

CAPABILITIES

Okta Input

Exported on July 15th, 2026 • Last updated July 15th, 2026

Overview

Transit supports log ingestion from **Okta**, allowing you to forward your Okta **System Log** events into the pipeline without standing up a separate forwarder, agent, or log-export job. When you create an Okta source, Transit reads System Log events directly from your Okta org over the Okta API and streams the events into the pipeline.

This method reads events from the Okta **System Log API** (`/api/v1/logs`).

This source ingests the Okta **System Log** (audit and security events). It does not read application logs, arbitrary log files, or data from other Okta APIs.

Setting up Okta ingestion has two parts, each covered step by step below:

1. **Install the GreyMatter Transit integration in your Okta org** (performed by an Okta administrator).
2. **Create the Okta source in Transit** (performed by a Transit user).

Prerequisites

Before you begin, you will need:

- An **Okta org**, reachable at its org URL — e.g. `https://<your-org>.okta.com` (or your custom domain / `.okta.gov` for OktaGov / `.oktapreview.com` for preview orgs).
-

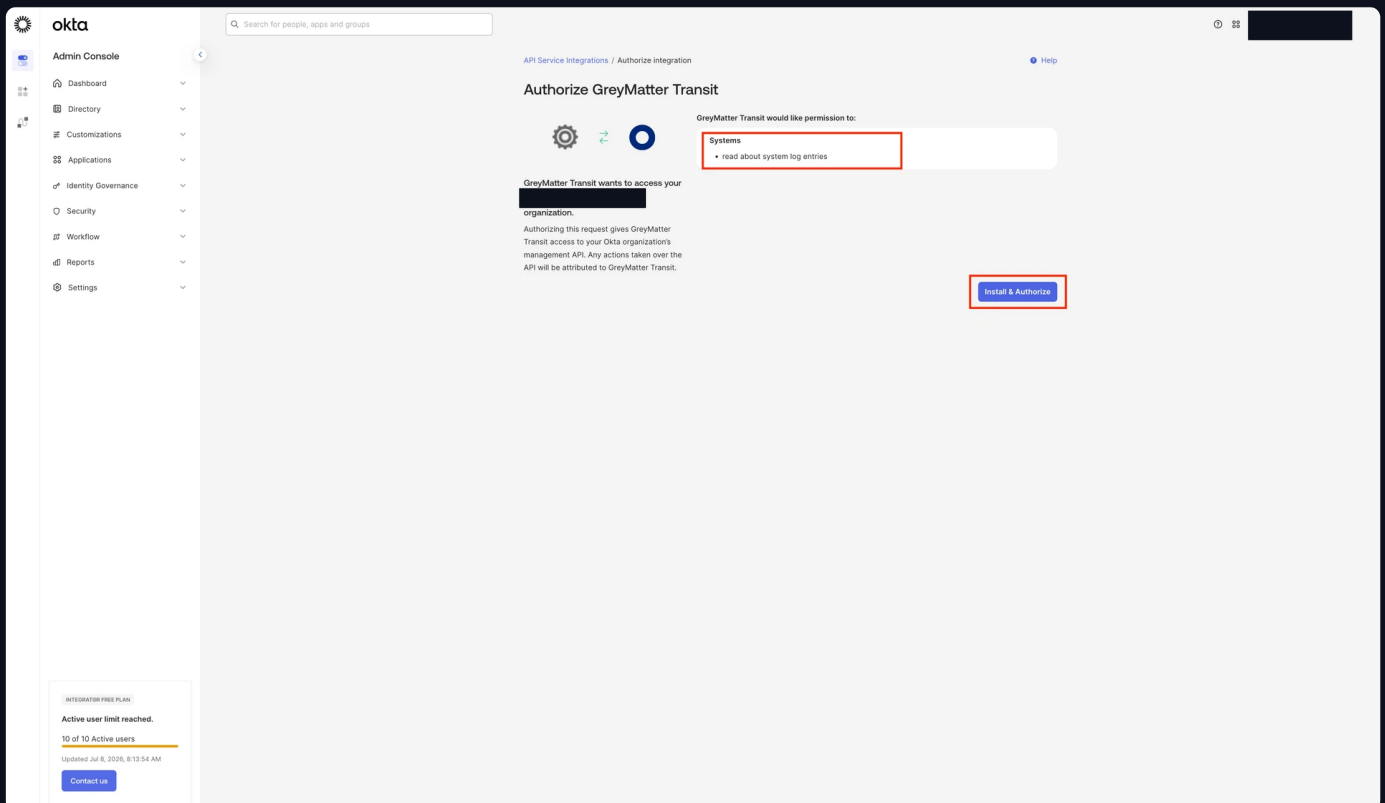
An **Okta administrator** able to install API Service Integrations and grant application scopes (Super Administrator, or an admin with rights to add and grant application scopes).

- A **GreyMatter Transit tenant** with access to create pipelines.

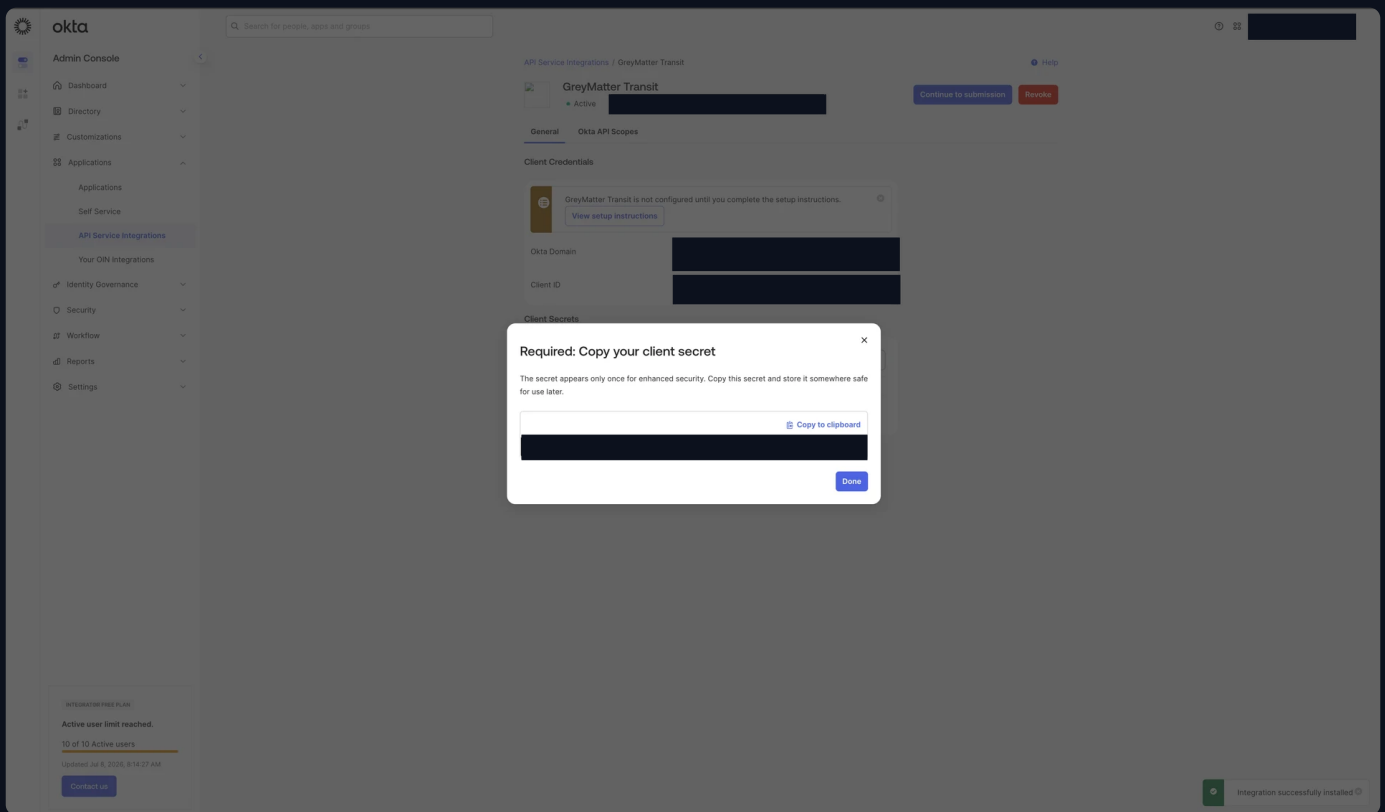
Step 1 — Install the GreyMatter Transit Integration in Your Okta Org

Before you can create a source, the **GreyMatter Transit** API Service Integration must exist in your Okta org. This is a one-time step performed by an Okta administrator.

1. In the Okta **Admin Console**, go to **Applications** 'Applications' **Browse App Catalog**.
2. Search for **GreyMatter Transit** and open the integration, then click **Add Integration**.
3. On the **Authorize GreyMatter Transit** screen, review the requested permission and click **Install & Authorize**.

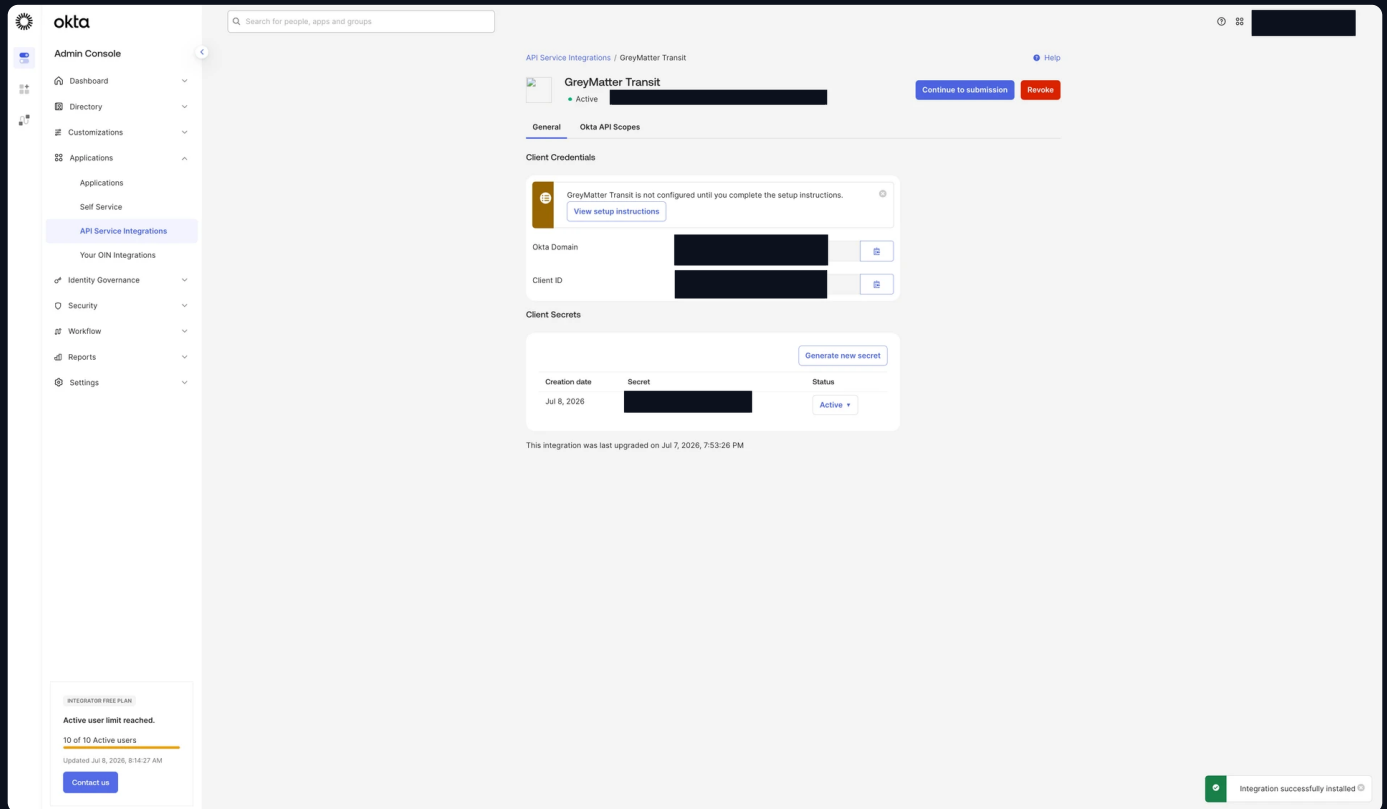


4. In the **Required: Copy your client secret** dialog, click **Copy to clipboard** and store the **Client Secret** securely, then click **Done**. The secret is shown only this once.



The Client Secret is displayed only at creation time and cannot be retrieved later. If it is lost, generate a new secret from the integration's **Client Secrets** section and update the source in Transit.

5. On the integration's **General** tab, under **Client Credentials**, copy the **Okta Domain** and **Client ID**. You will enter these values, along with the Client Secret, in Transit.



Required Information

Collect the following values from the install step — Transit will ask for all three:

Field	Description
Okta Org URL	The base URL of your Okta org as shown in the integration's Okta Domain field, e.g. <code>https://<your-org>.okta.com</code> .
Client ID	The Client ID generated when you installed the Grey-Matter Transit integration.
Client Secret	The Client Secret generated for that integration. Stored securely by Transit and used only to obtain access tokens.

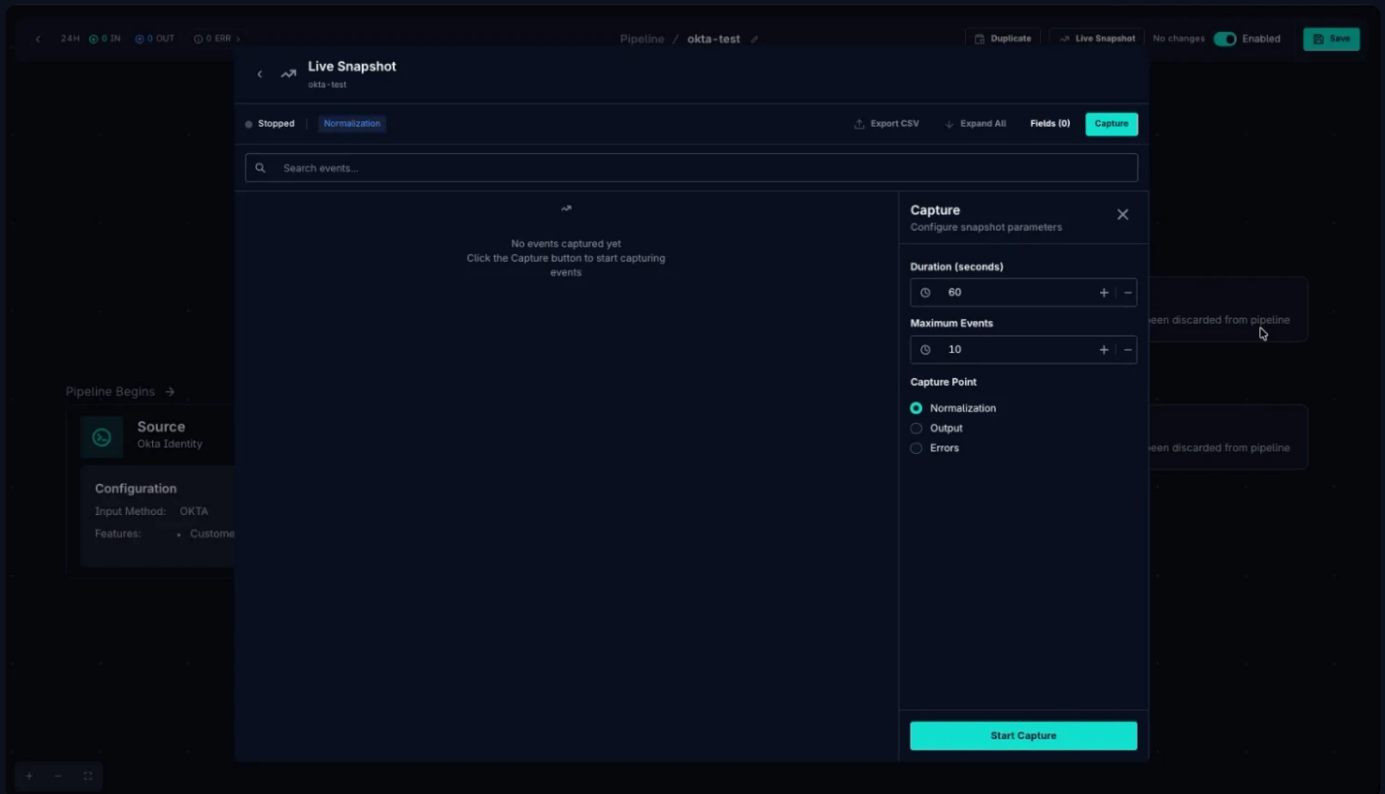
Step 2 — Create the Okta Source in Transit

1. In Transit, go to the pipelines list and click **+ Add Pipeline**.
2. On the **Supported Sources** step, search for **Okta**, then click **Configure** on the **Okta Identity** source.
3. On the **Basic Information** step, fill in the following, then click **Next**:
 - **Name** — a descriptive name for the source.
 - **Log Parser** — select **Okta Identity [JSON]**.
 - **Input Method** — select **Okta**.
4. On the **Source Configuration** step, enter the values collected from Okta — **Client ID**, **Okta Org URL**, and **Client Secret** — then click **Next**.
5. On the **Features** step, toggle the features you want this pipeline to monitor and click **Next**.
6. On the **Configuration** step, review the **Pipeline Confirmation** summary and click **Create**. Transit provisions a dedicated collector for this dataflow that begins reading the System Log immediately.
7. The pipeline canvas opens, showing the Okta Identity source connected to the rest of the pipeline. The source is now live.

Verify Ingestion

To confirm events are flowing end to end:

1. Generate activity in your Okta org — for example, sign in to the org or open the Admin Console. Each action publishes events to the Okta System Log.
2. In the Transit pipeline view, click **Live Snapshot**, then **Capture**. Set a duration (e.g. 60 seconds) and click **Start Capture**.



3. Within a minute or two, captured Okta System Log events appear in the snapshot – allow for the 60-second poll cadence plus Okta's short System Log indexing delay.

You can also confirm ongoing ingestion from the pipelines list, where the pipeline's **Bytes in (last 24h)** column increases as events arrive.

Troubleshooting

If Transit cannot authenticate or read the System Log, the system logs the error and retries on its normal polling cadence. A revoked scope or invalidated secret is the most common cause of ingestion stopping. Verify that:

- The **GreyMatter Transit** integration is still installed in your Okta org (Admin Console **'Applications API Service Integrations'**).
- The `okta.logs.read` scope is still granted (the integration's **Okta API Scopes** tab).
- The **Client ID**, **Client Secret**, and **Okta Org URL** configured in Transit match the integration's current values. If the secret was rotated, update the source in Transit.

Transient errors (rate limits, brief API unavailability) are retried automatically on the next poll cycle and do not require action.

If errors continue, please contact your GreyMatter Support team for assistance.