ITARIAN

Comodo
Client - Security for Linux

Software Version 2.2

Quick Start Guide

Guide Version 2.2.050820

Comodo Client Security for Linux - Quick Start Guide

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

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

Installation

Comodo Client Security (CCS) provides best-in-class threat prevention for Linux endpoints. The product is part of ITarian Endpoint Manager and is deployed from the Endpoint Manager console.

This section covers how to:

1. **Subscribe for Endpoint Manager**
2. **Enroll users**
3. **Enroll devices**

Subscribe for Endpoint Manager

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 ITarian platform.

- **ITarian** - Sign up for ITarian at **https://www.itarian.com/signup/**
  - After signup, login and 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.
  - You can access your EM instance at the URL provided during setup.

Enroll Users

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

- **ITarian MSP customers** - You can create multiple companies and enroll users to any of them.
- **ITarian 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'.
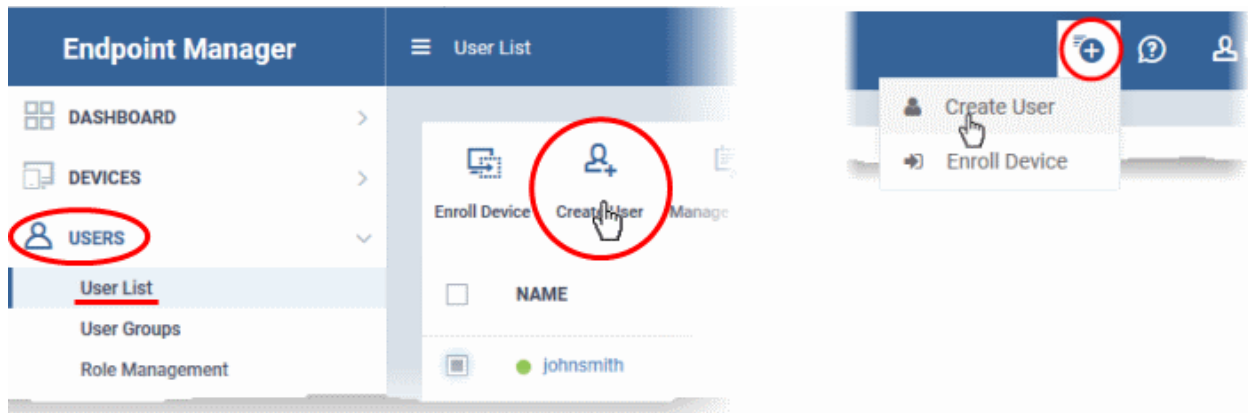
The create user form will open:

- **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.
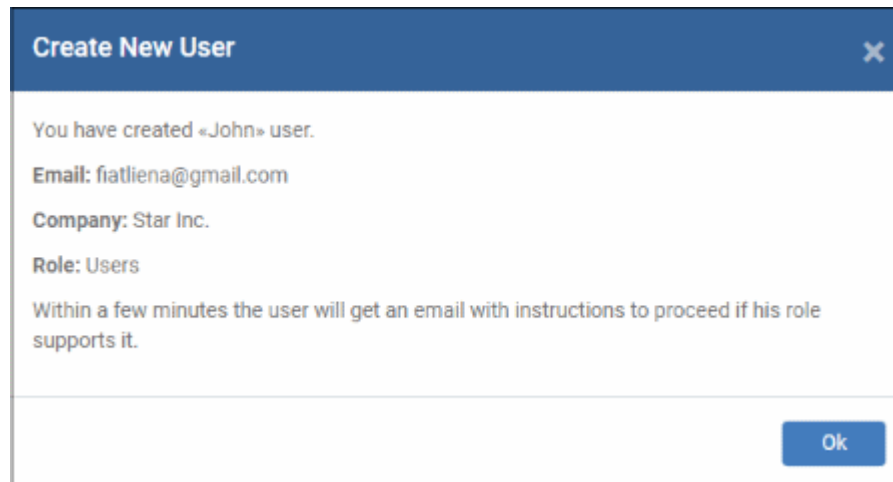- **Company** - The organization to which you want to add the user.
- **Role**

  A 'role' determines user permissions within the Endpoint Manager console itself. Endpoint Manager ships with two default roles:

  - **Administrator** - Full privileges in the Endpoint Manager console. The permissions for this role are not editable.
  - **User** - In most cases, a user is simply an owner of a managed device. They should not require

access to the Endpoint Manager console. Under default settings, users cannot login to Endpoint Manager.

- Click 'Submit' to add the user to Endpoint Manager.

A confirmation message is shown:

Create New User

You have created «John» user.

Email: fiatliena@gmail.com

Company: Star Inc.

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 are added to the 'Users' interface (click 'Users' > 'User List')

Tip: You can also bulk import users from a .csv file. See **https://community.itarian.com/help/topic-459-1-1005-14884-Import-Users-from-a-CSV-File.html** for more details.
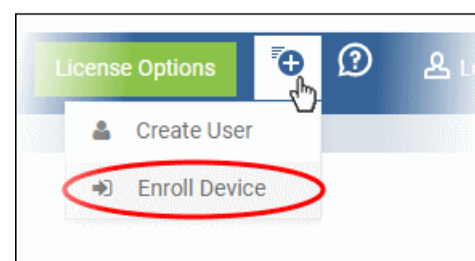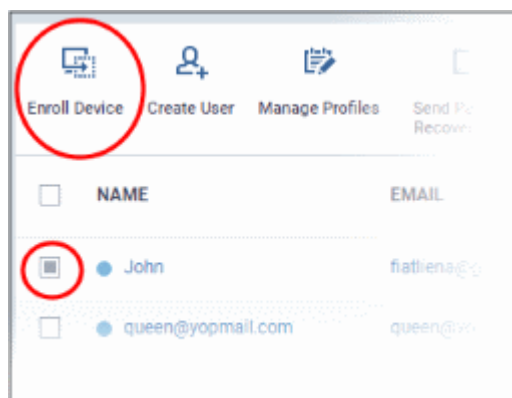
Enroll Devices

The next step is to add user devices so you can manage them with 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
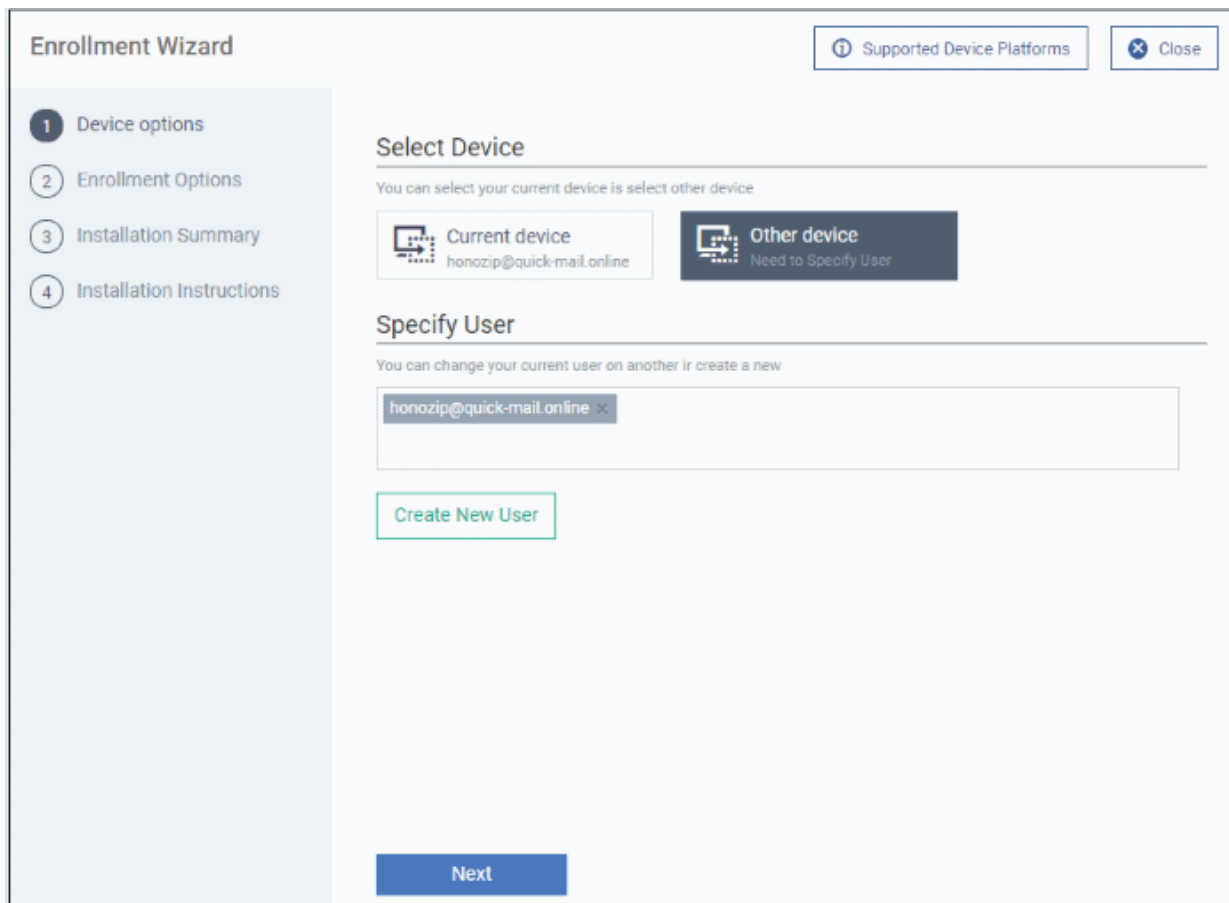
    OR

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

This starts step 1 of the device enrollment wizard:

Step 1 - Device Options

- **Current device -** Enrolls the device you are currently using. You may disregard this option at this stage as we are adding multiple devices with the 'Other device' option.

- **Other device** - Add devices owned by the users you selected previously. Those users should already be listed in the 'Specify User' box:

- You can add additional, existing users by simply typing their email address in the box. Endpoint Manager will auto-suggest users that have already been created.

- **Create New User** - Click if you want to add a new user to Endpoint Manager. You cannot add devices unless you have first added the users that own them.

- Click 'Next' to proceed to step 2.

Step 2 - Enrollment Options

Enrollment Type

Applies to Windows, Mac and Linux devices.

- **Enroll and Protect** - Installs both the communication client and the security client.

- **Just Enroll** - Installs only the communication client

Background. There are two types of client:

- **Communication Client** - Connects the device to Endpoint Manager for central management. It is mandatory to install this client.

- **Security Client** - This is the security software. Depending on the operating system, it includes antivirus, firewall, threat-containment, web-filtering, and more. It is optional to install this client.
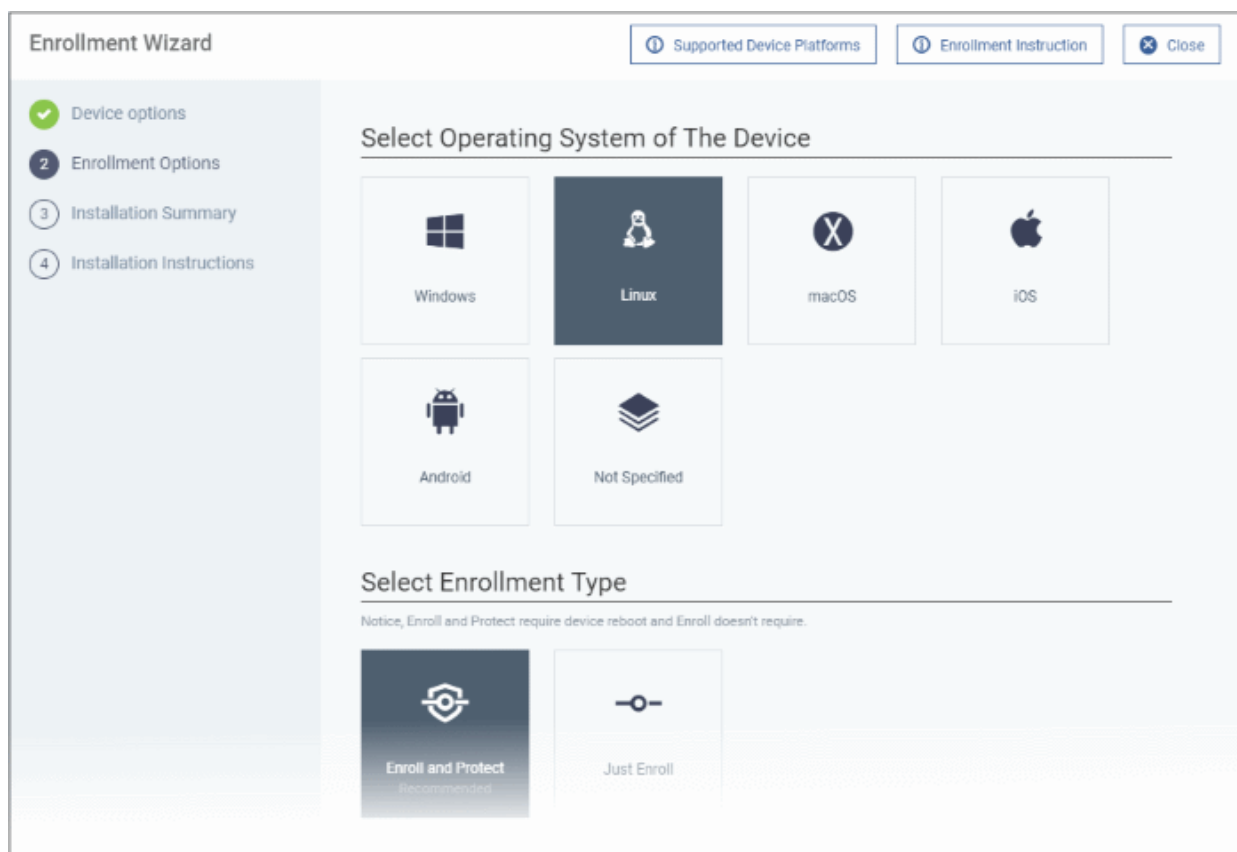
TLDR - 'Not specified' only installs the communication client so the device can connect to Endpoint Manager. It does not install the security client. Click one of the operating system tiles if you also want to install the security client.

Option 1 - Enroll + Protect - Single Operating System

- Choose this if you want to deploy both communication and security clients

  - Click the Linux OS box. Please make sure all your target devices use this operating system.

  - The wizard will send enrollment mails which *only* contain download links for the Linux clients.

  - You can customize enrollment options as required. You can configure items such as enrollment type, Linux OS version and device name.

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

Option 2 - Enroll Only - Multiple Operating Systems

- Choose this if you only want to deploy the communication client. If required, you can install the security client later after enrolling the endpoint.

  - Click 'Devices' > 'Device List'

  - Select the target devices

  - Click the 'Install or Update Package' button > Choose 'Install Comodo Client – Security'.

Click 'Next' to **skip to step 3** if you are happy with your choices thus far

OR

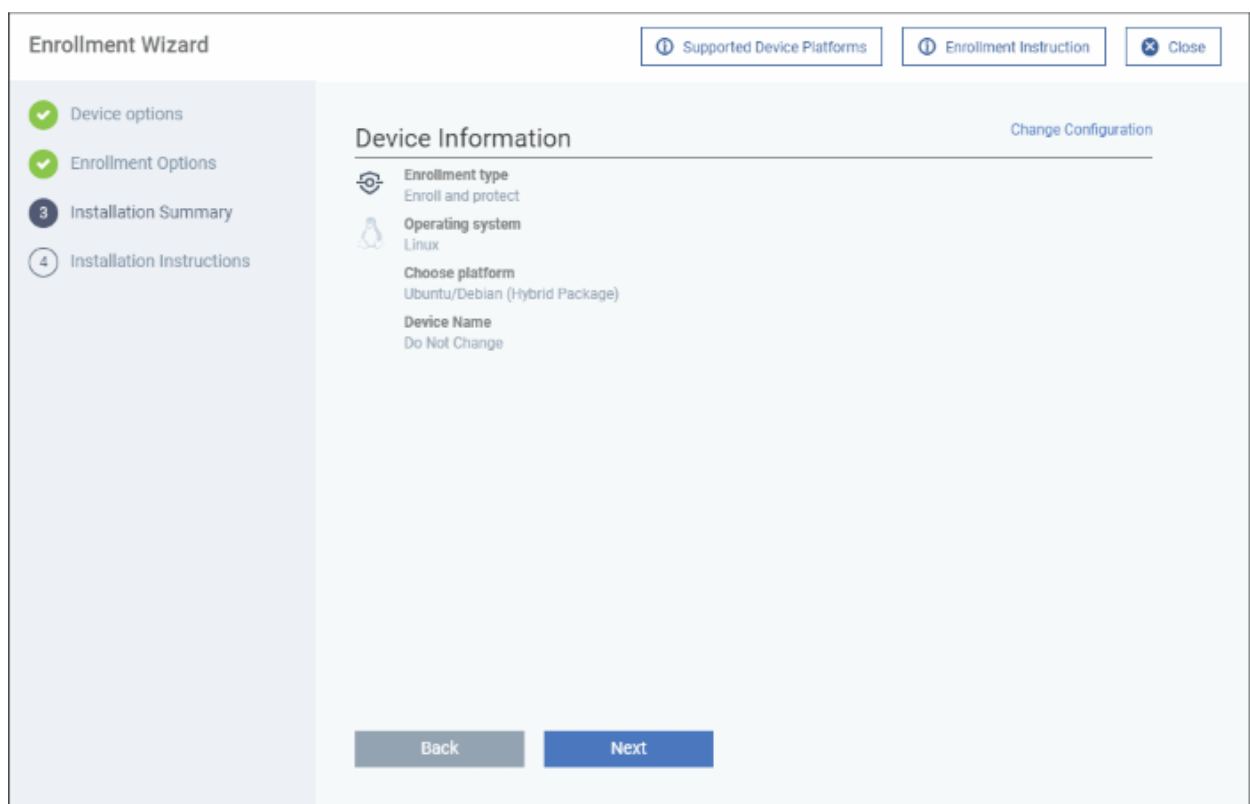See the table below for more information about the options on this page

Setting	Description
Choose platform	Select Linux OS version

	• Ubuntu / Debian (Hybrid Package)
	• RHEL / CentOS (Hybrid Package)
	• 'Hybrid' just means the package is suitable for both types of OS.
Device Name Options	• Do Not Change - The device's existing name is used to identify the device in Endpoint Manager.
	• Change - Enter a new device name. Note - You can restore the original name from the device list screen if required.

• Click 'Next' to proceed to step 3

Step 3 - Installation Summary

Review your choices so far.
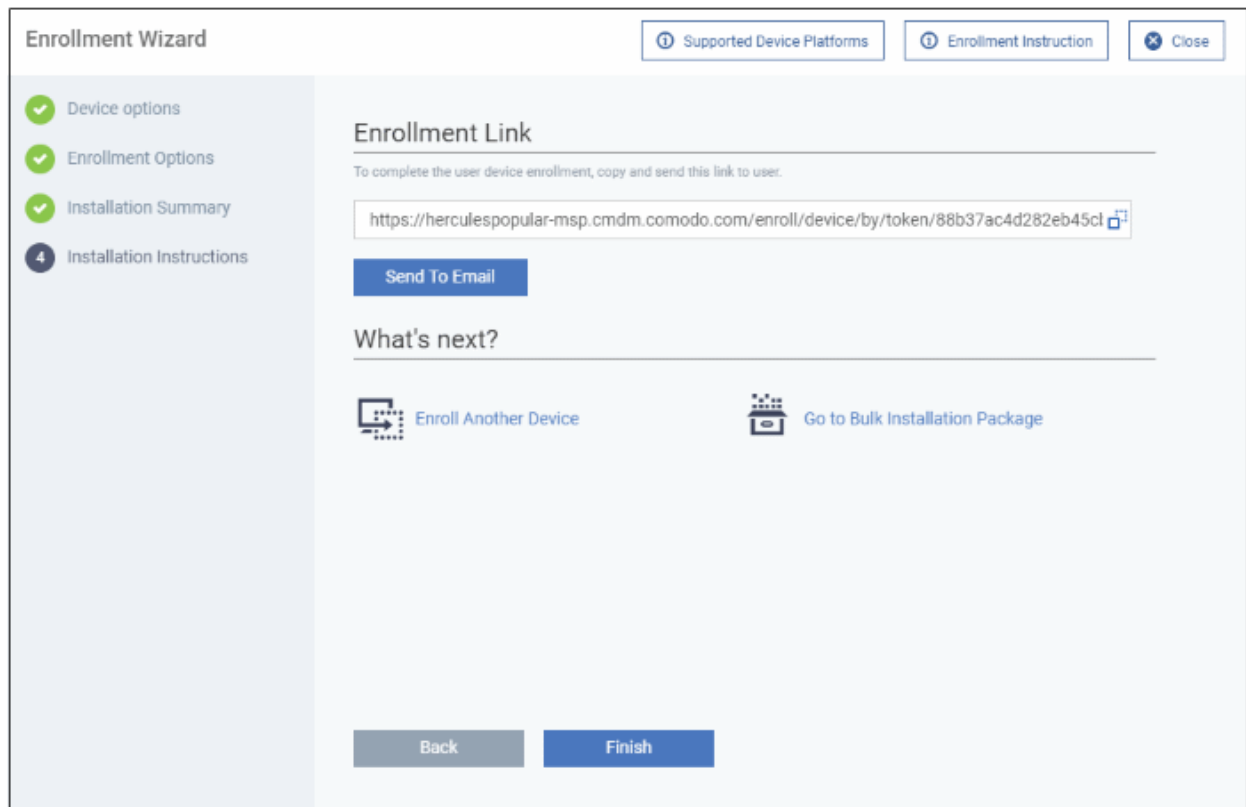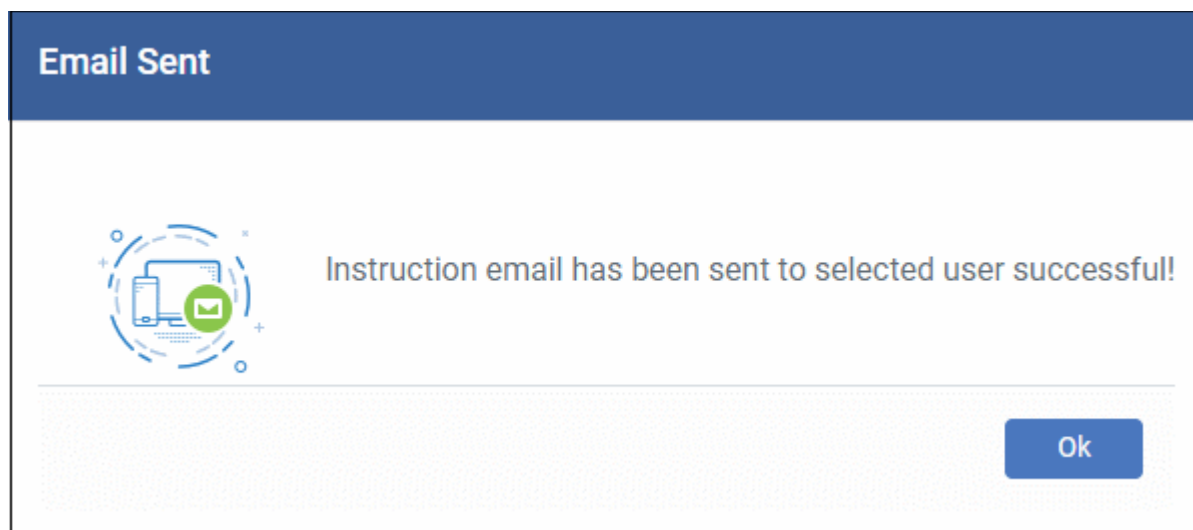

• Click 'Back' or 'Change Configuration' (top-right) to revise your choices.
• Click 'Next' to proceed to step 4

Step 4 - Installation Instructions

The final step is to send out the enrollment emails to the device owners:

- **Send To Email** - Click this to send enrollment mails to users with the settings you choose in steps 1 - 3.

- **Enroll Another Device** - Takes you back to step 1
- **Go to Bulk Installation Package** - Takes you to bulk installation package screen to configure and enroll users in bulk. See '**Bulk Enrollment of Devices**'
- Click 'Finish' to close the window.

An example mail is shown below:

Dear Grey Pelican,

Congratulations, your Endpoint Manager account has been successfully created.
Please click the following link to activate your account and set up your password:

https://herculespopular-msp.cmdm.comodo.com/user/site/activate/username
/Grey+Pelican/key/499cdc1039e5fd03080347b55a776adc658c5c77

Sincerely, Endpoint Manager team.

The user experience is as follows:

- User opens the email on the Linux endpoint you want to enroll.
- Click the enrollment link in the email to open the device enrollment page
- Click the 'Download Linux Installer' button:
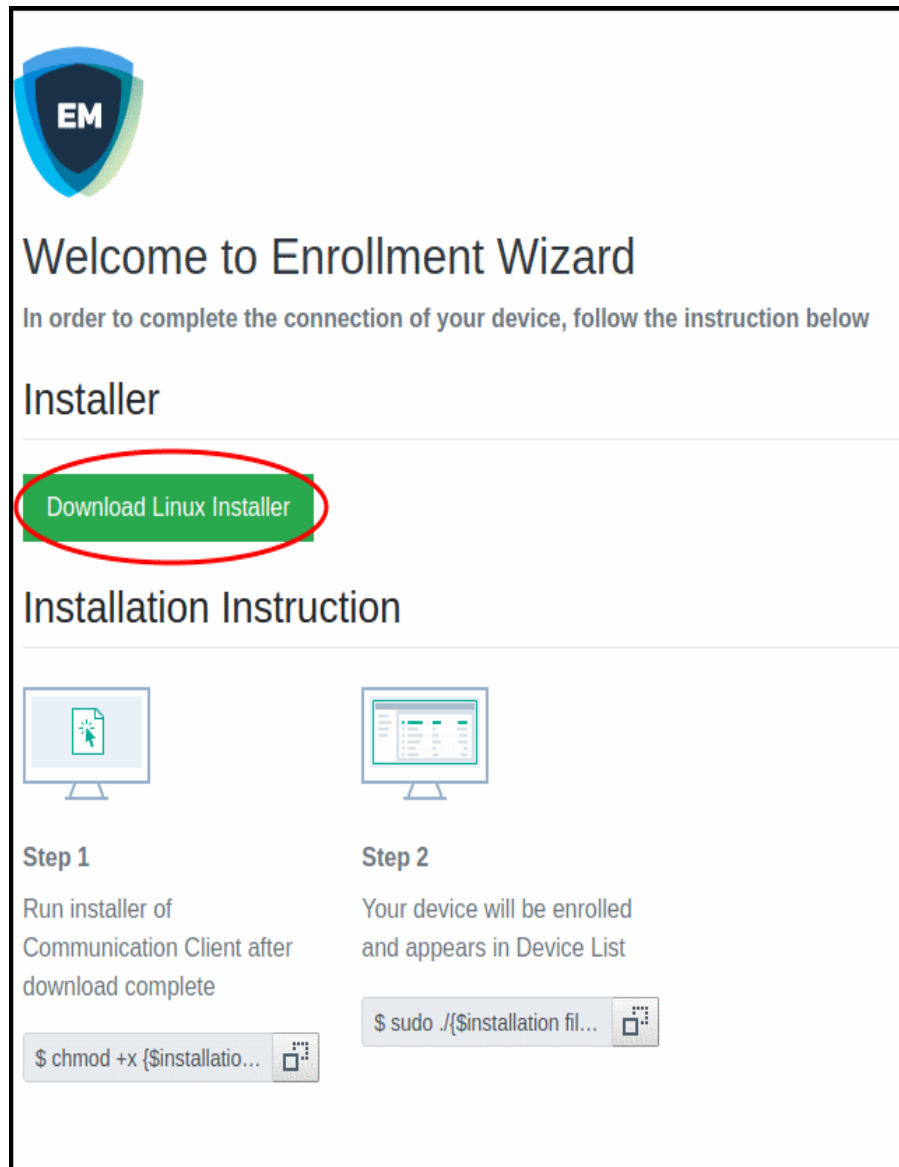
You can install the communication client on the Linux device by completing the following:

1. Change installer mode to executable - enter the following command:

   $ chmod +x {$installation file$}

2. Run installer with root privileges - enter the following command:

   $ sudo ./{$installation file$}

For example:

chmod +x itsm_cTjlw6gG_installer.run

sudo./itsm_cTjlw6gG_installer.run

- After installation, the communication client will connect to the Endpoint Manager and enroll the device. The EM communication client icon appears at the top-right of the endpoint screen.
- Protection is effective immediately after the computer restarts.

An Endpoint Manager (EM) security profile is applied to the device.

- If the user is already associated with a configuration profile in EM, then those profiles will be applied to the device. See **Assign Configuration Profile(s) to User Devices** and **Assign Configuration Profiles to a User Group** for more details.
- If no profiles are defined for the user then the default Linux profile(s) will be applied to the device. See **Manage Default Profiles** for more details.

The device can now be remotely managed from the EM console.

Start CCS

- After installation, Comodo Client Security (CCS) will load at computer start-up.
- Real-time protection and on-access scanning is automatically enabled, so you 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 Linux profile > Click the 'Antivirus' tab.
- However, you can also configure the application at a local machine should you wish. The rest of this guide explains how to configure and use the application locally.

You can access the management interface in the following ways:

- **Applications Menu** - Click 'Applications' to view CCS product group icons
  - Double-click 'Comodo Client Security' icon to to start the application.
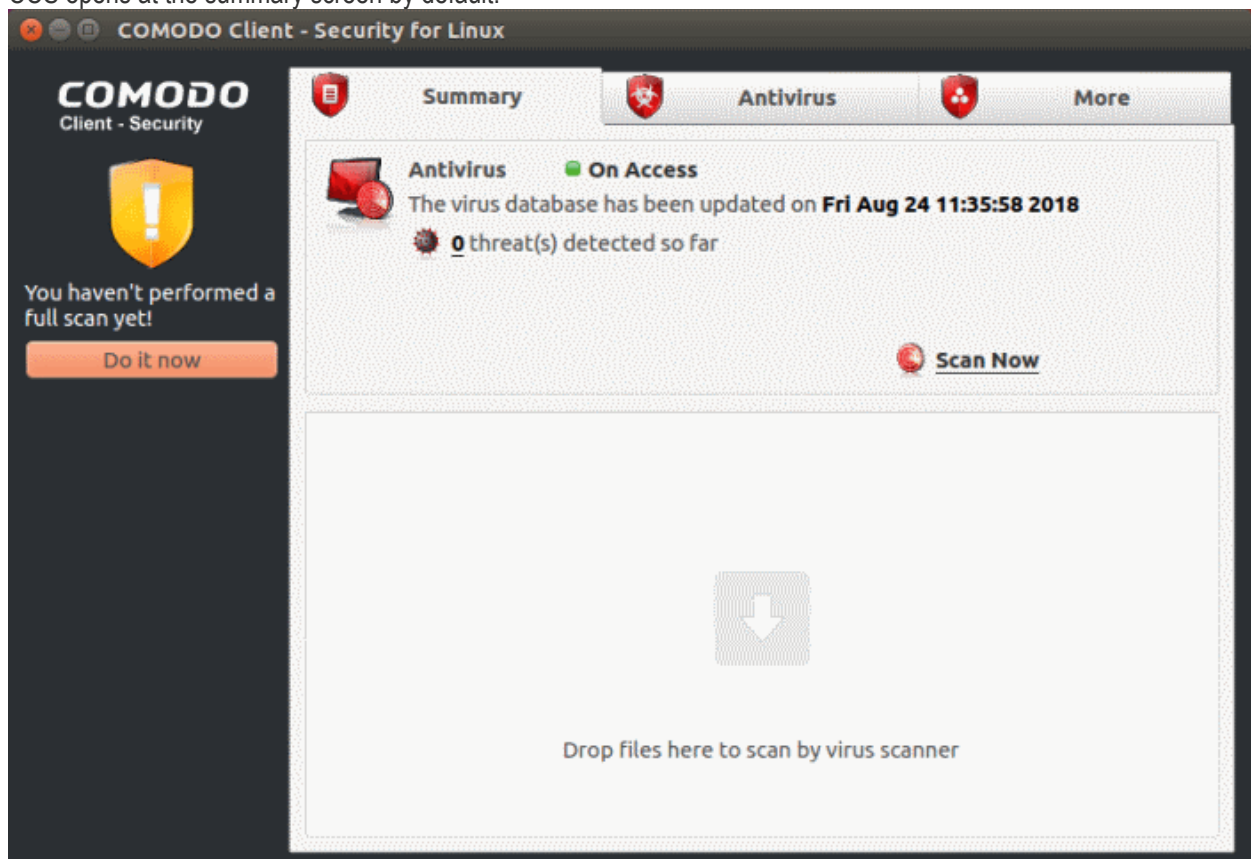
- **Desktop** - Double-click the 'Comodo Client - Security for Linux' shortcut

- **Dock Icon** - Double-click the CCS icon in the dock area

CCS opens at the summary screen by default:

- 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:

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.

Results are shown at the end of the scan:

- Click the 'Results' button to see detailed file information.
- The results window lists all threats discovered by the scan. You can remove selected threats or choose to ignore them:
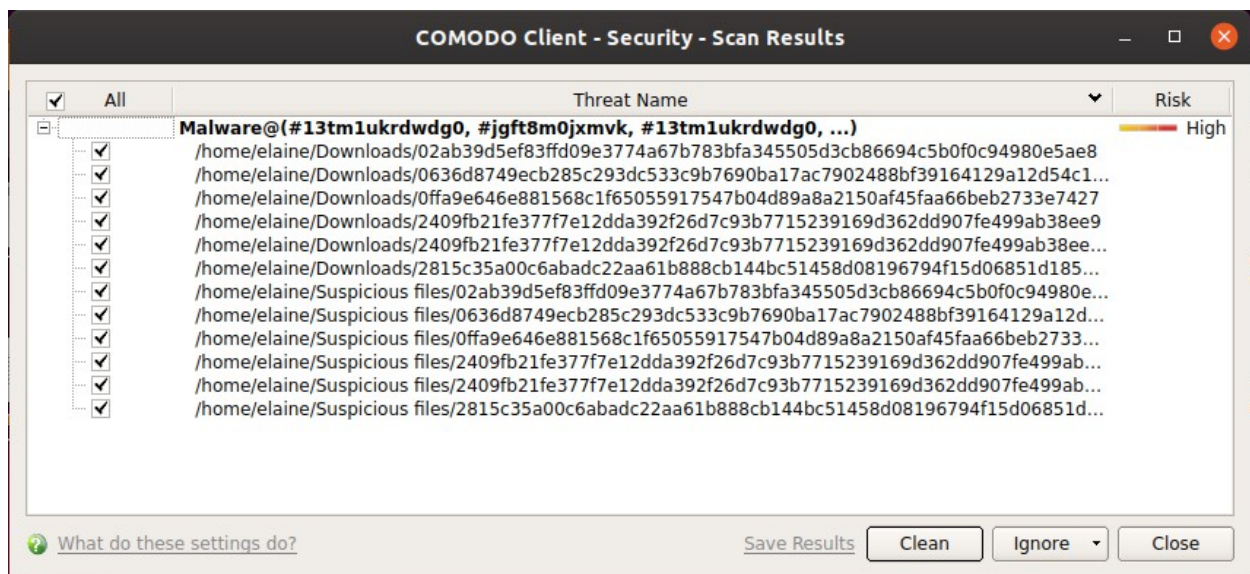
See **Scan and Clean Your Computer** for more details.

The Main Interface

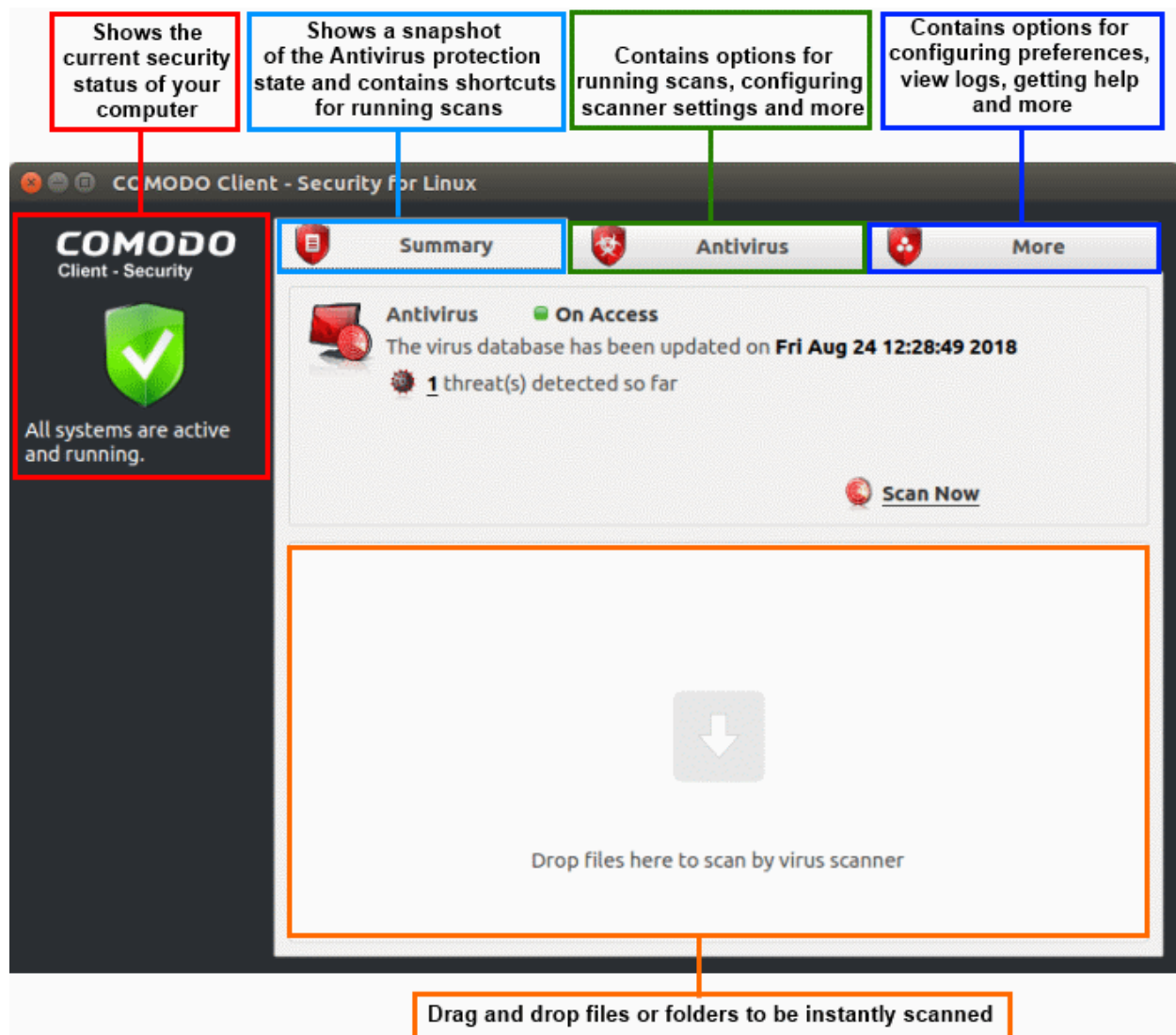The CCS interface is designed to be as clean and informative as possible while letting you carry out tasks with the minimum of fuss.

System Status

The shield icon on the left shows your current protection level. There are three colors - yellow, green and red

- **Yellow** - Your security is at risk. For example, because you need to run a full scan, because the database is outdated, or because the real-time scanner is switched off.
- **Green** - All systems are active and running.
- **Red** - Serious security risks. For example, you have malware on your system.

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:

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

  - **On Access**: Real-time virus 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://community.itarian.com/help/topic-459-1-1008-15078-Real-Time-Scan.html** for more details.

Please note: Real-time scanning is not supported on Debian. This feature is not available on Debian.

- **Database Updates**
  - The date when the virus database was last updated is shown as a link.
  - Click the link to run a database update.
  - See **https://community.itarian.com/help/topic-459-1-1008-15054-Update-Virus-Database.html** for more details
- **Number of Detected Threats**
  - The number of threats found in this session.
  - Click the number to view a list of threats detected.
  - For more details, see **https://community.itarian.com/help/topic-459-1-1008-15065-View-Antivirus-Events.html**
- **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.

  - For more details about this section, see **https://community.itarian.com/help/topic-459-1-1008-15044-Antivirus-Tasks---Introduction.html**

The 'More' Tab

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

- **Preferences** - Configure general CCS settings (interface language, log storage, update options, external device control and so on)

- **Manage My Configurations** - Manage, import and export CCS security settings as configuration profiles.

- **Diagnostics** - Identifies any problems with the CCS installation.
- **View Antivirus Events** - See logs of all antivirus events including files intercepted by real-time protection, manual scans, virus signature database updates and more.
- **Browse Support Forums** - Links to user forums.
- **Help** - The online user guide.
- **About** - Version and copy-right information about the product.
  - For more details about this section, see **https://community.itarian.com/help/topic-459-1-1008-15045-More-Options---Introduction.html**

Scan and Clean Your Computer

Click 'Antivirus' > 'Run a Scan'

- The 'Run a Scan' area lets you launch an on-demand scan on an item of your choice.
- You can scan your entire computer or specific files/ folders/ drives.
- You can also scan a wide range of removable storage devices, including external hard-drives, USB sticks, digital cameras and more.

Run an on-demand virus scan

- Open Comodo Client Security
- Click the 'Antivirus' tab
- Click 'Run a Scan' in the antivirus tasks area
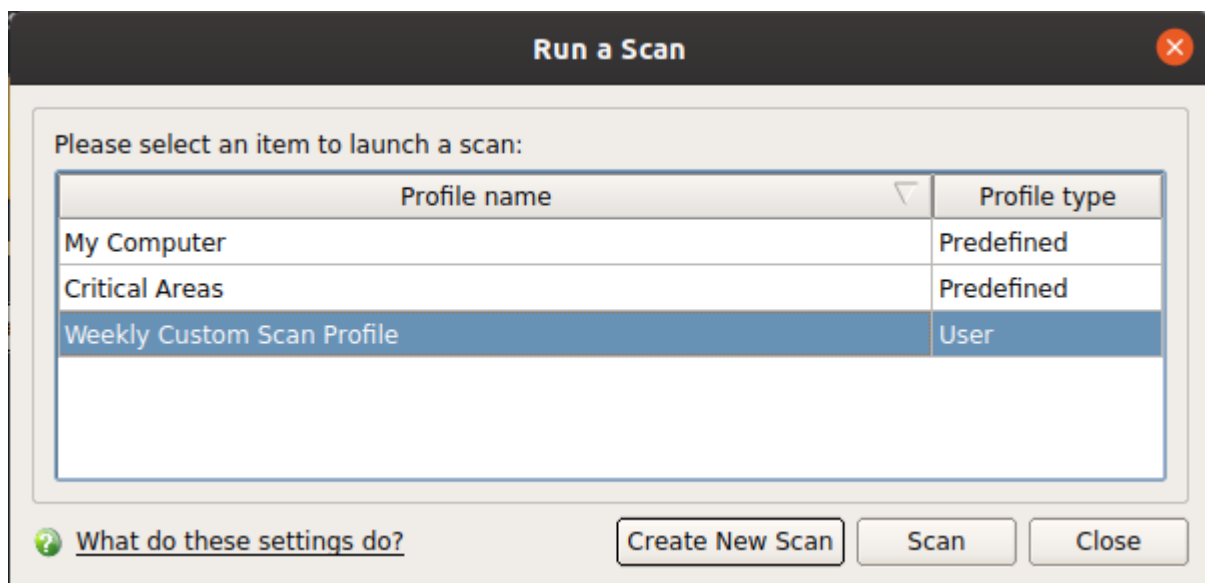
Choose one of the following options:

- **Profile name** - A scan profile defines the folders, drives or areas that are covered by the scan.

  CCS ships with two pre-defined scan profiles - 'My Computer' and 'Critical Areas'. These cannot be edited or removed:
  - **My Computer** - Scans every drive, folder and file on your system, including external connected devices
  - **Critical Areas** - A targeted scan of important operating system files and folders.
- **Profile Type** - Shows whether the profile is predefined (created by Comodo) or user-defined.
- **Create New Scan** - Create your own **custom scan** of specific files, folders or drives.

Click 'Scan' after making your selection.

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
- Click 'Apply'. Your new profile will be listed in the 'Run a Scan' dialog
    - Note - You can also create custom profiles in the scan profiles are (click the 'Antivirus' tab > 'Scan Profiles')
- 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:
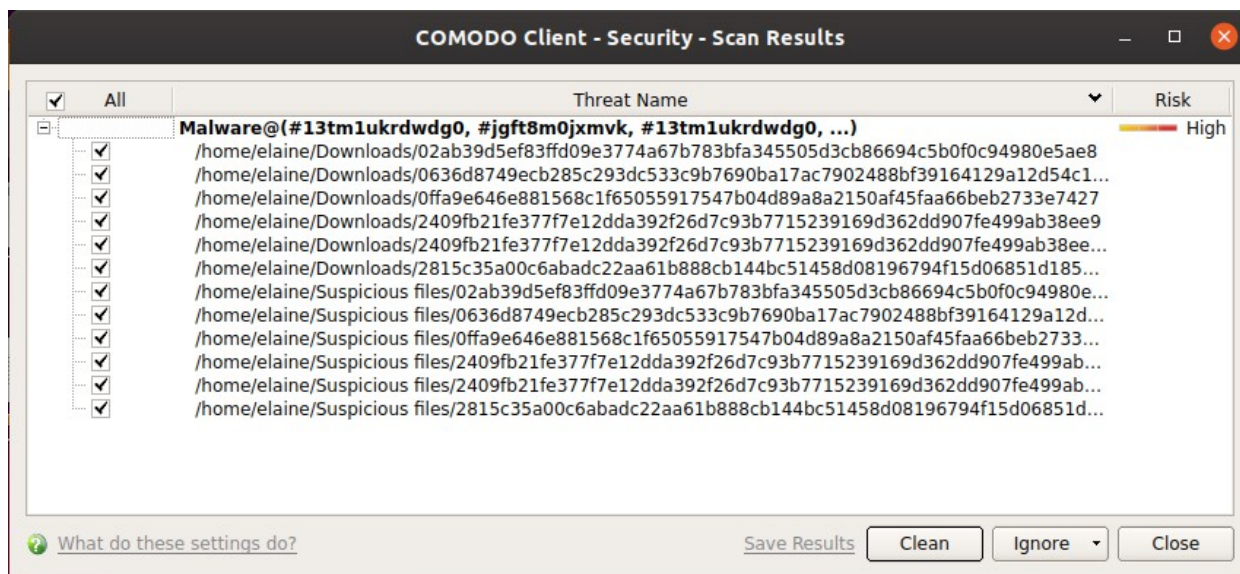
- Click 'Pause' to suspend the scan
- Click 'Resume' to recommence the scan
- Click 'Stop Scan' to abort the scan altogether.

Results are shown at the end of the scan:

- Click the 'Results' button to see detailed file information.
- 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 - Click the link to store the scan results as a text file.

    Clean - 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**.

    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.
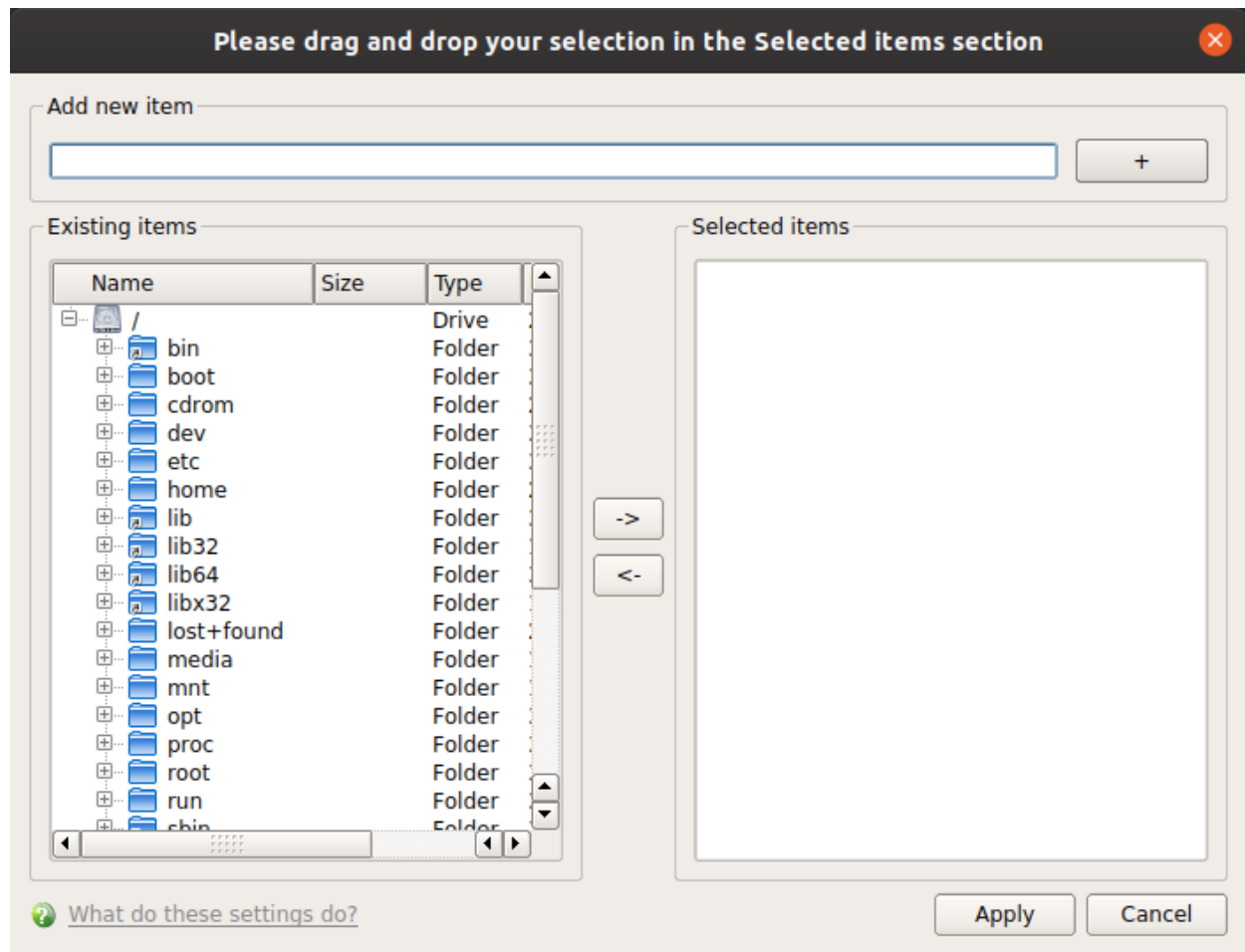
Create a Scan Profile

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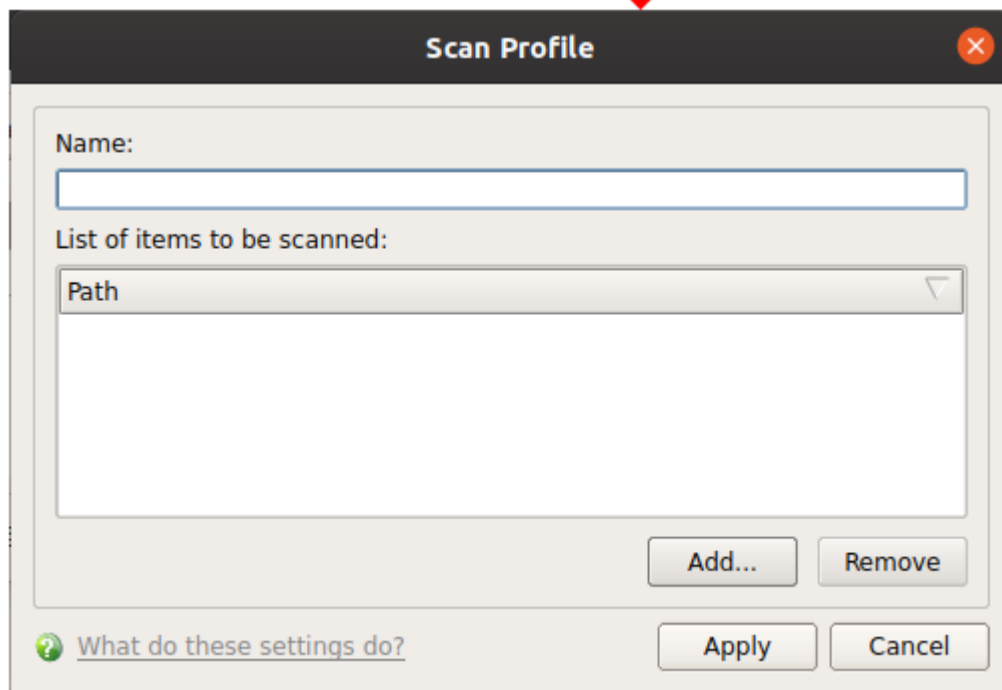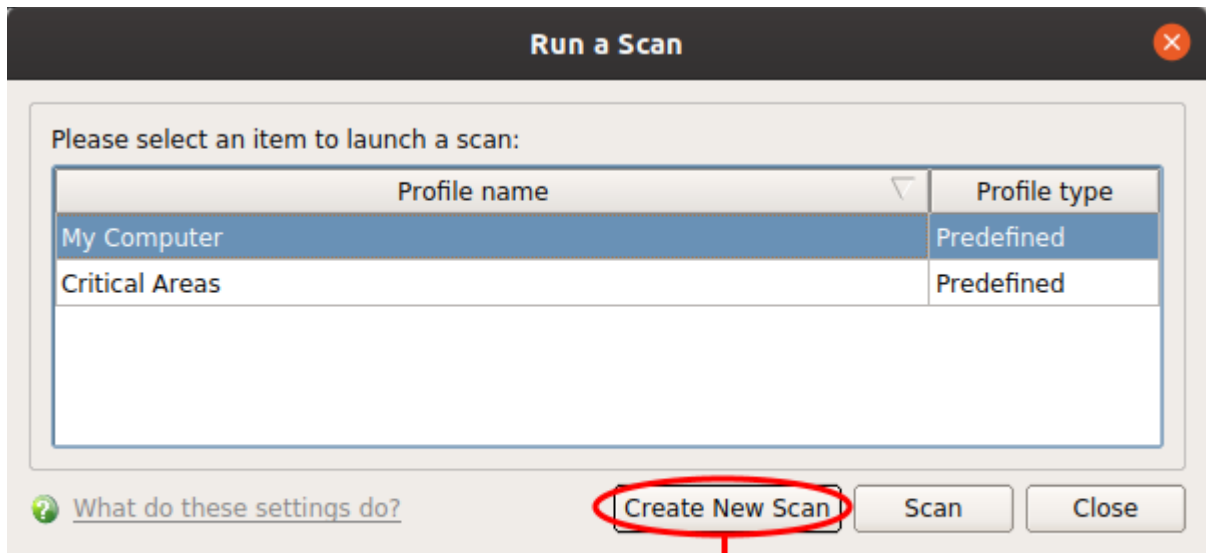
- **Name** - Enter a label for the scan profile.
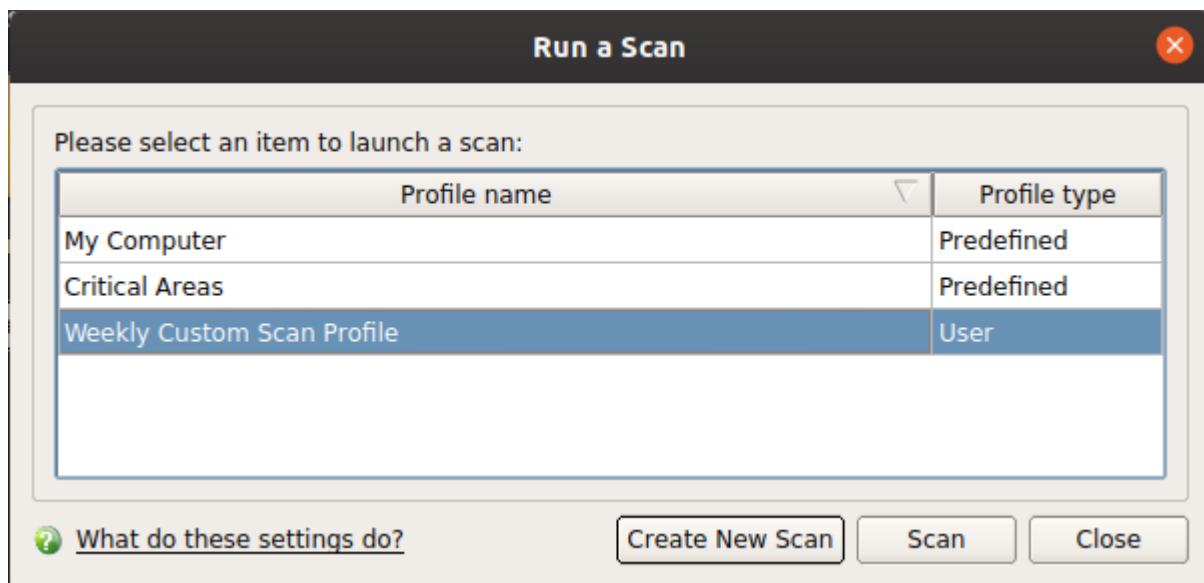- Click 'Add' to select the items you wish to include in the scan

You can add items in two ways:

- Manually enter the path in the 'Add new item' field and click the '+' button
- Drag and drop the files, folders and/or drives you require from the left pane to the right pane.
- Repeat the process to select multiple items
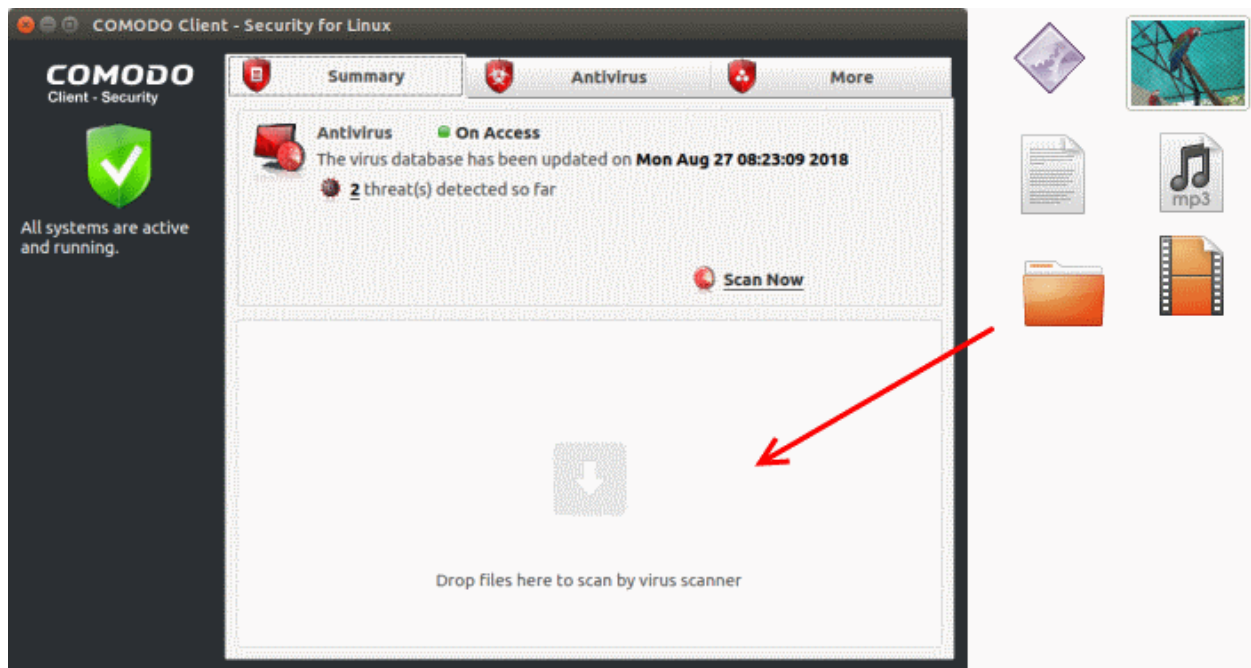- Click 'Apply'
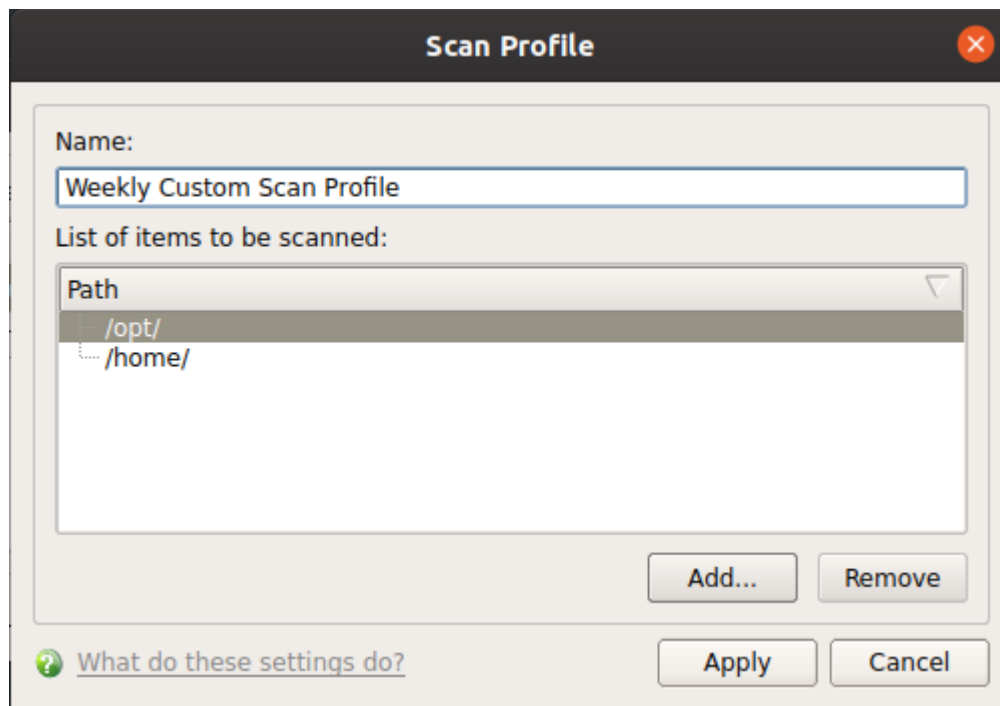
- Click 'Apply' in the scan profile dialog

You can also create profiles in the scan profiles area (open CCS > 'Antivirus' tab > 'Scan Profiles')

Run an Instant Antivirus Scan on Selected Items

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

More Help

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

Support Forums

- Open Comodo Client Security
- Click the 'More' tab
- Click 'Browse Support Forum'
- You will be taken to the community pages.
- Visit the ITarian community page at **https://forum.itarian.com/**
- Registration is free and you'll benefit from the expert contributions of developers and fellow users alike.

Online Help

- Click 'More' > 'Help'
- The help link opens the online user guide. Each area has its own dedicated page and contains detailed descriptions of the application's functionality.

You can also click the pdf icon at top-right to download the help guide in PDF format.