IT quick start

The network, the deploy, sign-in, exclusions and removal, for the person who rolls Jetstone Business out to a fleet. Every step is the console as it stands, at console.blackshard.com.

1. Network requirements and proxies
2. Protect a Windows PC
3. Roll out to many PCs with Intune, Group Policy or an RMM tool
4. PCs with another antivirus
5. Device groups and presets
6. Company sign-in
7. Add an exclusion
8. Tamper and uninstall protection
9. Remove a device
10. Windows blocked the installer
11. A device has not checked in

23 November 2026. Support: support@blackshard.com.au and https://blackshard.com.au/support/jetstone-business
Black Shard Pty Ltd, ABN 66 696 910 773

01

Network requirements and proxies

The hosts and ports the agent connects to, how it works through a proxy, and how to find where a connection stops.

1. Allow outbound TCP 443 from every computer that runs the agent to agents.blackshard.com and updates.blackshard.com.
2. Exempt both hosts from TLS inspection. The agent pins the certificate of the agent host and checks the signature of every update, and it refuses a connection that something on the path has opened.
3. Allow outbound TCP 80 to www.microsoft.com and oneocsp.microsoft.com. Windows reads there that the Black Shard Pty Ltd signature on the installer and on each update has not been revoked.
4. On a network where a direct connection does not reach the agent host, the agent uses the proxy Windows is set to use: the machine WinHTTP proxy, then the proxy of the Internet settings, then each proxy the proxy script of the network lists. It opens a tunnel through the proxy and keeps its own TLS inside.
5. To send every agent connection through one proxy, pass -Proxy http://host:port to Install-Jetstone.ps1 from a deployment pack, or set the property on the MSI. Running the script again with -Proxy sets it on a computer where the agent is already installed:

   ```
   msiexec /i <file>.msi /qn JET_PROXY_URL=http://proxy.example:8080
   ```

6. To see where a connection stops, run the check on the computer as an administrator. It walks the name lookup, the connection, the proxy tunnel, TLS and one request for each host, and names the hop that failed:

   ```
   "%ProgramFiles%\Jetstone\jet-agent-win.exe" check-connection
   ```

What the agent connects to

Host	Port	Used for	TLS inspection
agents.blackshard.com	TCP 443	Enrolment, telemetry and response commands	Exempt this host
updates.blackshard.com	TCP 443	The installer download and agent updates	Exempt this host
www.microsoft.com	TCP 80	Certificate revocation lists for the installer signature	Plain HTTP
oneocsp.microsoft.com	TCP 80	Certificate status for the installer signature	Plain HTTP

> A proxy that asks for a user name and password is set as proxy_url in agent.toml on the computer, in the form http://user:password@host:port, so the password is on no command line. An upgrade keeps the setting.

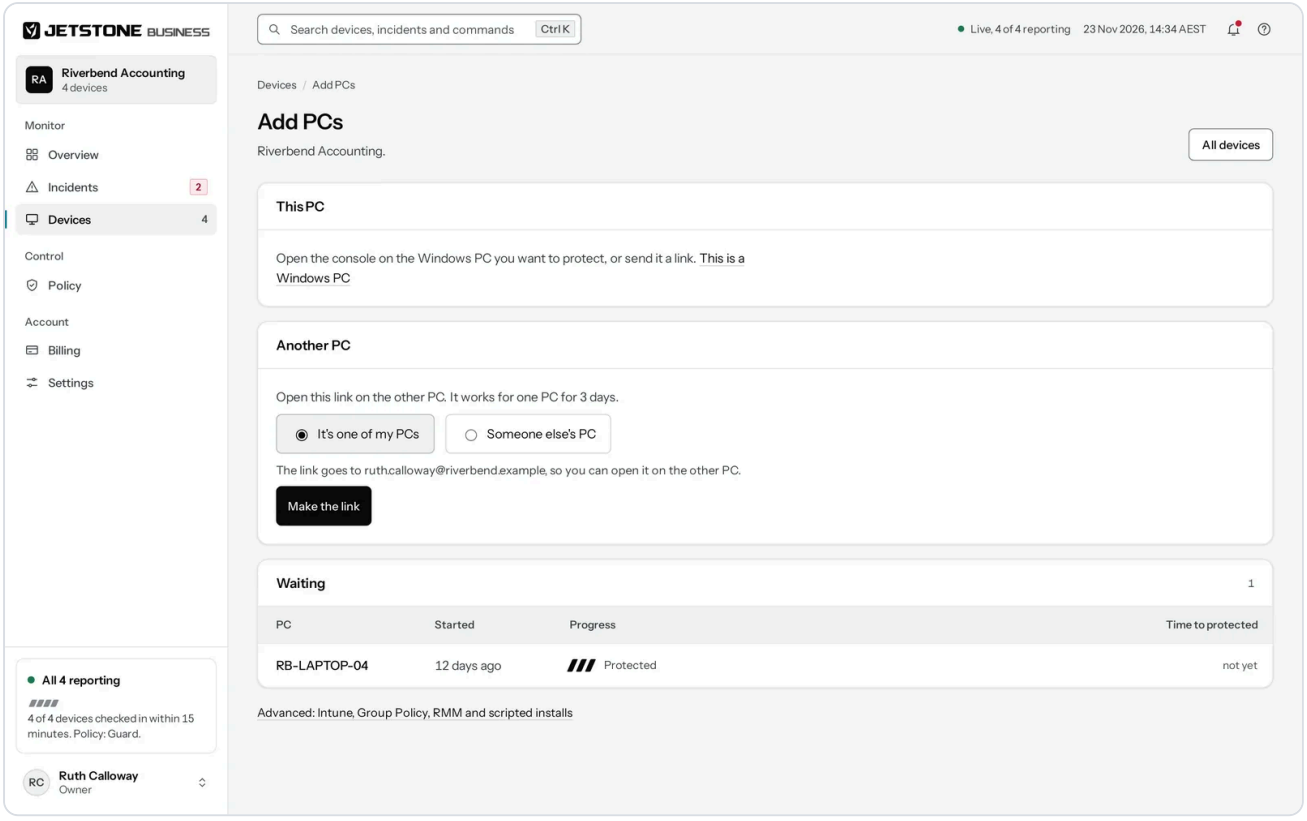
https://blackshard.com.au/support/jetstone-business/network-requirements

02

Protect a Windows PC

Protect the PC in front of you, send a link to another PC, or roll out to many PCs with Intune or an RMM tool.

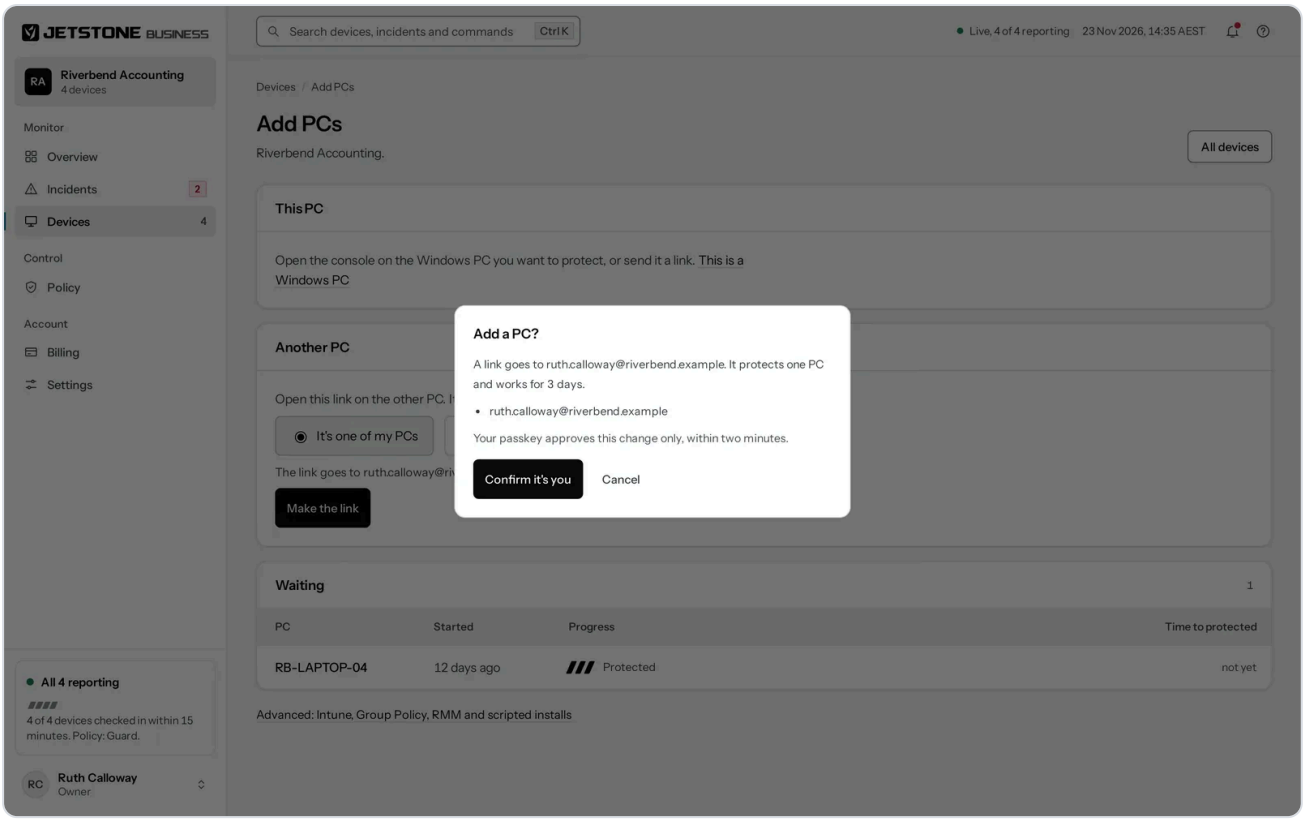
1. Open Devices, then Add PCs.



Add PCs: Protect this PC, Another PC and Advanced

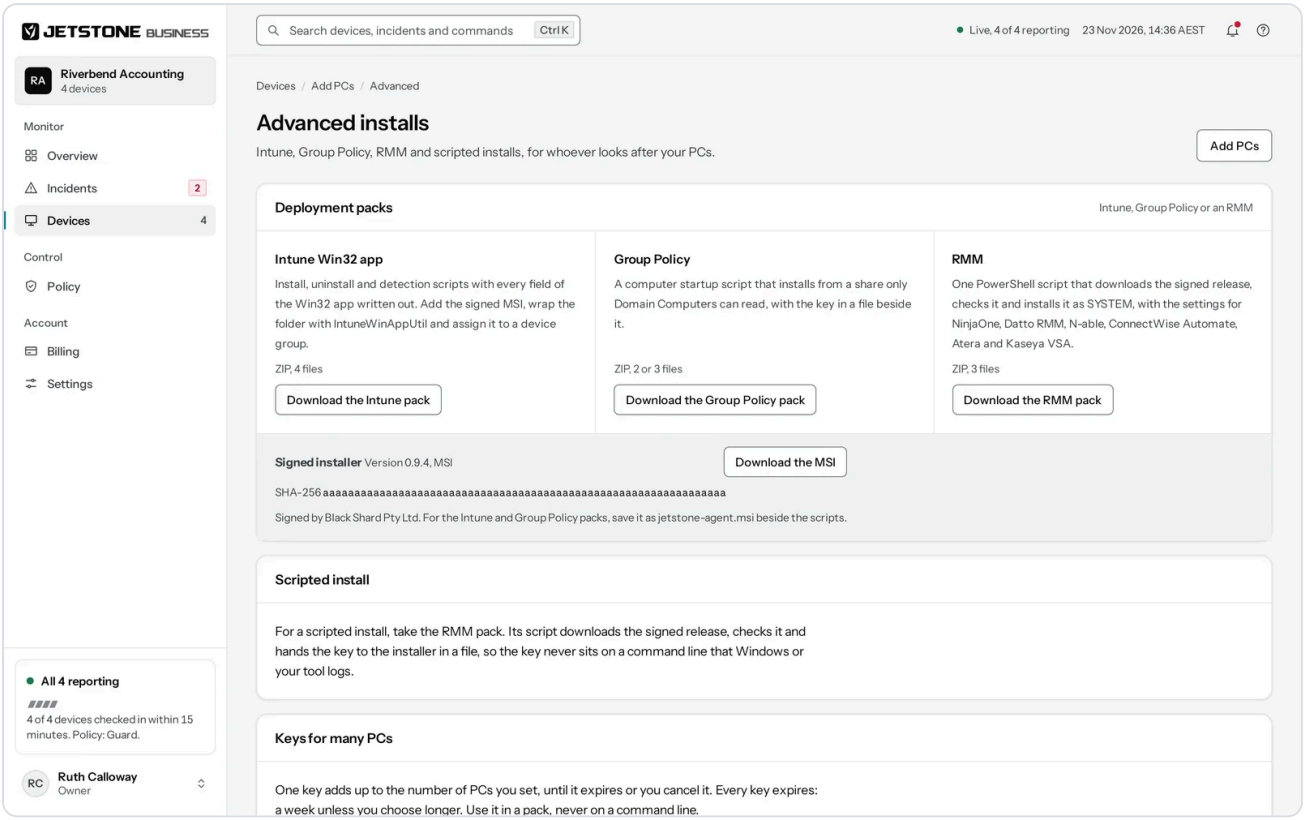
2. On the Windows PC, choose Protect this PC and confirm it is you. Open the download and say Yes when Windows asks. The PC shows as protected within a minute.

3. For another PC, choose Make the link under Another PC. The link protects one PC and works for 3 days.



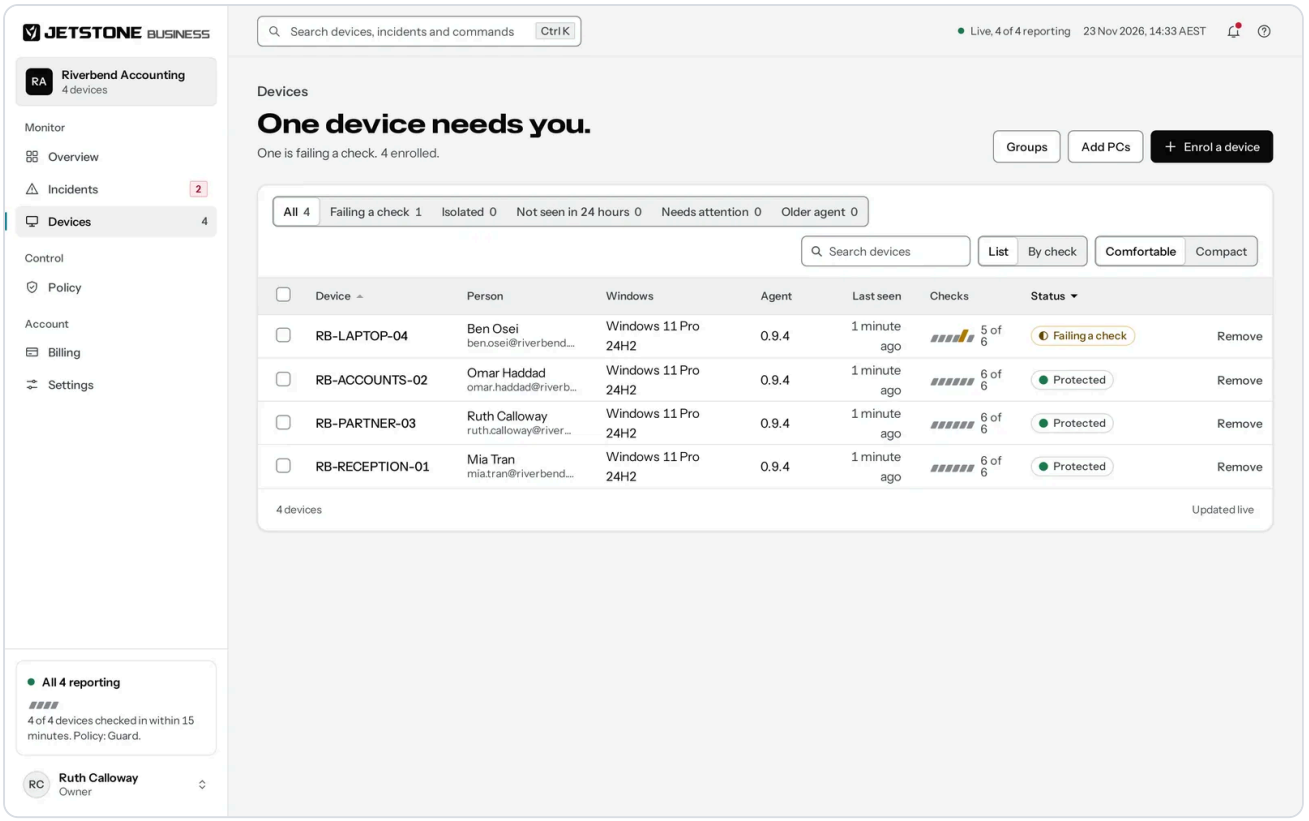
Add PCs with a one-time link made for another PC

4. For many PCs, open Advanced: Intune, Group Policy, RMM and scripted installs.



Advanced installs: Intune, Group Policy, RMM and scripted installs

5. Each PC shows under Waiting as Downloaded, Installing, then Protected.



Devices: every PC with its last check-in

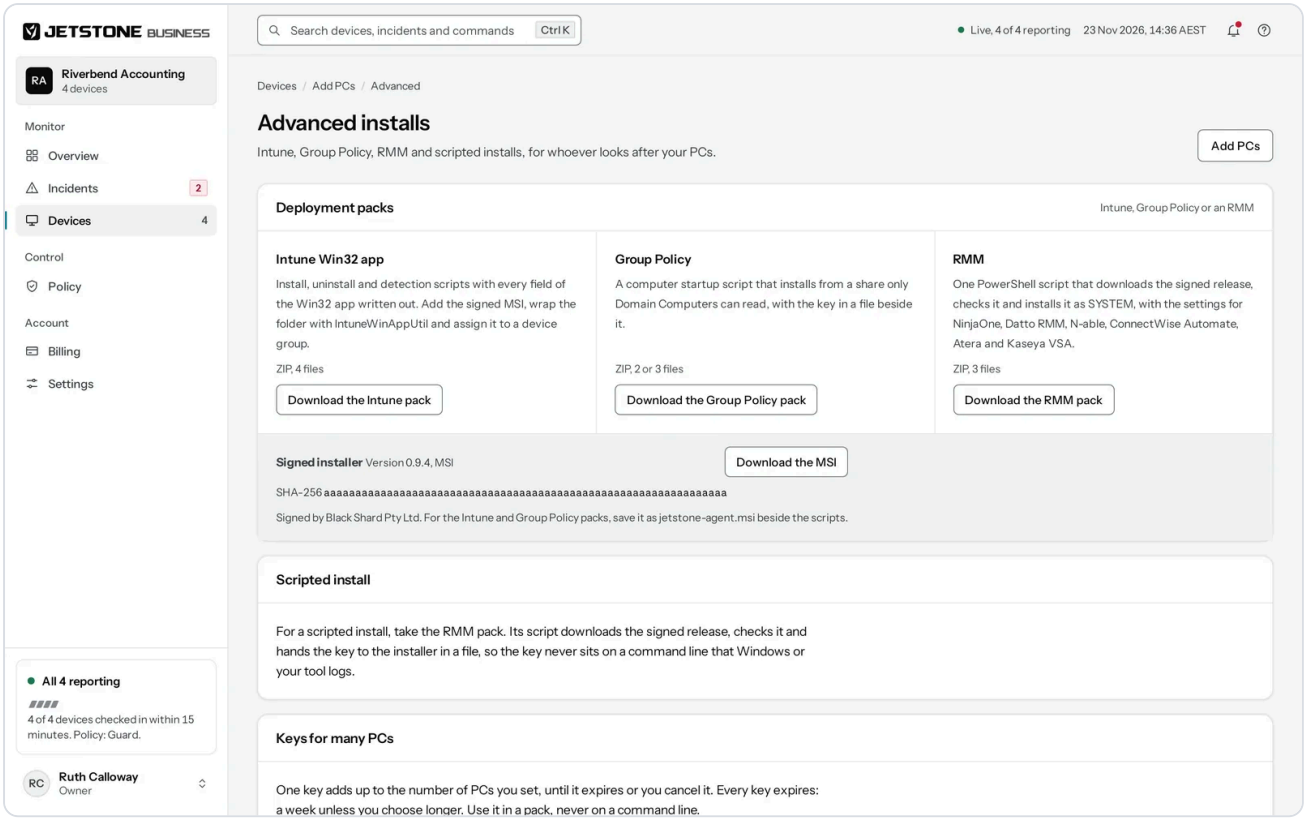
https://blackshard.com.au/support/jetstone-business/install-the-agent

03

Roll out to many PCs with Intune, Group Policy or an RMM tool

Make a key for many PCs on the Advanced page, then deploy with a pack.

1. Open Devices, then Add PCs, then Advanced. Choose Make a key for many PCs.



Advanced installs: Intune, Group Policy, RMM and scripted installs

2. Set the number of PCs, from 1 to 200, and how long the key works: 7, 30 or 90 days, a week unless you choose longer. After that the key enrols nothing; devices it enrolled stay.
3. Optionally pick a group, so each device joins it and its preset before its first check-in, and add tags.
4. Within five minutes of making the key, download the pack for your tool: the Intune pack, the Group Policy startup script, or the PowerShell script for RMM tools. Each pack hands the key to the installer in a file, so the key never sits on a logged command line.
5. Add PCs shows each PC under Waiting until it is protected.

> Anyone holding a key can add PCs up to its count until it expires or you cancel it. Cancel a key from Activation keys on the Advanced page.

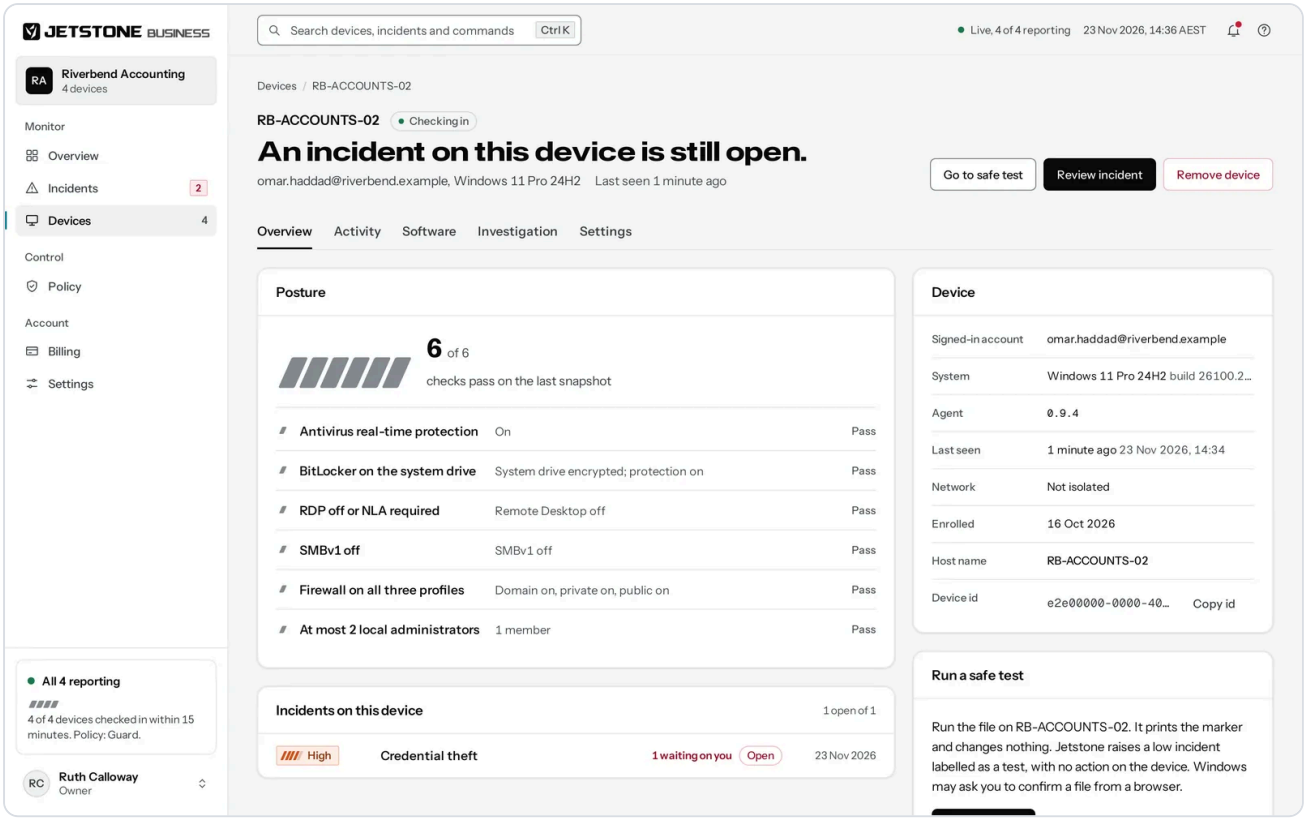
https://blackshard.com.au/support/jetstone-business/roll-out-to-a-fleet

04

PCs with another antivirus

What Jetstone reads and keeps running when a PC already has antivirus.

1. Keep the antivirus the PC already runs. Jetstone reads it from Windows Security and shows the PC as protected by that product, or tells you when its protection is off.



A device page: its checks, its incidents and Tamper and uninstall protection

2. Jetstone detection rules keep running beside it.
3. Installing another antivirus changes the protection Windows reports, so expect an incident for that PC.

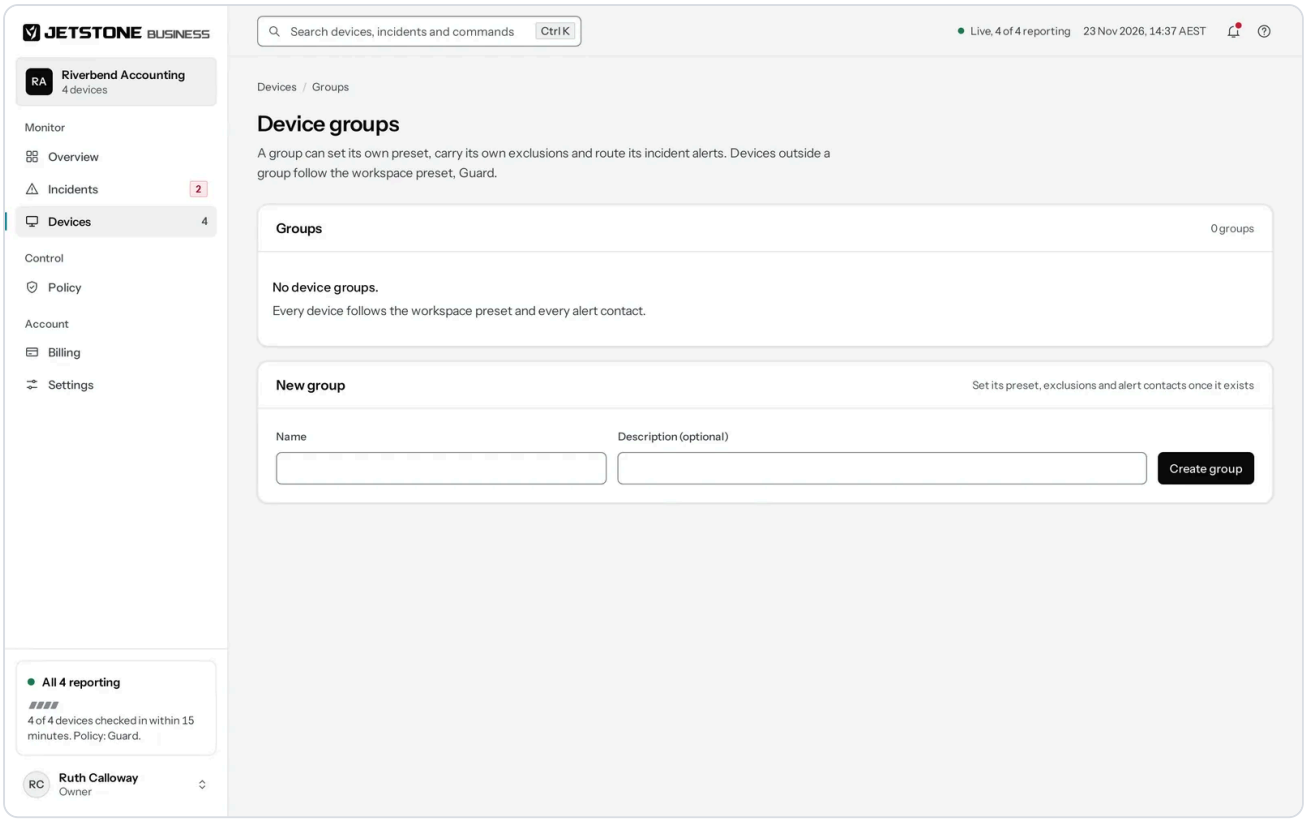
https://blackshard.com.au/support/jetstone-business/devices-with-another-antivirus

05

Device groups and presets

Give a group of devices its own preset, exclusions and alert routing.

1. Open Devices, then Groups, and choose New group. Give it a name and choose Create group.



Device groups and the preset each one follows

2. On the group, choose Change preset to decide its devices under another preset from their next decision.
3. Add exclusions scoped to the group, and route alert contacts to it from Settings.
4. Devices in no group follow the workspace preset. A device in several groups takes the least automatic preset among them.

> Removing a group keeps its devices enrolled. Exclusions scoped to it are removed and contacts routed only to it hear about every device again.

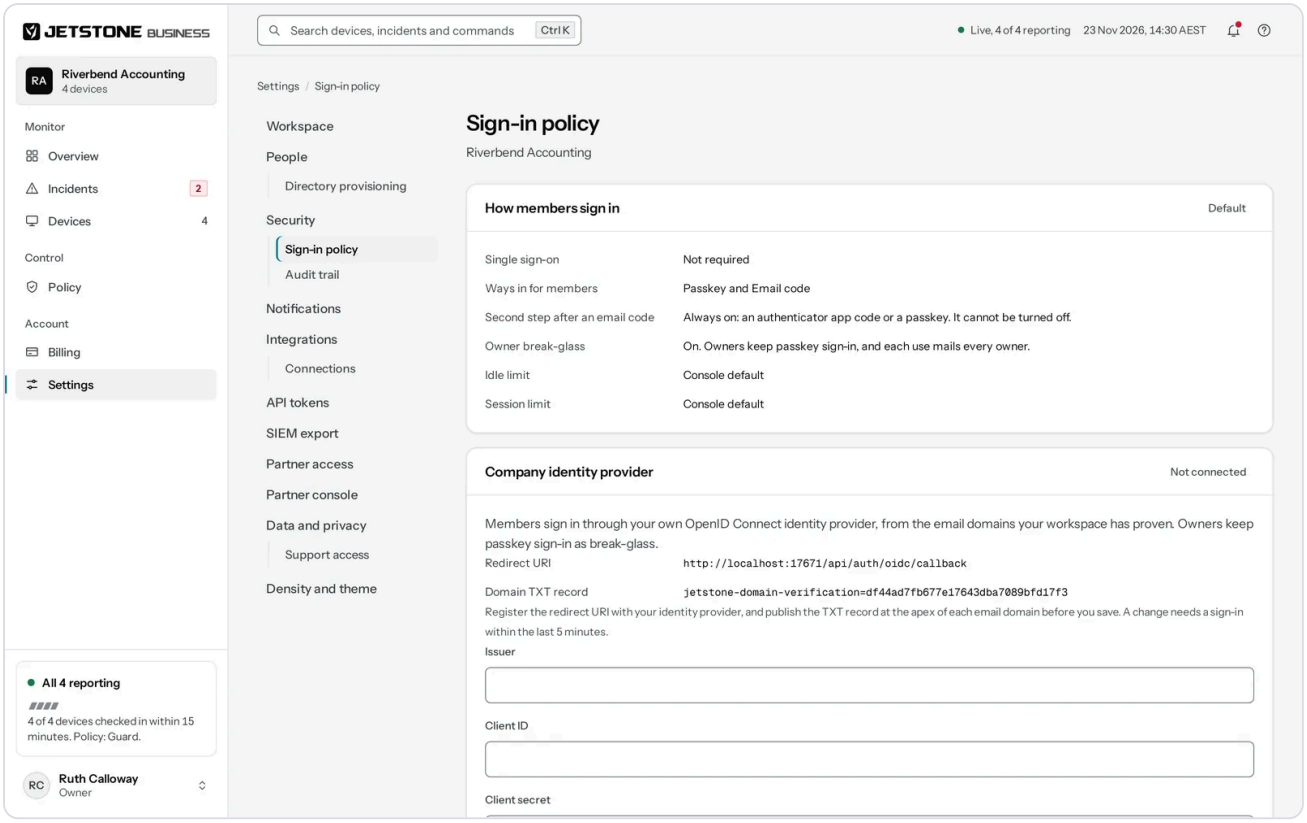
https://blackshard.com.au/support/jetstone-business/device-groups

06

Company sign-in

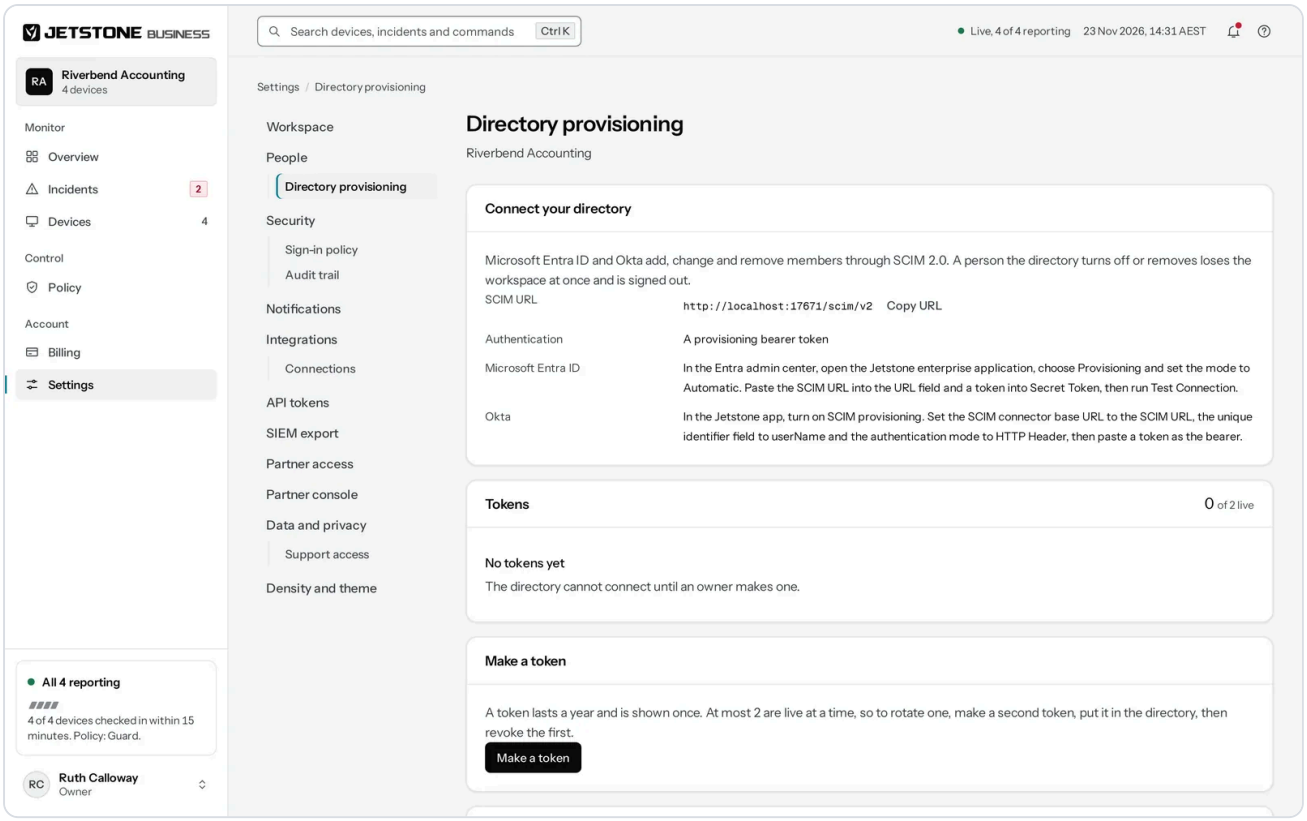
Require Microsoft, Google or your own identity provider for sign-in, set session limits and let people join from your directory.

1. Add a passkey to your own account first. Requiring single sign-on needs one, as the way back in.
2. Open Settings, Sign-in policy, and choose Change the policy. Only an owner can change it, and it needs a recent sign-in.



Sign-in policy: single sign-on, the company identity provider and session limits

3. Under Single sign-on choose Not required, Require Microsoft or Require Google, and list the accepted directory ids or domains.
4. Owner break-glass keeps passkey sign-in for owners while single sign-on is required, and each use mails every owner.
5. Set the Idle limit and Session limit. The idle limit cannot be longer than the session limit.
6. Optionally let people from the accepted directories and domains join as viewers on first sign-in. Choose Save the policy.
7. To add, change and remove members from Microsoft Entra ID or Okta, open Settings, Directory provisioning, choose Make a token and paste the SCIM URL and the token into the directory. Give each pushed group a role under Groups and roles.



Directory provisioning with SCIM

> A person the directory turns off or removes loses the workspace at once and is signed out.

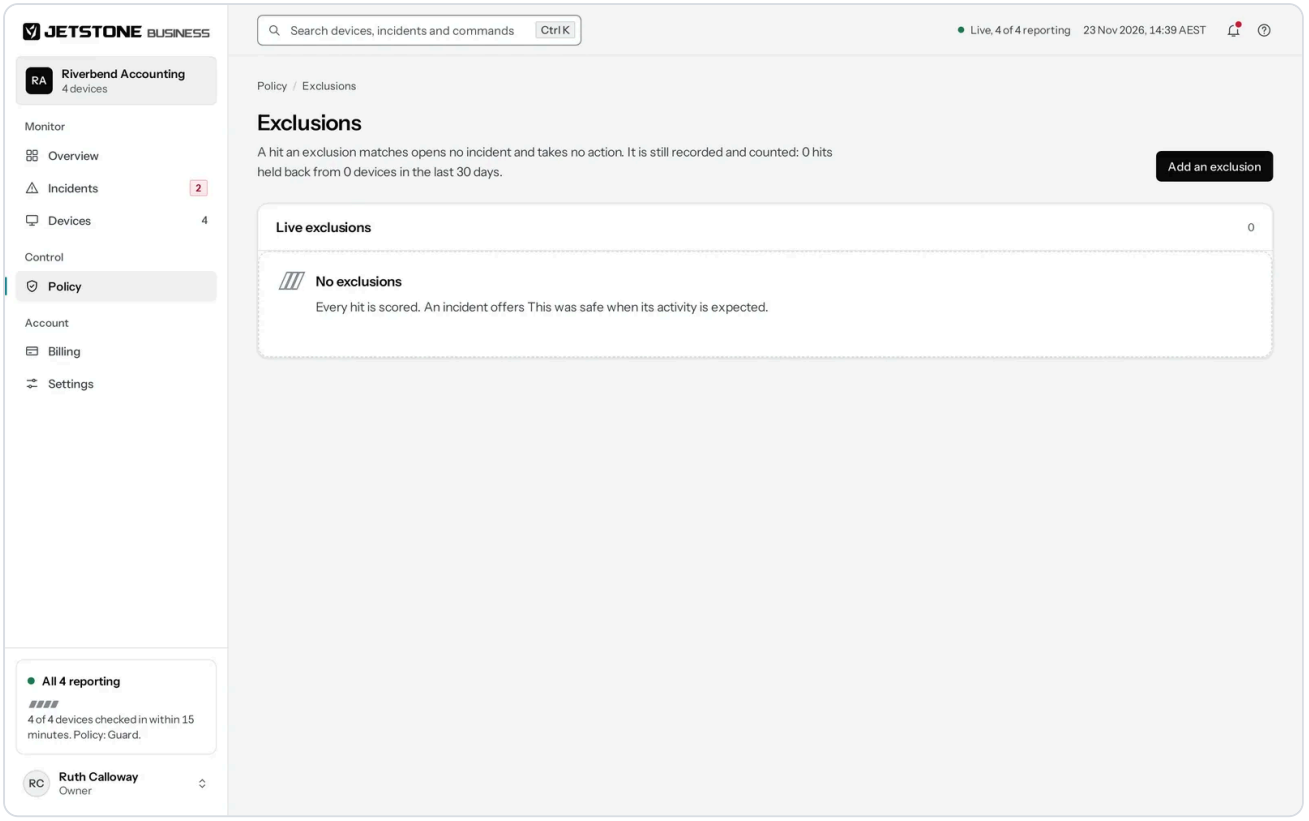
https://blackshard.com.au/support/jetstone-business/company-sign-in

07

Add an exclusion

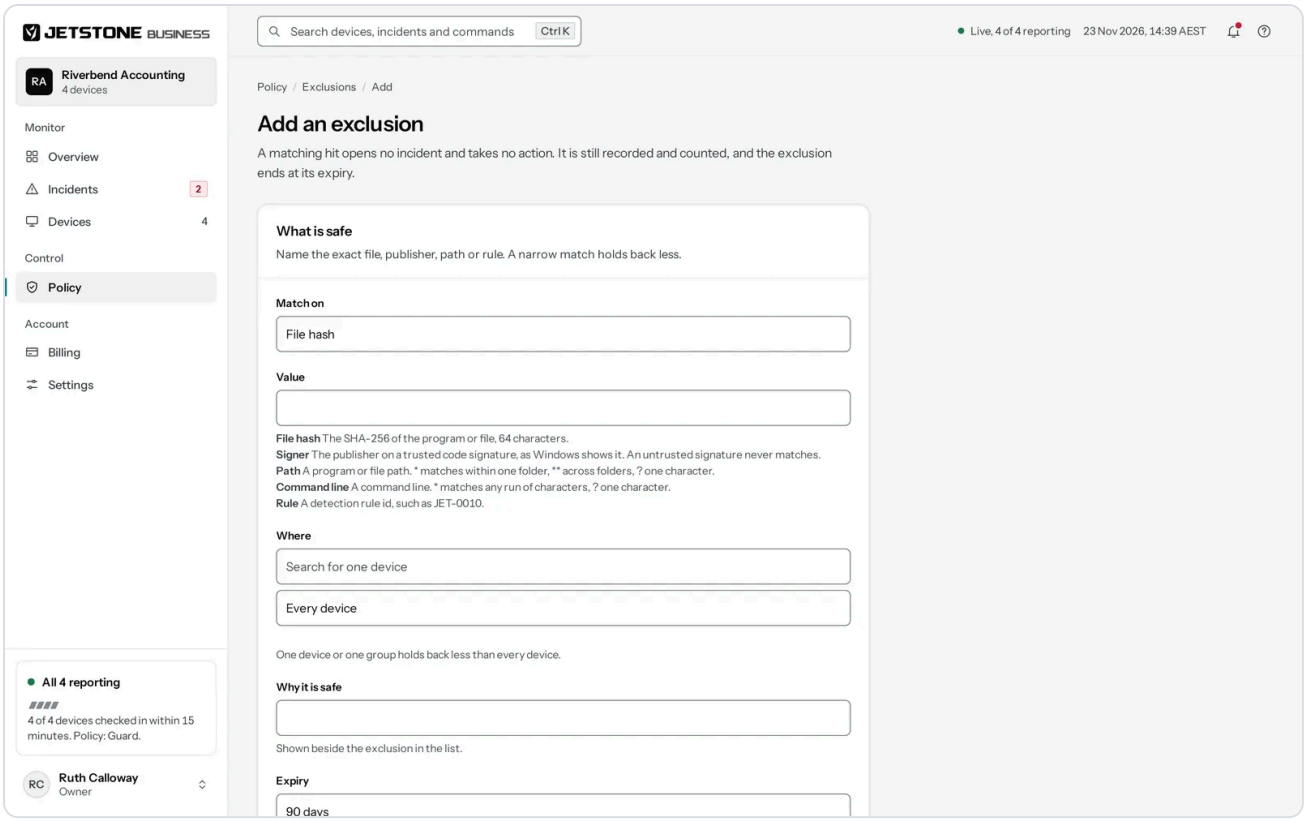
Stop expected activity opening incidents, by file hash, signer, path, command line or rule.

1. Open Policy, then Open exclusions, and choose Add an exclusion. From an incident, This was safe fills the form in for you.



Exclusions, with Add an exclusion

2. Pick what it matches: File hash, Signer, Path, Command line or Rule, and enter the value. In a path, * matches within one folder and ** across folders.



Add an exclusion: what it matches, where it applies and why it is safe

3. Choose where it applies: every device, one device or a device group. Say why it is safe and pick an expiry of 30 days, 90 days, 1 year or no expiry.
4. Review the hits it would hold back, then confirm with your passkey. Devices pick it up within five minutes.

> A hit an exclusion matches opens no incident and takes no action, but it is still recorded and counted. A broad exclusion asks you to type BROAD to confirm it. A workspace holds up to 2000 live exclusions. A rule exclusion for the rules that watch the canary files, the Jetstone agent, the ransomware hold, the antivirus engine and the rollback snapshots covers one device for up to 30 days, and a severity 5 rule needs an expiry when the exclusion covers every device.

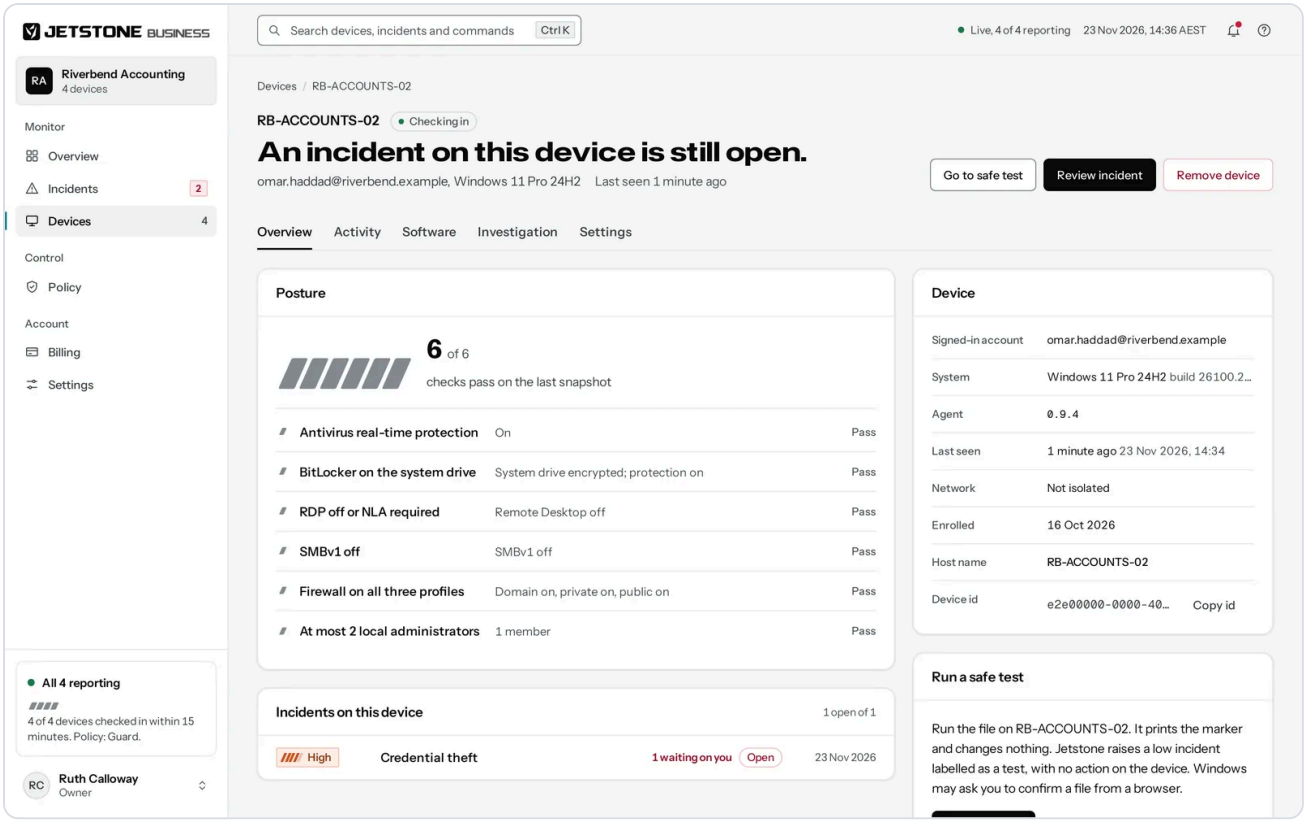
https://blackshard.com.au/support/jetstone-business/add-an-exclusion

08

Tamper and uninstall protection

The uninstall code, tamper incidents and the limits of what the agent can stop.

1. Removing the agent through Windows needs the computer’s uninstall code. A removal without it stops before anything changes and opens a tamper incident.
2. To uninstall, open the device and choose Show uninstall code under Tamper and uninstall protection. The code shows for five minutes and each showing is in the audit trail.



A device page: its checks, its incidents and Tamper and uninstall protection

3. Start the removal from Programs and Features, or run the PowerShell command the card shows, as an administrator.
4. A tamper incident is never acted on automatically under any preset. It comes to you to decide.

> The agent runs without a kernel driver and is not a Windows protected process. An administrator of the computer, or malware with system rights, can still stop it; the agent reports the stop as a tamper incident, normally within 15 minutes.

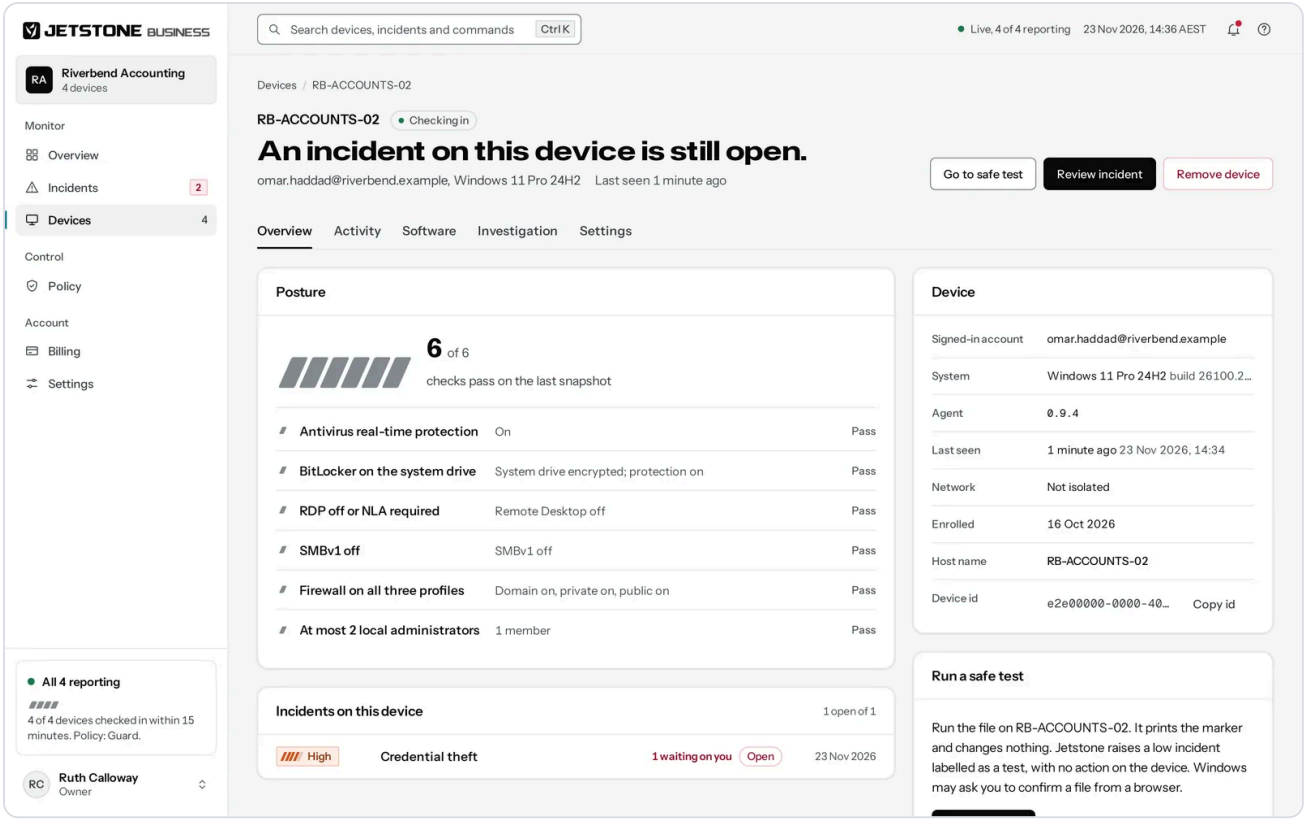
https://blackshard.com.au/support/jetstone-business/tamper-protection

09

Remove a device

Take a device out of the workspace when it is retired or reinstalled.

1. Uninstall Jetstone Business agent from Windows Settings on the PC.
2. Open the device in Devices and remove it. Its certificates stop working at once.



A device page: its checks, its incidents and Tamper and uninstall protection

3. An isolated device cannot be removed. Release it from its incident first.

https://blackshard.com.au/support/jetstone-business/remove-a-device

10

Windows blocked the installer

What to do when SmartScreen, your organisation or an antivirus stops the download.

1. On the blue Windows protected your PC screen, choose More info, then Run anyway.
2. If there is no Run anyway, your organisation blocks downloaded files. Give the file to whoever looks after your computers.
3. If your antivirus removed it, ask whoever runs it to allow the file, then download it again.
4. If the installer stops with a message that it "needs Windows 10 22H2 or Windows 11", the PC runs an older release of Windows 10, Windows Server or an Arm processor. Update an older Windows 10 and run the installer again. The message names Windows Server or an Arm processor when that is the cause.

> The file checks the Jetstone installer's signature and refuses to install it if that does not match.

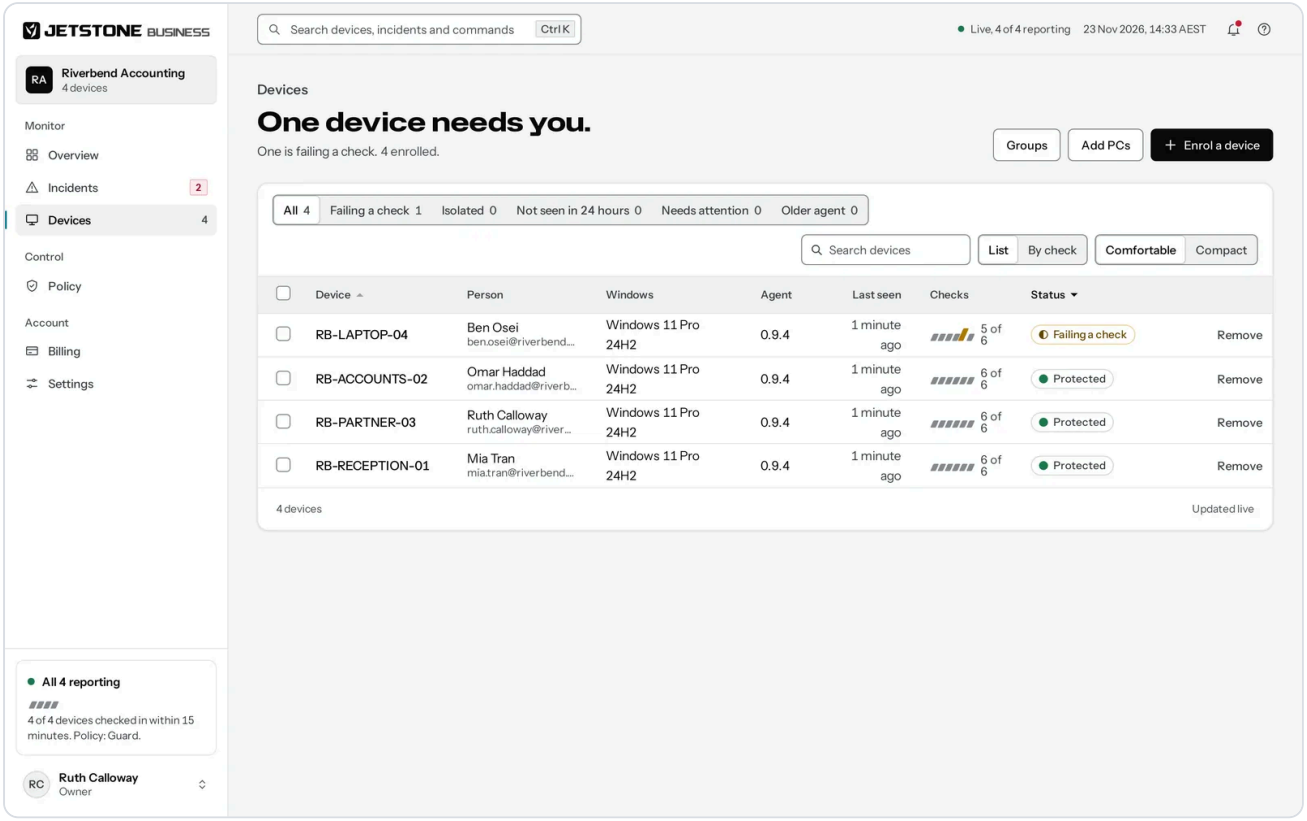
https://blackshard.com.au/support/jetstone-business/windows-blocked-the-installer

11

A device has not checked in

Checks for a new install that never appears, or a device not seen in 24 hours.

1. Keep the PC on and connected to the internet. A new device appears in the list on its first check-in.
2. Check the installer finished without an error and the JetstoneAgent service is running (services.msc). An installer that stops on the Windows release, on Windows Server or on an Arm processor installs nothing.
3. Check the computer reaches agents.blackshard.com on port 443, directly or through a proxy that passes the connection on without opening its TLS, and that its clock is within a few minutes of the real time. On the computer, jet-agent-win.exe check-connection names the hop that failed.
4. Read %ProgramData%\Jetstone\agent.log. It names the refusal when the agent host turned the key away; a used-up or mistyped key reads as a refusal there too.
5. On Devices, Enrolment health shows the last day of activations and certificates, and any refusals.



Devices: every PC with its last check-in

> A device not seen in 24 hours shows as not checking in and costs health score points.

https://blackshard.com.au/support/jetstone-business/device-not-checking-in