SECURITY
SOLVE

Company Portal

See and manage your company's Security Solve: servers, offices, people and devices, in one place

Guide for IT administrators · November 2026

by TECHNOLOGY SOLVE

securitysolve-portal.techsolve.io

WELCOME

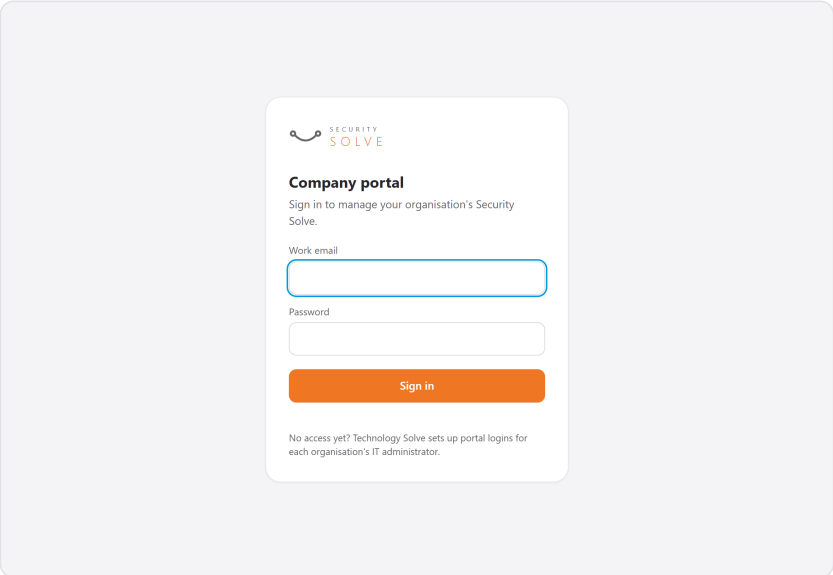
Your company's Security Solve, in one place

The company portal lets your IT administrator see how Security Solve is protecting the company and make everyday changes without waiting for a support ticket.

- **See everything at a glance:** your private VPN servers, office gateways, who's connected, and how many threats were blocked this week.
- **Manage people and devices:** add staff, reset passwords, create VPN profiles, and block a lost laptop in seconds.
- **Connect your offices:** link each office network to your VPN with one install command.
- **Set your own rules:** block or allow sites, choose your DNS, and decide whether devices can reach printers and file servers on local networks.
- **Ask for more:** request a new server, support or a plan change, and follow its progress.

Signing in

Open **securitysolve-portal.techsolve.io** and sign in with the work email and temporary password Technology Solve sent you. Then choose **Change password** from the account menu (your initials, top right). The portal works in any modern browser, on a computer, tablet or phone.



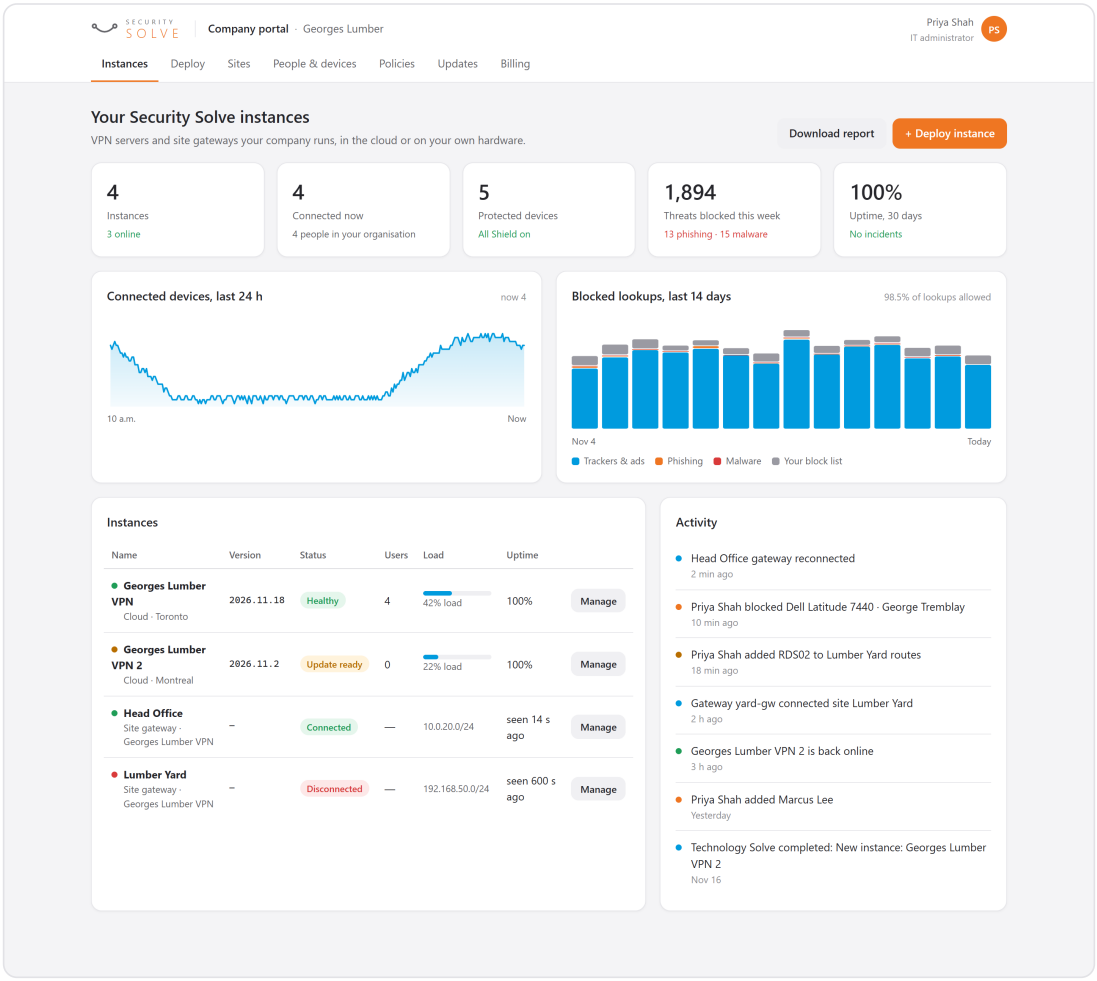
The sign-in page

Your organisation only. The portal only ever shows your own organisation. Security Solve never shows what your people browse: the portal shows counts of blocked threats, not the sites anyone visited.

INSTANCES

How everything is running

The first page you see. The tiles at the top answer the usual questions: is everything up, who's connected, and is the protection working?



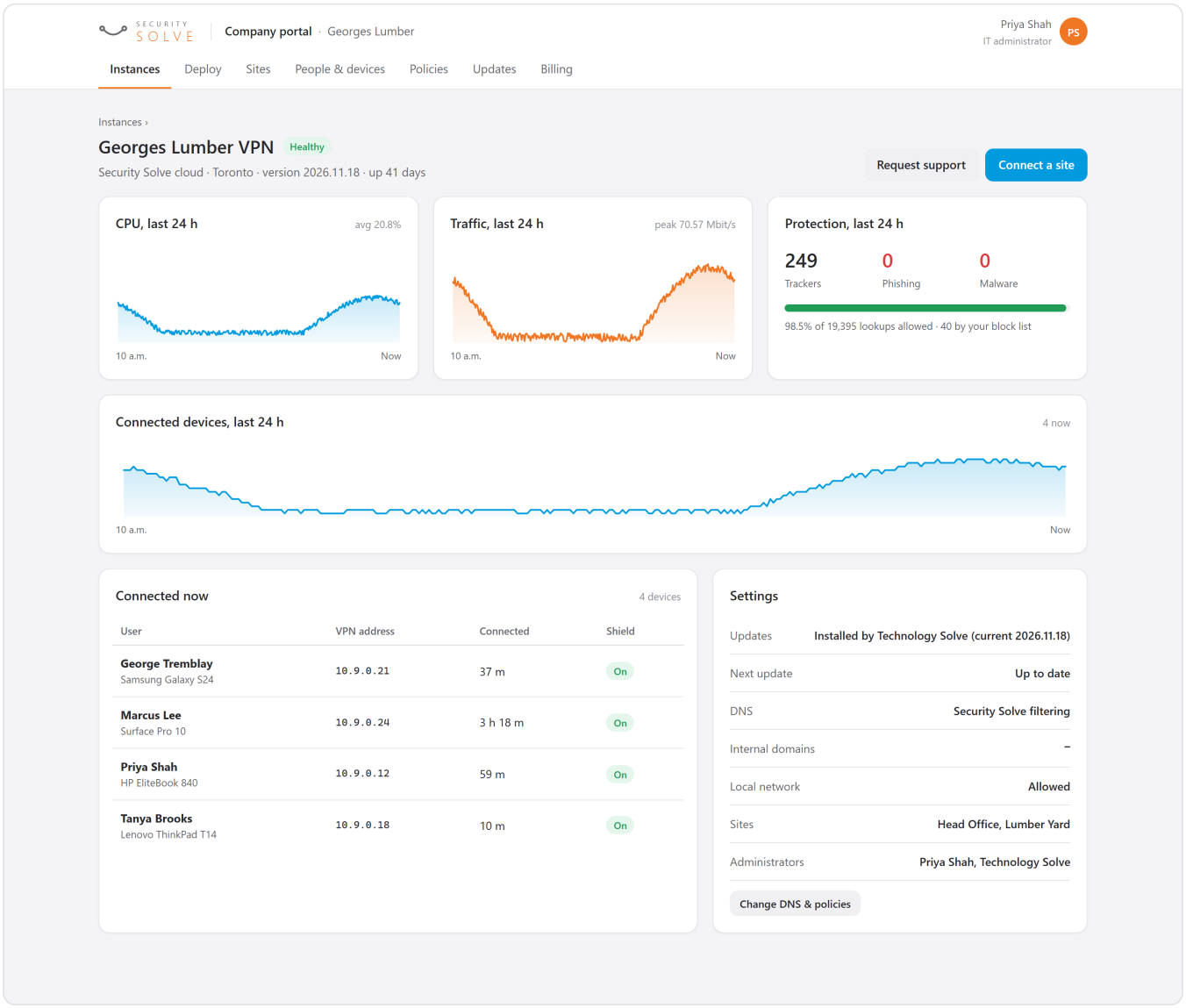
Instances: tiles, 24-hour and 14-day charts, every server and site gateway, and recent activity

- **Instances** lists your private VPN servers (in the Security Solve cloud) and the gateways at your offices, with their version, status, connected users, load and 30-day uptime. **Manage** opens the details.
- **Blocked lookups** shows, day by day, how many tracker, phishing and malware sites were stopped, plus any sites on your own block list. Hover over a bar for the exact numbers.
- **Activity** records changes and events: a gateway reconnecting, a person added, a request completed.
- **Download report** saves a spreadsheet (CSV) of these figures, handy for a monthly IT report.

INSTANCES

Inside a server

Select Manage on a server to see how hard it's working and who's using it right now.



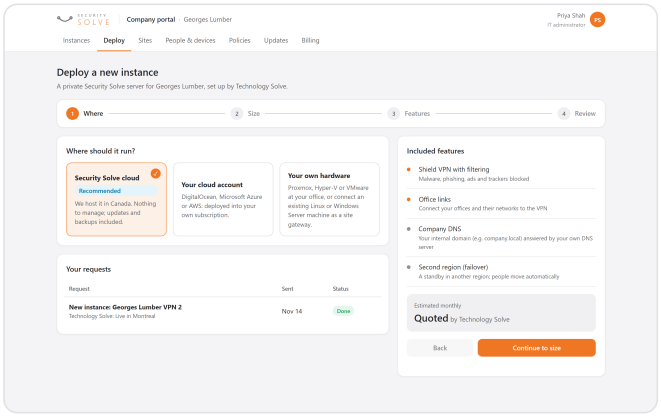
A private server: CPU, traffic, protection and connected devices over 24 hours, who's connected now, and its settings

- **Status** shows Healthy, or Update ready when Technology Solve has a new version to install. Updates are installed for you outside business hours.
- **Connected now** lists each person and device, their VPN address and how long they've been connected.
- **Connect a site** starts linking an office to this server. **Request support** sends a message straight to Technology Solve.

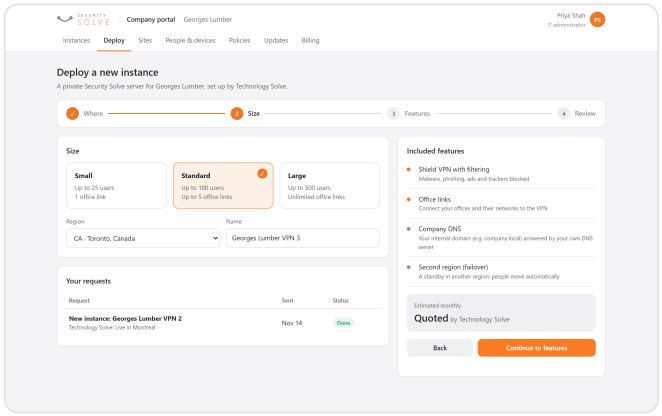
DEPLOY

Add a new server

Need a server in another region, a bigger one for more staff, or a Security Solve appliance in your own server room? Describe it in four short steps and Technology Solve takes it from there.



Step 1: where it should run



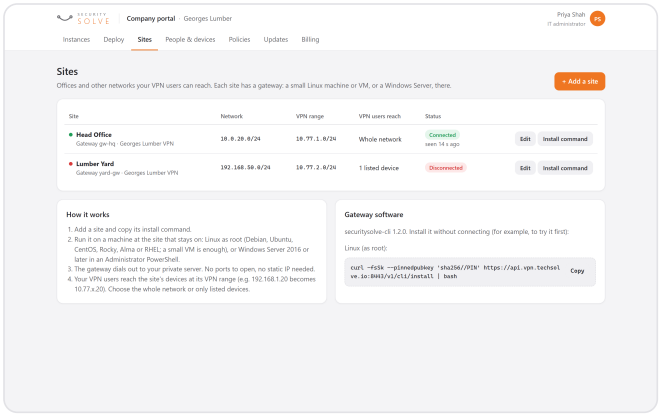
Step 2: size, region and name

Choose where it runs (the Security Solve cloud in Canada, your own cloud account, or your own hardware), the size, region and features, then send the request. Technology Solve confirms the details and price, usually within one business day, and the new server appears under Instances when it's live. Your requests and their status are listed on the same page.

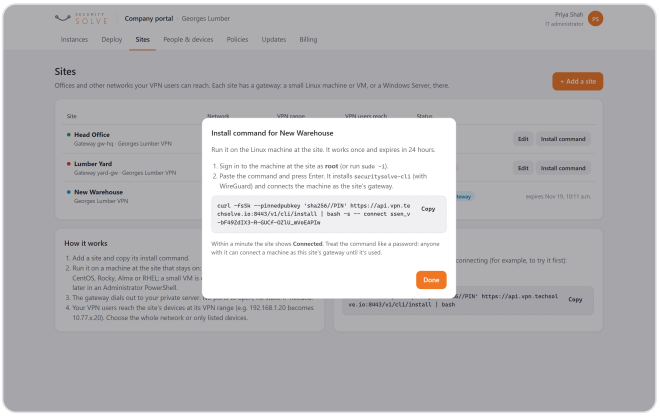
SITES

Connect your offices

A site is an office (or any network) your remote staff need to reach: file servers, remote desktops, printers. Each site has a small gateway: any Linux computer or virtual machine there.



Sites: each office, its VPN range and gateway status



The install command for a new site

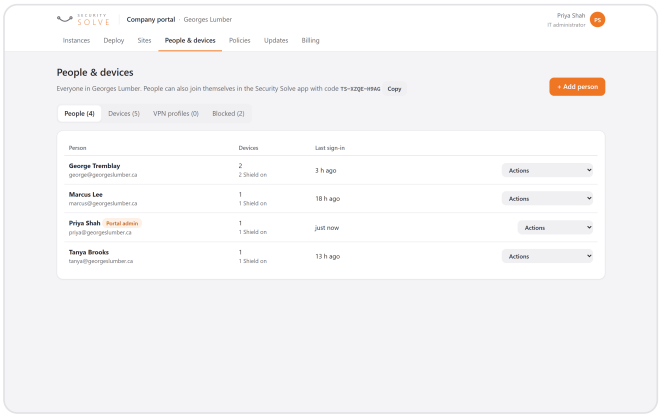
To add a site

- Select **+ Add a site**, pick your private server, and name the site (for example Head Office).
- Copy the one-line install command and run it on the gateway machine at the site (Debian, Ubuntu, CentOS, Rocky, Alma or RHEL). It works once and expires after 24 hours.
- The gateway connects out to your server, so there are no firewall ports to open and no static IP needed.
- Choose **Edit** to let VPN users reach the whole office network or only listed devices, such as a remote desktop server.

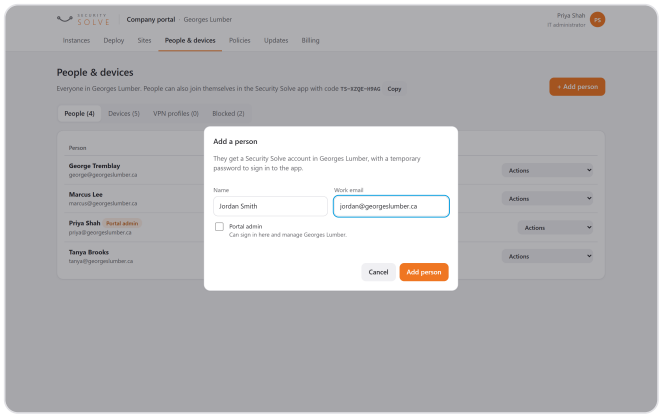
PEOPLE & DEVICES

Your team and their devices

Everyone in your organisation, their devices and VPN profiles, in one list.



People: portal admins, devices and last sign-in



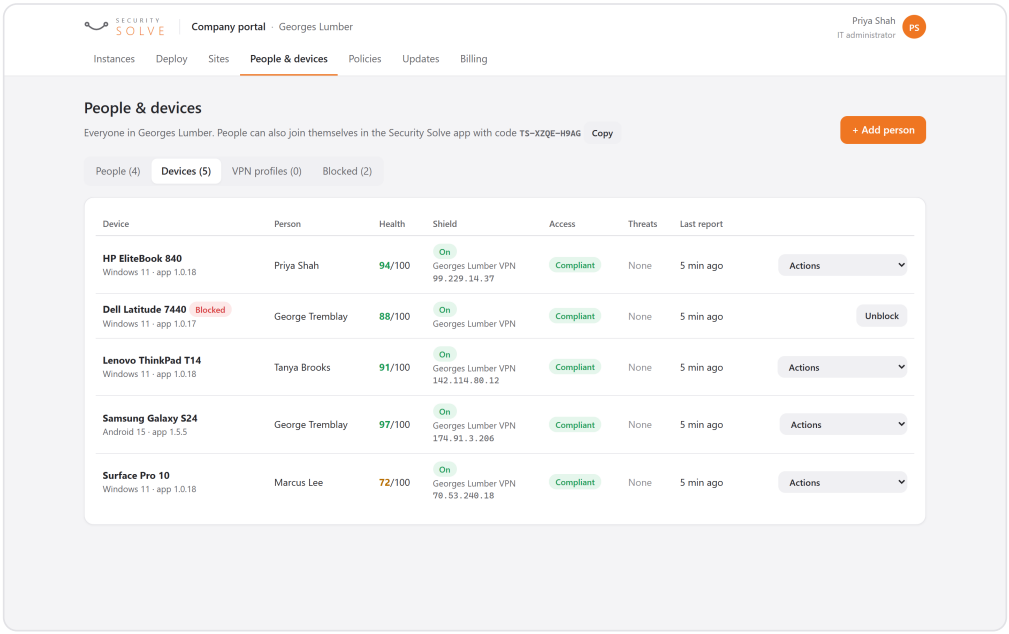
Adding a person

- **+ Add person** creates an account with a temporary password to pass on. Tick **Portal admin** to give them access to this portal too. Staff can also join on their own in the Security Solve app with your organisation code, shown at the top of the page.
- **Actions** on each person: reset password, sign out everywhere, give or remove portal access, disable the account, or remove them from the organisation.
- **VPN profiles** are for iPhones, iPads, Macs and PCs that use OpenVPN Connect instead of the Security Solve app: you get a download link, a username and a password to send to the person.

PEOPLE & DEVICES

Devices, and blocking one

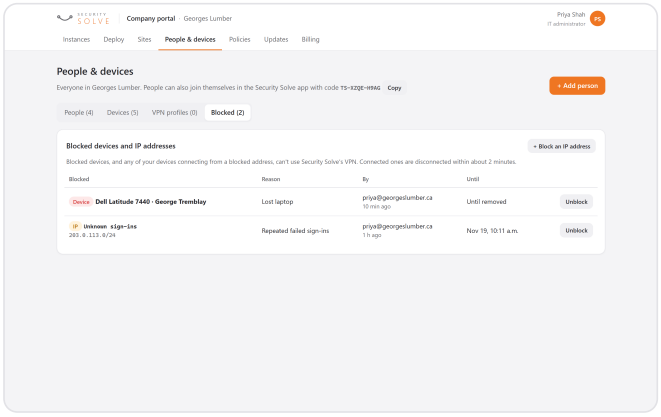
Every device reports its security health, whether Shield (the Security Solve VPN) is on, and any threats the app has found.



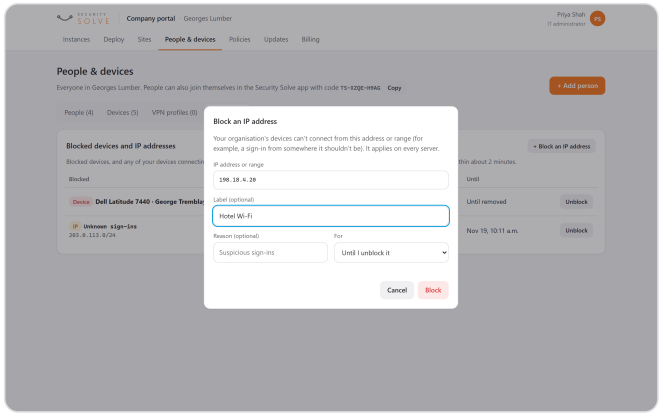
Devices: health score, Shield, compliance with access policies and threats

Block a lost device or a suspicious address

From **Actions** on a device, choose **Block this device**, or **Block its IP** to stop every one of your devices connecting from that address. You can also block any address or range from the **Blocked** tab, for an hour, a day, a week, a month or until you remove it. A connected device is disconnected within about two minutes. The person's account and other devices keep working, and **Unblock** restores access straight away.



The Blocked tab

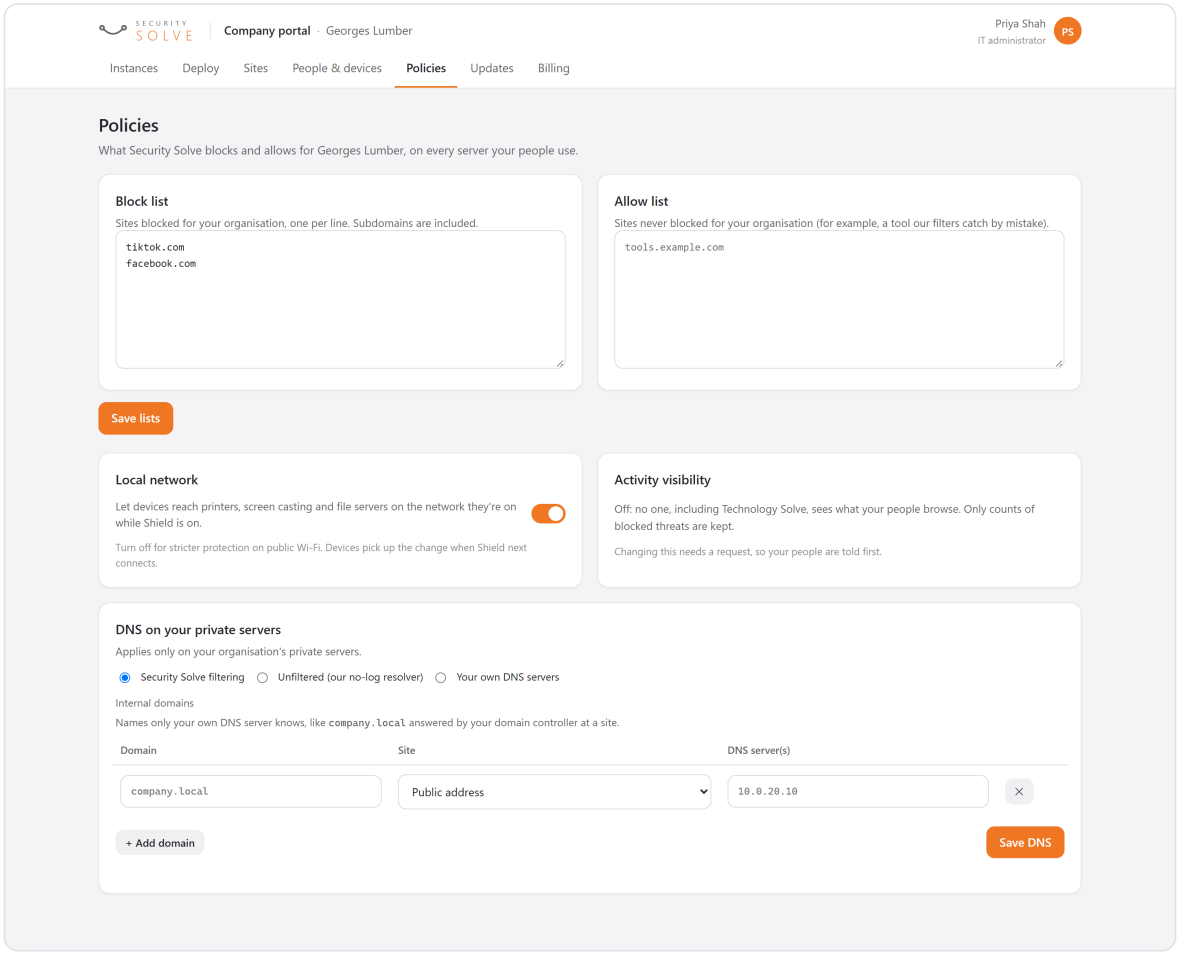


Blocking an IP address

POLICIES

Your rules

Security Solve already blocks malware, phishing, ads and trackers for everyone. Policies add your company's own rules on top, on every server your people use.



Policies: block and allow lists, local network access and DNS for your private servers

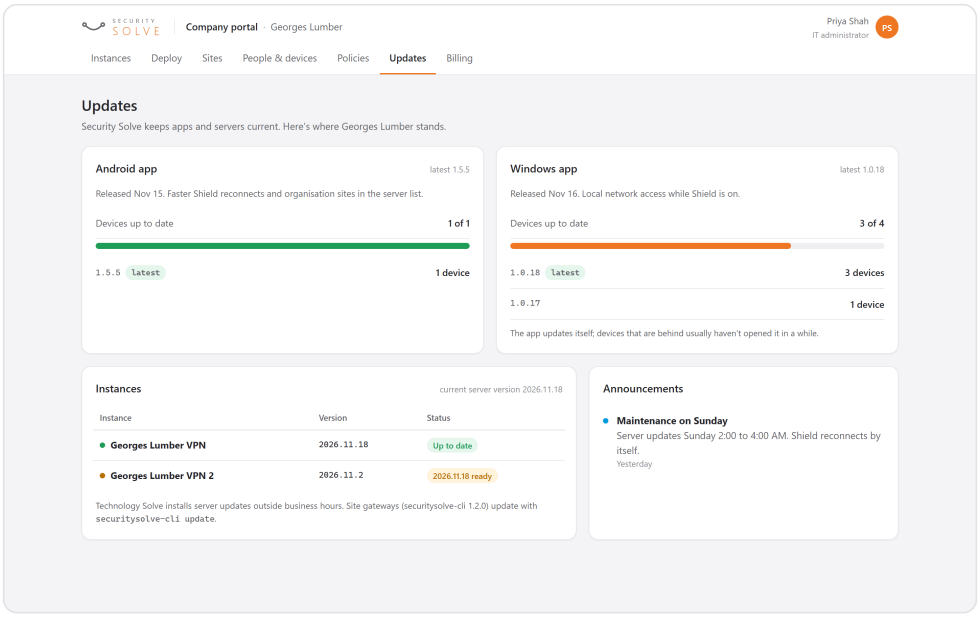
- **Block list:** sites your company doesn't allow (for example social media on work devices). Subdomains are included.
- **Allow list:** sites that should never be blocked, such as a business tool caught by mistake.
- **Local network:** lets devices reach printers, screen casting and file servers on whatever network they're on. Turn it off for stricter protection on public Wi-Fi.
- **DNS on your private servers:** keep Security Solve filtering, use our unfiltered no-log resolver, or your own DNS servers, and add internal domains such as company.local answered by your domain controller.

Changes apply within a minute.

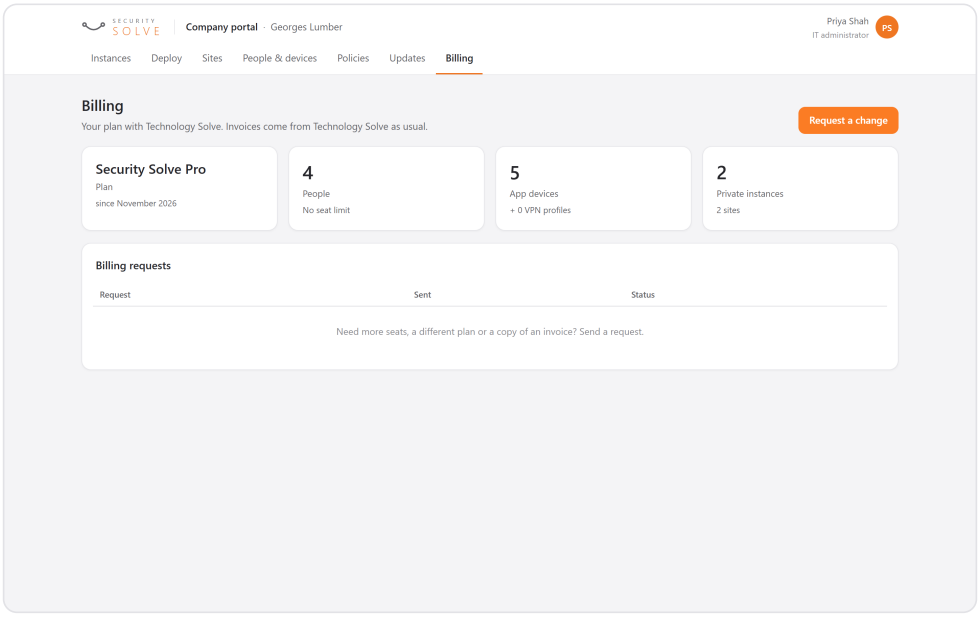
UPDATES & BILLING

Staying current, and your plan

Security Solve keeps its apps and servers up to date. These pages show where you stand.



Updates: app versions across your devices, server versions and announcements



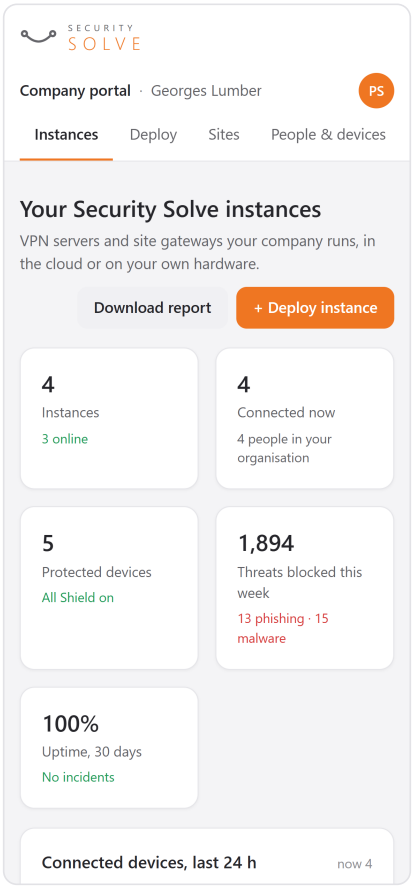
Billing: your plan, seats and usage, and billing requests

The apps update themselves; a device that's behind usually hasn't opened the app in a while. Need more seats, a different plan or a copy of an invoice? Choose **Request a change**.

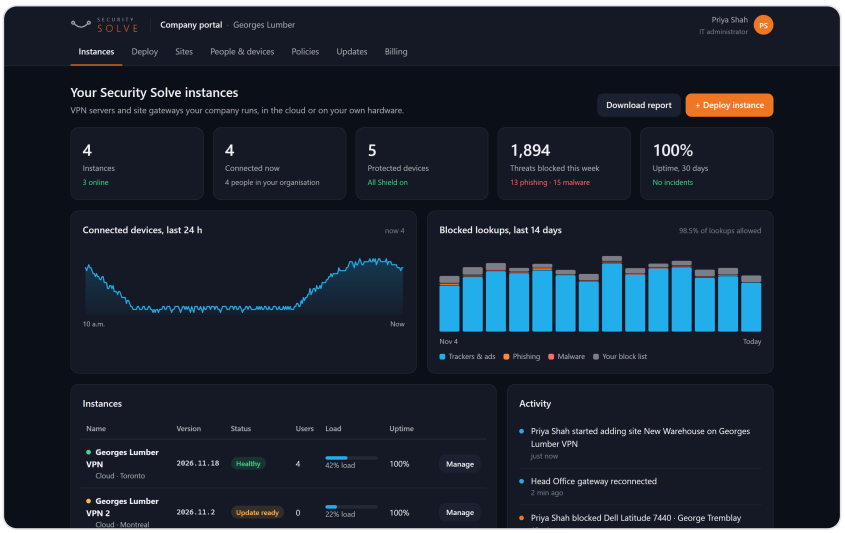
ANYWHERE

On your phone, light or dark

The portal adapts to small screens and follows your device's light or dark setting. You can also switch it from the account menu.



On a phone



Dark mode

Questions and good to know

Who can sign in? Your organisation's IT administrators. Technology Solve sets up the first login; you can give other people portal access from People & devices.

Can you see what my staff browse? No. The portal shows counts of blocked threats and connections, never the sites anyone visited.

What if something isn't working? Choose **Request support** on any server page, or contact Technology Solve as usual. Requests and their status appear in the portal.

Is the portal secure? It runs over HTTPS, your session is protected from other websites, and repeated wrong passwords are locked out for 15 minutes.