Release Candidate

IT Operation Platform

December Release

12/01/2018

Table of Contents

Introduction

This document contains detailed notes about the December 2018 release, scheduled to go live Saturday 1st December 2018 (12/1/2018). The release is expected to take 4 hours to deploy, during which time the platform will be in maintenance mode

Endpoint Manager

Endpoint Manager Core

Improvements

- **Support for the latest operating systems**
  We continue to develop Endpoint Manager as the platform which lets you manage EVERY device on your network or your customer's network. In addition to the existing list, you can now enroll devices which run the following operating systems:
  - Android 9
  - iOS 12
  - Ubuntu 18

- **Audit Logs**
  We improved the log interface to show both old and new values in logs which record profile changes.
  We improved the logs to store changes and updates under File Group Variables

- **Export scope**
  You can now export all information in the 'Device Summary' section of a device.

- **Enrollment Instructions**
  iOS and macOS enrollment instructions are now listed separately.

Patch Management

New Features

- Missing optional patches are now shown in the ‘Endpoint Patching Status’ tile on the platform dashboard. This is in addition to missing critical patches.

Improvements

- Patch Management audit logs are now available as a separate category. You can also filter patching events by event name.
- Patch scan intervals have been improved. Initial scans are started 10 minutes after agent initialization. Regular scans are run every 8 hours.
- The ‘Critical’ patch status now represents both critical updates and security updates whose severity is critical.

Comodo Client Security

Windows

New Features

- Restore disabled and quarantined autorun items. You can now restore items disabled or quarantined by a Windows boot area scan. The following actions are available in ‘General Tasks’ > ‘Unblock Autoruns’:
    - **Unblock**: Enable a previously disabled auto-run entry. When you unblock an auto-run item, the corresponding executable file is restored from quarantine. You should create an exclusion for the executable, or change its rating to ‘Trusted’, or else the two items will be caught again by the next scan.

Delete: You can delete an autorun item from its original location. If you delete a scheduled task from this list, it will also be removed from Windows Scheduled Tasks.

Improvements

- Optimization of file rating queries. The check to find the local admin rating of a file is now handled in the background. This improves file opening times and overall system performance.

- Improved parent process tree in containment logs. Containment logs now show all parent and child processes for contained applications.

- CCS User Interface changes

    - Program update options have been removed from the CCS interface on local machines. This helps solve several potential conflicts between local endpoints and Endpoint Manager policy. CCS updates can still be managed via a device profile.

    - We also removed the options concerning automatic installation of program updates in critical situations. The website filtering tab is also hidden and disabled by default.

Portal

New Features

- Password and account policies added to the ‘Settings’ area. Admins can now set:
    - **Lockout time** – Length of time user is prevented from logging in after 5 invalid login attempts. Options range from 30 – 150 minutes (30 mins default).
    - **Session timeout –** Maximum length of time a user can remain logged into the platform before they need to login again.
    - **Password expiry period** – Maximum length of time a user can keep the same password before they need to change it.

Mobile Applications

Improvements

- iOS 12 support
- Android 8 support
- Android 9 support

APPENDIX-1

New Client Versions:

TBA