System Wide Information Management (SWIM)

SWIM Cloud Distribution Service (SCDS)

General Guideline with Standards

Version 1.1

Document Change History

Version	Date	Description of Changes
1.0	August 5, 2024	Initial draft/submission
1.1	September11, 2024	Updated the Solace developer documentation URL to the footnote and glossary.

Table of Contents

1   SCOPE

The System Wide Information Management (SWIM) Program is a National Airspace System (NAS)-wide information system that supports Next Generation Air Transportation System (NextGen) goals. SWIM will enable increased common situational awareness and improved NAS agility to deliver the right information to the right place at the right time. SWIM-enabled systems and users are identified as producers and consumers of Federal Aviation Administration (FAA) data and NAS information. Consumers can request and receive information on demand or subscribe to selected information for automatic delivery as it is published. Producers publish information for use by subscribed consumers and provide information upon request from on-demand consumers.

This document specifies the guidelines, rules, standards, and compliance procedures (referred to herein as the "Standards") for consumers of the FAA SWIM Cloud Distribution Services (SCDS), which is a SWIM system. The following Standards are specific to the utilization of services and data products provided by SCDS. Violation of any of these Standards without first obtaining a standard exemption in accordance with this document, MAY result in termination of service at the FAA's discretion, per SCDS Service Access Agreement.

1.1. Background

SCDS is a publicly accessible cloud-based infrastructure dedicated to providing real-time SWIM data to the public via Solace Java Message Service (JMS) messaging. SWIM data sets provide information relating to weather, flight and flow, aeronautical, and surveillance. Accessing SWIM data formerly required all external consumers to have a dedicated Virtual Private Network (VPN) connection through the NAS Enterprise Security Gateway (NESG) to the NAS Enterprise Messaging System (NEMS). SCDS was developed to allow the dissemination of SWIM data without a dedicated VPN. This allows for a simplified, quicker method of accessing FAA data and lower costs for the upfront connection.

2   SCDS GENERAL STANDARD

The purpose of SCDS is to provide SWIM data to as diverse a population of users as possible. However, the goal of increasing user population is balanced with operational cost efficiency.

This section details the permitted use of data obtained via SCDS enabled services.

2.1. Appropriate Usage of SCDS Data

SWIM data obtained through SCDS is **not intended** for NAS-impacting usage and SHOULD NOT be used as the sole source for any aviation-safety related, law enforcement, or judicial activity that relies on the availability, validity, timeliness, or accuracy of SWIM data. SCDS Consumers MAY use SWIM data for non-NAS-impacting purposes.

2.1.1   Background

a.   NAS Security and Enterprise Operations (NASEO) manages SWIM user support. The SWIM Enterprise Control Center (SECC), the Enterprise Data Services (EDS), and groups within NASEO provide SWIM user support services, as per current NASEO processes.

The primary factor in defining the difference between SCDS and the NESG is the level of support offered to users of each SWIM enabled service. NASEO does not provide 365 24/7 support to SCDS, therefore users of SCDS MUST NOT use the data they obtain for NAS-impacting purposes.

b.   SCDS data consumers who use SWIM data and provide non-NAS impacting external business service operations will be responsible for notifying their users of planned or unplanned outages, and of the acceptable use of data obtained via SCDS as per this document.

c.   SCDS does not provide the following SWIM services:

   1.   Sensitive Data Access
   2.   Web Services or Request-Reply Services

2.1.2   Specific Exceptions

a.   **Collaborative Decision Making (CDM) Access**:

SCDS users may request Collaborative Decision Making (CDM) data only if they are a verified CDM member. CDM data access is limited to qualified aviation related entities that meet the data-sharing criteria specified in the current FAA CDM Memorandum(s) of Agreement (MOA) and that are verified CDM members.

3   DETAILED STANDARDS

3.1. Data Compression

3.1.1   Background

The FAA has enabled message compression for connections to SCDS. Message compression reduces the size of message data frames to be transmitted over a network link. Using data compression reduces bandwidth consumption between clients and SCDS, resulting in cost savings with data egress.

3.1.2   Applicability

The overarching goal is for all SCDS consumers to use data compression to ensure operational cost effectiveness. When connections are established using compression, messages sent are compressed before transmission, and they are decompressed when received by the client application.

3.1.3   Data Compression Standard Specifications

This section describes the standards for using compression on SCDS.

   a.   All users MUST keep compression enabled.

        Note: SCDS consumers MUST configure their consumer applications to compress the data so
        that it is optimized for size or for transmission speed. By default, connection factories have
        compression set to a compression level of 1.

   b.   If a user disables data compression, OR if a user is using a messaging Application Programming
        Interface (API) or protocol that does not support compression, SCDS administrators MAY
        disable or terminate the user's subscriptions.

   c.   The FAA will conduct audits periodically on all subscriptions to SCDS to ensure compression is
        being used in accordance with this document.

3.1.4   Data Compression Standard Exceptions

The FAA will consider exceptions to the Data Compression standard on a case-by-case basis pursuant to
Section 4, *Exemption Requests Standard*.

Note: Users who are granted Solace Java Message Service (JMS) connection exceptions will also be
exempt from the Data Compression standard.

3.2. JMS Connection

3.2.1   Background

SCDS supports the JMS 1.1 specification to provide connections to consumer queues. The Solace System
JMS implementation supports JMS 1.1.[1] Solace does not currently provide implementation for any
methods or interfaces introduced in JMS specification 2.0. Users must continue to use JMS specification
1.1 methods and interfaces in their applications[2]. The JMS libraries provided in the SCDS Jumpstart Kit
contain default configurations that comply with SCDS standards for native compression support in the
consumer application. SCDS's ability to deliver compressed data subscriptions are critical to maintaining
the operational cost of SCDS within its congressionally appropriated budget.

3.2.2   Applicability

The purpose of this JMS connection standard is to restrict access to SCDS so that only authorized clients
can establish and manage connections. This standard applies to all SCDS users.

3.2.3   JMS Connection Standard Specifications

This section describes the standards for using JMS connections.

   a.   JMS is the only authorized API for SCDS. Users MUST NOT access SCDS data products using other
        APIs or protocols without receiving a standard exemption. Users requesting exemptions must

---

[1]https://docs.solace.com/API/Solace-JMS-API/Quick-Start.htm
[2] https://docs.solace.com/API/Solace-JMS-API/JMS-API-supported-environments.htm#Messagi2

refer to Section 4, *Exemption Requests Standard*. Violation of this standard MAY result in termination of service at the FAA's discretion.

b. The JMS implementation provided by the SCDS Jumpstart Kit is officially supported by the FAA.

c. Connecting to SCDS using third party proprietary API libraries is NOT RECOMMENDED and users that choose this approach do so with limited technical support from the FAA.

3.2.4   JMS Connection Standard Exceptions and Stipulations

This section describes the exception standards and request process.

a. Users MAY request an exception for research and academic purposes.
b. Users that apply for a JMS connection exception MUST follow the standard exemption request process detailed in Section 4*, Exemption Requests Standard*.
   If users are approved for JMS connection exceptions, they are also exempt from the data compression standard detailed in Section 3.1, *Data Compression* above.
c. SCDS connections that use Compression Supported Messaging APIs (CSMA) have a standing exception to the JMS Connection Standard, per Section 3.2.4.1, *Compression Supported Messaging APIs (CSMA) Standard Exception Stipulation*, below.

3.2.4.1 Compression Supported Messaging APIs (CSMA) Standard Exception Stipulation

Solace provides enterprise messaging APIs that enable users to develop consumer applications in languages other than Java. Building SCDS clients using these CSMAs DOES NOT require a standard exemption request submission, described in Section 4, *Exemption Requests Standard*. If CSMAs other than Java are used, it is the user's responsibility to enable compression.

CSMA support can be obtained through the Solace website[3].

a. These proprietary connection APIs are exceptions to the SWIM SCDS Open Data Access standard and are therefore NOT authorized SCDS connection technologies. The FAA/SWIM makes no assurance that these CSMAs will be viable connection methods to SWIM Cloud-based systems in the future. Clients that use these methods do so at their own risk.
b. All SCDS Helpdesk trouble shooting ends at the verification of message population of the SCDS user's queue.
c. Use of CSMAs MUST comply with the data compression standard stated in Section 3.1.3, *Data Compression Standard Specifications*.

---

[3] https://docs.solace.com/API/Messaging-APIs/Solace-APIs-Overview.htm

3.3.   User Allowlist

3.3.1   Background

Allowlisting is a strategy under which a user can only take actions within their account that an administrator has explicitly allowed in advance. In the context of SCDS, allowlisting refers to granting a user permission to be excluded from standard SCDS account management practices.

3.3.2   Applicability

SCDS offers two types of exclusions: exclusion from subscription audits, and exclusions from account audits.

- Subscription Audits:
  - The FAA will disable inactive subscriptions after 60 calendar days of inactivity.
  - The FAA will delete disabled subscriptions 30 calendar days after disablement.
- Account Audits:
  - The FAA will disable accounts if a user has not logged in for more than 90 calendar days.
  - The FAA will send the user a warning email of pending deletion if the user has not logged into the account for more than 245 calendar days.
  - The FAA will delete accounts if a user has not logged in for more than 275 calendar days.

3.3.3   User Allowlist Standard Specifications

This section describes the standards for users requesting to be allowlisted.

a.   Users requesting to be allowlisted MUST follow the standard exemption request process detailed in Section 4,*Exemption Requests Standard*.

b.   Users granted exemption requests MAY be excluded from subscription audits, and/or account management audits, at the FAA's discretion.

3.4. Internal Data Redistribution

3.4.1   Background

Each SCDS subscription results in an expense to the FAA. To ensure that the cost of SCDS remains manageable, the Internal Data Redistribution standard governs high-volume SCDS users who consume more than 200 gigabytes (GB) of data per day, or a total data consumption limit of 2 terabytes (TB) of data per month. This allows the FAA to continue to provide SWIM data service free of charge to subscribers.

3.4.2   Applicability

Consuming duplicate SCDS subscriptions or using similar data feeds with identical product filters creates redundant data egress. Instead of creating duplicate subscriptions, users requiring data for multiple instances, for example, for development, testing, and operations environments, MUST re-distribute data internally from a single subscription. Users MAY, however, have multiple feeds with varying filter types.

3.4.3   Internal Data Redistribution Standard Specifications

This section describes the standards for users to re-distribute subscriptions.

a. Organizations that consume 200 or more GB per day OR 2 TB of data per month will be identified as high-volume users who MUST implement internal data redistribution.

b. Users MUST NOT create identical, duplicate subscriptions within the same user accounts. The SCDS team will be reviewing these connections.

3.4.4   Internal Data Redistribution Standard Exceptions

Organizations that exceed the data consumption limit will be contacted by the SWIM Program Office (PO) to explore opportunities and schedules to become compliant. Time-based exceptions will be granted to honor good faith efforts to meet this standard.

4   Exemption Requests Standard

The standards in this document are intended to create a sustainable SCDS operational model that supports most of the use cases of the SCDS user community. SCDS users with unique circumstances can request an exemption that will expire after a limited period. These exemptions will be evaluated on a case-by-case basis against SCDS security, cost, and other pertinent factors. Exemptions will be granted at the FAA's sole discretion.

a. Requestors MUST identify their <u>user type</u> to be approved for exemptions. Some examples of user types include industry user (academic, business, airline, research), NAS-impacting users, non-NAS impacting users, admin users, NASEO users, Tech Ops users, and FAA executive users.

b. Requestors MUST provide a summary of their organizational information as it relates to the FAA.

c. Requestors MUST submit a description of their intended use of the SWIFT Portal for review to be considered for exemptions.

d. When making a request for exemptions, requestors MUST provide a valid and verifiable email address.

e. Exemptions expire after the time period specified in the exemption approval notice. Users may apply to renew the exemption at that time.

5   REFERENCES

The following references were used to develop this standard and provide applicable guidelines and on writing the document.

5.1. Government Documents

- Writing User-Friendly Documents

https://my.faa.gov/content/dam/myfaa/tools_resources/branding_writing/plain_language/learn_more/Writing_User_Friendlier_Documents.pdf

- SWIM Controlled Vocabulary, March 2019[1].
  https://semantics.aero/pages/swim-vocabulary.html

- To establish writing standards for all FAA documents [2].
  FAA Writing Standards 1000.36

- M-13-13: Open Data Policy –Managing Information as an Asset [3]
  https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2013/m-13-13.pdf

- SWIM Cloud Distribution Service (SCDS) Service Access Agreement Standard, November 2023
  https://support.swim.faa.gov/hc/en-us/article_attachments/24884336778132

5.2. Non-Government Documents

- RFC 2119, Key words for Use in RFCs to Indicate Requirement Levels, Network Working Group, March 1997[4].
- rfc2119.txt.pdf (rfc-editor.org)

5.3. Order of Precedence

In the event of a conflict or inconsistency between the text in this document and the references cited herein, the text in this document takes precedence. This document does not take precedence over law, regulation, and in some cases, policy.

6   TERMS AND DEFINITIONS

6.1. Key Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [4]

6.2. Terms and Definitions

All terms used in this document are defined in the SWIM Controlled Vocabulary [1] along with information about terms' sources and relationships to other terms.

Please see the list below for additional terms and definitions relevant to this Standard:

Term	Definition
Collaborative Decision Making (CDM) Data	A joint government/industry initiative to improve the Air Traffic Management (ATM) system through increased information exchange among all stakeholders. The CDM process involves sharing data to create a common view on which to base decision-making and includes stakeholders in that process. CDM transcends specific programs and is both a philosophy and a process by which to accommodate stakeholder preferences to the maximum extent possible. CDM data facilitates this. For SCDS purposes, a user that is getting CDM data has a CDM Memorandum of Agreement (MOA) with the FAA to receive data that is not available to standard consumers. CDM data must be acquired from the NESG. See CDM website: CDM | Collaborative Decision Making faa.gov
Compression Supported Messaging API (CSMA)	An application using Solace messaging APIs which enables the consumer to access an event broker. See link for Message Compression Support for each Solace Messaging API: https://docs.solace.com/API/Messaging-APIs/Solace-APIs-Overview.htm. (Note: These messaging APIs do not use JMS) When using JMS, using the standard JMS API. SCDS is configured by default to use the ZLIB compression level for the connection to the broker connection factories are configured by default to use compression.

Java Message Service	An Application Programming Interface (API) for accessing enterprise messaging systems. It is part of the Java 2 Platform Enterprise Edition (J2EE).
SCDS Jump Start Kit	Downloadable self-service provisioning function for JMS publish/subscribe messaging from the SWIM Portal. The consumer jumpstart kit is a simple Java application to allow users to test their new subscription. It will connect to a queue and log message rates and/or messages to file or console. SWIFT Portal users can download a jumpstart kit directly from SWIFT Portal after provisioning a subscription.
NAS Enterprise Security Gateway (NESG)	A framework for compliance with boundary protection service requirements between NAS and non-NAS systems/networks in accordance with FAA Order 1370.114. The NESG infrastructure includes a layered security scheme to facilitate defense in depth security controls and provides a buffer between the NAS and external systems/networks to ensure no direct service connections to NAS systems. This follows the National Institute of Standards' approach to network security, which is mandatory for all agencies. (source: Data Management | Federal Aviation Administration faa.gov)
NAS-Impacting Usage	For purposes of SCDS, defined as data usage that **directly affects** the NAS. An example would be a company, such as an airline or a third-party vendor, that provides a service to airlines or pilots that affects their operational situational awareness and as a result directly affects the NAS
Non-NAS-Impacting Usage	For purposes of SCDS, defined as data usage that **does not directly affect** the NAS. An example would be a company that provides an app or a website that is not used in the operations of airlines, pilots, or any FAA programs.
Request Reply Services	Users who receive data from the FAA as well as send data to the FAA (via their direct VPN connection to the NESG).
SWIM Cloud Distribution Service (SCDS)	A publicly accessible cloud-based infrastructure dedicated to providing real-time SWIM data to the public via Solace Java Message Service (JMS) messaging. SCDS was developed to allow the dissemination of SWIM data without a dedicated Virtual Private Network (VPN) connection through the NAS Enterprise Security Gateway (NESG) to the NAS Enterprise Messaging System (NEMS).
Sensitive Data	A user that is getting Sensitive Data has gone through the FAA's NDRB approval process to be approved for consuming data that is not available to standard consumers. Sensitive technical data must be acquired from the NESG.

SWIM-Enabled Services	In the context of this document are the services that are provided via SCDS to standard external users and/or data obtained by directly connecting to the NESG. Data obtained by directly connecting to the NESG is NOT limited to Standard External Users like it is for SCDS.
SWIFT Portal	An interactive information sharing platform that provides customizable, real-time access and visibility to SWIM data. See SWIFT Portal: SWIFT Portal (faa.gov)
Web Services	SCDS capabilities do not include support for web services users. Web services users must be directly connected to the NESG.

6.3.   Acronyms and Abbreviations

AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
CSMA	Compression Supported Messaging API
EDS	Enterprise Data Services
JMS	Java Message Service
NAS	National Airspace System
NESG	NAS Enterprise Security Gateway
NEMS	NAS Enterprise Messaging System
CDM	Collaborative Decision Making
SCDS	SWIM Cloud Distribution Service
SECC	SWIM Enterprise Control Center
STTDS	SWIM Terminal Data Distribution System
SWIFT	SWIM Industry FAA Team
SWIM	System Wide Information Management
NASEO	NAS Security and Enterprise Operations
VPN	Virtual Private Network