Zendesk

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

CUSTOMER ONBOARDING · ZENDESK SUPPORT · SETUP GUIDE

This guide walks the IT/Zendesk administrator through creating a dedicated read-only custom role, creating a service-account agent to host the credential, enabling and generating an API token, verifying it, and entering it in the Info-Tech portal. It includes the Zendesk objects that need read-only access so the administrator can complete setup without a separate access-requirements document. Zendesk Support has a mature native Fivetran connector, so Fivetran is the primary extraction path; the credential generated here is what that connector uses.

Note — verify the authentication method your connector uses
Zendesk supports two API authentication methods: an **API token** (used as `{agent_email}/token:{api_token}` over basic auth) and **OAuth**. This guide documents the API-token path because it maps cleanly to a dedicated read-only agent. The Fivetran Zendesk connector can use either OAuth or an API token depending on how it is configured — confirm with your Info-Tech onboarding contact which method your connection will use before generating credentials. The object access requirements below are the same either way.

A Before you start

You will need:

- Administrator access to your Zendesk Support instance
- An available Zendesk agent seat for the integration account
- A service-account email address you control (e.g., `cioanalytics@yourcompany.com`)
- Your Zendesk subdomain (e.g., `yourcompany.zendesk.com`)
- Access to the Info-Tech portal where the API token will be entered

B Zendesk objects required

The integration requires read-only API access to the following Zendesk objects:

REQUIRED OBJECTS

- `tickets`
- `ticket_comments`
- `ticket_field_history`
- `ticket_metrics`
- `ticket_metric_events`
- `satisfaction_ratings`

REQUIRED OBJECTS (CONT.)

- `ticket_custom_fields`

- `ticket_custom_statuses`
- `users`
- `groups`
- `organizations`
- `sla_policies`

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

Note: satisfaction (CSAT) in Zendesk is captured in the dedicated `satisfaction_ratings` object — not as a field on the ticket — and must be granted and synced for CSAT reporting. Worklog/time entries: Zendesk has no standard row-level worklog object; a row-level `fact_worklog` is future scope and requires the Time Tracking app or a comparable tenant-supplied source.

Important — Zendesk's permission model
Zendesk grants API access through the role assigned to the agent the token authenticates as. The token inherits that agent's role permissions, so scope the role tightly. For this setup, create a custom role with read/view access to tickets and the related objects above. Do not host the token on a personal administrator account or a broad admin role.

STEPS IN THIS GUIDE

Step 1 Create a read-only custom role

Admin Center → People → Team → Roles → Create role (custom roles require a qualifying Zendesk plan)

Create a dedicated read-only custom role rather than reusing a broad built-in role. This keeps the integration's permissions scoped tightly and makes them easy to audit and revoke without affecting other Zendesk agents.

1. **Open Admin Center.** From the product tray, open **Admin Center**.
2. **Navigate to Roles.** Go to **People → Team → Roles**.
3. **Create a custom role.** Give it a clear name — for example, `CIOAnalytics Read-Only` — and a description like *Read-only access for the Info-Tech Customer Data Store integration.*
4. **Set ticket access to view-only.** Grant access to **all tickets** (so the integration sees every ticket, not just a group's), and set the permission to **view only** — no edit, no comment, no delete.
5. **Do not grant administration or write permissions** beyond read/view of the objects this integration needs.

6. **Save the role.** If your Zendesk plan does not include custom roles, note this for your Info-Tech onboarding contact — the integration agent will need the narrowest available built-in role with read access.

Step 2 Create a dedicated integration agent

Admin Center → People → Team members → Add team member (or Support → Add user, depending on layout)

Create an agent whose only purpose is API access for this integration. A dedicated account avoids tying the connection to a person and supports clean deactivation if access must be revoked. The API token authenticates as this agent, so its role determines what the integration can read.

1. **Add a team member.** Name `CIOAnalytics`; email `cioanalytics@yourcompany.com`.
2. **Assign the read-only custom role** created in Step 1. Do not assign an administrator role.
3. **Save the agent** and complete any activation/verification step Zendesk requires for the new account.

Step 3 Enable token access and generate the API token

Admin Center → Apps and integrations → APIs → Zendesk API → Settings / Tokens

Zendesk API tokens are created at the **account / API settings level** — they are not generated from an individual agent's profile. The token authenticates as whichever agent's email is used in the request: when the integration sends the username as `{agent_email}/token:{api_token}`, Zendesk evaluates API access against that agent's permissions. That is why we created a dedicated read-only role and agent in steps 1 and 2 — the token itself is account-level, but pairing it with the integration agent's email scopes its access to that agent's role.

1. **Open API settings.** Go to **Admin Center → Apps and integrations → APIs → Zendesk API**.
2. **Enable Token Access** if it is not already enabled.
3. **Add an API token.** Click **Add API token**, give it a description such as `Info-Tech CIOAnalytics`.
4. **Copy the token immediately.** Zendesk shows the full token only once at creation. Copy it exactly, with no leading or trailing spaces. Treat it like a password.
5. **Record the agent email and subdomain.** The credential is used as `{agent_email}/token:{api_token}` against `https://yourcompany.zendesk.com`. Make sure the agent email is the dedicated integration agent from Step 2 so the token carries the read-only role.

Step 4 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 tickets and the related objects the integration uses. Zendesk uses basic auth with the agent email plus `/token` suffix.

1. **Test a basic ticket read.** Run the following from a terminal, replacing the placeholders and using your subdomain:

   ```
   curl -u "cioanalytics@yourcompany.com/token:YOUR_API_TOKEN" \
     "https://yourcompany.zendesk.com/api/v2/tickets.json?per_page=1"
   ```

   You should see a JSON response containing one ticket. If you get `401 Unauthorized`, the email/token pair or token access setting is wrong. If you get `403 Forbidden`, the agent's role lacks the required read access.

2. **Test satisfaction ratings.** Confirm the satisfaction-ratings endpoint returns data (it may be empty if CSAT is not in use):

   ```
   curl -u "cioanalytics@yourcompany.com/token:YOUR_API_TOKEN" \
     "https://yourcompany.zendesk.com/api/v2/satisfaction_ratings.json?per_page=1"
   ```

   If this returns `403 Forbidden`, the role is missing satisfaction-rating access. If CSAT is not enabled in your tenant, an empty result is expected.

3. **Test related-object reads.** Confirm each of these endpoints returns a successful response:
   - `/api/v2/users.json`
   - `/api/v2/groups.json`
   - `/api/v2/organizations.json`
   - `/api/v2/ticket_fields.json` *(custom field definitions)*
   - `/api/v2/custom_statuses.json`
   - `/api/v2/slas/policies.json`

   If any return `403 Forbidden`, the agent's role is missing the required read permission for that object. Add the minimum read-only permission required, then test again.

Step 5 Enter the API token in the Info-Tech portal

Info-Tech portal

> The API token gives access to your Zendesk data as the integration agent. 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 Zendesk subdomain (e.g., `yourcompany.zendesk.com`) and the integration agent's email address.

NOTES ON THIS DOCUMENT

- Zendesk Admin Center navigation may differ by plan and version. If a menu item is not in the exact location shown, use the closest matching People, APIs, or Apps and integrations page.
- Custom roles require a qualifying Zendesk plan. If custom roles are unavailable, use the narrowest built-in role that grants read access and note this for your Info-Tech onboarding contact.
- Questions about anything in this guide can be directed to your Info-Tech onboarding contact.