Solarwinds

Last Modified on 06/29/2026 5:19 pm EDT

CUSTOMER ONBOARDING · SOLARWINDS SERVICE DESK · SETUP GUIDE

This guide walks the IT/SolarWinds Service Desk administrator through generating an API token (JSON Web Token) for the integration, scoping the associated identity to the least privilege the tenant allows, verifying the token, and entering it in the Info-Tech portal. It includes the SolarWinds Service Desk objects that need read-only access so the administrator can complete setup without a separate access-requirements document. SolarWinds Service Desk has a native Fivetran Lite connector, so Fivetran is the primary extraction path; the API token generated here is the credential that connector uses.

Important — verify token generation and privilege model in your tenant before relying on this guide
SolarWinds Service Desk navigation and screen labels change between releases, so treat any menu path here as a guide, not an exact label. Two points in particular need tenant verification before publishing or relying on this setup:

1. API tokens are administrator-generated. SolarWinds' own API documentation indicates that admins generate API tokens from the user setup page, and its roles documentation notes the Administrator role is the only one that can enable APIs within process workflows. Several third-party integration guides state more explicitly that token generation requires a Service Desk administrator account/license. Because this cannot be confirmed from SolarWinds' primary documentation, a dedicated *non-admin, read-only* user may **not** be able to generate or use a working token. Do not promise a read-only setup unless it has been tested in your own tenant.

2. The token carries the privileges of the identity it is generated for. Because the token may need to come from an administrator-licensed account, the practical guidance is to use the **least-privileged identity your tenant supports** for token generation, and to rely on SolarWinds' role/permission model to limit what the token can read where the tenant allows it. The authentication mechanism itself — an API token passed as a bearer token in the `X-Samanage-Authorization` header — is the SolarWinds method the Fivetran connector consumes.

A Before you start

You will need:

- Administrator access to your SolarWinds Service Desk instance
- The least-privileged token-holding identity your tenant supports
- A service-account email address you control (e.g., `cioanalytics@yourcompany.com`)
- Your SolarWinds Service Desk region / data center
- Access to the Info-Tech portal where the API token will be entered

B SolarWinds Service Desk objects required

The integration requires read-only API access to the following SolarWinds Service Desk objects:

REQUIRED OBJECTS

- `incidents`
- `incident_custom_field_values`
- `incident_request_variables`
- `incident_statistics`
- `users`

REQUIRED OBJECTS (CONT.)

- `groups`
- `departments`
- `sites`
- `categories`

No create, edit, delete, or write-back permissions are required.

Note: satisfaction (CSAT) in SolarWinds Service Desk is captured at the incident level on the `incidents` object itself (`customer_satisfaction_response` and `is_customer_satisfied` fields) — no separate survey-response object is needed unless your tenant has a separate source. Worklog/time entries: only the aggregate `total_time_spent` field on incidents is confirmed available; row-level time entries are future scope.

Important — SolarWinds Service Desk's permission model
An API token carries the permissions of the identity it is generated for. Because token generation may require an administrator-licensed account, grant the token-holding identity the **least privilege your tenant supports** rather than assuming a fully read-only user can host it. The integration only ever reads the objects listed above and never writes back to SolarWinds Service Desk — but the token may carry broader account privileges than the integration uses, so protect it accordingly and confirm your tenant's least-privilege options with your Info-Tech onboarding contact.

STEPS IN THIS GUIDE

Step 1 Set up the administrator-licensed account for the token

Setup → Users & Groups → Users / Roles (exact path varies by release)

SolarWinds' own API documentation indicates that admins generate API tokens from the user setup page, and SolarWinds' roles documentation notes that the Administrator role is the only role that can enable APIs within process workflows. Several third-party integration guides state more explicitly that API token

generation requires a SolarWinds Service Desk administrator account/license. Because it cannot be verified from SolarWinds' primary documentation that a read-only user can generate or use the required API token, **the expected model for this integration is a dedicated administrator-licensed account** created solely for the integration — not a personal admin login. Treat a least-privilege setup as something to tenant-test first, not something this guide can promise works.

1. **Create or identify a dedicated administrator-licensed service account** for the integration (for example, name `CIOAnalytics`, email `cioanalytics@yourcompany.com`). Third-party integration guides indicate a Service Desk administrator license is needed to generate a token, so an admin-licensed account is the safer default. Do not reuse a person's admin login.
2. **If you require least-privilege access, validate it before relying on it.** Test in your tenant — or confirm with SolarWinds — whether the required API endpoints (incidents and their child objects, users, groups, departments, sites, categories) can be read using a restricted role rather than full administrator access. Only adopt a read-only identity if that test passes. Do not assume a read-only user can generate or use a working token.
3. **Record which account model you used** and note for your Info-Tech onboarding contact whether least-privilege was possible, so the access model can be confirmed and audited.

Step 2 Generate the API token

Setup → API token, or the token-generating identity's Profile / API Token screen (exact path varies by release)

SolarWinds Service Desk authenticates REST API and connector access with an API token (JSON Web Token). The token is generated by an administrator (or, where the tenant allows it, by the identity chosen in Step 1) and carries that identity's permissions.

1. **Open the token screen.** Depending on your release, API tokens are generated from the **Setup** area's API/token section, or from the token-generating identity's **Profile** / **My Profile → API Token** screen. Use the closest matching screen if the label differs.
2. **Generate or reveal the token** for the identity chosen in Step 1. SolarWinds may only allow an administrator-licensed account to do this.
3. **Copy the token exactly**, with no leading or trailing spaces. Treat it like a password.
4. **Store it securely** until you enter it in the Info-Tech portal. If you cannot locate a token screen for the chosen identity, flag it with your Info-Tech onboarding contact — this is the most common point where the SolarWinds privilege model differs from expectations.

Step 3 Verify the API token works

Run a test API call from your machine, Postman, or another approved API client.

Before entering the token in the Info-Tech portal, confirm it can read incidents and the reference objects

the integration uses. SolarWinds Service Desk passes the token in the `X-Samanage-Authorization` header as a bearer token.

1. **Test a basic incident read.** Run the following from a terminal, replacing `YOUR_API_TOKEN` with the token from Step 2 and the host with your region's API base URL:

   ```
   curl -H "X-Samanage-Authorization: Bearer YOUR_API_TOKEN" \
     -H "Accept: application/vnd.samanage.v2.1+json" \
     "https://api.samanage.com/incidents.json?per_page=1"
   ```

   You should see a JSON response containing one incident. If you get `401 Unauthorized`, the token is wrong, expired, or the header is malformed. If you get `403 Forbidden`, the token-holding identity does not have read access to incidents.

2. **Confirm satisfaction and time fields are present.** In the incident payload from the previous step, confirm the `customer_satisfaction_response`, `is_customer_satisfied`, and `total_time_spent` fields appear (they may be null on tickets with no survey response or no logged time). If they are entirely absent from the schema, flag this with your Info-Tech onboarding contact.

3. **Test reference-object reads.** Confirm each of these endpoints returns data:
   - `/users.json`
   - `/groups.json`
   - `/departments.json`
   - `/sites.json`
   - `/categories.json`

   If any return `403 Forbidden`, the token-holding identity is missing the required read permission for that object. Adjust the identity's access where the tenant allows it, then test again.

Step 4 Enter the API token in the Info-Tech portal

Info-Tech portal

> The API token gives bearer access to your SolarWinds Service Desk data. Treat it like a password. **DO NOT SEND THIS TO INFO-TECH.** See the **Submit to Info-Tech Portal** article for the portal submission steps. You will also need your SolarWinds Service Desk region / data center so the correct API base URL is used.

NOTES ON THIS DOCUMENT

- SolarWinds Service Desk navigation varies by release. If a menu item is not in the exact location shown, use the closest matching Setup, Users, or Profile page.
- Token generation may require an administrator-licensed account — see Step 1 for details. Confirm the least-privilege options available in your tenant with your Info-Tech onboarding contact.
- Questions about anything in this guide can be directed to your Info-Tech onboarding contact.