SailPoint Integration Guide

Key2XS Platform

Unified Identity-to-Physical Access Management

Version 2.0 I April 2026

Key2XS B.V.

© 2026 Key2XS BV

Table of Contents

1. Key2XS SailPoint Integration Overview 4
1.1 Executive Summary 4
1.2 Integration Summary 4
1.3 Integration Architecture 5
1.4 How It Works 6
1.5 Authentication 6
1.6 Data Mapping 6
1.7 Security & Compliance 7
2. Supported Features 7
2.1 SCIM 2.0 Compliance 7
2.2 User Provisioning 7
2.3 Entitlements 8
2.4 Account Correlation & Aggregation 8
2.5 Governance Groups 8
2.6 Approval Delegation 9
2.7 Automated Integration Setup 9
2.8 Bulk Operations 9
2.9 Authentication Methods 9
2.10 REST API Sync (Outbound) 10
3. SailPoint Setup Guide 10
3.1 Prerequisites 10
3.2 Setup Overview 10
3.3 Stage 1: Credentials & Connection 11
3.4 Stage 2: SCIM Source Configuration 12
3.5 Stage 3: Governance (Optional, but Mandatory for automatic setup) 14
3.6 What SailPoint Administrators See 15
3.7 Lifecycle Events 15
3.8 Verifying the Integration 15
4. Approval Delegation 16
4.1 What Gets Delegated 16
4.2 How It Works 17
4.3 What SailPoint Approvers See 17
4.4 Approval Step Types 18
4.5 Two Types of Access Rules 18

© 2026 Key2XS BV

4.6 Access Profile Configuration Modes 18
4.7 Decision Flow 19
4.8 Prerequisites 19
5. Troubleshooting Guide 19
5.1 Quick Diagnosis 19
5.2 Connection Issues 19
5.3 Provisioning Issues 20
5.4 Access Profile Issues 20
5.5 Aggregation Issues 20
5.6 Attribute Sync Issues 21
5.7 Approval Delegation Issues 21
5.8 Integration Setup Issues 21
5.9 Common Scenarios 22
5.10 Diagnostic Information for Support 22
6. Known Limitations & Compatibility 23
6.1 Compatibility 23
6.2 Known Limitations 23
6.3 Performance 24
6.4 Integration Scope 24
6.5 Future Roadmap 24
6.6 Security Considerations 25
6.7 Support 25

© 2026 Key2XS BV

1. Key2XS SailPoint Integration Overview

1.1 Executive Summary

Key2XS is an enterprise middleware platform that bridges Identity and Access Management (IAM) systems with physical key-based access control. The platform eliminates the traditional gap between digital identity governance and physical security by providing automated, auditable, and compliant synchronization of access rights across both domains.

The SailPoint Identity Security Cloud integration enables organizations to extend their identity governance to physical access control. When users are created, modified, or terminated in SailPoint, Key2XS automatically provisions or revokes their physical access rights in connected key systems such as ASSA ABLOY, iLOQ, and others.

With Approval Delegation, organizations can go further: changes to physical access rules in Key2XS are routed to SailPoint for approval through its native Access Request workflow. SailPoint governance groups, managers, and Access Profile owners approve physical access changes alongside their regular IT access governance, providing a single pane of glass for all access decisions.

Key benefits include:

- Automated Joiner-Mover-Leaver (JML): Physical access is provisioned and revoked automatically based on SailPoint identity lifecycle
- Approval Governance: Physical access changes approved through SailPoint's native approval workflow
- Real-time Synchronization: Changes in SailPoint are reflected immediately in physical key systems
- Automated Setup: One-click integration setup configures the full SailPoint source automatically
- Unified Audit Trail: All access changes are logged with correlation across IAM and physical systems
- Compliance Ready: NIS2, CER, and GDPR-aligned audit logging

1.2 Integration Summary

Capability	Status
SCIM 2.0 Compliance	Full (RFC 7643, RFC 7644)
User Provisioning	Supported
User Deprovisioning	Supported
Attribute Sync	Supported
Entitlement Aggregation	Supported
Bulk Operations	Supported (max 100 per request)
Approval Delegation	Supported
Automated Integration Setup	Supported

© 2026 Key2XS BV

1.3 Integration Architecture

1.3.1 High-Level Data Flow



Communication paths:

Path	Direction	Protocol	Purpose
SCIM Inbound	SailPoint -> Key2XS	SCIM 2.0	Real-time user provisioning (join, move, leave)
REST Sync	Key2XS -> SailPoint	REST v2025	Bulk user sync with full PII for reconciliation
Governance	Key2XS <-> SailPoint	REST v2025	Approval requests, decision webhooks, entitlement management

© 2026 Key2XS BV

1.4 How It Works

1.4.1 User Lifecycle (Joiner-Mover-Leaver)

Joiner, New User:

SailPoint creates identity -> assigns Key2XS Access Profile -> sends SCIM POST to Key2XS -> Key2XS creates user -> provisions to physical key systems -> user receives access credentials.

Mover, User Change:

User attributes change in SailPoint (job title, department) -> SailPoint sends SCIM PATCH -> Key2XS recalculates access rights based on access matrix -> key systems updated.

Leaver, User Termination:

Identity terminated in SailPoint -> SailPoint sends SCIM PATCH (active=false) -> Key2XS revokes all physical access -> key systems updated -> audit trail records revocation.

1.4.2 Approval Delegation

When configured, physical access changes go through SailPoint governance:

1. Administrator creates or modifies an access rule in Key2XS
2. Key2XS submits an Access Request to SailPoint
3. SailPoint routes through the configured approval pipeline (governance groups, managers, AP owners)
4. Approver reviews and decides in the SailPoint UI
5. SailPoint notifies Key2XS of the decision
6. Key2XS applies or rejects the change and updates physical key systems

1.5 Authentication

Key2XS supports three authentication methods for the SCIM connection:

Method	Description	Recommended For
Bearer Token	Static token per connection	Most deployments (simple, secure)
Basic Auth	Username/password credentials	Legacy systems
OAuth 2.0	JWT tokens with client credentials flow	Enterprise security requirements

Bearer Token is the default in SailPoint SCIM connector configuration and is recommended for simplicity.

1.6 Data Mapping

Key2XS uses standard SCIM 2.0 schema, no custom attributes required. Compatible with SailPoint's built-in SCIM connector out of the box.

SCIM Attribute	Maps to Key2XS	Required
externalId or userName	User ID	Yes
name.givenName	First Name	Yes
name.familyName	Last Name	Yes
emails[0].value	Email	Yes
active	Account Status	No (default: true)

© 2026 Key2XS BV

title	Job Title	No
department	Department	No
phoneNumbers[0].value	Phone	No

1.7 Security & Compliance

Area	Implementation
Transport	All communication over HTTPS (TLS 1.2+)
Authentication	Per-connection credentials (Bearer/Basic/OAuth)
Credential Storage	All credentials encrypted at rest
Webhook Security	Decision webhooks secured with per-connection Basic Auth
Audit Logging	All operations logged with timestamps and correlation IDs
SCIM Compliance	RFC 7643 (Core Schema), RFC 7644 (Protocol)
NIS2	Audit logging aligned with directive requirements
CER	Physical access traceability for critical entity compliance
GDPR	Privacy by design, PII passed through to key systems, not stored

2. Supported Features

This section summarizes all SailPoint Identity Security Cloud features supported by the Key2XS connector.

2.1 SCIM 2.0 Compliance

Standard	Status
RFC 7643 (Core Schema)	Compliant
RFC 7644 (Protocol)	Compliant
RFC 7642 (Definitions)	Compliant

Supported SCIM operations: Create, Read, Update (full and partial), Delete, Bulk (max 100 per request), List with filtering and pagination.

Supported SCIM resources: Users, Groups (entitlements), ServiceProviderConfig, ResourceTypes, Schemas.

2.2 User Provisioning

Operation	Supported	Notes
Create User	Yes	Full user creation with all mapped attributes
Update User (full replace)	Yes	PUT replaces all attributes
Update User (partial)	Yes	PATCH updates specific attributes only

© 2026 Key2XS BV

Disable User	Yes	Sets active=false, preserves user record, revokes physical access
Enable User	Yes	Sets active=true, restores access based on access matrix
Delete User	Yes	Removes user and all physical access

2.2.1 Mapped Attributes

SCIM Attribute	Required	Used for
externalId or userName	Yes	Unique identifier for account correlation
name.givenName	Yes	First name
name.familyName	Yes	Last name
emails[0].value	Yes	Email address
active	No	Account status (default: true)
title	No	Job title, used for access matrix evaluation
department	No	Department, used for access matrix evaluation
phoneNumbers[0].value	No	Phone number

Enterprise extension department attribute supported as fallback.

2.3 Entitlements

Feature	Supported	Notes
Entitlement Aggregation	Yes	Key2XS access profiles, lock groups, and locks exposed as SCIM Groups
Account-Entitlement Linking	Yes	Via groups attribute on account schema
Access Profile Creation	Yes	Key2XS entitlements assignable to SailPoint Access Profiles
Entitlement Owner Assignment	Yes	Automatic, Key2XS patches owners after aggregation

Key2XS exposes its physical access objects as SailPoint entitlements. After entitlement aggregation, these appear in the SailPoint entitlement catalog and can be assigned to Access Profiles.

2.4 Account Correlation & Aggregation

Feature	Supported	Notes
Account Aggregation	Yes	Returns user list via GET /Users
Account Correlation	Yes	Via custom key2xsExternalId identity attribute (identity UUID)
Attribute Sync	Yes	All mapped attributes synchronize on identity changes

Important: Key2XS is privacy-by-design middleware, it does not store PII (name, email, phone) in its database. Account aggregation returns id, externalId, active, title, and department only. Use externalId (identity UUID) for correlation, not email.

2.5 Governance Groups

© 2026 Key2XS BV

Feature	Supported	Notes
List Governance Groups	Yes	Used for approval step configuration and user filtering
Get Group Members	Yes	Validates approver pool and displays membership
Group-Based User Sync	Yes	Filter sync to specific governance group populations

Key2XS integrates with SailPoint Governance Groups (workgroups) for two purposes: configuring approval steps on delegated workflows, and filtering which users sync to specific physical key systems.

2.6 Approval Delegation

Feature	Supported	Notes
Delegate approvals to SailPoint	Yes	Physical access changes submitted as SailPoint Access Requests
Governance Group approval step	Yes	Any member of the group approves
Manager approval step	Yes	User's SailPoint manager approves
Access Profile Owner approval step	Yes	AP owner approves
Select existing Access Profile	Yes	Reference an AP already configured in SailPoint
Create and manage Access Profile	Yes	Key2XS provisions the AP with configured approval steps
Separate policy and individual pipelines	Yes	Different approval flows for group-wide vs per-user access changes
Decision webhook	Yes	SailPoint notifies Key2XS automatically after approval/rejection
Automatic retry	Yes	Transient failures retried with exponential backoff

2.7 Automated Integration Setup

Feature	Supported	Notes
One-click setup	Yes	Configures source, correlation, entitlements, Access Profile, lifecycle assignment
Real-time progress	Yes	Phase-by-phase status updates during setup
Brownfield support	Yes	Detects existing configuration and completes only what's missing
Idempotent	Yes	Safe to re-run on already-configured tenants

2.8 Bulk Operations

Feature	Supported	Limit
Bulk Create / Update / Delete	Yes	100 operations per request
Mixed Operations	Yes	100 operations per request
Max Payload Size	,	1 MB

2.9 Authentication Methods

© 2026 Key2XS BV

Method	Token Expiration	Notes
Bearer Token	Never (until regenerated)	Recommended for most deployments
Basic Authentication	Never (until regenerated)	Username/password credentials
OAuth 2.0 Client Credentials	Configurable (default: 1 hour)	JWT-based

2.10 REST API Sync (Outbound)

Key2XS queries SailPoint via the REST v2025 Search API for complete user data during bulk synchronization:

Feature	Supported
Full PII retrieval (name, email, phone, department, job title)	Yes
Paginated sync with automatic cursor	Yes
Group-based user filtering (via Governance Groups)	Yes
Automatic retry with exponential backoff (429, 5xx)	Yes

3. SailPoint Setup Guide

This guide walks a SailPoint administrator through configuring Identity Security Cloud to integrate with Key2XS for physical access management.

3.1 Prerequisites

Requirement	Details
Key2XS platform	Deployed and accessible over HTTPS. Admin credentials available.
SailPoint ISC access	Admin role with permissions to create sources, API Clients, and Access Profiles
Network connectivity	SailPoint can reach the Key2XS SCIM endpoint over HTTPS (port 443)
SP Connect cluster	At least one Virtual Appliance cluster configured in your SailPoint tenant (required for SCIM sources)

3.2 Setup Overview

The integration is set up in three stages. Each stage unlocks additional capabilities:

Stage	What you configure	What it enables
Stage 1: Credentials & Connection	API Client in SailPoint, connection in Key2XS	REST API sync (Key2XS can query SailPoint for user data)
Stage 2: SCIM Source	SCIM 2.0 source in SailPoint pointing to Key2XS	User provisioning (join/move/leave), account aggregation, entitlement aggregation
Stage 3: Governance	Personal Access Token, approval delegation configuration	Approval workflows delegated to SailPoint, entitlement owner management

© 2026 Key2XS BV

Stages 1 and 2 can be completed in under 30 minutes. Stage 3 is optional and adds governance capabilities on top.

3.3 Stage 1: Credentials & Connection

3.3.1 Step 1.1: Create an API Client in SailPoint

Key2XS needs an OAuth2 API Client to query SailPoint during user synchronization.

1. Navigate to Admin -> Global -> Security Settings -> API Management
2. Click + New
3. Enter description: Key2XS Integration
4. Select Grant Types: Client Credentials
5. Set scope to sp:scopes:all, or add these 26 individual scopes:

```
idn:access-profile:read
idn:access-profile:manage
idn:accounts:read
idn:attr-sync-source-config:read
idn:entitlement:read
idn:identity:read
idn:identity-profile:read
idn:identity-profile:manage
idn:identity-profile-attribute:read
idn:identity-profile-lifecycle-state:read
idn:identity-profile-lifecycle-state:manage
idn:provisioning-policy:read
idn:provisioning-policy:manage
idn:source-schema:read
idn:sources:read
idn:sources:manage
idn:transform:read
idn:transform:manage
idn:workgroup:read
sp:my-personal-access-tokens:read
sp:search:read
sp:trigger-service-subscriptions:read
sp:trigger-service-subscriptions:manage
```

6. Click Create

Save the credentials:

- Client ID, visible anytime in API Management
- Client Secret, displayed once only. Copy it immediately.

Why separate credentials? The API Client handles read-heavy sync operations with standard scopes. The PAT provides ORG_ADMIN authority for governance write operations. PATs can be created with a custom expiry date or no expiry at all, Key2XS monitors PAT expiry automatically and warns 30 days before expiration regardless of the configured lifetime.

3.3.2 Step 1.2: Note Your Tenant Name

Your tenant name is the first segment of your SailPoint URL:

```
https://acme.identitynow.com
         ^^^^
         Tenant name
```

The API base URL is: https://acme.api.identitynow.com

3.3.3 Step 1.3: Create the Connection in Key2XS

In the Key2XS admin interface, create a new SailPoint connection and enter:

Field	Value
Provider	SailPoint

© 2026 Key2XS BV

Base URL	https://{tenant}.api.identitynow.com
Client ID	From Step 1.1
Client Secret	From Step 1.1

Key2XS automatically generates a SCIM bearer token for inbound provisioning. You'll need this token in Stage 2.

3.4 Stage 2: SCIM Source Configuration

3.4.1 Automated Setup (Recommended)

Key2XS provides a one-click setup orchestrator that configures the entire SailPoint SCIM source automatically, source creation, account correlation, provisioning policy mapping, attribute sync, entitlement schema, Access Profile creation, and lifecycle assignment.

In the Key2XS admin interface:

1. After finishing step 1, select automatic Setup
2. Choose to select an existing (brownfield) source, or create a new (greenfield) source and give it a name.
3. Click "Set up integration"
4. Wait for phases to complete (progress is shown in real-time)
5. When prompted, select which Identity Profiles should provision users to Key2XS (e.g., "HR", "Contractors")
6. Click Complete Setup

The orchestrator runs 17 configuration phases against your SailPoint tenant. Each phase is idempotent, if you re-run setup on a partially configured tenant, it picks up where it left off.

What gets configured automatically:

- SCIM source creation and SP Connect cluster assignment

- Connectivity verification

- Correlation identity attribute (key2xsExternalId) and transform

- Provisioning policy field mapping (name, email, title, department, phone)

- Account correlation rule

- Attribute synchronization

- Entitlement schema and aggregation

- Key2XS Access Profile

- Identity Profile lifecycle assignment

- Account aggregation

One manual step: The orchestrator pauses to provide you with SCIM connection credentials. The new source has been created in Sailpoint. Navigate in the Sailpoint UI to Admin -> Sources and click on the newly created source. Select connection settings and paste the Bearer token in the token field. Click on test connection in the side menu and click the button to test the connection. Now return to the Key2XS dashboard and confirm the step is finished. Next, the system needs to know which SailPoint Identity Profiles should provision users to Key2XS. This is a business decision, typically you select your primary profile and any contractor profiles whose users need physical access.

© 2026 Key2XS BV

Attribute limit: SailPoint allows a maximum of 15 searchable identity attributes per tenant. If the limit is reached, the orchestrator offers two options: free a slot in SailPoint, or use an existing searchable attribute for correlation.

3.4.2 Manual Setup (Brownfield Environments)

If your SailPoint tenant already has a partially configured SCIM source, or you prefer manual control, follow these steps in the SailPoint Admin Console:

Step 2.1: Create SCIM Source

1. Navigate to Admin -> Connections -> Sources -> New Source

2. Select SCIM 2.0 (SaaS) as the source type

3. Configure connection settings:

Field	Value
Source Name	Key2XS Physical Access
Base URL	https://<key2xs-host>/scim/v2/{connection_id}
Authentication Type	Bearer Token
Bearer Token	The token from Key2XS SCIM configuration

4. Click Test Connection to verify connectivity

Step 2.2: Configure Account Schema

SailPoint auto-discovers the SCIM schema. Verify these attributes appear:

userName, externalId, name.givenName, name.familyName, emails[0].value, active, title, department, phoneNumbers[0].value

Step 2.3: Configure Account Correlation

Key2XS correlates accounts using the SailPoint identity UUID. This requires a custom identity attribute:

1. Create a transform named Key2XS External ID that returns the identity's UUID

2. Add the identity attribute key2xsExternalId to each Identity Profile, sourced from this transform

3. Make the attribute searchable (requires ORG_ADMIN authority, see Stage 3 if you don't have a PAT yet)

4. In Account Creation settings, map externalId to the key2xsExternalId identity attribute

5. In Account Correlation, set: key2xsExternalId (identity) = externalId (account)

> *Important: Do not use email-based correlation. Key2XS is a privacy-by-design middleware, it does not store PII (name, email, phone). The externalId / identity UUID is the only reliable correlation key.*

Step 2.4: Configure Attribute Sync

Navigate to Account Management -> Attribute Sync. Enable synchronization for:

- name.givenName, name.familyName
- emails[0].value
- title, department
- phoneNumbers[0].value

Step 2.5: Configure Entitlements

1. In Entitlement Types and Schemas, configure the group type with id as the entitlement value and displayName as the name

© 2026 Key2XS BV

2. In Account Schema, add a groups attribute marked as Entitlement with type group

3. Run Entitlement Aggregation, should discover Key2XS entitlements (access profiles, lock groups, individual locks)

Step 2.6: Create Access Profile

1. Navigate to Admin -> Access -> Access Profiles -> Create Access Profile

2. Select the Key2XS SCIM source

3. Add the Key2XS User entitlement

4. Enable the Access Profile

> *Troubleshooting: If the enable toggle is greyed out, ensure the Account Schema groups attribute is linked to the entitlement type and entitlements have been aggregated.*

Step 2.7: Assign to Identity Profile

1. Navigate to Admin -> Identities -> Identity Profiles

2. Select your profile (e.g., "HR")

3. Go to the Access Profiles tab -> Add Access Profile -> Select Key2XS Access

4. Assign to lifecycle state Active

5. Click Apply Changes

This triggers provisioning for all active identities in the profile.

Step 2.8: Test

1. Test Connection from Source Configuration -> Review and Test

2. Run Account Aggregation, verify accounts appear and correlate to identities

3. Verify a test user was provisioned to Key2XS

3.5 Stage 3: Governance (Optional, but Mandatory for automatic setup)

Governance features enable approval delegation, physical access changes in Key2XS are routed to SailPoint for approval through governance groups, managers, and Access Profile owners.

3.5.1 Step 3.1: Create a Personal Access Token

Governance operations require ORG_ADMIN authority. Create a PAT:

1. Log in to SailPoint as an ORG_ADMIN user

2. Click your user icon (top-right) -> Preferences -> Personal Access Tokens

3. Click Create Token

4. Name: Key2XS Governance

5. Set scope to sp:scopes:all, or add these 14 individual scopes:

```
idn:access-profile:manage
idn:access-request:manage
idn:access-request-status:read
idn:attr-sync-source-config:manage
idn:entitlement:manage
idn:entitlement:read
idn:identity-profile:manage
idn:identity-profile-attribute:manage
idn:source-connector:manage
idn:source-schema:manage
idn:source-schema:read
idn:sources:manage
sp:my-personal-access-tokens:read
sp:trigger-service-subscriptions:manage
```

6. Copy the Client ID and Client Secret immediately (secret shown once only)

© 2026 Key2XS BV



7. Enter the PAT credentials in Key2XS on the SailPoint connection settings

PAT expiry: Personal Access Tokens can be created with a custom expiry date or no expiry. Key2XS monitors expiry automatically and warns 30 days before expiration. To rotate, create a new PAT and update the credentials in Key2XS.

3.5.2 Step 3.2: Enable Governance Features in Key2XS

In the Key2XS admin interface, navigate to configuration and click on the "Sailpoint" tab:

1. Enable Expose Entitlements, makes Key2XS access profiles visible as SailPoint entitlements
2. Enable Approval Delegation, allows approval workflows to delegate to SailPoint

3.5.3 Step 3.3: Configure Approval Workflows

With approval delegation enabled, Key2XS approval workflows can reference SailPoint for external approval. When a physical access change triggers an approval workflow, the request appears in SailPoint's Access Request queue. See the Approval Delegation section for details on:

- How approval pipelines are configured
- Which SailPoint approval step types are supported
- How decisions flow back to Key2XS

3.6 What SailPoint Administrators See

Once the integration is active, SailPoint administrators will see:

Where	What
Sources	A "Key2XS Physical Access" SCIM 2.0 source
Access Profiles	A "Key2XS Access" profile (and approval-specific profiles if delegation is configured)
Entitlements	Key2XS access profiles, lock groups, and locks as aggregated entitlements
Access Requests	Physical access approval requests from Key2XS (when approval delegation is enabled)
Event Triggers	A Key2XS Governance Decision Webhook trigger subscription (auto-created)
Tasks	Account and entitlement aggregation tasks for the Key2XS source

3.7 Lifecycle Events

Once configured, SailPoint automatically triggers Key2XS provisioning based on identity lifecycle:

Event	SailPoint Action	Key2XS Result
Identity created	SCIM POST /Users	User provisioned to physical key systems
Identity modified	SCIM PATCH /Users/{id}	Access rights recalculated based on new attributes
Identity terminated	SCIM PATCH /Users/{id} (active=false)	All physical access revoked
Identity deleted	SCIM DELETE /Users/{id}	User record removed

No manual intervention required, the SailPoint identity lifecycle drives physical access automatically.

3.8 Verifying the Integration

© 2026 Key2XS BV

Test	How	Expected Result
Connection	Source Configuration -> Test Connection	Successful connection to Key2XS
Schema Discovery	Run Account Aggregation	Accounts appear with externalId populated
Correlation	Check aggregated accounts	Accounts correlated to existing identities (not "uncorrelated")
Provisioning	Assign Access Profile to a test identity	User appears in Key2XS with correct attributes
Attribute Sync	Change a user's job title in SailPoint	Title updates in Key2XS within seconds
Deactivation	Terminate a test identity	Physical access revoked in Key2XS
Approval (Tier 4)	Create an access rule in Key2XS	Approval request appears in SailPoint Access Requests

4. Approval Delegation

Key2XS can route physical access approval decisions to SailPoint. When a change to physical access rules requires approval, Key2XS submits an Access Request to SailPoint. SailPoint governance groups, managers, and Access Profile owners review and approve the change through their normal workflow. Once approved, Key2XS applies the change and updates the physical key systems.

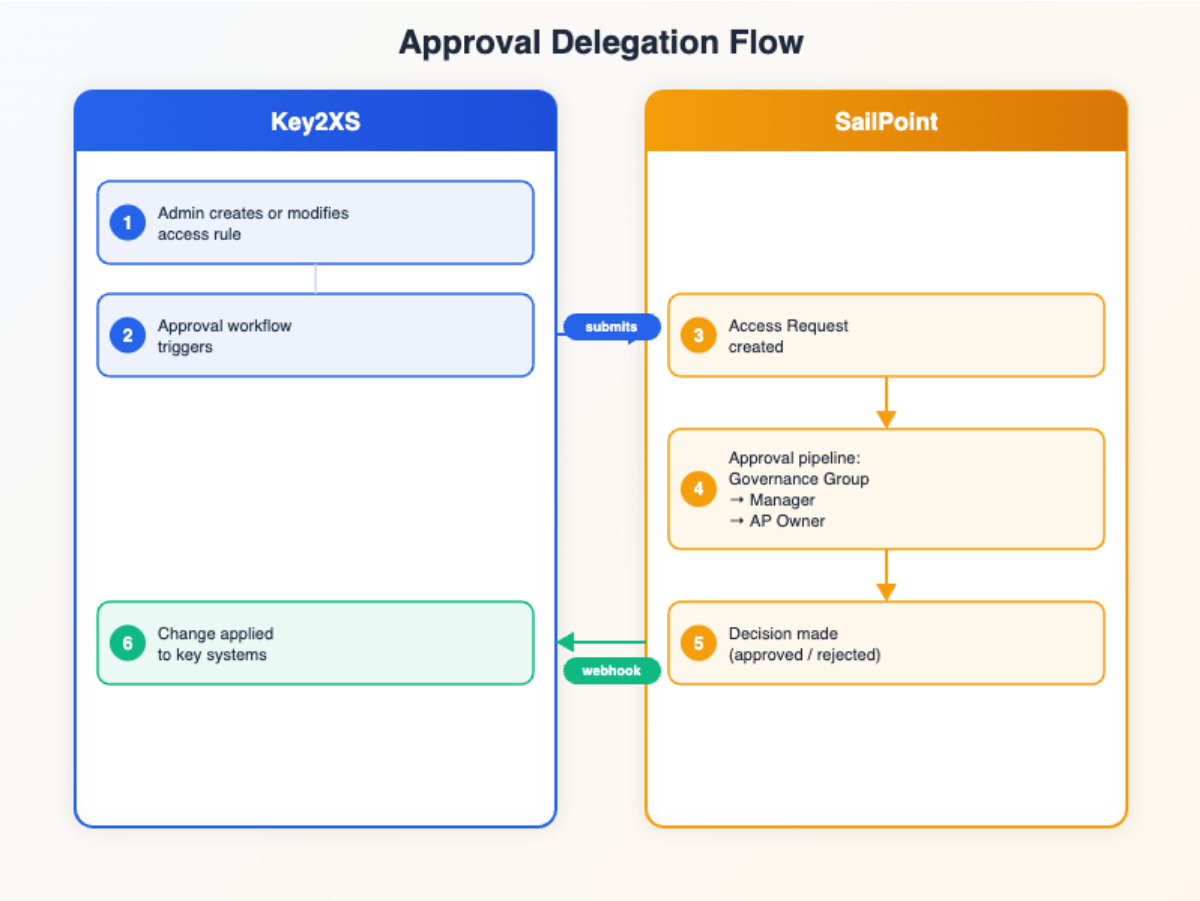
4.1 What Gets Delegated

Any change that requires approval in Key2XS can be delegated to SailPoint. Common examples:

Change	Example
New access rule	"Grant Security Guard job function access to East Wing"
Modified access rule	"Add Floor 3 locks to the Engineering access profile"
Removed access rule	"Revoke contractor access to Server Room"
Direct user access	"Give John Smith access to Building A entry"
Access profile change	"Create a new Visitor access profile"

© 2026 Key2XS BV

4.2 How It Works



1. An administrator creates or modifies a physical access rule in Key2XS
2. Key2XS submits an Access Request to SailPoint, referencing an Access Profile with configured approval steps
3. The request appears in SailPoint's access request queue
4. SailPoint routes the request through the approval pipeline, each step must pass sequentially
5. Approvers review and approve or reject in the SailPoint UI
6. SailPoint notifies Key2XS of the decision. Key2XS applies the change (or rejects it) and updates physical key systems

The entire process is automatic after initial configuration. No manual handoff between systems.

4.3 What SailPoint Approvers See

When a Key2XS approval request arrives in SailPoint, approvers see:

- Request name: Descriptive title (e.g., "Key2XS Approval, access_rules/INSERT")
- Requested for: The identity the access is for (individual rules) or the service owner (policy rules)
- Comment: Description of the change (e.g., "Access requested for Job Function: Security Guard: East Wing (Access)")
- Access Profile: The approval Access Profile with its configured steps

Approvers approve or deny through their normal SailPoint workflow, no separate tools or interfaces needed.

© 2026 Key2XS BV

4.4 Approval Step Types

When configuring an approval pipeline, three step types are available. Steps are sequential, all must pass in order.

Step	Who approves	How it works
Governance Group	Any member of a SailPoint workgroup	The group's entire membership is the approver pool. Any one member can approve.
Manager	The user's SailPoint manager	Resolves to the manager of the identity the request is for. Only relevant for per-user access rules.
Access Profile Owner	The designated AP owner	A specific identity configured as the approval policy owner.

Example pipeline: IT Security (governance group) -> User's Manager -> Physical Security Lead (AP owner)

Each step must be approved before the next step activates. If any step is rejected, the entire request is rejected.

4.5 Two Types of Access Rules

Key2XS distinguishes between two types of access changes, each with its own approval flow:

Policy rules, affect groups of users based on job function, department, or role. Example: "All Security Guards get access to East Wing." These can be approved by governance groups and/or the Access Profile owner. Manager approval is not relevant because there is no individual user involved.

Individual rules, grant access to a specific person. Example: "Give John Smith access to Building A." These can include Manager approval because there is a real person whose manager can make the decision.

Key2XS handles this automatically. When using "Create New" mode, it provisions two separate Access Profiles in SailPoint, one for policy rules (without Manager step) and one for individual rules (with Manager step). The correct profile is selected automatically based on the type of change.

4.6 Access Profile Configuration Modes

Each approval delegation references a SailPoint Access Profile that defines the approval pipeline. Two modes are available:

4.6.1 Select Existing

Reference an Access Profile already configured in SailPoint. Key2XS does not modify it, the approval scheme is whatever the SailPoint admin configured.

Best for: Organizations that already manage their approval schemes in SailPoint.

4.6.2 Create New

Define the approval steps in Key2XS. Key2XS creates and manages the Access Profile in SailPoint with those exact steps. Updates and deletes are handled automatically as the workflow configuration changes.

Best for: Organizations that want Key2XS to own the approval pipeline configuration. Required if you want separate approval flows for policy vs individual rules.

© 2026 Key2XS BV

4.7 Decision Flow

After the last approver makes their decision:

1. SailPoint fires a webhook to Key2XS with the approval or rejection
2. Key2XS records the decision and applies or rejects the physical access change
3. If approved, the access rule takes effect and physical key systems are updated

Reliability: Key2XS automatically provisions the webhook subscription in SailPoint, no manual trigger configuration needed. If a webhook is missed (network interruption), Key2XS polls SailPoint periodically to catch missed decisions. Transient failures are retried automatically with exponential backoff.

4.8 Prerequisites

Before enabling approval delegation:

1. SailPoint connection active in Key2XS with API Client credentials
2. SCIM source configured and entitlements aggregated in SailPoint
3. Personal Access Token (PAT) configured for governance operations
4. Entitlement exposure enabled in Key2XS
5. Approval delegation enabled in Key2XS

All prerequisites are covered in the Setup Guide (Stage 2 and Stage 3).

5. Troubleshooting Guide

This guide helps SailPoint administrators diagnose and resolve common issues with the Key2XS integration.

5.1 Quick Diagnosis

Symptom	See section
Can't connect to Key2XS from SailPoint	Connection Issues
Users not being created in Key2XS	Provisioning Issues
Access Profile can't be enabled or created	Access Profile Issues
Account aggregation failing or showing 0 accounts	Aggregation Issues
Attributes not syncing (job title, department)	Attribute Sync Issues
Approval requests not appearing or not completing	Approval Delegation Issues
Automated setup failing	Integration Setup Issues

5.2 Connection Issues

Error in SailPoint	Cause	Solution
401 Unauthorized	Invalid bearer token	Retrieve a fresh token from Key2XS SCIM configuration. Regenerate if necessary.
404 Not Found	Wrong endpoint URL	Verify the URL format: https://<host>/scim/v2/{connection_id}. Check the connection ID matches.

© 2026 Key2XS BV

Connection Timeout	Network issue	Verify firewall rules allow outbound HTTPS from SailPoint to Key2XS. Check DNS resolution.
SSL/TLS Error	Certificate issue	Ensure Key2XS has a valid SSL certificate. Check the certificate chain.
403 Forbidden	Connection disabled	Verify the connection is active in Key2XS.

Quick test: In SailPoint, navigate to Source Configuration -> Review and Test -> Test Connection. A successful test confirms network connectivity and authentication.

5.3 Provisioning Issues

Error	Cause	Solution
400, Missing required field: name.givenName	Name not mapped in provisioning policy	In Account Creation settings, ensure name.givenName is mapped to First Name
400, Missing required field: emails	Email not mapped	Map emails[0].value to Work Email
400, Missing required field: externalId	ID not mapped	Map externalId to the key2xsExternalId identity attribute (see Correlation Setup)
409, Uniqueness violation	Duplicate user	A user with the same ID or email already exists in Key2XS
500, Internal Server Error	Key2XS processing error	Contact Key2XS support with the timestamp and connection ID

5.4 Access Profile Issues

Problem	Cause	Solution
Enable toggle greyed out	Source configuration incomplete	Complete all required sections in the source: Account Schema, Account Correlation, and Entitlement Schema
"ENTITLEMENT was missing or empty"	Account schema not linked to entitlement type	In Account Schema, add groups attribute with Entitlement=Yes and Type=group
Entitlement aggregation shows 0	Key2XS Groups endpoint not responding	Verify Key2XS is running and the SCIM source can reach it. Test Connection first.
Can't add entitlements to Access Profile	Entitlement schema not configured	In Entitlement Types and Schemas, set id as the entitlement value

5.5 Aggregation Issues

Problem	Cause	Solution
Account aggregation "Error" with 0 accounts	Expected behavior	Key2XS is privacy-by-design middleware and returns minimal data. Use externalId for correlation, not email.
Accounts appear as "uncorrelated"	Correlation attribute not configured or not searchable	Verify key2xsExternalId is mapped in the Identity Profile and is searchable. Run the automated setup to configure correlation.
Attribute Sync shows 0 accounts	No correlated accounts exist yet	Account aggregation must succeed first. Run aggregation, then attribute sync.

© 2026 Key2XS BV

Connector stream broken	Network timeout	Usually transient. Retry. If persistent, check network connectivity.

5.6 Attribute Sync Issues

Job title or department not syncing:

1. In Source -> Account Creation, verify title is mapped to Job Title identity attribute
2. In Source -> Attribute Sync, verify title is enabled for synchronization
3. If users were provisioned before mapping was configured, trigger attribute sync or re-provision affected users

Other attributes not syncing:

Attribute	Check
department	Mapped in Account Creation? Enabled in Attribute Sync?
phoneNumbers[0].value	Mapped in Account Creation? Enabled in Attribute Sync?
name.givenName / name.familyName	Mapped correctly to First Name / Last Name?

5.7 Approval Delegation Issues

Symptom	Likely Cause	Solution
Approval request not appearing in SailPoint	Access Profile not enabled or not requestable	In SailPoint, verify the approval Access Profile is enabled and requestable
Request stuck, no decision arrives in Key2XS	Webhook not received	Verify the Key2XS endpoint is reachable from SailPoint. Check SailPoint Admin -> Event Triggers for the Key2XS Governance Decision Webhook subscription. Key2XS has an automatic polling fallback that catches missed webhooks for requests older than 1 hour.
Wrong approver on the "Owner" step	The request is "for" the same person as the AP owner	Key2XS uses the source owner as the request identity for policy rules to avoid this. Verify the SailPoint source has an owner configured.
Access rule approved but physical access not granted	Key system sync pending	Check the rule status in Key2XS. If it shows "No key assigned", the user needs a physical key in the key system before access can be granted.
"Delegation failed" status on pending change	SailPoint permanently rejected the request	Check the error details in Key2XS. Common causes: Access Profile not enabled, entitlements not yet aggregated, or connection credentials expired.

5.8 Integration Setup Issues

Problem	Likely Cause	Solution
Setup stalls at correlation phase	PAT not configured or lacks authority	Create a Personal Access Token with ORG_ADMIN authority (see Setup Guide Stage 3)
"Attribute cap reached" message	SailPoint has 15 searchable identity attributes	Free a slot by removing an unused searchable attribute, or use an existing attribute for correlation

© 2026 Key2XS BV

Source not found after setup	Source was deleted in SailPoint	Clear the Source ID in Key2XS and re-run setup
"Aggregation already running"	SailPoint task still in progress	Wait for the current aggregation to complete, then retry

5.9 Common Scenarios

5.9.1 Users Created in Key2XS but No Physical Access

1. Are access profiles assigned to the user in Key2XS?
2. Is the access matrix configured for their job function/department?
3. Are sync rules set up between the SailPoint connection and the target key system?
4. Is the key system connection active?

5.9.2 Deactivated Users Still Have Physical Access

1. Did SailPoint send a PATCH with active: false? Check SailPoint provisioning task results.
2. Is the Key2XS connection to the key system active?
3. Check Key2XS audit trail for the deactivation event.

5.9.3 Approval Stuck, No Progress

1. In SailPoint Admin -> Governance -> Access Requests, check the request status
2. Verify the governance group has active members
3. Verify the trigger subscription exists: Admin -> Event Triggers -> Key2XS Governance Decision Webhook
4. If the request is approved in SailPoint but Key2XS hasn't processed it, the polling fallback will catch it within an hour

5.10 Diagnostic Information for Support

When contacting Key2XS support, provide:

- SailPoint tenant name
- Key2XS connection ID (UUID)
- Timestamp of the issue
- SailPoint Task ID (for aggregation/provisioning issues)
- Error message or HTTP status code
- Screenshot of SailPoint provisioning task results (if applicable)

© 2026 Key2XS BV

6. Known Limitations & Compatibility

6.1 Compatibility

6.1.1 SailPoint Versions

SailPoint Product	Supported	Notes
Identity Security Cloud	Fully Supported	Primary integration target

6.1.2 SCIM Connector

- SailPoint SCIM 2.0 (SaaS) Connector: Fully compatible
- SCIM Version: 2.0 (RFC 7643, RFC 7644)
- Tested Operations: All standard SCIM operations verified

6.2 Known Limitations

6.2.1 SCIM Protocol

Limitation	Description	Workaround
No Sorting	SCIM sortBy parameter not supported	Use client-side sorting after retrieval
No ETags	Conditional requests not supported	Not typically needed for provisioning
Bulk Limit	Maximum 100 operations per bulk request	Split large batches into multiple requests
Payload Size	Maximum 1 MB per request	Split large payloads across requests

6.2.2 Data Handling

Limitation	Description	Reason
PII Not Stored	Key2XS does not store name, email, or phone in its database	Privacy by design, Key2XS is middleware that passes data through to physical key systems
Account Aggregation Returns Minimal Data	Only returns: ID, externalId, active, title, department	PII is passed through, not retained
No Email-Based Correlation	Cannot correlate accounts on email address	Use externalId (identity UUID) for correlation

6.2.3 Entitlements

Limitation	Description	Workaround
Read-Only Groups	Groups (entitlements) cannot be created or modified via SCIM	Manage access profiles in the Key2XS admin interface
No Nested Groups	Group hierarchy not supported	Use flat group structure with multiple groups
No Group Membership via SCIM	Cannot add/remove users from groups via SCIM	Group membership is determined by Key2XS access matrix rules

© 2026 Key2XS BV

6.2.4 Approval Delegation

Limitation	Description	Notes
Approval Threshold Always 1	SailPoint governance group threshold is always 1 per approval step	To require multiple approvals, configure multiple sequential steps
Manager Step for Individual Rules Only	Manager approval only meaningful for per-user access rules	For policy rules (job function, department), the Manager step routes to an irrelevant service account's manager
Single Webhook Delivery	SailPoint fires the post-approval webhook once (no automatic retry)	Key2XS polling fallback catches missed webhooks within 1 hour

6.2.5 Authentication

Limitation	Description
No SAML	SAML authentication not supported for the SCIM endpoint
No mTLS	Mutual TLS not supported (Bearer/Basic/OAuth only)

6.3 Performance

Metric	Value	Notes
Concurrent SCIM Requests	30 (default)	Configurable. Returns 503 with Retry-After header when exceeded.
Bulk Operations	100 per request	Hard limit per SCIM specification
Typical Response Time	< 500ms	May vary based on key system operations

6.4 Integration Scope

6.4.1 What Key2XS Does

- Receives SCIM provisioning requests from SailPoint
- Creates, updates, and deactivates users in connected physical key systems
- Revokes physical access immediately on identity termination
- Evaluates access matrix rules (job function, department, role-based access)
- Delegates approval decisions to SailPoint governance workflows
- Provisions and manages SailPoint Access Profiles for approval pipelines
- Maintains a full audit trail of all operations
- Provides automated integration setup (source, correlation, entitlements, lifecycle)

6.4.2 What Key2XS Does NOT Do

- Store user PII long-term (privacy by design)
- Manage SailPoint identities (Key2XS is a provisioning target, not a source)
- Create or modify access profiles via SCIM (managed in Key2XS admin interface)
- Provide email-based account correlation (use externalId instead)

6.5 Future Roadmap

© 2026 Key2XS BV

Feature	Status
Manage key assignments to users from SailPoint	Planned
Certification campaigns for physical access	Planned
SoD policy integration	Under evaluation

6.6 Security Considerations

6.6.1 Credentials

Credential	Recommendation
SCIM Bearer Token	Rotate periodically (annually recommended). Does not expire automatically.
API Client	Created in SailPoint Admin -> API Management. Does not expire.
Personal Access Token (PAT)	Configurable expiry (custom date or no expiry). Key2XS monitors and warns 30 days before expiration.

6.6.2 Network

Consideration	Recommendation
Transport	HTTPS required for production
IP Allowlisting	Restrict SCIM endpoint to SailPoint IP ranges
Firewall	Allow outbound HTTPS (443) from SailPoint to Key2XS

6.7 Support

Contact Key2XS Support:

- Email: support@key2xs.com

© 2026 Key2XS BV