



COMODO

Creating Trust Online®

Comodo ONE

IT Operating Platform

June 2018 Release

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

©2018 Comodo and the Comodo brand are trademarks of the Comodo Group Inc. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Table of Contents

Introduction	3
IT and Security Manager	3
New Features	3
Improvements	4
Bug Fixes	5
Comodo Client Security	6
New Features	6
Improvements	6
Bug Fixes	6
Service Desk	7
New Features	7
Improvements	7
Bug Fixes	7
C1 Portal	8
New Features	8
Improvements	8
Bug Fixes	8
Comodo Quote Manager	9
New Features	9
C1 Tools	9
New Features	9
Improvements	9
C1 Mobile (Android)	10
New Features	10
APPENDIX-1	11
New Client Versions:	11

Introduction

This document contains detailed notes about the Comodo One June 2018 release, scheduled to go live Saturday 9th June 2018 (06/09/2018). The release is expected to take 4 hours to deploy, during which time Comodo One will be in maintenance mode.

Important Notice! - New version of Unknown File Hunter will be released at 18th June 2018

IT and Security Manager

New Features

Remote Control

We are excited to add two frequently requested features to Comodo Remote Control:

- The ability to list, filter and search devices by 'Company' and 'Group'. Especially useful for those who manage multiple companies or groups, this simple addition reduces your time-to-connect so you can serve your clients quicker and easier.

Please see the wiki post [here](#)

- Two-factor authentication when logging in to the remote control viewer. To use this service, you must first enable two factor in C1. Once setup, you will login to the viewer with your C1 credentials as usual. You will then be directed to the two-factor screen where you'll enter the code generated by the Google Authenticator application. Please see [our help guide page](#) if you need help to configure two factor authentication.

Please note that sign-in with back-up codes and 'Don't ask for this device' will be available in future releases. Please note that Two Factor Authentication is only supported for Comodo ONE sign-in option.

Please see the wiki post [here](#)

Security Monitoring

You can now monitor devices for the occurrence of a range of security events. You can set up alerts if an event occurs, improving your visibility and response time should problems arise on your network. The

following types of event can be monitored:

- Security Events
 - Malware handled
 - Malware detected
 - Unknown applicaiton running inside container
 - Unknown applicaiton gets new rating
 - New device blocked by device control
 - Number of Firewall actions
 - Threat handled by VirusScope
- Security Client Events - you can reach the wiki of this feature from [here](#).
 - Comodo Client Security process error ocured
 - Comodo Client Security communication error ocured
 - Comodo Client Security outdated
 - Another Anti Virus solution installed
 - Anti Virus scan failed
 - Anti Virus Database update failed
- Audit logs now capture changes in ITSM Profiles > Containment settings. This extra visibility adds to the already comprehensive view provided by our logs, helping decrease the time you spend on troubleshooting and root cause analysis. As with other logs, you will be able to see the event name, the affected object, and the old and new values. You can reach the wiki of this feature from [here](#).

Improvements

- You can now export data from the following ITSM pages:
 - Security Sub-Systems > Antivirus > Current malware list
 - Security Sub-Systems > Antivirus > Device list
 - Security Sub-Systems > Antivirus > Threat history

Exported data is available in 'Dashboard' > 'Reports' as a new report. In the following months we will implement this functionality on all table views. You can reach the wiki of this feature from [here](#).

- Device List
 - The color of the 'Containment' icon in the 'Active Components' column will change to blue if an endpoint is in 'Baselining' mode.
 - Info-box added near the search box to show hints about searching methods.
- Baselining. Any time remaining on a baselining operation is now clearly shown in the 'Comodo Client Security' info box. Click 'Device List' > open a device > 'Summary' > 'Comodo Client Security'.
- Remote Control audit logs: Added 'Disconnection Reason Text' field.
- Sorting improvements:
 - Execution logs of OS & 3rd party patch procedures can now be sorted by the 'Device Name' column.
 - Operating system patch inventory can now be sorted by the 'Release Date' column. You can find the wiki for this feature from [here](#)
- Global Patch Management inventory is now presented with a new tree based structure! Patches are listed together with expanded / collapsed device groups hierarchy on global patch management inventory. Admins can select the root and see all patches, or view patches by device group. You can find the wiki for this feature from [here](#)

Bug Fixes

- 'Third Party Applications' screen. Fixed a bug where the number of 'Installed Devices' and 'Upgradeable Devices' was shown incorrectly after removing a device.
- Fixed a bug which affected multi-monitor support
- Bulk Installation Packages were saved with incorrect file name when downloaded using Microsoft Edge browser. Issue is fixed
- An issue with adding applications to ITSM Android store is fixed.
- Fixed a bug for mouse cursor to be shown on windows resizing within CRC session.
- Fixed a bug for multi and single monitor support within CRC session.

Comodo Client Security

New Features

- The parent process of a contained application is now logged. When an application is contained, the process which launched the application will now be recorded in 'Event Logs' > 'Containment Events'. This includes the path to the file and its hash. This is useful in a number of circumstances. For example, it will allow you to find out which process is responsible for launching a file-less script. You can reach the wiki of this feature from [here](#).
- Create containment rules based on parent process. You can now create rules to contain applications if a parent process matches one specified in a rule. You can set how many levels of parent processes CCS should inspect.
- Containment rules now let you specify a 'File Rating' as an extra condition for 'Files Created by Applications' and 'Files Started by Processes'. This allows you to create even more granular rules than before, granting you additional control over your security policy.

Improvements

- Error messages caused by a missing local verdict database are no longer shown if CCS has only just been installed.
- Now, assigning a profile without Firewall section will not cause CCS to lose green/secure color. In addition, if you add and enable Firewall section in the profile later, the component is installed automatically.

Bug Fixes

- An issue with moving files to quarantine is fixed

Service Desk

New Features

- Added ability to assign staff to different departments. This allows you to classify your staff by different departments. You can find the wiki for this feature from [here](#)
- Detailed contract reports. The new reports grant you greater insight into the progress of all contracts in your organization. You can find the wiki for this feature from [here](#)
- Automated user registration. Instead of registering users after you create them, you can now automatically send them an activation email, or set a temporary registration password. You can find the wiki for this feature from [here](#)
- ‘First reply’ time. You can now view the response time of your staff to a ticket. You can find the wiki for this feature from [here](#)
- Thread filters. You can now filter threads inside a ticket by staff, client posts or internal notes. You can find the wiki for this feature from [here](#)
- Audit logs now record changes made in the ‘Alerts and Notices’ area (‘Admin Panel’ > ‘Settings’ > ‘Alerts and Notices’). You can find the wiki for this feature from [here](#)

Improvements

- Indexing on some tables has been improved in order to load pages quicker.

Bug Fixes

- Fixed issue on Microsoft Edge whereby some functionalities of Service Desk were not working properly.

C1 Portal

New Features

- cWatch EDR module added to the store. EDR is available for both MSP and Enterprise accounts.
cWatch EDR is a cloud-based endpoint detection and response solution that gives unrivalled visibility into what's happening in your environment.
cWatch EDR Benefits:
 - Dramatically increases threat visibility on your endpoints
 - Visualize the full attack chain
 - Protects against file-less attacks
 - Shows lateral movement of malicious files
 - Immediately alerts you about suspicious activities
- Added a 'What's New' notification box. The notification will show the top 5 features after you log into C1.

Improvements

- Health check has been done for C1 Portal microservices

Bug Fixes

- Mobile browser did not show ticket buttons inside of ticket details - (Safari).It has been fixed.

Comodo Quote Manager

New Features

- Added ability to delete quotes.

C1 Tools

Important Notice! - New version of Unknown File Hunter will be released at 18th June 2018

New Features

New version of 'Unknown File Hunter'. New features and improvements include:

- Brand new design.
- Ability to login as a guest user.
- You can now view all previous scans that you performed on the same endpoint.
- Specify email recipients for scan results.
- '% complete' rate is now shown during the file upload process.

Improvements

- Several performance improvements which mean you get faster verdicts on unknown files.
- Maximum size of Valkyrie uploads has been increased from 25 MB to 150 MB. This means UFH can now analyze more files, improving your ability to deliver security to endpoints and networks under your control.

C1 Mobile (Android)

New Features

- US region users are able to login to C1 Mobile now.
- Service Type selection is now available in C1 Mobile.

Bug Fixes

- Attachments on service desk tickets and email notifications are now available.
- Displaying notifications for the logged in user is fixed.
- Company copyright is updated.
- Validation error messages are updated with respect to missing field.
- Users can now attach files and photos on the service desk tickets.
- Comments to be added as optional fields.
- Saving billable hours is now fixed.
- Default department field is synchronizied with Service Desk portal.
- Category names are made consistent with Service Desk portal.
- Maximum file size is made consistent with Service Desk portal.
- Materials added via mobile app is now available on Material Details on Service Desk portal.

APPENDIX-1

New Client Versions:

- Windows Client - Communication 6.19.12672.18060
- Windows Client - Security 10.6.0.6727
- Windows Remote Control 6.19.12614.18060
- macOS Client - Communication 6.19.12726.18060
- macOS Remote Control 6.19.12609.18060