



TRIAL GUIDE · AZURE MARKETPLACE

Test Evaluator ATM Skimmer Detection in your own Azure

A step-by-step guide to your first trial: from GPU quota and sign-in to your first detection, what it costs, and how to remove everything afterwards.

About 2 hours once you have GPU quota

Runs in your subscription

Confidential GPU

No Evaluator fee for uploaded clips

START HERE

Azure Marketplace → "Evaluator ATM Skimmer Detection"

Scan the code, or open

portal.azure.com/#create/evaluator-ai.evaluator-atm-securitystandard

Evaluator · Trial guide version 1.1 · September 2026 · Prices are Azure pay-as-you-go list prices and can differ in your agreement.



What you are testing

Evaluator ATM Skimmer Detection analyzes short event clips from your ATM, point-of-sale and fuel-pump cameras and flags **card-reader tampering**: someone fitting a skimmer, overlay, insert or other foreign device to the machine, or repeatedly manipulating the card reader. Each result comes with the model's reasoning and the clip, so a person can check it before acting.

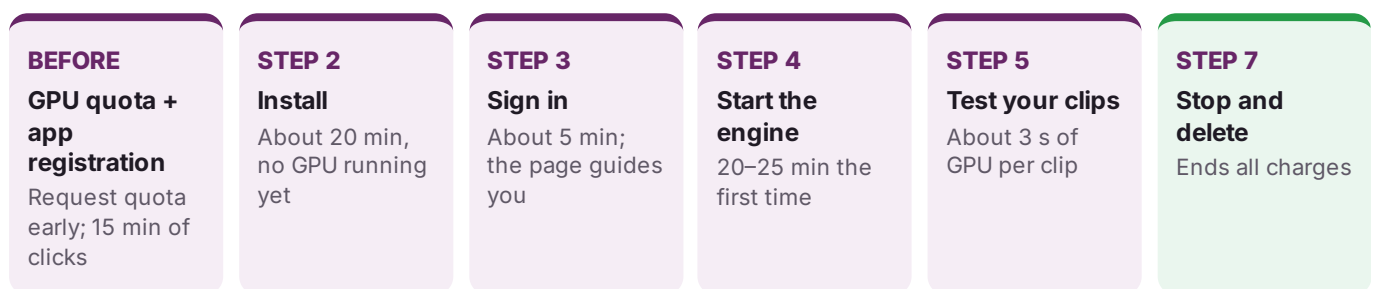
It installs as a **managed application in your own Azure subscription**: a web dashboard, storage for clips and results, and an AI engine that runs on an **Azure confidential VM with an NVIDIA H100 GPU in confidential mode**. Your clips and detection results stay in your subscription.

What to expect from the results

The model is trained and tested on ATM, point-of-sale and fuel-pump footage. Heavily compressed or low-quality footage lowers accuracy.

Results are produced by AI and can be wrong. They support human review and do not replace it. The model detects tampering as it is captured on camera; it does not find a device that was fitted out of view or before monitoring began.

The trial at a glance



What a trial costs

- **Azure, while installed:** about \$5–7 a day, even with the engine stopped.
- **Azure, while the engine runs:** \$6.98–8.90 an hour, by region.
- **Evaluator fee:** \$0 while you test with uploaded clips.

Example: install, test for 2 hours and delete the same day: about \$20 in Azure. Details on page 8.

What you need

- An Azure subscription you can create resources in.
- Permission to create an app registration in Microsoft Entra ID.
- GPU quota in Central US, East US 2 or West Europe.
- A few short clips from your own cameras.

Before you start

1. Azure permissions

You need **Owner** or **Contributor** on the subscription, or on the resource group you will install into. The install creates its own resource group (the "managed resource group") for everything it deploys.

2. Microsoft Entra permissions

Dashboard sign-in uses one **app registration** in your directory, which you create in Step 1. You can create it if your organization lets users register applications, or if you hold a role such as *Application Developer*. Granting consent for the whole organization needs an admin role such as *Cloud Application Administrator*; without it, each person is asked to consent at their first sign-in (if your organization allows that).

3. GPU quota: request it first

The engine runs on the confidential H100 VM size `Standard_NCC40ads_H100_v5`, which exists in only three regions. Each running engine instance needs **40 vCPUs** of quota.

1. In the Azure portal, search for **Quotas** and open **Compute**.
2. Filter by **NCC** and by the region you will use: **Central US**, **East US 2** or **West Europe**.
3. Select **Standard NCCads2023 Family vCPUs** and request a new limit of **40**.

Do this first. Quota requests can take from minutes to several days. Quota is per region and does not transfer: install in the region where you have it. Without quota, the install still succeeds, but starting the engine fails with an allocation error.

4. Test clips

- **Format:** MP4, AVI or MOV; up to 200 MB and 10 minutes each.
- **Best results:** one event per clip, 50 seconds or under, as your cameras or video management system record them. Longer clips are analyzed in full, in segments.
- **For a fair test:** include normal visits as well as tampering, use your usual camera angles, and avoid heavily re-compressed copies (for example, clips forwarded through messaging apps).
- **Privacy:** uploaded clips stay in your Azure subscription.

5. Time and budget

Plan about **2 hours** for the first session, once quota is granted: Step 1 takes about 15 minutes, the install about 20, sign-in about 5, the first engine start 20–25, then testing. Budget about **\$20** in Azure for a same-day trial (page 8).

1 Create the app registration for sign-in

About 15 minutes, before you install. The install wizard asks for its Client ID.

1. **Register.** In the Azure portal, search for **App registrations** → **New registration**.
 - Name: `Evaluator ATM Skimmer Dashboard`
 - Supported account types: **Accounts in this organizational directory only (Single tenant)**
 - Redirect URI: leave empty for now (you add it in Step 3).

Click **Register**, then copy the **Application (client) ID** from the Overview page.

2. **Manifest.** Under `"api"`, set `"requestedAccessTokenVersion": 2` and click **Save**. (In the older manifest view, set `"accessTokenAcceptedVersion": 2`.) **If you skip this, sign-in works but every page says access is denied.**
3. **Expose an API.** Next to **Application ID URI**, click **Add**, keep the proposed `api://<client ID>` and **Save**. Then **Add a scope**: scope name `access_as_user`; who can consent **Admins and users**; display name *Use the ATM Skimmer Detection dashboard*; description *Lets the dashboard call its own API as the signed-in user*; state **Enabled**.
4. **App roles.** Click **Create app role** five times. For each: allowed member types **Users/Groups**, tick **Enable this app role**, and type the **Value** exactly as shown:

Display name	Value	What it allows
Skimmer Admin	<code>Skimmer.Admin</code>	Everything, including configuration and users
Skimmer Analyst	<code>Skimmer.Analyst</code>	Detections, clip review, acknowledging, uploads
Skimmer Operator	<code>Skimmer.Operator</code>	Health, throughput and scaling; no video
Skimmer Auditor	<code>Skimmer.Auditor</code>	Read-only detections, clips and audit log
Skimmer Reviewer	<code>Skimmer.Reviewer</code>	Skimmer detections and their clips only

5. **API permissions** → **Add a permission**. Microsoft Graph → Delegated: tick `openid`, `profile`, `offline_access`. Then **My APIs** → **Evaluator ATM Skimmer Dashboard**: tick `access_as_user`. Finally click **Grant admin consent** (needs an admin role).
6. **Assign yourself.** On the Overview page, open the link under **Managed application in local directory**. In **Properties**, set **Assignment required?** to **Yes** and save. In **Users and groups** → **Add user/group**, select yourself and the role **Skimmer Admin**. Nobody becomes an admin automatically.

Prefer two commands instead? [Ask us](#) for the Azure Cloud Shell setup script: it creates the same registration in about 2 minutes and makes you Skimmer Admin.

2 Install from Azure Marketplace

About 20 minutes. No GPU runs, and no GPU is billed, during or after the install.

Open the offer (scan the code on the cover, or search **Evaluator ATM Skimmer Detection** in Azure Marketplace) and click **Create**. The wizard has five tabs:

Tab	What to enter
Basics	Your subscription; a new resource group (for example <code>rg-evaluator-trial</code>); the region where you have GPU quota (the list offers only the three possible ones); a solution name prefix (the default <code>atmskim</code> is fine); an application name.
Confidential GPU	For a trial, keep Instances when started at 1 and set Maximum instances to 1 , so the engine never scales beyond one GPU. Leave the diagnostic box unticked.
Alerting & SIEM	Keep Decide later . You can connect a webhook, Microsoft Sentinel, Splunk or CEF syslog on the dashboard at any time.
Access & Teams	Dashboard network access: Public (internet, Entra sign-in) for a trial. Dashboard app (client ID) : paste the ID from Step 1. Leave all group fields empty.
Review + create	Read the terms and click Create . Deployment takes about 20 minutes.

3 Allow sign-in and open the dashboard

About 5 minutes. Azure assigns the dashboard's address during the install, so this comes after it.

1. In the Azure portal, open **Managed applications** → your application → **Parameters and Outputs**, and copy **dashboardUrl**. Open it in your browser.
2. Until sign-in works, the page itself shows what is left. It gives the exact address with a **Copy** button, a button to your app registration, and a **live check** that turns green when the address is registered.
3. In the app registration: **Authentication** → **Add a platform** → **Single-page application** → paste the address exactly (it starts with `https://` and has no `/` at the end) → **Configure. Use Single-page application, not Web.**
4. Back on the dashboard, sign in with the account that holds **Skimmer Admin**.

If a sign-in fails, the page says why and which step fixes it. The most common causes are on page 9.

4 Start the engine

20–25 minutes the first time. GPU billing starts here.

1. On the dashboard, open **Setup** and click **Start engine** under *Start the detection engine*. The confirmation shows the hourly GPU rate for your region.
2. The status at the top changes from **Engine off** to **Starting...** and then **Engine on**, with a running time and cost counter.
3. The first start prepares the confidential VM, downloads the encrypted engine and releases the model's key only to that attested VM. Later starts take about 11 minutes if you keep the engine's disk (Step 7).

5 Test with your clips

About 3 seconds of GPU per clip once it has uploaded.

1. Wait for **Engine on**, then open **Analyze clip**.
2. Drop one or more clips on the page, or click to browse. They are uploaded and analyzed one after another.
3. Each result shows:
 - **the category: Skimmer placement** or **Normal transaction**;
 - **the confidence: High**, or **Borderline** · **review** when the call is close;
 - the segments analyzed and the time taken;
 - **the model's reasoning** in plain words.

Limit	Value
Uploads per person	10 a minute, 120 an hour
Size and length per clip	Up to 200 MB and 10 minutes
Best results	One event per clip, 50 seconds or under (longer clips get an amber note)
Who can upload	Skimmer Admin and Skimmer Analyst

Good to know

- Every upload is recorded in the audit log (**Access & audit**).
- An uploaded clip is scored in your subscription and then removed from the upload area.
- Uploads never count towards the Evaluator fee.

Read results the right way

- The model judges what hands do at the card reader, as captured in the clip.
- It will not flag a normal customer using a machine that was tampered with earlier.
- Check the clip before acting on any result.

6

Optional: connect a camera feed and alerts

For a pilot on real devices. The Evaluator fee applies from here: \$0.65 per connected device per day.

1. **ATMs page** → **Enroll an ATM**: give each device an ID (for example `ATM-0047`) and its site, bank, region and type. Point-of-sale terminals and fuel pumps are enrolled the same way. Only enrolled IDs are accepted.
2. **Integrations** → **Generate upload credential**: a write-only credential for the private intake storage.
3. **Configure your camera or video management system** (or Evaluator Proximity Monitor) to upload each event clip to `incoming/<device ID>/<clip>.mp4`. The folder is the device ID, so every clip is tagged by where it was uploaded.
4. Results appear on **Live feed** (every clip) and **Detections** (skimmer placements, with Review and Ack).
5. **Alerts**: on Setup or Integrations, configure a **webhook**, **Microsoft Sentinel**, **Splunk** or **CEF syslog** and click **Send test**. Changes apply within about a minute, with no redeploy.

Billing counts each enrolled device that sent clips that day. Remove a device on the ATMs page and its clips are no longer accepted, so it drops out of the count from the next day.

7

Stop the engine and clean up

Stopping ends GPU billing. Deleting the application ends all charges.

1. **Stop**: click **Stop** at the top of the dashboard (or on Setup) and confirm **Stop engine**. The status shows **Engine off** once Azure confirms it.
 - By default the engine's disk is kept (encrypted data only), so the next start takes about 11 minutes. It costs about \$35–42 a month.
 - Tick **Delete the engine VM instead** if you will not restart soon: no disk charge, but the next start takes about 20 minutes again.
2. **Delete when you are done**: Azure portal → **Managed applications** → your application → **Delete**. This removes everything it created, including your clips and results. It takes about 35 minutes. You can also delete the app registration from Step 1.

Remember: an installed application costs about \$5–7 a day in Azure even with the engine stopped. Delete it when the trial ends.

COSTS

What the trial costs

There are two separate charges: **Azure infrastructure**, billed by Microsoft to your subscription, and the **Evaluator fee**, which applies only to connected devices.

Item	When	Cost
Base resources: private registry, network gateway, private endpoints, dashboard, storage, database, logs	While installed, even with the engine stopped	About \$5–7 a day
Confidential H100 GPU	Only while the engine runs, including the start-up	\$7.89/h Central US \$6.98/h East US 2 \$8.90/h West Europe
Engine disk kept after Stop	Until you delete it (Step 7)	About \$35–42 a month
Evaluator fee	Enrolled devices sending clips (Step 6)	\$0.65 per device per day
Evaluator fee for clips uploaded on Analyze clip	Always	\$0

Example: a same-day trial

Install in Central US, run the engine for 2 hours (including its start-up), test your clips, then delete the application: about **\$5** of base resources + **\$16** of GPU = **about \$20**. The dashboard's Infrastructure page shows the live run rate and month-to-date spend.

Azure pay-as-you-go list prices from September 2026, measured on real test installs. Your agreement, region and usage change the total.

How your data is handled

- ✓ **Your subscription:** clips and detection results are stored in your Azure subscription. Evaluator does not receive them.
- ✓ **Confidential computing:** the model and the video frames it analyzes are processed in encrypted memory that the Azure host cannot read. Clips and results at rest use Azure encryption.
- ✓ **Protected model:** the model is delivered encrypted, and its key is released only to an attested confidential VM of your installation.
- ✓ **Access control:** sign-in is through your Microsoft Entra ID, with five roles, and clip views and changes are recorded in an audit log.
- ✓ **Publisher access, disclosed:** Evaluator's license service holds Contributor access to the installation's managed resource group, to deliver the encrypted engine. Every change it makes appears in your Azure Activity Log. Our security disclosure for version 1.0 explains this and the other known limits; [ask us](#) for a copy.

Privacy policy: evaluatorsecurity.com/privacy

HELP

If something does not work

What you see	Cause	Fix
AADSTS50011 (redirect URI mismatch)	The dashboard address is not registered exactly	Step 3: add it as a Single-page application, exactly as shown
AADSTS9002326	The address was added under Web	Remove it and add it as Single-page application
Signed in, but every page says access is denied	Access tokens are version 1	Step 1.2: <code>requestedAccessTokenVersion 2</code>
AADSTS50105 (user not assigned)	This account holds no role	Step 1.6: assign a role, such as Skimmer Admin
"Need admin approval"	Consent was not granted for the organization	An admin clicks Grant admin consent (Step 1.5)
AADSTS700016 (application not found)	The Client ID in the wizard is wrong	Compare it with the app registration
Start fails with an allocation or quota error	No GPU quota in the install's region	Request 40 vCPUs of Standard NCCads2023 Family quota there
An upload waits, then fails	The engine is not running	Start it (Step 4) and wait for Engine on
The dashboard does not open	Private network access was chosen at install	Open it from inside the virtual network, or reinstall with Public



Ready to try it?

Scan to open **Evaluator ATM Skimmer Detection** in Azure Marketplace.



Questions, a guided trial, or the Cloud Shell setup script: evaluatorsecurity.com/contact