Secure Configuration Guide

9.3.0

Table of Contents

About This Guide

The Secure Configuration guide provides recommended best practices for secure OneStream installation, configuration, and operation. The best practices in this guide are intended for anyone who implements OneStream to help reduce security risk, enforce least-privilege access, and promote consistent, well-governed deployments. Use the reference tables in this guide regularly to ensure your implementation is secure.

Platform Services

This section provides best practice guidance for installing, configuring, and operating Platform Services:

- Access Management
- Authentication
- Networking
- Data Integration
- File Management
- Application Auditing
- Application Settings and Operation
- Web Server Settings and Operation

Access Management

Use the reference tables below to identify access management best practices for Platform Services and their corresponding IDs.

Administrator Groups

Rule ID	Best Practice
OS-BP-PS-AM-001	Restrict members of the Administrator group to five or fewer to simplify administrative activities.

Access Groups

Rule ID	Best Practice
OS-BP-PS-AM-002	Use Application Security Roles to distribute application management.
OS-BP-PS-AM-003	Separate administrative duties using System Security Roles to manage Users, Access Groups, and System Security assignments. Users do not have to be a member of the Administrators Group to manage Users, Groups, or System Security Assignments.

OneStream IdentityServer Security Roles

Rule ID	Best Practice
OS-BP-PS-AM-004	Selectively and independently grant users permission for accessing and managing Personal Access Tokens (PATs) such as AccessAsNonInteractiveUser and AdministerNonInteractiveUser to reduce the risk of unauthorized API data access.
OS-BP-PS-AM-005	Selectively and independently grant users permission to manage Identity Providers (IdPs) such as ManageIdentityProviders to reduce the risk of unauthorized user authentication.

OneStream IdentityServer Portal

Rule ID	Best Practice
OS-BP-PS-AM-006	Revoke Personal Access Tokens when no longer in use or when generated by a user no longer with the company.

Smart Integration Connector Security Roles

Rule ID	Best Practice
OS-BP-PS-AM-007	Selectively grant users permission to administer Smart Integration Connector using SmartIntegrationConnectorAdminPage.

Authentication

Use the reference tables below to identify authentication best practices and their corresponding IDs.

Authentication Types

Rule ID	Best Practice
OS-BP-PS-AN-001	Integrate with a local Identity Provider for Single Sign On because it provides the highest level of secured authentication.
OS-BP-PS-AN-002	Consider NativeIDs the exception, and use all available password controls, like rotating passwords and establishing complexity rules.
OS-BP-PS-AN-003	Disable the ability to create and use Native IDs if they are not in practice to prevent unauthorized access.

Login Inactivity

Rule ID	Best Practice
OS-BP-PS-AN-004	Use a Logging 'days inactive' threshold to prevent unauthorized access through inactive users.

User Activity Inactivity Timeout

Rule ID	Best Practice
OS-BP-PS-AN-005	Establish user activity timeouts to close OneStream sessions after a period of inactivity.

Authentication Configuration

Rule ID	Best Practice
OS-BP-PS-AN-006	Use JSON Web Encryption (JWE) to encrypt data with strong algorithms, manage encryption keys securely, and minimize data exposure.
OS-BP-PS-AN-007	Use Demonstrating Proof-of-Possession (DPoP) in OAuth 2.0 by providing unique proofs for each request, securely storing keys, using reliable signing algorithms, and validating timestamps and nonces to prevent replay attacks.

Networking

Use the reference tables below to identify networking best practices and their corresponding IDs.

Network Encryption

Rule ID	Best Practice
OS-BP-PS-NT-001	Configure SSL or TLS for all application traffic to secure network transport. OneStream supports TLS versions 1.2 or 1.3.

Software as a Service (SaaS) Instance Access

Rule ID	Best Practice
OS-BP-PS-NT-002	Whitelist IP access to OneStream SaaS to ensure authorized access to OneStream only comes from valid IP addresses.

Smart Integration Connector Azure Relay Access

Rule ID	Best Practice
OS-BP-PS-NT-003	Whitelist Azure Relay to your Firewall to ensure authorized access to Azure Relay. See "Networking and Whitelisting" in the *Smart Integration Connector Guide*.

Data Integration

Use the reference tables below to identify data integration best practices and their corresponding IDs.

Passwords

Rule ID	Best Practice
OS-BP-PS-DI-001	Rotate all data integrated source passwords regularly to prevent prolonged access to data sources.

Smart Integration Connector Local Gateway

Rule ID	Best Practice
OS-BP-PS-DI-002	Implement SIC Local Gateway Server redundancy to ensure high availability failover.

Smart Integration Connector Local Gateway IP Whitelist

Rule ID	Best Practice
OS-BP-PS-DI-003	Whitelist Azure Relay to your Firewall.

Smart Integration Connector Setup

Rule ID	Best Practice
OS-BP-PS-DI-004	Establish a Web API Key to secure Smart Integration Connector Gateway to Local Gateway connections for full control over who can access data sources in your network.

File Management

Use the reference tables below to identify file management best practices and their corresponding IDs.

File Uploads

Rule ID	Best Practice
OS-BP-PS-FM-001	Use File Extension whitelisting to prevent unauthorized executables from being uploaded to the Application Server.

File Operations

Rule ID	Best Practice
OS-BP-PS-FM-002	Do not perform file operations directly on the server in Business Rules or other customizations due to maintenance concerns, storage cleanup, and security considerations.

Database

Use the reference table below to identify database best practices and their corresponding IDs.

Maintenance Groups

Rule ID	Best Practice
OS-BP-PS-DB-001	Limit access and Maintenance Groups for Ancillary Tables to designated users, instead of setting the access to Everyone.

Application Auditing

Use the reference tables below to identify application auditing best practices and their corresponding IDs.

Business Rules

Rule ID	Best Practice
OS-BP-PS-AA-001	Establish periodic reviews to ensure coding and maintenance activity aligns with organization objectives.

Data Management Jobs

Rule ID	Best Practice
OS-BP-PS-AA-002	Establish periodic reviews to ensure coding and maintenance activity aligns with organization objectives.

Users

Rule ID	Best Practice
OS-BP-PS-AA-003	Establish periodic reviews to ensure registered users align with organization objectives.

Access Groups

Rule ID	Best Practice
OS-BP-PS-AA-004	Establish periodic reviews to ensure Access Group membership aligns with organization objectives.

Application Settings and Operation

Use the reference tables below to identify application settings and operation best practices and their corresponding IDs.

Task Inactivity

Rule ID	Best Practice
OS-BP-PS-ASO-001	Set Task Inactivity Timeout to manage queued tasks.

Logging

Rule ID	Best Practice
OS-BP-PS-ASO-002	Ensure 'Detailed Error Logging' is set to False.

Web Server Settings and Operation

Use the reference table below to identify Web Server settings and operation best practices and their corresponding IDs.

Logging

Rule ID	Best Practice
OS-BP-PS-WSSO-001	Ensure 'Detailed Error Logging' is set to False.
OS-BP-PS-WSSO-002	Ensure 'Native App Detailed Logging' is set to False.
OS-BP-PS-WSSO-003	Ensure 'Enable SSO Logging' is set to False.

AI Services

This section contains best practice guidance for installing, configuring, and operating AI Services. See Access Management.

Access Management

Use the reference table below to identify access management best practices for AI Services and their corresponding IDs.

Access Groups

Rule ID	Best Practice
OS-BP-AIS-AM-001	Adhere to least privilege access control schema for AI Solutions.
OS-BP-AIS-AM-002	Adhere to least privilege access control schema for AI Data Tools.