IT Operation Platform

April Release

04/13/2019

Table of Contents

Introduction

This document contains detailed notes about the ITarian April 2019 release, scheduled to go live Saturday 04/13/2019.

The release is expected to take 5 hours to deploy, during which time Comodo ONE and ITarian will be in maintenance mode. Post-deployment tests are expected to continue until 4pm EST during which you may observe minor glitches. If you observe any issues, please feel free to share with us under the release forum post.

Endpoint Manager

Endpoint Manager Core

New Features

License Management for Advanced Endpoint Protection

You can now manage Advanced Endpoint Protection (AEP) licenses in the Endpoint Manager. Apart from general license management, you can also:

- Distribute seats from a single license to different customers, and assign seats from multiple licenses to the same customer.
- Create license usage reports to track the activities of a specific license.
- Get notifications when your licenses are about to expire.
  Here is the wiki of this feature.

Maintenance Windows

You can now define maintenance windows in order to create a planned update calendar. With this feature, you can:

- Create maintenance windows for specific timeframes.
- Schedule procedures to a specific window.
- Randomize task running order to prevent performance issues.

- Stop monitors in the defined maintenance window time frame

This is the first phase of this feature. Future releases will see the ability to block specific tasks, pause maintenance windows on holidays and procedures to handle offline devices.
Here is the wiki of this feature.

Management of Communication and Security Client Versions

You can now set a specific version of the communication and security clients as your default. The default version will be used for enrollment, bulk installation, client updates and dashboard sections. You can also specify which version of the client can be installed or updated by your staff. This helps admins to ensure that older versions of the clients are not introduced to the network, and that incompatible clients are not inadvertently installed.
Here is the wiki of this feature.

Improvements

- Support for operating systems
  We continue to develop Endpoint Manager as the platform which lets you manage EVERY device on your network or your customer's network. In addition to the existing list, you can now enroll devices which run the following operating systems:
  - Windows Server 2003 SP2
  - Windows Server 2008 SP2
  - Windows Server 2012

Bug Fixes

- Fixed the issue of uninstallation of softwares from global software inventory.
- Fixed the issue of event count alignment with portal dashboard and list in security sub systems.
- Fixed the issue with CCSM version in device list exported report.
- Fixed the issue of e-mail and help link shared in question mark at top right of the screen.
- Fixed the issue of addition of file group with sign "?".
- Fixed the issue with warning while adding iOS application to iOS app store.
- Fixed the issue of high CPU usage for Android mobile device management clients

Security

New Features

- Countdown timer for 'Training Mode' lets you specify that HIPS and Firewall only run in training mode for a specific period. Staying in training mode for extended periods can create an excessive amount of rules, resulting in performance issues on endpoints.
  Here is the wiki of this feature.

- Added Valkyrie sections to MacOS and Linux profiles. Unknown executables detected on MacOS endpoints can now be uploaded to Valkyrie for testing. Once enabled, unknown files like dmg, Mach-o and .elf are automatically sent to Valkyrie to establish whether they are trusted or malicious. Here is the wiki of this feature.

- Security Dashboards - Device View. The new view aggregates security events by device, letting you view the latest events on a particular device the related CCS component.
  Here is the wiki of this feature.

- Restore suspicious autorun entries. You can now monitor the current status of suspicious Windows Services and scheduled tasks etc, and restore the item and any quarantined files affiliated with the entry.

- New management capabilities for the Virtual Desktop:

    - Password Protection. If enabled, users will need to enter a password in order to close the virtual desktop. This prevent guests or regular-users from closing the virtual desktop and potentially exposing the computer to danger.

    - Launch Virtual Desktop upon user login. Starts the virtual desktop automatically as soon as the endpoint is booted. Enable this setting in CCS at 'Advanced Settings' > 'Containment' > 'Virtual Desktop'.

    - Automatically reset Virtual Desktop on session termination. Resetting the virtual desktop provides privacy and security by removing all user data and undoing all system changes.

Improvements

- Added WerFault.exe, the Windows error reporting tool, to "Windows system applications" file group. It can now be easily excluded from security policies in CCS.

Bug Fixes

- Fixed the issue of not reporting some contained files
- Fixed the loading issues with "Something went wrong" message in Application Control.
- Fixed the issue of time inconsistency of Containment events in Security Dashboards

Remote Tools

New Features

File Explorer - Folder Support

The remote tools feature lets you browse managed devices, perform folder operations, and transfer folders and files to/from devices through Upload and Download functionalities.

You can find the related wiki here

Remote Control

New Features

File Transfer via Remote Control Application

- Use the Remote Control application to transfer files to and from managed devices. Go to the device list to initiate your session.
- Initiate File Transfer sessions through Endpoint Manager
- Use the queue panel to queue file transfers and start/stop transfers
- Create, rename, delete files/folders on the remote device
- Run File Transfer simultaneously when you are in a Remote Control session.

  You can find the related wiki here

  Next for File Transfer:
  - Role based access control, device profile settings, and audit logs.
  - Additional ways to start and manage file transfers.

Bug Fixes

- Wrong device status on Endpoint Manager portal and/or Remote Control application, misleading users to initiate a remote connection.
- Remote Control application returned error while connecting due to an underscore on the customer name which was not supported by the framework standards. The issue is fixed by extending these cases to cover as well.

Remote Monitoring and Management

New Features

- **'Create Discovery' tile** – New shortcut lets you create discoveries faster than ever.
  You can find the related wiki here

- **Scheduled Discoveries**

  - Schedule daily, weekly or monthly discovery operations. Choose the time of day that the operation runs.
    You can find the related wiki here

- **Device View for Discovered Devices**

  - You can now view summary and network details of a discovered device by clicking device name inside discovered devices list.

- **Device Type**

  - You can now assign labels to your discovered devices so you can easily identify their type at a glance. Each device has a different icon and you can easily change a device's type when required.

    Available Device Types:

    - Router
    - Printer
    - UPS
    - Switch
    - Load Balancer
    - Firewall
    - Workstation
    - Server
    - Mobile
    - Other
    - Unknown

    You can find the related wiki here

- **Passing Parameters for Auto Remediation**
    - You will also be able to use procedures with parameters in auto remediation section while creating a monitor.

Improvements

- Procedure log statuses are now colored for better traceability.

Bug Fixes

- Fixed the issue of RMM agent not monitoring events from "Microsoft-Windows-Windows Defender/Operational" channel.
- Security Client Events monitoring is started with delay when endpoint is restarted, in order to prevent CCS communication error.
- Fixed the issue of online/offline monitoring error.
- Fixed the issue of RMM Service consuming HDD with too much active time.
- Fixed the issue of RMM Service high disk usage on normal hard drives.
- Typo correction (“Her names”) in Discover Now widget.
- Fixed the issue of unknown application running inside container monitoring event triggering even if the containment events are ignored.
- Fixed the issue of alert emails not being sent consistently.

Patch Management

Bug Fixes

- Fixed the issue of Device Management view Patch Status columns shows incorrect number of missing patches.
- Fixed the issue of 'Uninstall application' for selected companies deletes applications from all devices for all companies
- Fixed the issue of PM agent not detecting Windows Update KB4462933 as available update.

Comodo Client Security

Windows

New Features

- Virtual Desktop improvements.
    - PIN protection for paused sessions. When enabled, a password is generated when a user pauses a virtual desktop session.
    - Manage which programs are shown on the Virtual Desktop and its start menu. This lets admins better control the applications available to their users.
    - Limit paused session for auto termination. This lets admins to set a time duration for a paused session to be terminated automatically once the paused session duration exceeds the defined interval

  You can find the related wiki here.

- Advanced firewall rules. Granular application control rules let you control exactly how applications connect to the internet and other networks. You can also create rules which run on files with a specific trust rating, age or containment status.

- Ipv6 address ranges can now be specified in firewall rules.

Improvements

- 'At Risk' status on Windows Servers. The endpoint will change to "At Risk" when containment is disabled. This status is clearly shown in the device's icon in the device list.
- Rating Source and File Hash columns in File List Changes Logs. In detailed CCS Logs section, you can see the source of the provided file rating and the file hash of that file in newly added two columns

Bug Fixes

- Fixed the absence issue of Containment logs which are related to containing non-executable files
- Fixed the issue of high memory usage on Windows Server 2016
- Fixed the incompatibility issue between External Device Control and auto-scanning of plugged-in devices

- Fixed the issue of displaying the scan result windows for portal-initiated scans
- Fixed the containment issues that blocks launch of unknown files located at CD/DVD drives.

MacOS

New Features

- **Valkyrie Integration**. As mentioned earlier in the document, we added Valkyrie to CSS for MAC. When CCS detects an executable with an unknown trust rating, it will upload the file to Valkyrie for behavior testing. The test results will tell CCS whether the file is trustworthy or malicious. CCS with either allow or block the file based on the result.
- **TLS 1.2 Upgrade.** To comply with the best industry security practices, we are upgrading the protocol used in our security client to Transport Layer Security (TLS) 1.2.

Portal

New Features

- Multi-language support in ITarian. Phase one sees us introduce support for two additional languges - Russian and Spanish with UI translations only (metadata updates such as in table values will be coming in next sprints). You'll see the support for Portal, Service Desk and Endpoint Manager in this release. In addition, more languages will be added soon.

  You can find the related wiki here.

Bug Fixes

- Scheduled report was not working.It has been resolved.
- 2FA verification code couldnt be entered in Safari Browser on MACos.It has been fixed.
- Missing Dome Shield Module has been added to the portal
- Customer was unable to open EM and Dome Shield from C1.It has been fixed.

Service Desk

New Features

- From now on you can be able to delete all the selected tickets for the related lists.
  You can find the related wiki here.

- With April release you will be able to add new fields more than 5 to the Custom forms.

Improvements

- Fixed Service Desk latency issues.
- Fixed issue where exporting a PDF with a large number of records led to a '500' error.

Mobile Applications

Bug Fixes

- Login issue of CAM accounts are fixed for Comodo ONE and ITarian applications on both platform (iOS and Android applications).

APPENDIX

New Client Versions:

- **Windows Communication Client** - 6.27.25138.19040
- **Windows Client - Security** - 11.2.0.7313
- **Windows Remote Control** - 6.27.25030.19040
- **macOS Communication Client** - 6.27.24066.19040
- **macOS Client - Security** - 2.4.3.826
- **macOS Remote Control** - 6.27.25029.19040
- **Linux Communication Client** - 6.27.24888.19040
- **Android - Comodo ONE Mobile -** 1.19.4
- **Android - ITarian Mobile -** 1.19.4
- **iOS - Comodo ONE Mobile -** 1.3.5
- **iOS - ITarian Mobile -** 1.3.5
- **Android - Endpoint Manager - MDM Client (Comodo)**- 6.13.6.9
- **Android - Endpoint Manager MDM Client (ITarian)** - 6.13.6.9