



Patch Management

Reviewer's Guide 2021



Table of contents

Introduction.....	3
What is Avast Business Patch Management?.....	4
How to get started	5
Configuring Patch Management	7
Patches page	10
Alerts.....	10
Reports	12
Resources	13
Avast Privacy Policy	15
Contact	17

Introduction

57% of data breaches are attributed to poor patch management¹. Prompt patching is vital for cybersecurity. When a new patch is released, attackers use software that looks at the underlying vulnerability in the application being patched. This is something that hackers perform quickly, allowing them to release malware to exploit the vulnerability within hours of a patch release. Their goal is to intrude systems as long as the patch hasn't been applied yet, and they count on the fact that often, vulnerabilities remain unpatched for weeks, months, or even years after they have become known. Therefore, applying security patches is vital to prevent hackers and cybercriminals from exploiting vulnerabilities that could halt operations.

If a vulnerability is successfully exploited, businesses risk:

- Ransomware
- Having their data lost or stolen
- Significant time lost while restoring data or reinstalling operating systems and applications
- Incompliance with industry regulations and business requirements
- Lack of data integrity
- Losing credibility and trust with customers and prospects

With security breaches being the new normal, the rush is on to implement effective security practices and ensure proper patch compliance. And with the rising number of vulnerabilities in third-party applications, this includes solutions that install critical security updates for more than just Microsoft products.

Whether your endpoints are behind the firewall, remote, physical, or virtual, patching your critical operating systems and apps in a timely, efficient, and cost-effective manner remains challenging. Patching can be extremely time-consuming. Each patch needs to be



reviewed, prioritized, and then tested to make sure it won't break existing systems. When there are dozens of patches to evaluate, this process can easily take days, if not longer, which pulls resource-strapped IT professionals away from other critical initiatives.

Employees also present a risk to organizations. They desire convenience and rarely consider security during their day-to-day operations - they simply want to get their work done as easily as possible without interruption or distraction. Patching software tends to be an annoyance for end users (employees) and all too often, recommended patches go ignored. Users typically ignore software updates because they lack the technical knowledge, it's time-consuming, and/or because they worry about potential issues with updating applications.

A solid patch management process is an essential requirement for any size business. Unfortunately, many organizations do not have the expertise, software, or necessary processes/systems in place to effectively secure their infrastructure. Manually checking for and applying patches is an almost-impossible task.

Ignoring software updates isn't an option. Having a strong endpoint security foundation is crucial to protecting businesses from cyberattacks – and antivirus alone isn't enough to combat these threats. If patches are not applied in a timely manner, networks can be severely compromised.



Avast Business Patch Management

What is it?

Avast Business Patch Management is a security service that simplifies and automates the patching process, saving companies both time and money. This service automatically scans devices, identifies vulnerabilities, and deploys critical patches to all endpoints to prevent breaches, ensure regulatory compliance, and stay in control. With this, IT admins no longer have to review, prioritize, and test hundreds of patches to ensure they don't break existing systems before being deployed.

Avast Business Patch Management is available in the Business Hub, an integrated, cloud-based security platform that gives IT admins access to granular, accurate control over the entire patching process, including patch discovery, distribution of software updates, and reporting - all from a single pane of glass.

Avast's team of patch content engineers carefully inspects each patch before it gets released to users, ensuring proper compliance. The Avast team applies its over 30 years of industry experience and innovation to the test, empowering businesses to quickly patch and secure third-party apps.

How to get started

How to get started

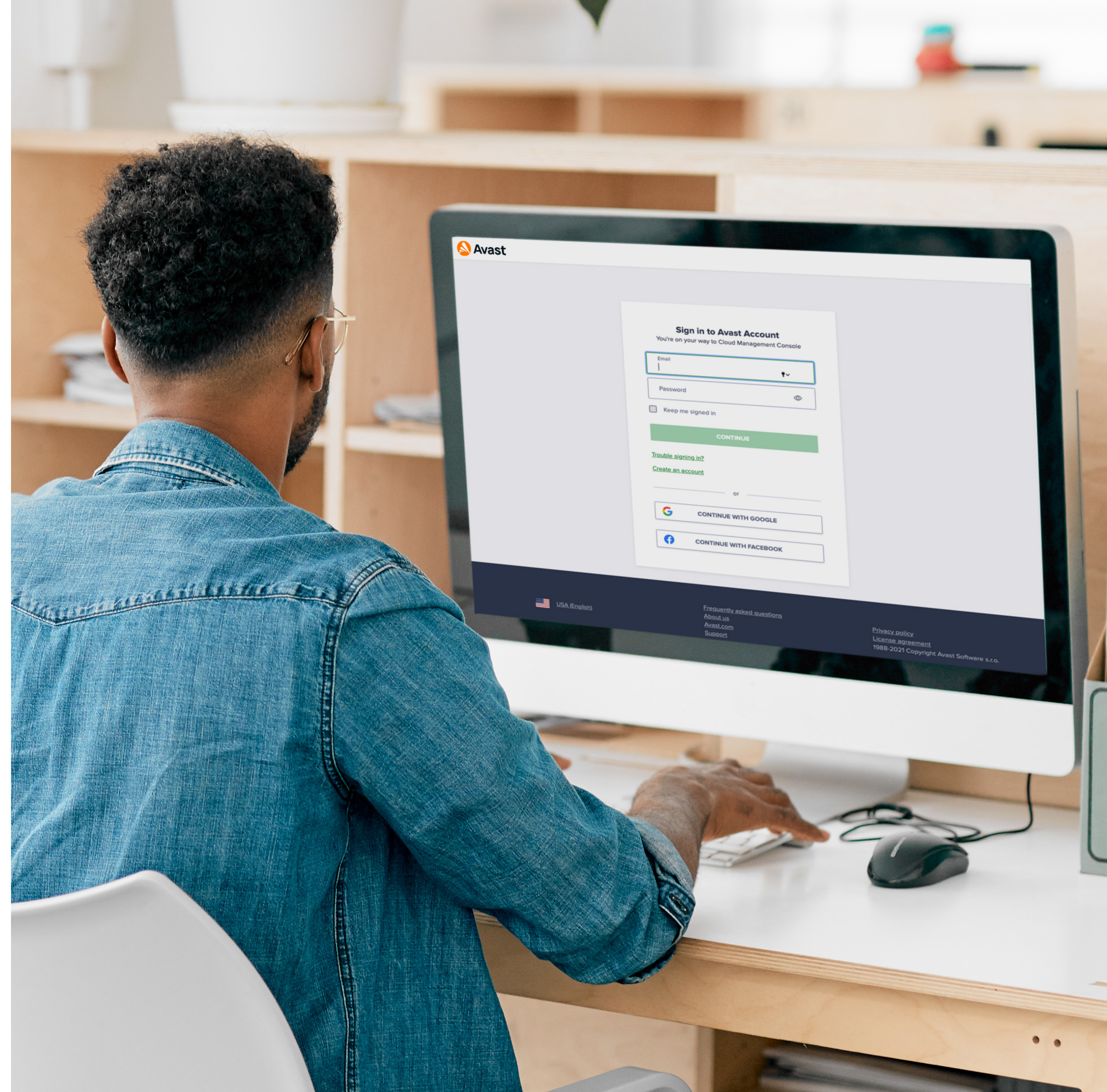
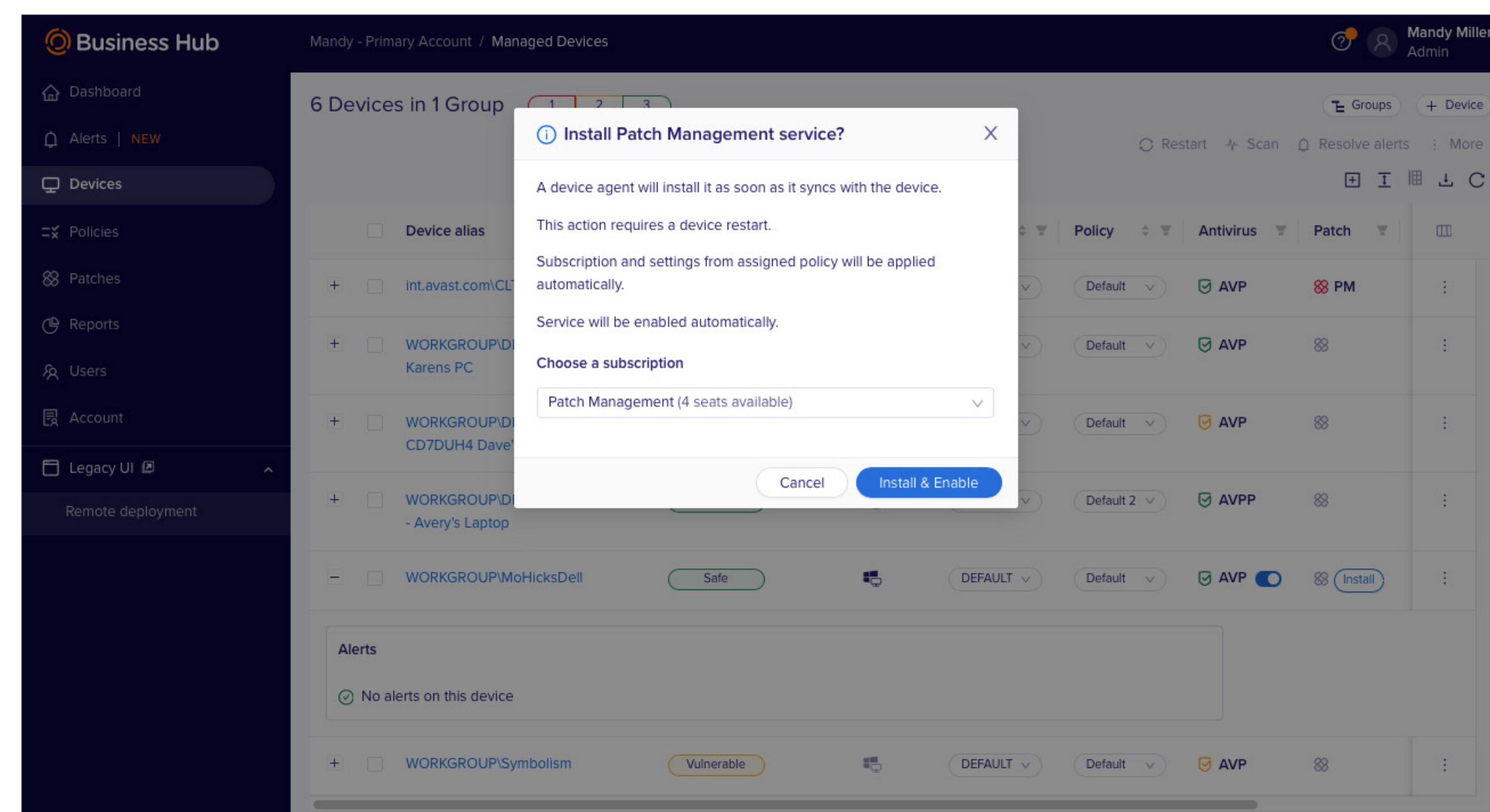
Create your Avast Business Hub Account

The Avast Business Hub is an integrated, cloud-based security platform that allows IT admins to easily manage all Avast Business security solutions deployed in their networks. It provides real-time visibility of threats, comprehensive reporting, and management capabilities, all from one single interface.

Visit <https://businesshub.avast.com/> to register and create your account. Once your console is created, click on "Account" on the menu to access the company profile and subscription page. On this page, you will enter the license number to activate the Patch Management service.

How to install the patch service on a device(s)

1. Go to the devices page
2. Click "install" in the patch column to enable and install the service



Configuring Patch Management

Configuring Patch Management



After the service is activated, go to the “Policies” page to configure your settings. In the policies section, you can configure the settings for scheduled patch scans, how and when missing patches are deployed, customize patch exclusions, and configure restart options.

In the Service Settings, you will find a Patch Management tab. In this section, you will be able to configure patch scans, deployments, and other settings, such as clear local patch cache.

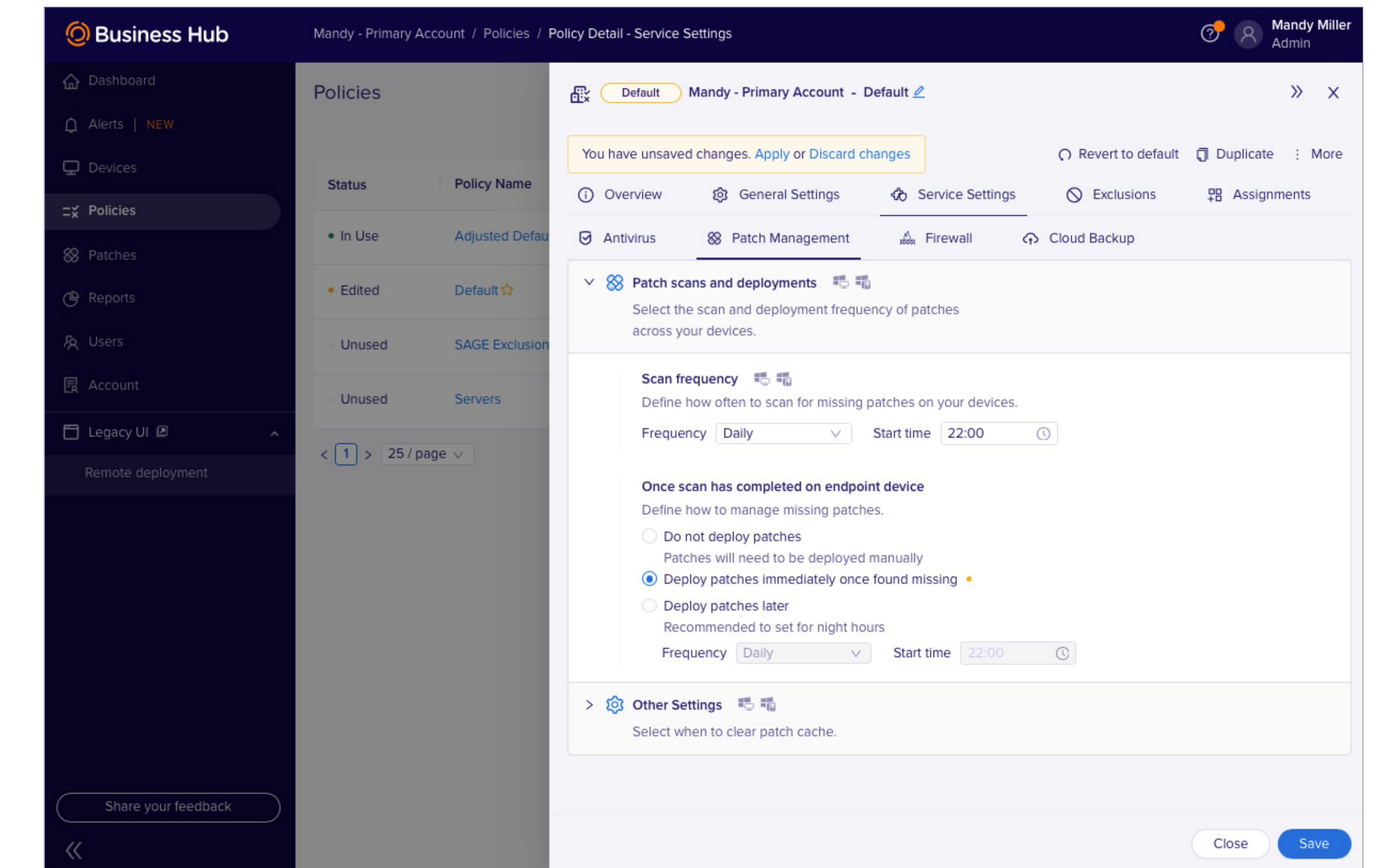
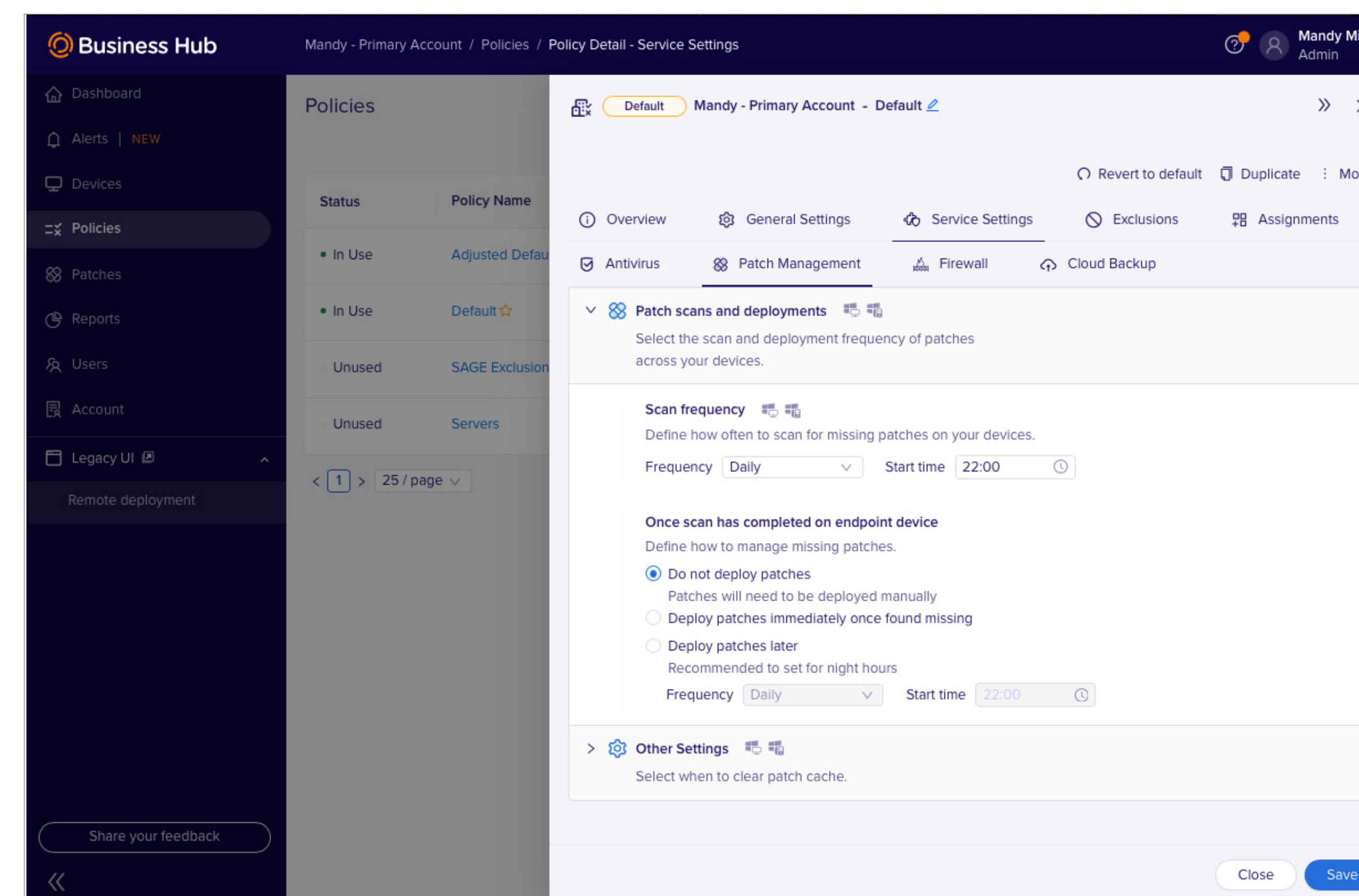


Scan Frequency

The Patch Scan checks all devices tied to the particular policy for missing software application updates (patches). After a scan is completed, the results for missing patches are displayed in the Patches page.

For scanning, you can select from the following options:

- **Daily:** will run a scan every day at the selected start time.
- **Weekly:** will run a scan every week on the selected day and start time of the week.
- **Monthly:** will run a scan every month on a specific day of the month and start time, which you select.
- For Monthly scans, we do not recommend selecting the 29th, 30th, or 31st day of the month for the scan, as these dates do not occur every single month.



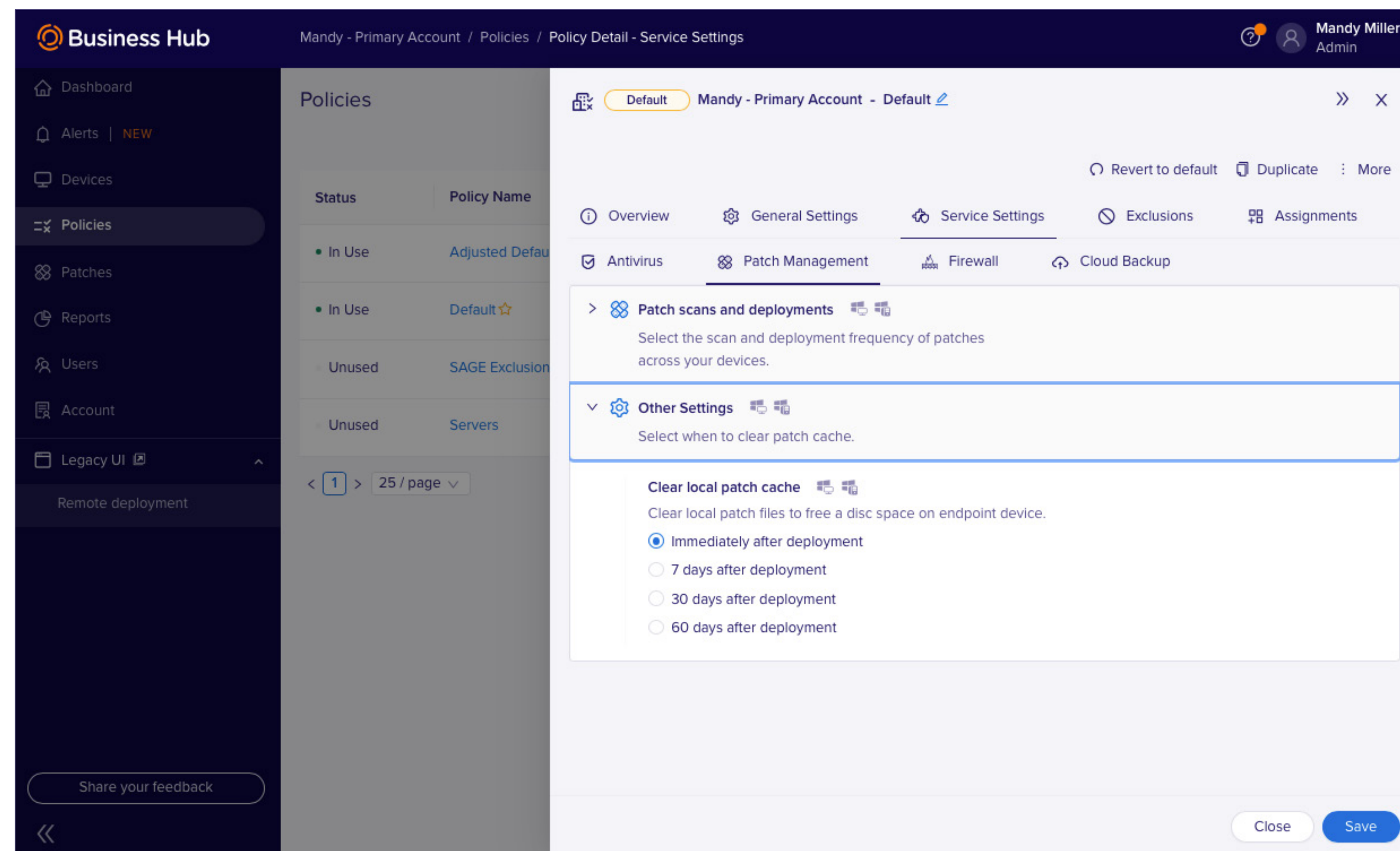
Patch Deployment

Enabling automatic patch deployment in the policy will deploy missing patches on an automatic, recurring basis. If you would like to perform a one-time manual patch, you can do so from the Patches tab for one or multiple devices or from the devices page.

You can choose from the following options for automatic deployment once a patch scan has completed on the device and identified missing patches:

- **Do not deploy patches:** Patches will need to be deployed manually.
- **Deploy patches immediately once found missing**
- **Deploy patches later:** Recommended to set for night hours. You can schedule patches to be deployed daily at a chosen time, weekly on a chosen day of the week and time of day, or monthly on a specific day of the month and time of day.

Configuring Patch Management



Clear local patch cache

In this section, you can select when to clear patch files to free disc space on your devices. You have the following options:

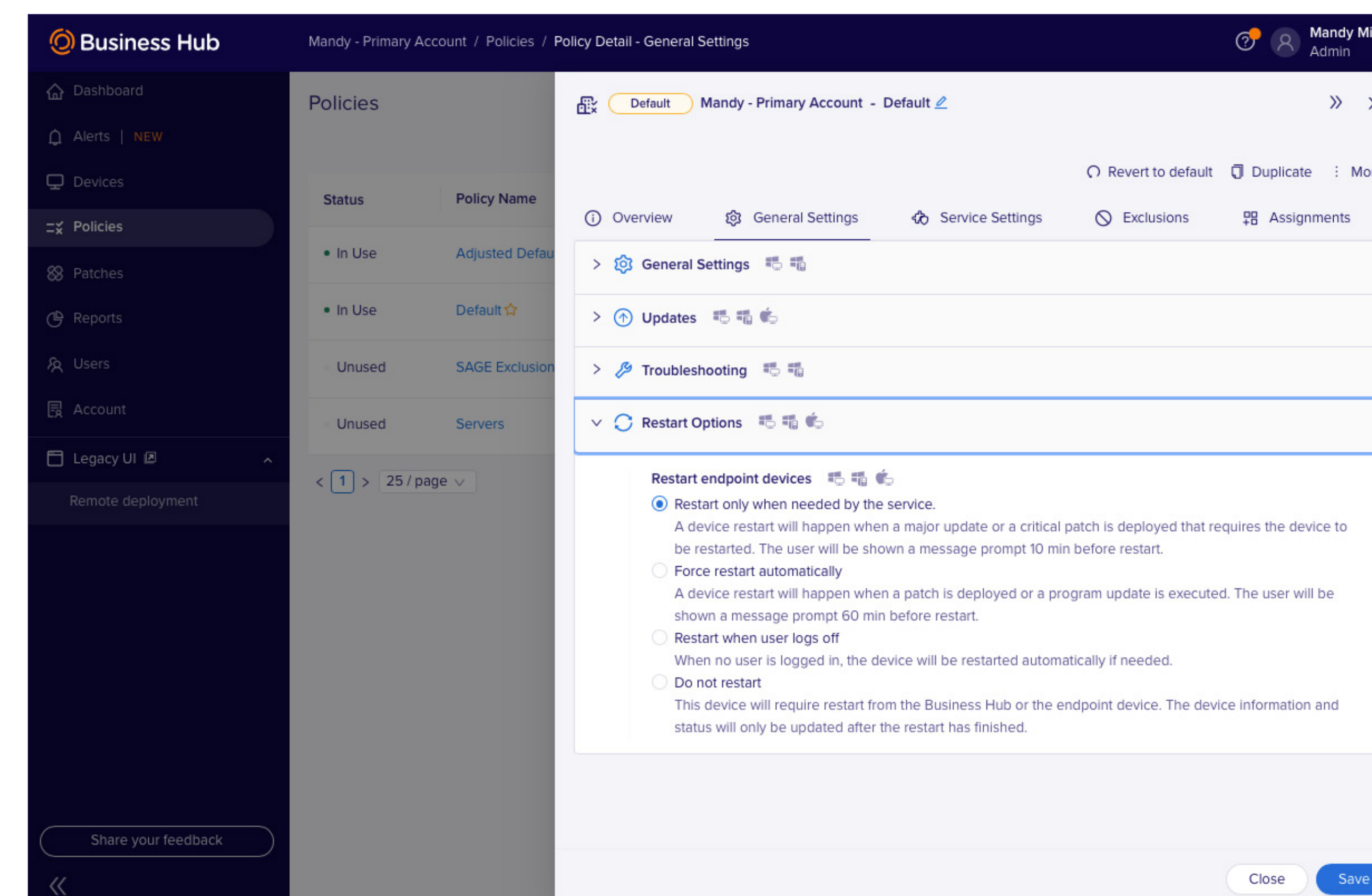
- Immediately after deployment
- 7 days after deployment
- 30 days after deployment
- 60 days after deployment

Device restart

Often, patches require devices to be restarted after installation. When you install patches using the policy settings, you can tell devices to restart and control when that restart begins. If patches are installed but those patches don't require a restart, the devices won't be restarted.

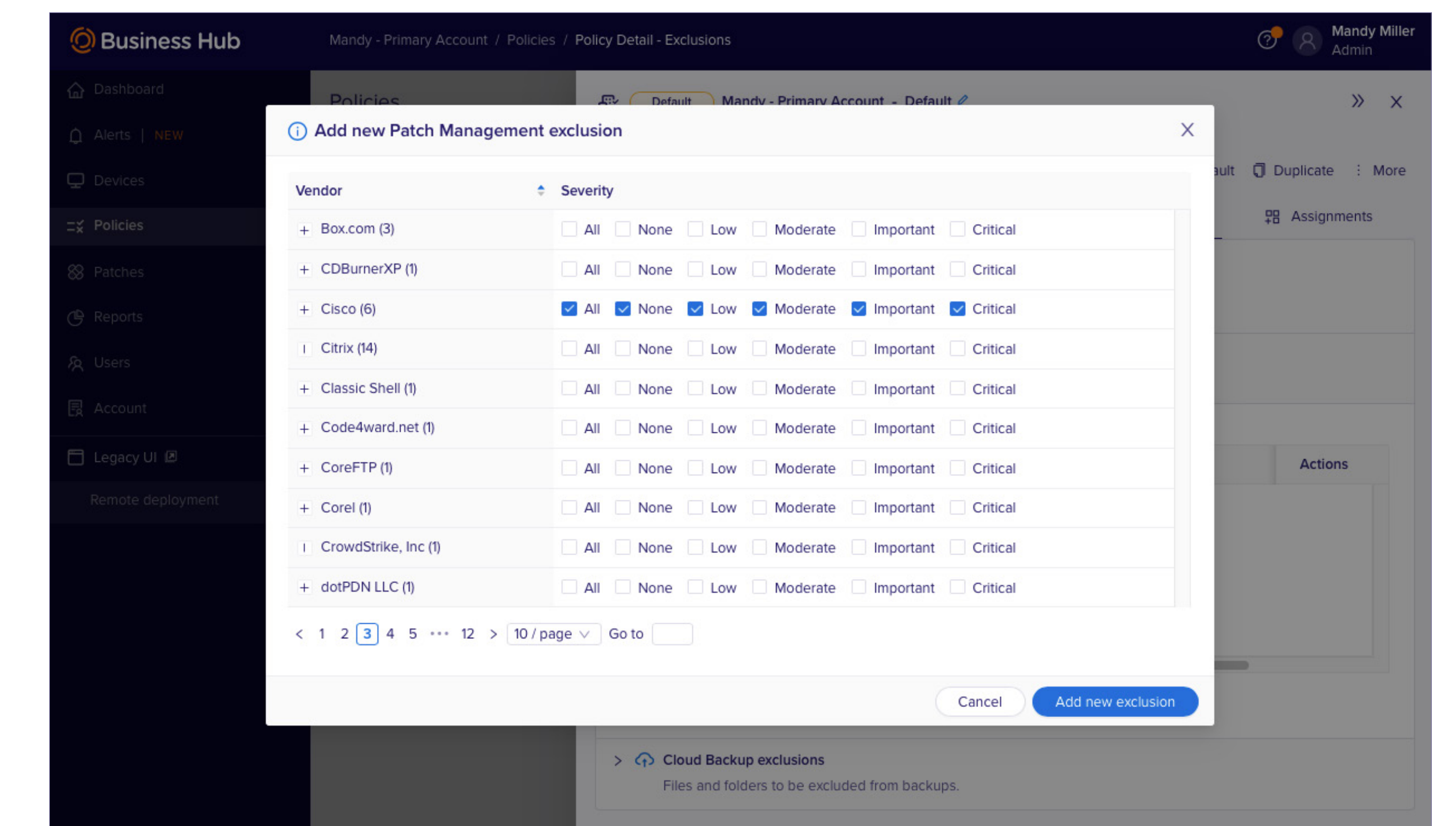
In the General Settings, go to the Restart Options section and select one of the following options for endpoint device restart:

- **Restart only when needed by the service:** A device restart will happen when a major update or a critical patch is deployed that requires the device to be restarted. The user will be shown a message prompt ten minutes before restart.
- **Force restart automatically:** The device will be set to be restarted automatically, and a warning message will be displayed on the user's machine an hour prior to device restart. However, the user will be



able to either postpone the restart up to three times or cancel the restart altogether, depending on which box is selected.

- **Do not restart:** You will have to restart manually either from the Console or on the physical endpoint device.
- **Restart when user logs off:** Display a message that restart is needed to the endpoint user. If no one is logged in, the device will restart automatically.
- **Do not restart:** The device will require a restart from the Business Hub or the endpoint device. The device information and status will only be updated after the restart has finished.



Exclusions

In the Exclusions settings tab, you will find a section for Patch Management. Here, IT admins can add exclusions so that patches will not be deployed to devices.



Patches page and Alerts

Patches Page

At the top of the Patches page, IT admins will find a quick summary of the status of the patches along with the number of affected devices.

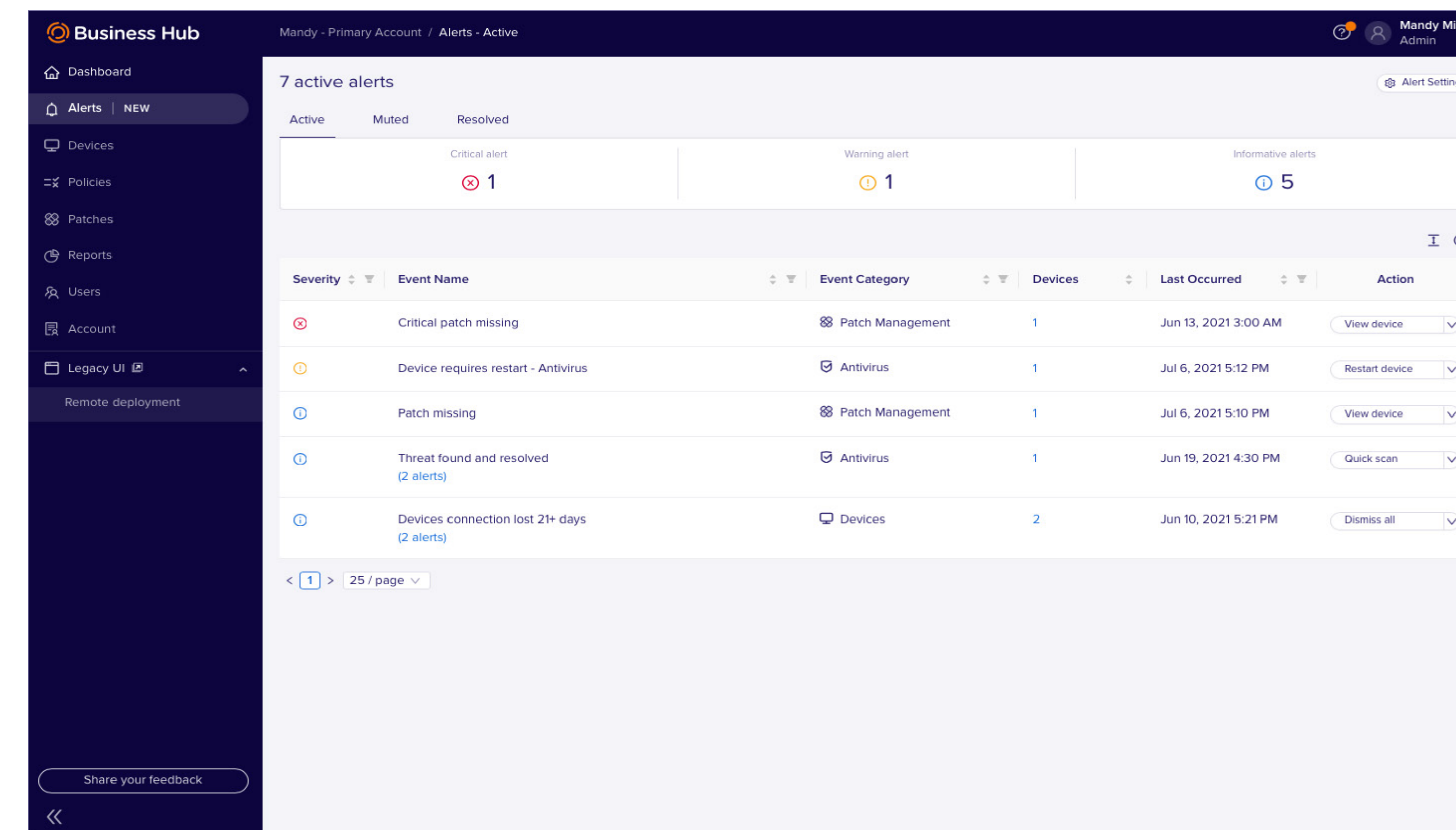
- Missing patches
- Scheduled patches
- Downloading patches
- Installing patches
- Devices pending restart
- Failed to install

The Patches page is designed to provide a comprehensive view of all OS and third-party patches. The dashboard will display the patch name, type of patch, severity, CVSS score, status, and action needed so that IT admins can streamline their work, and easily prioritize and deploy patches from a central dashboard.

67 OS patches	
OS patches	Third-party patches
Missing patches 4 on 2 devices	Scheduled patches 4 on 2 devices
Downloading patches 0 on 0 devices	Installing patches 0 on 0 devices
Pending restart 1 on 1 device	Failed to install 0 on 0 devices

Patch name	Type	Severity	CVSS score	Released	Devices	Status	Action
Service stack update for Windows 10, version 2004 and 20H2; December 8, 2020 (KB4593175)	Security	Critical	-	7 months ago	2	Missing	Install
KB4589212: Intel microcode updates for Windows 10, version 2004 and 20H2, and Windows Server, version 2004 and 20H2	Non-security	None	5.6	5 months ago	4	Missing	Install
June 11, 2021 - KB5004476 (OS Builds 19041.1055, 19042.1055, and 19043.1055) Out-of-band	Non-security	None	-	13 days ago	5	Missing	Install
Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (955218)	Security	Critical	4.3	13 years ago	1	Scheduled	Install
November 19, 2020-KB4586819 (OS Builds 18362.1237 and 18363.1237) Preview	Non-security	None	-	7 months ago	2	Scheduled	Install

Alerts



Severity	Event Name	Event Category	Devices	Last Occurred	Action
Critical alert	Critical patch missing	Patch Management	1	Jun 13, 2021 3:00 AM	View device
Warning alert	Device requires restart - Antivirus	Antivirus	1	Jul 6, 2021 5:12 PM	Restart device
Informational alert	Patch missing	Patch Management	1	Jul 6, 2021 5:10 PM	View device
Informational alert	Threat found and resolved (2 alerts)	Antivirus	1	Jun 19, 2021 4:30 PM	Quick scan
Informational alert	Devices connection lost 21+ days (2 alerts)	Devices	2	Jun 10, 2021 5:21 PM	Dismiss all

On the alerts page, you will find alerts for different categories, including Patch Management. The alert types include critical patches missing, patches missing, and device restart needed.

For alerts that have related tasks that can be created to resolve the issue, a link will appear beside the alert for the appropriate action. You can take immediate action from this page and initiate a scan, restart a device, etc. All alerts will display the number of affected devices, and a link you can click to review more alert and threat details.





Patch Reporting

In the reports section, you will find reports for each service, including Patch Management. The Patch report will provide IT admins with a consolidated view of the status of all patches and devices during a predetermined period of time. You can view a report on demand or create a schedule to automatically receive reports via email. The report will include:

- Patch name
- Severity
- Vendor name
- Patch status
- Deployment method (reason)
- Date and time
- Number of deployed patches
- Number of missing patches
- Number of failed patches
- Number of scheduled patches
- Number of ignored patches

Patches	Deployed patches	Missing patches	Failed patches	Scheduled patches	Ignored patches
6	0	6	0	0	0

Device alias / name	Patch name / Bulletin ID	Severity	Vendor	Application	Status	Reason	Date and time
int.avast.com\CLTA-000003 CLTA-000003	Service stack update for Windows 10, version 2004 and 20H2: December 8, 2020 (KB4593175) MS20-12-SSU-4593175	Critical	Microsoft	Windows	Missing	-	Jul 6, 2021 5:13 PM
int.avast.com\CLTA-000003 CLTA-000003	Google Chrome 91.0.4472.124 CHROME:210624	None	Google	Chrome	Missing	-	Jul 6, 2021 5:13 PM
int.avast.com\CLTA-000003 CLTA-000003	KB4589212: Intel microcode updates for Windows 10, version 2004 and 20H2, and Windows Server, version 2004 and 20H2 MSNS21-01-4589212	None	Microsoft	Windows	Missing	-	Jul 6, 2021 5:13 PM
int.avast.com\CLTA-000003 CLTA-000003	VLC Media Player 3.0.16 VLC:210629	None	VideoLAN	VLC	Missing	-	Jul 6, 2021 5:13 PM
int.avast.com\CLTA-000003 CLTA-000003	June 29, 2021 - KB5004760 (OS Builds 19041.1082, 19042.1082, and 19043.1082) Out-of-band MSNS21-06-W10-5004760	None	Microsoft	Windows	Missing	-	Jul 6, 2021 5:13 PM
int.avast.com\CLTA-000003 CLTA-000003	June 21, 2021 - KB5003690 (OS Builds 19041.1081, 19042.1081, and 19043.1081) Preview MSNS21-06-W10-5003690	None	Microsoft	Windows	Missing	-	Jul 6, 2021 5:13 PM

Resources



Resources

Avast Business Patch Management

[Product URL](#)

[Screenshots](#)

[Box Shot](#)

[Customer support options](#)

1 year/1 seat \$14.99

1 year/1 seat \$144.90

30-day free trial

*Up-to-date pricing can be found on the Avast website.



Privacy Policy



Privacy Policy

As one of the world's most trusted antivirus software companies, Avast defends businesses against threats in cyberspace. To do so, Avast may have to collect personal data to provide its users with the best weapons and the most up-to-date security. Avast does not take this trust for granted. Avast has developed a Privacy Policy that covers how Avast collects, uses, discloses, transfers, and stores users' personal data. Avast's full privacy policy, which includes why and how Avast processes data, and how Avast discloses and protects its users' personal data, can be found [here](#).

Contact

If you are a member of the press, please contact PR@avast.com for any questions regarding Avast Business or any of its products.

Media materials can be found at <https://press.avast.com>. If you are a customer and have a question about Avast Business or any of its products, please contact the Avast Support Team by visiting <https://www.avast.com/en-us/business/support>.

¹Ponemon Institute, State of Endpoint Security Risk, 2018

