

Release Notes: Avast Business CloudCare (October 29, 2019)

CloudCare Agent version: 4.17

Cloud Backup Client version: 7.4.1 – No Change

Antivirus Client version: 19.6 – No change

Console version: 5.0

Release Summary

We're pleased to announce a new service offering in the CloudCare platform – Patch Management.

Patch Management allows you to provide your customers with an additional layer of security that protects at the device level. Patch Management complements Avast Business Antivirus and other CloudCare services by identifying critical operating system and software application vulnerabilities and makes it easy to deploy patches across all customers endpoints.

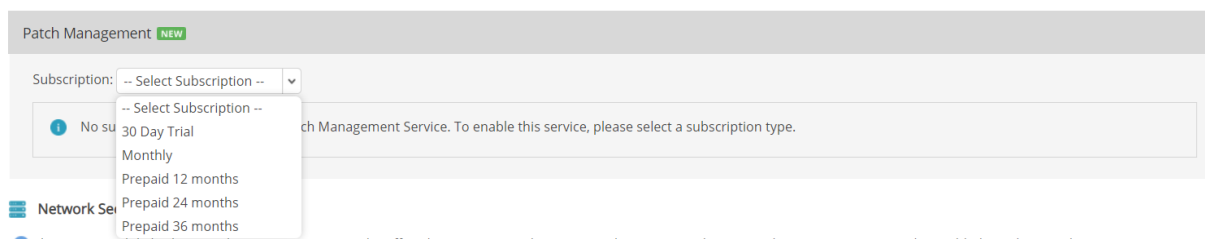
This release also focuses on improvements and resolving numerous bug fixes within the console and services.

Patch Management

For the first release of Patch Management in the CloudCare platform, our focus is to provide the Patch service at the customer level. Below are the following additions to the platform:

Services

Patch Management service will be located under the customer services section:



You can:

- Select a 30 day trial for your customer
- Monthly, 12, 24 and 36 month subscriptions are also available

Policies

The Patch Management policy is located under Endpoint Protection and is available at the partner and customer level:

Endpoint Protection

- > Antivirus
- > Firewall and Antivirus Add-ons
- ▼ Patch Management NEW

Patch Settings Auto-Approval Rules Ignored Patches

Scan Frequency ⓘ Choose how frequently patch scans should occur:

Daily at: 10:00 AM

Weekly every: Monday

Monthly every: 1 day of the month

Patch Deployment ⓘ Once scan has completed on endpoint device:

Do not deploy patches (Patches will be installed manually)

Deploy approved patches immediately after scan ⓘ

Deploy approved patches later (Patches will be installed following this schedule)

Clear local patch cache ⓘ Clear local patch cache files to free up disc space on endpoint device:

Immediately after patch deployment

7 days after patch deployment

30 days after patch deployment

60 days after patch deployment

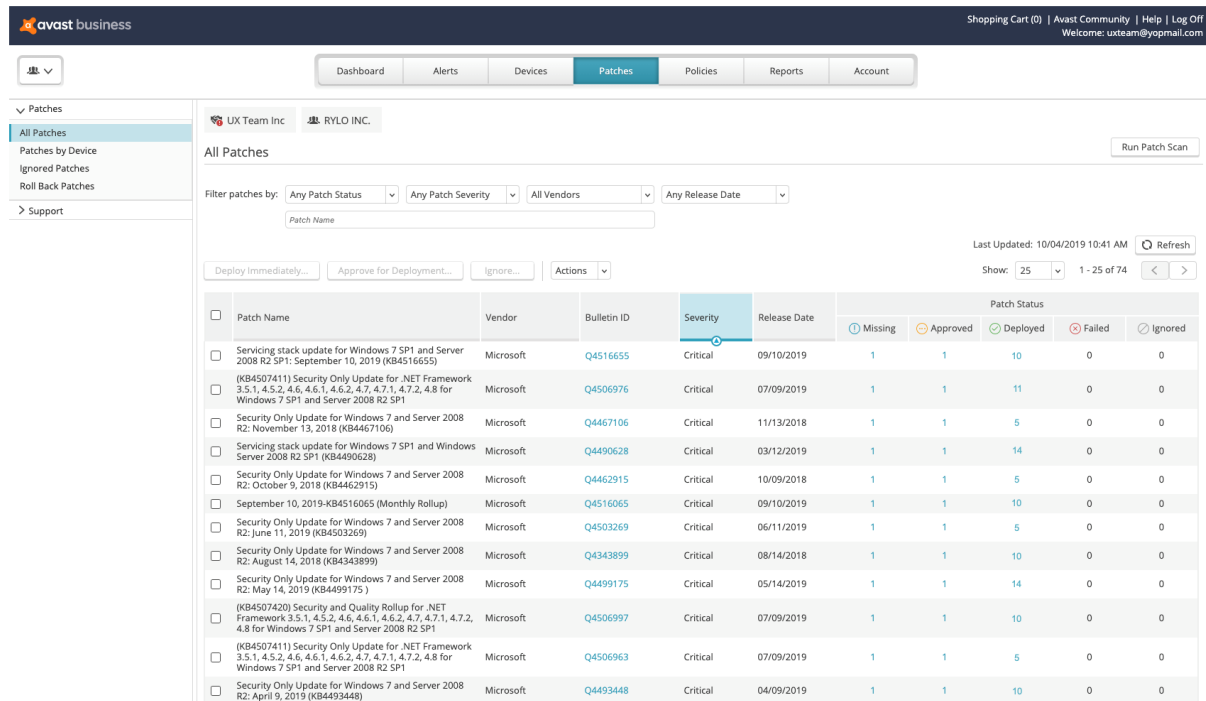
Restart Options After patch deployments are complete, some patches may require a device restart. These patches will not show as Installed until the restart is complete. When a restart is required, the devices will follow the settings defined in the Restart Options section (General Settings > General > Restart Options).

You can set up:

- Scan schedules – Set up time/day to scan your customer’s devices
- Patch deployment schedules – Set up time/day to deploy approved patches
- Clear cache options – Clear the devices local cache where patches are stored
- Auto approval rules – Automatically approve vendors, applications and severity of patches for deployment
- Ignored patches – View ignored patches, and add patches to be ignored from deployment. Only available for customer level policies

Patches

There is a new Patches button in the top navigation menu. Patches page under your customers Patch account will show you detailed patch pages:



The screenshot shows the Avast Business interface for the 'Patches' section. The top navigation bar includes 'Dashboard', 'Alerts', 'Devices', 'Patches', 'Policies', 'Reports', and 'Account'. The left sidebar has 'Patches' expanded with options: 'All Patches', 'Patches by Device', 'Ignored Patches', 'Roll Back Patches', and 'Support'. The main content area is titled 'All Patches' and shows a list of patches for 'UX Team Inc' and 'RYLO INC.'. The list includes columns for Patch Name, Vendor, Bulletin ID, Severity, Release Date, and Patch Status (Missing, Approved, Deployed, Failed, Ignored). A table of patches is displayed below.

Patch Name	Vendor	Bulletin ID	Severity	Release Date	Patch Status				
					Missing	Approved	Deployed	Failed	Ignored
Service pack update for Windows 7 SP1 and Server 2008 R2 SP1; September 10, 2019 (KB4516655)	Microsoft	Q4516655	Critical	09/10/2019	1	1	10	0	0
(KB4507411) Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 7 SP1 and Server 2008 R2 SP1	Microsoft	Q4506976	Critical	07/09/2019	1	1	11	0	0
Security Only Update for Windows 7 and Server 2008 R2; November 13, 2018 (KB4467106)	Microsoft	Q4467106	Critical	11/13/2018	1	1	5	0	0
Service pack update for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB4490628)	Microsoft	Q4490628	Critical	03/12/2019	1	1	14	0	0
Security Only Update for Windows 7 and Server 2008 R2; October 9, 2018 (KB4462915)	Microsoft	Q4462915	Critical	10/09/2018	1	1	5	0	0
September 10, 2019-KB4516065 (Monthly Rollup)	Microsoft	Q4516065	Critical	09/10/2019	1	1	10	0	0
Security Only Update for Windows 7 and Server 2008 R2; June 11, 2019 (KB4503269)	Microsoft	Q4503269	Critical	06/11/2019	1	1	5	0	0
Security Only Update for Windows 7 and Server 2008 R2; August 14, 2018 (KB4343899)	Microsoft	Q4343899	Critical	08/14/2018	1	1	10	0	0
Security Only Update for Windows 7 and Server 2008 R2; May 14, 2019 (KB4499175)	Microsoft	Q4499175	Critical	05/14/2019	1	1	14	0	0
(KB4507420) Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 7 SP1 and Server 2008 R2 SP1	Microsoft	Q4506997	Critical	07/09/2019	1	1	10	0	0
(KB4507411) Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 for Windows 7 SP1 and Server 2008 R2 SP1	Microsoft	Q4506963	Critical	07/09/2019	1	1	5	0	0
Security Only Update for Windows 7 and Server 2008 R2; April 9, 2019 (KB4493448)	Microsoft	Q4493448	Critical	04/09/2019	1	1	10	0	0

Under All Patches in the left navigation, you will be able to:

- View all missing patches for your customers' devices
- View patch statuses for each patch
- Deploy patches immediately
- Approve patches for deployment (all missing patches are automatically set as missing and will not be deployed to devices until they are approved manually or by using the auto-approve in policy settings)
- Ignore patches
- Filter patches
- Run a patch scan

Under Patches by device, you will be able to:

- View missing patches for an individual device
- Deploy one or more patches immediately to device
- Approve patches for deployment based on deployment schedule
- Ignore patches
- Filter patches
- Run a patch scan
- Dismiss failed patches

Under Ignored patches, you will be able to:

- View already ignored patches
- Add patch to ignore list for some or all devices
- Remove patch from ignore list
- Filter ignored patches

Under Roll back patches, you will be able to:

- View patches that have been rolled back
- Roll back patch for some or all devices
- Ignore patch after it has been uninstalled
- Filter patches that have been uninstalled

Patch Management Future Features and Enhancements

- Patch Management dashboard widget
- Patch Management alerts
- Patch Management reports
- Partner level patches page
- Master Update Agent distribution
- Auto-approval groups
- And much more...

Software Updater

Due to this feature only supporting a small number of third-party applications, the lack of management capabilities from the CloudCare platform or locally on the user interface, and possible conflicts with our new Patch Management service, we have decided to EOL the Software Updater feature.

Resolved Issues

[CC-7453]	Fixed an issue where the master agent could not be set or changed.
[SMBP-393]	Fixed issue with device registration when the master agent is enabled on the network.
[SMBP-507]	Fixed issue with out of date virus definition alerts that were triggered too early before having time to update the devices.
[CC-8159]	Virus Definitions Overdue alerts will be set to 7 days as default (you will still be able to change the days)

Additional Information

Localized CloudCare UI in all supported languages