COMODO
Creating Trust Online®

Comodo
Client Security for Mac

Software Version 2.4

Quick Start Guide

Guide Version 2.4.071319

Comodo Client Security for Mac - Quick Start Guide

This tutorial explains how to use Comodo Client Security for Mac (CCS).

- **Install CCS**
- **Start CCS**
- **The main interface**
- **Scan and clean your computer**
- **Run an instant antivirus scan on selected items**
- **More help**

Install CCS

You can use the Endpoint Manager (EM) interface to deploy Comodo Client Security (CCS) to your endpoints. You can purchase EM as stand-alone application or as a part of the Comodo Dragon or Comodo One platform.

This section covers how to:

- **Subscribe for Endpoint Manager**
- **Enroll users**
- **Add devices**
- **Deploy CCS on Mac endpoints**

Skip to straight to **Deploy CCS** if you have already completed the first three steps.

Subscribe for Endpoint Manager

You can purchase Endpoint Manager as stand-alone application or as part of the Dragon / Comodo One suite:

- Dragon / C1 -
  - Sign up for Dragon at **https://platform.comodo.com/signup** or C1 at **https://one.comodo.com/signup**
  - After sign-up, login to the portal then click 'Applications > 'Endpoint Manager'.
- Stand-alone Endpoint Manager
  - Visit **https://secure.comodo.com/home/purchase.php?pid=98&license=try** for the trial version or **https://secure.comodo.com/home/purchase.php?pid=98** for the full version.
  - After sign-up, you can access your Endpoint Manager at the URL provided during setup.

Enroll Users

You must add users to Endpoint Manager before you can install CCS on your endpoints.

- **Dragon MSP / Comodo One MSP customers** - You can create multiple companies in the Dragon / C1 interface, and can enroll users to any of these companies.
- **Dragon Enterprise / C1 Enterprise and stand-alone Endpoint Manager customers** - All users are enrolled to the default company.
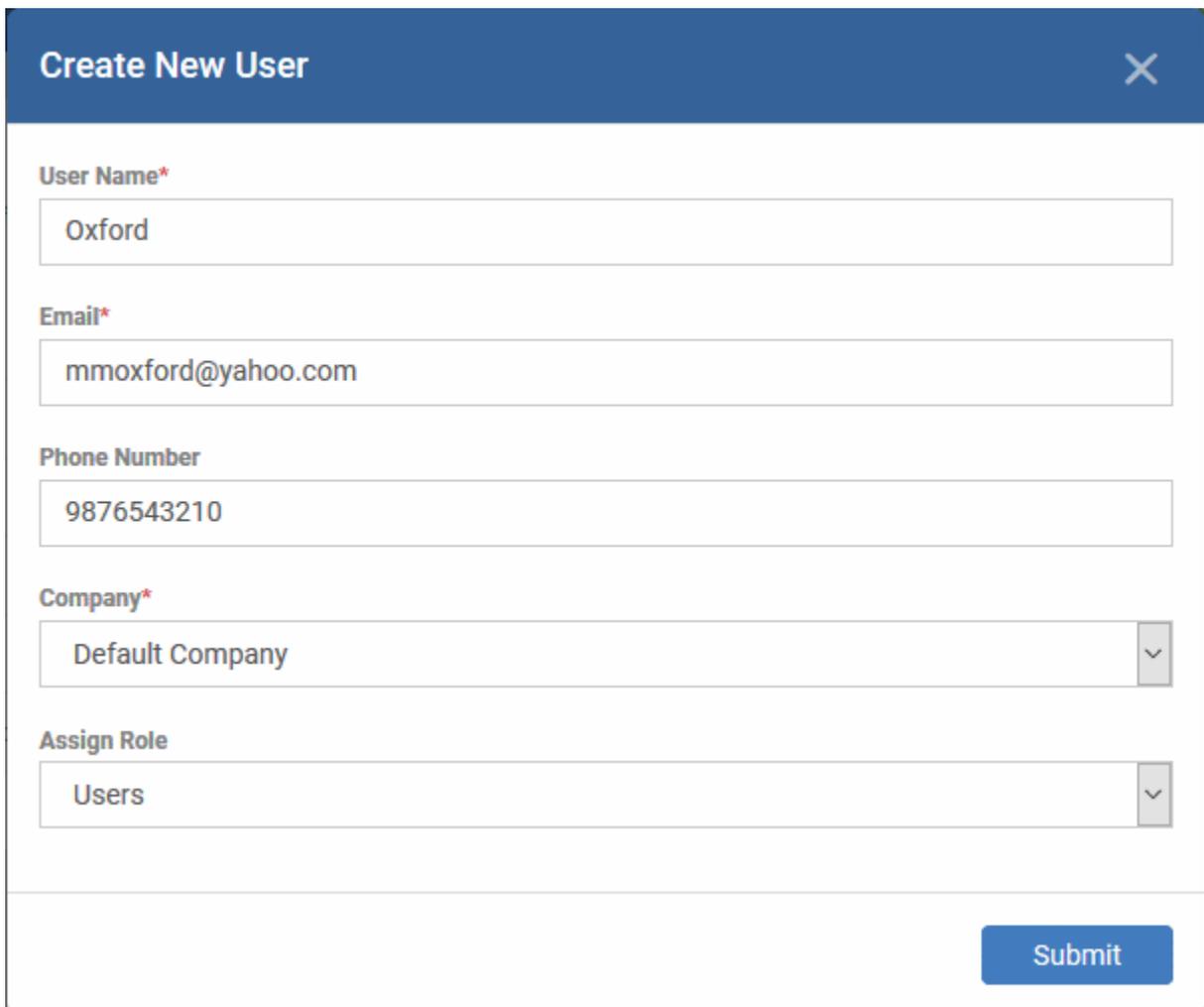
Add a user

- Open Endpoint Manager
- Click 'Users' > 'User List'

- Click 'Create User'

  or

- Click the 'Add' button on the menu bar and choose 'Create User'.
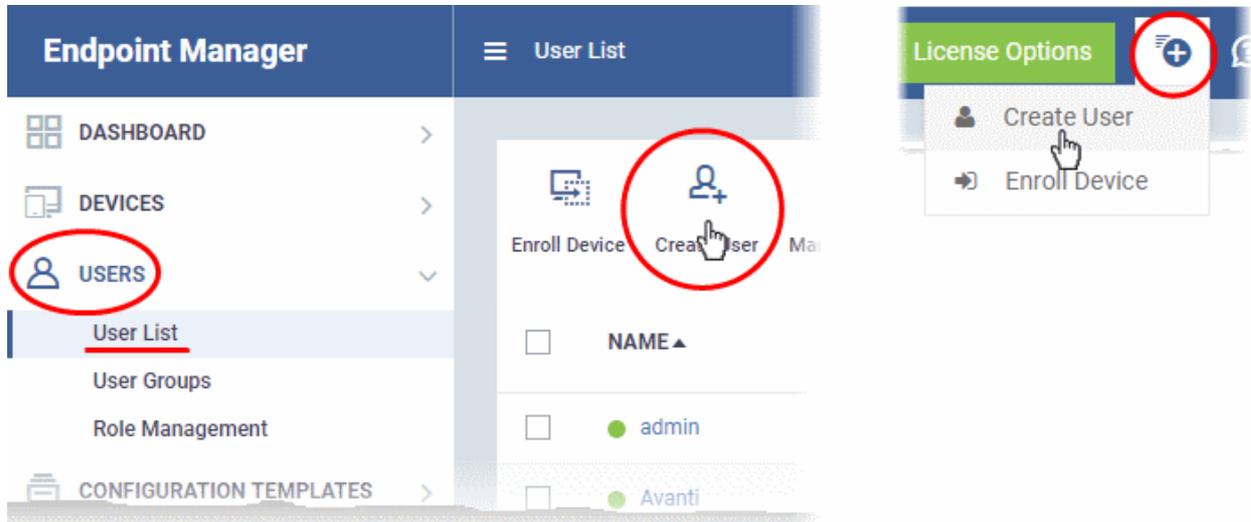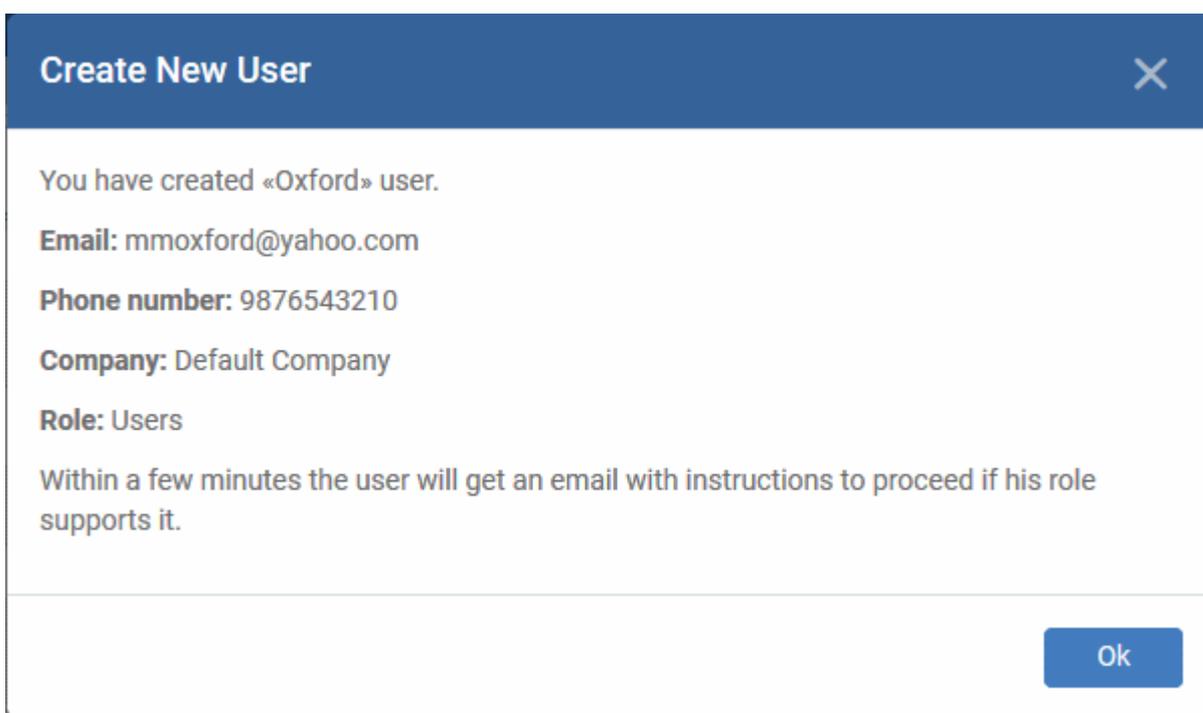

Complete all mandatory fields on the new user form:

- **User Name** - Enter the login username of the user. They will appear under this name in the EM interface.
- **Email** - Account and device activation mails will be sent to this address.
- **Phone Number** - The contact number of the user.
- **Company** – The organization to which you want to add the user.
  - Dragon MSP and C1 MSP customers can add users from companies/organizations enrolled in their account.
  - Dragon Enterprise, C1 Enterprise, and EM stand-alone customers can only add users to the default company.
- **Assign Role** - A role determines user permissions within the Endpoint Manager console itself. EM ships with two default roles:
  - **Administrators** - Full admin privileges in the EM console. The permissions for this role are not editable.
  - **Users** - In most cases, a user will simply be an owner of a managed device who should not require elevated privileges in the management system. Under default settings, 'Users' cannot login to Endpoint Manager.
- Click 'Submit' to add the user to Endpoint Manager.

You should see the following confirmation message:

Create New User ✕

You have created «Oxford» user.

Email: mmoxford@yahoo.com

Phone number: 9876543210

Company: Default Company

Role: Users

Within a few minutes the user will get an email with instructions to proceed if his role supports it.

Ok

- Repeat the process to add more users.
- New users will be listed in 'Users' > 'User List'

Tip: You can also import a list of users from a .csv file, and bulk enroll users/endpoints from Active Directory (AD). See **https://help.comodo.com/topic-399-1-786-10125-Create-New-User-Accounts.html** if you want to learn more about these options.

Enroll Devices

The next step is to add devices which belong to your users. Afterwards, you can manage the devices using Endpoint Manager.
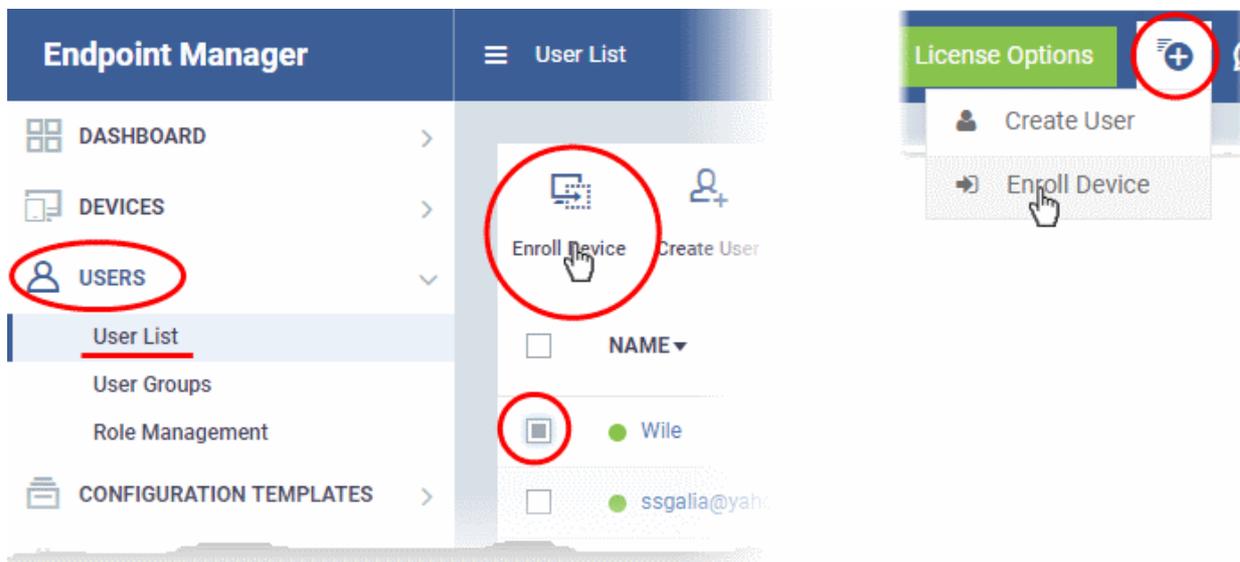
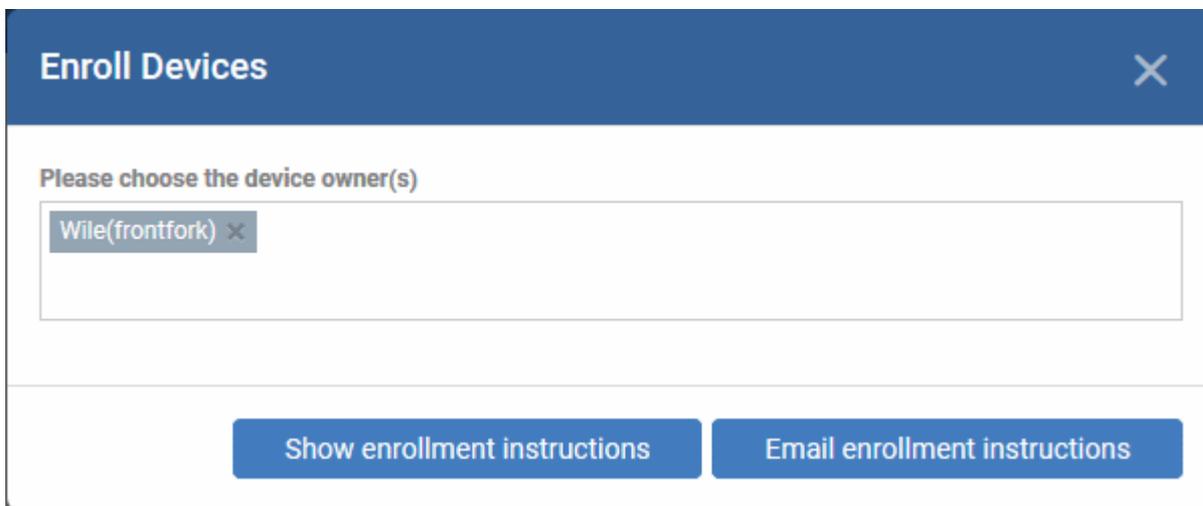**Enroll devices**

- Click 'Users' > 'User List'

- Select users for whom you want to enroll devices
- Click the 'Enroll Device' button above the table

   OR

- Click the 'Add' button on the menu bar and choose 'Enroll Device'.


The 'Enroll Devices' dialog will open:

The device owners field is pre-populated with the users you selected in the previous step.

- To add more users, start typing first few letters of their username and choose from the results
- **Show Enrollment Instructions** - Displays enrollment advice in a pop-up. Useful for admins who want to enroll their own devices.
- **Email Enrollment Instructions** – Will send device enrollment instructions to all selected users. Users must enroll their own devices by following the instructions in the email. The following confirmation is shown after clicking this button:
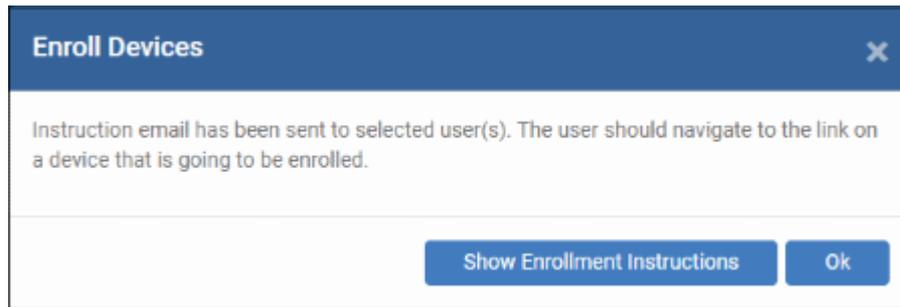
An example mail is shown below:
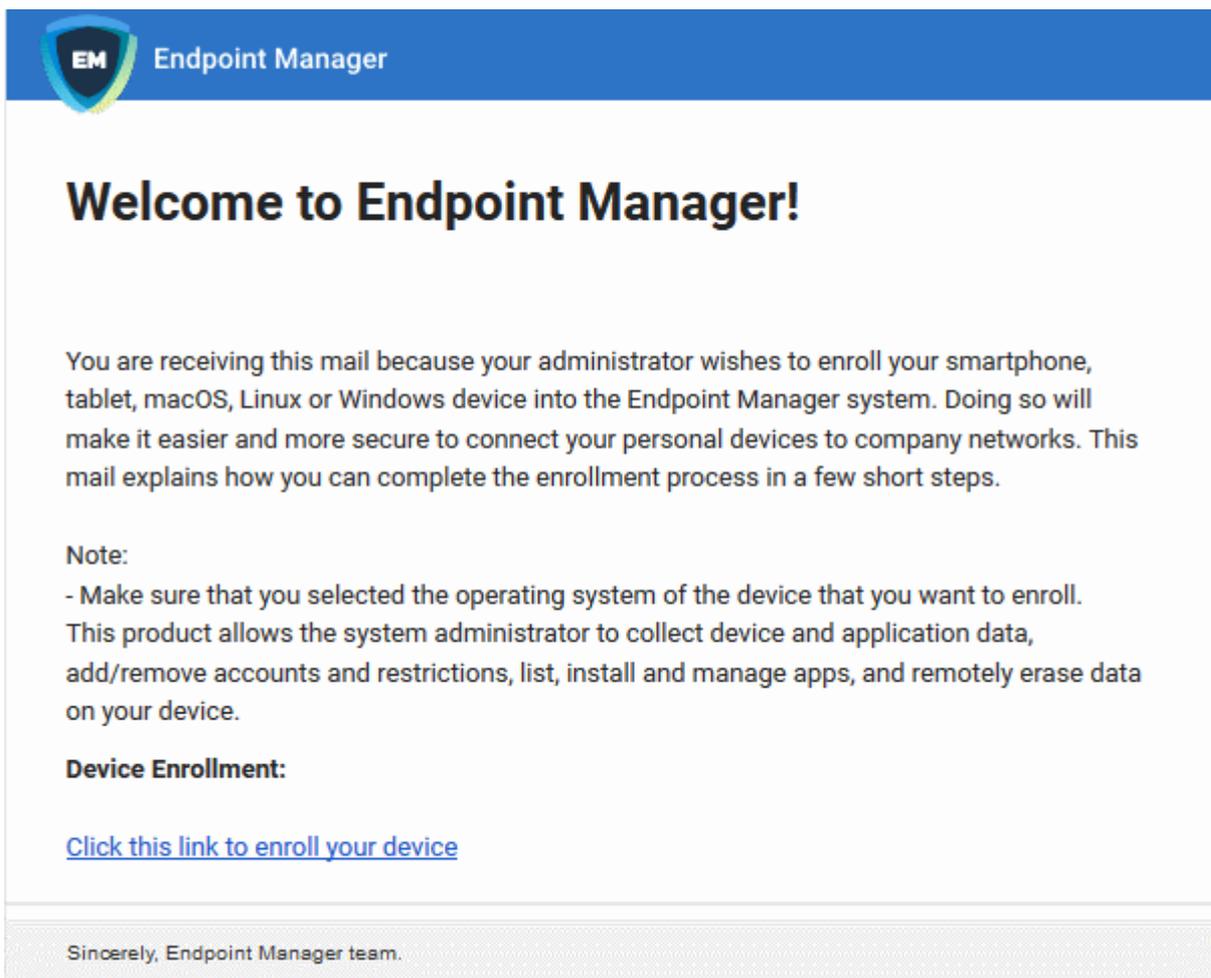
- • The link takes the user to a page which lets them download the communication client and profile:
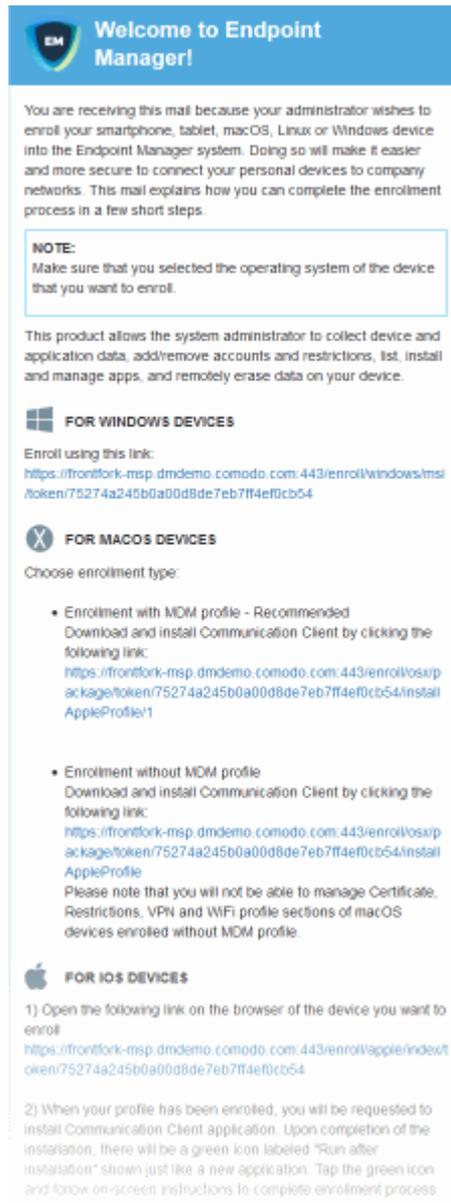
You can add MAC devices either with or without installing the Endpoint Manager (EM) profile.

- Background - Apple only allow one portal to manage network features on a MAC device. This causes issues with customers who want to use Endpoint Manager in conjunction with another management platform.

- 'Profile-less' enrollment lets you use EM to manage security/remote control while using another platform for general Mac management.

- However, you cannot use EM to manage certain items if you use profile-less enrollment. See the following table for details:
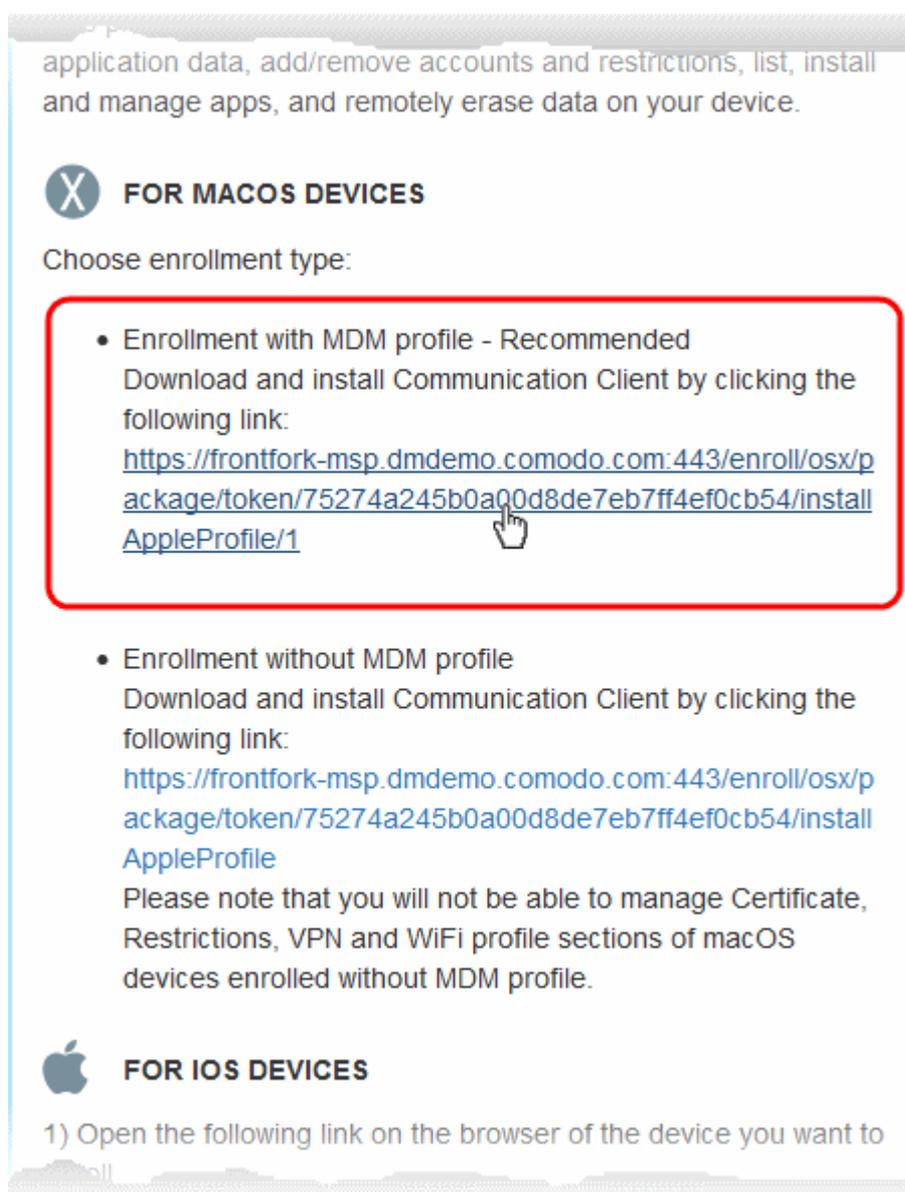
Enroll with MDM Profile	'Profile-less' enrollment
Use Endpoint Manager to manage: • Antivirus Settings • Remote Control Settings • Valkyrie Settings • Certificates	Use Endpoint Manager to manage: • Antivirus Settings • Remote Control Settings • Valkyrie Settings

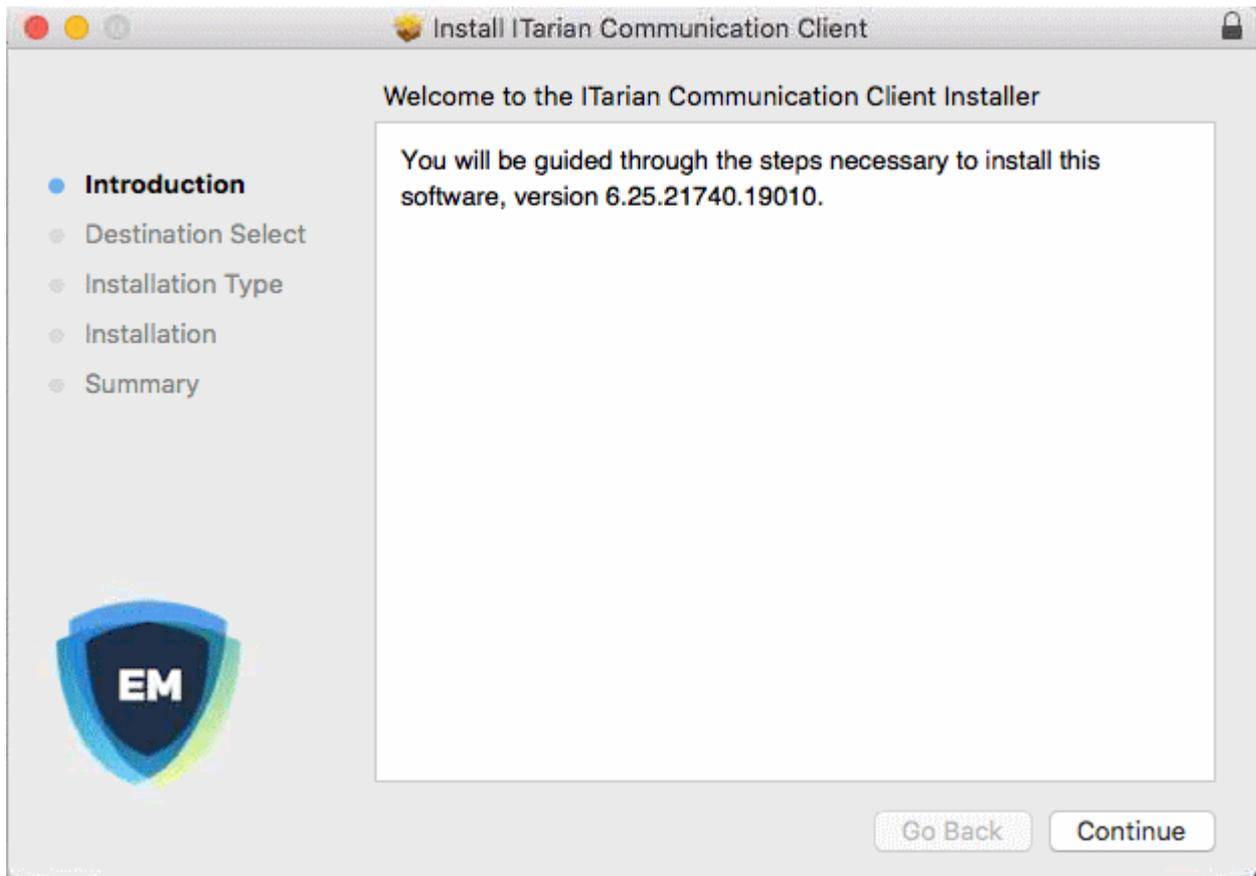| • Restrictions • VPN • Wi-Fi	

- Click the following links for help with either method:

    - **Enroll with MDM Profile**

    - **Enroll without MDM Profile**

Enroll with MDM Profile

- Users should open the mail on the device you want to enroll

- They should scroll to the 'FOR MAC OS DEVICES' section.

- Click the 'Enrollment with MDM profile' link:

This will start the installation wizard:

- The user follows the wizard and completes the installation.
- The device profiles screen appears when installation is complete:

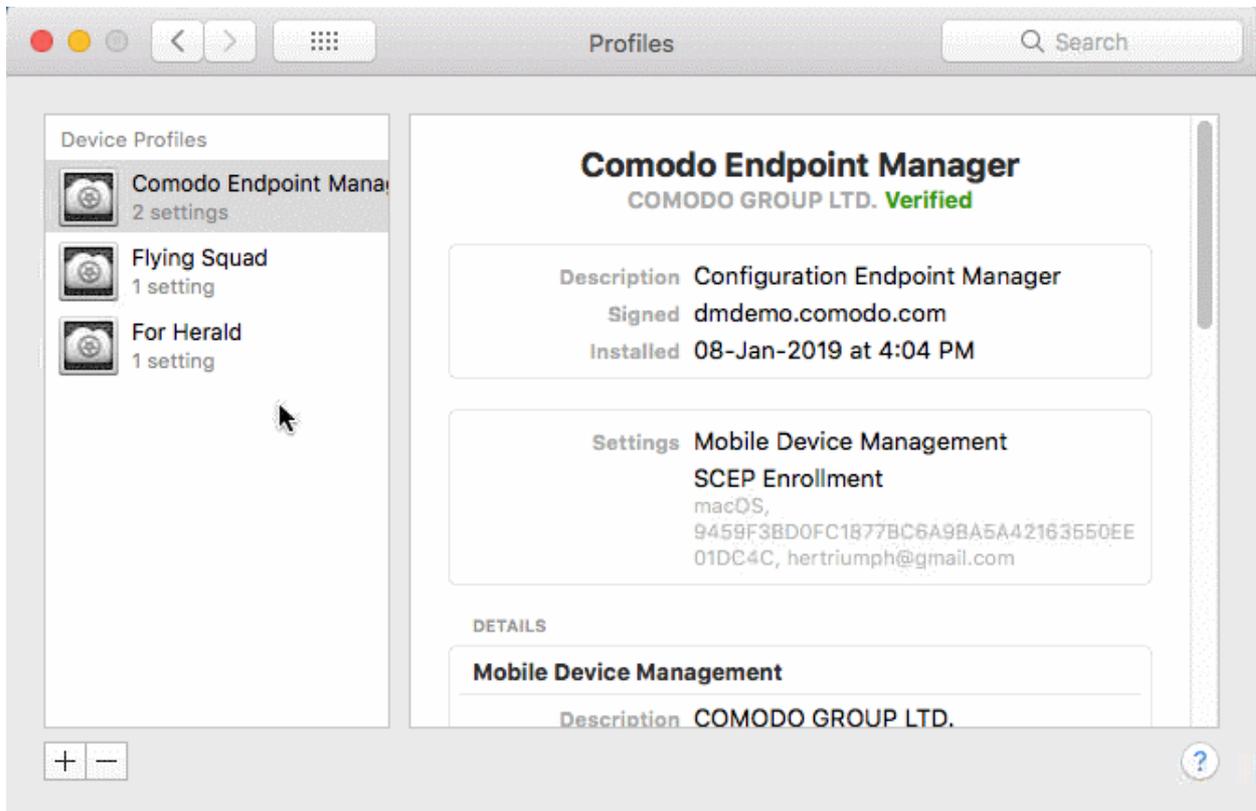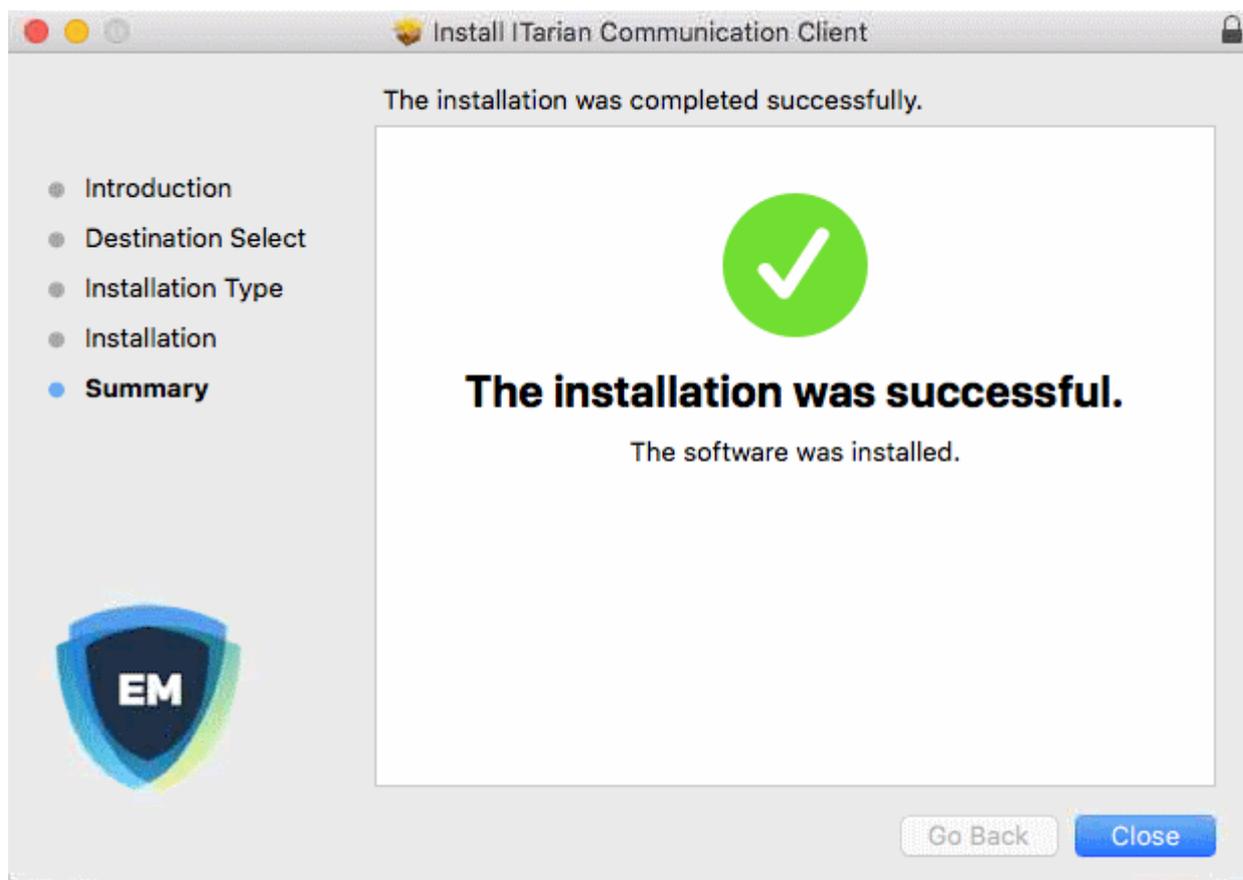The client will connect to the EM server:

Enroll without MDM Profile

• Users should open the mail on the device you want to enroll

• They should scroll to the 'FOR MAC OS DEVICES' section.

• Click the 'Enrollment without MDM link:

application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

X FOR MACOS DEVICES

Choose enrollment type:

- Enrollment with MDM profile - Recommended
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile/1

- Enrollment without MDM profile
  Download and install Communication Client by clicking the following link:
  https://frontfork-msp.dmdemo.comodo.com:443/enroll/osx/package/token/75274a245b0a00d8de7eb7ff4ef0cb54/installAppleProfile
  Please note that you will not be able to manage Certificate, Restrictions, VPN and WiFi profile sections of macOS devices enrolled without MDM profile.
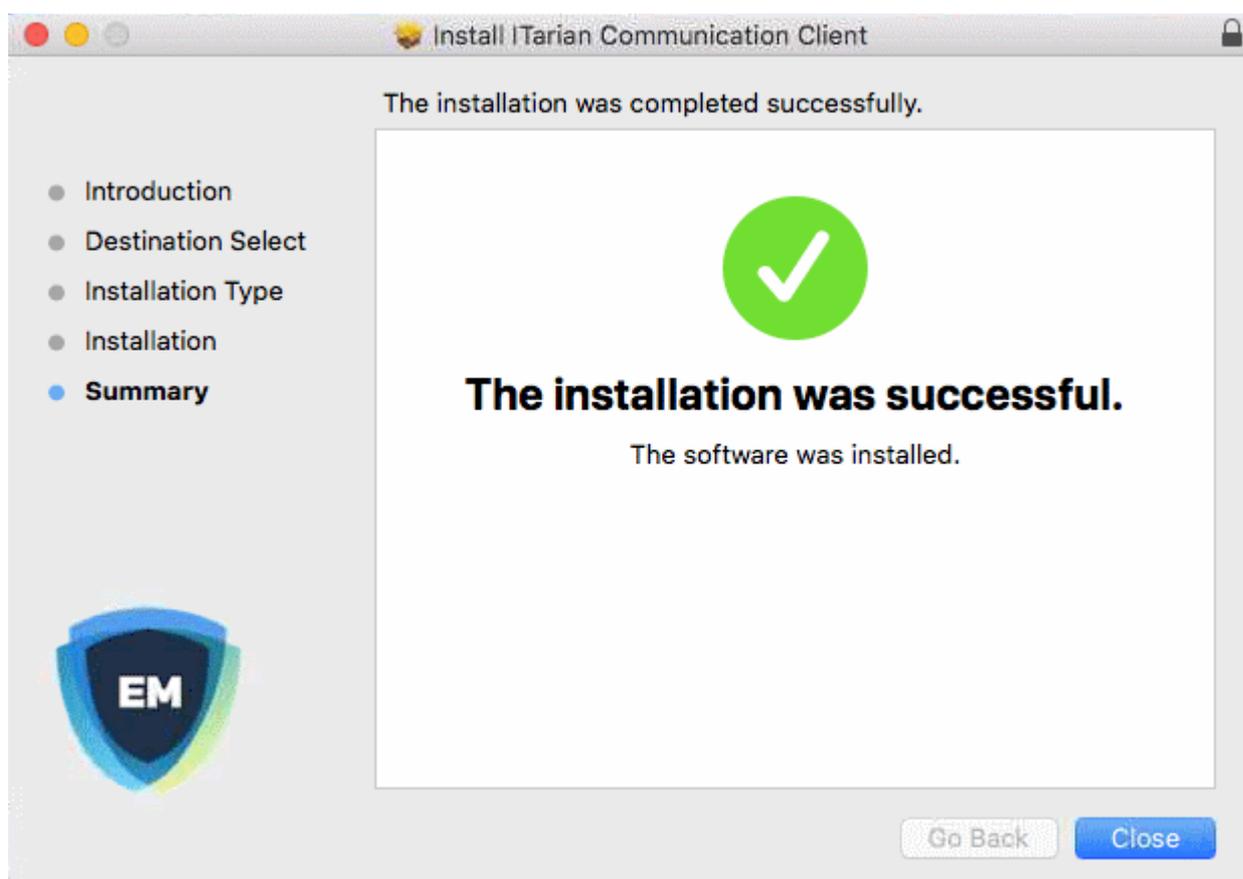
 FOR IOS DEVICES

1) Open the following link on the browser of the device you want to

This will start the installation wizard for the communication client:
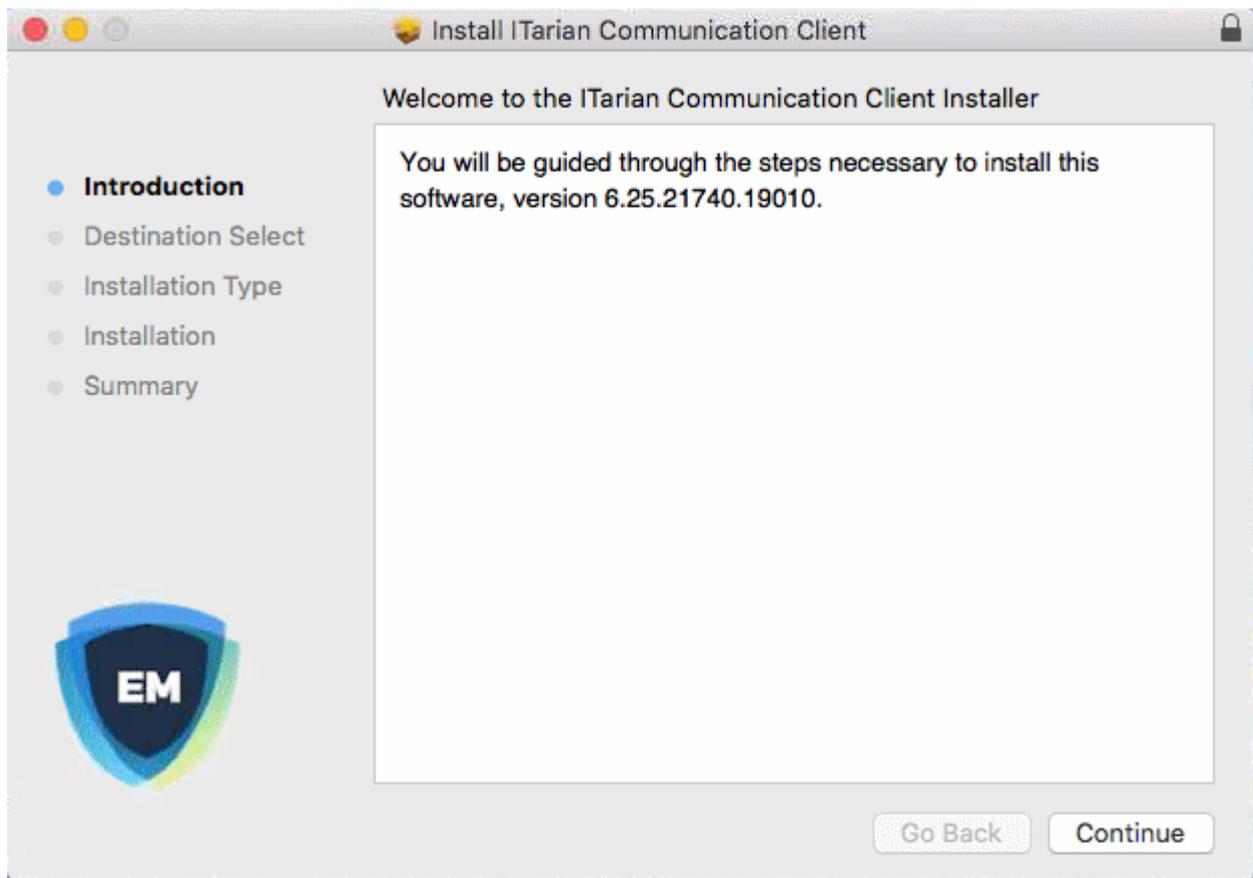
- The user follows the wizard and completes the installation.
- Once installation is complete, the client starts communicating with the EM portal.
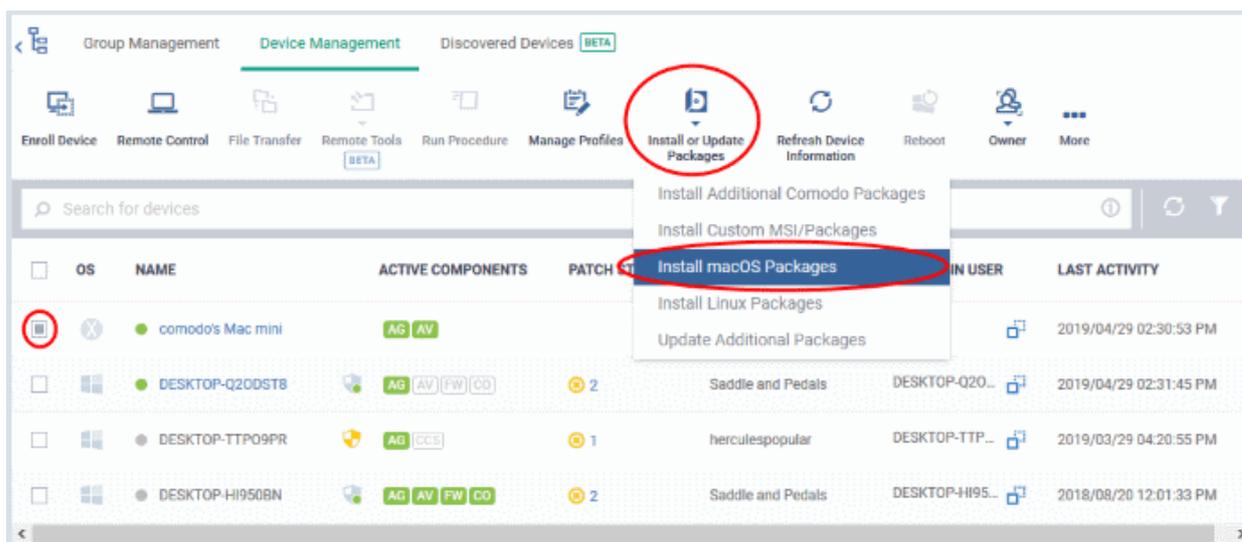
Deploy Comodo Client Security

Note - Please uninstall any other antivirus products from target endpoints before proceeding. Failure to do so could cause conflicts that mean CCS will not function correctly.

Install CCS

- Log into Dragon / Comodo One

- Click 'Applications' > 'Endpoint Manager'

- Click 'Devices' > 'Device List'

- Click the 'Device Management' tab

  - Click the funnel icon on the right and select 'MacOS', to see only Mac OS endpoints
  - Click 'All Devices' to view every device in Endpoint Manager

- Select your target Mac devices using the check-boxes on the left

- Click 'Install or Update Packages':

- Select 'Install macOS Packages' from the drop-down.
- Choose 'Install Comodo Client - Security'
- Click 'Install':
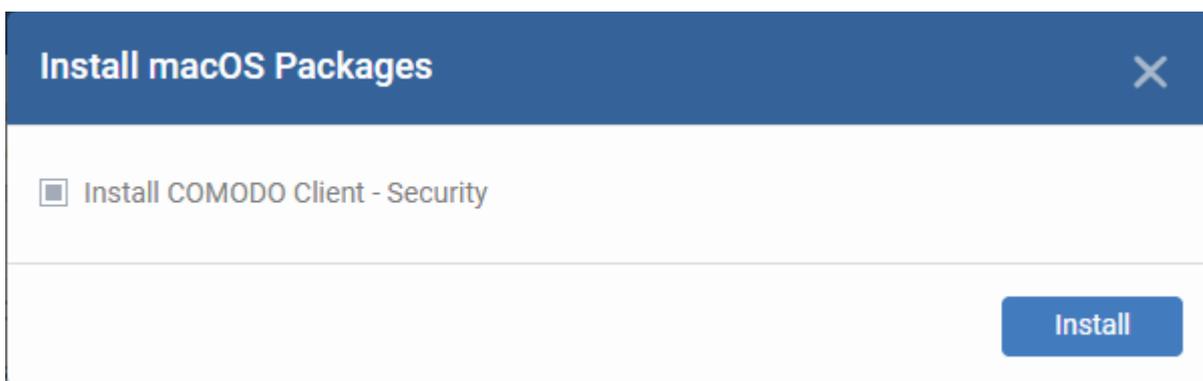
- A command will be sent to target endpoints to install CCS
- The EM agent on the endpoint will download and install CCS

The application will become effective immediately after installation.

- You can configure CCS settings in the EM profile which is applied to the endpoint.
- See **https://help.comodo.com/topic-399-1-786-10854-Profiles-for-Mac-OS-Devices.html** for more details on this.

Start CCS

- After installation, CCS will automatically start up when the endpoint boots.
- The real-time virus monitor is enabled by default, so endpoints are protected immediately after the restart.
- **Important** - We recommend admins configure CCS via an Endpoint Manager profile rather than locally.
  - Log into 'Endpoint Manager' > Click 'Configuration Templates' > 'Profiles' > open a Mac OS profile > Click the 'Antivirus' tab.
- However, you can also configure the application at a local machine should you wish. The rest of this guide addresses how to use the application locally.
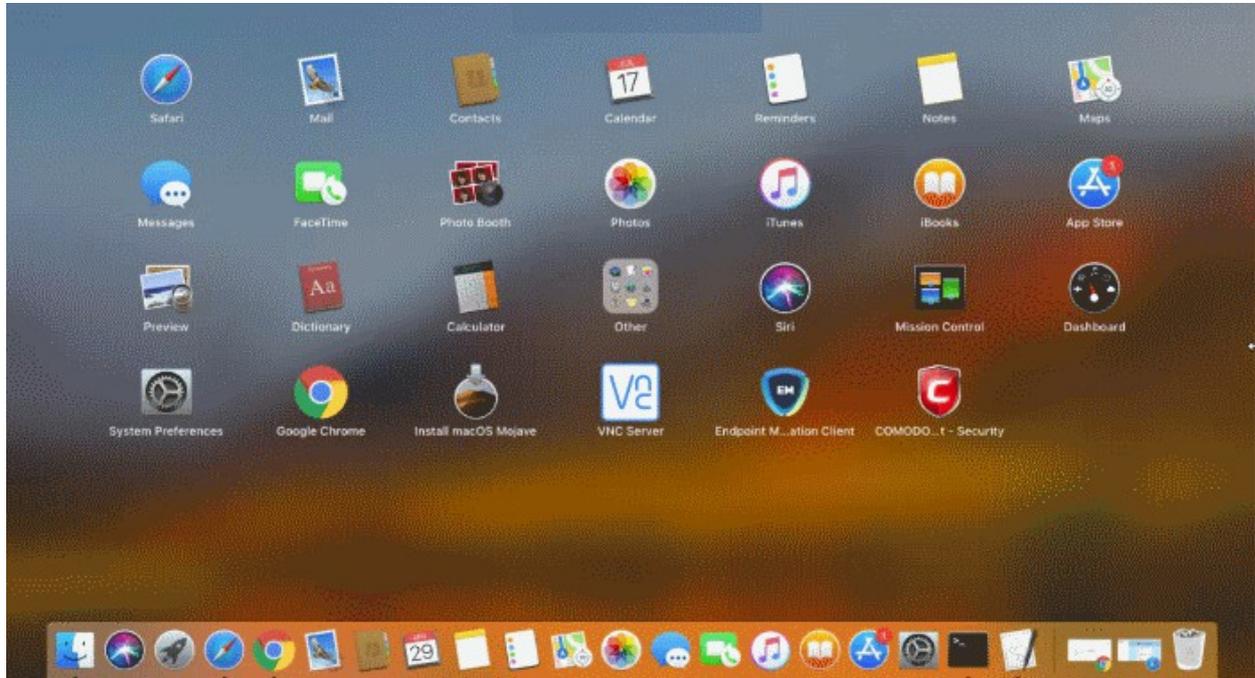
You can access the management interface in the following ways:

- **Launch Pad**
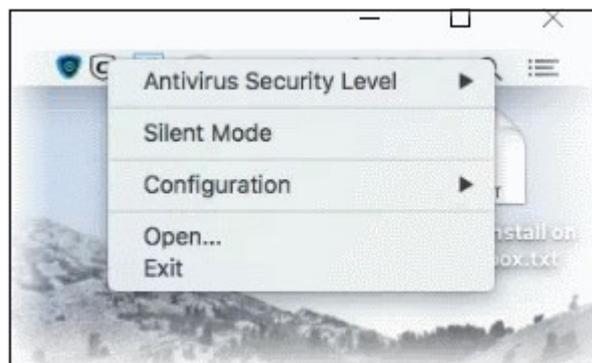
- **Task bar icon**
- **Dock icon**

Launchpad

- Open the launchpad on your Mac device

- Click the Comodo Client Security icon to open the application

Taskbar icon

The taskbar (top-right) lets you open the application, enable/disable real-time scanning, switch to silent mode, and manage your CCS configurations.

- **Antivirus Security Level** – Enable or disable the real-time virus monitor:
  - **On Access** - Any file opened is scanned before it is allowed to run.
  - **Disabled** - Switches the real-time scanner off.
- **Silent Mode** - Temporarily disable alerts so they don't interrupt you when running a full screen presentation or playing a game. Protection remains enabled.
- **Configuration** - Create, import and export CIS security configurations. This is useful if you want to implement specific settings on multiple endpoints.
- **Open**... - Open the CCS main interface.

- Click 'Open' to launch the application.

Dock Icon

- Use the quick launch icon on the MAC OS dock to open the interface at any time:

Tip: You can scan a file or folder by simply dragging it onto the CCS dock icon. If the icon is not present, you can add it as follows:

- Click the 'Finder' icon on the Dock

- Click 'Applications' on the left menu

- Click, hold and drag 'Comodo Client Security' icon onto the dock.
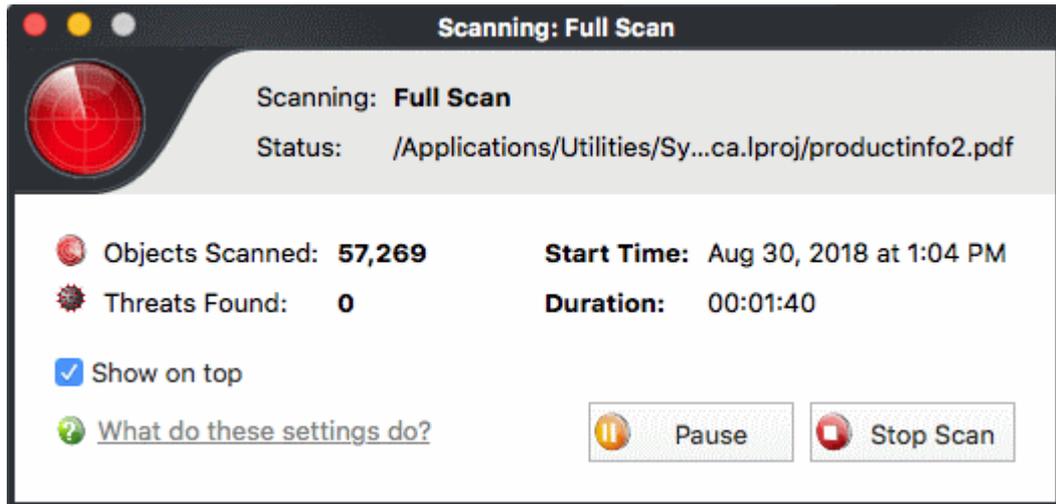

The summary screen opens:
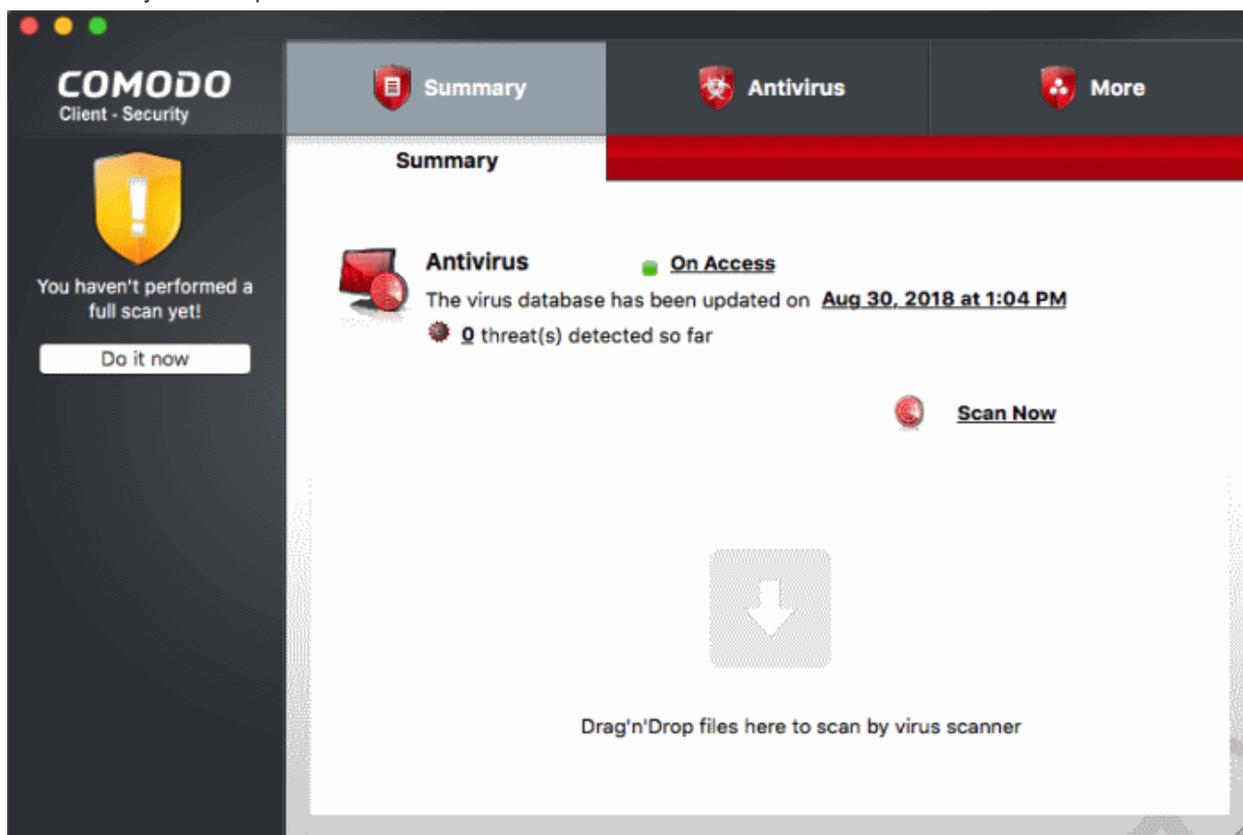
- Click 'Do it now' to run your first full computer scan.

Before running the scan, CCS will first check for AV database updates. If updates are available they will be downloaded and installed.
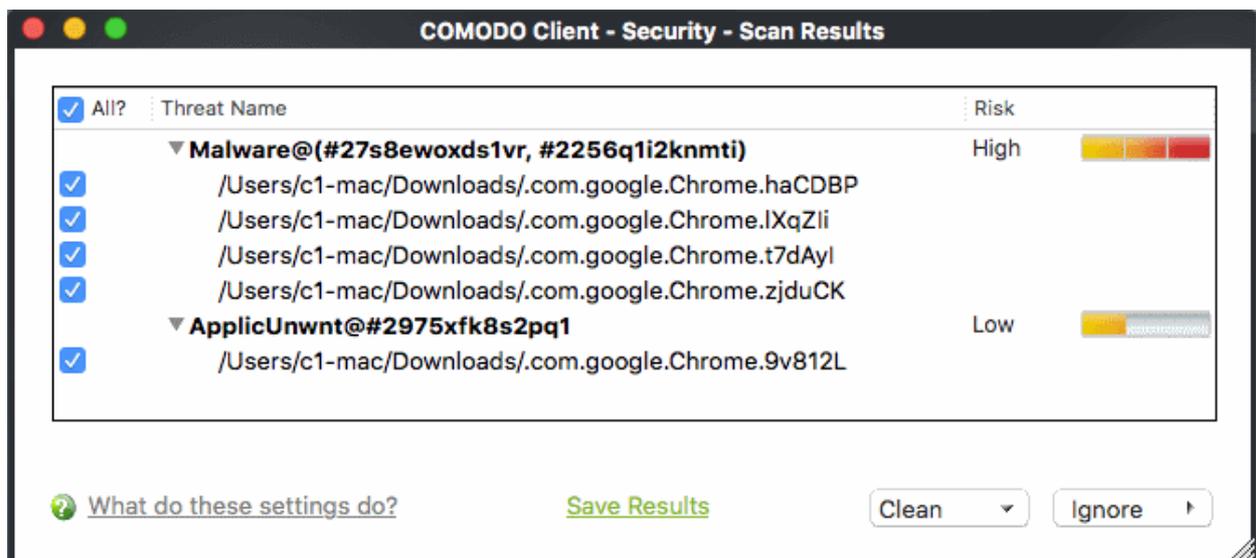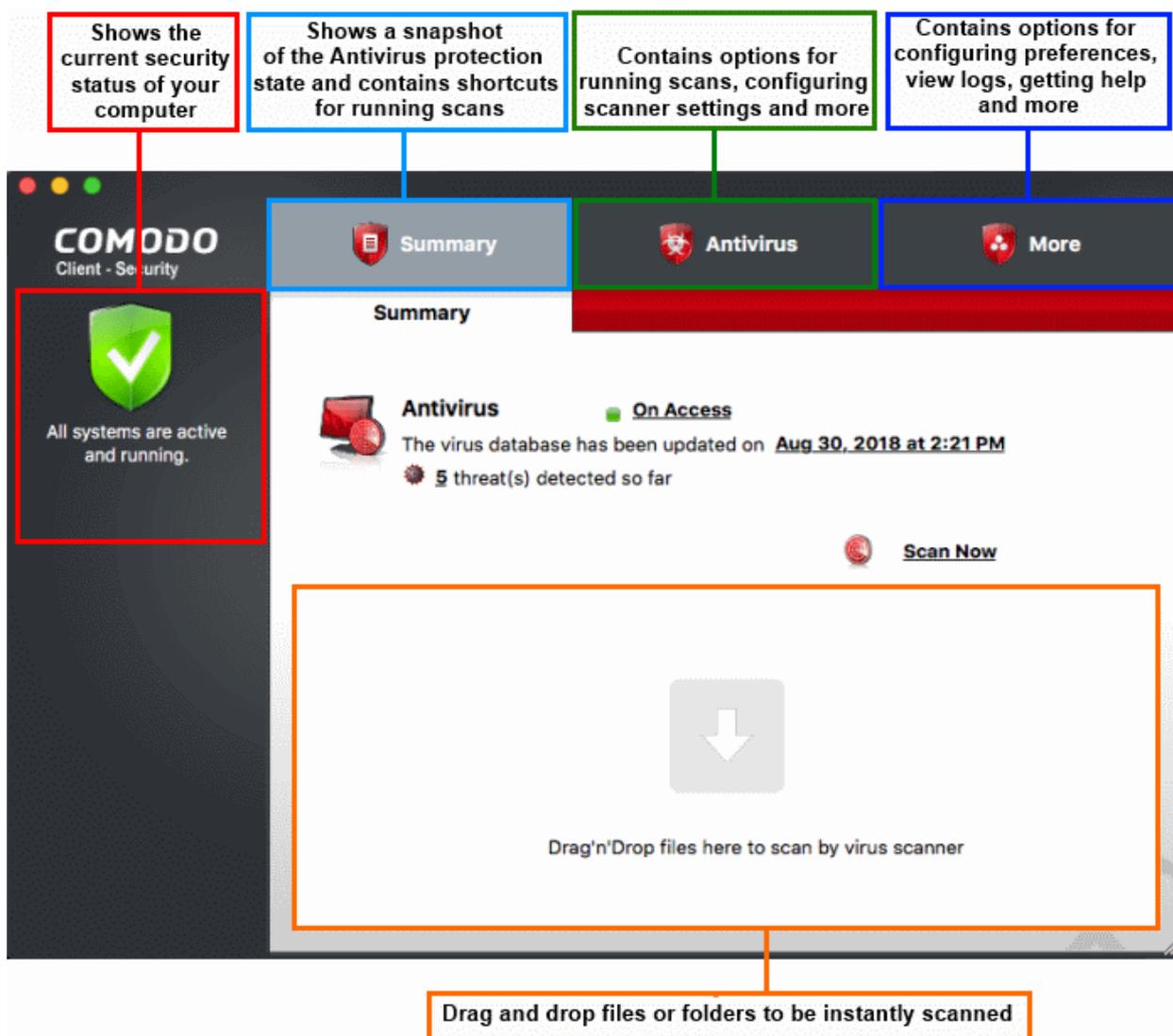
The scan will commence after the update:

Once the scan is complete, the results window opens:

- The results window lists all threats discovered by the scan. You can remove selected threats or choose to ignore them:

See **Scan and Clean Your Computer** for more details.

The Main Interface

System Status

- The shield icon on the left shows the current protection level. There are four statuses: yellow, green, red and blue

  - **Yellow** – There are actions you need to take. For example, because you need to run a full scan or because the real-time scanner is switched off.

  - **Green** - All systems are active and running.

  - **Red** - Serious security risks. For example, threats have been found on the computer, or the Endpoint Manager agent is not running.

  - **Blue** - Silent mode is active. Alerts are temporarily disabled.

The tabs along the top of the screen let you configure different aspects of CCS:

- **The 'Summary' tab**
- **The 'Antivirus' tab**
- **The 'More' tab**

The 'Summary' tab

The summary tab contains two areas:

- Antivirus Summary
- Drop Files to Scan

Antivirus Summary

The antivirus summary box shows:

i. **Scanner status** - Shows whether the 'always-on' virus monitor is active or not. Possible options are:

- On Access: Real-time protection is enabled. All files you open or download are scanned before they are allowed to open.
- Disabled: Real-time protection is switched off.

- Click the status to configure real-time protection. See **https://help.comodo.com/topic-399-1-924-12500-Real-Time-Scan.html** for more details.

ii. **When the Virus Database was Last Updated**

The day and time at which the virus database was most recently updated.

- Click the date/time to start the the database update. See **https://help.comodo.com/topic-399-1-924-12486-Update-Virus-Database.html** for more details

iii. **Number of Detected Threats**

- Click the <number of threats> to open the 'Antivirus Events' panel. For more details, see **https://help.comodo.com/topic-399-1-924-12481-View-Antivirus-Events.html**.

iv. **Scan Now**

Click the 'Scan Now' link to start an **on-demand scan**.

Fast scans

Drag a file, folder or drive into the scan box on the 'Summary' screen.

The 'Antivirus' tab

The Antivirus tab contains links for various tasks:

- Run a scan - Launch an on-demand scan on an item of your choice.
- Update Virus Database - Manually check for the virus database and download updates
- Scheduled Scans - Timetable virus scans according to your preference. You can configure scheduled scans to scan your entire computer or specific areas.
- Quarantined Items - View threats which were moved to quarantine. Quarantined files are encrypted and cannot be run.
- Scan Profiles - Create and manage custom profiles to scan specific folders, drives or areas.
- Scanner Settings - Configure settings for real-time scans, manual scans and scheduled scans. You can also configure exclusions.

The 'More' Tab

The 'More' tab gives you access to the following:

- Preferences – Configure general CCS settings (interface language, log storage, update options and so on)
- Manage My Configurations - Manage, import and export CCS security settings as configuration profiles.
- Diagnostics – Identifies any problems with the CCS installation.
- Check For Updates - Launches the CCS program updater.
- Browse Support Forums - Links to Comodo User Forums.

- Help - The online help guide.

- About - Version and copy-right information about the product.

- View Logs - Launches the 'Log Viewer' module that displays the logs generated during real-time protection, after running an update, and for various other events.

Scan and Clean Your Computer

- The 'Run a Scan' area lets you launch an on-demand scan on an item of your choice.

- The item can be anything you choose - your entire computer, a specific drive or partition or even a single file.

- You can also scan a wide range of removable storage devices, such as external hard-drives, USB sticks and more.

Run an on-demand virus scan

- Open Comodo Client Security

- Click the 'Antivirus' tab

- Click the 'Run a Scan' box

Next, choose the type of scan you want to run:
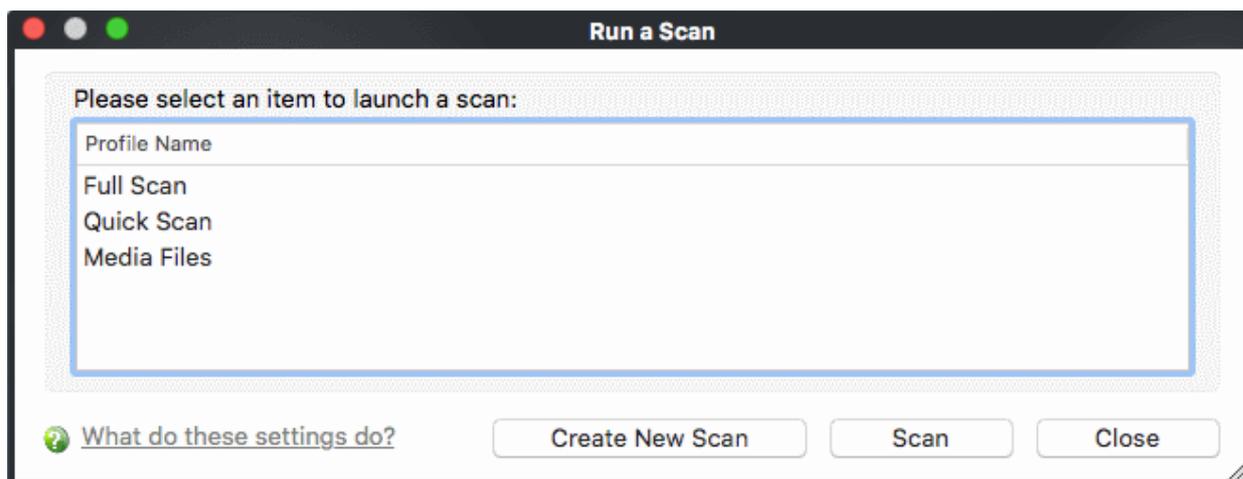
- CCS ships with two pre-defined scan profiles - 'Full Scan' and 'Quick Scan'. These cannot be edited or removed:

    - **Full Scan** - Scans every drive, folder and file on your system, including external connected devices.

    - **Quick Scan** - Scans important operating system files, system memory, auto-run entries, registry keys and hidden services.

    - **Create New Scan** – Create your own custom scan of specific files, folders or drives. See **Create a custom scan profile** if you need more details.

Click 'Scan' after making your selection (or just double-click the profile name).

Custom Scan

You need to create a scan profile in order to run a custom scan. Once created, you can re-run the scan in future.

- Open Comodo Client Security

- Click the 'Antivirus' tab

- Click the 'Run a Scan' box

- Click 'Create New Scan'
- Type a name for your new profile. For example, 'My External Drives'.
- Click 'Add' to choose files, folders or drives you want to include in the profile
- Repeat the process to add multiple items
- Click 'Apply'. Your new profile will be listed in the 'Run a Scan' dialog
- Select your new profile in the list and click 'Scan'
- Next, see:
  - **Scan progress and results**
  - **Create a custom scan profile**
  - **Instantly scan items**

Tip: If you just want to scan a file or folder, you can just drag it into the scan box in the 'Summary' area.

Scan Progress and Results

Before running the scan, Comodo Client Security will first check for AV database updates. If updates are available they will be downloaded and installed.
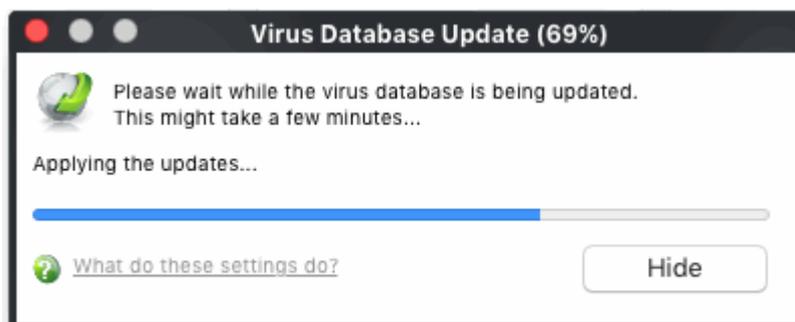
The scan, based on the profile you selected, will begin immediately.

The progress dialog shows the profile name, the location that is currently being scanned, the start time and duration of the scan, the total number of objects scanned so far and the number of threats found.
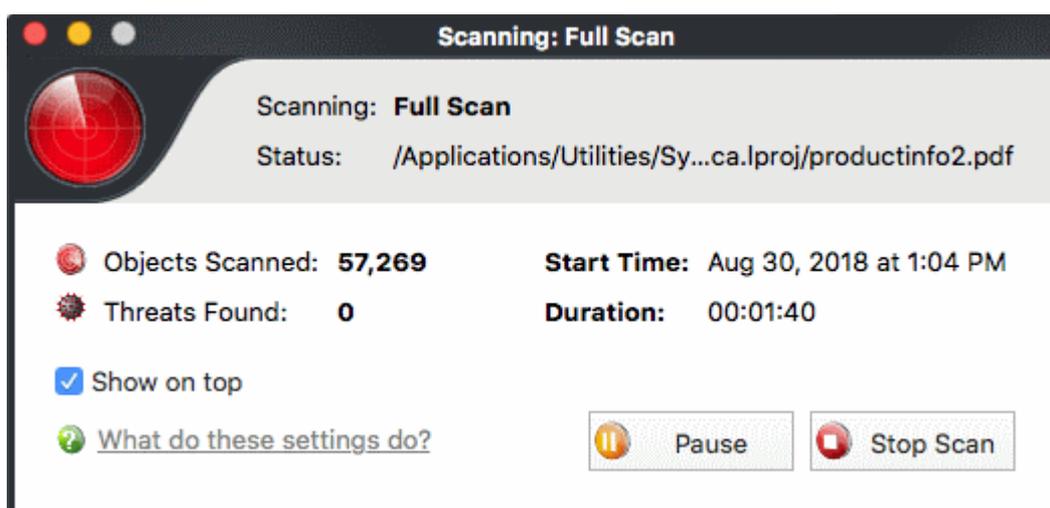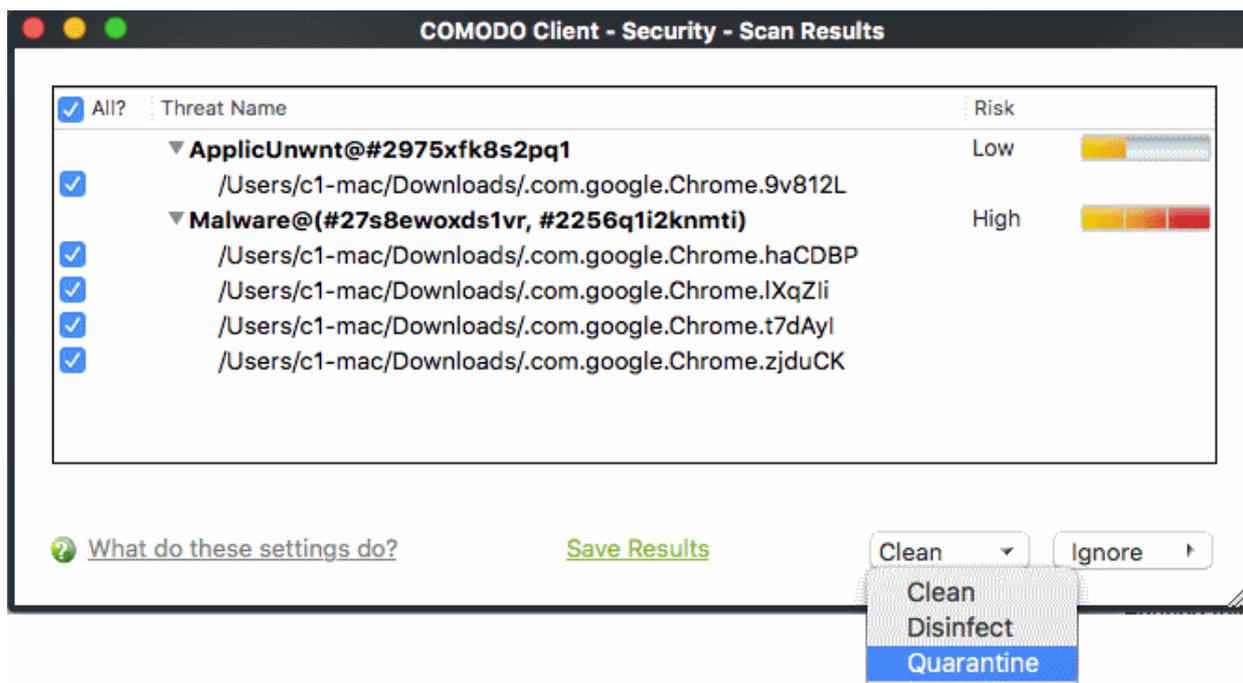

- Click 'Pause' to suspend the scan
- Click 'Resume' to recommence scanning
- Click 'Stop Scan' to abort the scan process altogether.

Once the scan is complete, the results window opens:

- The results window lists all threats discovered by the scan and provides controls which let you deal with the

them:

- Click the 'Threat Name' column header to sort results in alphabetical order
- Click the 'Risk' column header to sort results by risk level
- Select 'All' if you want to apply 'Clean' or 'Ignore' actions to every threat.

  Save Results - Save the scan results as a text file.

  Clean – There are three options to deal with an infected file:

  - **Clean** – The selected items will be completely deleted from your computer
  - **Disinfect** - If a disinfection routine exists, CCS will remove the infection and retain the original file. If no disinfection routine exists, CCS will move the file to quarantine.
  - **Quarantine** – Moves the selected files to quarantine. Files moved in this way are encrypted and not allowed to run. You can view the files at a later time, and choose to delete or restore the file to its original location. See **https://help.comodo.com/topic-399-1-924-12487-Quarantined-Items.html** for more details.

  Ignore - Two options:

  - **Once** - The file is removed from the threat results. The file isn't, however, added to the list of exclusions. The file will be detected as a threat again by the next scan.
  - **Add to Exclusions** - The file is moved to the exclusions list. CCS will skip this file in future scans and not consider it to be a threat.

Create a Scan Profile

'Scan Profiles' let you set up custom scans on specific areas on your system. Scan profiles can be run on-demand at any time.

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Run a Scan'
- Click the 'Create New Scan' button

OR

- Open Comodo Client Security

- Click the 'Antivirus' tab

- Click 'Scan Profiles'

- Click the 'Add' button in the scan profiles dialog
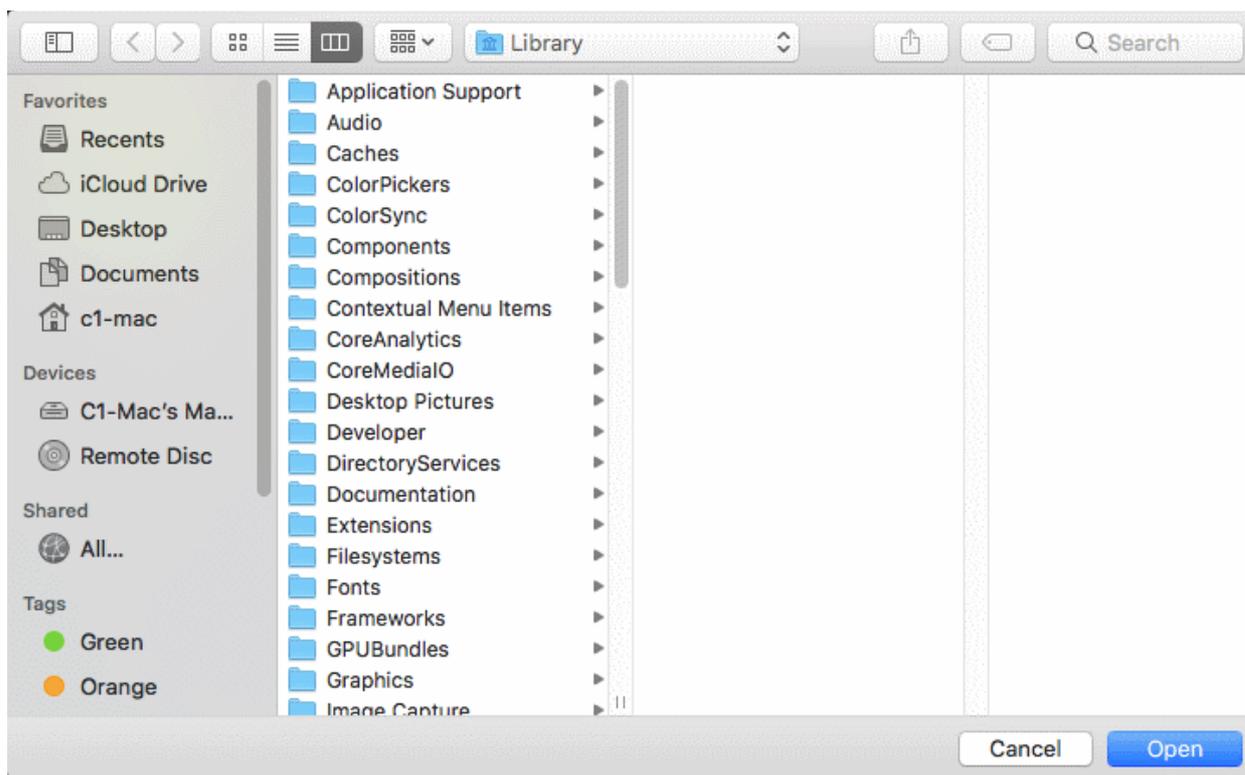
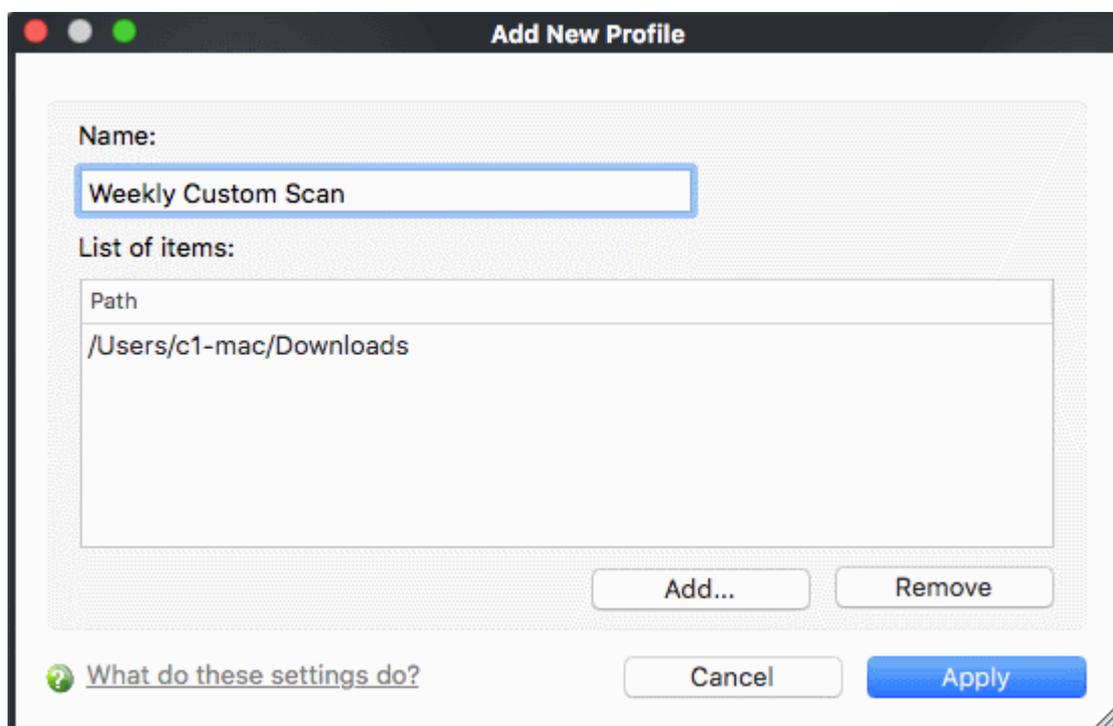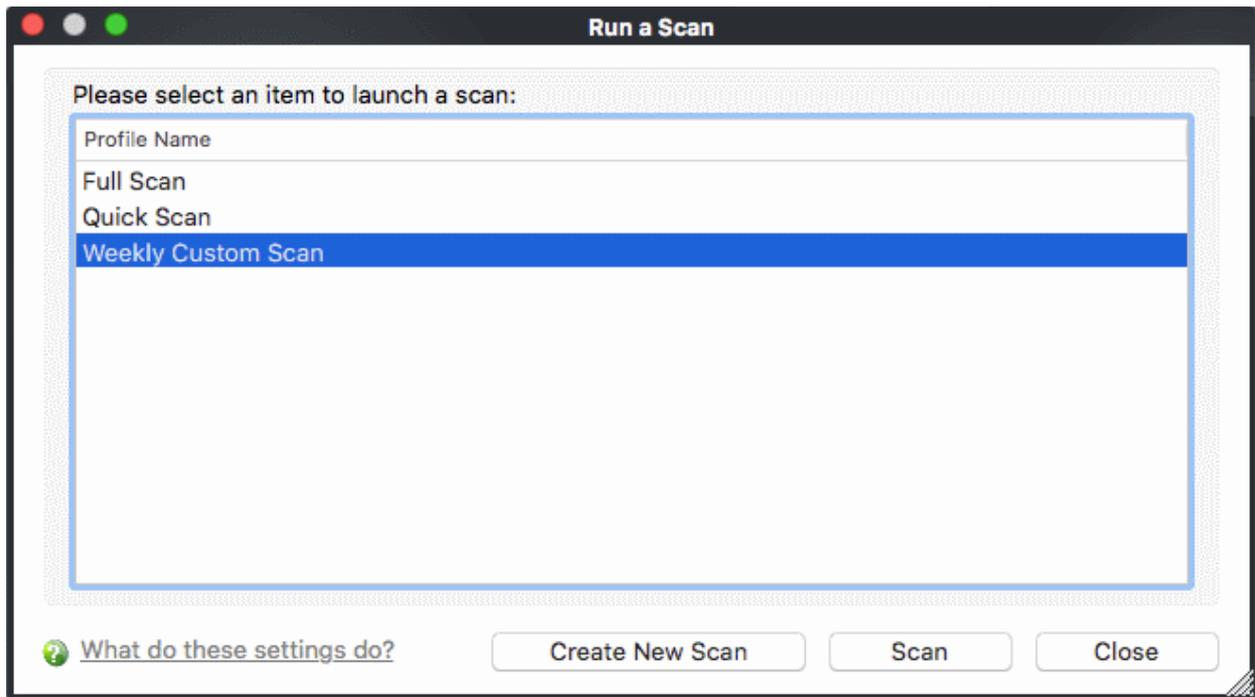The 'Add New Profile' dialog opens:

- **Name** – Enter a label for the scan profile.
- Click 'Add' to select the items you wish to include in the scan.

- Navigate to the location of the target item, select it and click 'Open'
- Repeat the process to select multiple items
- Click 'Apply' to add items for the new scan profile.

- Click 'Apply'
- The profile will be added to the list of scan profiles:

- Repeat the process to add more scan profiles

Run an Instant Scan on Selected Items

You can scan individual files or folders instantly to check whether they contain threats. There are three ways in which you can scan individual items:

- **Drag and drop items on the Summary Screen**
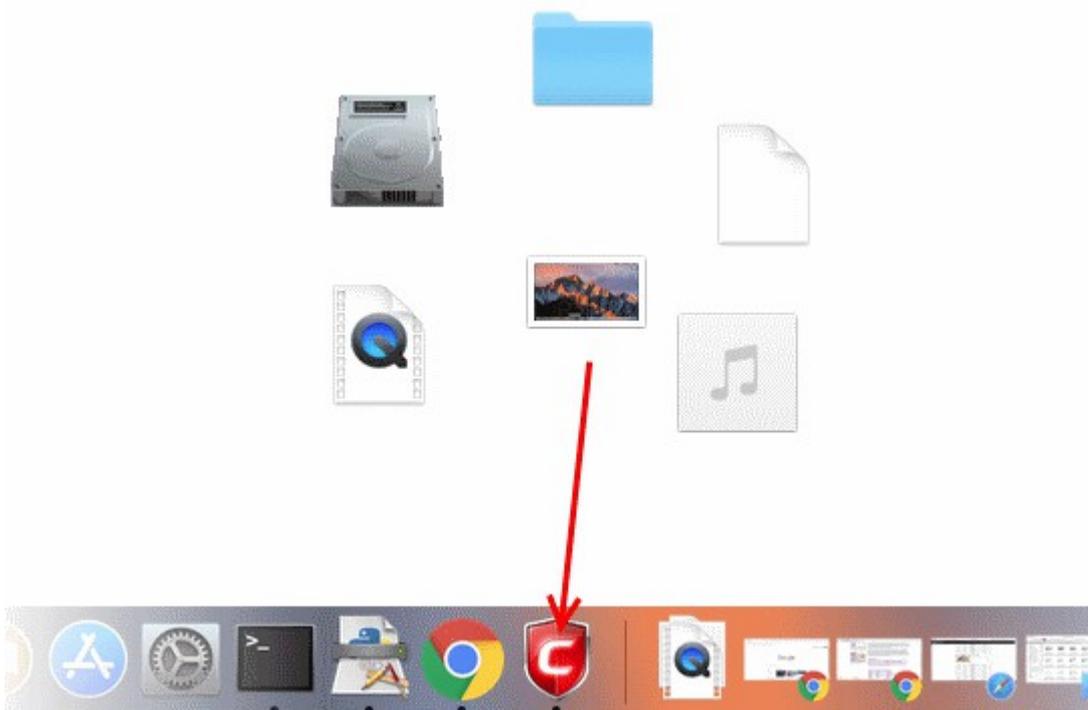- **Drag and drop items on the dock icon**
- **Right-click on an item**

Summary Screen

- Drag items into the scan box on the summary screen.
- You can drag virtually any type of item - files, folders, photos, applications or drives.
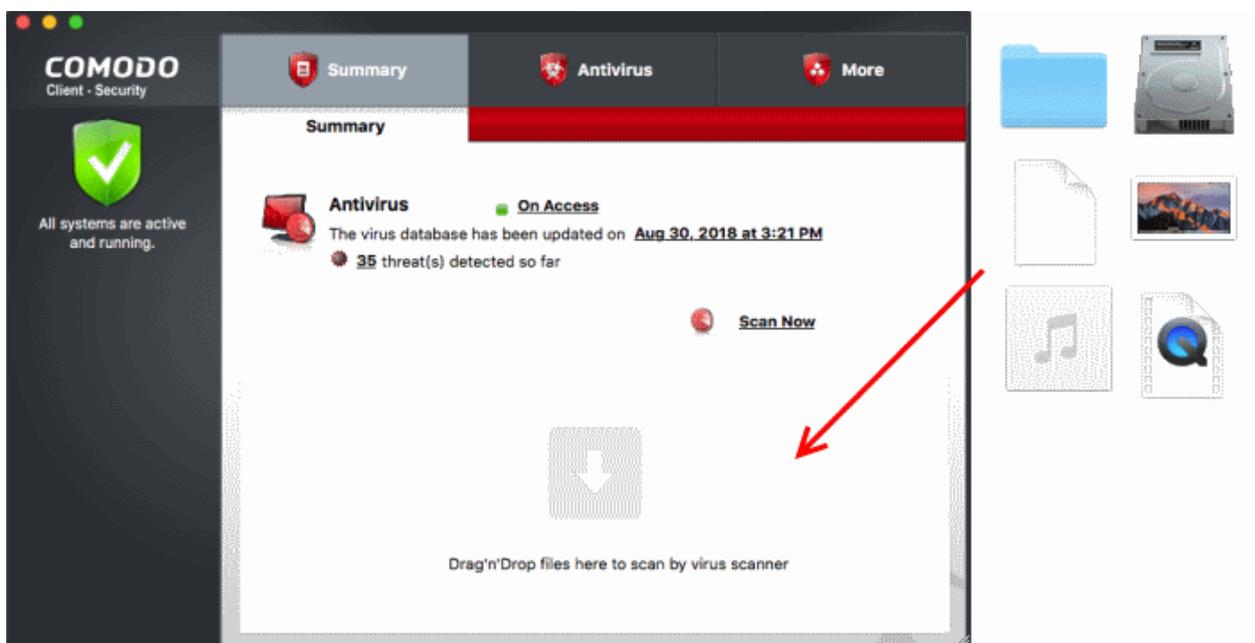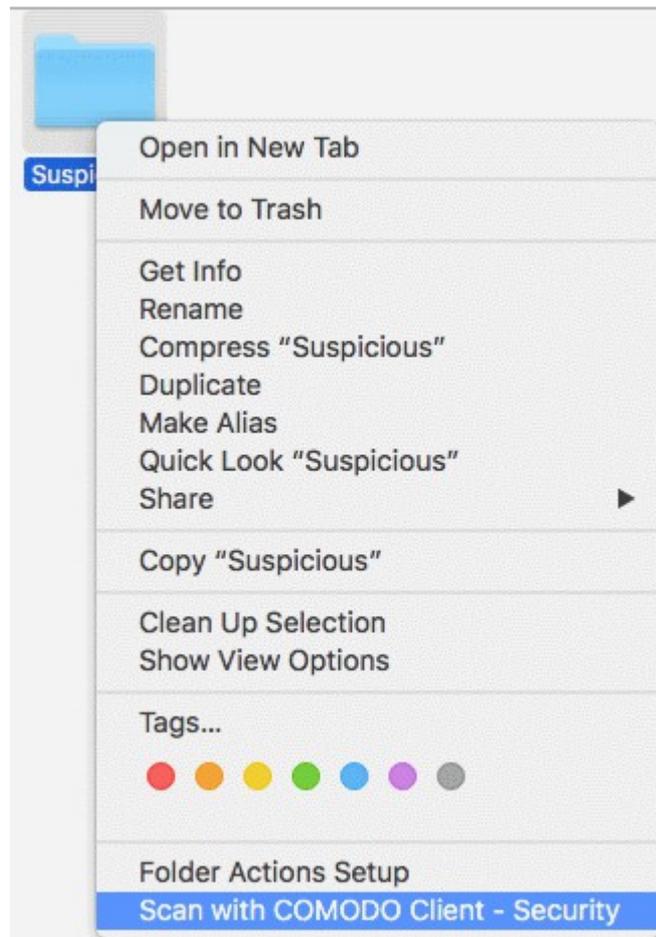
Dock icon

- Drag items into the CCS shield icon in the dock (bottom right)

- You can drag virtually any type of item - files, folders, photos, applications or drives.

Context sensitive menu

- Right click on a file, folder or drive and select 'Scan with COMODO client - Security' from the context sensitive menu:

- The scanner will check whether your virus signature database is up-to-date then start the scan
- The results will be shown on scan completion
- The results window lists all threats discovered by the scan. You can remove selected threats or choose to ignore them.
- See **Scan and Clean Your Computer** for more details.

More Help

The 'More' tab contains links to get help and support for the CCS for Mac application.

Support Forums

- Open Comodo Client Security
- Click the 'More' tab
- Click 'Browse Support Forum'
- You will be taken to the Dragon / Comodo One community pages.
- Registration is free and you'll benefit from the expert contributions of developers and fellow users alike.

Online Knowledge Base

An online knowledge base and support ticketing system is available at **http://support.comodo.com**. Registration is free.

Online Help

- Open Comodo Client Security
- Click the 'More' tab
- Click 'Help'
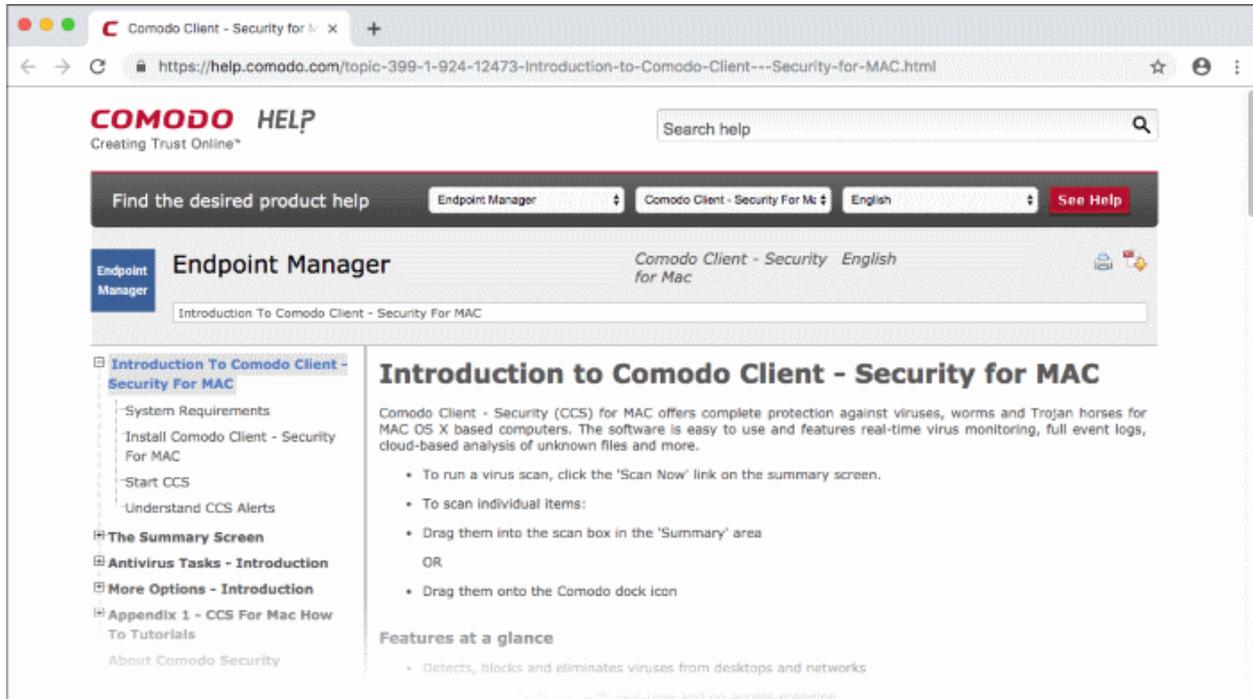
You can also download the .pdf version of the guide from here.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email**: EnterpriseSolutions@Comodo.com**