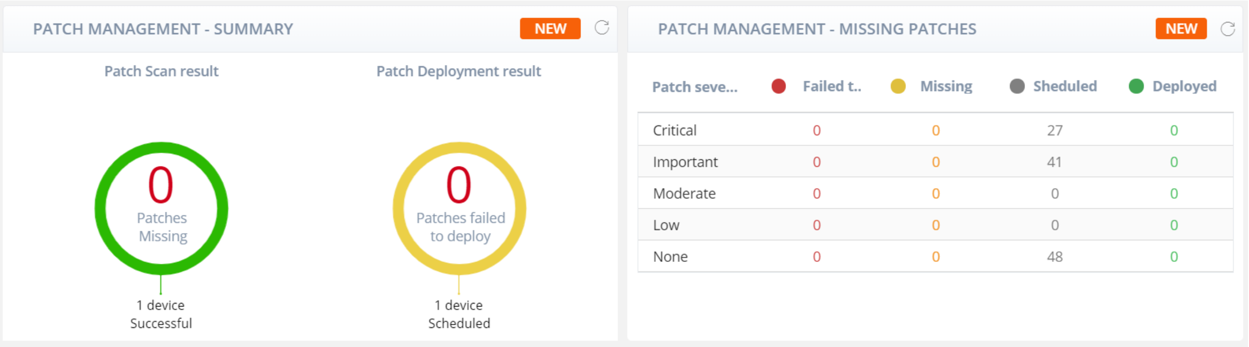
Avast Business Patch Management – Quick Start Guide

Patch management plays a critical role in cybersecurity. Patches are released to fix vulnerabilities or security gaps in Windows operating systems and 3rd party application software. If patches are not applied in a timely manner, networks can be severely compromised.

The new Avast Business Patch Management service solves these issues by making it easy to centrally set up, acquire, test, approve, and install system updates and patches with default patch scans and deployment settings.

Here is a quick start guide to what's new in the Avast Business Cloud Management Console.

Patch Dashboard Widgets



PATCH MANAGEMENT - SUMMARY NEW

Patch Scan result: 0 Patches Missing — 1 device Successful

Patch Deployment result: 0 Patches failed to deploy — 1 device Scheduled

PATCH MANAGEMENT - MISSING PATCHES NEW

Patch seve...	● Failed t..	● Missing	● Sheduled	● Deployed
Critical	0	0	27	0
Important	0	0	41	0
Moderate	0	0	0	0
Low	0	0	0	0
None	0	0	48	0

Our Patch Management - Summary widget provides up-to-date, at a glance information on:

- Missing patches
- Successfully installed patches
- Patches that failed to deploy/install.

The data in the widget is interactive, so if you would like to find out more about Patches that failed to deploy, you can click on the number in Red which will take you to the Patches Page and filter those devices that are missing patches or have patches that failed to deploy.

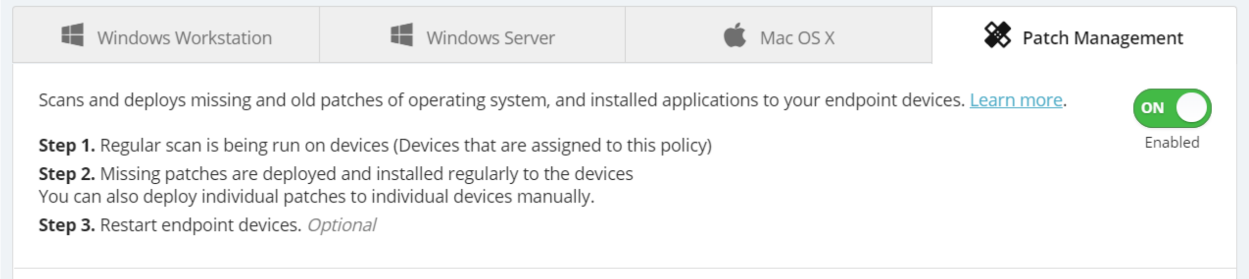
Our Patch Management - Missing Patches widget provides you with a high level overview of failed to deploy, missing, scheduled and deployed status for missing patches

This is filtered by severity with critical patches being the most important.

Device Settings - Patch Management

Under Device Settings > Select Policy (default for example) and you will see a tab called “Patch Management”.

This is a new tab which houses your Patch Management settings. The settings are split into 4 steps. First, you can deactivate Patch Management. If the service is deactivated, no scanning of devices for missing patches will occur and no deployment of missing patches will occur.



Scans and deploys missing and old patches of operating system, and installed applications to your endpoint devices. Learn more.

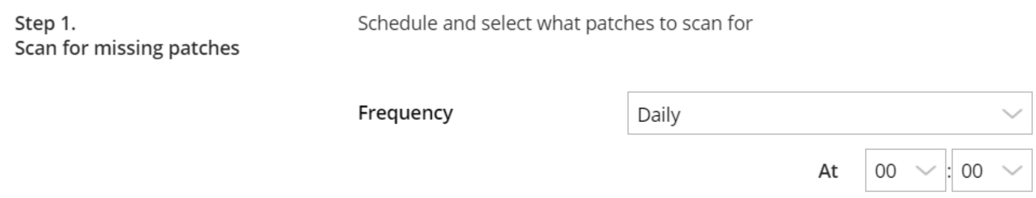
ON
Enabled

Step 1. Regular scan is being run on devices (Devices that are assigned to this policy)

Step 2. Missing patches are deployed and installed regularly to the devices
You can also deploy individual patches to individual devices manually.

Step 3. Restart endpoint devices. *Optional*

Step 1 - Scan for missing patches



Step 1.
Scan for missing patches

Schedule and select what patches to scan for

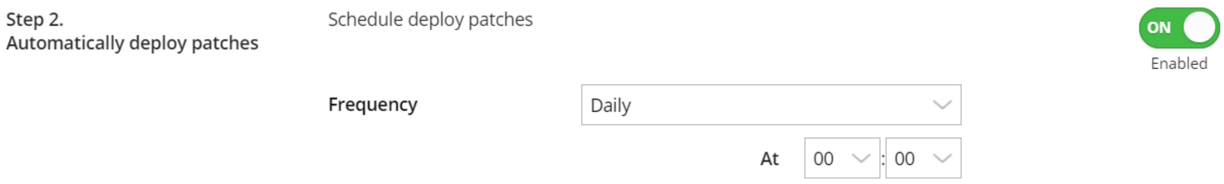
Frequency Daily

At 00 : 00

The Patch Scan will scan all devices for missing software application updates (patches) to all devices that are tied to this device setting policy. After the scan has been completed, the results for missing patches are displayed in the ‘Patches’ page and under the ‘Patch Results’ tab under a device (Devices page).

Here you can select the frequency of the patch scan from Daily, Weekly and Monthly and at a time that you would like the scan to take place.

Step 2 - Automatically deploy patches



Step 2.
Automatically deploy patches

Schedule deploy patches

ON
Enabled

Frequency Daily

At 00 : 00

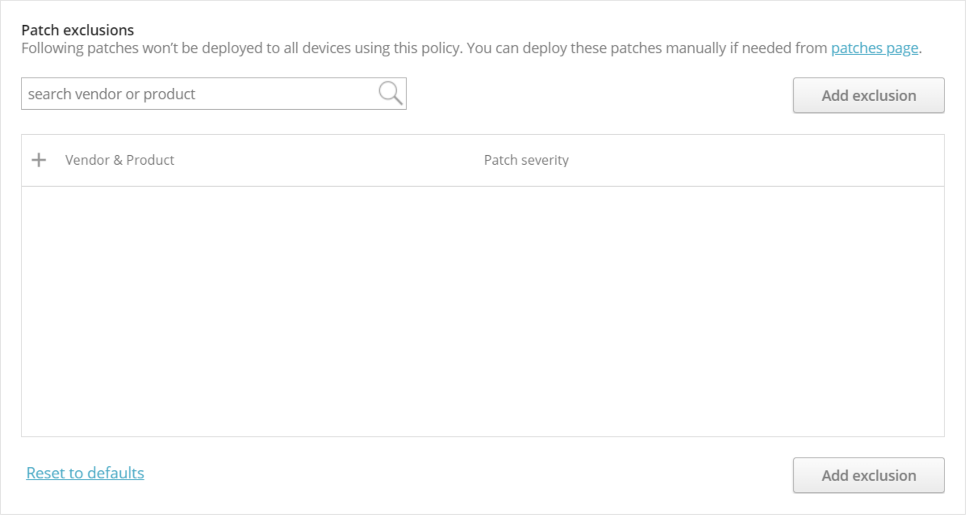
Automatically deploy patches will deploy missing software application updates (patches) to all devices that are tied to this device setting policy.

Here you can select the frequency of the patch deployment from Daily, Weekly and Monthly and at a time that you would like the deployment to take place.

By default, **all Vendors, Software Applications and Severities** will be patched unless you exclude them.

Patch Exclusions

To exclude Vendors, Software Applications and Severities:



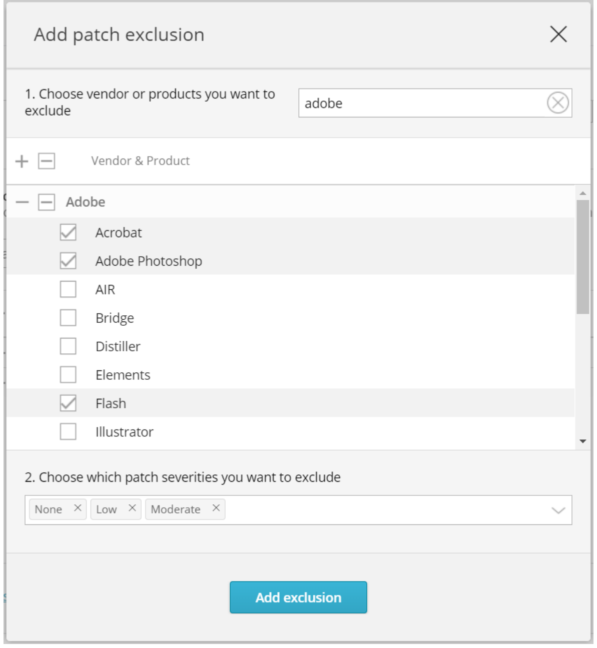
Patch exclusions

Following patches won't be deployed to all devices using this policy. You can deploy these patches manually if needed from patches page.

Here you can easily add Vendors, Software Applications and Severities to the exclusions list which means that they will be excluded from being updated (patched).

To exclude, click on 'Add exclusion' button. You will see a list of Vendors and Software Applications that belong to the Vendor. You can search a Vendor or Software Application (Product) or scroll down the list.

Simply select which vendors and software applications you would like to exclude and then select which severities you would like to exclude. An example is below:



Add patch exclusion

1. Choose vendor or products you want to exclude: adobe

Vendor & Product

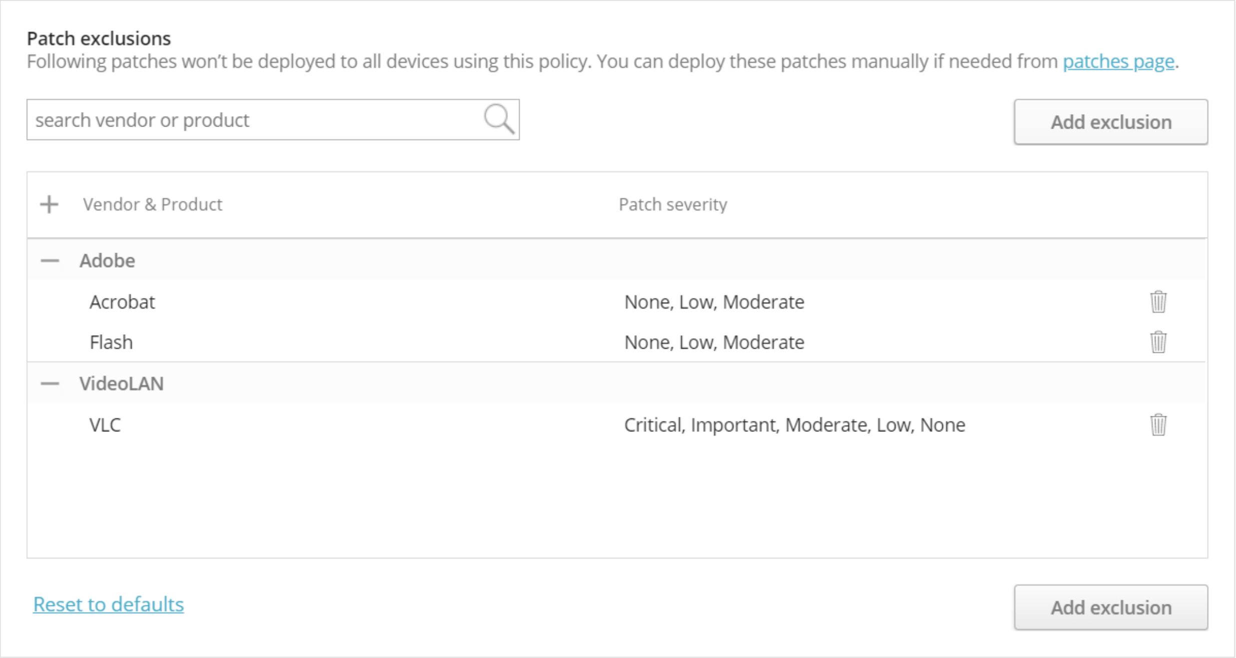
Adobe

- ☑ Acrobat
- ☑ Adobe Photoshop
- □ AIR
- □ Bridge
- □ Distiller
- □ Elements
- ☑ Flash
- □ Illustrator

2. Choose which patch severities you want to exclude: None, Low, Moderate

As an example: I have decided to exclude only some products under the Adobe Vendor along with none, low and moderate update severities. Therefore, only Adobe Acrobat Critical and Important Updates will be patched.

Here is what it looks like when I add additional vendors and products to be excluded:



Patch exclusions

Following patches won't be deployed to all devices using this policy. You can deploy these patches manually if needed from patches page.

Vendor & Product	Patch severity
Adobe	
Acrobat	None, Low, Moderate
Flash	None, Low, Moderate
VideoLAN	
VLC	Critical, Important, Moderate, Low, None

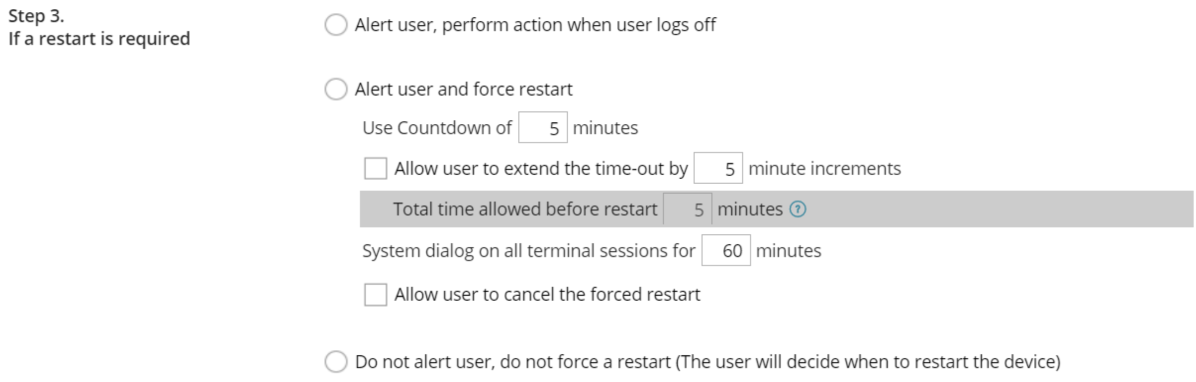
You can easily search for vendors or products from the search bar if you have a large list of exclusions.

Exclusions can be deleted. You cannot edit the exclusion, you will need to delete it and re-create the one you want.

You can also restore to defaults which wipes the whole exclusions list without a confirmation.

Step 3 – Restart options

There are multiple restart options that can be selected after patches have been successfully deployed. By default the 'Do not alert user, do not force a restart (The user will decide when to restart the device)' option is selected.



Step 3.
If a restart is required

○ Alert user, perform action when user logs off

○ Alert user and force restart

Use Countdown of 5 minutes

□ Allow user to extend the time-out by 5 minute increments

Total time allowed before restart 5 minutes ⓘ

System dialog on all terminal sessions for 60 minutes

□ Allow user to cancel the forced restart

○ Do not alert user, do not force a restart (The user will decide when to restart the device)

Options:

1. **Alert user, perform action when user logs off** – User will be alerted that a restart is required, just a text based alert and when the user logs off from their Windows Account, the restart will occur.
2. **Alert user and force restart:**
   a. Use Countdown of 5 Minutes – number of minutes can be configured. Countdown will complete and restart will occur.
   b. Check box - Allow user to extend the time-out by 5 minute increments – number of minutes can be configured. Countdown will occur and user can keep on extending without a forced reboot. If user is not present at the device, reboot will occur unless they extend it.
   c. Total time allowed before restart 5 minutes – number of minutes can be configured. This provides a total amount of time before the restart occurs. For example if you allow the user to extend the time-out by 5 minutes increments and then set the total time allowed before the restart to 15 minutes, they will get 3 extensions until the reboot is forced.
   d. System dialog on all terminal session for 60 minutes – number of minutes can be configured. If you are running terminal sessions (or have Patch on devices connected to a terminal server), then system dialog will show for all devices connected to the terminal for 60 minutes which cannot be closed and restart will occur after then.
   e. Checkbox - Allow user to cancel the forced restart – end user can cancel the restart until next patch deployment occurs when the restart will appear for them, which they can then cancel.

3. **Do not alert user, do not force a restart –** Restart prompts will not show to the user, and no restart will occur. This could affect future patch deployments if there is a restart pending on the Windows Operating system.

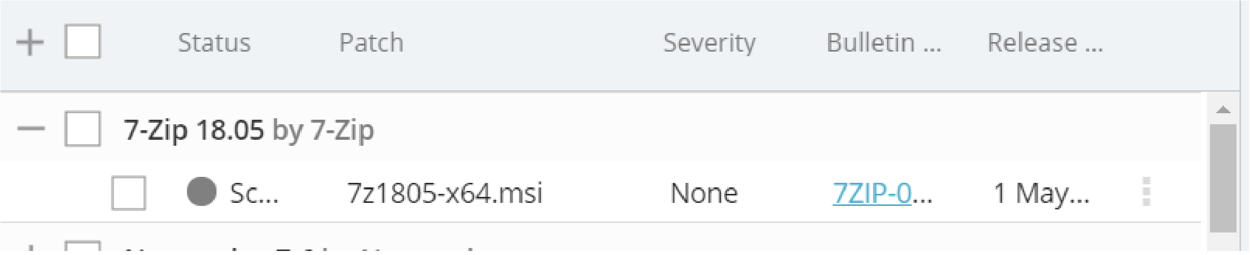
Step 4 - Clear Cache - Retention

The retention setting will allow you to automatically delete locally stored patches on your devices, saving valuable hard drive space.

Patches Page

The ‘Patches’ page allows you to see all missing patches for all devices connected to your console that are assigned to a device policy with the Scan Patches activated. All device results will show in this page.

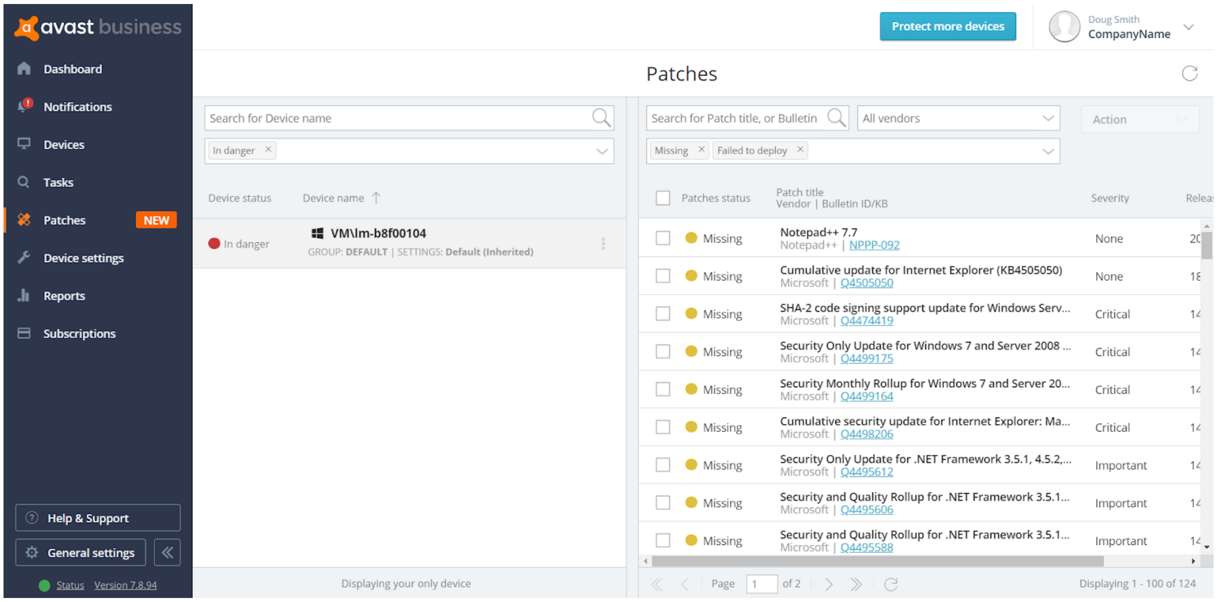
The right side panel will show you all missing patches:



□	Status	Patch	Severity	Bulletin ...	Release ...
□	7-Zip 18.05 by 7-Zip				
□	● Sc...	7z1805-x64.msi	None	7ZIP-0...	1 May...

The columns explained:

- **Status**: Status of patch which will show as missing and that it is scheduled to be deployed to your devices
- **Patch**: Name of the patch (update)
- **Severity**: If it is a Critical, Important, Moderate, Low or None
- **Bulletin ID/KB**: This will be a link to the Vendors page that will show you the release notes for the patch
- **Release Date**: Date in which the patch was released
- **Context Menu** (3 dots): Deploy on Schedule and Don’t Deploy. Deploy on schedule means that this particular patch that is selected will be deployed via the deployment schedule. Don’t Deploy means it will be skipped for the next scheduled deployment.
- **Actions** button: Same as the context menu



Patches

Search for Device name

In danger ×

Device status	Device name ↑
● In danger	VM\lm-b8f00104 GROUP: DEFAULT | SETTINGS: Default (Inherited)

Displaying your only device

Search for Patch title, or Bulletin

All vendors

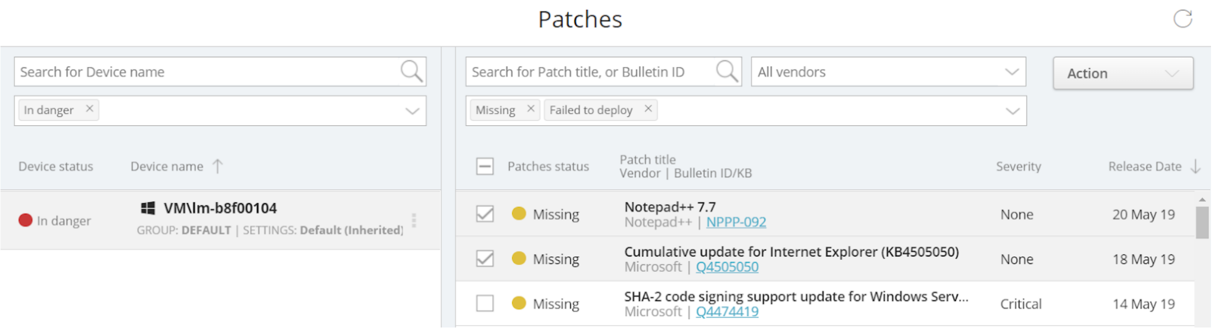
Missing × Failed to deploy ×

□	Patches status	Patch title Vendor | Bulletin ID/KB	Severity	Releas
□	● Missing	Notepad++ 7.7 Notepad++ | NPPP-092	None	20
□	● Missing	Cumulative update for Internet Explorer (KB4505050) Microsoft | Q4505050	None	18
□	● Missing	SHA-2 code signing support update for Windows Serv... Microsoft | Q4474419	Critical	14
□	● Missing	Security Only Update for Windows 7 and Server 2008 ... Microsoft | Q4499175	Critical	14
□	● Missing	Security Monthly Rollup for Windows 7 and Server 20... Microsoft | Q4499164	Critical	14
□	● Missing	Cumulative security update for Internet Explorer: Ma... Microsoft | Q4498206	Critical	14
□	● Missing	Security Only Update for .NET Framework 3.5.1, 4.5.2,... Microsoft | Q4495612	Important	14
□	● Missing	Security and Quality Rollup for .NET Framework 3.5.1... Microsoft | Q4495606	Important	14
□	● Missing	Security and Quality Rollup for .NET Framework 3.5.1... Microsoft | Q4495588	Important	14

Page 1 of 2

Displaying 1 - 100 of 124

The left side panel will list all devices that require missing patches by selecting the patch on the right panel, the right panel will update and show you which devices are missing that patch:



Patches

Search for Device name

In danger ×

Device status	Device name ↑
● In danger	VM\lm-b8f00104 GROUP: DEFAULT | SETTINGS: Default (Inherited)

Search for Patch title, or Bulletin ID

All vendors

Action

Missing × Failed to deploy ×

☐	Patches status	Patch title Vendor | Bulletin ID/KB	Severity	Release Date ↓
☑	● Missing	Notepad++ 7.7 Notepad++ | NPPP-092	None	20 May 19
☑	● Missing	Cumulative update for Internet Explorer (KB4505050) Microsoft | Q4505050	None	18 May 19
☐	● Missing	SHA-2 code signing support update for Windows Serv... Microsoft | Q4474419	Critical	14 May 19

Rollback

There is a roll-back feature, that allows you to select an already deployed patch and roll it back (uninstall it). This feature will benefit you if a deployed patch is causing issues for the operating system and/or software application. This feature allows the admin to troubleshoot the issue after the rollback.

Deploy Immediately

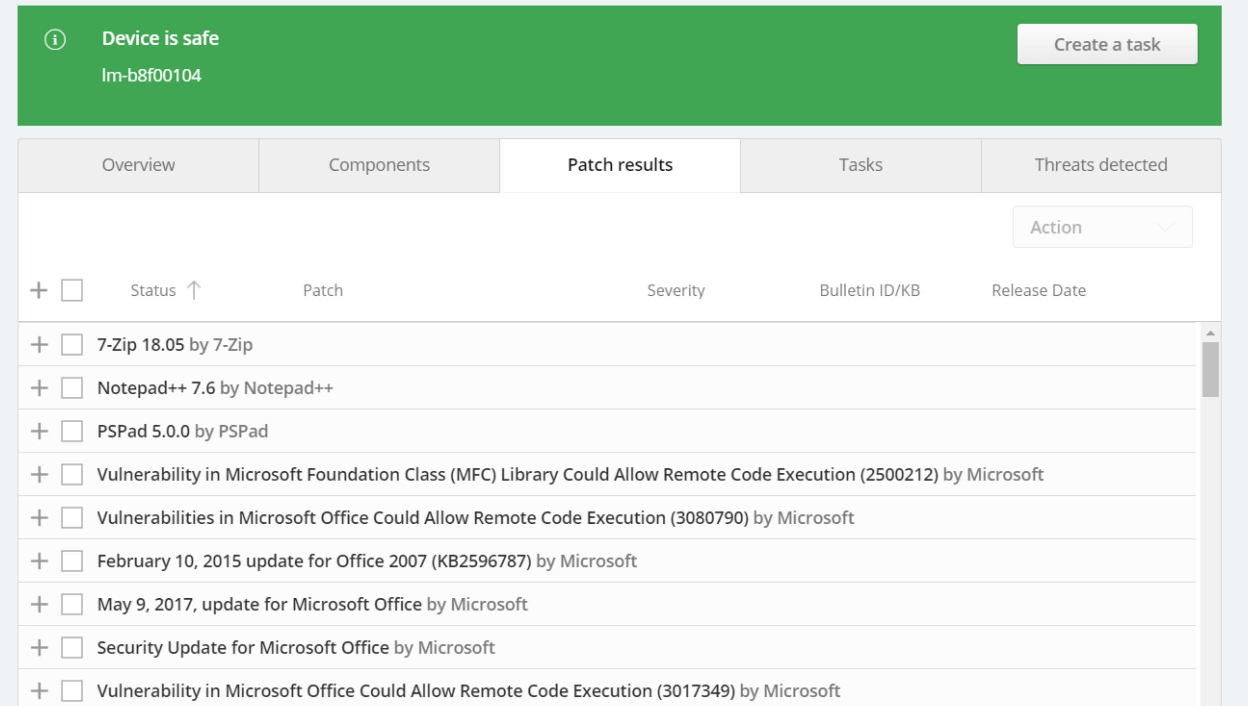
This action will allow the admin to deploy patches to devices and not wait on the deployment schedule time. This action will benefit customers that require to deploy a critical patch to devices straight away rather than waiting on the scheduled deployment time.

Ignore

This action will allow the admin to ignore patches that they do not wish to deploy and can hide them from the list.

Patch Results - Device

To see what patches are missing for a particular device, you can dive deeper by going to **Devices > Select Device > Patch results** tab.
Here you will be able to see the same information as the 'Patches' page but you will see missing patches only for this device.



Device is safe

lm-b8f00104

	□	Status ↑	Patch	Severity	Bulletin ID/KB	Release Date

+ □ 7-Zip 18.05 by 7-Zip

+ □ Notepad++ 7.6 by Notepad++

+ □ PSPad 5.0.0 by PSPad

+ □ Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212) by Microsoft

+ □ Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3080790) by Microsoft

+ □ February 10, 2015 update for Office 2007 (KB2596787) by Microsoft

+ □ May 9, 2017, update for Microsoft Office by Microsoft

+ □ Security Update for Microsoft Office by Microsoft

+ □ Vulnerability in Microsoft Office Could Allow Remote Code Execution (3017349) by Microsoft

Reports

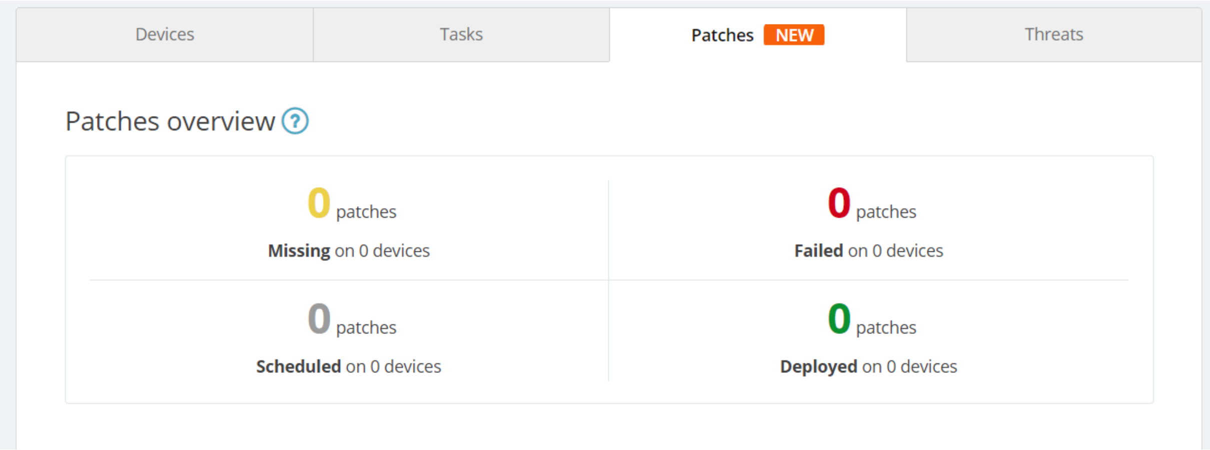
There are a total of 5 reports that can be viewed from the “Reports” > “Patches” section of the console.

Available reports are:

- Top 10 devices with patches successfully Deployed
- Top 10 devices with patches Failed to deploy
- Top 10 devices with patches Missing
- Top 10 patched applications
- Top 10 patched vendors

These reports can be exported to PDF using the “Print preview” button.

There is a Patches overview section that provides a summary of Missing, Deployed, Scheduled and Failed for all devices in your network.



Patches overview ?

0 patches
Missing on 0 devices

0 patches
Failed on 0 devices

0 patches
Scheduled on 0 devices

0 patches
Deployed on 0 devices

Notifications

There are a total of 3 new Patch Management notifications.

- Patches failed to deploy - Provides a notification in console and by email on how many patches have failed to deploy on devices
- Patches missing - Provides a notification in console and by email on how many patches are missing on devices
- Reboot required - Provides a notification in console and by email on how many devices require a reboot