

SECURITY • FOR IT ADMINS

Require healthy devices (posture and device trust)

Check device health (posture) and decide which devices Cloudraw trusts, then require healthy devices in your access rules.

Last updated 7 October 2026

Overview

Cloudraw Connect checks the health of each Windows computer and sends a report to Cloudraw every 15 minutes. This report is called the device's **posture**. It says, for example, whether BitLocker is on and whether the antivirus is up to date.

You use the report in two places:

1. **Device trust rules** decide whether a device is *trusted* at all. Once your workspace has a trust rule, a device that matches none of your trust rules gets no access to any app.
2. **Access rules** can ask for a health check for one app. For example: the *Finance* group may open the finance server, but only from a computer with BitLocker on.

Registering a device with Cloudraw makes it *known*, not trusted. Trust always comes from a trust rule or from an admin.

You need

- The *Owner* or *Security admin* role in the Cloudraw admin console. Other roles can view trust and health, but not change them.
- Cloudraw Connect installed on the computers. See [Install Cloudraw Connect](#).

NOTE

The health report is **reported by the device**. Cloudraw shows it with that label. It is a strong signal, but it is what the computer says about itself.

What each health check means

Open a device under **Devices** to see its last report. Each check is *met*, *not met* or *not reported*. Here is what Cloudraw Connect looks at on Windows.

Check	Rule field	What it checks on Windows
Disk encrypted	<code>disk_encrypted</code>	BitLocker is on for the Windows (system) drive. If BitLocker is <i>suspended</i> , the check is not met.
Antivirus installed	<code>antivirus_present</code>	At least one antivirus product is registered in Windows Security Center. This can be Microsoft Defender Antivirus or another product.
Antivirus on	<code>antivirus_on</code>	At least one registered antivirus is turned on and its signatures are up to date , as Windows reports it.
EDR sensor running	<code>edr_present</code>	An endpoint detection and response (EDR) sensor service is running. Cloudraw Connect recognises Microsoft Defender for Endpoint, SentinelOne, CrowdStrike, Sophos, ESET and Cortex. An antivirus alone does not count.
Firewall on	<code>firewall_on</code>	Windows Firewall is on for all three profiles: Domain, Private and Public. If any profile is off, the check is not met.
System up to date	<code>os_updated</code>	The last Windows update was installed within the maximum patch age (30 days by default), and no restart has been pending longer than the pending restart limit (7 days by default).
Screen lock	<code>screen_lock</code>	A screen lock policy for the computer is on, and its timeout is no longer than the screen lock limit (15 minutes by default). Cloudraw reads the computer policy, not each user's own setting. On computers without a policy this check is often <i>not reported</i> .
Joined to a domain	<code>domain_joined</code>	The computer is joined to an Active Directory domain.
Workgroup computer	<code>workgroup</code>	The computer is not joined to an Active Directory domain. Computers joined only to Entra ID, or only enrolled in MDM, count as workgroup computers.

Check	Rule field	What it checks on Windows
Joined to Entra	entra_ joined	The computer is joined to Microsoft Entra ID.
Enrolled in MDM	mdm_en rolled	The computer is enrolled in a mobile device management (MDM) service, as Windows reports it.
Managed by your organization	manage d	Any one of: joined to a domain, joined to Entra, or enrolled in MDM.

Rules can also use **Computer type** (domain computers, workgroup computers, or either) and, in trust rules only, the **operating system**.

Change the limits

Three checks use limits you can change in **Settings** → **Device health**:

Setting	Default	Allowed range
Maximum patch age	30 days	1 to 365 days
Pending restart limit	7 days	0 to 90 days
Screen lock limit	900 seconds (15 minutes)	30 to 7200 seconds

The new limits apply to each device's next report.

Reports must be fresh

A report older than 60 minutes counts as **not reported**. Then every check is unmet, and rules that need a check do not match. A computer that is off or offline therefore loses health-based access until it reports again.

One exception protects you from a Clouddraw or network outage. If at least half of your reporting devices stop reporting at the same moment, Clouddraw keeps their last report for up to 2 more hours and shows an event about it.

What people see

The device page and Clouddraw Connect split the report into three parts:

- **Required:** the checks your rules ask for on this device, each *met* or *not met*.

- **Recommended:** good-practice checks that fail but that no rule requires. These never block anything.
- **Facts:** things like domain or workgroup, Entra and MDM. They are not good or bad on their own.

Device trust rules

A trust rule says which devices Clouddraw trusts. A device is trusted when it matches **at least one** enabled trust rule.

1 Open trust rules

Go to **Devices** → **Trust rules** and click **Add trust rule**.

2 Choose the conditions

Trust rules use the same conditions as access rules. Useful ones are a group of people, health checks, computer type and operating system. For example: *Disk encrypted* AND *Antivirus on* AND *Firewall on*.

3 Check the preview

Before you save, the preview lists the devices the rule would trust now, and who would **gain** or **lose** trust compared to today. Devices you trusted or blocked by hand, and quarantined devices, are not in this list.

4 Save

Clouddraw checks every device again right away. Each device that changes state creates a *trust* event.

WARNING

Your first trust rule changes how the whole workspace works. Before it, devices that are not trusted still keep their access. **After it, every device that matches no trust rule loses access to every app.** Look at the **would lose** list in the preview before you save the first rule.

Trust or block one device by hand

On a device, the trust control has three choices:

Choice	What happens
Trust this device	The device is trusted, whatever your rules say.
Block	The device is not trusted and loses access to every app. Its open sessions end at once.
Follow trust rules	Removes your manual choice. Trust comes from the rules again.

Some things win over a manual *Trust this device*: a suspended person, and a required new sign-in. A quarantined device cannot be changed here. Release it from quarantine first.

Private networks and edge admission

- **Private networks** need a trusted device by default, even if you have no trust rules. Until you add a trust rule, trust devices by hand to reach a private network.
- **Edge admission:** Cloudraw can also hide untrusted devices from the Cloudraw network completely. The console shows if this is on for your workspace. Cloudraw support turns it on. Contact support@cloudraw.com (mailto:support@cloudraw.com).

Health checks in access rules

An access rule can ask for a health check for one app. Add the check under **Require** in the rule editor. For example:

```
Group is Finance AND Disk encrypted is on AND Antivirus on is on
```

Rules to know:

- A rule must always name **who**: a group, a person or a device. A rule with only health checks would let every healthy device in. Cloudraw saves it, but marks it as not enforced, and it grants nothing.
- Each check can be **is on** (true) or **is off** (false). Both are enforced. For example, *Workgroup computer is on* for an app only contractors' own laptops may use.
- A device that has not reported, or whose report is too old, matches neither *on* nor *off*. It is denied.
- The operating system condition works in trust rules only. In an access rule, use computer type or the health checks.
- Access follows the device's latest report at once. When a check fails, new connections to that app are refused.

Browser sessions cannot prove device health

When someone opens an app in the browser from the Cloudraw portal, there is no Cloudraw Connect on that computer. So Cloudraw cannot check its health.

If the only rule that gives a person an app also asks for a health check (or a trusted device), the app appears in the portal as a **locked** tile. The tile names what is needed, for example "disk encrypted". The person can still open the app from Cloudraw Connect on a computer that meets the rule.

TIP

To also allow browser access, add a second rule for the same app with just the group. Keep the health-check rule for Cloudraw Connect. Only do this if browser access without a health check is acceptable for that app.

Why can't this device open the app?

Use **Test access** on a device or an app. Cloudraw checks both gates in order and tells you where the device stops:

1. **Trust**: is the device trusted? If not, the reason, such as "Disk encryption (BitLocker) is off".
2. **Access**: does a rule give this device the app? If a rule names the person's group but a health check fails, it lists the failing checks.

Defender, CrowdStrike, SentinelOne and Intune

Clouddraw does **not** connect to the Microsoft Defender portal, CrowdStrike Falcon, SentinelOne or Intune. It does not read their risk scores or compliance results. It only uses what Windows itself reports on the computer:

Product	How it shows up in Clouddraw
Microsoft Defender Antivirus	<i>Antivirus installed</i> and <i>Antivirus on</i> , from Windows Security Center and the Defender status on the computer.
Other antivirus (for example Sophos, ESET)	<i>Antivirus installed</i> and <i>Antivirus on</i> , if the product registers with Windows Security Center.
Microsoft Defender for Endpoint, CrowdStrike, SentinelOne, Sophos, ESET, Cortex	<i>EDR sensor running</i> , when the product's sensor service is running on the computer.
Intune or another MDM	<i>Enrolled in MDM</i> (and <i>Managed by your organization</i>), when Windows reports the computer as enrolled. Clouddraw does not read the Intune compliance state.
Entra ID join	<i>Joined to Entra</i> , when Windows reports the computer as Entra-joined.

IMPORTANT

An EDR product that Clouddraw Connect does not recognise does not count for *EDR sensor running*. If you use another EDR, ask support@clouddraw.com before you require this check.

Advanced: the Clouddraw API can set a device's health checks from your own tools (`POST /v0/tenants/{workspace}/devices/{device}/posture`). The device's own next report replaces these values, and they also expire after 60 minutes. See [Automate Clouddraw with the API](#).

Troubleshooting

Message or symptom	Cause and fix
Every device lost access after I saved a trust rule	Your first trust rule makes every device that matches no rule untrusted. Turn the rule off, or trust the devices you need by hand, and use the preview's would lose list next time.

Message or symptom	Cause and fix
<i>"not reported by the device"</i>	The computer did not send that value. For <i>Screen lock</i> this is common on computers without a screen lock policy. Set one by Group Policy or MDM, or do not require this check for those computers.
<i>"device health report is out of date"</i>	No report in the last 60 minutes. Check that the computer is on, online and signed in to Clouddraw Connect.
<i>"Disk encryption (BitLocker) is off" but BitLocker is on</i>	BitLocker may be <i>suspended</i> , for example after a BIOS or Windows update. Resume protection with <code>manage-bde -protectors -enable C:</code> or from the BitLocker settings.
<i>"Antivirus is off or out of date"</i>	Update the antivirus signatures, then wait for the next report (up to 15 minutes).
<i>"Windows Firewall is off for some networks"</i>	One of the Domain, Private or Public profiles is off. Turn it on in Windows Security or by Group Policy.
<i>"Windows updates are overdue"</i>	The last update is older than the maximum patch age, or a restart has been pending too long. Install updates and restart.
<i>"No endpoint detection & response (EDR) sensor running"</i>	The EDR service is stopped, or it is a product Clouddraw Connect does not recognise. See Defender , CrowdStrike , SentinelOne and Intune .
App shows as locked in the browser portal	The rule needs a health check, which a browser cannot prove. See Browser sessions cannot prove device health .
Access rule shows <i>not enforced</i>	The rule names no group, person or device, or it uses a condition that is not enforced in access rules yet (such as time or operating system). Add a group and use health checks or computer type.
Cannot change trust: <i>"This device is quarantined"</i>	Release the device from quarantine first. Its trust then follows your rules.