IT Operation Platform

July Release

2019-07-13

Table of Contents

Introduction

This document contains detailed notes about the ITarian July 2019 release, scheduled to go live Saturday 2019-07-13.

The release is expected to take 30 minutes to deploy, during that time platform will be under maintenance mode. Post-deployment tests are expected to continue until 2 pm EST during which you may observe minor glitches. If you observe any issues, please feel free to share with us.

Important Notice! - The new version of Comodo Client Security for Linux will be released later. The new date will be announced.

Endpoint Manager

Endpoint Manager Core

New Features

Proxy Mechanism for Clients

You can now specify local endpoints as proxies from which other endpoints can collect installation packages and database updates. This helps save network traffic and accelerates package deployment when a large number of endpoints are involved.

You distribute the following packages with this feature:

- Comodo Communication Client
- Comodo Client Security
- Virus database updates

You can define the maximum amount of traffic to be used for package distribution, and the maximum number of proxy endpoints.

Here is the wiki of this feature.

Bug Fixes

- Fixed the issue of auto-remediation procedure triggers despite it is disabled in monitor settings on portal.
- Fixed the issue of MacOS Communication Client connection failure.
- Fixed the issue of maintenance window being shown as "OFF" while it is actually in the preset interval.
- Fixed the issue of location tracking for mobile devices.
- Fixed the issue of download servers from security profile not being applied to client immediately.
- Fixed the issue of translation inconsistencies for Remote Control and Remote Tool settings in profiles.
- Supported Device Platforms page is updated in order not to cause disinformation.

Security

New Features

Virtualization Exclusions for Removable Media

You can now exclude removable media such as USB sticks and external drives from virtualization. Doing so allows apps in the Virtual Desktop to write and make changes to specific media attached to the endpoint. This provides another way to export data from the Virtual Desktop in addition to Shared Space.

You can configure these exceptions in the ‘Containment’ section of an Endpoint Manager profile.

Set Custom Disclaimer for Virtual Desktop

Expanding our white-label options, you can now configure a custom disclaimer message for the Virtual Desktop. Users must accept the disclaimer before starting the virtual session.

You can configure the disclaimer in the ‘Containment’ section of an Endpoint Manager profile.

See this wiki if you want help to white label/rebrand the Endpoint Manager clients.

Allow User to Override Virtual Desktop settings

When enabled, Endpoint Manager will not reverse local Virtual Desktop settings that are different to those in the endpoint's profile. Ordinarily, Endpoint Manager checks devices to see if the local settings match those in the device profile. It will re-implement the profile settings if it detects any deviation.

The new setting gives admins greater flexibility and control over individual endpoints. For example, you can now disable the exit password on a specific endpoint, avoiding the need to create a whole new profile just to accomplish this one task.

This addition complements the existing override option in the ‘Client Access Control’ section of a profile, which allows local changes to *every* CCS setting. Admins can now allow local override of just the virtual desktop settings, while preventing changes to other CCS settings.

You can configure the override setting in the ‘Containment’ section of an Endpoint Manager profile.

Here is the wiki of this feature.

Show only Virtual Desktop settings on endpoint

New option to only show virtual desktop options when users click the CCS tray icon on an endpoint. End-users can then access and launch the virtual desktop, but cannot change other CCS settings.

This feature is useful when used with the override option described above.

You can configure this setting in the ‘UI Settings’ section of an Endpoint Manager profile.

Here is the wiki of this feature.

Improvements

Auto-updates disabled by default in CCS

Automatic updates to the CCS client are now disabled by default in predefined profiles. This change was made after valued feedback from our customers who manage complex, sometimes delicately balanced networks. To avoid potential disruptions, customers prefer to be notified when updates are available so they can review them before installation.

New default actions for unknown autorun entries

This setting determines what CCS should do if an application tries to create/modifiy a service, auto-start entry, or scheduled task. You can find it at 'Configuration Templates' > 'Profiles' > open a level 2 or 3 profile > Click the 'Miscellaneous' tab.

The previous default was 'Ignore'. The new defaults are:

- Security Level 2 profiles - 'Terminate and Disable'
- Security Level 3 profiles - 'Quarantine and Disable'

You can find background information on this setting at https://help.comodo.com/topic-399-1-904-11900-miscellaneous-settings.html#action_on_tasks

Remote Control

New Features

File Transfer: Folder Transfers

You can now send/receive folders via file transfer in the Remote Control application.

You can track folder transfer status in the file transfer queue pane.

Here is the wiki of this feature.

Role-based access control for Remote Control file transfer

You can now limit file transfer capabilities for specific devices and/or device groups.

Similarly, you can now limit file transfer capabilities by role.

Here is the wiki of this feature.

Bug Fixes

- Fixed the issue of connecting to MacOS with Remote Control.

Patch Management

Bug Fixes

- Fixed the issue of not showing Russian characters in the Global Software Inventory.
- Fixed the issue of available but not displayed 3rd party patches problem.
- Fixed the issue of Software Inventory loading failure.

Remote Monitoring and Management

Bug Fixes

- Fixed the issue of RMM service crashing.
- Fixed the issue of Disk Space Monitoring's false alerts.
- Fixed the issue of incorrect output in monitoring results.

Comodo Client Security

Windows

New Features

‘Virtual Desktop only’ mode

As mentioned in the Endpoint Manager section earlier, we have added the ability to show only virtual desktop options when users click the CCS tray icon on an endpoint.

When enabled in a profile, CCS will only show these two items when you click the tray icon:

- Run Virtual Desktop - Opens the Virtual Desktop
- Open Virtual Desktop Settings – Opens the Virtual Desktop settings area in CCS

End-users cannot access any other area of CCS.

Improved password policy for the Virtual Desktop

Admins can prevent end-users from accessing the local computer by setting an ‘exit’ password on the Virtual Desktop. Once set, users will need to enter the password if they want to switch from the virtual environment to the local environment. We added the following settings to improve the security of this password:

- 90-day validity period. The exit password will expire, and must be changed, after 90 days.
- Password complexity requirements. Passwords must now be 8-16 characters and contain a mix of uppercase letters, lower case letters, numbers, and special characters.

Detection of msi installation through URL

Added a default containment rule that prevents the installation of msi packages via a URL in a command line. This feature is tightly coupled with Script Analysis as it will be detected in the list of enabled interpreters.

Virtualization exclusions for removable media.

Under default conditions, apps in the virtual desktop write to a virtual file system, and cannot save changes to the host or any peripherals. As covered earlier, you can now create exceptions to this rule for specific removable media. Creating such an exception allows users to more easily export data from the virtual desktop to USB sticks, external storage drives, or CD/DVD.

Extended Virtual Desktop Logs

Virtual desktop logs have been moved out of the ‘Containment Logs’ section and now have their own section. This improves log visibility and makes it easier to conduct investigations, analysis and forensics.

Bug Fixes

- Fixed the issue of aborted AV Full Scans
- Fixed the issue of adding timeout value in the duration of Virtual Desktop session
- Fixed the issue of internal process crashes on Windows 10 Pro, Server 2016 and Server 2012 R2
- Fixed the issue of twitching CCS icon
- Fixed the issue of incompatibility between the security agent and Google Chrome Enterprise
- Fixed the issue of mapping drives under incorrect directories
- Fixed the issue of failed Antivirus signature database updates

MacOS

New Features

Disable real time scans on network items

Real time virus scans are now optional for items on shared network drives. This can improve performance by eliminating needless scans on write-restricted files. If an endpoint does not have the rights to delete/quarantine files in a shared folder anyway, then there is little reason to scan them at this point. Any files copied to the endpoint will, of course, still be scanned locally.

Here is the wiki of this feature.

Linux

New Features

External Device Control logs

We added event logs for the USB control rule. The rule allows admins to block the use of USB devices on Linux endpoints. The new logs let you analyze events where there was an attempted breach of the rule.

Here is the wiki of this feature.

Bug Fixes

- Fixed the issue of requesting password on scan initiation attempt

Service Desk

New Features

With July release Audit Data Logs will include the action time.

Portal

New Features

Comodo Dragon platform

As you may remember we introduced Itarian platform in October release. In that release, all functionality was the same for both the ITarian and Comodo ONE platforms. The only difference was the platform skin (either ITarian or Comodo ONE branded).

However, the ultimate goal was reaching to a point that we have two perfect platform. The first one, ITarian Platform, would mainly bring IT Management aspects into the forefront which is strengthened with security products. With the second platform we aim to create ALL-IN-ONE CLOUD-NATIVE CYBERSECURITY PLATFORM that brings security aspects into the forefront which is strengthened by IT Management features. You will find MDR, EDR, Network Security products and much more that are directly integrated in this platform. With this new platform you now become MSSP!!! Yes, you can offer full MSSP capabilities with your own whitelabelled SOC! Just enable COMODO Dragon Platform and start offering MSSP services, no expertise, no staff, no costly SIEM licenses! It is literally MSSP in a box!!!

Now it is time to do this. By introducing Comodo Dragon Platform we aim to create ALL-IN-ONE CLOUD-NATIVE CYBERSECURITY PLATFORM that provides Active Breach Protection in a single platform. Enable this and become an MSSP!!!

This release will be the first step toward this goal. Comodo One will turn into Dragon Platform step by step. We will first start with rebranding and continue with powerful dashboards, with built-in security products and much more.

Nothing will change from Itarian side. Itarian will continue to be your centralized IT management platform with much more powerful features.

APPENDIX-1

New Client Versions:

- Windows Communication Client 6.29.27210.19070
- Windows Client - Security 11.4.0.7615
- Windows Remote Control 6.29.27171.19070
- macOS Communication Client 6.29.27177.19070
- macOS Client - Security 2.4.4.844
- macOS Remote Control 6.29.27180.19070
- Android Mobile Device Management Client 6.13.8.2