

SECURITY · FOR IT ADMINS

Allow only specific programs to use an app (app firewall)

Let only the programs you choose open an app through Cloudraw, for example only Remote Desktop for a server.

Last updated 7 October 2026

Overview

Access rules decide **who** may open an app. The app firewall decides **which program** on their computer may open it. For example, a remote desktop server can be opened only with Remote Desktop (`mstsc.exe`), not with a scanner or a script that happens to run on the same laptop.

You set the list of allowed programs per app. Cloudraw Connect enforces it on each computer. For every connection to the app, it checks which program opened it. A program that is not on the list is refused, or only reported while you test.

It works for every app type you publish, including websites published through a connector. For example: only browsers may open your CRM.

You need

- The *Owner*, *Security admin* or *Connector operator* role in the Cloudraw admin console.
- Cloudraw Connect **0.4.0 or later** on the computers. Older versions ignore the list and connect as before.

NOTE

The app firewall applies to Cloudraw Connect only. Browser sessions from the Cloudraw portal run in Cloudraw's own gateway, so there is no local program to check.

Step 1. Turn it on in Simple mode

Simple mode checks the program's **file name**, for example `mstsc.exe`. It is easy to set up and catches most mistakes and unwanted tools.

1

Open the app

In the Cloudraw admin console go to **Apps**, open the app, and open the **Allowed applications** tab.

2

Choose Simple

Set the mode to **Simple**.

3

Add programs

Click a preset (see [Presets](#)) or **Add program** and type the file name, for example `mstsc.exe`. You can add up to 50 programs per app.

4

Keep Report only on

Leave **Report only** on for now (it is on by default) and save. See [Step 2](#).

People see the list in Cloudraw Connect, for example *"Allowed from: Remote Desktop"*.

TIP

In the console's **Simple** view you see Simple mode and the presets only. Switch the console to **Expert** to see Strict mode and file hashes.

To remove all limits for an app, set the mode to **Off** or remove every program. An empty list means no limit.

Presets

Presets add common programs in one click. Each comes with the signer name, so it also works in Strict mode.

Preset	Programs it adds	Signer (publisher)
Remote Desktop	<code>mstsc.exe</code>	Microsoft Windows
Browsers	<code>msedge.exe</code> (Microsoft Edge) <code>chrome.exe</code> (Google Chrome) <code>firefox.exe</code> (Firefox)	Microsoft Corporation Google LLC Mozilla Corporation
SSH	<code>ssh.exe</code> (OpenSSH) <code>putty.exe</code> (PuTTY)	Microsoft Windows Simon Tatham

A preset adds to your list. You can still add other programs.

Strict mode: signed programs only

Simple mode trusts the file name, and anyone can rename a file. Strict mode checks the program itself. A program is allowed only when all of these are true:

- It is **digitally signed** by the publisher you enter. Cloudraw Connect accepts a signature in the file and the Windows catalog signature, so built-in tools like `mstsc.exe` work.
- Its built-in **original file name** matches the name you entered. A renamed copy of another program is refused.
- If you entered a **SHA-256** hash, the file matches it exactly.

1 Choose Strict

On the app's **Allowed applications** tab, set the mode to **Strict (signed programs only)**. You may need the Expert view.

2 Add each program with its publisher

Strict mode needs a publisher for every program. Presets fill it in for you.

3 Pin a hash only when you must

A SHA-256 hash allows one exact version of a file. Leave it empty in most cases.

Find the publisher and the hash

- **Publisher:** right-click the program file, choose **Properties** → **Digital Signatures**, and copy the *Name of signer* exactly. Windows built-in programs often have no such tab because they use a catalog signature. Their publisher is `Microsoft Windows`.
- **SHA-256:** in PowerShell run `Get-FileHash "C:\Path\To\program.exe" -Algorithm SHA256` and copy the 64-character hash.

WARNING

A pinned hash stops matching when the program updates. Windows Update, a browser auto-update or a new PuTTY release will then be refused. Use the publisher alone unless you really need one exact version.

Step 2. Report only, then Enforce

Every new list starts in **Report only**. This is the monitor phase.

Setting	What happens
Report only (default)	Every program still connects. Programs that are not on the list are recorded as would have blocked .
Enforce	Programs that are not on the list are refused and recorded as blocked .

- 1 Run in Report only for a few days**
Let people work normally.
- 2 Review "would have blocked"**
The events table on the app's **Allowed applications** tab lists each attempt: time, device, person, program, publisher and reason. Add any program you want to allow.
- 3 Switch to Enforce**
Turn on **Enforce**. Cloudraw first shows how many connections the list would have blocked in the last 7 days. Confirm if that number is what you expect.

NOTE

Devices send these events with their health report, every 15 minutes. A new attempt can take up to 15 minutes to appear. Cloudraw keeps the last 50 decisions per device. The view shows the last 7 days by default.

Alerts

Each app has an **Alert me** setting on its **Allowed applications** tab:

Alert me	You get an alert when
When something is blocked (default)	A program is refused in Enforce mode.
Also when it would be blocked	A program is refused, and also every <i>would have blocked</i> in Report only. Useful just before you switch to Enforce.
Never	No alerts for this app. Events are still recorded and still sent to your SIEM.

To avoid noise, Cloudraw sends:

- At most **one alert per device, app and program per hour**.
- One summary when your workspace passes **30 app firewall alerts in an hour**. After that it stays quiet for the rest of the hour. The events table still has everything.
- A **critical security alert** when the **same program is refused on 3 or more devices within an hour**. If you don't know the program, investigate: it may be a tool spreading in your network.

Choose where alerts go under **Settings** → **Alerts**, category **App firewall**. By default they go to the console, Telegram and Slack, and not to e-mail. See [Alert channels](#).

If you stream to a SIEM, **every** decision is sent there, without the hourly limit and whatever **Alert me** says. See [SIEM and log export](#).

Blocked attempts on the map

The network map shows app firewall decisions from the **last 24 hours**:

- A device with a **blocked** program is flagged as a security case.
- A **blocked** line goes from the device to the app, with the program name and the count.
- The **needs attention** list names the program, the app and the device, for example: *"telnet.exe was blocked from File server on LAPTOP-12: it is not an allowed application"*.
- Report-only decisions (*would have been blocked*) show as information, not as a security case.

Troubleshooting

Message or symptom	Cause and fix
Nothing is blocked or reported	The computer runs Cloudraw Connect older than 0.4.0. Update it. Also check that the list is not empty and the mode is not Off .
A new attempt does not appear yet	Events arrive with the device's next health report, up to 15 minutes later.
The right program is refused in Strict mode	Check the publisher text against <i>Name of signer</i> exactly. If you pinned a SHA-256, the program may have updated. Remove the hash or enter the new one.
A renamed copy of an allowed program is refused	This is Strict mode working. It checks the built-in original file name, not the name on disk.
A program that opens the app through a helper is refused	Some programs connect through a separate helper process. The events table shows the program that really opened the connection. Add that program too.

Message or symptom	Cause and fix
Save fails with <i>"strict mode needs the publisher"</i>	Every program in Strict mode needs a publisher. Fill it in, or use Simple mode.
Save fails with <i>"The allowed-applications policy could not be applied right now; nothing was changed"</i>	A temporary problem. Nothing changed. Try again in a minute.
Too many alerts	Set Alert me to <i>When something is blocked</i> , or turn off the App firewall category for a channel under Settings → Alerts .