ITarian

IT Operating Platform

September 2021 Release

Table of Contents

Introduction

This document contains notes about the ITarian September 2021 release. The release schedule will be as follows:

US Region Portal -> The release will start on 15th September 2021 Wednesday at 1 AM EDT

EU Region Portal and agents -> The release will start on 16th September 2021 Thursday at 5 AM GMT

The release is expected to take 30 minutes to deploy, during that time the platform will be under maintenance mode, where you may observe minor glitches. If you observe any issues, please feel free to share with us.

Endpoint Manager

Endpoint Manager Core

New Features

- **Support for Windows 11**
  Endpoint Manager now fully supports Windows 11.

- **Latest Stable version**
  We are introducing the "latest stable" version under Agent Update Settings. You will be able to choose "Latest Stable Version" and make sure that agent gets the update only after a newer version is marked as "stable".

- **Signed Bulk Packages**
  From now on, you will be able to download and execute default signed bulk packages, which will prevent Microsoft Windows UAC warning messages when installer is executed. You will still be able to customize your bulk packages according to your needs.

- **Restart control options for Comodo Client - Security Uninstallation**
  Restart control options are added to Comodo Client - Security Uninstallation wizard.

- **Export functionality for Global Software Inventory**
  Global Software Inventory can be exported to csv.

- **Shortened URLs for Bulk Installation Package Links**
  Enrollment and bulk package links will be offered in shortened form in order to increase usability and distribution.

- **Android MDM Report**
  Android MDM report can be generated under the reports section, including much information regarding your Android devices.

Improvements

- **"Service Availability Check" procedures links under Comodo Client - Security install page and on Device List**
  From now on, you will be able to check our firewall requirements before you install Comodo Client - Security.

- **Missing Available Comodo AEP Seat Warning**
  While you are deploying Comodo Client - Security agent to your endpoints, there will be a warning message shown if you don't have enough Comodo AEP seats, indicating that the system will switch to postpaid for overuses.

- **Automatic Restoration of Endpoint Manager Portal from On Hold State**
  Endpoint Manager now automatically restarts account restoration process when an account is on hold because of inactivity.

Bugfixes

- Unable to enroll a user for Comodo Client - Security on MacOS
- Unable change owner for bulk with 20 devices. Server error 502.
- Certificate issue with macOS installation packages – packages can be installed ONLY after manual approval by end-user
- Third-Party app scan is not being finished
- Bug allowing to install CCS on Linux and macOS endpoints despite "Comodo Client – Security" extension is disabled
- Companies are not populated within Beta reports
- Not Sending EDR Trial License Expiration Emails
- Bulk installation package is blocked on Windows 10 21H1
- A license key should not be used on multiple portals

Security

Improvements

- **Extend Predefined Antivirus Exclusions for Improved Performance**
  Files related to Windows Update, Windows Security, Windows Group Policies and Windows User Profiles are excluded from Antivirus scans in order to increase performance. Those exclusions are enabled on all predefined profiles.

- **Whitelisting Improvements**
  Whitelisting is made easier! From now on, the only thing you will need to do is to add file paths under "Global Whitelist" default file group variable (empty by default) and voila! All necessary exclusions are already in place on several security related components, like Antivirus, Containment, HIPS and Firewall.
  Moreover, additional whitelisting rules for commonly used applications are added on HIPS, Containment and Firewall sections on default profiles. Additional rules are disabled by default, where you can enable them if needed.

Bugfixes

- Unable to change files rating under Autoruns through portal
- Pagination is missing for Application Control

Remote Monitoring and Management

Bugfixes

- Endpoint Manager sends New Infection Detected alert for the same item every time the item reported from the device

Patch Management

Bugfixes

- 3rd party patch operations occur for declined apps
- A search for Vulnerability CVE-2021-34527 in comodo showed no results

Remote Control

New Features

- **Multiple Sessions to Same Endpoint**
  Remote Control now supports multiple sessions to be opened to the same endpoint at the same time. This way, you will be able to take control of the same endpoint from different machines simultaneously.

Comodo Client Security

Windows

New Features

- **CIS Report Tool Improvements**
  From now on, CIS Report tool collects much more different kinds of data in order to better understand the problematic area(s) whenever an issue occurs. Moreover, EDR logs are now being collected.

- **Ability to Turn On/Off HIPS and Firewall Application Rules**
  HIPS and Firewall rules can now be turned off, which will allow users to temporarily or permanently disable rule(s) without deletion.

- **Block Option for SQL Script Execution via Virtualized OSQL and SQLCMD**
  SQL script executions by some applications via OSQL and SQLCMD can now be blocked.

- **Synchronous Local Verdict Server Lookup Option**
  From now on, Comodo Client - Security can be configured to use synchronous Local Verdict Server lookup, which will ensure that a file has the most recent rating.

- **Termination of Entire Process Tree Instead of a Single Process of Malware**
  From now on, when a malicious process is detected, entire process tree can be terminated instead of only termination of the malicious process

Bugfixes

- Different behavior for application running inside and outside of Containment (Kryptik not working in containment)

- Unable to type Chinese symbols in Containment

Portal

Improvements

- **API Tokens should be passed to account admin when related staff is deleted.**
  When an API token is generated under a staff, it can be still used even if the staff is deleted. The ownership of the API token is now passed to the account admin user.

Bugfixes

- Acronis Payment issue
- Malware Status table contains incorrect data in Executive Windows Antivirus Report

APPENDIX

New Client Versions

Windows Communication Client : 6.42.40854.21090

Windows Comodo Client – Security: v12.8.1.8597 (previous)

Windows Remote Control : 6.42.40803.21090

macOS Communication Client: 6.42.40864.21090

macOS Comodo Client – Security : 2.4.4.897 (previous)

macOS Remote Control: 6.42.40804.21090

iOS Mobile Device Management Client : 1.3.0 (previous)

Android Mobile Device Management Client: 6.17.1.5 (previous)

Linux Communication Client: 6.38.39165.20090 (previous)

Linux Comodo Client – Security: 2.3.1.540 (previous)