

IT Operation Platform

April Release

04/30/2020

Table of Contents

Introduction	3
Endpoint Manager	3
Endpoint Manager Core	3
New Features	3
Bug Fixes	3
Security	4
New Features	4
Improvements	4
Bug Fixes	4
Remote Tools	4
New Features	4
Remote Control	5
New Features	5
Bug Fixes	5
Remote Monitoring and Management	5
New Features	5
Patch Management	5
New Features	5
Reporting	6
New Features	6
Bug Fixes	6
Comodo Client Security	6
Windows	6
New Features	6
Bug Fixes	6
APPENDIX	7

Introduction

This document contains notes about the ITarian April 2020 release, scheduled to go live 30 April 2020 at 8 AM. The release is expected to take 1 hour to deploy, during which time the platform will be in maintenance mode. Please feel free to share any feedback or issues with us on the release forum post. Post-deployment tests are expected to continue until 4pm EST.

Endpoint Manager

Endpoint Manager Core

New Features

- **Public API sharing - Must Have Items Part 2**

We are releasing the following APIs as Part 2 of our project to release our common APIs to the public:

- Procedures
- Monitors
- Alerts

These join last month's release of our APIs for users, devices, and device group properties.

- **Mark Duplicate Devices by MAC address**

In addition to the device name, you can now use MAC addresses to identify duplicate devices. This improves search accuracy when devices in separate organizations or networks may have the same name.

[Here](#) is the wiki of this feature.

Bug Fixes

- Fixed the issue of inability to clone a profile after the account is migrated from EU region to US region.
- Fixed the issue of CCC and CCS Branding settings are not applied.
- Fixed the issue of global software inventory doesn't filter software for selected companies/groups but shows software for all the customers.
- Fixed the issue of Endpoint Manager users being unable to takeover device when 2FA is enabled.
- Fixed the issue of maintenance windows are not available for procedures scheduling.
- Fixed the issue of inconsistency between device statuses on Endpoint Manager portal and Remote Control application.
- Fixed the issue of inability to reset screen passcode on iOS device through portal.

Security

New Features

- 'Added 'Quarantined Files' tab to the Mac OS device details. You can get a list of 'Quarantined files' from particular device.'

[Here](#) is the wiki of this feature.

- We improved file searches in Endpoint Manager's Valkyrie page by adding Start/end date filters.

Data Loss Prevention:

- Added the ability to view logs of DLP monitoring rules.
- Added a 'Patterns' column to the discovery logs detail window.
- You can now delete or quarantine files discovered by a DLP discovery scan.
- You can now create custom search patterns for DLP scans. Custom patterns can consist of specific keywords, keyword groups and data formats.

[Here](#) is the wiki of this feature.

Improvements

- We started 'Export to csv' action in Audit logs (from all pages).
- 'Threat history' became 'Android threat history'. We continue collection all logs. But right now, all logs from Mac/Win/Linux are not available to view from Threat History page.

Bug Fixes

- Fixed an issue of "Unable to add network path to Containment virtualization exclusions"
- Fixed an issue of "FW blocking communication (missing cmdprots.exe in predefined file group)"

Remote Tools

New Features

- Audit logs now record all command prompt and PowerShell actions.

[Here](#) is the wiki of this feature.

- Admins can now choose whether to access the remote device as the current user or as a local system user. This choice is available for file explorer, process explorer, service explorer and the command interface.

[Here](#) is the wiki of this feature.

Remote Control

New Features

- Added ability to pause and resume file transfer.
- Added ability to suspend and resume file transfer session.

[Here](#) is the wiki of this feature.

Bug Fixes

- Fixed an issue of "Takeover failed to start.Connection data is invalid." while connecting to macOS devices.

Remote Monitoring and Management

New Features

- **Procedures for Mac OS**

You can now create, run and schedule procedures on MacOS devices.

[Here](#) is the wiki of this feature.

- **Set Alias or Friendly Name for Network Devices**

You can now change network device names to memorable/understandable names.

[Here](#) is the wiki of this feature.

Patch Management

New Features

- **Enable / Disable Patch Management from Profiles**

You can now disable all patch management operations in active profiles. Admins can disable all updates/installations via:

- On-demand patch installations
- Scheduled patching operations
- Patch installations via procedures

[Here](#) is the wiki of this feature.

Bug Fixes

- Fixed the issue of patches being applied outside maintenance windows.

Reporting

New Features

- **Customer Assessment Report**

The customer assessment procedure lets you quickly evaluate the security of your managed Windows endpoints. The procedure generates a report which summarizes the following:

- Device Vulnerability: List of operating system and 3rd party patches that need to be installed
- Endpoint Security: Details of malware and unknown files found on devices.
- Phishing and Internet Risks: Test whether your endpoints can connect to harmful websites.
- Comodo Agent: An overview of which Comodo agents are installed on your endpoints.

[Here](#) is the wiki of this feature.

Comodo Client Security

Windows

New Features

Data Loss Prevention:

- New DLP monitoring rule lets you block users from taking screenshots while specific applications are running. This is useful for applications which are known to handle sensitive data.
- Added ability to create custom search patterns for DLP scans. As mentioned in the Endpoint Manager section earlier, custom patterns can consist of specific keywords, keyword groups and data formats.
- Added search support for more file types to discovery rules.

[Here](#) is the wiki of this feature.

Bug Fixes

- Fixed an issue of "Connection to NAS via VPN is not possible via SMB2/SMB3 with CCS installed"
- Fixed an issue of "Device gets very slow with CCS and Windows classic shell"

Service Desk

Bug Fixes

- Fixed the issue of "While trying to bulk close or delete tickets in the Open tickets screen, the tickets close/delete but it redirects to the login screen."

APPENDIX

New Client Versions:

Windows Communication Client : 6.35.37275.20040

Windows Comodo Client - Security: 12.2.0.8121

Windows Remote Control : 6.35.37178.20040

Endpoint Detection and Response: 2.3.0.195

macOS Communication Client: 6.35.37113.20040

macOS Comodo Client - Security : 2.4.4.851

macOS Remote Control: 6.35.37179.20040

iOS Mobile Device Management Client : 1.3.0

Android Mobile Device Management Client: 6.15.0.10

Linux Communication Client: 6.28.26228.19060

Linux Comodo Client - Security: 2.2.1.501

