

COMODO
Creating Trust Online®



Comodo SecureBox Management Console

Software Version 1.9

Quick Start Guide

Guide Version 1.9.120318

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo SecureBox Management Console – Quick Start Guide

This tutorial briefly explains how admins can use the central management console (CMC) to enroll endpoints, create security policies, create endpoint groups and apply policies to endpoint groups.

The Secure Box Central Management Console is available in both SaaS and on-premises deployment models. Endpoints can easily be imported via active directory or work-group.

On-Premise Installation

CMC installation will be carried out by Comodo engineers at your premises after finalizing your order. For more details, contact us at secureboxsupport@comodo.com. Afterwards, you will be able to login to the console using the URL configured during installation.

Software as a Service

The Management Console is hosted on our cloud servers and can be accessed from anywhere in the world. After you have finalized your order, Comodo will provide you the log-in address. For more details, contact us at secureboxsupport@comodo.com.

The guide will take you through the following processes:

- **Step 1 – Login to the Management Console**
- **Step 2 – Add Organization**
- **Step 3 – Add License**
- **Step 4 – Configure the Management Console**
- **Step 5 – Add User-Groups and Users**
- **Step 6 – Add Policies and Secure Items**
- **Step 7 – Add Endpoint Groups and Enroll Endpoints**
- **Step 8 – View Reports**

Step 1 – Login to the Management Console

The Management Console can be accessed by entering your unique, customer URL in the address bar of any internet browser. If you do not have this URL then please contact your Comodo representative or create a support ticket at support.comodo.com

Management Console : Login

SECURE BOX

E-Mail Address

Password

Login

[Forgot Password](#)
[Change Password](#)
[Create your organization](#)

- Enter your email address and password in the respective fields and click the 'Login' button

After successful verification, the next screen displayed depends on the CMC version:

- **On-Premises version** - Administrators can manage multiple organizations and create new organizations. Move onto **Step 2** to add organizations
- **SaaS version** - The home screen of the management console will be displayed after logging in. Move onto **Step 3** to add licenses.

Step 2 – Add Organization

After logging in, the 'Select Organization' screen will be displayed for on-premise versions of the solution. Primary administrators can create new organizations by clicking 'Create your organization'. The number of organizations and endpoints that can be enrolled depends on the type of subscriber license. Once you have created an organization(s), you will be able to choose which organization you wish to manage directly after logging in.

If you want to manage an existing organization, select it from the drop-down and click the 'Select' button and proceed to **Step 3**.

- To add a new organization, click the 'Create New Organization' link

Management Console : Select Organization

You can manage more than one company.
Please select company from the list below.

Select Organization ▼

[Create New Organization](#)

Management Console : New Organization

Name

Description

Active

Auto Accepted

Technical Contact

Name

E-Mail Address

Phone

Administrative Contact

Name

E-Mail Address

Phone

Add Organization – Form Parameters	
Form Element	Description
Name	Enter the name of your new organization/company
Description	Provide an appropriate description for the organization/company
Active	Select to activate the organization. Endpoints can only be added to and managed from active organizations.
Auto Accepted	Endpoints that are enrolled need to be confirmed by administrators in order to be paired with CMC. If this option is selected, then newly enrolled endpoints will be automatically registered with CMC for this organization.
Technical Contact - The person whom Comodo will contact for resolving technical problems for their account	
Name	Enter the name of the technical contact
E-Mail Address	Enter the email address of the technical contact
Phone	Enter the phone number of the technical contact
Administrative Contact – Person who can log into the management console and manage this organization. The admin will be allowed to manage only this organization. You can, of course, make this person the admin of other organizations when you add new organizations.	
Name	Enter the name of the administrator
E-Mail Address	Enter the email address of the administrator. We will send an account activation mail to this address.
Phone	Enter the phone number of the administrator

- Click the 'Save' button

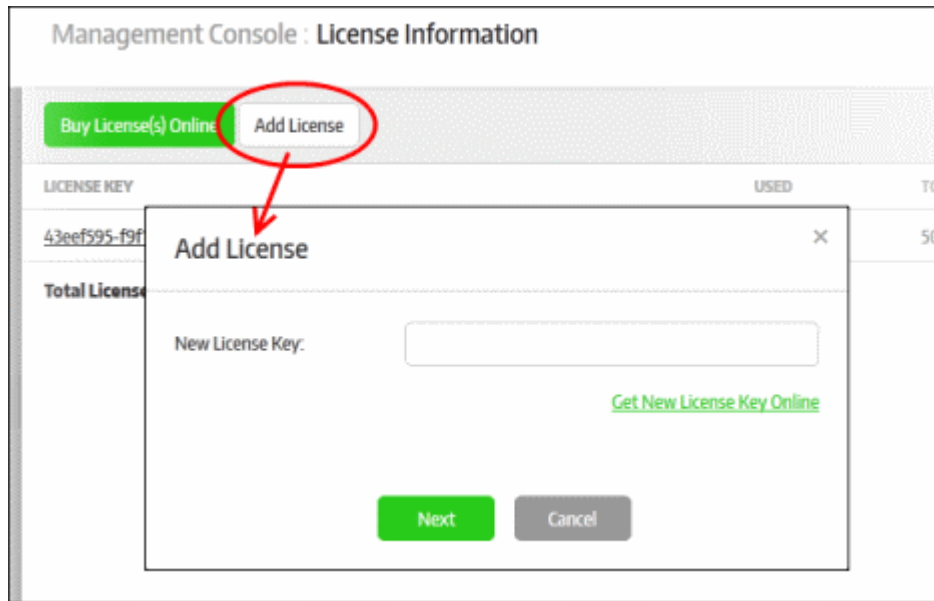
The new organization will be created and an account activation email will be sent to the administrative contact.

After the account has been activated, the administrative user can log-in to the management console to manage the organization. For more information refer to the section '[Managing Organizations](#)'.

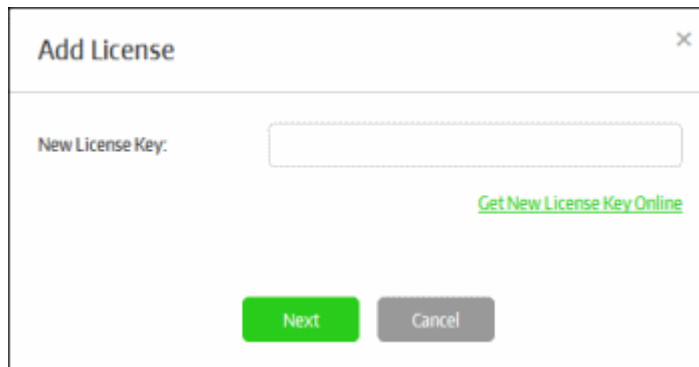
Before enrolling endpoints, the administrator has to add a license and upload CSB packages in order to install them on endpoints.

Step 3 – Add License

- To add a license for an organization, log into the management console and click 'License Information' then 'Add License':

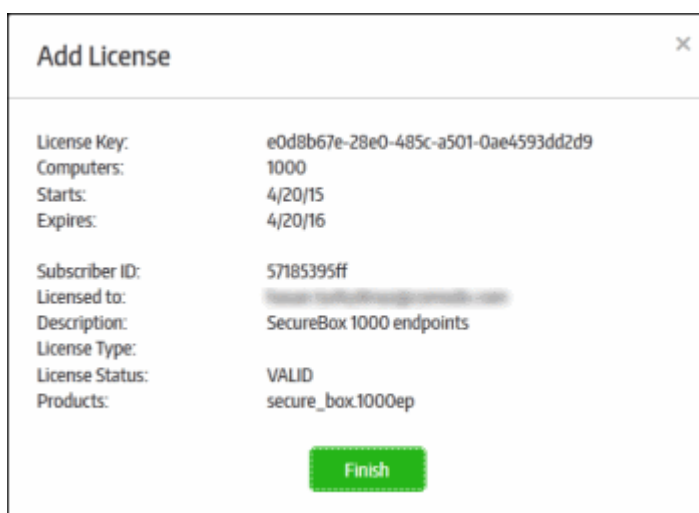


The 'Add License' dialog will be displayed:



- Enter the license key that you received in the registration email then click the 'Next' button.

The license key will be verified and, if validated, you will see a confirmation message as follows:



- Click the 'Finish' button

The new license key will be applied to the organization. All licenses for an organization are listed in the 'License Information' screen along with details such as number of endpoints, validity and start/expiry date:

LICENSE KEY	USED	TOTAL	STARTS	EXPIRES	STATUS	WARRANTY
83ee1295-f9f1-429f-96a2-7cbassa8b04d	1	50	1/14/16	4/14/16	VALID	
e0d8b57e-28d0-4d5c-a501-0a4c573d02d9	446	1000	4/20/15	4/20/16	VALID	

Total Licenses: 2

Note - you can add multiple licenses if you want to enroll more endpoints than allowed under the current subscription. You can also use a single license for multiple organizations/departments as long as the total number of endpoints is within the licensed limit. To get more licenses, simply repeat the procedure explained in this step.

The next step is to configure settings for the management console and global settings for enrolled endpoints.

Step 4 – Configure the Management Console

The settings configured in the 'Preferences' section determine the behavior of the management console. You can also configure global settings that will be applied to enrolled endpoints.

- To configure preferences, click 'Preferences' on the left:

Management Console : Preferences

COMODO Administrator Test Organization

Select Organization

Home

Computers Management

Policies Management

Reports

Preferences

License Information

User Administration

About

General

Language: English

Timezone: Asia/Istanbul

Password Expiration Days: 90

Unreachable Endpoint Time Limit (Unit): Disable

Unreachable Endpoint Time Value: 0

Save Changes

Save

Reset

Click the following links for more details on each setting:

- [General Settings](#)
- [Endpoint Settings](#)
- [Report Settings](#)
- [Polling Interval Settings](#)
- [External Services](#)
- [Packages](#)
- [Email Notifications](#)
- [Threat Notifications](#)
- [Activity Notifications](#)
- [License Notifications](#)
- [SMTP Settings](#)
- [Auto-Discovery Settings](#)
- [Code Signing Certificate](#)

General Settings

This section allows you change interface language, timezone, password lifetime, endpoint time-outs and warning icon schedules.

General

Language: English

Timezone: Asia/Istanbul

Password Expiration Days: 90

Unreachable Endpoint Time Limit (Unit): Hours

Unreachable Endpoint Time Value: 2

Absent Time(Unit): hours

Absent Time Value: 1

Absent Time(Unit): minutes

Absent Time Value: 5

CMC SecureApp Only

- **Language** - Select the console language from the drop-down. Currently only 'English' is supported.
- **Timezone** - Select the management console operational timezone.
- **Password Expiration Days** - The number of days after which the management console password must be changed. The maximum number of days that can be set is 90 days. Enter the days or increase/decrease the days from the combo box.
- **Unreachable Endpoint Time Limit (Unit)** - The unit of time for the 'Unreachable Endpoint Time Value' setting. The options available are:
 - Disable
 - Hours
 - Days
 - Weeks
- **Unreachable Endpoint Time Value** -The maximum time an endpoint can go without contacting the management console before CSB applications will be prevented from launching on that endpoint. For example, if this value is set to 1 and the time unit is set to 'Days' then CSB applications will not be allowed to launch on the endpoint if communication is lost for more than 1 day. After the endpoint starts to communicate with CMC it will be allowed to run CSB applications again.
 - Enter the value or increase/decrease the value from the combo box.
- **Absent Time (Unit)** and **Absent Time Value** – CSB shows an alert icon in the 'Computers' screen if an

endpoint has been unresponsive for a period of time.

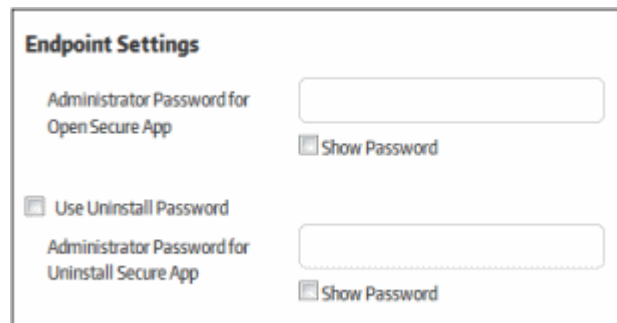
- Red icon - Define how much time should pass without communication from an endpoint before the red icon is shown. Icons appear next to 'Connection' in the '**Computers**' screen.
- Yellow icon - Define how much time should pass without communication from an endpoint before the yellow icon is shown. Icons appear next to 'Connection' in the '**Computers**' screen.

For example, if you want to display the red icon in the 'Computers' screen for endpoints that are not connected to CMC for more than a day, then select 'Days' from the Absent Time (unit) drop-down and '1' from the 'Absent Time Value' drop-down.

- **CMC Secure App Only** - If selected, only CSB applications which use policies from this management console will be allowed to run. CSB applications copied from another policy or created with the SAW (Secure Application Wizard) tool will not be allowed to run on endpoints.

Endpoint Settings

Endpoint settings allow you to set passwords to open and uninstall secure box apps.



Endpoint Settings

Administrator Password for Open Secure App Show Password

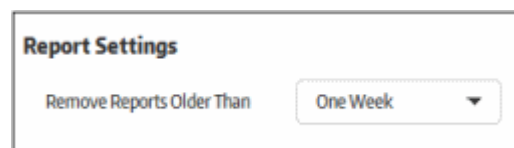
Use Uninstall Password

Administrator Password for Uninstall Secure App Show Password

- Administrator Password for Open Secure App – Specify a password which must be entered before a secure application will launch on an endpoint. This works only for secure applications which have 'Open Password' set under the 'SECURE APPS' tab when creating a secure application.
- Use Uninstall Password – Choose whether or not a password is required to uninstall a secure app from an endpoint. Users will be prompted to enter the password before uninstallation will continue.
- Administrator Password for Uninstall Secure App – Specify the uninstall password.

Report Settings

Allows you to set the report period that will be displayed on the 'Reports' section.



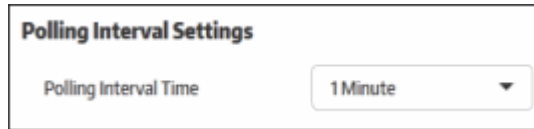
Report Settings

Remove Reports Older Than

- Remove Reports Older Than - Threat and activity reports for your account will be removed from the server as per the period set here.

Polling Interval Settings

Allows you to set the frequency at which CSB communicates with CMC to check for various updates.



- Polling Interval Time - Select the frequency at which CSB on the endpoints connects to the management console to check for updates. Available frequencies range from 15 seconds to 2 minutes.

External Services

Allows you to configure global settings for external services such as log server, time server and Secure Box installer upgrade server.



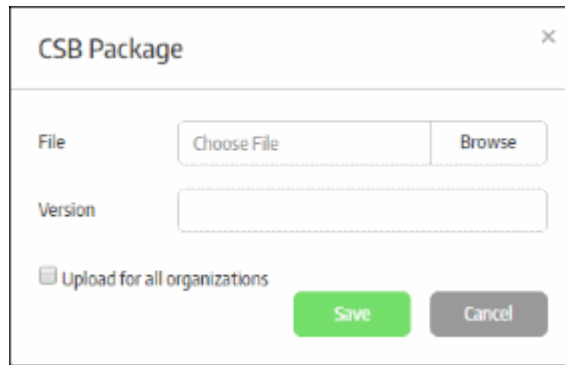
- Log Server – Global Log Server setting. Enter the address of the server to which endpoint should send logs. Once set, the 'Log Server' field in the 'Management' tab will be filled with the global setting when creating a secure application.
- Time Server – Global Time Server setting. Enter the address of the server that endpoints should use to sync their system time. Once set, the 'Time Server' field in the 'Settings' tab will be filled with the global setting when creating a secure application.
- Secure Box Installer Upgrade Server – Global Upgrade Server setting. Enter the address of the server you wish to use to provision updates to CSB applications on endpoints. Once set, the 'Upgrade Server' on the 'Management' tab will be filled with the global setting when creating a secure application.

Packages

Allows you to upload CSB installation files which will become available for selection when enrolling endpoints.



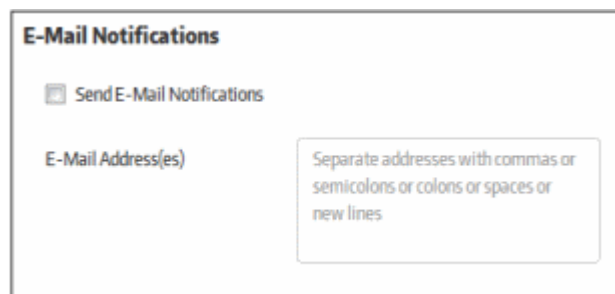
- To upload the latest CSB installer package, click 'Manual Upload of SecureBox Package'



- Click 'Browse', navigate to the location where the package is stored and click 'Open'
- Enter the version number of the package in the 'Version' field.
- Upload for all organizations – If enabled, the CSB package will be uploaded to all organizations in your account.
- Click the 'Save' button.
- To delete a package, click the 'Remove' button
- To upgrade CSB on endpoints, select the package and click the 'Upgrade Now' button. The enrolled endpoints will be automatically updated to the selected application.
- If there was some problem during CSB installation on the endpoints, or if the application is malfunctioning, select the package(s) and click the 'Repair' button. The respective CSB applications on the endpoints will be repaired remotely.

Email Notifications

Allows you to configure email settings for threat notifications, endpoint activities and licenses.



- Send E-Mail Notifications - If enabled, email notifications will be sent to the specified email addresses for enabled categories. Categories include threat notifications, endpoint activities and licenses. If this setting is disabled, no notifications will be sent, even if 'threat', 'activity' and 'license' notifications have been enabled individually.
- E-Mail Address(es) - Enter the email addresses of administrators to whom the configured notifications should be sent.

Threat Notifications

Enable notifications to be sent when certain categories of threat are discovered.

Threat Notifications

Send Threat Notifications

CATEGORY	STATUS	THRESHOLD
----------	--------	-----------

Add New

- Send Threat Notifications - If enabled, threat notifications will be sent to the recipients listed in the 'Email Notifications' area.
- To configure a new threat notification, click the 'Add New' button.

Threat Notifications [X]

Category: Sniffing Attempt

Status: Enabled [v]

Threshold: 2 [icon]

Save **Cancel**

- Category - The type of threat that you want to receive notifications about. Refer to the section '**Threats Report**' for more details on threat categories.
- Status – Select whether you want to enable or disable notifications for this category.
- Threshold – The number of threats detected of this type before a notification is sent.
- Click the 'Save' button.

Activity Notifications

Configure if, and upon which events, you want to receive activity alerts.

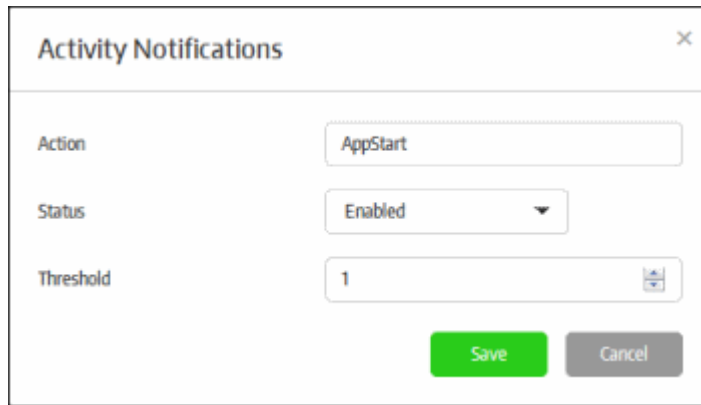
Activity Notifications

Send Activity Notifications

ACTION	STATUS	THRESHOLD
--------	--------	-----------

Add New

- Send Activity Notifications - If enabled, endpoint activity notifications will be sent to the recipients listed in the 'Email Notifications' area.
- To configure a new activity notification, click the 'Add New' button.



The screenshot shows a window titled "Activity Notifications" with a close button (X) in the top right corner. Inside the window, there are three rows of configuration options:

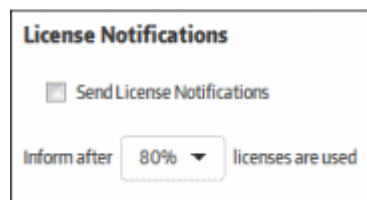
- Action:** A text input field containing "AppStart".
- Status:** A dropdown menu currently set to "Enabled".
- Threshold:** A text input field containing "1" with a small up/down arrow icon to its right.

At the bottom of the window, there are two buttons: a green "Save" button and a grey "Cancel" button.

- Action - The type of activity that you want to receive notifications about. Refer to the section '**Activity Report**' for more details on action categories.
- Status – Select whether you want to enable or disable notifications for this type of activity.
- Threshold – The number of activities detected of this type before a notification is sent.
- Click the 'Save' button to apply your choices.

License Notifications

Receive alerts if the number of enrolled endpoints hits a certain percentage of the maximum allowed by your license.

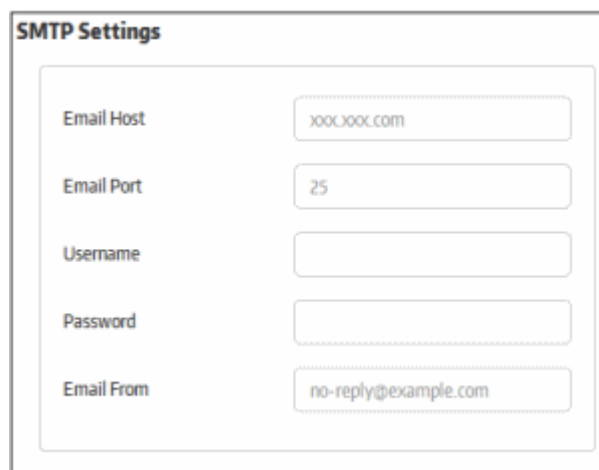


The screenshot shows a window titled "License Notifications". It contains a checkbox labeled "Send License Notifications" which is checked. Below this, there is a label "Inform after" followed by a dropdown menu set to "80%" and the text "licenses are used".

- Send License Notifications – Enable or disable license notifications. Notifications will be sent to subscribed administrators if the number of enrolled endpoints hits a certain % of your license allowance.
- Specify the percentage of licenses consumed. Notifications will be sent to subscribed administrators if the number of enrolled endpoints hits this percentage of your license allowance.

SMTP Settings

Allows you to configure the outgoing mail server you want to use for sending email notifications.



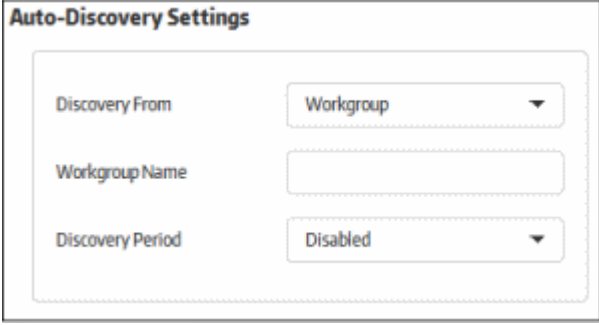
The screenshot shows a window titled "SMTP Settings". It contains five rows of configuration options, each with a label and a text input field:

- Email Host:** xoox.xoox.com
- Email Port:** 25
- Username:** (empty field)
- Password:** (empty field)
- Email From:** no-reply@example.com

- Email Host - Enter the SMTP server from which notification mails will be sent
- Email Port - Enter the outgoing port of the SMTP server
- Username - Enter the username for the email account from which the notification mails are to be sent
- Password - Enter the password for the email account
- Email From - Enter the address to be displayed in the 'From' field of notification emails

Auto-Discovery Settings

Allows you to configure 'Active Directory' and 'Workgroup' in order to enroll endpoints within a network



The screenshot shows a form titled "Auto-Discovery Settings". It contains three fields:

- Discovery From:** A dropdown menu with "Workgroup" selected.
- Workgroup Name:** An empty text input field.
- Discovery Period:** A dropdown menu with "Disabled" selected.

- Discovery From – Specify where you will import endpoints from. The options available are 'Active Directory' and 'Workgroup'
- If 'Active Directory' is selected, provide the following details:
 - Domain to scan – Enter your AD domain name
 - Host – The host name or IP address of the AD server
 - Username – The username of an AD administrator account
 - Password – The administrator password
- If 'Workgroup' is selected, provide the following details:
 - Workgroup Name – Enter the name of the workgroup in the network
- Discovery Period – Specify the time intervals at which the console should scan for endpoints in the network. If enabled, the console will periodically run scans at the set interval to discover new endpoints. If 'Disabled', then no scanning will be performed.

Code Signing Certificate

Allows you to upload a code signing certificate which will be used to sign your secure applications. CSB on the endpoints will check the certificate and, if validated, will allow the secure application to run. The code signing certificate section is divided into 2 parts: SHA2 and SHA1 certificate. Secure applications will be signed with both of these certificates if they are configured. SHA2 is the stronger, industry standard algorithm and is accepted by all modern operating systems. A SHA1 certificate is only required if you plan to run your secure application on Windows XP.

Code Signing Certificate

Upload sha2 certificate

File: N/A
Uploaded: N/A

Upload Revoke

Upload sha1 certificate for compatibility

File: N/A
Uploaded: N/A

Upload Revoke

Note - If you do not have a code signing certificate, please contact your Comodo account manager.

- To upload a certificate, click the 'Upload' button

Upload Certificate

File Choose File

Keystore Password

Cert Password

Upload for all organizations

Upload Cancel

- Click 'Browse', navigate to the location where the certificate is stored and click 'Open'
- Enter the 'Keystore' and 'Cert' passwords in the respective fields. Normally, the same password can be used for both.
- Upload for all organizations – If enabled, the certificates will be added for all organizations in your account.
- Click the 'Upload' button.

The certificate will be uploaded and its details will be displayed under the 'Code Signing Certificate' section. This certificate will be used to sign your secure apps when you create them.

Code Signing Certificate

Upload sha2 certificate

File: codesign_new.pfx
Uploaded: 2016-08-29T14:07:34+00:00

Upload Revoke

Upload sha1 certificate for compatibility

File: Code_Sign_cert_sha1.pfx
Uploaded: 2016-09-05T09:43:17+00:00

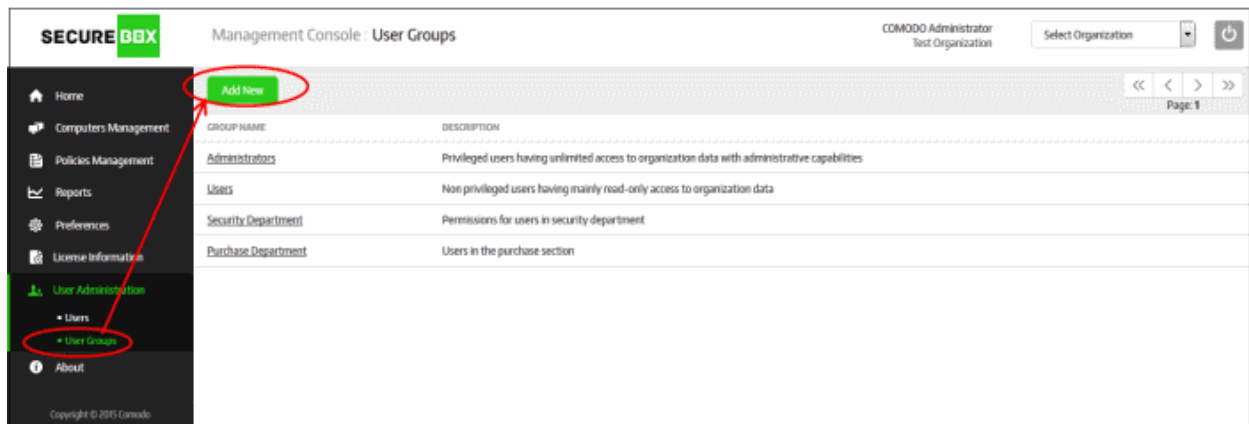
Upload Revoke

- To revoke the existing code signing certificate, click the 'Revoke' button. You will need to upload a new, valid code signing certificate in order to sign your applications.
- Click the 'Save' button to apply your changes.

Step 5 – Add User-Groups and Users

Users that are added to the management console must be placed in a group in order to manage an organization. CMC has two default groups - Administrators and Users. The 'Administrators' group has access to all major functionality while the 'Users' group has limited privileges. You can also create custom user groups with more nuanced privilege levels as per your organization's requirements.

To add user groups, click 'User Administration' on the left and then 'User Groups' below it:



- Click the 'Add New' button

The 'User Group Properties' dialog box has the following fields and table:

Title:

Description:

PERMISSION	READ	WRITE
User Management	<input type="checkbox"/>	<input type="checkbox"/>
Policy Management	<input type="checkbox"/>	<input type="checkbox"/>
Computer Management	<input type="checkbox"/>	<input type="checkbox"/>
Organization Preferences	<input type="checkbox"/>	<input type="checkbox"/>
License	<input type="checkbox"/>	<input type="checkbox"/>
Reports Access	<input type="checkbox"/>	

Buttons: Delete Group, Save, Cancel

- Title - Enter the name of the group
- Description - Enter an appropriate description for the group
- Permissions – Allows you to define read/write privileges for the users in the group
 - Read – Only view privilege

- Write – Add, edit and delete privileges

You can configure group permissions for the following items:

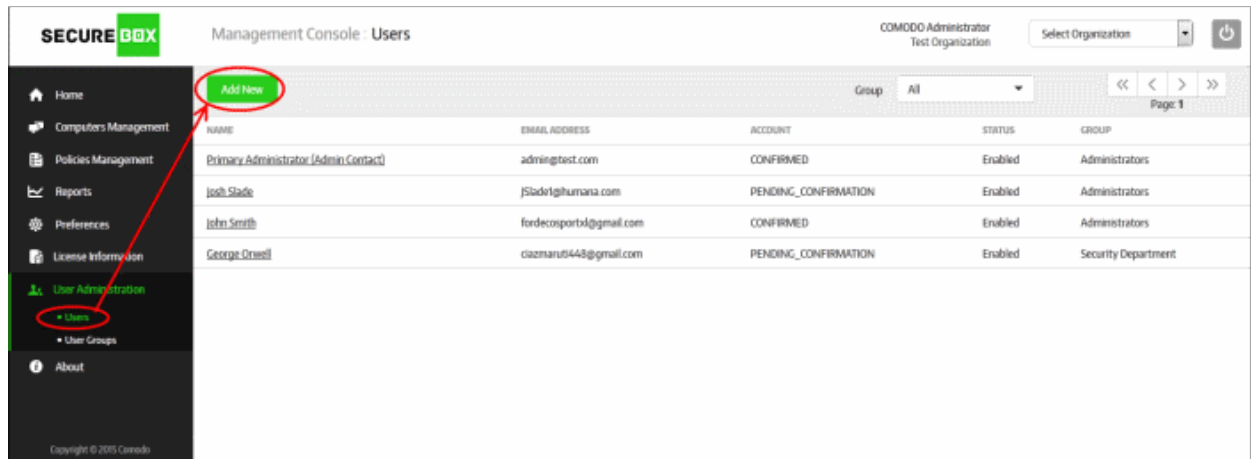
User Group Privileges	
Form Element	Description
User Management	Allows group members to add and configure users and user groups. Refer to the section ' Users and User Groups ' for more details.
Policy Management	Allows group members to create and edit CSB policies. Refer to the section ' Policies ' for more details.
Computer Management	Allows group members to enroll new endpoints, create groups, assign policies and more. Refer to the section ' Endpoints and Endpoint Group ' for more details.
Organization Preferences	Allows group members to configure management console settings. Refer to the section ' Configuring the Management Console ' for more details.
License	Allows group members to view the current license and add additional licenses. Refer to the section ' License Information ' for more details.
Reports Access	Allows group members to view and create threat and activity reports. Refer to the section ' Reports ' for more details.

- Select the privileges you would like for the group and click the 'Save' button

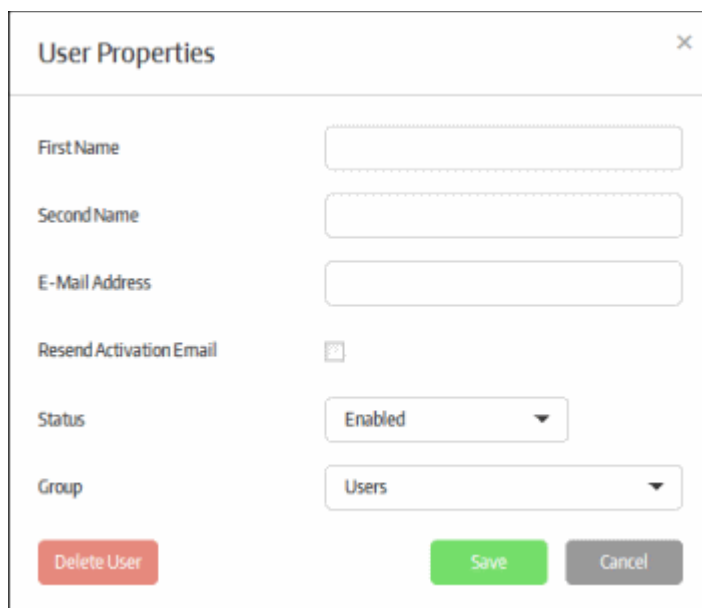
Once saved, the new user group will be available for selection when adding/editing users. Users assigned to the group will be able to manage the organization according to group privileges.

Now, the next step is add users.

To add users, click 'User Administration' on the left and then 'Users' below it:



- Click the 'Add New' button.



- First Name - Enter the first name of the user.
 - Second Name - Enter the surname of the user.
 - E-Mail Address - Enter the email address of the user. The activation mail will be sent to this address.
 - Resend Activation Email - Allows you to send another activation email if the password in the initial mail has lapsed, or if the user is removed and added again with the same email address. Click 'Save' to resend the mail.
 - Status - Select whether the user should be allowed to access the management console. An activation mail will be sent to the user even if 'Disabled' is selected. However the user cannot access the management console until the access is enabled by the administrator.
 - Group - Select the group to which the user should belong. Groups can be created in the 'User Groups' section explained above.
- Click the 'Save' button.

An email will be sent to the user which contains an activation link and a temporary password. The user's account will be activated on clicking the activation link in the mail and the user can access the management console using the temporary password. It is advisable the user changes the password immediately for continued access to the console.

For more details about users and user-groups, refer the section '[Users and User Groups](#)'.

Step 6 – Add Policies and Secure Items

In order to deploy secure applications onto endpoints you first have to create a policy, or use the default policy that ships with CMC. You can add multiple secure applications to a policy according to your organization's requirements. The policy can then be assigned to an endpoint group, which may have a single endpoint or multiple endpoints. The secure apps in the policy will be automatically rolled out to the endpoint(s) in the group.

To add policies, click 'Policies Management' on the left:

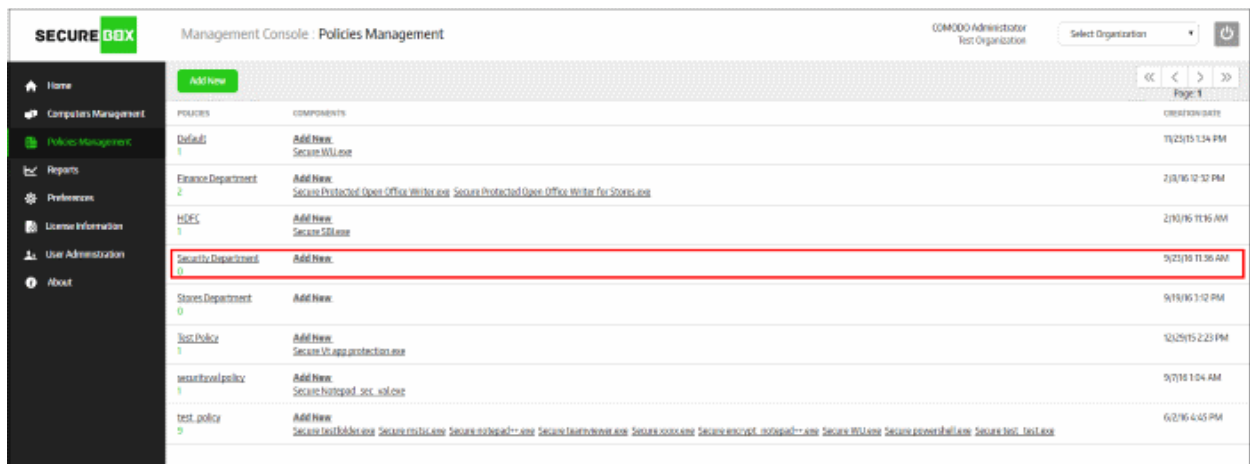


- Click the 'Add New' button

The 'Policy Properties' dialog box has a title bar with a close button. It contains two text input fields: 'Policy Name' and 'Description'. At the bottom, there are three buttons: 'Delete' (red), 'Save' (green), and 'Cancel' (grey).

- Policy Name - Create a name for the policy
- Description – Add an appropriate description for the policy
- Click the 'Save' button

The policy will be added and listed in the 'Policy Management' screen:



The next step is to and and configure the secure application(s) for the policy. Click the 'Add New' link under the 'Components' column.

The 'Application Policy Properties' screen will be displayed:

There are three types of secure application:

- **URL Mode** – A specific URL will be opened in a browser inside the secure box environment. For example, this might be the URL of a company portal or web application. Refer to '**Configuring a Secure URL**' for more details.
- **APP Mode** – A specific application on the endpoint will be run inside the Secure Box environment. Doing so will protect the application from attack from any local or internet threats. You may also configure the application to only open in the SB environment. Refer to '**Configuring a Secure APP**' for more details.
- **Folder Mode** – A specific folder or an entire partition can be protected. Any item opened on the protected folder or drive will be run inside the secure environment. Items inside the protected folder can be configured not to run outside of CSB. Refer to '**Configuring a Secure Folder**' for more details.

After specifying the type of application, you can configure more granular settings as follows:

- **Secure Apps** tab – Configure basic information and protection settings for the secure application
- **Management** tab – Allows you to configure a local server for updating CSB, the root certificate list, redirect FLS URL, CAM URL and more. Please note this tab can be configured if the organization has a strict network environment and does not allow internet updates.
- **Settings** tab – Configure basic settings for the secured item.
- **Encryption** tab – Specify paths for data that should be encrypted and accessible with read/write permissions for secure apps only.
- **Filtering** tab – Define checks for a secured environment - such as to allow only certain applications to

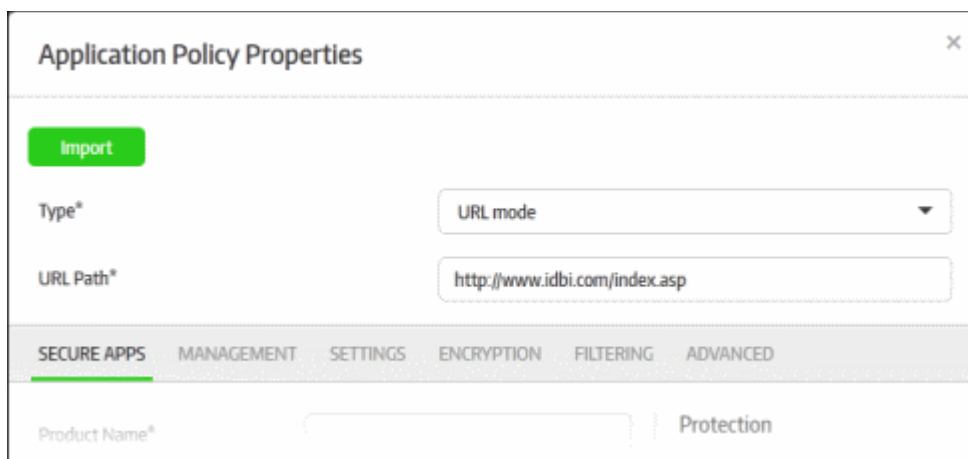
run, to block certain IP ranges and so on.

- **Advanced** tab – Configure advanced settings for IE based secure applications as well as define actions for the 'Root Cert Check' feature.

The parameters in the sections differ depending on the type of app selected. Refer to '**Configuring Granular Secure Box Application Settings**' for more details.

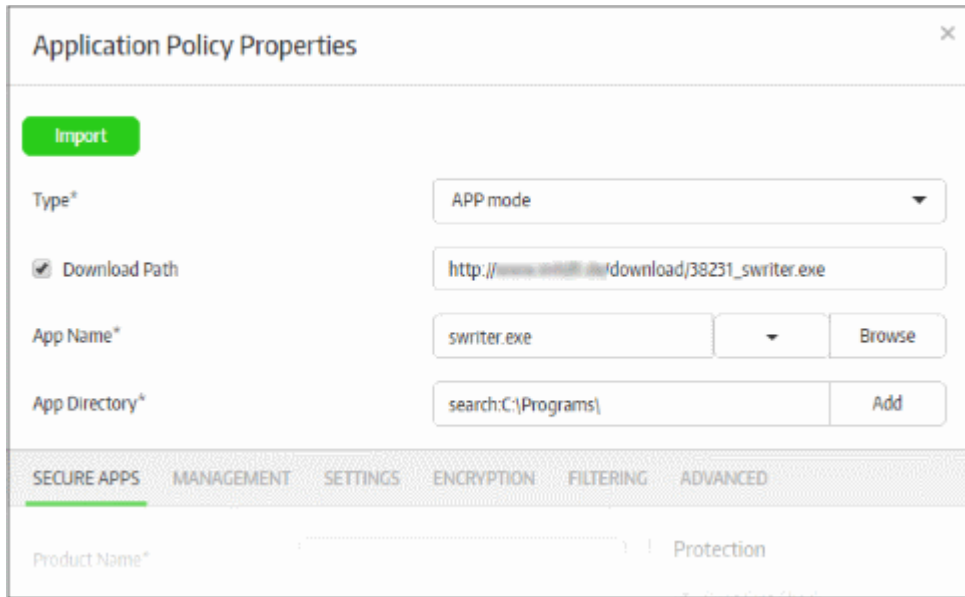
Configuring a Secure URL

- Select 'URL mode' from the 'Type' drop-down
- Enter the URL that you want to secure in the 'URL Path' field



Configuring a Secure APP

- Select 'APP mode' from the 'Type' drop-down
- Enter your application's name in the 'App Name' field (this should have .exe extension). Alternatively, click the 'Browse' button, navigate to the location of the application and click the 'Open' button. Note that the 'Vendor' and 'SHA1' fields will be auto-populated in the 'Secure Apps' section if you select the 'Browse' method. If you want to define the 'Vendor' and 'SHA1' fields manually, then type the app name instead. When the application is run, CSB will check if the admin defined vendor and SHA1 values match with its own. The app will be allowed to run only if there is a match. The drop-down allows you to select Word, Excel or Powerpoint apps. If any of these are selected then app name and app directory will be configured automatically.
- Enter the full path of the application that you want to secure in the 'App Directory' field. You can also enter search parameters here. For example, to search the folders for the app, enter 'search: C:\Programs\...' without the quotes. Application paths support system variables. For example, C:\Users\%username%\app\app.exe
- Download Path – If some of the endpoints do not have the configured app, then enable this option and enter the download path of the application. If the application is not installed on the endpoints it will be downloaded and installed during the secure application launch.



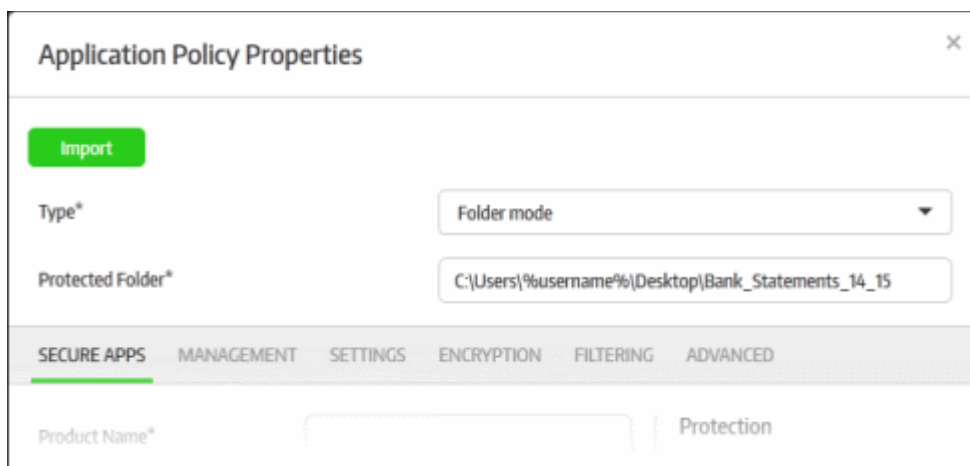
- Click the 'Add' button

The app (along with vendor name and SHA1 values if selected) will be added to the management console. Repeat the process to add more secure apps. To remove an application path, click the 'Remove' link beside it.

Configuring a Secure Folder

- Select 'Folder mode' from the 'Type' drop-down
- Enter the full path of the folder that you want to secure in the 'Protected Folder' field

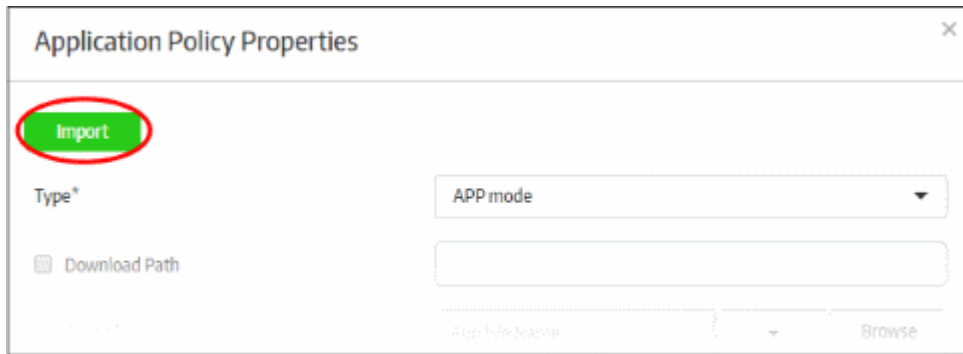
The path of folders support system variables. For example, C:\Users\%username%\Desktop\folder_name



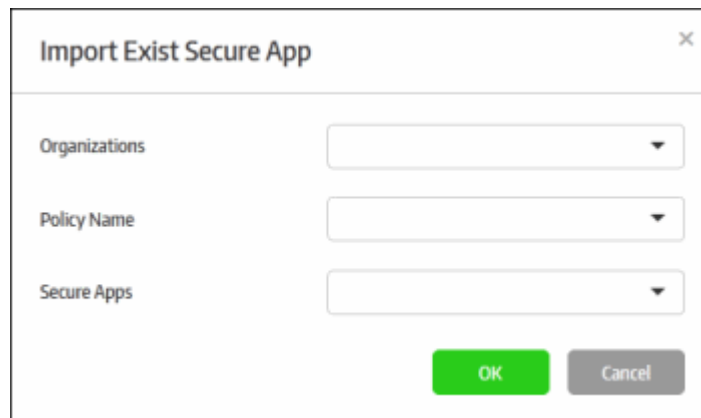
To create a new policy using an existing policy as a base

CMC allows administrators to create a new policy using the policy of an existing app. This can save time when rolling out a new policy, with or without modifications, to other endpoint groups.

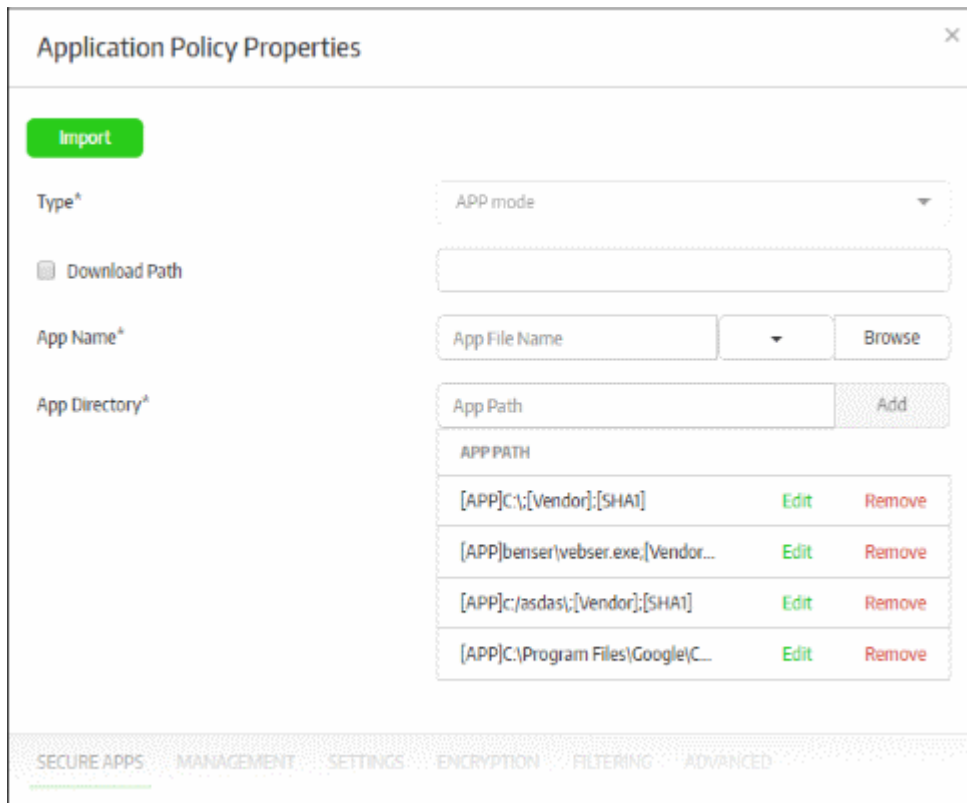
To import the settings of an existing policy, click the 'Add New' link or on the name of a secure app under 'Components' and click the 'Import' button at the top.



The 'Import Exist Secure App' dialog will be displayed.



- **Organizations** – Lists the organizations available for the account. Select the organization from which you want to import a policy. Please note this feature will be available for administrators with super admin privileges only.
- **Policy Name** – Lists all the policies available in the selected organization. Select the policy from the drop-down.
- **Secure Apps** – Lists all the secured items that are configured for the selected policy. Select the secured item from the drop-down that you want to import.
- Click 'OK'.

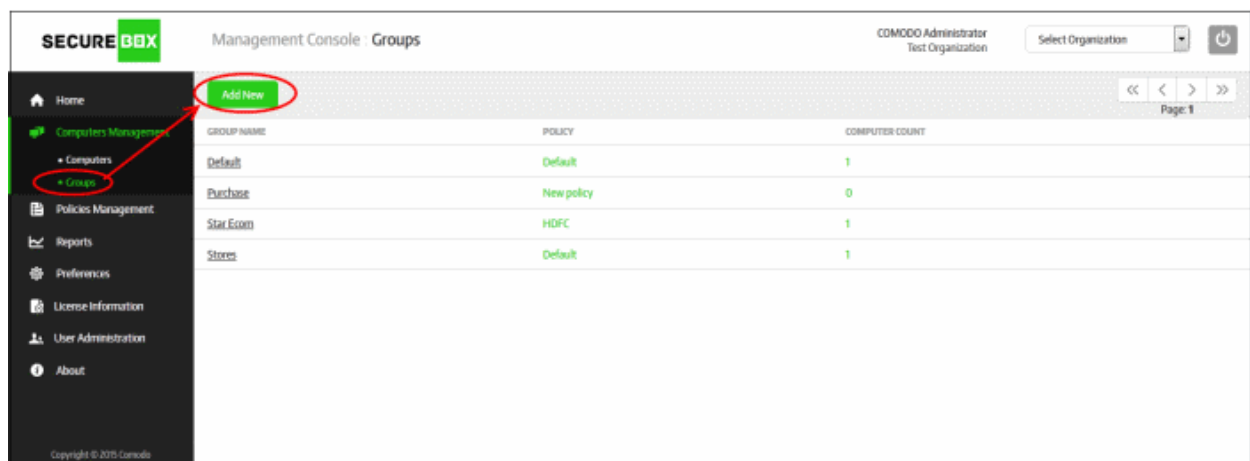


The secure item will be imported with all its settings including the product name. You can save it with the same settings or modify them according to requirements. This is similar to the process explained earlier in step 6 when creating a new policy. [Click here](#) to find out more about configuring settings in an imported policy.

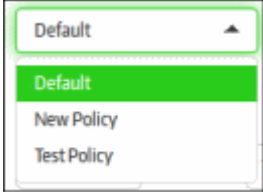
Step 7 – Add Endpoint Groups and Enroll Endpoints

When a policy with secure applications is assigned to an endpoint group, all secure applications in the policy are installed on the endpoints. CMC ships with a default group. Endpoints that are enrolled via the email method are automatically placed in this group.

To create a new endpoint group, click 'Computers Management' on the left and then 'Groups' below it:



- Click the 'Add New' button

Group Properties – Form Parameters	
Form Element	Description
Log Filter	Select which events should be recorded in group logs. Refer to the section ' Reports ' for more details.
Group	Enter the name of the endpoint group
Description	Enter an appropriate description for the group
Policy	<p>Select the policy to be applied to the endpoints from the drop-down.</p>  <p>The policies available from drop-down are configured from the 'Policies Management' section. Refer to the section 'Creating a New Policy' for more details about adding new policies.</p>

Quarantine Duration (Week Day)	Select the day of the week on which the quarantine should apply. Refer to ' To schedule quarantine period for the endpoint group ' for more details.
Quarantine Duration Time	Enter the quarantine time duration for the selected quarantine day. Refer to ' To schedule quarantine period for the endpoint group ' for more details.
Quarantine Times	Displays the quarantine schedule. Refer to ' To schedule quarantine period for the endpoint group ' for more details.

To schedule quarantine period for the endpoint group

Quarantining prevents the secure items on the endpoints from opening. You can automate the process of quarantining endpoints in the group.

- Select the week day that you want to enforce the quarantine from the 'Quarantine Duration (Week Day)' drop-down

- Enter the quarantine time duration time the selected quarantine day in the 'Quarantine Duration Time' fields

- Click the 'Add' button below

Repeat the process for scheduling more quarantines. The scheduled quarantines will be listed below 'Quarantine Times'

Quarantine Transitions (WeekDay) Sunday

Quarantine Duration Time 8:30 To 18:45

Add

QUARANTINE TIMES	
Wednesday, 9:00-12:00	Remove
Friday, 0:00-12:30	Remove
Sunday, 0:00-23:59	Remove

Delete Group Save Cancel

Now, the secured items configured for the selected policy will be automatically blocked from opening on the endpoints in the group.

- To remove a quarantine schedule from the list, click the 'Remove' link beside it
- Click the 'Save' button

The new endpoint group will be added and displayed in the list.

The next step is to enroll endpoints.

To enroll endpoints, click 'Computer Management' on the left and then 'Computers' below it:

SECURE BOX Management Console : Computers

Home Add New Deploy Package Move to Group

Computers Management

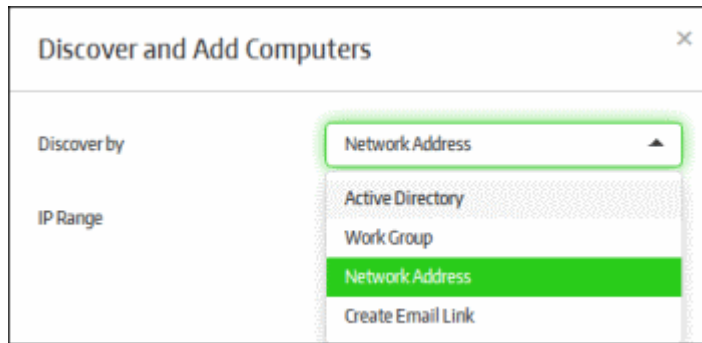
- Computers
- Groups

Policies Management Reports Preferences License Information User Administration

CONNECTION	ABSENT TIME	COMPUTER ID
	11 hours	IE11W017
	0 minute	ANM009C
	0 minute	DESK:10-4894991
	16 hours	-

- Click the 'Add New' button.

The 'Discover and Add Computers' dialog will be displayed:



There are four ways to enroll endpoints:

- **Active Directory**
- **Work Group**
- **Network Address**
- **Create Email Link**

The first three methods are particularly useful for enrolling endpoints within a network (on-premise installation) and the last method is suitable for endpoints outside the network. Refer to the section '**Initial Setup**' for more details.

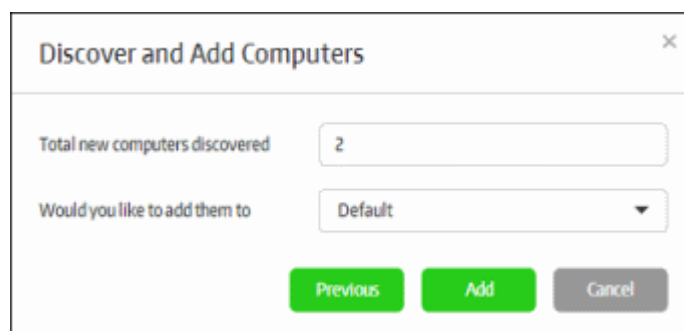
Enrolling using Active Directory, Work Group or Network Address

Please note endpoint enrollment via AD will work only if CMC is added into domain during premise installation and the other two methods, Work Group and Network Address, will work only if CMC is not added during installation. The email enrollment will work for all the methods. Refer to the section '**Initial Setup**' for more details.

Select the appropriate method from the drop-down:

- If you choose 'Active Directory', you next have to enter the IP address of the domain controller, name of the domain and the administrator username and password for that domain.
- If you choose 'Work Group', then you have to enter the name of the work-group.
- If you chose 'Network Addresses', you next have to specify the IP range.
- Click the 'Start' button.

The management console will run a scan to discover endpoints and if available, will show the number of endpoints discovered and provide the option to add them to endpoint groups. Refer to the sections '**Creating a New Endpoint Group**' and '**Assigning Endpoints to Groups**' for more details.



- Select the endpoint group from the 'Would you like to add them to' drop-down and click the 'Add' button.

The newly enrolled endpoints will be added to the 'Computers' screen:

MESSAGE	CONNECTION	ABSENT TIME	COMPUTER NAME	EXTEND	ALIAS	MACHINE ID	GROUP NAME	STATUS	CSB VERSION	CREATED	DISCOVERED AS	SOURCE
<input type="checkbox"/>		--/--	DESKTOP-TTPO5PR				Default	TBC		2/2/17 3:47 PM	DESKTOP-TTPO5PR	MANUAL
<input type="checkbox"/>		104 days	IE11Win7	569		4AEF7DC2B486874D84F7269771DE52D	Default	MCD	2.10.397304.436	7/27/16 1:02 AM	IE11Win7	EMAIL
<input type="checkbox"/>		0 minute	VMWIN10CONTENT	AB12CE	John Computer	4508D08F37E3A485786FFED93C28BE94E	Purchase	MCD	2.11.401468.430	2/20/17 12:47 PM	VMWIN10CONTENT	MANUAL
<input type="checkbox"/>		133 days	BURSER-C32BA071				test group			9/22/16 7:37 PM	BURSER-C32BA071	MANUAL
<input type="checkbox"/>		133 days	WIN-060HRIA0VA			9488B358003421D218149610132FFD9	test group	MCD	2.11.400703.428	9/22/16 1:55 PM	WIN-060HRIA0VA	MANUAL
<input type="checkbox"/>		129 days	WIN-BLMD39HJL2F			19208AB97A307882337CF6D478210E83	DEMO	MCD	2.6.380060.373	9/22/16 4:28 PM	WIN-BLMD39HJL2F	MANUAL
<input type="checkbox"/>		109 days	TEST_TOOLS				kedragon	TBC		10/27/16 6:41 PM	TEST_TOOLS	MANUAL
<input type="checkbox"/>		77 days	ANM0124	PDM			PDM_TEST			11/7/16 2:55 PM	ANM0124	MANUAL

The next step is to deploy the CSB package that should be installed on the endpoints. Installing a package will allow you to assign policies and manage the endpoint.

MESSAGE	CONNECTION	ABSENT TIME	COMPUTER NAME	EXTEND	ALIAS	MACHINE ID	GROUP NAME	STATUS	CSB VERSION	CREATED	DISCOVERED AS	SOURCE
<input checked="" type="checkbox"/>		--/--	DESKTOP-TTPO5PR				Default	TBC		2/2/17 3:47 PM	DESKTOP-TTPO5PR	MANUAL
<input type="checkbox"/>		104 days	IE11Win7	569		4AEF7DC2B486874D84F7269771DE52D	Default	MCD	2.10.397304.436	7/27/16 1:02 AM	IE11Win7	EMAIL
<input type="checkbox"/>		0 minute	VMWIN10CONTENT	AB12CE	John Computer	4508D08F37E3A485786FFED93C28BE94E	Purchase	MCD	2.11.401468.430	2/20/17 12:47 PM	VMWIN10CONTENT	MANUAL
<input type="checkbox"/>		133 days	BURSER-C32BA071				test group			9/22/16 7:37 PM	BURSER-C32BA071	MANUAL
<input type="checkbox"/>		133 days	WIN-060HRIA0VA			9488B358003421D218149610132FFD9	test group	MCD	2.11.400703.428	9/22/16 1:55 PM	WIN-060HRIA0VA	MANUAL
<input type="checkbox"/>		129 days	WIN-BLMD39HJL2F			19208AB97A307882337CF6D478210E83	DEMO	MCD	2.6.380060.373	9/22/16 4:28 PM	WIN-BLMD39HJL2F	MANUAL
<input type="checkbox"/>		109 days	TEST_TOOLS				kedragon	TBC		10/27/16 6:41 PM	TEST_TOOLS	MANUAL
<input type="checkbox"/>		77 days	ANM0124	PDM			PDM_TEST			11/7/16 2:55 PM	ANM0124	MANUAL
<input type="checkbox"/>		97 days	ANM0096				PDM_TEST			11/7/16 2:55 PM	ANM0096	MANUAL

- Click the 'Deploy Package' button after selecting the endpoint

The 'Deploy Package' dialog will be displayed.

- Select the package to deploy to the selected endpoint from the first field.
- Enter the Active Directory domain credentials and click the 'Start' button

The selected package will be deployed and the status of the endpoint will change to 'MGD TBC' - meaning it has to be accepted by the administrator. If the 'Auto accept' option was enabled while adding the organization, then enrolled endpoints will be automatically accepted. Refer to the section '**Adding a New Organization**' for more details.

- Select the endpoint and click 'Accept'.

The 'Accept Confirmation' dialog will be displayed.

- **Alias Name** (Optional) - Specify an alternative name for the endpoint so you can easily track it in the console.
- **Extra ID** (Optional) - The 'Extra ID' is an identification tag assigned to the endpoint. This tag is added to the X-token of the HTTP header in the HTTP requests generated by secure URL applications from the endpoint. The console uses the extra ID and the machine ID to authenticate the endpoint during initial registration and subsequent connection requests. Extra IDs should be specified as a combination of letters and numbers in the text box.

- Click 'Yes' (if Auto-accept is enabled for the organization, click on the blank fields under Alias and Extra ID columns in the 'Computers' screen and provide the alias and extra ID details).

The endpoint will show as connected and managed in the screen and the policy assigned to the endpoint group will be applied to the endpoints.

Enrolling using email method

- Click the 'Create Email Link' option from the drop-down:

The 'Package to Deploy' drop-down displays all CSB applications uploaded by the administrator.

- Select the installer package from the drop-down
- Deploy with script file / Deploy with executable file - You have the option to install the package via script or executable.
- Enter the email address to which the CSB installer package download link will be sent and click the 'Add' button. Repeat the process to add more recipients.

Discover and Add Computers

Discover by: Create Email Link

Package To Deploy: csb_installer.msi (2.6.380060.373BR)

- Deploy with script file
- Deploy with executable file

Email Address

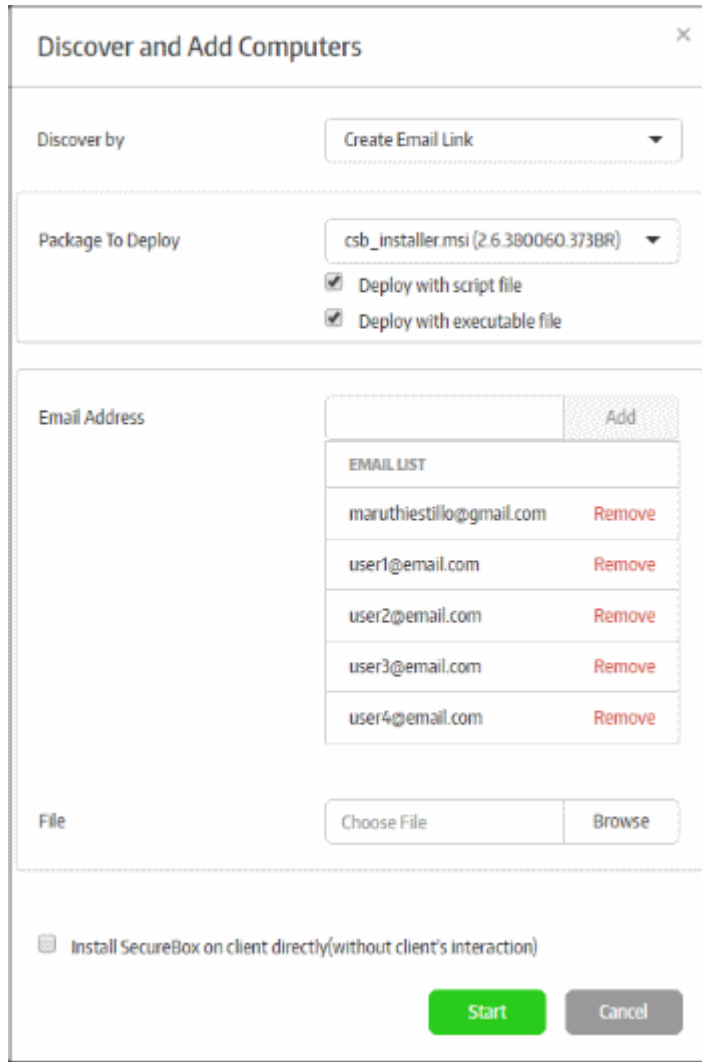
Email Address	Action
EMAIL LIST	
maruthiestillog@gmail.com	Remove

File: Choose File | Browse

Install SecureBox on client directly (without client's interaction)

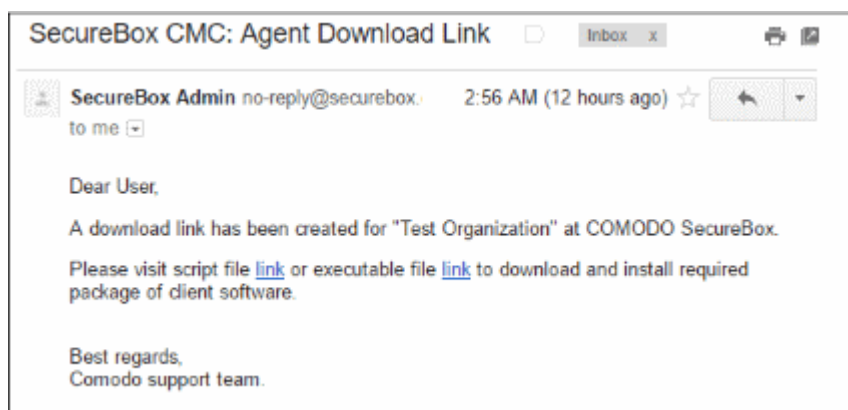
Start | Cancel

- For bulk enrollment, you can use the 'File' option. Recipient email addresses should be entered on each line of a .txt file. Click 'Browse', navigate to your file and click the 'Open' button. All imported recipients will be listed in the dialog:



- To remove a recipient, click the 'Remove' link.
- 'Install Secure Box on client directly (without client's interaction)' – If selected, the endpoint user will only see the installation progress bar. They will not be shown the EULA or the configuration page.
- Click the 'Start' button

The endpoint user(s) will receive an email from Comodo containing the CSB app download link(s).



The user should click any of the links to download the CSB installer package and save it on the endpoint. After CSB is installed on the endpoint and restarted, it will appear on the 'Computers' screen as 'MGD TBC' - meaning the endpoint has to be approved by the administrator. If 'Auto accept' was selected when you created the organization

then enrolled endpoints will be automatically accepted. Refer to the section '[Adding a New Organization](#)' for more details.

MESSAGE	CONNECTION	ABSENT TIME	COMPUTER NAME	EXTRA ID	ALIAS	MACHINE ID	GROUP NAME	STATUS	CSB VERSION	CREATED	DISCOVERED AS	SOURCE
<input type="checkbox"/>		--/--	DESKTOP-TTPO9PR				Default	TBC		2/21/17 3:47 PM	DESKTOP-TTPO9PR	MANUAL
<input type="checkbox"/>		104 days	IE17WH7	509		4AEF7DC2B4886874D84F7269771DE52D	Default	MCD	2.10.397304.495	7/27/16 1:02 AM	IE17WH7	EMAIL
<input type="checkbox"/>		0 minute	VMWIN10CONTENT	AB10CE	John Computer	4508D08F3E3A4B5786FFED93C2BBE94E	Purchase	MCD	2.11.401468.430	2/23/17 12:47 PM	VMWIN10CONTENT	MANUAL
<input type="checkbox"/>		133 days	BURSER-C32BA071				test group			9/22/16 7:37 PM	BURSER-C32BA071	MANUAL
<input type="checkbox"/>		133 days	WIN-060HRIA0VA			948B3358003A21D21B1496150132FFD9	test group	MCD	2.11.400703.428	9/22/16 1:55 PM	WIN-060HRIA0VA	MANUAL
<input type="checkbox"/>		129 days	WIN-BLMD09HJUZ			192084857A307882337CF6D478210E83	DEMO	MCD	2.6.380060.373	9/22/16 4:28 PM	WIN-BLMD09HJUZ	MANUAL
<input type="checkbox"/>		109 days	TEST_TOOLS				kedragon	TBC		10/23/16 6:41 PM	TEST_TOOLS	MANUAL
<input type="checkbox"/>		77 days	ANM0124	PDM			PDM_TEST			11/7/16 2:55 PM	ANM0124	MANUAL

- Select the endpoint and click 'Accept'

The 'Accept Confirmation' dialog will be displayed.

Accept Confirmation

Are you sure you want to accept selected computer(s)?
This action cannot be undone!

Computer Name	Alias Name	Extra ID
DESKTOP-TTPO9PR	<input type="text"/>	<input type="text" value="letters or nu"/>

- **Alias Name** (Optional) - Specify an alternative name for the endpoint so you can easily track it in the console.
- **Extra ID** (Optional) - The 'Extra ID' is an identification tag assigned to the endpoint. This tag is added to the X-token of the HTTP header in the HTTP requests generated by secure URL applications from the endpoint. The console uses the extra ID and the machine ID to authenticate the endpoint during initial registration and subsequent connection requests. Extra IDs should be specified as a combination of letters and numbers in the text box.
- Click 'Yes' (if Auto-accept is enabled for the organization, click on the blank fields under Alias and Extra ID columns in the 'Computers' screen and provide the alias and extra ID details).

The endpoint will be shown as connected and managed in the 'Computers' screen.

The CSB agent communicates its status to the management console in 1 min intervals. The status will change to managed after the next round of communication.

The endpoint will be automatically placed in the 'Default' group. To move it to a different group, first select the endpoint then click the 'Move to Group' button. See '[Assigning Endpoint to Groups](#)' and '[Managing Endpoint Groups](#)' if you need more help with groups.

Step 8 – View Reports

The 'Reports' section provides administrators the details of threats detected and the activity on the endpoints:

- Threat Report – It provides the details of threats detected such as malware, fake certificate, remote attempt and more.
- Activity Report – It provides the details secure apps activity that the user has done on the endpoints such as when the application started, switching in and out of CSB desktop and more

Refer to the section '**Reports**' for more details.

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](https://www.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