# IT Operation Platform

## June Release

## 2019-06-08

# Table of Contents

# Introduction

This document contains detailed notes about the ITarian June 2019 release, scheduled to go live Saturday 2019-06-08.

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.

# Endpoint Manager

## Endpoint Manager Core

### New Features

- **Bulk installation packages for Linux**

  Customers can now create bulk installation packages of the Linux communication and security clients, simplifying the mass-enrollment of Linux devices. A much requested feature, MSPs can now use the same fast setup process they currently use for Windows and MAC devices.

- **Improved Maintenance Windows**

  A maintenance window is a designated time-slot for your Endpoint Manager procedures to run. You can assign multiple procedures to a single window so they all run at the same, convenient time. Since introducing the feature in the last release, we've made several improvements to make maintenance windows even more useful:
  - **Individual maintenance window settings**
    The previous version allowed you to add multiple maintenance windows to a profile, and to set whether you want to randomize task start times and/or stop monitors during the window. However, you had to use these same randomize and monitor settings for all maintenance windows on the profile. The June release lets you create different settings for each window, and we've also added some totally new settings:
    - Stop or allow monitors on a per-window basis
    - Set task randomization options on a per-window basis

- Set procedure options for non-responsive devices:
  - Run as soon as the device comes online
  - Run in the next maintenance window after the device comes online
- Define times when maintenance windows should not run. For example, during holidays or vacations.
- Block the following tasks if someone tries to run them outside of the maintenance time-slot:
  - Remote Control session
  - Remote Tool session
  - On-demand patch installation
  - MSI package installation
  - On-demand script procedures
  - On-demand patch procedures
  - Reboot system

  You also have the option to receive notifications instead of blocking the task.

  Here is the wiki of this feature.

### Bug Fixes

- Fixed the issue of being unable to update to default security client version from device list.
- Fixed the issue of adding Google Play application to application store.
- Fixed the issue of uninstalling applications from all endpoints even though only a few is selected.
- Fixed the issue of translation for language change through portal.

## Security

### New Features

- **Comodo EDR agent deployment**

  You can now deploy the Comodo Endpoint Detection and Response (EDR) agent to your devices direct from the Endpoint Manager interface.

  Comodo EDR is a powerful event analysis tool which provides real-time monitoring and detection of malicious events on Windows endpoints. EDR lets you clearly visualize threats in a detailed timeline while instant alerts keep you informed if there is an attack on your

network. The panoramic threat intelligence provided by EDR makes it a invaluable complement to the uncompromising security of Comodo Client Security.

Customers can find EDR in the ITarian store, and at 'Applications' > 'cWatch EDR'.

The EDR agent can be distributed to your devices from the Endpoint Manager 'Device List'.

Here is the wiki of this feature.

- **Automatic reappraisal of quarantined items**

  This new scan type lets you re-check all quarantined items on your endpoints to identify and restore false-positives. The new scan will be added to predefined profiles by default. You can find the related settings in under Scan Profiles under Antivirus settings.

- **Additional Virtual Desktop Settings**

  The virtual desktop is a sandbox environment in which users can run programs and browse the internet without fear those activities will damage the endpoint. Applications in the virtual desktop are isolated from other processes, write to a virtual file system, and cannot access user data. Admins can even set up their endpoints so users and guests log straight into the virtual desktop, denying them access to the host.

  We added the following new features and settings to the virtual desktop:

  - Pause and lock a virtual desktop session with a randomly generated PIN number.
  - Set an expiry time for a paused virtual desktop. Paused sessions are terminated when the time expires. This prevents the virtual desktop from being locked indefinitely by the previous user.
  - Auto-launch the virtual desktop at logon for specific users. This allows admins to set up a fully-virtualized experience for their users.

  Here is the wiki of this feature.

- **Linux and Mac antivirus logs now available in 'Security Dashboards'**

  CCS antivirus events on Linux and Mac endpoints are now recorded as logs in the security dashboard. This is part of our commitment to create a truly centralized event management system for endpoints of all stripes.

- **Full Parent Process Tree for Contained Applications in 'Containment'**

Virtualized application with process name and id are recorded including all process tree starting from the first contained one. With the help of this feature, investigation of the containment can be done with more details. You can display the logs by clicking the file name in Parent Process column in File Details under Containment. A pop-up will be prompted with the tree which will show the exact recorded chain for the contained application in corresponding device.
Here is the wiki of this feature.

### Bug Fixes

- Fixed the issue of filtering on Security Dashboards
- Fixed the issue of “Something went wrong” in Application Control

# Remote Tools

### New Features

- Added the ability to download multiple remote folders via Endpoint Manager’s ‘File Explorer’ feature. To use the feature, click 'Devices' > 'Device List' > select a running Windows device > Click 'Remote Tools' > 'File Explorer’.
  Here is the wiki of this feature.

### Improvements

- Live search added to the process explorer feature. Filtered processes are shown as soon as you start typing in the search box.
  Here is the wiki of this improvement.
- Audit logs for remote tools added to the existing set of audit logs.
  Here is the wiki of this improvement.
- Multi-language support for the notifications shown on an endpoint when an admin starts a remote session.

# Remote Control

### New Features

- Russian and Spanish languages are now supported in the Windows and Mac remote control applications.

### Improvements

- You can now cancel a connection attempt while still on the ‘connecting...’ screen. Previously, admins had to wait for the connection to complete before they could terminate the session.
- Delete functionality for user email or domain/login information on the login screen is now available for Windows and MacOS Remote Control applications.

### Bug Fixes

- Fixed region auto-select issue on the US portal.
- Inability to use "File Transfer Session" when Floppy Disk Drive exists on target device is now fixed.
- Fixed connection errors that occurred when remotely connecting to MacOS devices.
- Fixed ‘Device not ready’ errors during remote sessions.
- Fixed error where devices were showing online in Endpoint Manager, but showing as offline in the remote control application.

## Remote Monitoring and Management

### New Features

- **Maintenance Window compliance warnings**

  Endpoint Manager will warn you if you set an end-time for a patch procedure which is outside that of the maintenance window. The warning will list the maintenance window times so you can adjust accordingly.

- **Passing Parameters for Custom Script Monitors**

  You can now use custom procedures with parameters when creating a monitor.
  Here is the wiki of this feature.

### Improvements

- **Procedure Log Enhancements**

  You can now filter execution logs by the following columns:

  - Device online status
  - Device Name
  - Started at
  - Started by
  - Launch Type
  - Finished at

    - Status
    - Last status update

- New fields added to device execution logs. You can now export these logs with the following additional fields:

    - Last execution time
    - Last execution status
    - Additional information
    - Service Desk ticket link
    - Service Desk ticket status
    - Service Desk ticket created date

### Bug Fixes

- Fixed the issue of Endpoint Manager Portal sending late email notifications about triggered monitors.
- Fixed the issue of incorrect time within email notifications about triggered monitors.
- Fixed the issue of being unable to set “End Time Settings” correctly for scheduled procedures.

## Patch Management

### Bug Fixes

- Fixed the issue about incorrect number of patches reported and shown in device list section in Endpoint Manager portal.
- Fixed the issue about inability to silently uninstall RStudio1.1.463 64bit application.
- Fixed the issue about inability to update OneDrive application.

# Comodo Client Security

## Windows

### Connectivity Issues Regarding CCS v11.2

- The engineering team investigated the issue from the first day of the incident, as some firewall-sourced connectivity issues were reported from some customers. Eventually, the issue is identified as it sourced from the complications of Firewall module refactoring during the transition from v11.1 to 11.2. Therefore, it has been decided that these refactorings should be reverted in this release. Internal tests and the tests on several customer environments were completed successfully. The team will keep working in depth to prevent recurrence of similar incidents. Due to this reversion, a few recent Firewall features will disappear. The detailed feature list can be found below. Please note that these features were not reflected to Endpoint Manager. Therefore, it will not require you to make any changes on your configuration under usual circumstances.
    - Features to be reverted:
        - Ability to specify criteria for Firewall rules.
        - Rating, Containment status, Age, Parent Process etc
        - Ability to create Firewall rules for IPv6 address ranges

## New Features

- The antivirus scanner will now skip files that take longer than 5 minutes to scan. This improves performance in manual and scheduled scans. Skipped files are shown in the scan results screen.

## Improvements

- New rule to auto-contain .msi installers. The new ‘Run Virtually’ rule applies to msiexec.exe files if the parent process is in the 'Management and Productivity Applications' group. This improves security by virtualizing any unknown files launched via msiexcec.exe by legitimate applications in the group.
- View logs straight from the tray icon. You can now access the ‘View Logs’ interface by simply right-clicking on the CCS tray icon.
- Enable/disable HIPS from the tray icon. Quickly activate or deactivate HIPS from the right-click menu of the CCS tray icon.
- Added ‘Block’ actions to the containment parent process tree. Processes blocked by the containment module are now logged in Containment Logs > Parent Process records. This improves visibility during forensic investigations.
- ‘Reputation’ column renamed as ‘Rating’ in the auto-containment rules screen. This change is to improve language consistency across product interfaces.
- Caps-Lock Warning. You are now warned if caps-lock is on when entering the client access password.

### Bug Fixes

- Fixed the issue of not minimizing Virtual Desktop
- Fixed the issue of Full Antivirus scan failures
- Fixed the issue of reporting internal containment services to EM
- Fixed the issue of BSOD after CCS installation
- Fixed the issue of BSOD when a cellular modem is enabled on the endpoint
- Fixed the issue of internal Comodo services crashs on Windows Server 2012 R2

## Linux

### New Features

- External device control rule for USB Devices. New rule lets you block the use of USB devices on Linux endpoints. You can create exceptions for specific devices if required.

# Portal

### Bug Fixes

- Customer name can exceed characters count limit with Edit option has been fixed.
- C1 Portal Notifications - html tag was shown. It has been fixed.
- Error 500 was appears after session timeout.It has been fixed.
- There was a problem on changing Daylight Saving Time settings. It has been fixed.

# APPENDIX-1

## New Client Versions:

- Windows Communication Client  6.28.26320.19060
- Windows Client - Security 11.3.0.7475
- Windows Remote Control 6.28.26299.19060
- macOS Communication Client 6.28.26178.19060
- macOS Client - Security 2.4.4.834
- macOS Remote Control 6.28.26274.19060

- iOS Mobile Device Management Client 1.2.27
- Android Mobile Device Management Client 6.13.6.9
- Linux Communication Client 6.28.26228.19060
- Linux Client - Security 2.2.1.458