

AQUILA - Digital Guardian Integration

Integrating **Digital Guardian (DG)** with **AQUILA** for security log ingestion typically involves exporting logs from DG and then parsing and ingesting them into **AQUILA**.

Digital Guardian is a Data Loss Prevention (**DLP**) and endpoint protection tool. It logs:

- Data access
- File operations (copy, move, print, etc.)
- Application usage
- User behavior analytics

Goal: Extract these logs and ingest them into **AQUILA** to enable searching, visualization, and alerting.

Digital Guardian's native integration with **Aquila Agent** requires:

- ARC Server URL
- Authorization Server URL
- ARC Export Profile ID
- Client ID
- Client Secret

Working with the **Digital Guardian ARC Cloud API** (Advanced Reporting & Correlation), which is used to export events via a secure API.

Steps on getting the required information before integrating it to AQUILA

1. ARC Server URL

- This is the base URL for the **Digital Guardian ARC cloud instance**.
- It looks like:
 - **https://arc.digitalguardian.com**
- Sometimes it's region-specific (e.g., EU or US ARC instance).

2. Authorization Server URL

- This is the OAuth2 token server used for authenticating API calls.
- It may look like:
 - **https://auth.digitalguardian.com**
- Or it may be included in your API documentation.

3. ARC Export Profile ID

- This is a **profile ID** that determines which logs (event types, time windows, etc.) are exported via the API.
- It is **configured by a DG admin** inside the **DG Management Console** under the **ARC export profiles** section.
- Steps for the DG Admin:
 - Log in to the **Digital Guardian Console**.

- Go to **ARC > Export Profiles**.
- Create or view an export profile with appropriate filters.
- Copy the **Export Profile ID** from the profile details.

4. Client ID & Client Secret

- These are **OAuth2 credentials** used to authenticate your API access.
- Generated via the **API client registration** feature in the DG admin interface.
- Steps for the DG Admin:
 - Log into the **Digital Guardian ARC Console**.
 - Navigate to **ARC > API Clients / Applications**.
 - Register a new application.
 - Assign the **Export Profile ID**.
 - Set appropriate scopes (usually “read:events”).
 - A **Client ID** and **Client Secret** will be generated.
- **IMPORTANT:** The **Client Secret** is shown **only once**, so it must be secure.

Sample Information needed from DG Admin

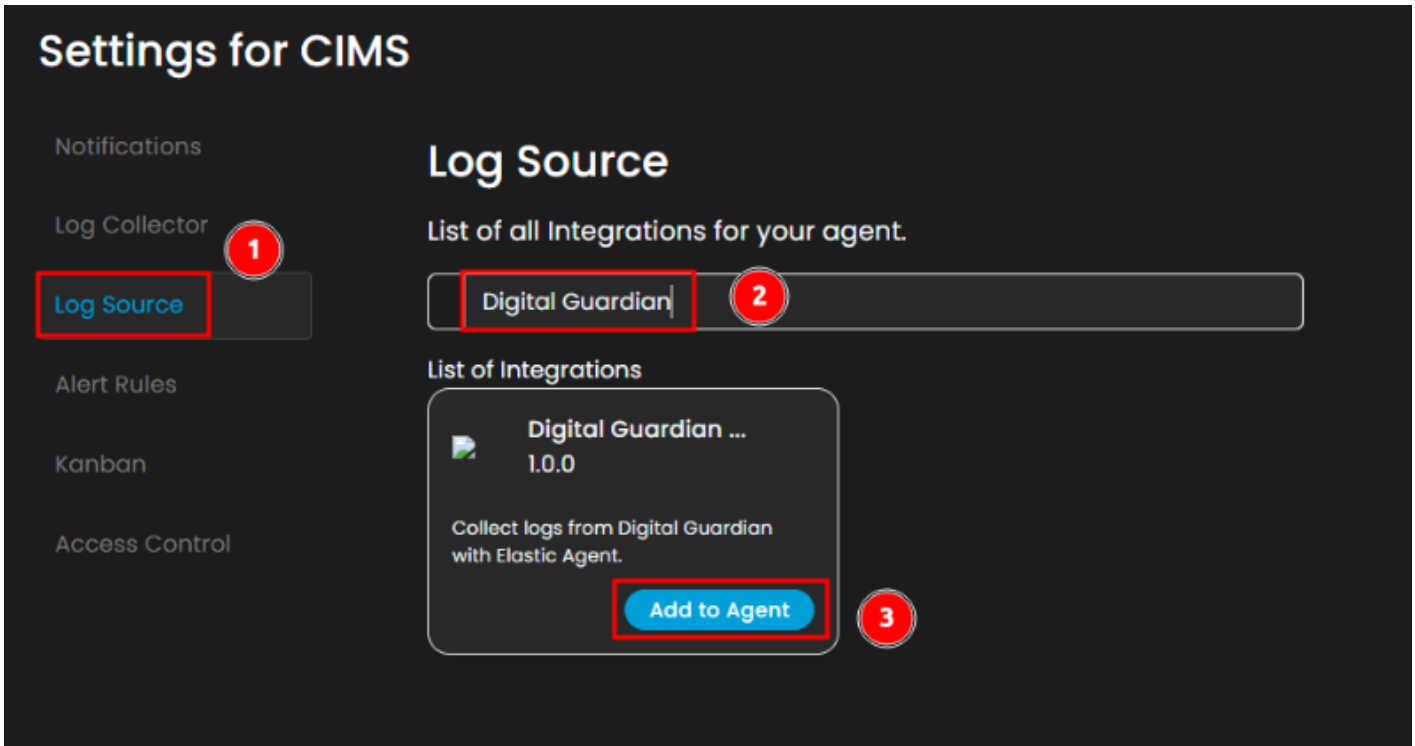
Parameter	Example Value
ARC Server URL	https://arc.digitalguardian.com
Authorization Server URL	https://auth.digitalguardian.com/oauth2/token
Export Profile ID	3454b8d2-6d5f-431c-92df-9b1edc9e4d57
Client ID	dg-elastic-integration-12345
Client Secret	d83jK083jd92JD...

Integration to AQUILA

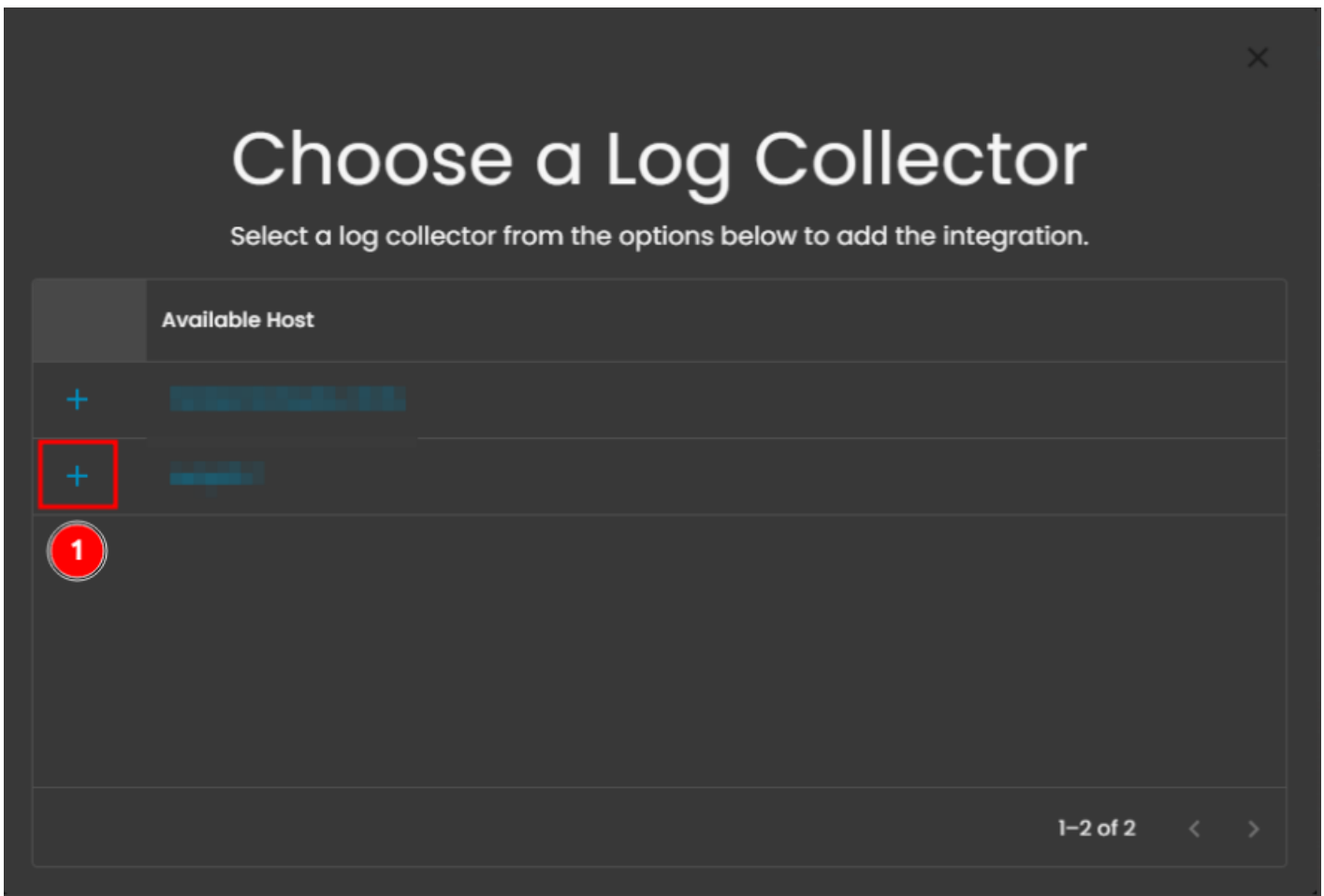
1. Log in to **CyTech - AQUILA**. Choose **Cyber Monitoring -> Cyber Incident Management -> Settings**.

The screenshot displays the CyTech - AQUILA dashboard interface. On the left is a navigation menu with a 'Settings' option highlighted under the 'Cyber Incident Management' section. The main dashboard area features several circular gauges for 'Cyber Monitoring' (54.12% Control Effectiveness), 'Cyber Governance' (25.00% Control Effectiveness), 'Cyber Compliance' (18.57% Control Effectiveness), 'Risk Management' (18.65% Control Effectiveness), 'Identity Security', and 'Data Security'. Each gauge is accompanied by 'Accomplishments', 'Open Tasks', and 'Open Alerts' counts. A 'Settings' button is highlighted with a red box and a '3' in the bottom left corner of the dashboard area.

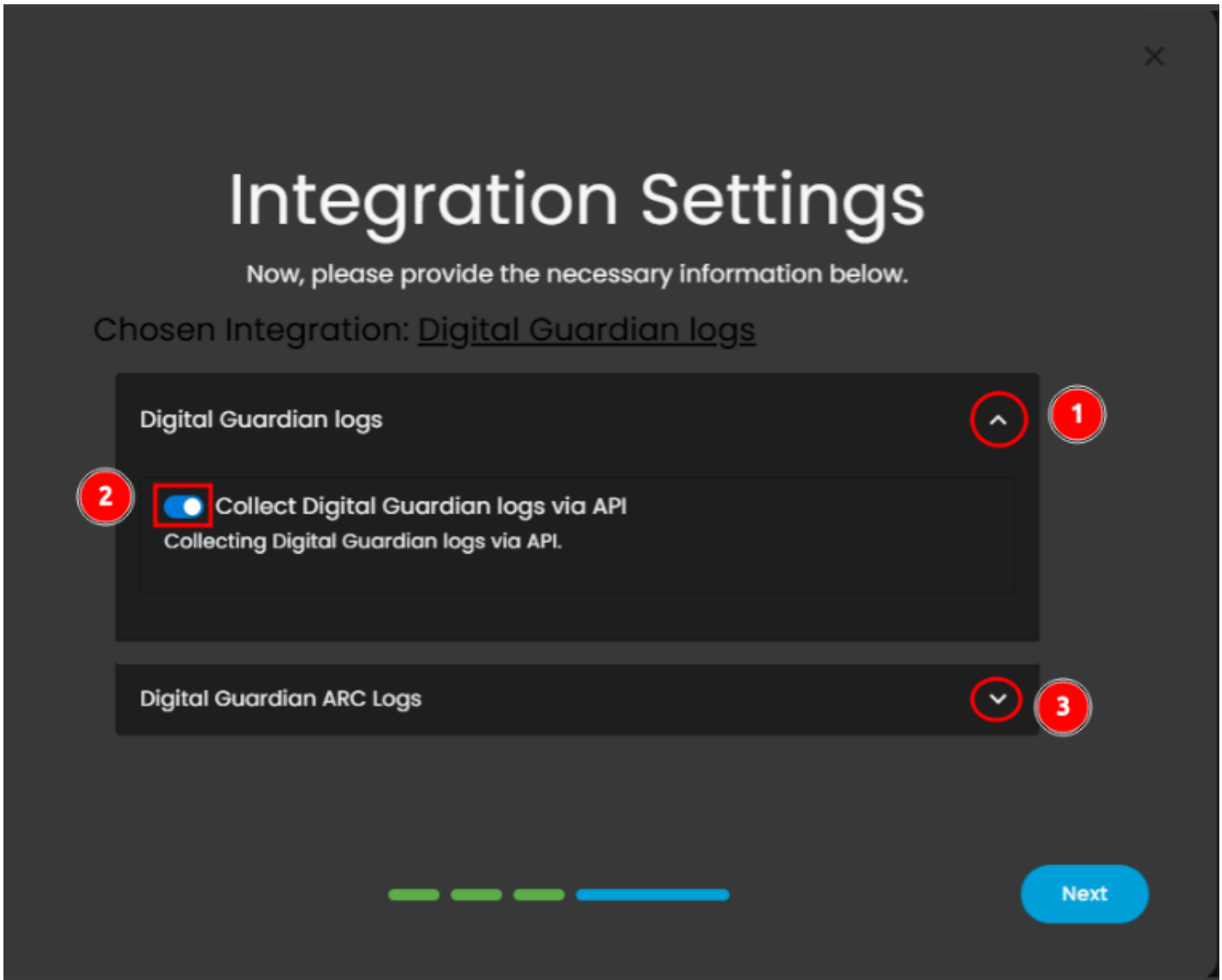
2. Click **Log Source**. In the text box type **Digital Guardian**, the log source will show up and click the **Add to Agent**.



3. Choose the **Log Collector** name you installed. Click the + sign.



4. Enable the **Collect Digital Guardian logs via API**.



5. Paste the information you gather on each text box. **ARC Server URL**, **Authorization Server URL**, **ARC Export Profile ID** and **Client ID**. Then scroll down.

Collecting Digital Guardian ARC logs via API.

1 ARC Server URL *
Gateway Base URL of the Digital Guardian ARC API.

2 Authorization Server URL *
Authorization Server URL to get valid token.

3 ARC Export Profile ID *
ARC Profile GUID to Export.

Interval *
1h
Interval between two REST API calls. Supported units for this parameter are h/m/s.

4 Client ID *
Client ID of Digital Guardian.

Next

6. Paste the information you gather on each text box. **Client Secret**, then click the **Tags** text box, it will show 2 tags you will need to add.



1

Client Secret *

Client secret of Digital Guardian.

Scope *

client

Scope of Digital Guardian.

HTTP Client Timeout *

10m

Duration before declaring that the HTTP client connection has timed out.
Valid time units are ns, us, ms, s, m, h.

2

Tags *

Preserve original event *

Preserves a raw copy of the original event, added to the field `event.original`.



Next

Client Secret *

Client secret of Digital Guardian.

Scope *

client

Scope of Digital Guardian.

HTTP Client Timeout *

10m

Duration before declaring that the HTTP client connection has timed out.
Valid time units are ns, us, ms, s, m, h.

Tags *

Enter Tags

1 forwarded

2 digital_guardian-arc

Next

7. Then click **Next** so that the integration will process the information you inputted.

Client Secret *

Client secret of Digital Guardian.

Scope *

client

Scope of Digital Guardian.

HTTP Client Timeout *

10m

Duration before declaring that the HTTP client connection has timed out.
Valid time units are ns, us, ms, s, m, h.

Tags *

forwarded × digital_guardian-arc × Enter Tags ×

Preserve original event *

Preserves a raw copy of the original event, added to the field `event.original`.

1 Next

8. Wait for the **Successful** window to display, this will confirm the successful integration.



Setting up your service

Great start! Now, please wait 2-3 minutes while we get everything ready for you.



Adding User Info to our SIEM

0%



If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #1

Created 18 July 2025 23:29:29 by Jeff Saguing

Updated 19 July 2025 01:15:24 by Jeff Saguing