IT Operation Platform

January Release

2019-01-19

Table of Contents

Introduction

This document contains detailed notes about the Comodo One January 2019 release, scheduled to go live Saturday 19th January 2019 (2019-01-19). The release is expected to take 4 hours to deploy, during which time Comodo One will be in maintenance mode.

Endpoint Manager

Endpoint Manager Core

New Features

- **New enrollment options for macOS Devices**

  You can now enroll macOS devices to Endpoint Manager without needing to first install a device profile. This also applies to bulk enrollments.

  This lets customers use Endpoint Manager to manage security on Mac devices while continuing to use their preferred platform for general Mac management.

  Apple only allow one portal to use the protocol which manages devices. This caused problems with customers who wanted to use Endpoint Manager in conjunction with another MDM platform. The new enrollment method solves this issue and lets Endpoint Manager co-exist with solutions from other vendors.

  Note. If you use this type of enrollment you will not be able to manage the following sections in an Endpoint Manager profile:
  - Certificates
  - Restrictions
  - VPN
  - Wi-Fi

You can reach the wiki of the feature from here.

- **Export functionality for Audit logs**

  We added exporting mechanism to Audit Logs section.

- **ITarian branded Android and iOS mobile agents**

  The iOS and Android agents will be renamed as 'Mobile Device Management Client', published by ITarian. The following branding changes will apply to iOS and Android agents:

  - Agents renamed as 'Mobile Device Management Client'
  - Endpoint Manager branding and logos used on all agents
  - ITarian LLC added as the publisher of the clients

  The clients will be available on Google Play and the Apple Store as well as through the Endpoint Manager interface.

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:

  - Linux CentOS 7
  - macOS 10.14
  - Windows Server 2019

- **Audit Logs**
  Improved log interface. Both old and new values are now shown in logs which record changes to UI Settings.Here is the wiki of this feature.

Bug Fixes

- Fixed the issue of filtered view of devices when an installed app name is clicked from inside device details->installed apps section.
- Fixed the issue of not working installation of custom MSI packages from device list

Security

New Features

- **Export functionality added to the 'Security Dashboards' section**

  You can now export security component logs from the 'File View' and 'Event View' tabs. Click 'Security Sub-Systems' > 'Security Dashboards' to open the security dashboard.

  You can reach the wiki of this feature from here.

- **File Rating Columns added to security dashboards**

  Added 'Admin' and 'Comodo' rating columns to the 'File View' and 'Event View' tabs. Both new columns show old and current values.

  The 'Old' rating is the file rating before the event occurred. 'Current' rating is the most recent verdict since the event.

- **File Details in Security Dashboards**

  You can now view more granular details about files caught by Endpoint Manager security components. Security components include the antivirus scanner and file-rating scans.

  From January, you can select a file then click the 'File Details' button to view:

  File Details

  - **Last detected file name:** Name of the file when it was most recently scanned
  - **SHA1:** SHA1 hash value of the file
  - **First Seen by Comodo:** Date the file was first reported to Comodo threat labs
  - **First Seen on my Network:** Date the file was first detected on one of your devices
  - **Number of endpoints:** Number of endpoints on which the file was found
  - **Comodo Rating:** The trust verdict on the file from Comodo threat labs
  - **Last Update of Comodo Rating:** Time the Comodo rating last changed

File History

A detailed breakdown of a file's activity on your endpoints. You can see all endpoints on which the file was found, the security component that detected it, and the action that was taken against the file.

You can take the following actions from this page:

- Change the file rating
- Delete the file from specific or all endpoints
- Restore the file from quarantine

Here is the wiki of this feature.

Bug Fixes

- Fixed the issue of re-enabling Baseline after any change on EM Windows Profile is saved.
- Fixed the saving issues of Containment rules with "Started By" criteria

Remote Tools

New Features

- Admins can now set remote tool options in profiles. You can now configure access for different Remote Tools - File Explorer and Process Explorer. The following options are available:
  - **Silent connection**
    Connect without notifying the end-user
  - **Ask then allow** (waiting time is configurable in seconds)
    Ask end-user permission but connect anyway if they don't respond within a set time
  - **Ask then deny access** (waiting time is configurable in seconds)
    Ask end-user permission but close the connection if they don't respond within a set time
  - **In order to block connection**
    Turn off all Remote Tools options

  - **Show notification**

    Display a message on the target device which states that a remote session is active and the name of the admin who is connected. If enabled, you can also set the following:

- Allow endpoint user to terminate the connection
- Keep the notification window open after the session is terminated

Here is the wiki of this feature.

Remote Control

Improvements

- **Support for the latest operating systems.** We continue to develop 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 remote control to your managed endpoints which are running on macOS 10.14.

Bug Fixes

- There was a UI display issue when admin connected to MacOS Sierra device, this is fixed with January release.
- Mac devices were showing offline in Remote Control application, however, devices were online on Endpoint Manager portal, this is also fixed and available with January release.

ITarian Remote Access

Improvements

- **Support for the latest operating systems.** We continue to develop the tools which lets you manage EVERY device on your network or your customer's network. In addition to the existing list, you can now remote access to your unmanaged endpoints which are running on macOS 10.14 through our standalone application.

Remote Monitoring and Management

New Features

- You can now **monitor operating system patch events**. Operating system patches can be monitored by patch classification, severity level and other conditions. OS patch event logs are available in 'Device list' > device > 'Logs' > 'Monitoring Logs'.
  Here is the wiki of this feature.

Improvements

- **New columns in 'Profile' > 'Procedures'** - 'Added By (user)' and 'Added On (date)'
- **New filters added to 'Procedures' > 'Execution Logs'** - You can now filter by script procedure.
- **Monitor status' indicator** - added to 'Device' > 'Monitoring Logs' > 'Details' > 'Status'.

Patch Management

New Features

- It's now easier than ever to create a patch procedure. Simply click the 'Create Patch Procedure' button in the 'Patch Management' area and away you go.

  Here is the wiki of this feature.

Bug Fixes

- On Endpoint Manager portal, patch release date information was showing in wrong format. This is fixed with January release.
- On Global Software Inventory page, link to installed devices was showing 'no results' message. This is fixed with January release.
- Skype 7.40.151 on Windows 10x64 was not uninstalling via Software Inventory, this is now available.

- Even though patches were installed on endpoints, Endpoint Manager was showing that patches were failed. This reporting problem is fixed with January release.
- Even though a patch was selected to be applied to a single device, Endpoint Manager was applying it to all devices automatically. This is now fixed.
- Patch Procedures now scans the latest available patches for the device at the time of scheduled date/time is up hence keeps the device up to date all the time!
- DisplayCAL packages require Level Selection option to be set for silent uninstall, hence silent uninstall for DisplayCAL is now available with January release.

Comodo Client Security

Windows

New Features

- Admin rating lookups from Local Verdict Server are handled in the background when a file is executed. File rating flow is enhanced with a refactoring of Local Verdict Lookups. Now, file launches are not be affected by rating checks, which improves the performance of endpoint.
- Parent process tree in Containment Logs. Now, starting from the first initiator of a contained application, all process tree is available in Containment Logs in CCS. You can display the very first application of a contained process and detect which application is the first one contained.
- Restore disabled and quarantined Autoruns items. As the extension of Windows Boot Area Scan and Monitoring features, now you can manage the items which are blocked and quarantined by these abilities. Following actions are available in CCS General Tasks>Unblock Autoruns section:
    - **Unblock**: Enable selected scheduled task/Windows Service/Autostart entry which was disabled previously. When you unblock an item, related executable file will be restored from quarantine. Unless an exclusion rule is created for that file or its rating is changed to Trusted, it will be quarantined while the same autoruns item is disabled.
    - **Delete:** You can delete an autoruns item from its original location. If you delete a scheduled task item from this list, it will be removed from Windows Scheduled Tasks as well.

- Blocking specific external device. Now, it is possible to block only specific external devices. By selecting a currently plugged-in device or entering a device ID, you can create rule to block it in Device Control section. By doing so, you have the option to allow a whole device class with some exceptions.
- Detection of firewall driver status in Windows network adapter settings. From now on, status of Comodo Firewall adapter, which is installed to Windows Network & Internet settings, is monitored. When it is disabled by any reason, it will be detected and logged by CCS automatically. When such event occurs, Security Status Information section is switched to “At Risk” status by stating “Firewall driver is disabled in network adapter settings” message. In addition, you can set CCS to re-enable it from Firewall Settings section. By default, the functionality is enabled in “Log Only” mode.
- Defining size limits for archive files scanned by Real-time AV. With this functionality, you can manage file size limits for archive file types to be decompressed and scanned during real-time AV scan. By configuring limits for specific files extensions, you can optimize your endpoint performance.

Improvements

- Program Updates options removed from CCS Updates Settings
    - Program updates options removed in Updates tab in order to solve management and security issues.
    - Automatically Download Program updates and Automatically Install Program Updates in Critical Situations options are removed from endpoint UI .
- Hiding Website filtering section in CCS UI
    - CCS UI upgraded to solve management and authorization issues by hiding Website Filtering section. Also we provide more clear view and a better user experience by hiding Website Database Update Filtering by default.
- Periodic updates of Local Verdict Server is refactored in order to be handled at a separate schedule. Now, Antivirus Database updates and Local Verdict Server updates will be performed as different tasks in different schedules. By default, LVS updates is checked at every 1 hour.
- Skipping online resource look-ups in case of no internet connection. In order to improve performance of the endpoints, CCS checks the status of Internet connection before performing online look-ups such as Antivirus DB updates, file submission to Valkyrie. In case of no available

internet connection, these lookups will be skipped to prevent resource consumption. This setting is disabled by default.

- Updated CCS installation package according to Microsoft requirements. CCS Installation package is refactored so that registration of our product to Windows Security Center could be completed smoothly. Thus, CCS installation routine is compatible with latest requirements of Microsoft.

Bug Fixes

- Fixed the issue of obtaining file verdict using software vendor.
- Fixed the issue of launching CCS window during each logon.
- Fixed some performance issues due to interaction of some internal processes with 3rd party softwares.
- Fixed the connections and mapping issues with network drives
- Fixed the issue of crashes on Windows 10 preview builds.
- Fixed the issue of Virusscope incompatibilities with Media Player Classic and LibreOffice.

Portal

New Features

- New ITarian domain. ITarian accounts will be hosted on itarian.com from January onwards.
- 'ITarian Remote Access' tool. New utility added to the 'Tools' section.
- Patch Management charts on the dashboard. We added dashboard tiles for the following:
    - 'Total Security Patches Needed by Severity'
    - 'OS Patches by Classification'
    - 'Patch Management Third Party Applications'
    - 'Missing Important Patches' (item added to the patches tile)

Here is the wiki of this feature.

Bug Fixes

- There was an issue on the Dashboard for "Outdated Virus Database". Specifically this pertains to Smartphones. This issue has been fixed.
- There was an issue regarding add additional contracts to customer accounts this issue has been fixed.

Service Desk

Improvements

- **User deletion.** Currently, the user removal process is different in the user list and user detail interfaces. We unified this process so that the same pop-up is shown regardless of the interface you use.

- **New Materials.** Materials that can be measured by quantity will be available. You can also now choose material type when creating a new material.

- **'New Ticket' tweak.** 'Create new user' will be disabled by default when creating a new ticket. It is currently enabled by default.

- **Default opening page.** From January, 'My Tickets' will be the default opening page instead of 'Open Tickets'.

- **Performance upgrades.** Optimized the ticket close event to improve speed and performance of this action.

Bug Fixes

- Fixed the issue that can't add organization to a user.
- There was an issue regarding incorrect due date reported.It was fixed.
- Fixed the issue about unable to assign SD Users to a customer.
- Fixed the issue of support email in the loading screen for Service Desk.

- When ticket was exported, Column customer seemed empty.It has been fixed.
- Fixed the issue regarding unable to add multiple domains to SD Customer.
- There was a problem on the UPLOAD tab under IMPORT USER feature and copy paste tab.It has been fixed.
- Issue with Fonts in Helpdesk has been fixed.
- Fixed the issue regarding Unable to select the radio button to use the Custom Logo.
- Ticket creation page data got wiped out if all required fields are not filled out.Issue has been fixed.

APPENDIX-1

New Client Versions:

- Windows - Communication Client 6.25.21986.19010
- Windows - Comodo Security Client 11.0.0.7181
- Linux - Communication Client 6.25.21662.19010
- macOS - Communication Client 6.25.21980.19010
- macOS - Security Client 2.4.2.777
- iOS - Mobile Device Management Client 1.2.25
- Android - Mobile Device Management Client 6.13.4.14