MARS Platform — Acronis Cyber Protect Cloud Integration Guide

Overview

This document guides you through the steps required to integrate your Acronis Cyber Protect Cloud tenant with the MARS Platform. MARS connects to Acronis as a **read-only data source** using an **Acronis API client** (OAuth 2.0 client credentials). No interactive login is involved, and MARS never changes anything in your Acronis tenant.

What MARS Collects

Data	Acronis API	Requires Advanced Security + XDR pack
EDR incidents	MDR / Incidents API	Yes
Platform alerts	Alert Manager API	No
Workload (device) inventory	Resource Management API	No
Protection plans (policy posture)	Policy Management API	No
Endpoint sensor telemetry — process create/terminate, network, registry, script execution, file access, logon/logoff and sensor detections	EDR Management (XDR search) API	Yes — **Windows workloads only**

> ℹ️ Acronis exposes raw endpoint telemetry for **Windows** workloads only. macOS and Linux workloads still contribute incidents, alerts and inventory.

> ℹ️ A tenant **without** the Advanced Security + XDR pack can still be connected — alerts, inventory and protection plans work normally; EDR incident and telemetry data will simply be empty until the pack is applied to your workloads.

Prerequisites

Before starting, make sure you have:

- Access to the **Acronis Management Portal** as a **Company administrator** of the customer tenant whose data MARS should read
- (Optional, for EDR data) the **Advanced Security + XDR** pack enabled for the tenant and applied to its workloads

---

Step 1: Create an API Client

The API client must be created **inside the customer tenant whose data MARS will read** (not at a different partner/customer level). Its access is scoped to that tenant and all of its units.

1. Sign in to the **Acronis Management Portal** as a Company administrator
2. Go to **Settings** → **API clients**
3. Click **Create API client**
4. Enter a recognizable name, for example: `mars-platform-integration`, then click **Next**
5. The client is created with **Active** status

Step 2: Copy the Credentials

On the confirmation screen, copy and store the following values securely:

- **Client ID**
- **Client secret**
- **Data center URL** (for example `https://eu8-cloud.acronis.com`)

> ⚠️ **The client secret is shown only once.** If you lose it, it cannot be retrieved — you must reset the secret and send MARS the new one.

> ℹ️ Acronis hosts tenants in regional data centers, and an API client only works against the data center where it was created. If the data center URL isn't

> shown, copy it from your browser's address bar while signed in to the Management Portal (scheme + host only, e.g. `https://eu8-cloud.acronis.com`).

Step 3: Securely Send MARS the Following

Credential / Detail	Where to Find It
Data Center URL	Shown in Step 2, or the Management Portal address bar (e.g. `https://eu8-cloud.acronis.com`)
Client ID	Shown in Step 2
Client Secret	Shown once in Step 2

> ⚠️ **Use a secure transfer method.** Do not send credentials over email or chat. Use a secrets-sharing tool, one-time secret link, password manager share, or encrypted file when transmitting these values to the MARS team.

Revoking Access

To revoke MARS's access at any time, go to **Settings** → **API clients** in the Management Portal and disable or delete the `mars-platform-integration` client. Resetting its secret also immediately invalidates the credentials MARS holds.