ITarian

IT Operating Platform

March 2019 Release

ITarian LLC.
1255 Broad Street
Clifton, NJ 07013
United States
Tel: +1 (888) 266-6361
Tel: +1 (703) 581-6361
Fax: +1 (973) 777-4394

Table of Contents

Introduction

This document contains notes about the ITarian March 2020 release, scheduled to go live Saturday 9th of March 2020. The release is expected to take 15 minutes to deploy, during which time the platform will be in maintenance mode. Post-deployment tests are expected to continue until 4pm EST during which you may observe minor glitches. Please feel free to share any feedback or issues with us on the release forum post.

Endpoint Manager

Endpoint Manager Core

New Features

Forward Audit Logs to SIEM tools

- You can now forward audit logs to a SIEM server, emulating the existing feature in CCS.
- Users can configure syslog forwarding at ‘Settings’ > ‘Portal Set-Up’ > ‘Logging Settings’ > ‘Audit Logs’.

More Granular RBAC for devices, device groups, and remote control

- We improved role based access control (RBAC) for device operations, and to differentiate device operations with remote control permissions:
    - Updated the description of the "users.allow-portal-login" permission.
    - Device group permissions now have a more granular structure:
        - Create
        - Rename
        - Delete
        - Assign
    - **Remote control permissions now have a separate structure with the following permissions:**
        - Takeover,
        - File-Transfer,
        - File-Transfer(Upload),
        - File-Transfer(Download)

...and more granular RBAC for procedures

- **We separated alerts and procedure management controls. Procedures now have the following sub-permissions:**
    - Create Procedure
    - Edit Procedure
    - Delete Procedure
    - Approve Procedure
    - Execute Procedure
    - Export Procedure List
- **Alerts now have the following, separate, permissions:**
    - Read only > configuration.alerts
    - Full Control > configuration.alerts, manage

Results per Page Option for Device Tree

- You can now view device tree with additional pagination options, as you can already in the regular device list. Users can now limit the device tree results with the following number of item options:
    - 20
    - 50
    - 100
    - 200

Added support for Ubuntu 19.0

- Endpoint Manager clients now support devices using Ubuntu 19.04.

Public API Sharing - Must Have Items Part 1

- We aim to make all our common APIs public. This release sees stage 1 of this process, with the release of APIs for:
    - Users
    - Devices
    - Device Group categories

Dark Mode for Android MDM Client

- Devices on Android 10+ can now switch to the MDM client to dark mode.

Improvements

CCS - End of Support for Windows 7

- In line with Microsoft policy and security best practices, we are ending official support for CCS on Windows 7 devices. We encourage all customers to upgrade their Windows based systems to Windows 8 /8.1/ 10.

- CCS on Windows 7 will continue to work up-to previous version. New versions of CCS will not be supported.

- The following operating systems are affected:

    - Windows 7

    - Windows Server 2008 R2

Security

New Features

- Profile Section Addition with Default Settings - Windows profile (HIPS/Antivirus/Containment sections): Import profile settings while adding new section

- You can now schedule virus scans on specific days of the week in a Windows profile.

- AV usability improvements, Windows: On demand items request operation from portal: Quarantined items

Data Loss Prevention:

- You can now populate keyword groups by importing keywords from a file. This, for example, allows customers to populate the ‘Names’ group with a list of client users or employees.

- New DLP monitoring rules let you block users from copying or moving files to USB devices.

- Added ‘Quarantine’ action to DLP discovery rules. This lets admins isolate files containing sensitive information to prevent their exfiltration while a review of the files is in progress

Remote Control

New Features

- Added ability to use the command prompt and PowerShell to manage remote devices:
    - You can connect to the commands interface of the remote device
    - You can run commands in the remote device's command prompt
    - You can run commands on the remote device's PowerShell
- Added file versioning to file transfer operations. Endpoint Manager can now rename files that have the same name as a file on the remote machine, adding a version number to the name of the new file. This allows admins to retain both versions of the file on the destination.

Remote Monitoring and Management

New Features

Clone Monitors

- Users can now clone generic and network monitors

SNMP Monitoring: Performance and Disk Monitor

- Admins can now retrieve the following device information over SNMP:
    - Performance
    - CPU Usage
    - RAM Usage
    - Disk
        - Free space left on the system drive
        - Free space left on all drives
        - Free space change on the system drive

Run Procedures on device groups and customer

- Admins can now run procedures on all devices belonging to a customer or to a group. You can run procedures on:
    - Device groups
    - User groups
    - Customers

Patch Management

New Features

Security Vulnerability Notifications

- Added recipient logic for 'Security Vulnerability' notifications.

Improved patch information

- Patch Management interface now shows the most recent successful and failed patch scans dates for OS and 3rd party patches.

Comodo Client Security

Windows

New Features

- Maintenance mode for Windows 7

Data Loss Prevention

- Delete and quarantine actions added to DLP discovery rules
- New DLP monitoring section lets admins block files from being copied to USB devices.

New Features

- Comodo Client Security Mac – Added support for macOS Catalina

Bug Fixes

- Fixed an issue with antivirus database updates run from the device itself
- Fixed an issue with diagnostic utility reports

Portal

New Features

Managed Detection and Response (MDR) added to the ‘Store’ area

- Managed detection and response (MDR) is a 24/7 threat monitoring solution that delivers 24/7 protection against threats emerging on your network. MDR combines advanced technologies at the host and network layers with continual supervision and threat investigation from Comodo’s team of human security experts.

Technology Assessment Platform (TAP)

TAP moves to full release

Following last month’s beta of the product, we are proud to launch the full version of the Technology Assessment Platform (TAP) with the March release. TAP helps MSPs audit client networks and generates detailed reports which grade the customer on each aspect of their set-up. The reports form an action-plan to address gaps in their coverage which you can share with your customers.

We also added the following new improvements for the full release:

- You can now customize the default questions for each of your customers. This allows you to easily construct a questionnaire tailored to the precise needs of your client.

- Redesigned the final reports to make them even more professional, informative and easier to understand. In future releases will we add the ability to rebrand these reports.

- Complete interface redesign and more informative dashboard stats. TAP has a fresh new look we think you'll like.

Customers can access TAP as follows:

- Log in to your C1/Dragon/ITarian account

- Click 'Applications' > 'Technology Assessment Platform'

- Login to TAP with the same credentials you use for C1/Dragon/ITarian