ManageEngine ServiceDesk Plus

Last Modified on 06/25/2026 2:09 pm EDT

CUSTOMER ONBOARDING · MANAGEENGINE · SETUP GUIDE

This guide walks a customer IT or ManageEngine ServiceDesk Plus administrator through preparing a dedicated read-only integration identity, granting read access to the required ServiceDesk Plus data, validating API access, and entering the connection details through the Info-Tech submission flow. It is written for customer administrators and includes both ServiceDesk Plus Cloud and ServiceDesk Plus on-premises setup paths.

Reviewed against current public documentation
This version has been checked against the public ManageEngine ServiceDesk Plus Cloud v3 API request and request worklog documentation, Cloud OAuth 2.0 guidance, Cloud API index, on-premises v3 request/header examples, on-premises API-key FAQ, and published common/status-code documentation available as of May 8, 2026.

A Before you start

You will need:

- Administrator access to your ManageEngine ServiceDesk Plus instance
- Your deployment type: ServiceDesk Plus Cloud or ServiceDesk Plus on-premises
- Your ServiceDesk Plus base URL and, for Cloud, the correct regional API domain
- A dedicated integration identity (e.g., `cioanalytics`)
- Access to the Info-Tech portal where the OAuth or API-key details will be entered

B ManageEngine source objects required

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

REQUIRED DATA AREAS

- `requests` — ticket/request records
- `request worklogs` — technician work performed on requests
- `users / technicians` — requester and technician reference data
- `groups` — assignment group reference data
- `sites` — location/site reference data
- `departments` — department reference data
- `priorities`, `statuses`, `modes`, `request types`, and `levels` — request classification metadata
- `categories`, `subcategories`, and `items` — request category path metadata

- `SLAs` — service-level agreement metadata and request-level SLA fields

CONDITIONAL OR DEFERRED DATA AREAS

- `satisfaction / survey responses` — conditional. Do not require this during standard setup unless Info-Tech confirms the customer's tenant exposes the required survey data through the selected connector or an approved export/API path.
- `additional service catalog objects` — deferred unless a future release explicitly adds catalog-level analytics beyond request records.
- `changes`, `problems`, `assets`, `projects`, and `CMDB` — not required for the early Customer Data Store release unless added under a separate scope agreement.

No create, update, delete, administrative, asset-management, or write-back permissions are required.

Important — ManageEngine Cloud and on-premises authentication are different
ServiceDesk Plus Cloud uses OAuth 2.0 access tokens and the `Authorization: Zoho-oauthtoken` header. ServiceDesk Plus on-premises uses an API key/authtoken associated with a technician or user, commonly sent in the `authtoken` request header. Do not mix Cloud OAuth headers and on-premises API-key headers.

STEPS IN THIS GUIDE

Step 1 Confirm deployment type and base URL

ServiceDesk Plus administrator console · Instance URL and deployment confirmation

Info-Tech needs the exact ServiceDesk Plus base URL and deployment type before credentials can be validated. Cloud customers must also use the correct regional API domain.

1. **Confirm deployment type.** Identify whether the instance is **ServiceDesk Plus Cloud** or **ServiceDesk Plus on-premises**.
2. **Record the base URL.** Examples: `https://sdpondemand.manageengine.com`, `https://servicedeskplus.ca`, or `https://servicedesk.yourcompany.com`. Do not include extra navigation paths unless your tenant specifically requires a portal path such as `/app/<portal>/api/v3`.
3. **For Cloud, confirm the API domain.** Use the customer data center/API domain returned by OAuth token handling or confirmed in the ServiceDesk Plus Cloud documentation. Do not hardcode the United States domain for all customers.

4. **For on-premises, confirm network reachability.** The integration runtime must be able to reach the ServiceDesk Plus server over HTTPS. If the instance is internal-only, a network path or allowlist may be required.

Step 2 **Create a dedicated integration identity**

Administration · Users / Technicians

A dedicated identity makes access auditable and easy to revoke. It also avoids breaking the connection when a human employee changes roles or leaves the organization.

1. **Create or select a dedicated account.** Suggested name: `cioanalytics` or `Info-Tech CIOAnalytics`.
2. **Use a controlled email address.** Suggested email: `cioanalytics@yourcompany.com`.
3. **For on-premises API-key setup, ensure the account has login permission.** ManageEngine on-premises API keys are generated for users or technicians with login permission.
4. **Do not use a broad administrator account unless required by local policy.** The preferred model is a purpose-built read-only role or technician profile.
5. **Keep the account active.** If the user or technician is disabled, the associated token or API key may stop working.

Step 3 **Grant read-only access to required data**

Administration · Users / Technicians · Roles / Permissions

Grant only the permissions needed to read ServiceDesk Plus request data and supporting reference metadata. The Customer Data Store does not require write-back access.

1. **Grant read access to requests.** The integration must be able to list and read request records and request fields.
2. **Grant read access to supporting metadata.** Include statuses, priorities, modes, request types, levels, categories, subcategories, items, sites, departments, groups, technicians/users, and SLA metadata.
3. **Grant read access to request worklogs.** Worklogs are needed for technician work effort reporting.
4. **Grant read access to satisfaction/survey responses only if enabled.** Survey data is conditional and should be validated tenant by tenant.
5. **Do not grant create, edit, delete, or administrative write permissions.** The integration is read-only.
6. **Confirm field-level visibility.** Some tenants restrict technician email, requester email, site, department, SLA, or survey fields. These restrictions can cause nulls even when the request endpoint itself is readable.

Step 4 **Configure Cloud OAuth or on-premises API key**

Cloud: Zoho API Console / OAuth consent · On-premises: Admin > Users / Technicians > API key

Choose the authentication setup that matches the customer's ServiceDesk Plus deployment.

1. **For ServiceDesk Plus Cloud, use Zoho OAuth 2.0.** Register or authorize an OAuth client using the customer-approved flow. Use read-only scopes such as `SDPOnDemand.requests.READ` and read access to setup/reference metadata such as `SDPOnDemand.setup.READ`, if required for the selected endpoints.
2. **For Cloud API calls, use the OAuth access token header.** The header format is:

   ```
   Authorization: Zoho-oauthtoken YOUR_ACCESS_TOKEN
   ```

3. **For ServiceDesk Plus on-premises, generate an API key/authtoken.** Create the key for the dedicated integration technician or user. Select an expiration policy approved by the customer's security team.
4. **For on-premises API calls, use the API key/authtoken header.** The common v3 header format is:

   ```
   authtoken: YOUR_API_KEY
   ```

5. **Store secrets securely.** OAuth client secrets, refresh tokens, API keys, and service-account passwords must be entered only through the approved Info-Tech submission flow.

Step 5 **Verify the credentials and required API reads**

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

Before submitting credentials, confirm the integration identity can read the required ServiceDesk Plus API resources.

1. **Test a Cloud request list read.** Replace the domain and token with customer values. If your tenant uses a portal path, include `/app/<portal>` before `/api/v3`.

   ```
   curl -G "https://sdpondemand.manageengine.com/api/v3/requests" \
     -H "Accept: application/vnd.manageengine.sdp.v3+json" \
     -H "Authorization: Zoho-oauthtoken YOUR_ACCESS_TOKEN" \
     --data-urlencode 'input_data={"list_info":{"row_count":1}}'
   ```

2. **Test an on-premises request list read.** Replace the base URL and API key with customer values.

   ```
   curl -G "https://your-sdp-server.example.com/api/v3/requests" \
     -H "Accept: application/vnd.manageengine.sdp.v3+json" \
     -H "authtoken: YOUR_API_KEY" \
     --data-urlencode 'input_data={"list_info":{"row_count":1}}'
   ```

3. **Confirm a successful response.** A successful response should include a `response_status` success value and a request list or an empty but authorized result.
4. **Test API-verified supporting data.** Confirm the same credential can read representative request details and request worklogs. Confirm that reference values embedded on requests are populated for status, priority, mode, request type, level, category, subcategory, item, requester, technician, group,

department, site, and SLA.

5. **Do not validate survey data as a standard required endpoint.** Satisfaction/survey responses are conditional and must be validated separately with the final connector or customer-approved export/API path before they are included in onboarding.
6. **Capture failures by code and body.** ManageEngine responses often include both an HTTP status and a `response_status` object. Keep both when troubleshooting.

Step 6 **Enter connection details through the Info-Tech submission flow**

Info-Tech submission flow — interim guidance until the formal portal is available

> The OAuth client secret, refresh token, API key/authtoken, and any service-account password are sensitive credentials. Do not send them to Info-Tech by email, chat, ticket attachment, or screen share. Use only the approved Info-Tech submission flow. See the **Submit to Info-Tech Portal** article for interim placeholder guidance until the formal site is available.

NOTES ON THIS DOCUMENT

- ManageEngine navigation varies by Cloud/on-premises edition, installed version, role model, and enabled modules.
- Cloud customers should use the correct regional API domain and should not hardcode one ManageEngine data-center URL for all tenants.
- Questions about business purpose, data scope, or onboarding sequencing can be directed to your Info-Tech onboarding contact.