. Use, for example, another Search base that retrieves only active SoD policies from your specific project folder or define a query folder that retrieves all exceptions for a specific name. Use, for example, the filter:

(objectClass="dxrSodException" and cn="*$Name[Smith]*")

2.2.6. Set Up Access Policies

Think about the following access policies for your scenario:

- For the SoD reports you have defined, decide and define who is allowed to execute them.

2.3. Running the Use Case

After setting up the SoD scenario, the policies have an immediate effect, which means that they are evaluated during each privilege assignment. SoD mitigation workflows are started as necessary to request approval.

2.3.1. Setting Up or Modifying SoD Policies

After setting up or modifying an SoD policy, we recommend that you test it.

2.3.2. Checking the Full SoD Check Result

Don’t forget to check the full SoD check runs, especially after setting up new SoD policies.

Using DirX Identity Manager or Web Center, assign all privileges of a policy or pairs of these privileges to a user. If the policy is correctly configured, the workflow engine notes the

conflict and asks you if you want to proceed. Abort the assignment (otherwise a real approval workflow is started!).

2.3.3. Using SoD Reports or Queries

Note that SoD exceptions are always stored below the relevant SoD policy. You can view all exceptions either from the user side (that means all exceptions valid for that user) or from the policy side (all users that have exceptions for that policy).

You can use reports or queries or a combination of both.

2.4. Alternative or Extended Configurations

There are currently no extended or alternative configurations available for the use case just described.

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.