



ADMINISTRATOR GUIDE

TPX MLS & Syndication Server

Operational guidance for administering organizations, API access, exchange inventory, syndications and platform controls within a private TPX property network.

Guide scope

This guide covers the administrative model already established for TPX and clearly identifies operational functions that are planned but not yet implemented.

Contents

The Administrator Guide is intended for the TPX network operator and authorized platform administrators.

Section	Title	Coverage
01	Administrator Role	Responsibilities and administrative boundaries
02	Agency Management	Membership, status and network participation
03	API Client Management	Integration credentials and access control
04	Property & Source Oversight	Canonical records, sources and diagnostics
05	Exchange Administration	Shared inventory and availability
06	Syndication Administration	Distribution relationships and revocation
07	Synchronization Oversight	Failures, reconciliation and operational status
08	Security & Access Control	Credential handling and agency isolation
09	Operational Procedures	Routine administration and incident handling
10	Audit, Logging & Monitoring	Operational visibility and planned controls
11	Administrator Checklist	Recommended recurring checks

01 - Administrator Role

The TPX administrator controls membership and central network operations while source agencies retain ownership of their canonical property records.

The administrator is responsible for the integrity of the private network rather than day-to-day editing of member listings. Property information should normally be corrected by the originating agency and synchronized back to TPX.

Primary Responsibilities

- Create and maintain authorized agency records.
- Control whether agencies are active within the network.
- Issue, suspend and revoke API client access.
- Oversee exchange inventory and syndication relationships.
- Investigate property-source and synchronization problems.
- Protect source ownership and organization isolation.
- Maintain operational records rather than deleting history unnecessarily.

Administrative principle

TPX administration should generally change status and access rather than destructively delete canonical properties, agencies or syndication history.

02 - Agency Management

Every participating organization is represented by an agency record and must be authorized before it can operate within the TPX network.

Agency Status

An agency's active state is part of the authorization boundary. If an agency is inactive, API clients associated with it should not be permitted to perform protected operations even when their credentials are otherwise valid.

AGENCY LIFECYCLE

```
CREATE AGENCY
|
VERIFY / APPROVE
|
ACTIVATE
|
NETWORK PARTICIPATION
|
SUSPEND OR DEACTIVATE IF REQUIRED
```

Recommended Agency Record

Administrative Data	Purpose
Organization identity	Identifies the member participating in the private network.
Status	Controls whether the organization is operational.
Verification state	Records whether the organization has been approved for participation.
Associated users	Identifies human users operating under the organization.
API clients	Identifies connected websites and systems belonging to the organization.
Properties and sources	Provides traceability to canonical inventory introduced by the organization.

Suspending an Agency

Suspension should immediately prevent new protected API operations for that organization. The underlying agency, property and syndication records should normally remain intact so that access can be restored or reviewed later.

Do not use deletion as suspension
Deleting an agency can break source relationships, property ownership history and integration references.
Use an inactive or suspended state instead.

03 - API Client Management

API clients provide machine-to-machine access for Houzez connectors and other approved integrations.

Client Credentials

AUTHENTICATION

```
X-TPX-Client-ID: YOUR_CLIENT_ID  
X-TPX-Secret: YOUR_CLIENT_SECRET
```

Each API client is associated with an agency. The authentication layer checks the client, its secret, active/expiry state and the status of the associated organization.

Administrative Actions

- Create credentials for an approved integration.
- Associate the client with the correct agency.
- Activate or suspend the client.
- Set or review expiry where used.
- Revoke credentials that are compromised or no longer required.
- Review last-used information where available.
- Issue separate clients for distinct integrations where practical.

Credential Rotation

If a secret is suspected to be exposed, the administrator should replace or revoke the affected credential and require the connected system to be updated. Secrets should never be sent in public URLs or stored in browser-side code.

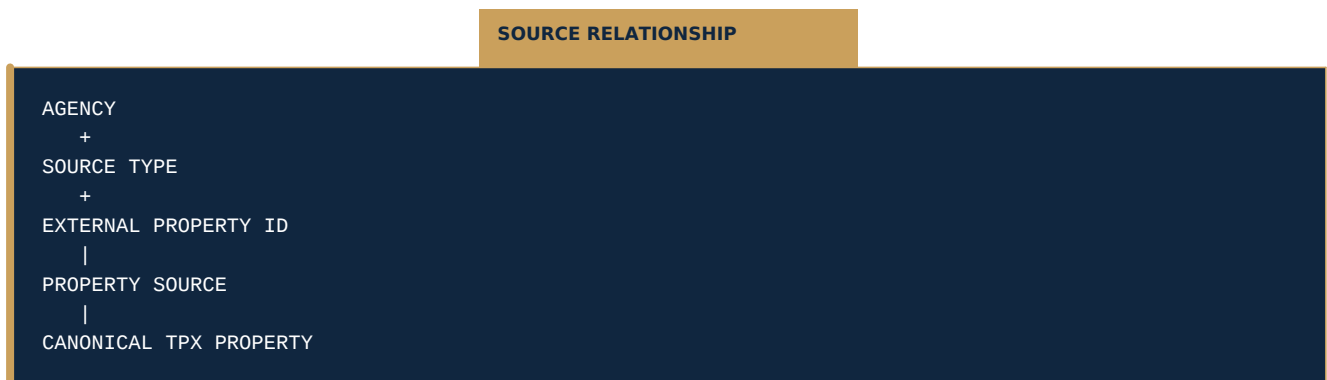
Secret storage

TPX should store client secrets securely and validate them server-side. Administrators should not distribute secrets more widely than required for the specific integration.

04 - Property & Source Oversight

Administrators need visibility into canonical properties and their external source relationships without taking ownership away from the source agency.

Canonical Property



The PropertySource relationship is essential when diagnosing duplicates or failed updates. It tells TPX which external record owns and updates a canonical property.

Administrative Diagnostics

- Confirm the canonical TPX property ID.
- Confirm the source agency.
- Confirm the source type, such as Houzez.
- Confirm the external property identifier.
- Check whether the property is available to the exchange.
- Review active or revoked syndication relationships.
- Confirm that a receiving copy has not been misclassified as an owner property.

Duplicate Investigation

If duplicate canonical properties appear, first compare source agency, source type and external ID. A connector that changes external identifiers or uploads a syndicated receiving copy as a new source can create duplication.

Ownership protection

An administrator should not manually reassign canonical ownership simply to resolve a synchronization problem. Establish the correct source relationship first.

05 - Exchange Administration

The private exchange contains canonical properties deliberately made available by their source organizations.

Current Exchange Administration

The TPX application includes an administrative exchange area at /admin/exchange. This is the central place for reviewing exchange-oriented property information as the administration interface develops.

EXCHANGE STATE

```
exchange_available = false
|
NOT SHARED

exchange_available = true
|
AVAILABLE TO PRIVATE NETWORK
```

Source Control

The source agency controls whether its property is available to the TPX network. Administrators oversee the exchange but should not routinely override an agency's sharing decision.

Withdrawal

When a property moves from available to unavailable, the server records the withdrawal state and revokes active non-revoked syndications associated with that property.

Administrator Checks

- Confirm that an available property belongs to an active authorized source agency.
- Confirm that withdrawn inventory is no longer offered for new syndication.
- Review unexpected availability changes with the source agency.
- Investigate exchange records that lack a valid source relationship.

06 - Syndication Administration

A syndication records the controlled distribution of a canonical TPX property to another authorized organization.

Current Syndication Administration

The TPX application includes an administrative syndication area at /admin/syndications for reviewing syndication records and their state.

SYNDICATION RELATIONSHIP

```
graph TD
    A[CANONICAL PROPERTY] --> B[SOURCE AGENCY]
    B --> C[SYNDICATION RECORD]
    C --> D[RECEIVING AGENCY]
    D --> E[LOCAL MANAGED COPY]
```

Administrator Responsibilities

- Confirm that the source property was available when the syndication was created.
- Confirm that the receiving organization is an authorized network member.
- Review whether a syndication is active or revoked.
- Investigate orphaned or inconsistent relationships.
- Avoid creating a second canonical source property for a syndicated copy.

Revocation

Revocation should terminate the receiving organization's right to continue publishing the managed syndicated copy. The syndication record should remain for history and auditability.

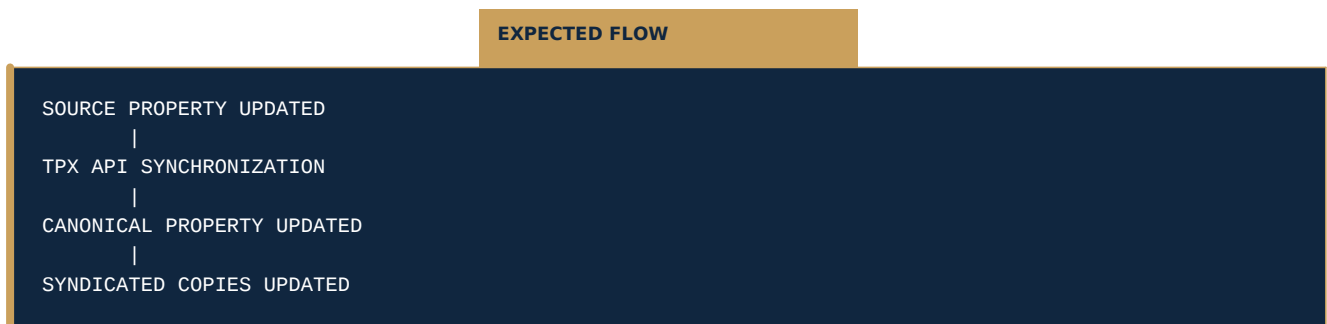
Receiving-site behavior

Once connector distribution is implemented, revocation should normally cause the receiving website to unpublish, draft or otherwise disable the TPX-managed local copy rather than permanently delete it.

07 - Synchronization Oversight

Administrators need a clear operational view of property synchronization and failed integrations.

Synchronization Model



Initial Reliability Strategy

The designed connector architecture combines direct synchronization after source changes with a scheduled 10-15 minute reconciliation process as a safety net. Failed operations should be queued, logged and retried.

Useful Administrative States

State	Meaning
Synced	Latest known property state was successfully processed.
Pending Sync	A synchronization operation is waiting to run.
Syncing	An operation is currently being processed.
Error	The last operation requires investigation or retry.

Implementation status

Full queue, retry and synchronization-log administration is part of the planned connector/operations layer and should be documented as live only after implementation.

08 - Security & Access Control

Administrative controls protect the closed network, its source ownership model and integration credentials.

Access Principles

- Only authorized organizations should participate in the network.
- API credentials belong to a specific client and agency.
- Inactive agencies must not continue operating through API clients.
- Expired or revoked clients must fail authentication.
- One agency must not overwrite another agency's canonical property.
- Administrative accounts should be restricted to personnel who require central platform access.
- Secrets should be rotated after suspected disclosure.

Incident Response

CREDENTIAL INCIDENT

```
SUSPECTED SECRET EXPOSURE
|
IDENTIFY API CLIENT
|
SUSPEND / REVOKE CLIENT
|
ISSUE REPLACEMENT IF REQUIRED
|
UPDATE CONNECTED SYSTEM
|
VERIFY AUTHENTICATION
```

Data Integrity

The owner-versus-syndicated distinction must be preserved at every layer. A syndicated receiving copy must never be allowed to create a new owner-originated canonical record.

09 - Operational Procedures

Routine administration should focus on network health, controlled access and preserving property relationships.

New Member Onboarding

ONBOARDING

```
CREATE / VERIFY AGENCY
|
ACTIVATE AGENCY
|
CREATE API CLIENT
|
CONNECT WEBSITE OR SYSTEM
|
TEST /api/auth-test
|
SYNC TEST PROPERTY
|
VERIFY SOURCE RELATIONSHIP
|
ENABLE PRODUCTION USE
```

Member Suspension

SUSPENSION

```
IDENTIFY AGENCY
|
SET AGENCY INACTIVE
|
REVIEW API CLIENTS
|
REVIEW ACTIVE SYNDICATIONS
|
PRESERVE RECORD HISTORY
```

Property Incident

- Identify the TPX property ID.
- Identify the source agency and external ID.
- Check the latest source synchronization.
- Check exchange availability.
- Review syndications.
- Correct the source/integration issue.

-
- Re-run or retry synchronization where supported.
 - Verify the resulting canonical state.

10 - Audit, Logging & Monitoring

A production TPX network should provide enough operational evidence to explain property, access and syndication state changes.

Recommended Audit Areas

- Agency activation and suspension.
- API client creation, revocation and credential rotation.
- Property synchronization failures.
- Exchange availability changes.
- Syndication creation and revocation.
- Administrative interventions.
- Queue and scheduled reconciliation failures.
- Application and API errors.

Health Monitoring

The current API provides GET /api/health as a simple application health check. Production monitoring should eventually combine application health, database availability, queue status and scheduled-job status.

CURRENT HEALTH ENDPOINT

GET /api/health

Planned operations layer

Detailed audit logs, queue dashboards and automated alerting are operational requirements for production deployment but should not be represented as completed modules until implemented.

11 - Administrator Checklist

A concise operational checklist for maintaining a controlled TPX network.

Regular Checks

- Review active agencies and confirm that membership status remains correct.
- Review API clients and revoke obsolete integrations.
- Check for repeated authentication failures.
- Review exchange inventory for anomalous source or availability states.
- Review active and revoked syndications.
- Investigate duplicate or orphaned property-source relationships.
- Review synchronization errors when logging/queue tooling is available.
- Verify scheduled reconciliation is operating when deployed.
- Confirm backups and recovery procedures are current before production operation.

Before Adding a New Integration

- Confirm the organization is approved and active.
- Create a dedicated API client.
- Test authentication.
- Synchronize a small test property.
- Verify canonical property identity and ownership.
- Test a subsequent update using the same external ID.
- Test exchange availability changes.
- Confirm that syndicated copies are marked as syndicated rather than owner-originated.

Current Administrative Surface

Area	Current Reference
Exchange administration	/admin/exchange
Syndication administration	/admin/syndications
API health	GET /api/health
Authentication test	GET /api/auth-test
Property synchronization	POST /api/v1/properties/sync

TPX - Real Estate Technology for Houzez

Private MLS, property syndication and integration infrastructure for controlled real-estate networks.