TeamDynamix

Last Modified on 06/25/2026 2:07 pm EDT

CUSTOMER ONBOARDING · TEAMDYNAMIX · SETUP GUIDE

This guide walks a TeamDynamix administrator through creating the required TeamDynamix roles, creating a dedicated service account, assigning the account to the IT Tickets application, validating TeamDynamix Web API access, and entering connection details through the Info-Tech submission flow. It is written for customer administrators and assumes TeamDynamix REST/JSON Web API extraction.

Reviewed against current public documentation
This guide is aligned to TeamDynamix Web API behavior: JSON request/response handling, Bearer JWT authentication, 24-hour token lifetime, ticketing application identifiers, UTC ISO 8601 dates, and API rate limiting with HTTP 429 responses. TeamDynamix tenant configuration varies, so the first connection test must confirm the exact base URL, ticketing application ID, permissions, custom attributes, and enabled modules.

A Before you start

You will need:

- TeamDynamix administrator access
- Your TeamDynamix base URL
- The ticketing application ID (`appId`) Info-Tech should read
- A dedicated integration identity (e.g., `cioanalytics`)
- Access to the Info-Tech portal where the connection details will be entered

B TeamDynamix data areas required

The integration requires read-only API access to the following TeamDynamix data areas. These are API resources or source objects, not necessarily database tables.

REQUIRED DATA AREAS

- `tickets` and ticket search/report results.
- `ticket feed` entries, comments, and updates for notes and derivation checks.
- `time entries` for worklog reporting, where time tracking is enabled.
- `people / users` for requester and technician identifiers and display names.
- `groups` for responsible group and support-team reporting.
- `ticket statuses` , `ticket types` , `priorities` , `impacts` , `urgencies` , and `sources` .
- `accounts / departments` , `locations` , and `SLA` fields when configured in the tenant.
- `custom attributes` on tickets, users, and reference objects when used for category, department, tier, location, or resolution details.

CONDITIONAL OR DEFERRED DATA AREAS

- `satisfaction / survey responses` — conditional. Do not require during standard setup unless Info-Tech confirms the tenant exposes survey data through an approved API/report/export path.
- `ticket tasks` — conditional. Enable only if the customer uses tasks for ticket execution or time-entry attribution.
- `assets`, `CMDB`, `projects`, `portfolio`, `knowledge base`, and attachments — not required for the early Customer Data Store release unless separately scoped.

No create, update, delete, administrative write-back, or ticket-modification access is required.

Important — TeamDynamix authentication model
TeamDynamix Web API calls use a Bearer token in the `Authorization` header. The token is a JWT returned by the authentication API and expires after 24 hours. Requests use `Content-Type: application/json`, and ticketing endpoints require the correct `appId` in the URL.

STEPS IN THIS GUIDE

Step 1 Create the IT Tickets application security role

TDAdmin / Applications / IT Tickets / Users and Roles / Security Roles

Create the application-level role that will be available on the IT Tickets application assignment for the integration user.

1. **Open the IT Tickets security role area.** In `TDAdmin`, navigate to `Applications`, open `IT Tickets`, then go to `Users and Roles` and `Security Roles`.
2. **Create a new role.** Click `New`.
3. **Name the role.** Example: `CIO Analytics Role`.
4. **Set the license type.** Select `Technician + Reporting`.
5. **Leave all permission checkboxes unchecked.** Do not enable create, edit, delete, assign, manage, or administrative permissions at this application-role step.
6. **Save the role.**

Step 2 Create the read-only user security role

TDAdmin / Users and Roles / Security Roles

Create the global user security role used by the service account. This role should provide only the visibility needed for the TeamDynamix ticketing data that Info-Tech reads.

1. **Open global security roles.** In `TDAdmin`, navigate to `Users and Roles`, then `Security Roles`.
2. **Create a new role.** Click `New`.
3. **Name the role.** Example: `CIO Analytics Security Role`.
4. **Set the license type.** Select `Technician + Reporting`.
5. **Select only these permissions:** `View All Accts/Depts`, `View All Types`, `View People from Accts/Depts`, and `View all requests belonging to assigned Accts/Depts`.
6. **Leave write/admin permissions unchecked.** Do not enable permissions that create, edit, delete, modify, manage, approve, import, move, merge, assign, or update records.
7. **Save the role.**

Step 3 Create the dedicated service account

TDAdmin / Users and Roles / Users

Create a named service account for the integration so API access is auditable, easy to rotate, and easy to revoke without depending on a named employee account.

1. **Open the user list.** In `TDAdmin`, navigate to `Users and Roles`, then `Users`.
2. **Create the service account.** Click `Create` or `New`, then choose the service-account option if your tenant presents one.
3. **Name the account.** Use a clear integration name, for example `CIO Analytics` or `Info-Tech CIO Analytics`.
4. **Click Next and complete the user details.** Fill out the required fields such as first name, last name, username, email, and any other required tenant fields.
5. **Assign the security role.** Set the user security role to the CIO Analytics role approved for this integration. If your tenant separates global and application roles, assign the global role from Step 2 on the user profile and assign the IT Tickets application role in Step 4.
6. **Finish the user creation flow.** Keep the account active so it can authenticate successfully.

Step 4 Assign the service account to the IT Tickets application

TDAdmin / Users and Roles / Users / [Service Account] / Applications

The service account must be assigned to the actual TeamDynamix ticketing application before API ticket

reads will work.

1. **Open the new service account.** Go to `TDAdmin`, `Users and Roles`, `Users`, and open the service account created in Step 3.
2. **Open the Applications tab.**
3. **Enable the ticketing application.** Make sure `IT Tickets` is checked. Do not rely only on `Client Portal` access.
4. **Assign the application security role.** For `IT Tickets`, select `CIO Analytics Role` or the equivalent read-only application role created in Step 1.
5. **Save the user.**
6. **Retest API access after saving.** If the API still returns `403 Forbidden`, generate a fresh token and confirm the service account is assigned to the correct Accts/Depts and the correct IT Tickets application.

Step 5 **Configure API authentication**

TeamDynamix Web API authentication

Info-Tech will use the TeamDynamix Web API to authenticate, retrieve a JWT, and read the required ticketing resources.

1. **For standard login authentication, use the auth endpoint.**

```
curl -X POST "https://yourorg.teamdynamix.com/TDWebApi/api/auth" \
  -H "Content-Type: application/json" \
  -d '{"username":"INTEGRATION_USER","password":"INTEGRATION_PASSWORD"}'
```

2. **For key-based administrative service account authentication, use loginadmin only if approved.**

```
curl -X POST "https://yourorg.teamdynamix.com/TDWebApi/api/auth/loginadmin" \
  -H "Content-Type: application/json" \
  -d '{"BEID":"YOUR_BEID","WebServicesKey":"YOUR_WEB_SERVICES_KEY"}'
```

3. **Store the returned JWT securely.** The token is used as `Authorization: Bearer YOUR_TOKEN` on later requests and expires after 24 hours.
4. **Do not send secrets through unapproved channels.** Passwords, BEID values, web services keys, and bearer tokens must be submitted only through the approved Info-Tech submission flow.

Step 6 **Verify credentials and required API reads**

Run a test API call from an approved API client.

Before submitting credentials, confirm the integration identity can authenticate and read the required TeamDynamix resources.

1. **Confirm the token can identify the authenticated user.**

```
curl "https://yourorg.teamdynamix.com/TDWebApi/api/auth/getuser" \
  -H "Authorization: Bearer YOUR_TOKEN" \
  -H "Content-Type: application/json"
```

2. **Test ticket search.**

```
curl -X POST "https://yourorg.teamdynamix.com/TDWebApi/api/APP_ID/tickets/search" \
  -H "Authorization: Bearer YOUR_TOKEN" \
  -H "Content-Type: application/json" \
  -d '{"MaxResults":1}'
```

   Replace `APP_ID` with the ticketing application ID from step 1.

3. **Test a single ticket read.** Use a ticket ID returned by the search call:

```
curl "https://yourorg.teamdynamix.com/TDWebApi/api/APP_ID/tickets/TICKET_ID" \
  -H "Authorization: Bearer YOUR_TOKEN" \
  -H "Content-Type: application/json"
```

4. **Test ticket feed access.** If the endpoint is enabled for the tenant, read the ticket feed for the same ticket to confirm comments and history are visible.
5. **Test time-entry access if worklog reporting is in scope.** Confirm the time search or time entry output can return entries associated with tickets.
6. **Record failures by HTTP status and response body.** TeamDynamix uses 401 for authentication or permission problems and 429 when rate limits are exceeded.

Step 7 **Enter connection details through the Info-Tech submission flow**

Info-Tech submission flow

> The authentication secret and any returned token are sensitive credentials. Do not send them by message, attachment, or screen share. See the **Submit to Info-Tech Portal** article for the submission checklist.

NOTES ON THIS DOCUMENT

- TeamDynamix menu names vary by tenant, role, and edition. If a path is not visible, ask the local TeamDynamix administrator to search by object name, such as ticketing application, security role, Web API, web services key, ticket statuses, or time entries.
- Questions about business purpose, data scope, or onboarding sequencing can be directed to your Info-Tech onboarding contact.