COMODO
Creating Trust Online®

SECURE BOX

Comodo
SecureBox Management Console

Software Version 1.9

Administrator Guide

Guide Version 1.9.021220

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1.Introduction to Comodo SecureBox

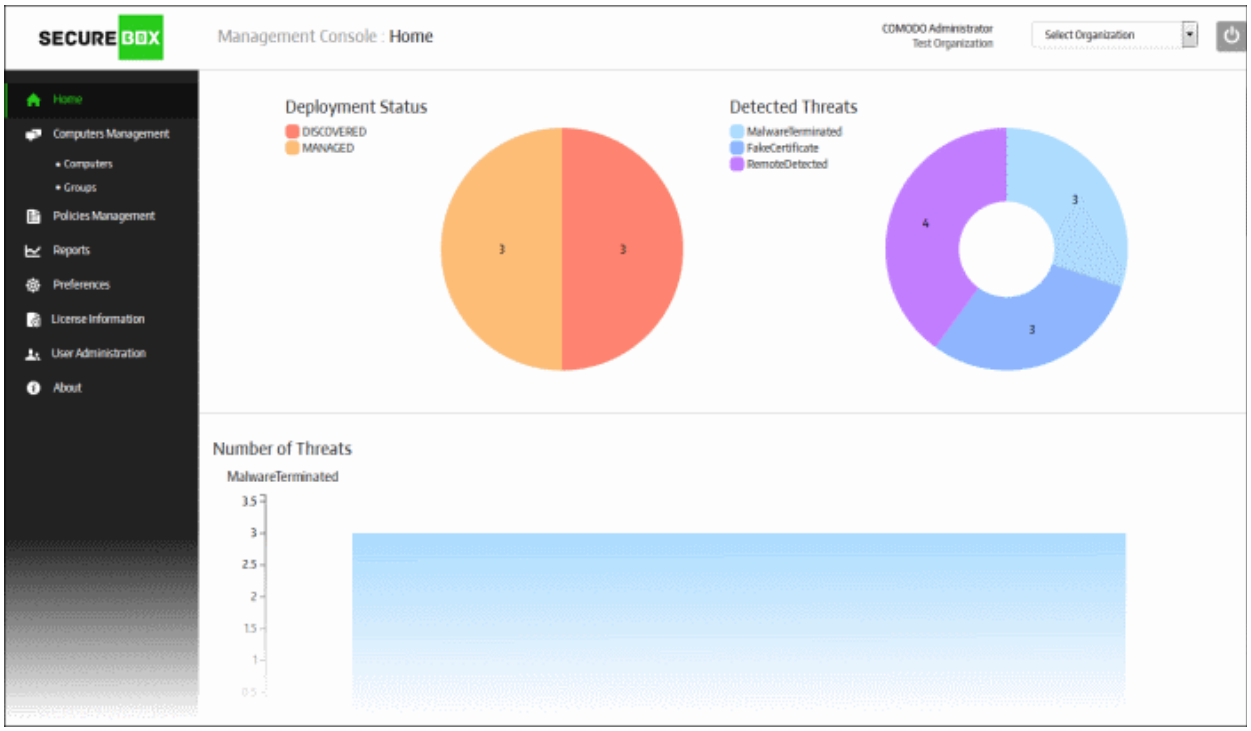
Comodo SecureBox protects applications by isolating them inside a heavily-protected, fully functioning container within an endpoint operating system. Unlike a traditional sandbox which is used to house potentially hostile files, SecureBox protects the application itself and treats all outside processes as hostile. By isolating critical applications from other running processes, Comodo SecureBox prevents data exfiltration, remote takeover, key-logging, SSL sniffing, memory scraping and zero-day malware.

The Management Console allows administrators to control and monitor large-scale deployments of SecureBox on enterprise networks. It features a highly informative graphical dashboard, a detailed reporting sub-system, instant threat and activity notifications and the ability to define granular security policies for different endpoint groups. Security policies are constructed by adding one or more of the following types of secure app:

- 'URL Mode' app - Opens specified websites inside the secure box environment
- 'App Mode' app - Opens specified applications inside the secure box environment
- 'Folder Mode' app - Opens specified folders and files inside the secure box environment

The console is available in both SaaS and on-premises deployment models while endpoints can easily be imported via active directory or work-group.

SecureBox will allow you to create a threat-resistant tunnel to specific websites or portals, protect client applications from outside interference during run-time and to shield entire data repositories from attack.



Features

- Capable of securing applications in URL, application and folder modes
- Root certificate checking
- Website certificate checking
- Protects against the following:
  - SSL connections sniffing
  - DLL injection
  - Keyboard sniffing

- Copy/paste operation
- Access by other processes
- Virus damage
- Remote control
- Unauthorized data access (data isolation)
- Unauthorized application running (application filtering)
- Unauthorized URL access (URL filtering)

Guide Structure

This guide is intended to take you through the configuration and use of Comodo Secure Box and is broken down into the following main sections.

1.1. Initial Setup

The Secure Box Central Management Console is available in two formats - it can be installed on a customer's premises or offered as Software as a Service (SaaS).

Premise Installation

Host System Requirement

- CPU Intel i5 and higher
- RAM 8 Gb and more
- Up to 100 Gb of free disk space
- OS Ubuntu 14.04 x64 installed
- Internet access
- Linux user "securebox" is created and has sudo permissions

The Secure Box management console will be expertly set up by Comodo engineers at your premises. If required, Comodo engineers can also host the application on your cloud servers. After the installation is complete you can login to the console using the URL configured during installation. Please note that customers opting for on-premise installation/hosting on their own servers will have the ability to manage multiple organizations. Comodo will also configure a super administrator for your account. For more details, contact us at **secureboxsupport@comodo.com**

Software as a Service

The Secure Box management console will be hosted on Comodo cloud servers. After you have finalized your order, Comodo will provide you with the URL to access your account. Customers that opt for Comodo's SaaS should contact Comodo to add new organizations. For more details, contact us at **secureboxsupport@comodo.com**

Next, **login** to the console using the URL provided by Comodo.

Endpoint's Supported Operated Systems

- Windows XP
- Windows 7 - 32bit and 64 bit
- Windows 8 - 32bit and 64 bit
- Windows 8.1 - 32bit and 64 bit
- Windows 10 - 32 bit and 64 bit

1.2. Quick Start

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.

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 in 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 - click on any link to go straight to that section as per your current requirements.

- **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.**

- 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:

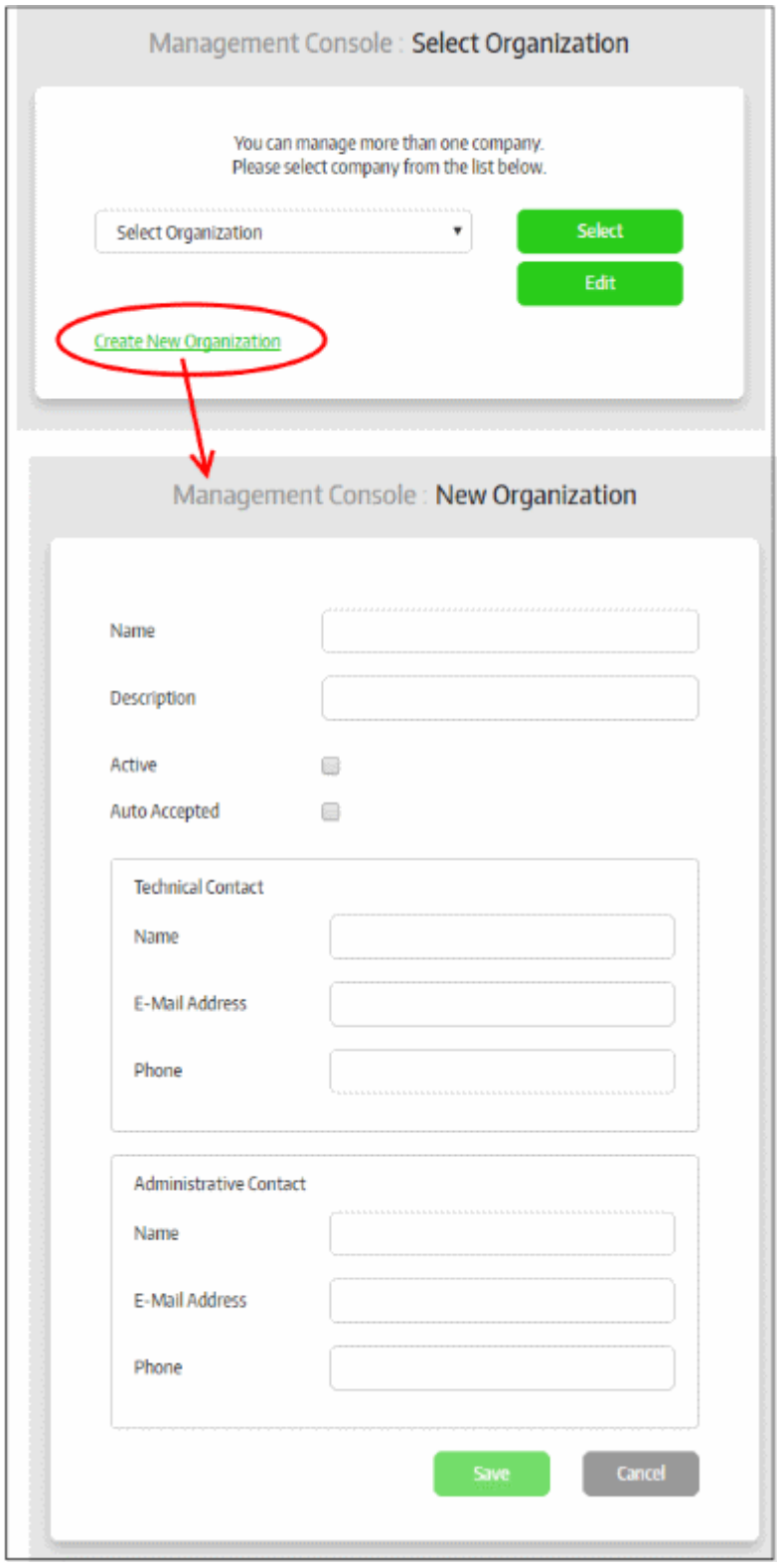
- **On-Premises version** - Administrators can manage multiple organizations and create new organizations. Move onto **Step 2** to add organizations
- **SaaS version** - The home screen of the management console will be displayed after logging in. Move onto **Step 3** to add licenses.

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



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

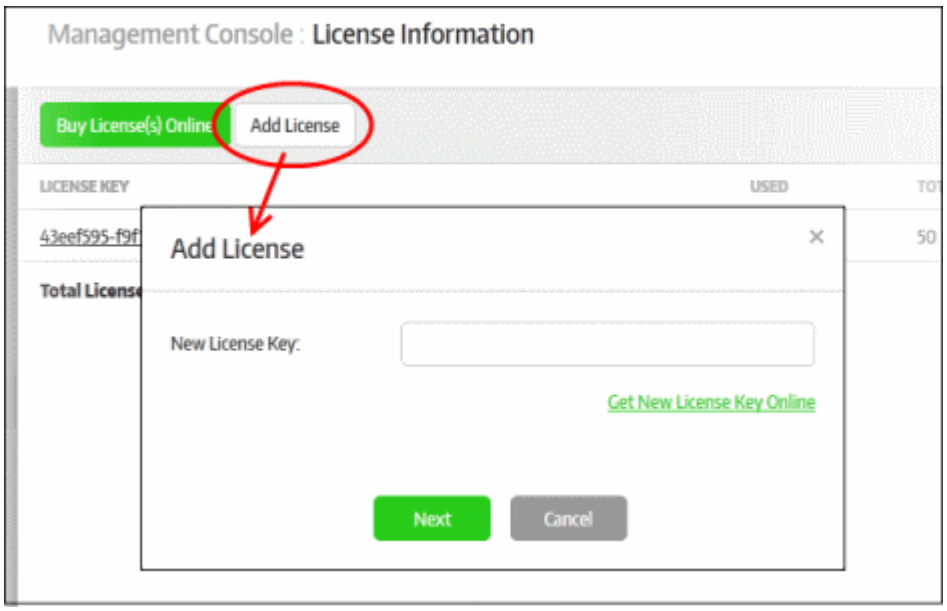
The new organization will be created and an account activation email will be sent to the administrative contact.

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

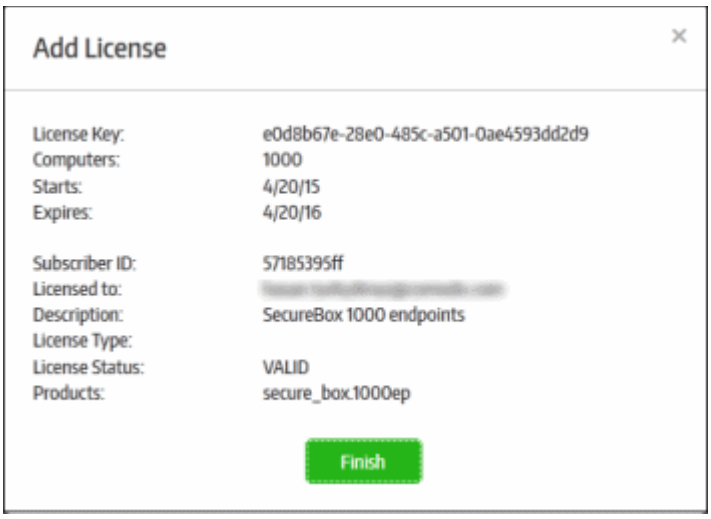
- To add a license for an organization, log into the management console and click 'License Information' then 'Add License':



The 'Add License' dialog will be displayed:

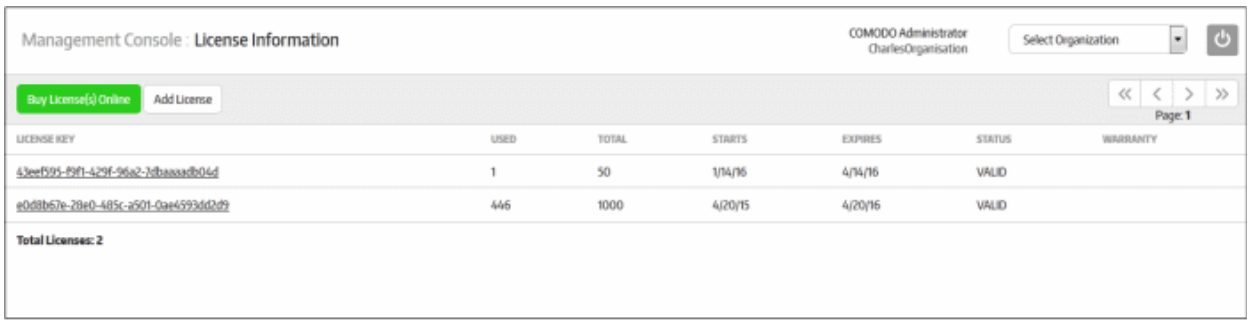
- Enter the license key that you received in the registration email then click the 'Next' button.

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:



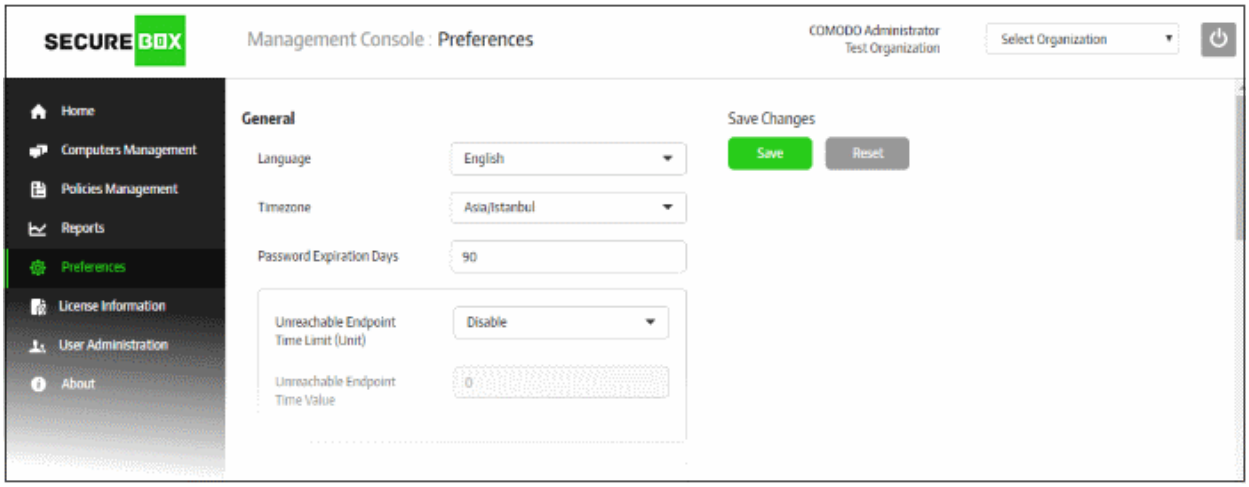
Note - you can add multiple licenses if you want to enroll more endpoints than allowed under the current subscription. You can also use a single license for multiple organizations/departments as long as the total number of endpoints is within the licensed limit. To get more licenses, simply repeat the 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 determines the behavior of the management console. You can also configure global settings that will be applied to the enrolled endpoints.

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

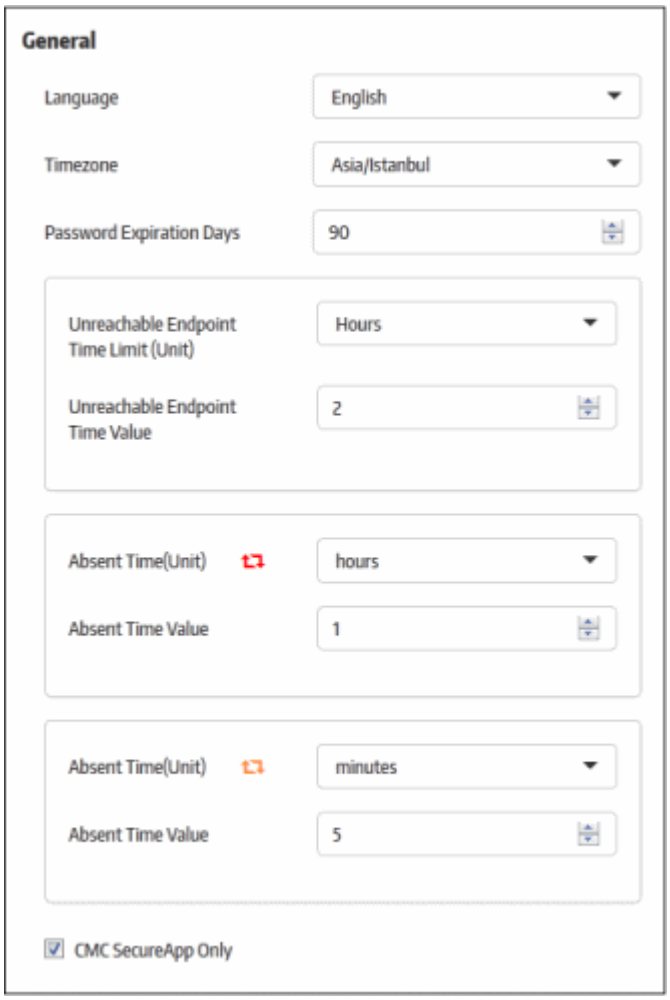


Click the following links for more details on each setting:

- **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.



- **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

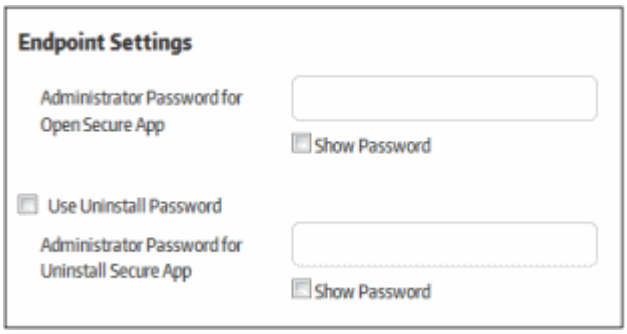
yellow icon is shown. Icons appear next to 'Connection' in the '**Computers**' screen.

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.



- 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.

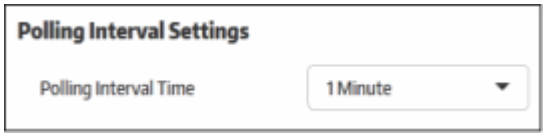
Report Settings

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

- Remove Reports Older Than - The threat and activity reports for the account will be removed from the server as per the period set here. Select the period from the drop-down after which the reports will be removed.

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

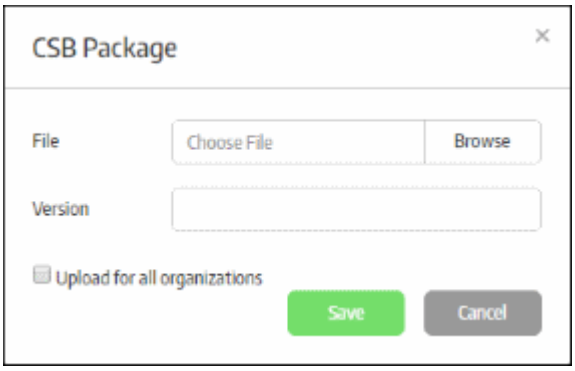
Allows you to configure global settings for external services such as log server, time server and Secure Box installer upgrade server.

- 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.

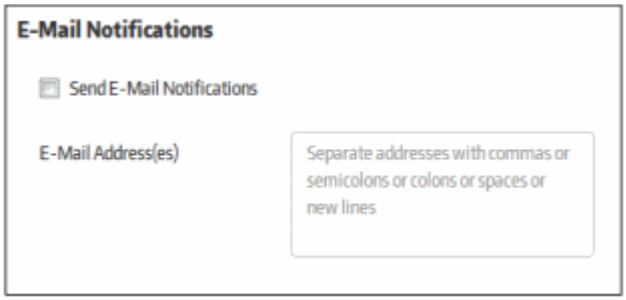
- To upload the latest CSB installer package, click 'Manual Upload of SecureBox Package'



- 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

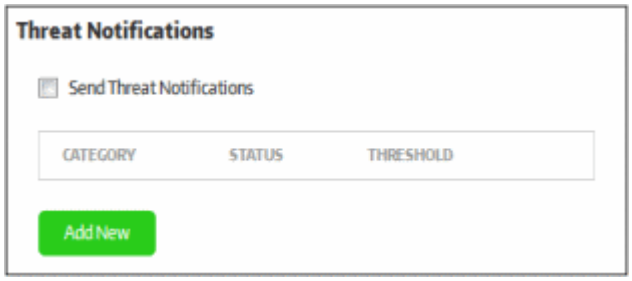
Allows you to configure email settings for threat notifications, endpoint activities and licenses.



- 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.

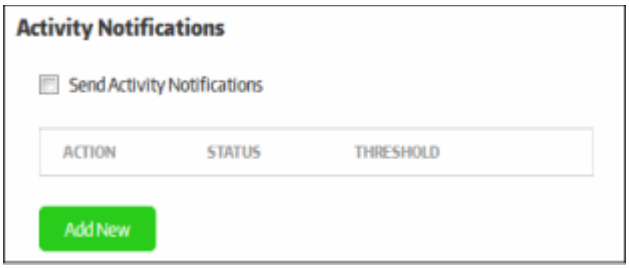


- Send Threat Notifications - If enabled, threat notifications will be sent to the recipients listed in the 'Email Notifications' area.
- To configure a new threat notification, click the 'Add New' button.

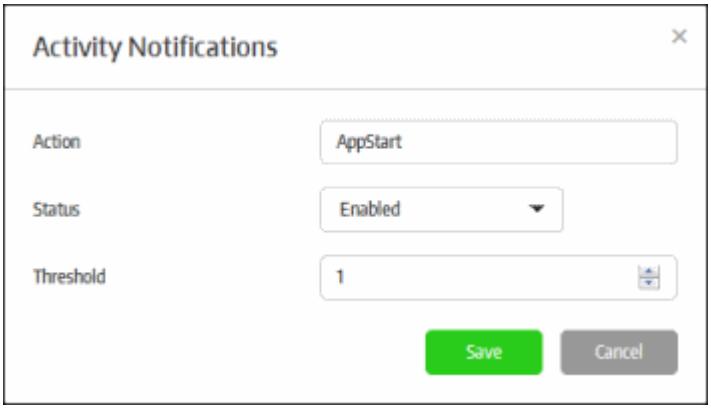
  - Category - The type of threat that you want to receive notifications about. Refer to the section '**Threats Report**' for more details on threat categories.
  - Status - Select whether you want to enable or the disable notifications for this category.
  - Threshold - The number of threats detected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



- 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.

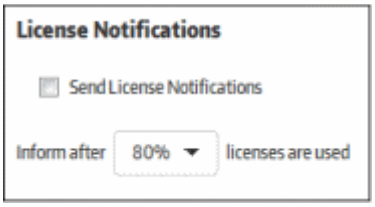


  - Action - The type of activity that you want to receive notifications about. Refer to the section '**Activity Report**' for more details on action categories.
  - Status - Select whether you want to enable or disable notifications for this type of activity.
  - Threshold - The number of activities detected 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.



- 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.

- 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

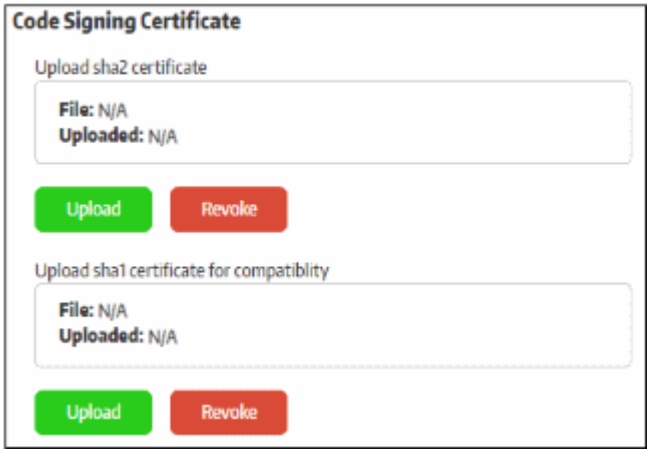
- Discovery From - Specify where you will import endpoints from. The options available are 'Active Directory'

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.

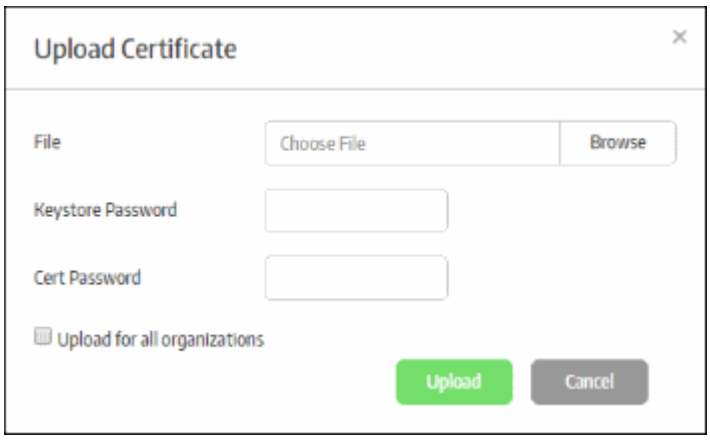
Code Signing Certificate

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.



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

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

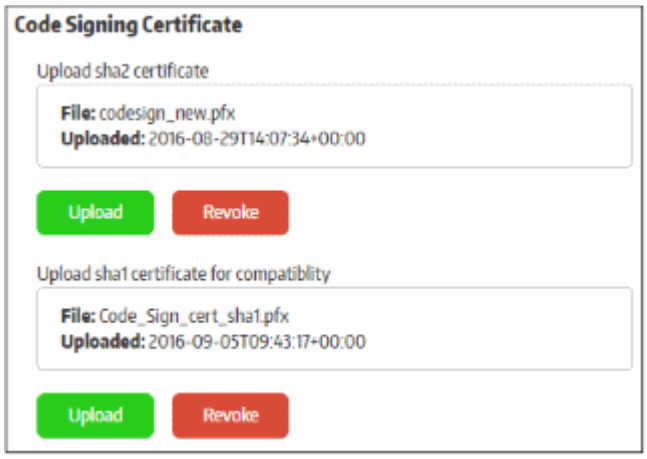


- Click 'Browse', navigate to the location where the certificate is stored and click 'Open'
- Enter the 'Keystore' and 'Cert' passwords in the respective fields. Normally, the same password can be

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.

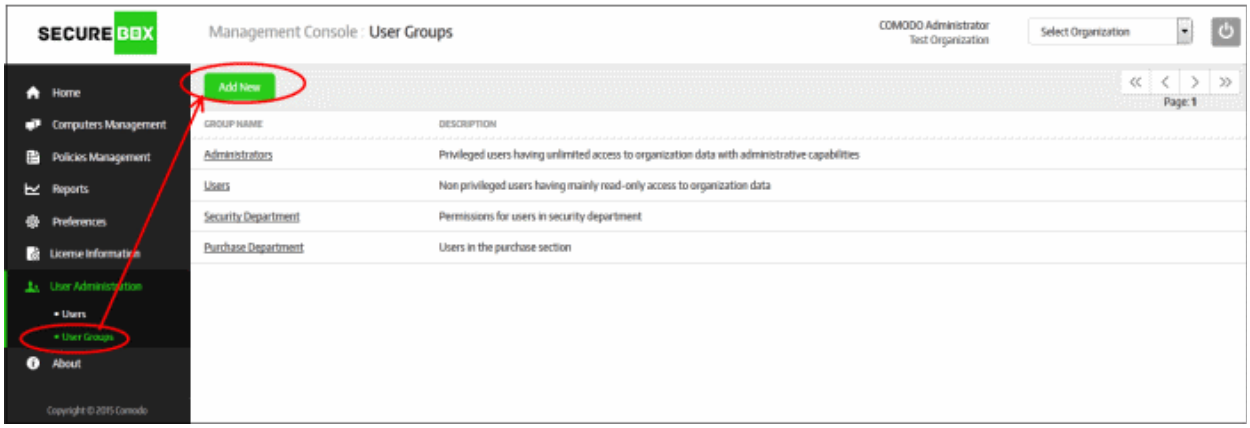


- To revoke the existing code signing certificate, click the 'Revoke' button. You will need to upload a new, valid code signing certificate in order to sign your applications.
- Click the 'Save' button to apply your changes.

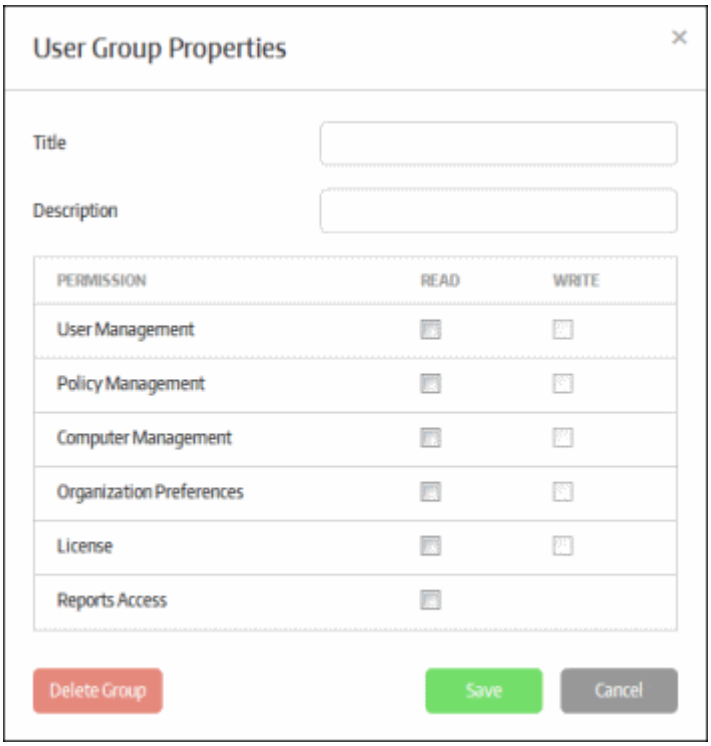
Step 5 - Add User-Groups and Users

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



- 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:

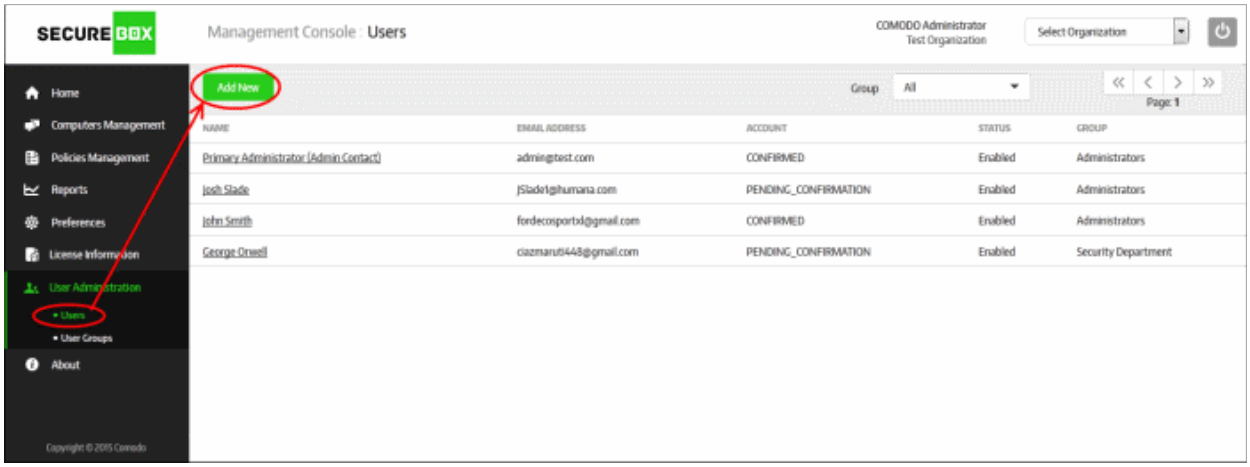
User Group Privileges	
Form Element	**Description**
User Management	Allows group members to add and configure users and user groups. Refer to the section '**Users and User Groups**' for more details.
Policy Management	Allows group members to create and edit CSB policies. Refer to the section '**Policies**' 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	View the threats detected by Secure Box and report of activities on the endpoints related to secure box. Refer to the section '**Reports**' for more details.

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

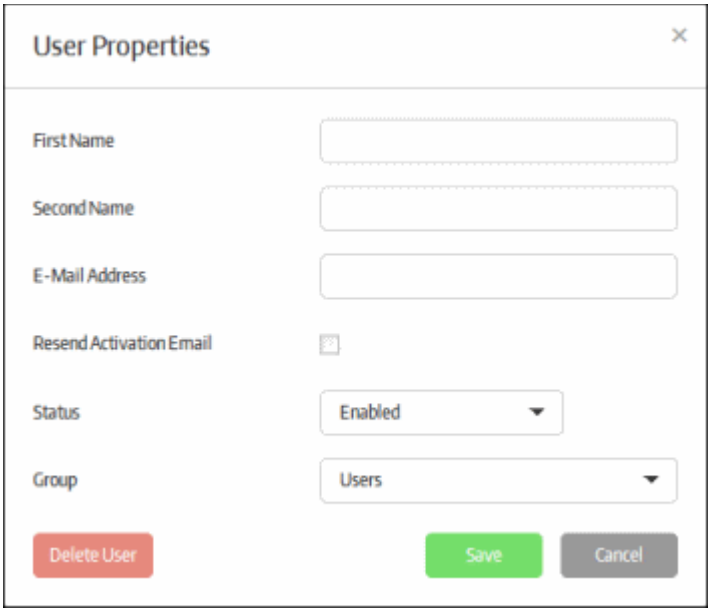
Once saved, the new user group will be available for selection when adding/editing users. Users assigned to the group will be able to manage the organization according to group privileges.

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.

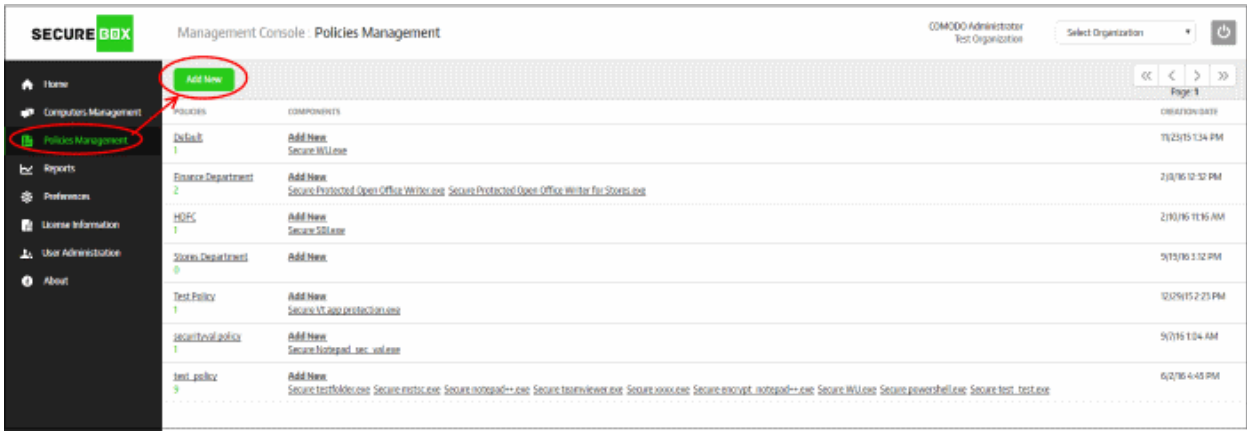
An email will be sent to the user which contains an activation link and a temporary password. The user's account will be activated on clicking the activation link in the mail and the user can access the management console using the temporary password. It is advisable the user changes the password immediately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

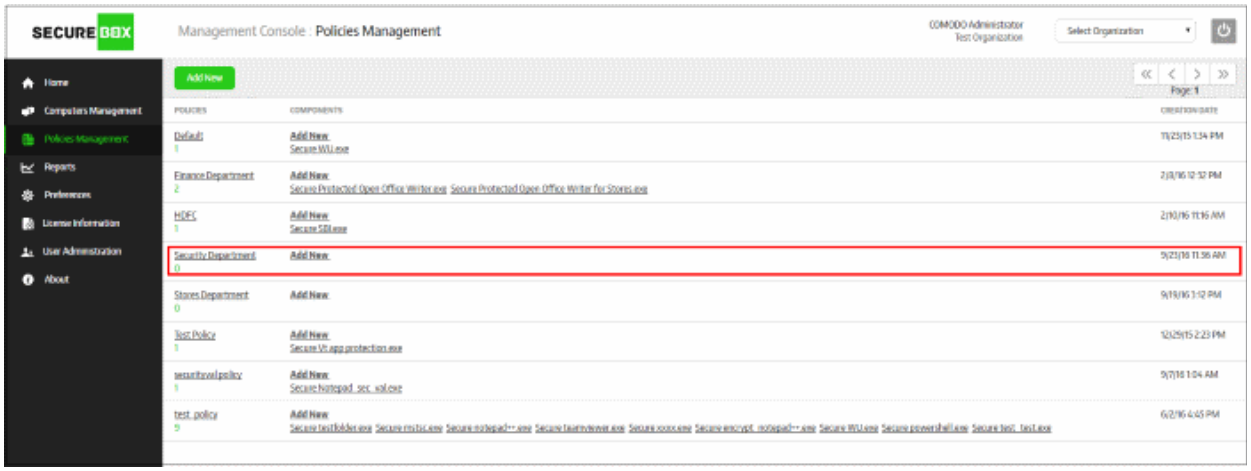
To add polices, click 'Polices Management' on the left:



- Click the 'Add New' button

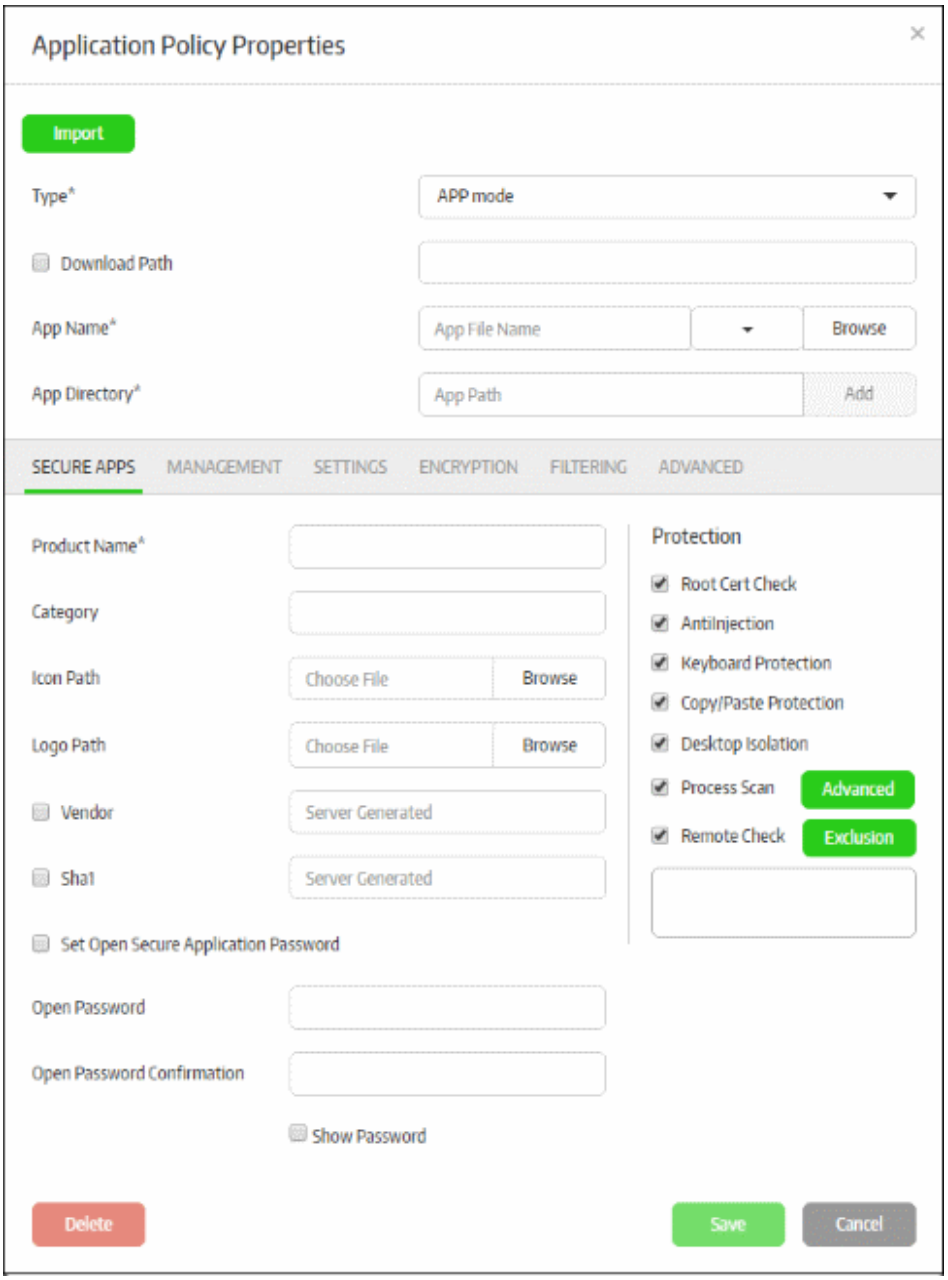
- Policy Name - Create a name for the policy
- Description - Add an appropriate description for the policy
- Click the 'Save' button

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 applications:

- **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:

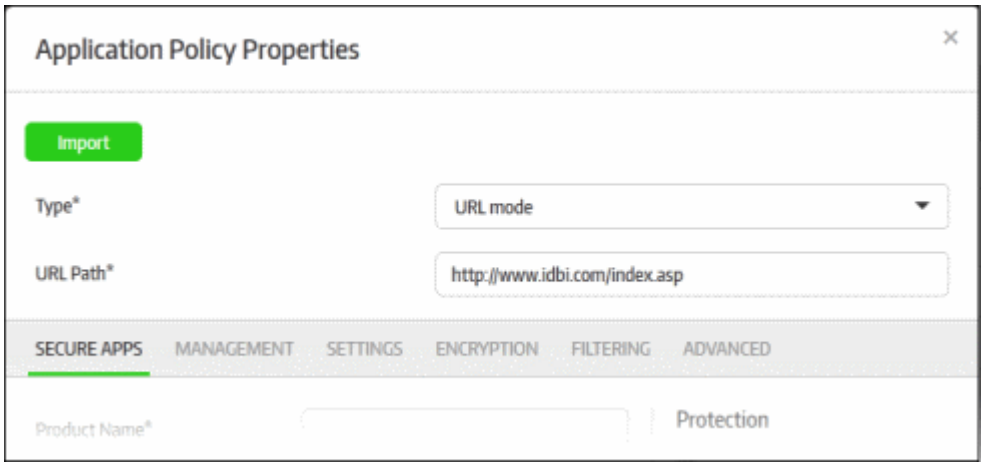
- **Secure Apps** tab - Configure basic information and protection settings for the secure application

- **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.

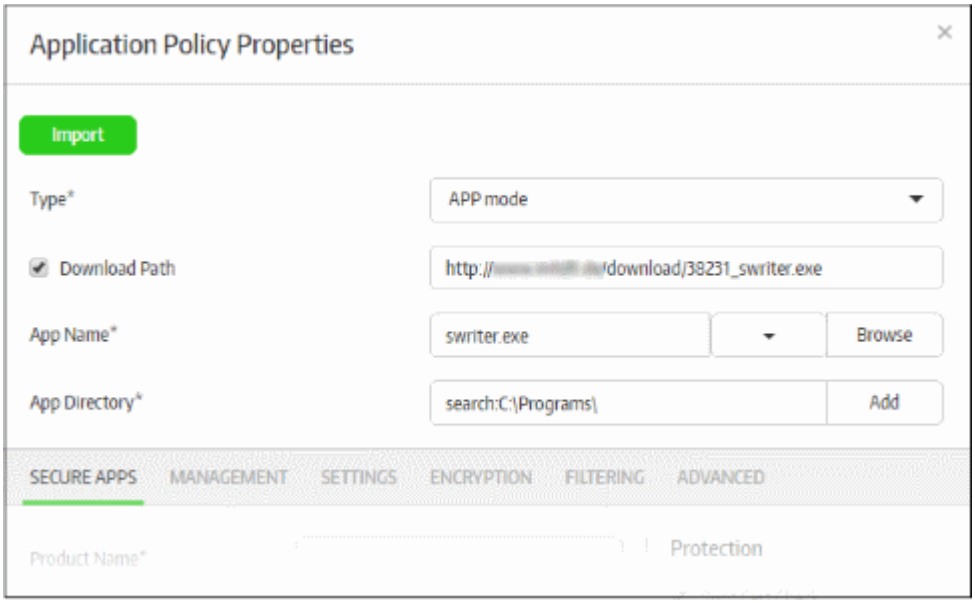
Configuring a Secure URL

- 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.



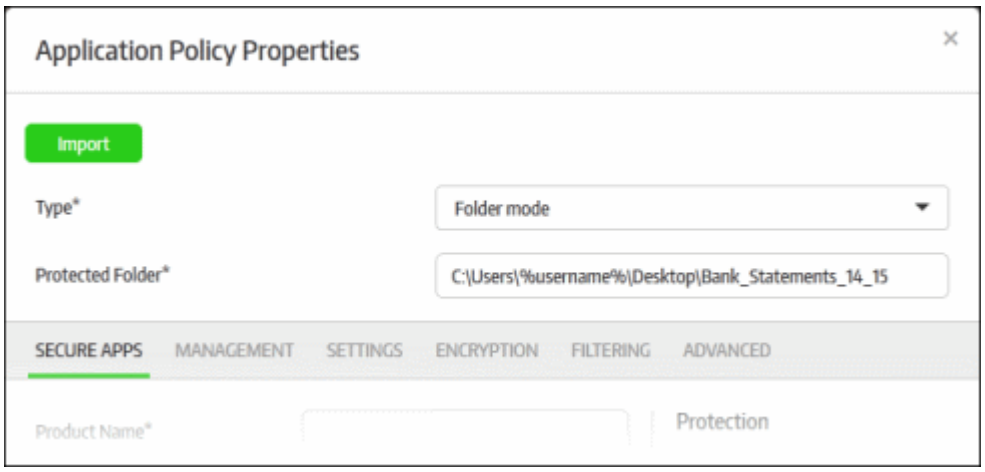
- Click the 'Add' button

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

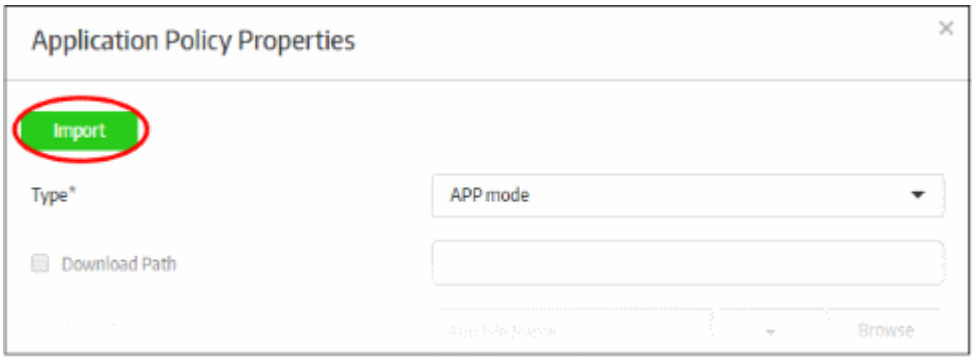
The path of folders support system variables. For example, C:\Users\%username%\Desktop\folder_name



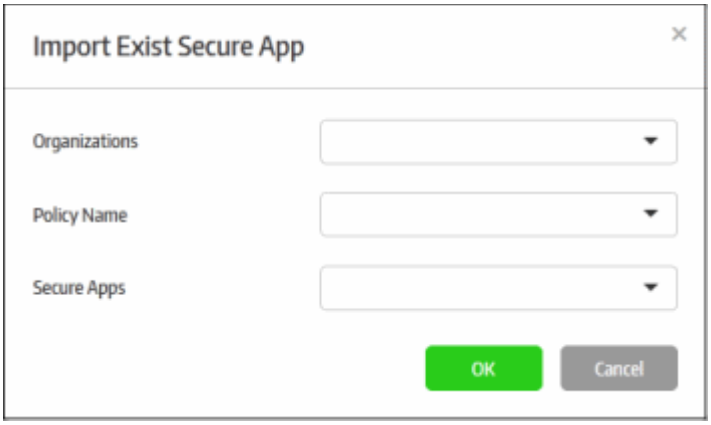
To create a new policy using an existing policy as a base

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.

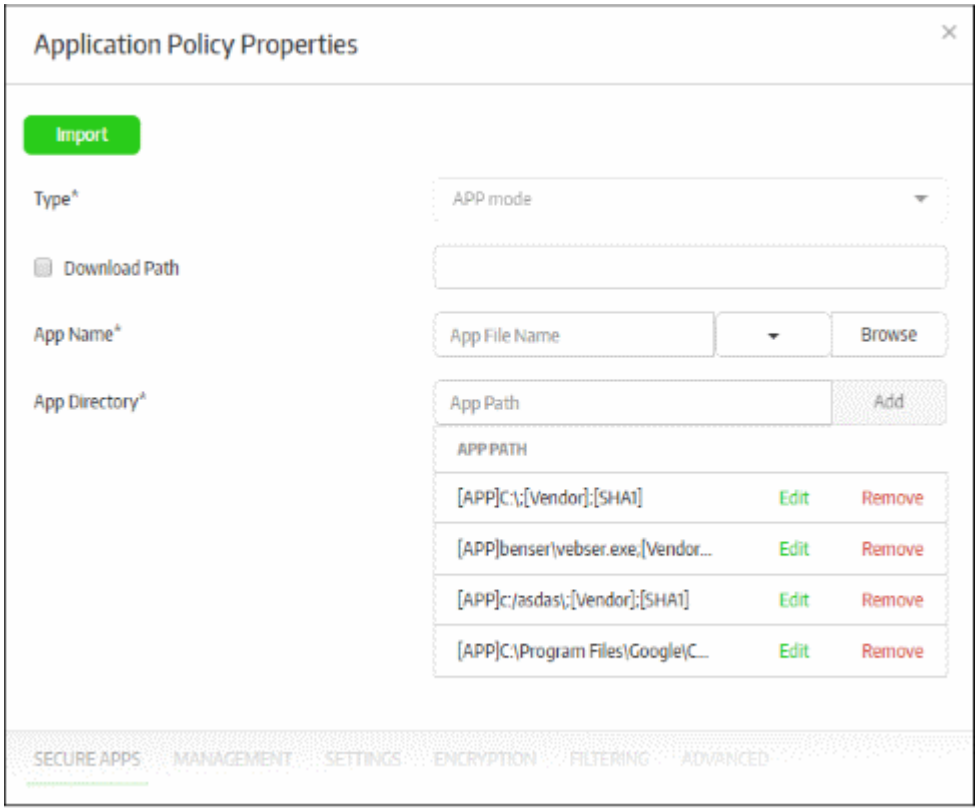
To import the settings of an existing policy, click the 'Add New' link or on the name of a secure app under 'Components' and click the 'Import' button at the top.



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'.

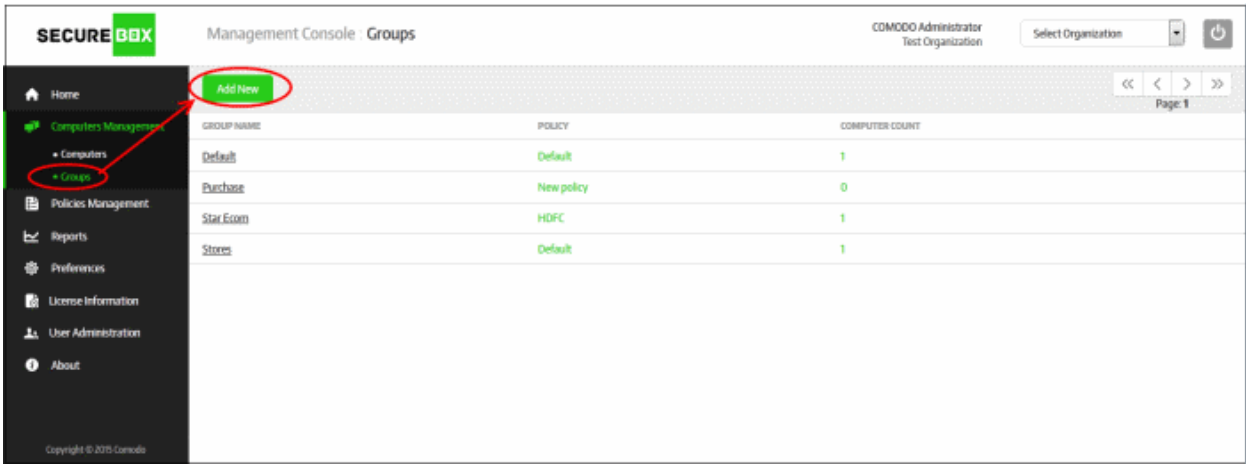


The secured item will be imported with all its settings including the product name. You can save it with the same settings or modify them according to requirements. This is similar to the process explained earlier in step 6 when creating a new policy. **Click here** to find out more about configuring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

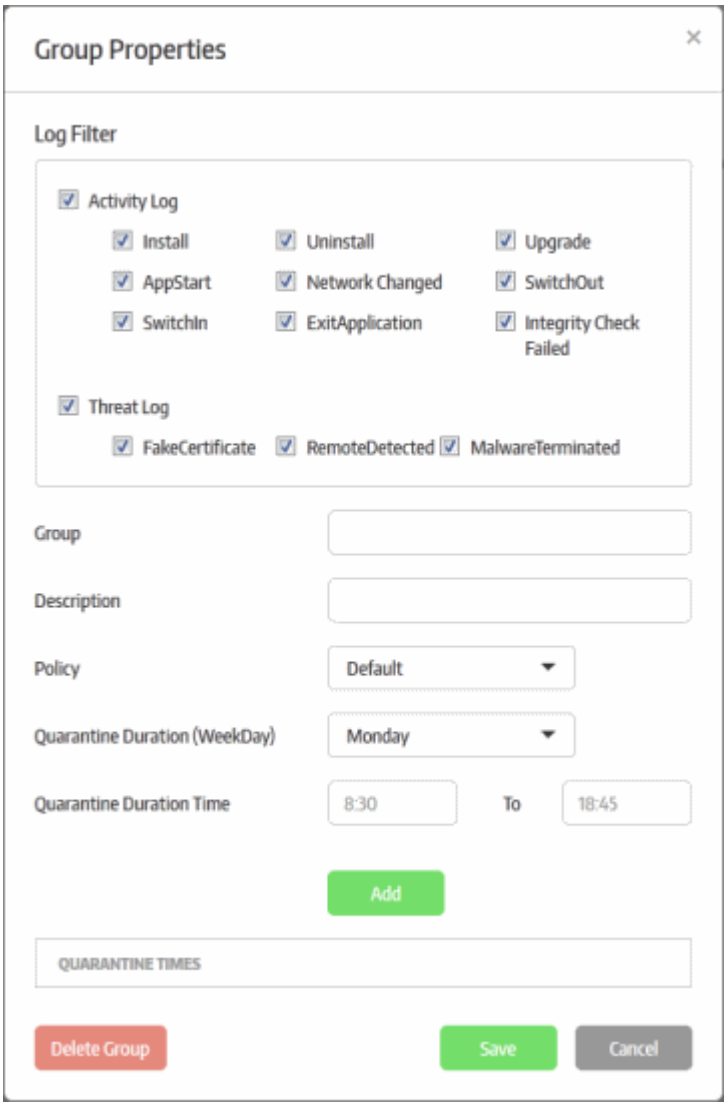
Step 7 - Add Endpoint Groups and Enroll Endpoints

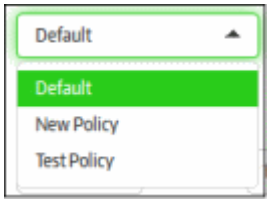
When a policy with secure applications is assigned to an endpoint group, all secure applications in the policy are installed on the endpoints. CMC ships with a default group. Endpoints that are enrolled via the email method are automatically placed in this group.

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



- Click the 'Add New' button



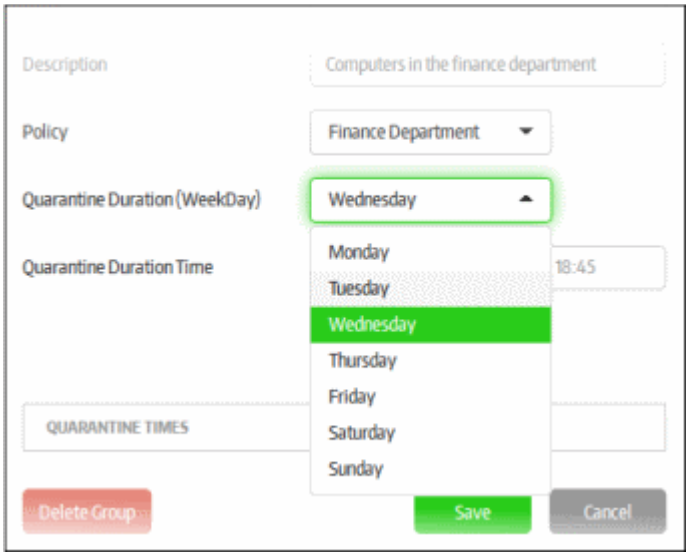
Group Properties - Form Parameters	
Form Element	**Description**
Log Filter	Select which events should be recorded in group logs. Refer to the section '**Reports**' for more details.
Group	Enter the name of the endpoint group
Description	Enter an appropriate description for the group
Policy	Select the policy to be applied to the endpoints from the drop-down.  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 polices.
Quarantine Duration	Select the day of the week on which the quarantine should apply. Refer to '**To**

(Week Day)	**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.

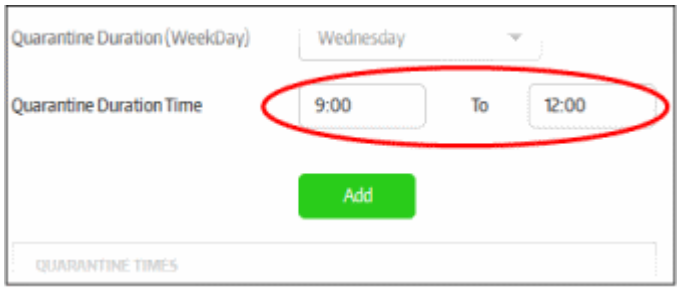
To schedule quarantine period for the endpoint group

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

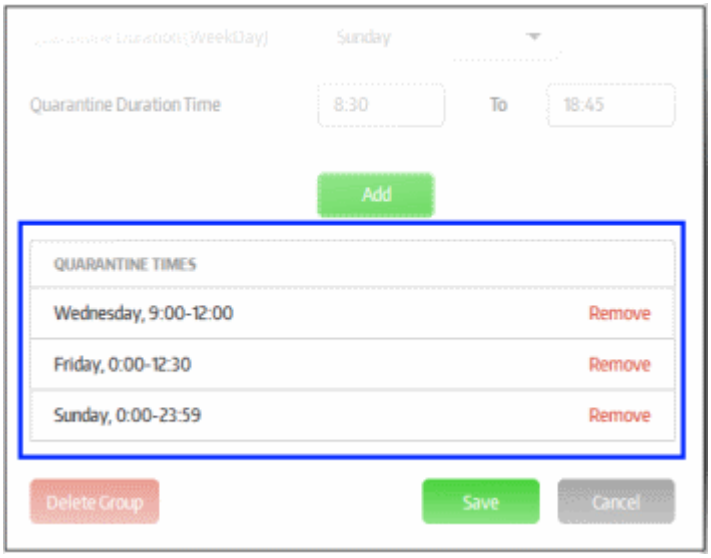


- Enter the quarantine time duration time the selected quarantine day in the 'Quarantine Duration Time' fields



- Click the 'Add' button below

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



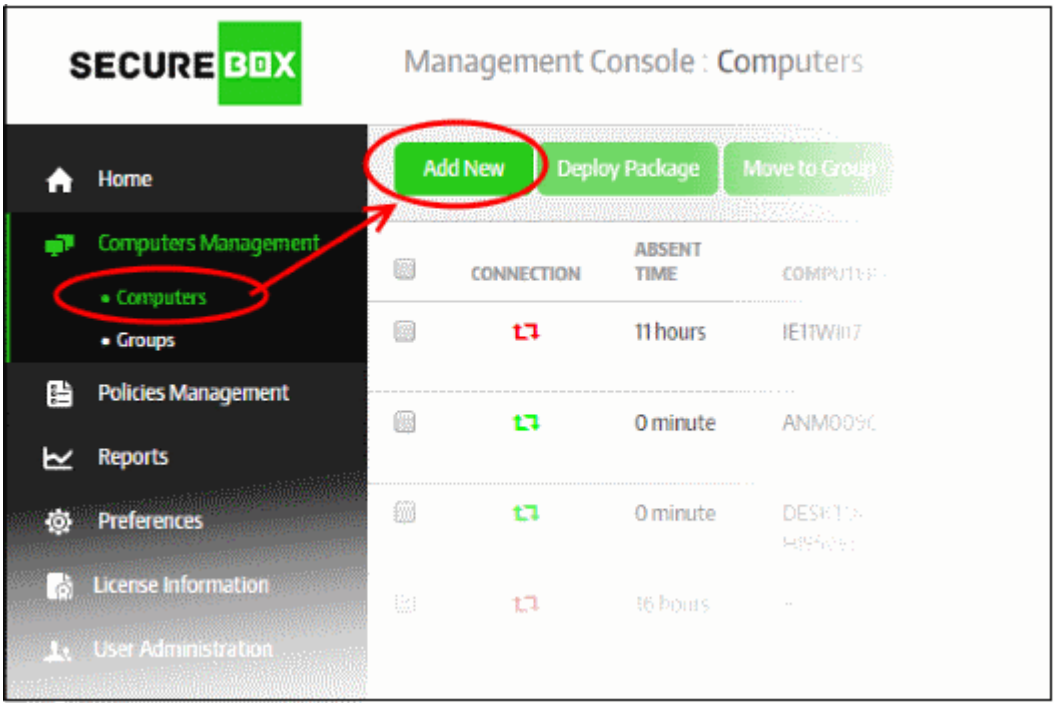
Now, the secured items configured for the selected policy will be automatically blocked from opening on the endpoints in the group.

- 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.

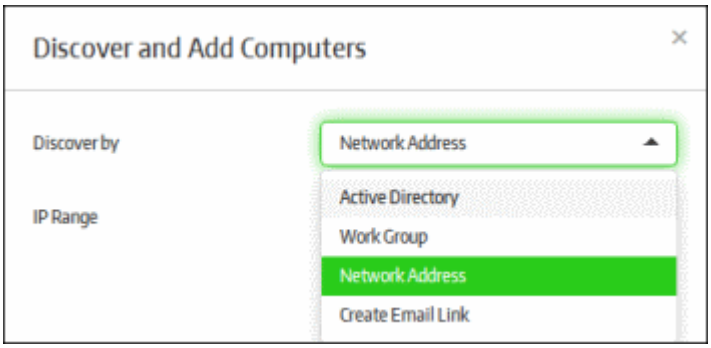
The next step is to enroll endpoints.

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



- 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.

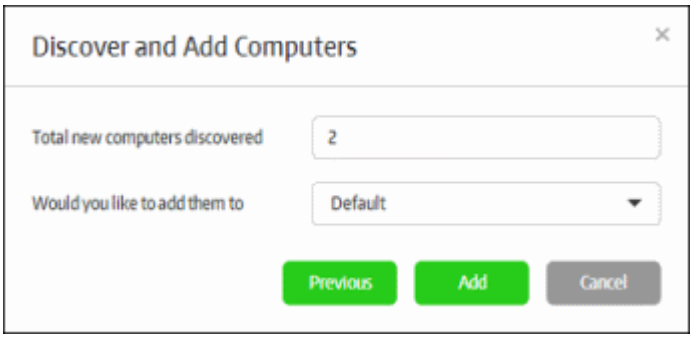
Enrolling using Active Directory, Work Group or Network Address

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:

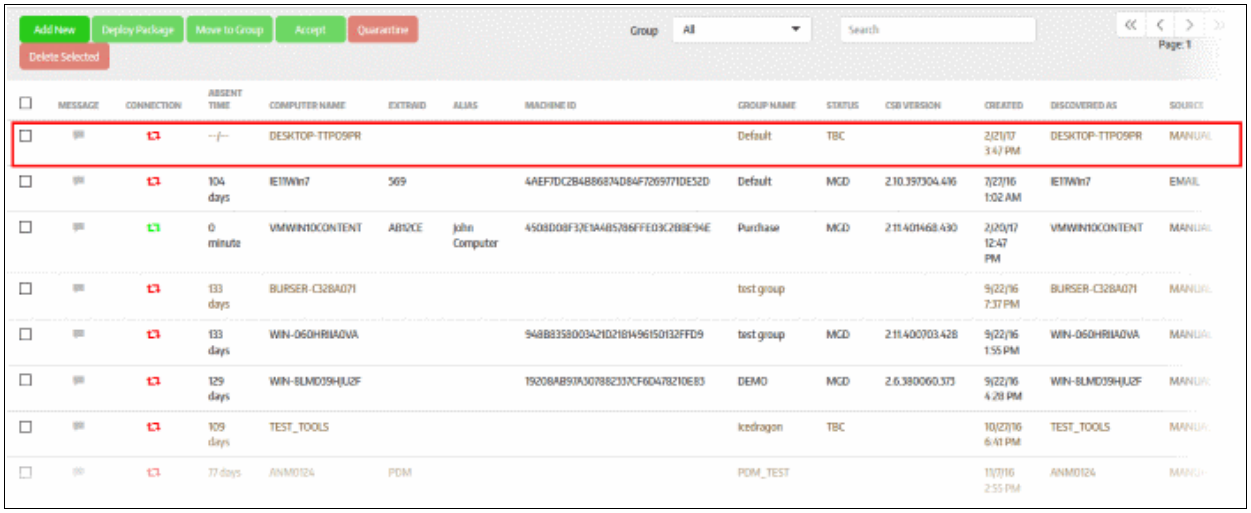
- If you choose 'Active Directory', you next have to enter the IP address of the domain controller, name of the domain and the administrator username and password for that domain.
- If you choose 'Work Group, then you have to enter the name of the work-group.
- If you chose 'Network Addresses', you next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

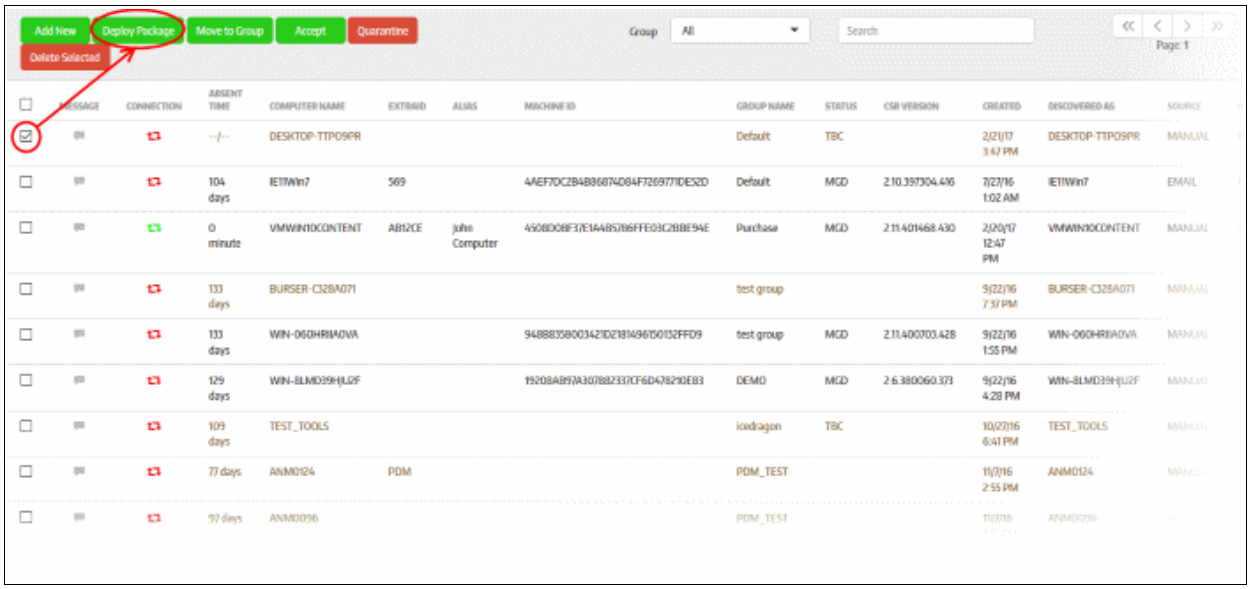


- Select the endpoint group from the 'Would you like to add them to' drop-down and click the 'Add' button.

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

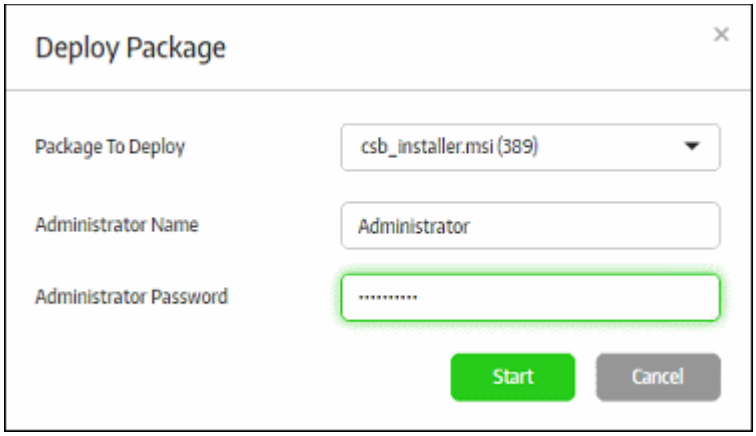


The next step is to deploy the CSB package that should be installed on the endpoints. Installing a package will allow you to assign policies and manage the endpoint.



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

The 'Deploy Package' dialog will be displayed.



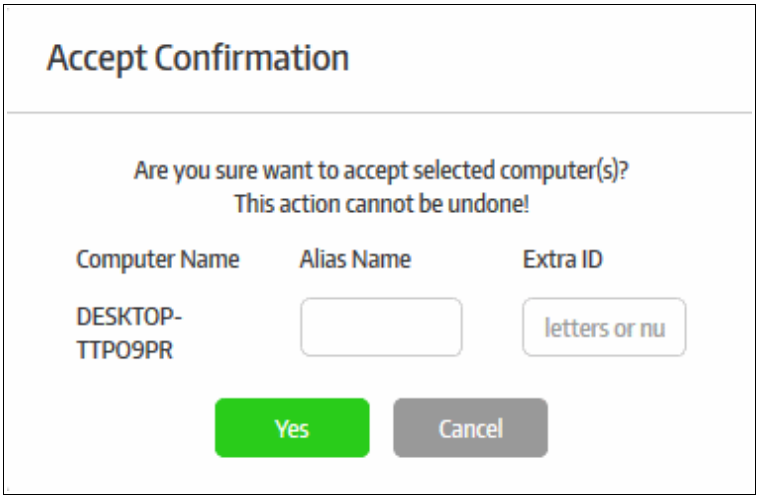
- Select the package to deploy to the selected endpoint from the first field.
- Enter the Active Directory domain credentials and click the 'Start' button

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.

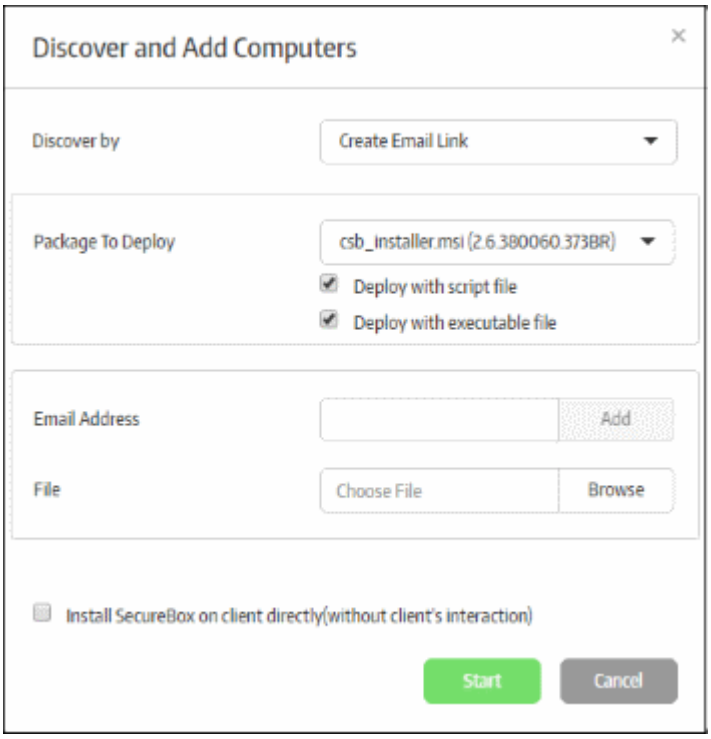


- Click 'Yes' (if Auto-accept is enabled for the organization, click on the blank fields under Alias and Extra ID columns in the 'Computers' screen and provide the alias and extra ID details).

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.

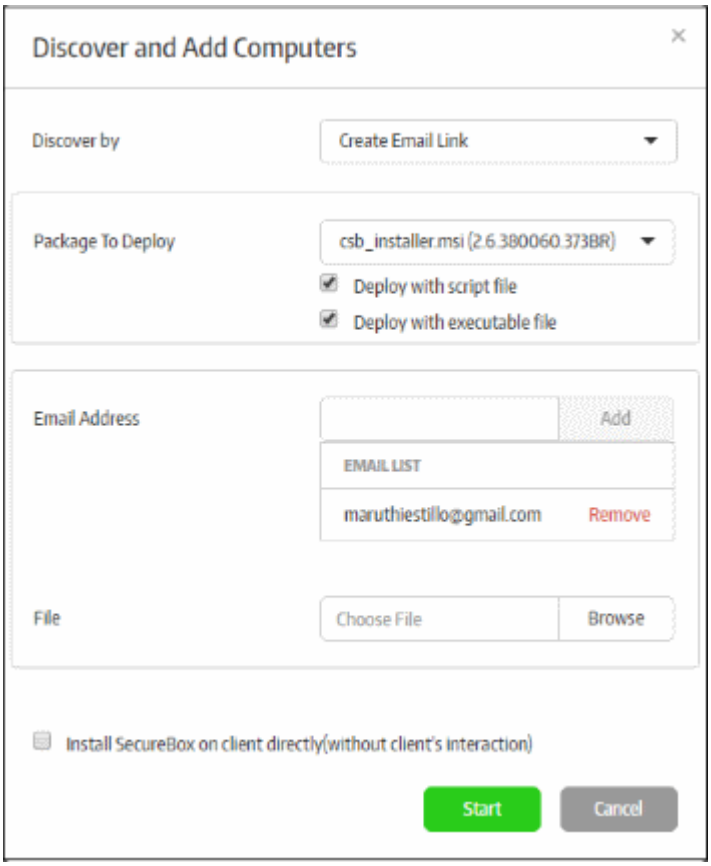
Enrolling using email method

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

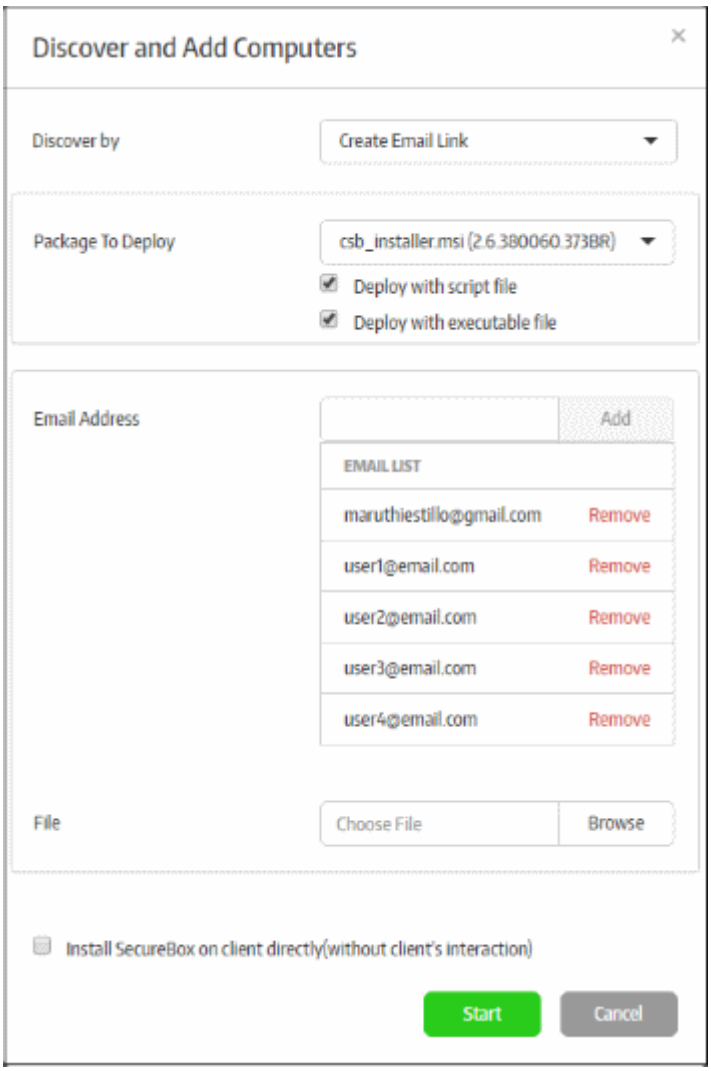


The 'Package to Deploy' drop-down displays all CSB applications uploaded by the administrator.

- 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.

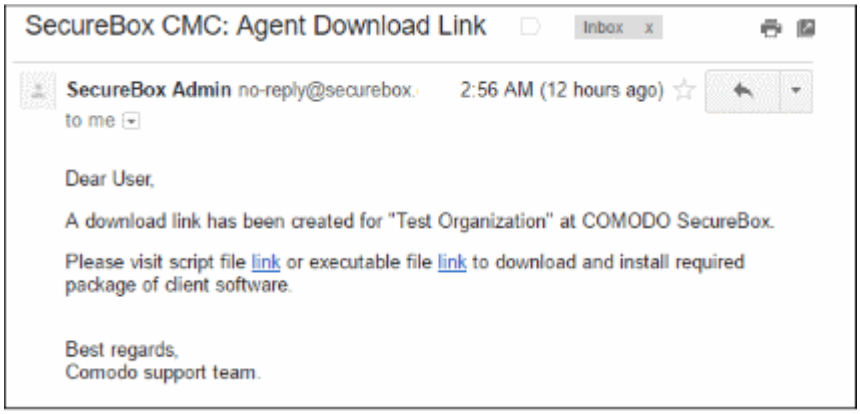


- For bulk enrollment, you can use the 'File' option. Recipient email addresses should be entered on each line of a .txt file. Click 'Browse', navigate to your file and click the 'Open' button. All imported recipients will be listed in the dialog:



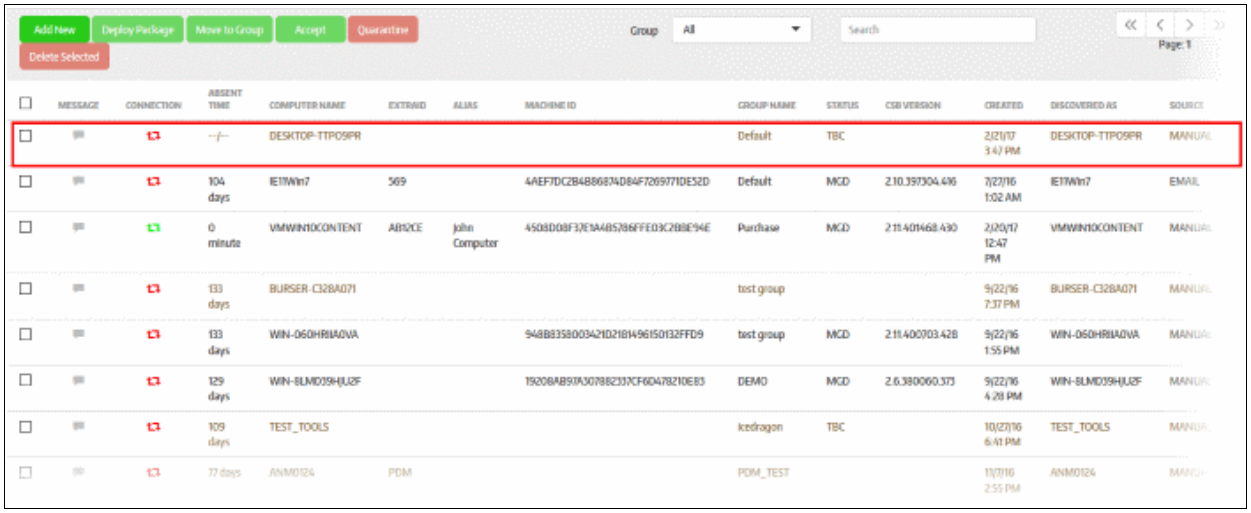
- To remove a recipient, click the 'Remove' link.
- 'Install Secure Box on client directly (without client's interaction)' – If selected, the endpoint user will only see the installation progress bar. They will not be shown the EULA or the configuration page.
- Click the 'Start' button

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



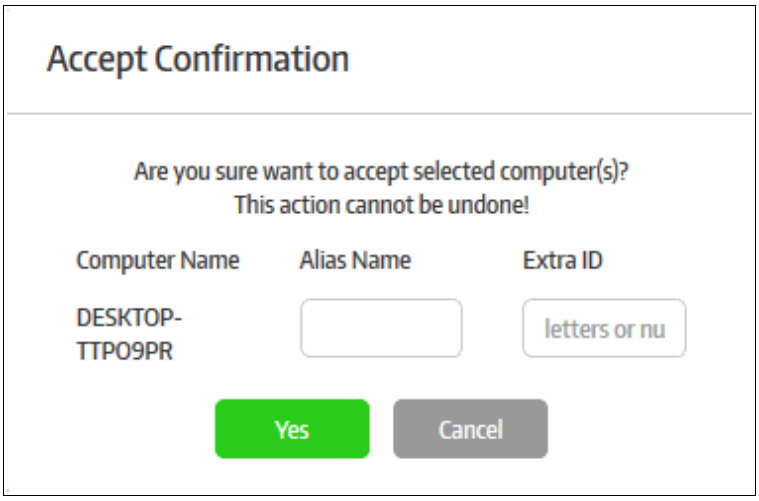
The user should click any of the links to download the CSB installer package and save it on the endpoint. After CSB

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.



- 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 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.

1.3. Logging-in to the Management Console

The Management Console can be accessed using any Internet browser by the entering the URL provided by Comodo in the address bar of the browser.

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

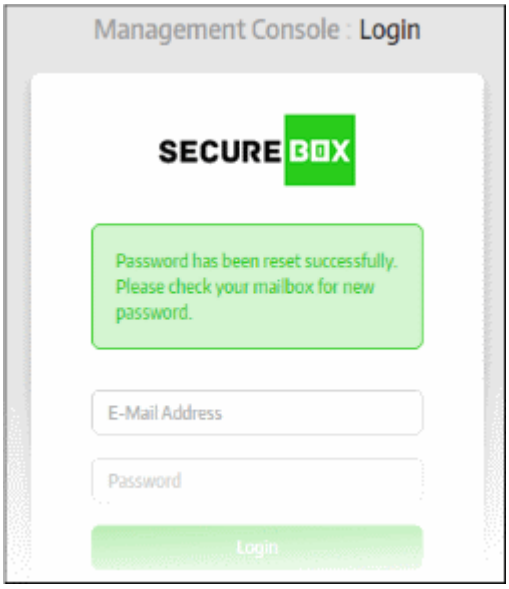
After successful verification, the Comodo SecureBox CMC will be displayed.

To set a new password

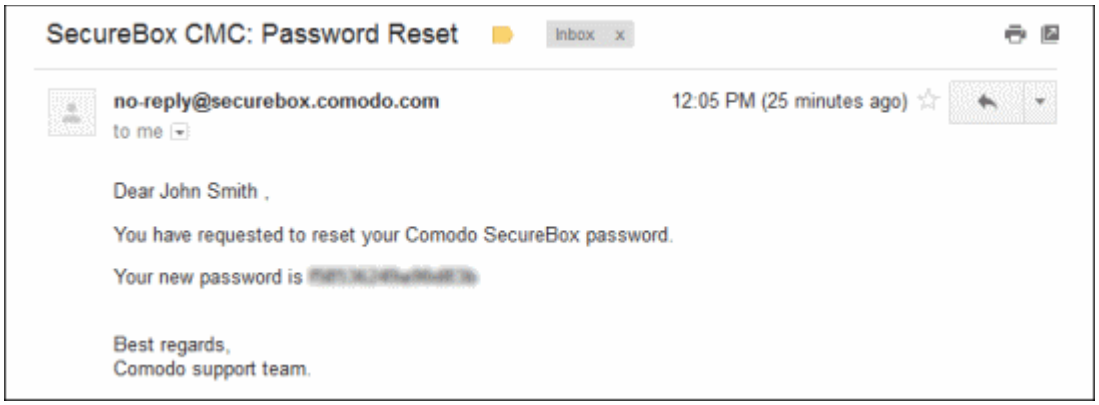
If you have forgotten your current password, you can set a new password by clicking the 'Forgot password' link in the 'Login' interface.

- Enter the email address that you want to receive the password reset instructions in the 'Email Address' field, verify that you are human in the 'Captcha text' field and click the 'Reset' button

A 'Password has been reset successfully' message will be displayed.



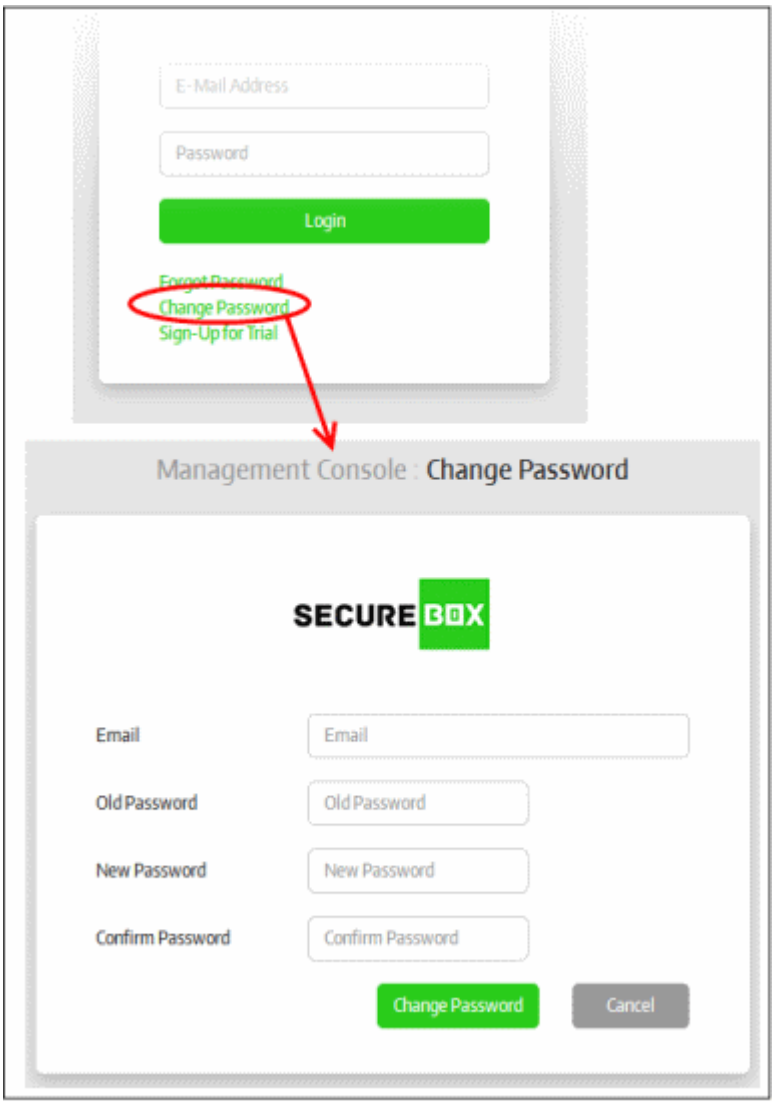
- Check the in-box of the email address that you entered.



Use the new password to access the Secure Box Management Console. It is advisable to change the password after logging-in to the console.

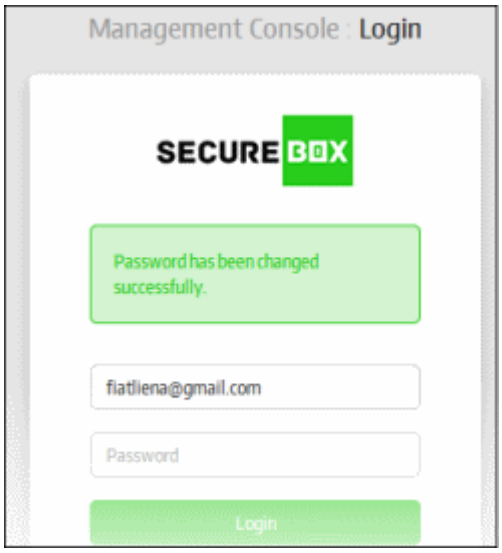
To change the current password

- Click the 'Change Password' link

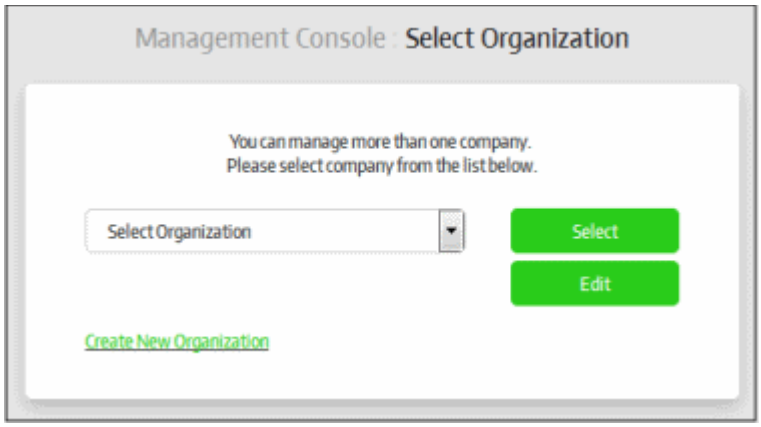


- Enter the registered email address used for logging-in to the console in the first field
- Enter your current password in the 'Old Password' field
- Enter the new password and confirm it in the respective fields. Please make sure to include a number and a special character in the new password.
- Click the 'Change Password' button

A 'Password has been changed successfully' message will be displayed.



Make sure to use the new password to access the console. After successfully logging-in, you have to select the organization that you want to manage.

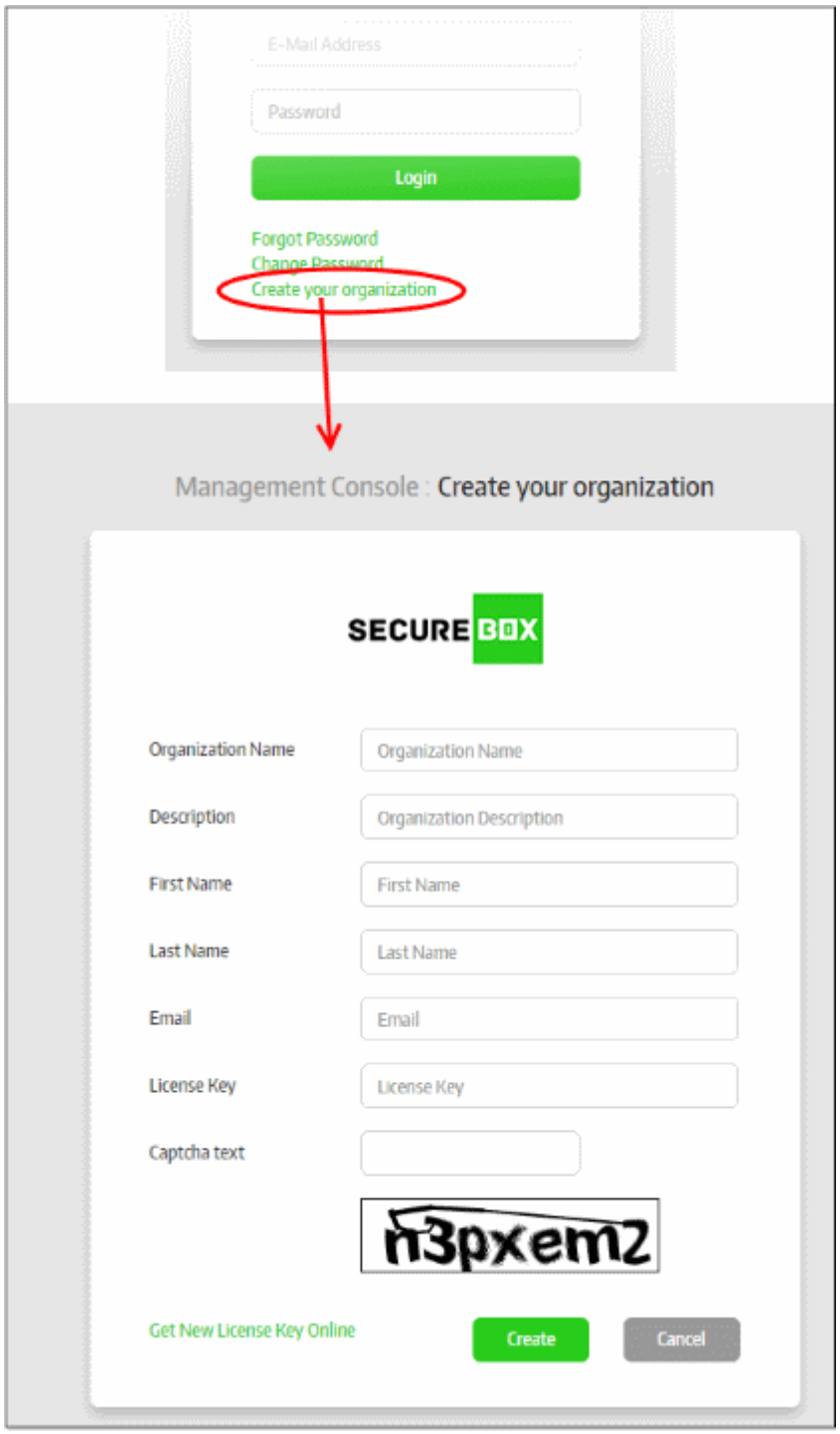


You can add multiple organizations for your account and these will be listed from the 'Select Organization' drop-down. Refer to the section '**Managing Organizations**' for more details about adding organizations to your account. Please note that managing and adding multiple organizations for an account is allowed for Central Management Console that is installed on customer's premises only.

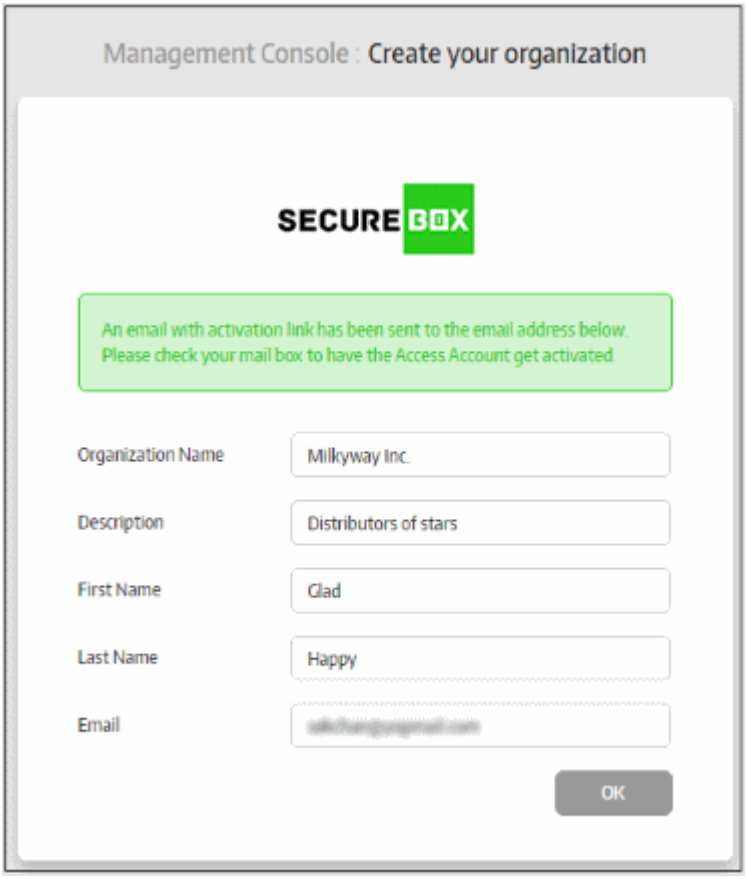
Choose your required organization from the drop-down and click the 'Select' button. The Secure Box Management Console for the selected organization will be displayed. Please note only the administrator with super administrator privileges can manage multiple organizations. Refer to the next section '**The Central Management Console**' for more details.

To use the CMC trail version

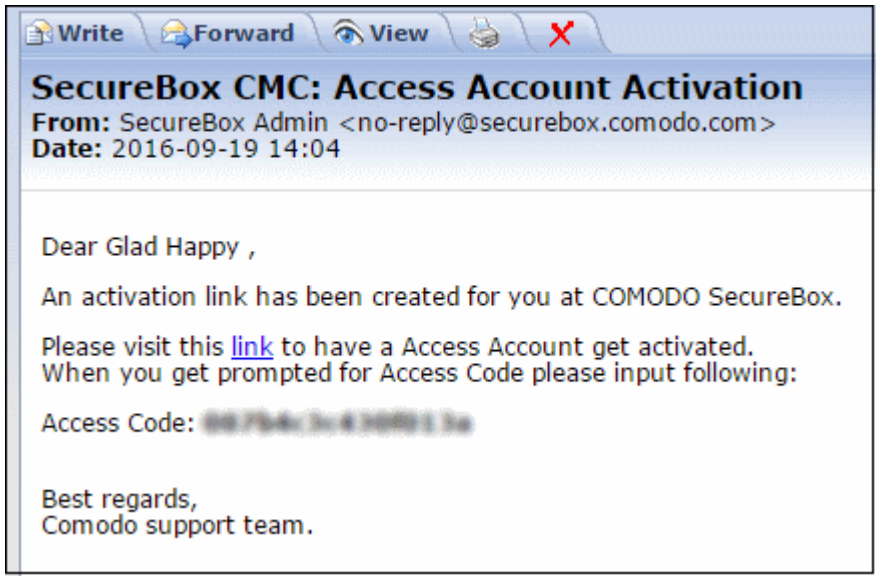
- Click the 'Create your organization' link



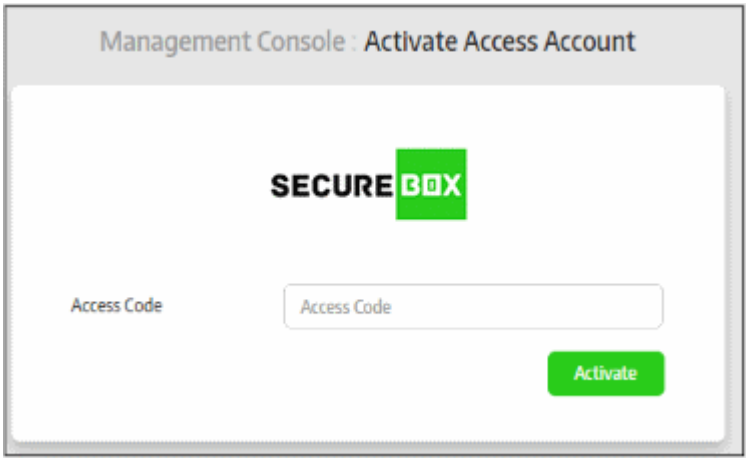
- Enter the details in the form.
- If you do not have a license, click 'Get New License Key Online' link. You will be taken to Comodo Accounts Manager (CAM) page at **https://accounts.comodo.com/** page. Complete the sign up process to get the trial license.
- Click 'Create' after entering all the details.



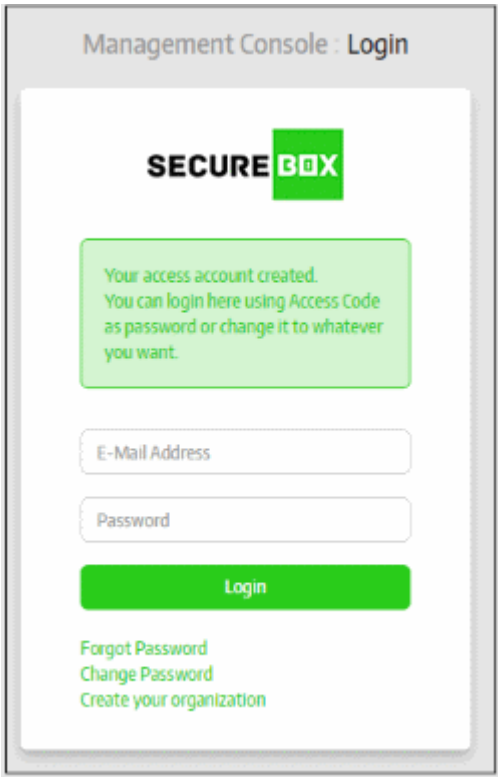
An activation email will be sent. You have to activate your CSB account by clicking the link in the mail.



- In the 'Activate Access Account' dialog, enter the 'Access Code' that was provided in the email.



- Click 'Activate'



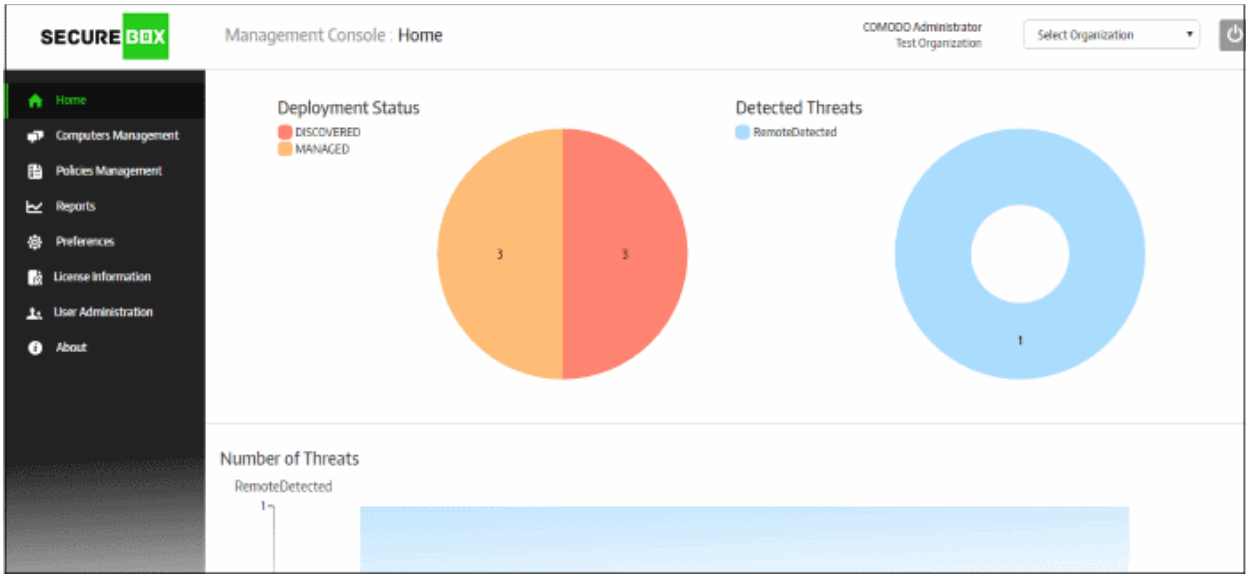
On successful verification, you will be taken to CMC login page.

- Enter the email address that you used for signup for user name and the access code for password. You can also change your password by clicking the 'Change Password' link. The process is explained above in this section.
- Click 'Login'.

The 'Home' screen of the **Management Console** will be displayed.

2. The Central Management Console

The central management console allows admins to add users and endpoint groups, create policies and apply them to endpoint groups, view reports, configure console settings and more.



Once logged-in, the administrator can navigate to different areas of the console by clicking the tabs on the left hand side. By default the 'Home' screen will be displayed after logging-in to the console.

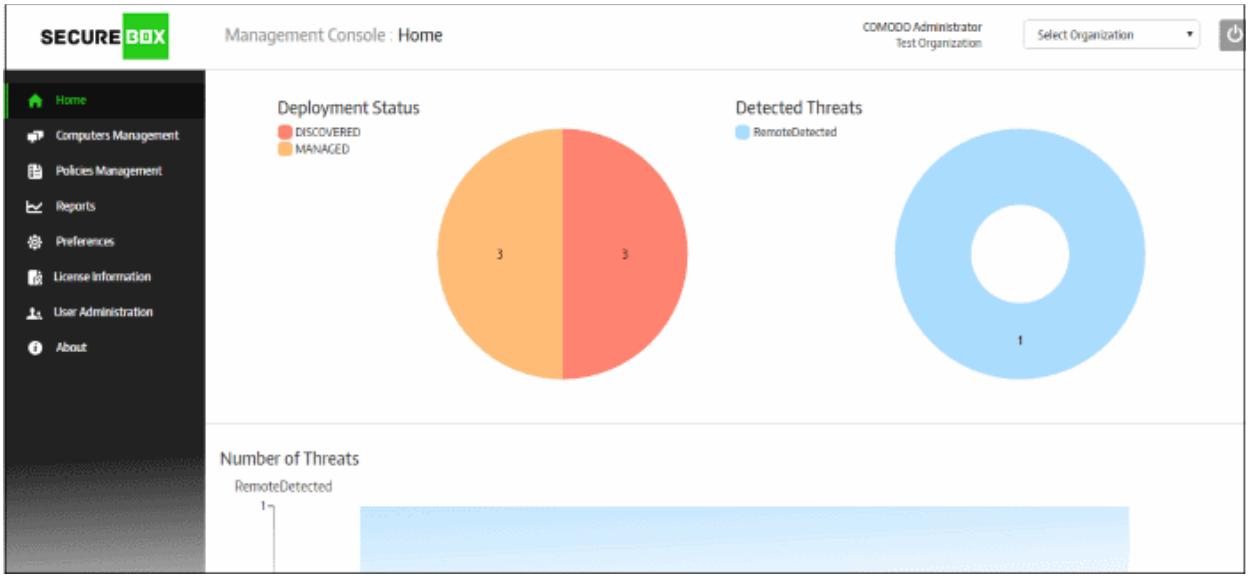
- **Home** - Allows administrator to view snapshot summaries of details such as managed and discovered systems, number of detected threats, number of endpoints on which the threats were discovered and the name of the discovered threats. Refer to the section '**The Home Screen**' for more details.
- **Computers Management** - Allows administrators to add computers to the management console by different methods such as Work Group, Active Directory, Network Address and by email link. Refer to the section '**Endpoints and Endpoint Group**' for more details.
- **Policies Management** - Allows administrators to create polices in order to run applications, URLs and folders inside the secured environment. Refer to the section '**Policies**' for more details.
- **Reports** - View the threats detected by Secure Box and report of activities on the endpoints related to secure box such as starting a secured application and more. Refer to the section '**Reports**' for more details.
- **Preferences** - Allows administrators to configure the settings for the management console. Refer to the section '**Configuring the Management Console**' for more details.
- **License Information** - Allows administrators to view details of current license and add and buy additional licenses. Refer to the section '**License Information**' for more details.
- **User Administration** - Allows administrator to add users as well as administrators with different privileges and group them as per the organization's requirement. Refer to the section '**Users and User Groups**' for more details.
- **About** - Provides details about the console such as version number, customer ID as well as allow administrators to view online help guides and post queries on the support forums. Refer to the section '**Management Console Details and Support**' for more details.

At the top right of the interface displays the name the organization and the name of the user currently logged in for the organization. Clicking the  button allows the user to log out of the console.

3.The Home Screen

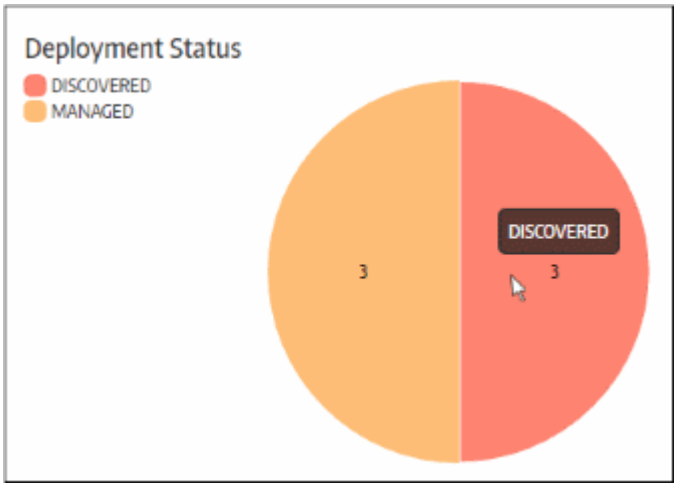
The 'Home' screen contains a snapshot of your SecureBox deployment, showing pie charts of managed/discovered endpoints and detected threats. Threats are also displayed as a bar graph for each category and on which endpoints they were detected.

The 'Home' screen will be displayed by default after logging-in to the console. You can also return here by clicking 'Home' at the top of the interface.



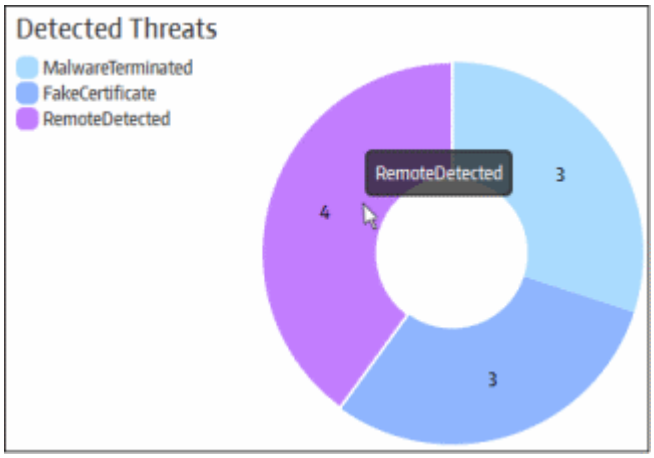
Deployment Status

The 'Deployment Status' pie chart displays a summary of endpoints on customer networks. The 'Discovered' segment includes endpoints that were scanned in the network and discovered via Work Group, Active Directory and Network Address. These discovered endpoints will become managed after the CSB package is deployed and accepted by the administrator. The 'Managed' segment provides the number of endpoints on which the SB application is installed and connected to the console. Placing the mouse cursor over a sector displays more details. Refer to the section '**Enrolling Endpoints for Management**' for more details.



Detected Threats

The 'Detected Threats' chart displays an overview of threats encountered by Secure Box on your managed endpoints. The threats displayed here depend on the protection settings defined in your SecureBox policies. Refer to the section '**Policies**' for more details. Place your mouse cursor over a sector to view more details.



The bar graphs below the pie chart section provide further details about detected threats. These include the number of each type of threat and the details of the endpoints on which they were detected. Placing your mouse cursor over a graph displays more details.

An example of bar graph for a detected threat:

An example of bar graph displaying the details of endpoints on which a threat was detected:

Detected threats in graphical format:

4.Manage Organizations

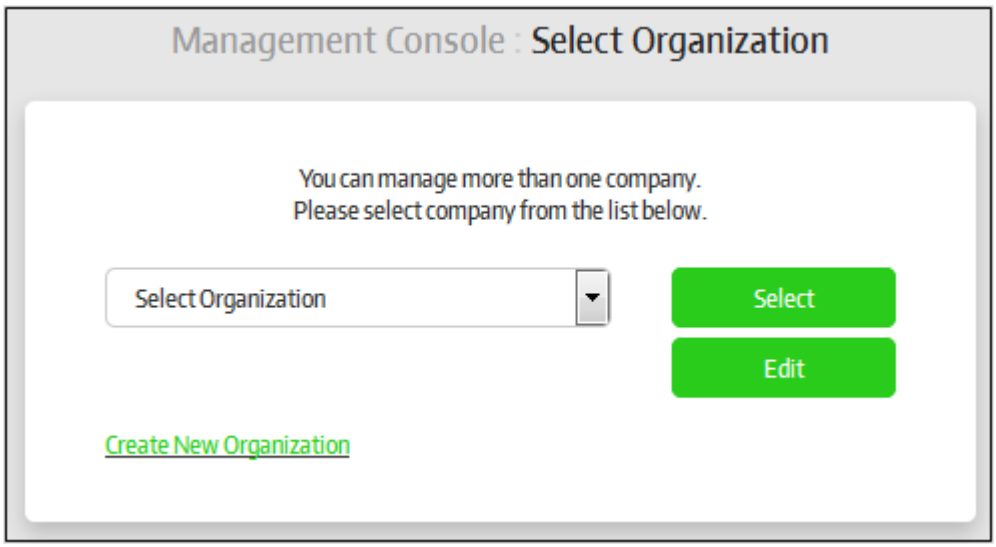
The Secure Box Central Management Console allows administrators to add organizations/companies/departments as per their requirements. This helps you to consolidate and manage all your SB deployments from a single console.

Each organization can contain several endpoint groups and each group may be applied with a security policy. For more details on creating endpoint and applying policies, refer to the section **Managing Endpoint Groups**.

The number of new organizations and endpoints that can be added depends on your account license. Refer to the section '**License Information**' for more details about viewing your current license status and to buy more licenses.

Note: Organization management is only available for consoles installed on customer premises. Administrator with super admin privileges only can manage multiple organizations for an account. Customers using the SaaS console should contact Comodo for organization management.

The next screen after **logging-in** to the management console allows you to manage organizations:



Refer to the following sections for more details about adding and editing organizations:

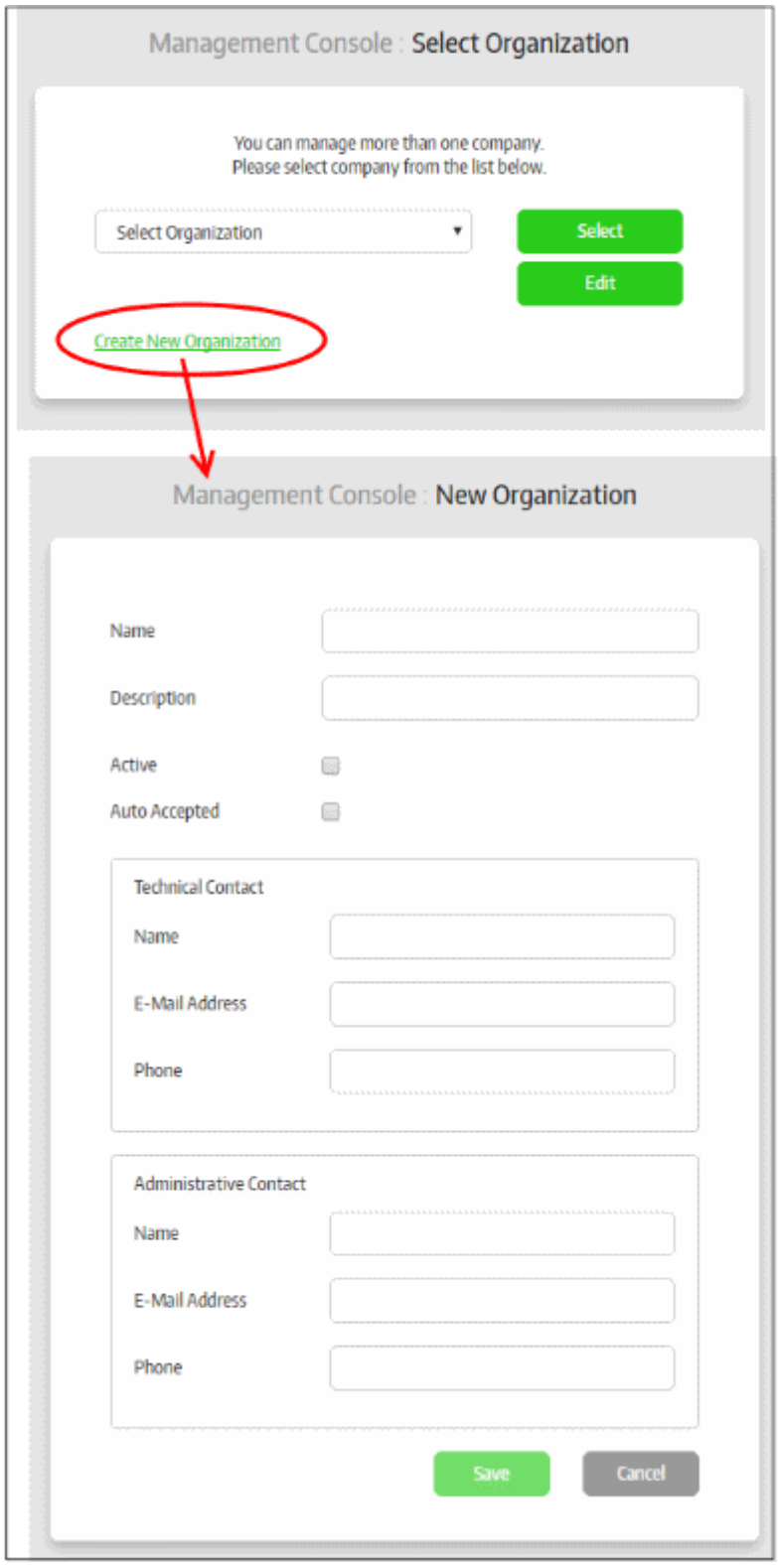
- **Add a new organization**
- **Edit and deactivate an organization**

4.1.Add a New Organization

The SB Management Console allows administrators with super admin privileges to add organizations/departments for a single account. This will help them to manage all the enrolled endpoints of different organizations from the Central Management Console. The primary administrator can, if required, add another administrator who can access the added organization in the console for managing it.

Note: Organization management is only available for consoles installed on customer premises. Administrator with super admin privileges only can manage multiple organizations for an account. Customers using the SaaS console should contact Comodo for organization management.

To add a new organization, click the 'Create New Organization' link in the 'Select Organization' screen, which appears after **logging-in** to the management console.

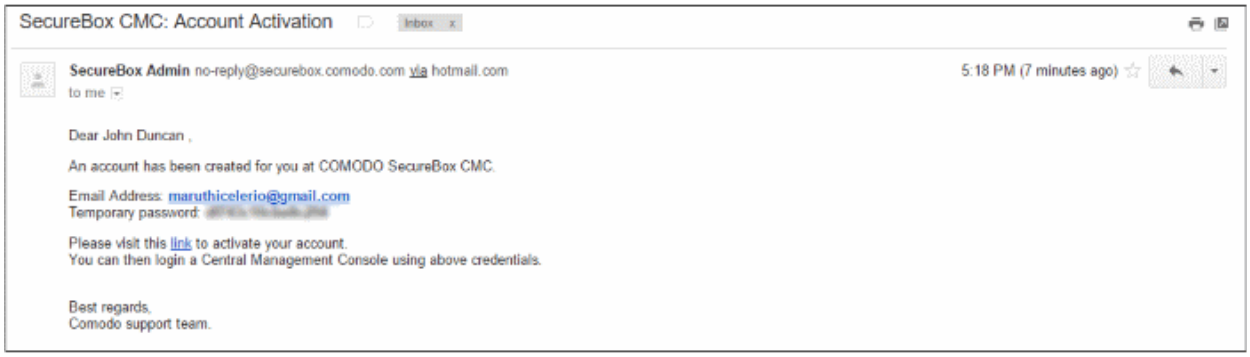


Add Organization - Form Parameters	
Form Element	**Description**
Name	Enter the name of the organization/company
Description	Provide an appropriate description for the organization/company
Active	Select the check box if you want to activate the organization. Only if the organization is

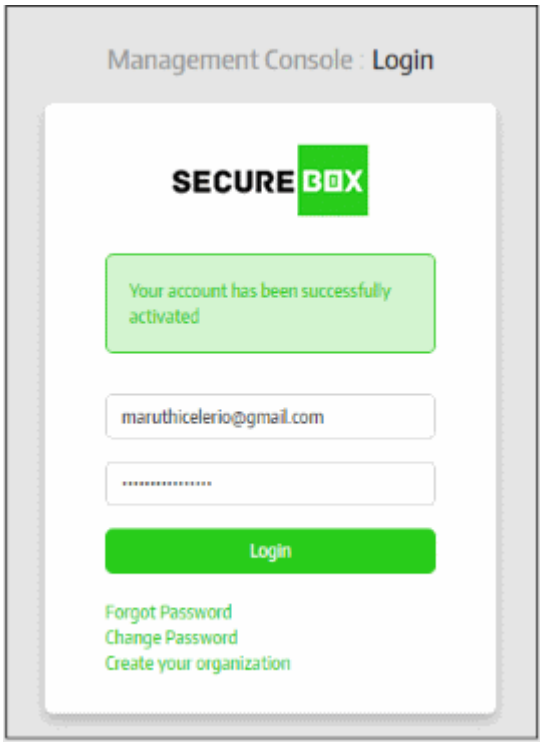
	active, can the endpoints be added and managed from the management console.
Auto Accepted	Endpoints that are enrolled need to be confirmed by administrators in order to be paired with CMC. If this option is selected, then newly enrolled endpoints will be automatically registered with CMC for this organization.
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 - The person who can log into the management console with access only to the added organization	
Name	Enter the name of the administrator
E-Mail Address	Enter the email address of the administrator to which the activation link will be sent
Phone	Enter the phone number of the administrator

- Click the 'Save' button

The added organization will be saved and an email containing the activation link to activate the administrator account will be sent.



The administrator's account will be activated on clicking this activation link.



The administrator should change the password immediately, since he/she is provided only with a temporary password. Refer to the section '**Logging-in to the Management Console**' for more details about changing the current password. By default, the added user will have administrative privileges and the primary administrator can reset the privilege levels from the 'User Groups' section. Refer to the section '**Managing User Groups**' for more details.

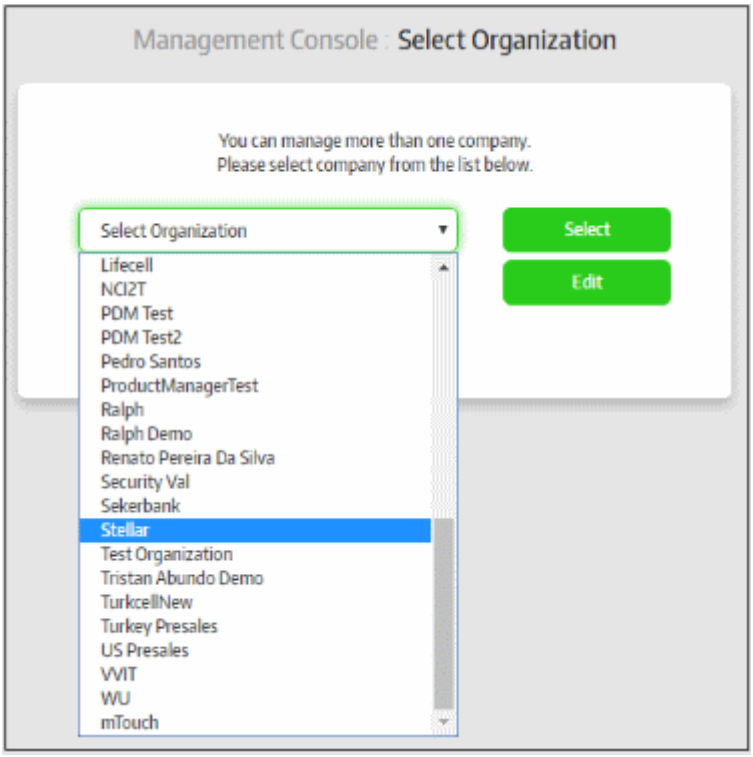
After the account has been activated, the administrative user can log-in to the management console for managing the newly added organization only. Before enrolling endpoints, you have to add license and upload installer packages in order to install them on endpoints. Refer to the section '**License Information**' and '**Configuring the Management Console**' for more details.

4.2. Edit and Deactivate an Organization

The Central Management Console installed on customer's premises allows primary administrators to edit organization details and deactivate the organization if required.

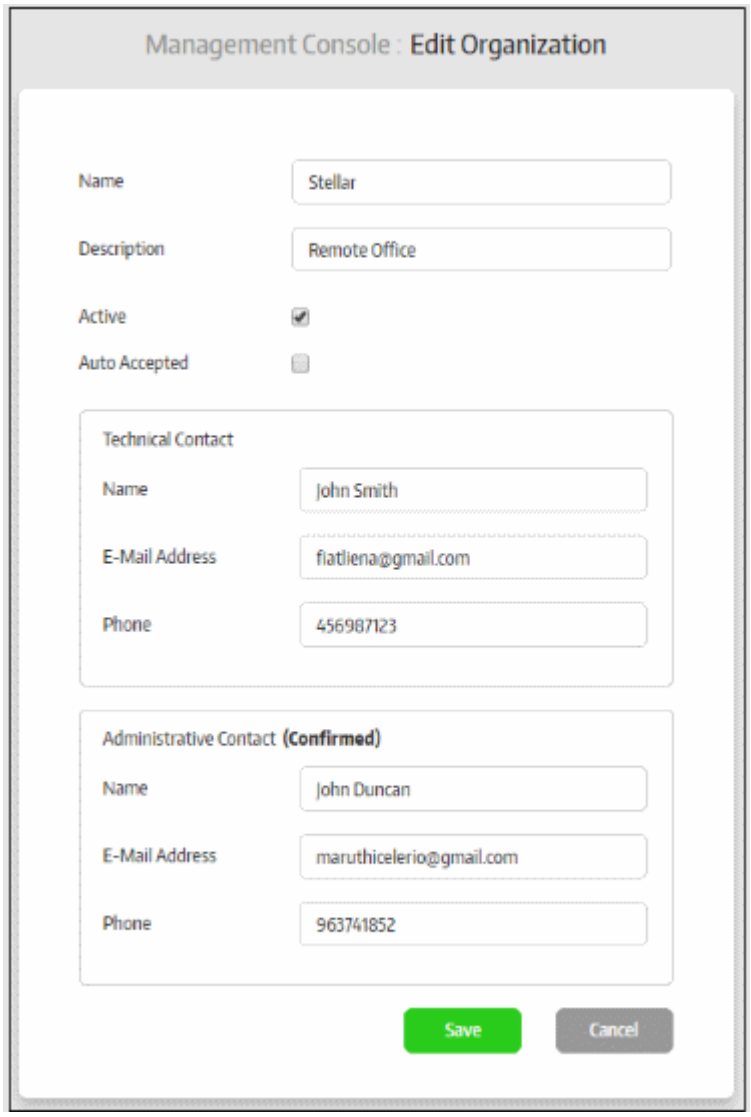
Note: Organization management is only available for consoles installed on customer premises. Administrators need super admin privileges to manage multiple organizations for an account. Customers using the SaaS (web-based) console should contact Comodo for organization management.

To edit an organization, select the organization from the drop-down in the 'Select Organization' screen, which appears after **logging-in** to the management console.



- Click the 'Edit' button

The 'Edit Organization' screen will be displayed:



Edit organization details as required. The form is that as used when adding an organization. Refer to the section '**Adding a New Organization**' for more details. Please note that if you change the administrative contact, an activation email will be sent to the administrator as explained in the previous section, '**Adding a New Organization**'.

- Click the 'Save' button to apply your changes.
- Uncheck the 'Active' check box to deactivate an organization.

Endpoints belonging to deactivated organizations can no longer be managed, meaning policies cannot be deployed and the Secure Box applications on the endpoints will be disabled.

5. Users and User Groups

The 'User Administration' section allows administrators to add users with different privilege levels according to the organization's requirement. The users have to be placed inside groups and each group can be assigned the required privileges which will automatically apply to the users in the group. The section allows you to add as many groups as you require so as to place the users accordingly for managing the endpoints in the organization.

Refer to the following for more details:

- **Manage Users**
- **Manage User Groups**

5.1. Manage Users

The 'Users' screen allows administrators with appropriate privileges to add new users to the Secure Box Management Console for managing an organization. The scope of operations that a user can perform depends on the privileges assigned to the group to which the user belongs. Refer to **'Managing User Groups'** if you wish to know more about privilege levels.

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

Users - Table of Column Description	
Column	**Description**
Name	The username of an individual user. User's with (Admin Contact) after their names were chosen as admin contact when the organization was created. Refer to the section **'Adding a New Organization'** for more details. Clicking on a username will open the 'User Properties' screen, which is the same screen displayed for adding a user. Refer to **'Adding a user'** for more details.
Email Address	The email address provided for the user while adding

Account	Indicates whether the user has activated his account by clicking the activation link in the activation email that was sent during the adding process
Status	Indicates whether the user is allowed to access the management console or not. A disabled user cannot access the management console.
Group	Indicates to which group the user was added. Refer to the section '**Managing User Groups**' for more details. Please note the 'Admin Contact' will by default added to the 'Administrators' group.

Sorting and filtering options

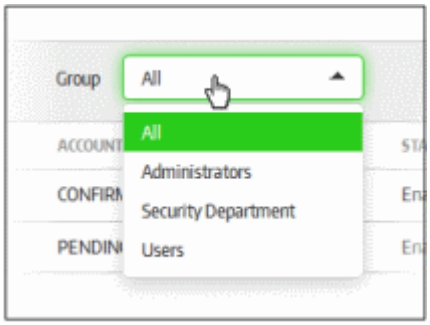
Sorting the entries

Clicking any column heading sorts the entries based on the ascending/descending order of the entries as per the information displayed in the respective column. Please note the sorting option is not available for 'Group' column.

Using the filter option

The users list can be filtered to display the entries based on a group. Refer to the section '**Managing User Groups**' for more details.

- Select the group from the 'Group' drop-down



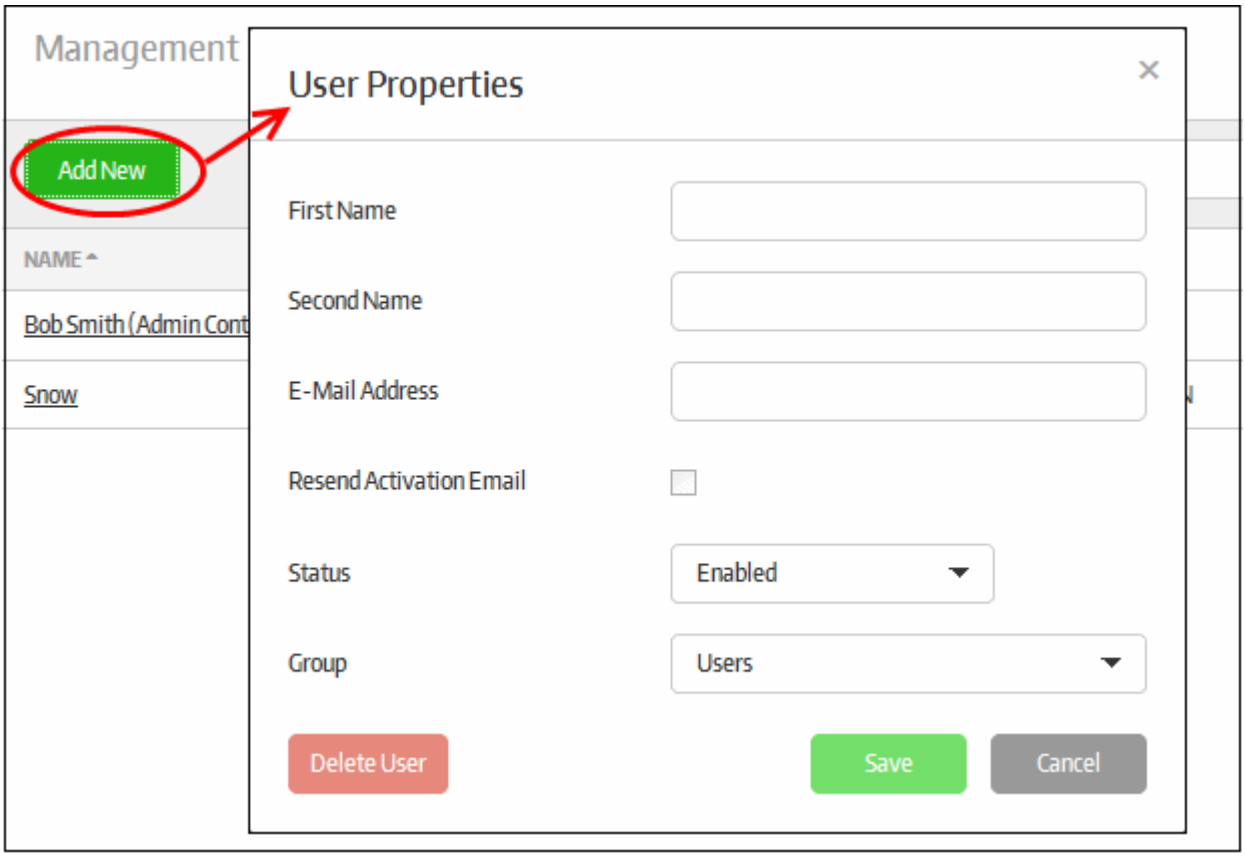
The users belonging to the selected group will be displayed on the screen.

The screen allows administrators to:

- **Add a new user**
- **Edit a user**
- **Delete a user**

To add a new user

- Click the 'Add New' button at the top of the table



The 'User Properties' screen will be displayed.

User Properties - Form Parameters	
Form Element	**Description**
Name	Enter the first name of the user
Second Name	Enter the second name of the user
E-Mail Address	Enter the email address of the user to which the activation mail will be sent
Resend Activation Email	Allows to send another activation email if the password in the initial mail is lapsed or if the user is removed and added again with the same email address.
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 you want to place the user. The groups can be created from the 'User Groups' section. Refer to the section '**Managing User Groups**' for more details.

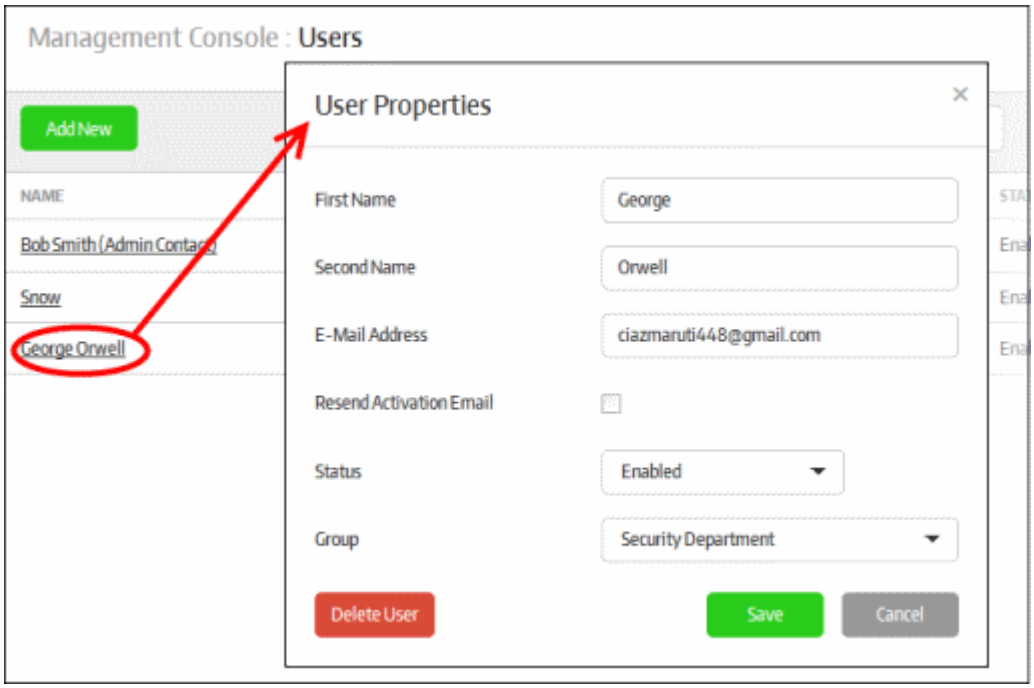
- Click the 'Save' button.

An activation mail 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 can access the management console using the temporary password. It is advisable the user changes the password immediately for continued access to the console. Refer to the section 'Logging-in to the Management Console' to know more about changing console access password.

To edit a user

- Click on the name of the user that you want to edit

The 'User Properties' screen with details of the selected user will be displayed.

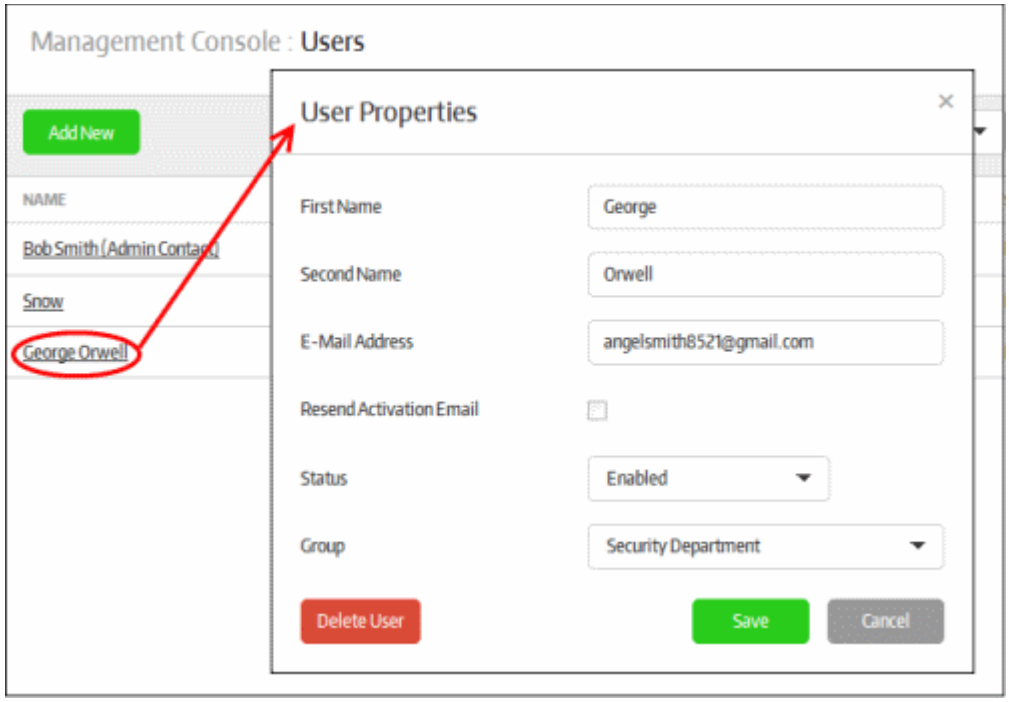


- Edit the details as required. Please note if you change the email address of the user, a new activation mail will be sent to the changed email address. The user has to once again activate the account for accessing the management console.
- Click the 'Save' button

To delete a user

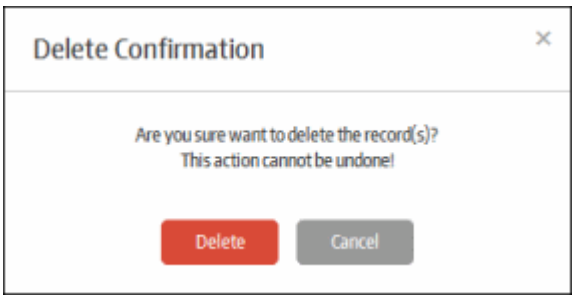
- Click on the name of the user that you want to delete

The 'User Properties' screen with details of the selected user will be displayed.



- Click the 'Delete User' button at the bottom

A confirmation dialog will be displayed.



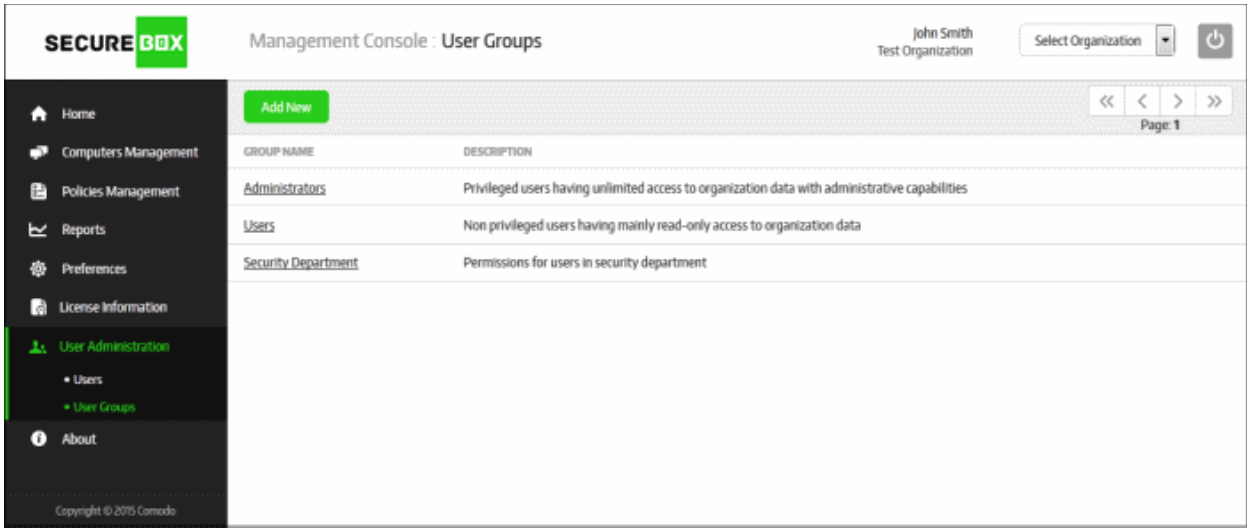
- Click 'Delete' to confirm removal of the user

The user will be removed from the list.

5.2. Manage User Groups

Users that are added to the management console have to be placed in a group in order to manage an organization. By default, there are two groups shipped with the console, Administrators and Users. The 'Administrative' user group provides unlimited access to the organization with administrative capabilities whereas the 'Users' group provides mainly read-only privileges to organization data. In addition, you can also create groups with different privilege levels and add user into them as per the organization's requirement.

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



User Groups - Table of Column Description	
Column	**Description**
Group Name	The name of the user group that was provided while adding. The 'Administrators' and 'Users' groups are shipped with the console. These two default groups cannot be deleted but other details such as privilege levels can be edited. Clicking on a user group name will open the 'User Group Properties' screen. Refer to '**To edit a user group**' for more details.
Description	The description provided for the group while adding.

Sorting options

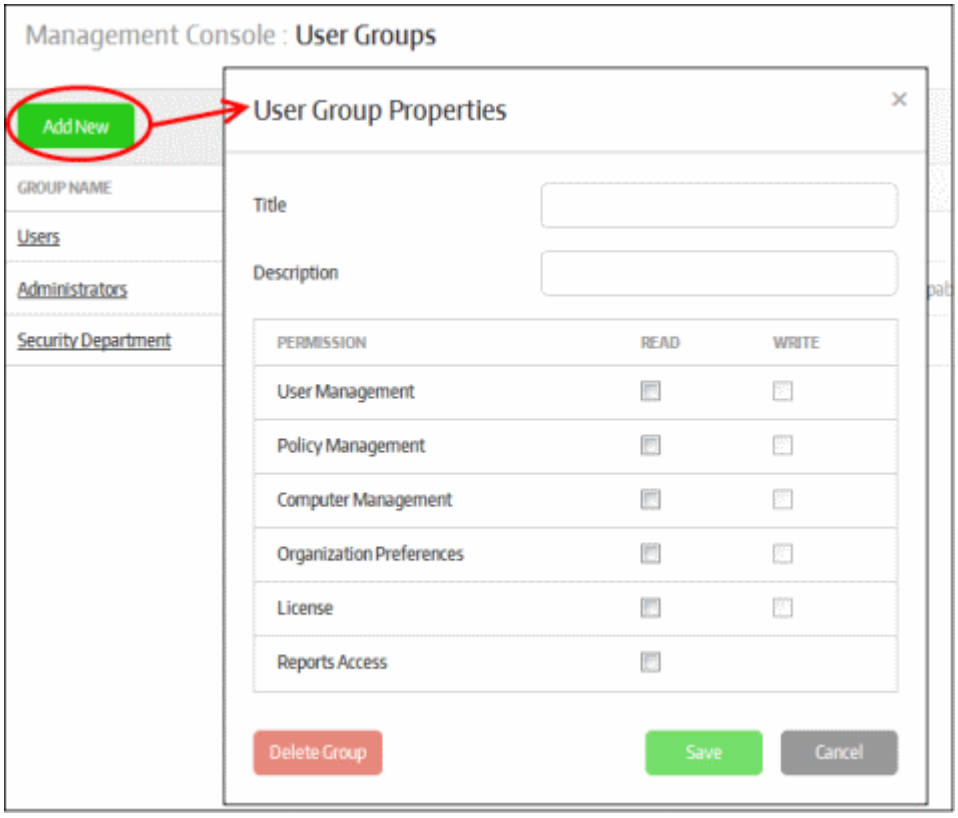
Clicking any column heading sorts the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

The screen allows administrators to:

- **Add a new user group**
- **Edit a user group**
- **Delete a user group**

To add a new user group

- Click the 'Add New' button at the top of the table



The 'User Group Properties' screen will be displayed:

User Group Properties - Form Parameters	
Form Element	**Description**
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	
User Management	This area allows the management of users such as add user, add groups and more. Refer to the section '**Users and User Groups**' for more details.
Policy Management	This area allows management of policies such as create new polices, edit and more. Refer to the section '**Policies**' for more details.

Computer Management	This area allows to manage computers such as enroll new endpoints, create groups, assign policies and more. Refer to the section '**Endpoints and Endpoint Group**' for more details.
Organization Preferences	This area allows to configure the management console settings. Refer to the section '**Configuring the Management Console**' for more details.
License	View details of current license, add and buy additional licenses. Refer to the section '**License Information**' for more details.
Reports Access	View the threats detected by Secure Box and report of activities on the endpoints related to secure box. Refer to the section '**Reports**' for more details.

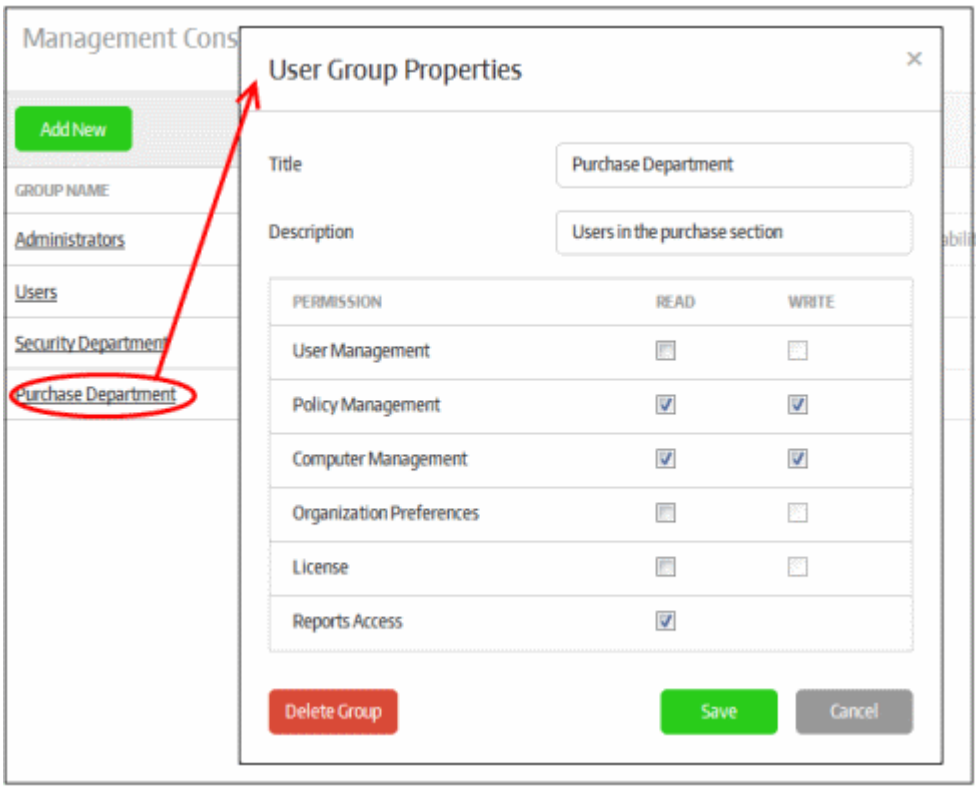
- Click the 'Save' button

The newly added user group will be listed in the screen and will also be available for selection while adding/editing users. Refer to the section '**Managing Users**' for more details about adding / editing users. The users after logging-in to the console can manage the organization as per the privileges assigned for his/her group.

To edit a user group

- Click on the name of the user group that you want to edit

The 'User Group Properties' screen with details of the selected user will be displayed.



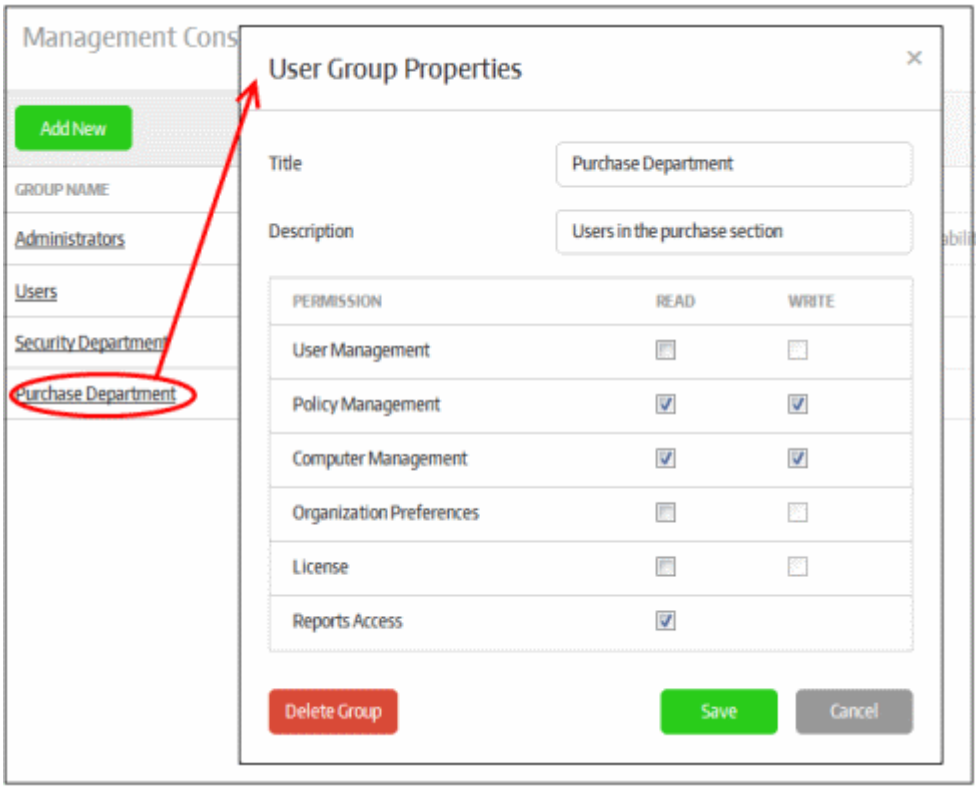
- Edit the details as required. Please note if you change privileges for the group, the users in the group will be automatically assigned the new permissions. Refer to the section '**To add a new user group**' for more details about privileges.
- Click the 'Save' button

To delete a user group

You cannot delete a group in which users are available. To delete a group, you have to first reassign the users to another group or delete them from the user list. You can only delete a group that has no users in it.

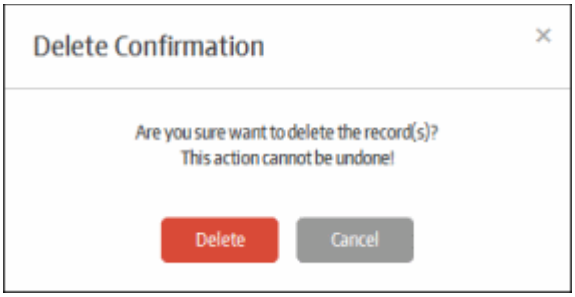
- Click on the name of the user group that you want to delete

The 'User Group Properties' screen with details of the selected user will be displayed.



- Click the 'Delete Group' button

A confirmation dialog will be displayed.



- Click 'Delete' to confirm removal of the user group

The user group will be removed from the list.

6.Endpoints and Endpoint Groups

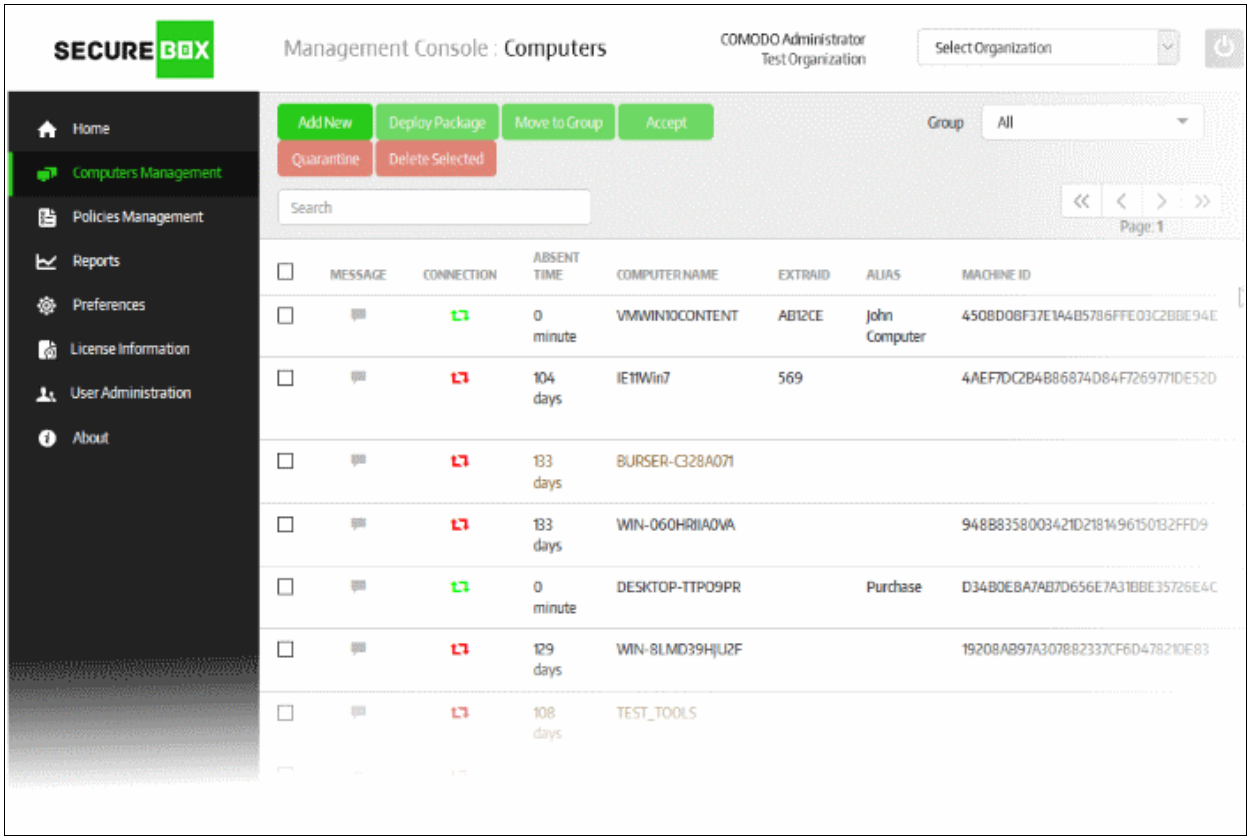
Endpoints belonging to an organization must be enrolled to the Central Management Console in order to manage them. There are multiple ways by which the endpoints can be added. The methods, Active Directory, Network Address and Work Group, can be used for enrolling endpoints within an organization's network and for endpoints outside the network (use the 'Create Email Link' to enroll external endpoints).

Enrolled endpoints have to be added to 'Groups' in order to assign polices to them. Even if you want to assign a policy to a single endpoint, you still need to create a group for it. Each policy contains a set of Secure Box applications to be run on the endpoints.

- For more details on creating endpoint groups and applying policies, refer to **Creating a New Endpoint Group**
- For more details on creating and managing policies, refer to **Creating a New Policy**

The groups also serve the purpose of defining the quarantine period for endpoints belonging to it. During the quarantine period, a user cannot use the SB applications on the endpoints.

The 'Computer Management' section allows administrators with appropriate privileges to enroll endpoints and assign policies to them.



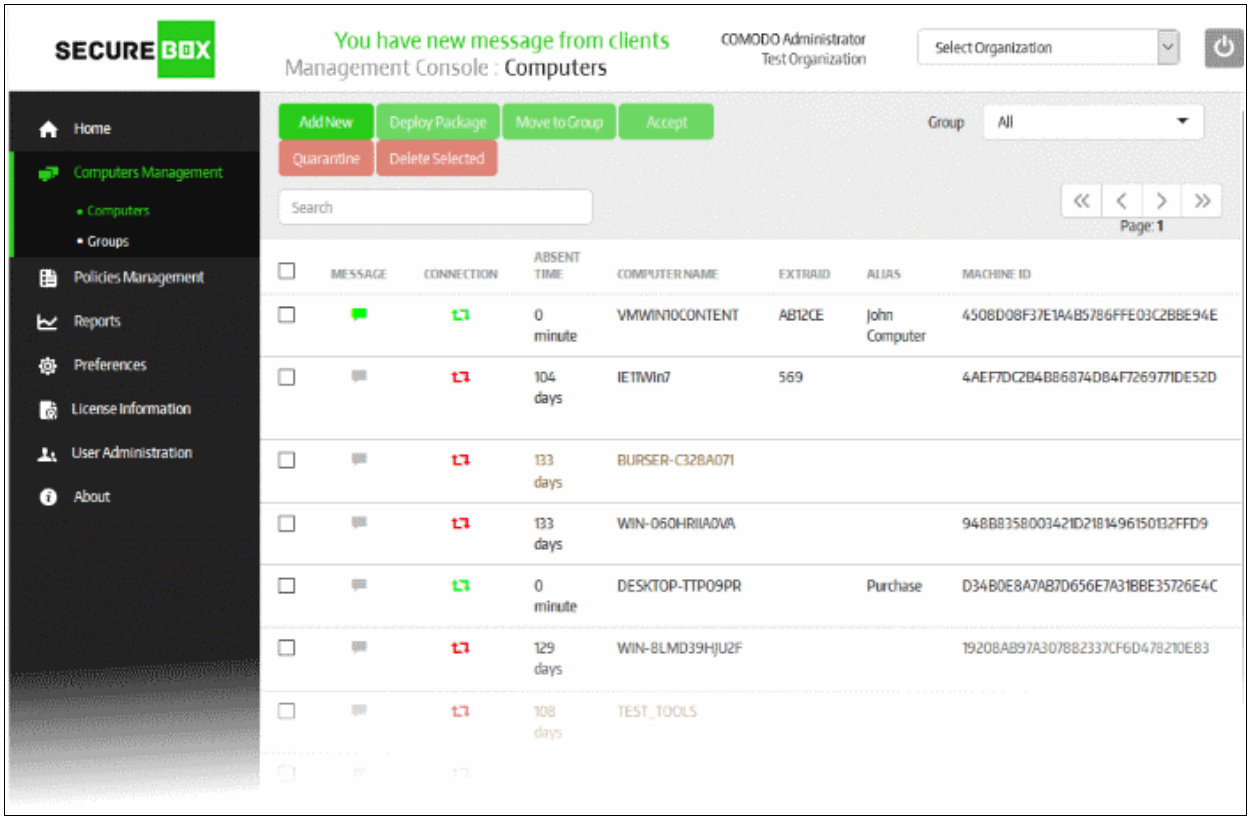
Click the following links for more details:

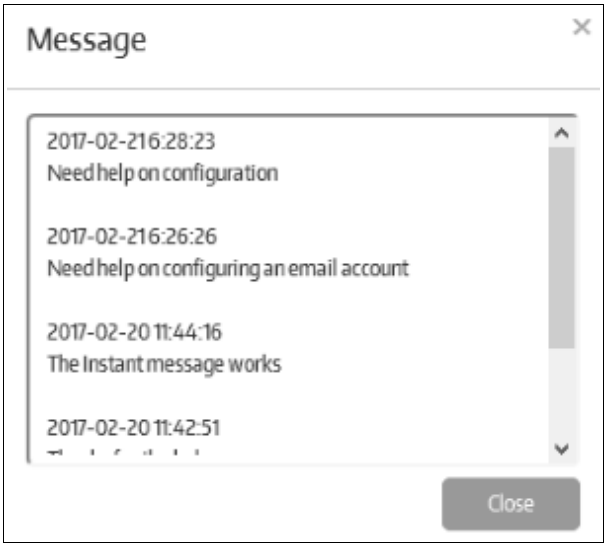
- **Managing Endpoints**
- **Managing Endpoint Groups**

6.1. Manage Endpoints

The 'Computers' section allows administrators to enroll, quarantine or delete endpoints, and to move them to endpoint groups so security policies can be applied to them. Endpoints can be added in various ways, including 'Active Directory', 'Work Group', 'Network Address' and by 'Create Email Link'. While the first three methods are suitable for bulk enrollment within the network, the latter method can be used for enrolling endpoints outside the organization's network.

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



Computers - Table of Column Description	
Column	**Description**
Message	Indicates whether or not a message has been received from the user of the endpoint. - Indicates that a new message has been sent from an endpoint Click the green icon to view the message: 

Connection	Indicates the status of endpoint connection to the management console: - Indicates the endpoint is connected to CMC - Indicates the connection is lost for more than the configured time in the first 'Absent Time' setting from the '**Preferences**' screen. - Indicates the connection is lost for more than the configured time in the second 'Absent Time' setting from the '**Preferences**' screen.
Absent Time	Indicates the period the endpoint is not connected to CMC. This depends on the configuration done in the Preferences section. Refer to the section '**Configuring the Management Console**' for more details. A blank indicates the endpoint is in 'Confirmation Pending' status.
Computer Name	The name of the enrolled endpoint
Extra ID	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. The console uses the extra ID in addition to the machine ID to authenticate the endpoint. The extra ID can be assigned to an endpoint in two ways: • **Organizations configured for manual approval of endpoints**. The extra ID can be specified during the approval process. Refer to the section **Enrolling Endpoints for Management** for more details. • **Organizations configured for auto-approval of endpoints**. Enrolled endpoints will be approved automatically without an extra ID. Administrators can manually assign an extra ID by entering a value in the 'Extra ID' field in the row of the endpoint. Administrators can change the extra ID of an endpoint by clicking on the existing value and entering a new value. The assigned IDs will be automatically pushed to endpoints during the next polling cycle of the CSB agent.
Alias	Alternative name of the endpoint. If required, administrators can specify an alias name to more easily identify the machine.
Machine ID	The ID assigned by CMS to the endpoint
Group Name	Indicates to which group the endpoint is assigned. Refer to the section '**Managing Endpoint Groups**' for more details.
Status	Indicates whether the CSB installed on endpoints are paired with CMC or not. After the CSB installation on endpoints, it will send a connection request to the management console. The administrator should click 'Accept' button after selecting the endpoint in the list. There are three statuses: • MGD - The connection request has been accepted and the endpoint in now managed. • Confirmation Pending - CSB is installed on endpoint, but the administrator has not yet accepted the connection request. Click the 'Accept' button to change the status to managed. • Not Managed - Endpoints that were in managed status, but when CSB is uninstalled on endpoints, it will show as 'Not Managed'. When the CSB is installed again, it will show as managed again and administrator's acceptance is not required. This field will display an installation ID for endpoints with new CSB installations. This

	can be used by administrators to identify endpoints which need approval.
CSB Version	Indicates the version of installed CSB version on the endpoints
Created	The date and time on enrollment of the endpoint to CMC
Discovered As	The name of the endpoint
Source	The method of enrollment of the endpoint whether 'Active Directory', 'Work Group', 'Network Address' or by 'Email'
IP	The IP address of the enrolled endpoint
External IP	The public IP address assigned by your Internet Service Provider, which is used for identifying your network/endpoint from outside the network.

Sorting, filtering and searching options

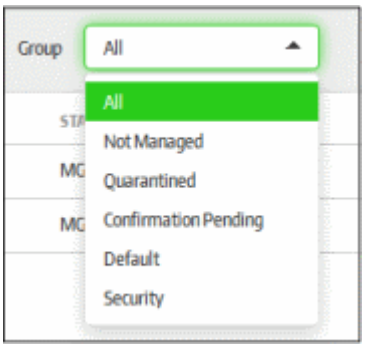
Sorting the entries

Clicking on a column heading sorts the entries based on the ascending/descending order of the entries as per the information displayed in the respective column. Please note the sorting option is not available for 'Group Name' and 'Status' columns.

Using the filter option

The endpoints can be filtered to display the entries based on group, status and quarantined.

- Click the 'Group' drop-down



- Select the option from the drop-down
  - All - Displays all the endpoints
  - Not Managed - Displays the endpoints in which the CSB app is uninstalled and the status has changed to 'Not Managed'
  - Quarantined - Displays the endpoints that are quarantined. Refer to the section '**Quarantining Endpoints**' for more details.
  - Confirmation Pending - Displays the endpoints in which the CSB is installed but not yet accepted by the administrator.

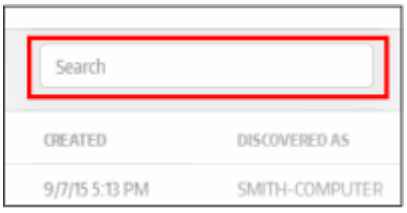
The options below this are the endpoints groups. Refer to the section '**Managing Endpoint Groups**' for more details.

  - Default - Displays the endpoints that are in the default endpoint group
  - Group Name - Displays the endpoints that are in the selected group.
- Select the group for which the endpoints should be filtered.

The list will display the endpoints based on the selected filter options.

Using the search option

The search option in the screen allows to search for endpoints based on computer name, machine ID, source and IP.



- Enter the details fully or partially in the 'Search' field and click anywhere on the screen or 'Enter' on the keyboard

The list will be searched for the entered text and endpoints displayed accordingly. To display all the items again, clear the field and click anywhere on the screen or 'Enter' on the keyboard.

The interface allows an administrator with appropriate privileges to:

- **Enroll endpoints for management**
- **Assign endpoint to groups**
- **Quarantine endpoints**
- **Delete endpoints**

6.1.1. Enroll Endpoints for Management

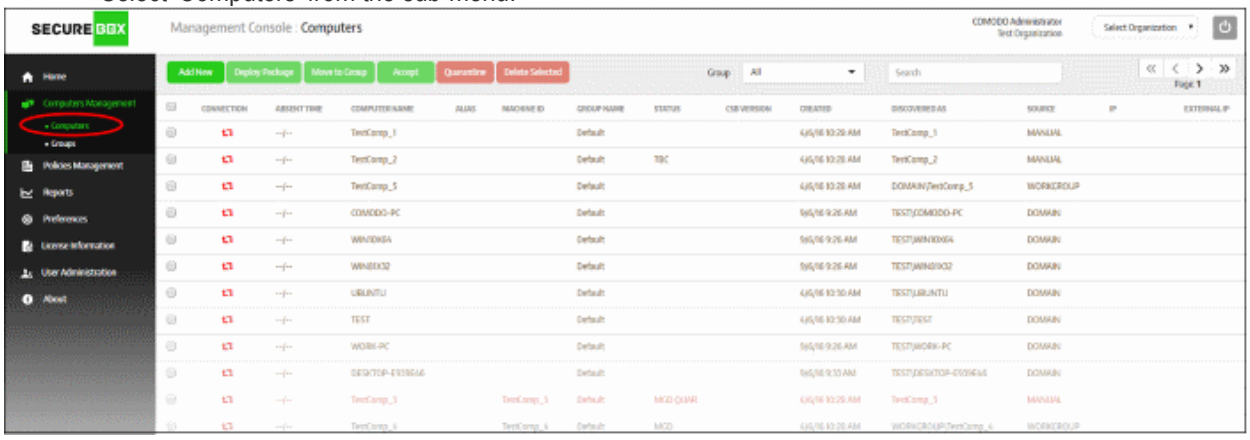
SecureBox allows administrators to enroll computers for central management using any of the following methods:

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

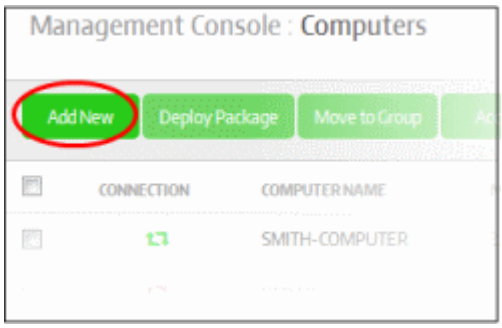
The first three methods are suitable for enrolling local computers using a Secure Box management console that is installed on-premises. Endpoints are automatically discovered and added for management per the 'Auto-Discovery Settings' configured in the '**Preferences**' section. The 'Email Link' method is used for enrolling endpoints over the internet and is the only method available for customers using the SaaS version of CMC.

To enroll endpoints:

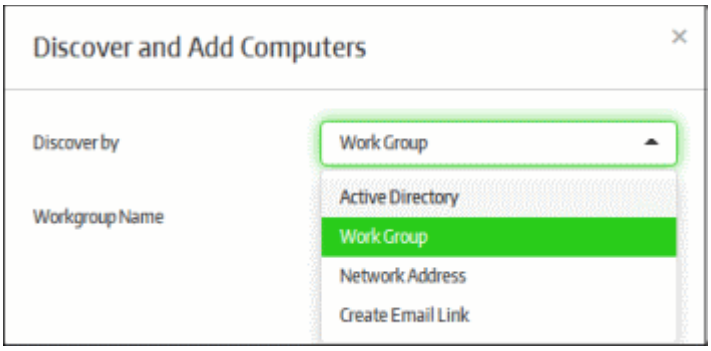
- Click 'Computers Management' on the left
- Select 'Computers' from the sub-menu:



- Click the 'Add New' button



- This will open the 'Discover and Add Computer' dialog.
- Click the 'Discover by' drop-down and select the method by which you want to add the endpoints:



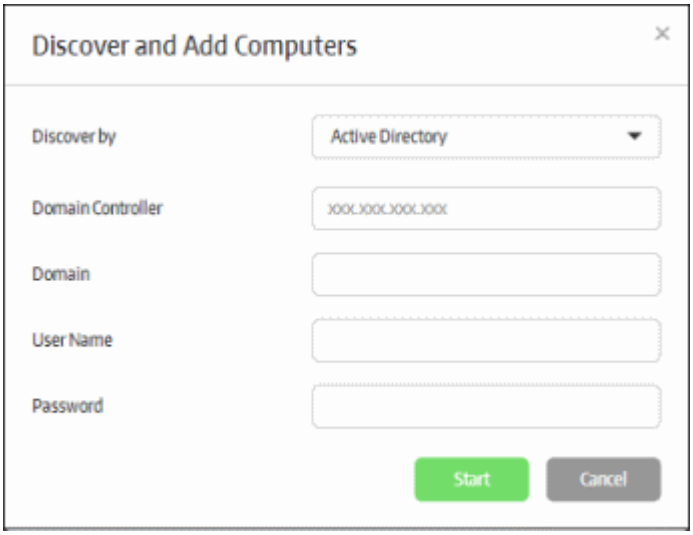
Click the following links for explanations of each enrollment method:

- **Enrollment via Active Directory**
- **Enrollment via Work Group**
- **Enrollment via Network Address**
- **Enrollment via Email Link**

Enrollment via Active Directory

Please note endpoint enrollment via AD will work only if CMC is added to your domain during on-premise installation. Refer to the section **Initial Setup** for more details.

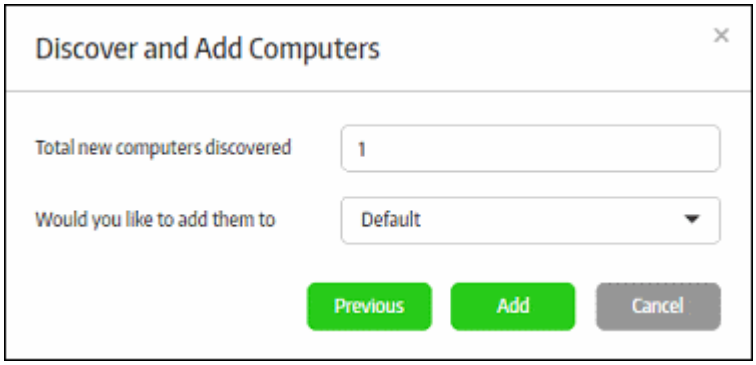
- Select the 'Active Directory' option from the drop-down:



- Enter the required Active Directory configuration information and click the 'Start' button

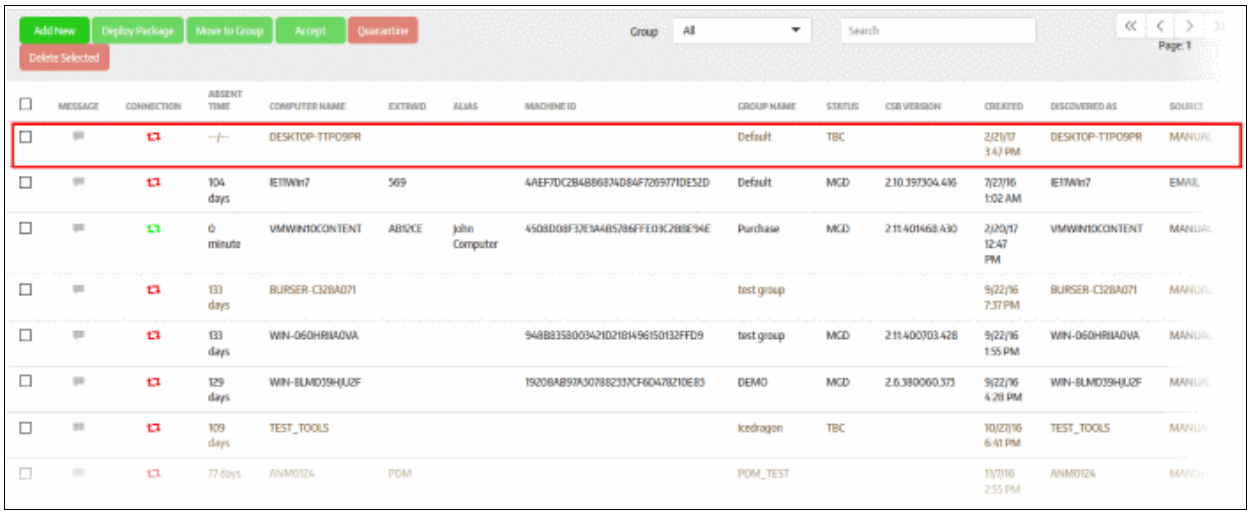
The management console will run a scan to discover endpoints and, if available, will show the number of endpoints

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.

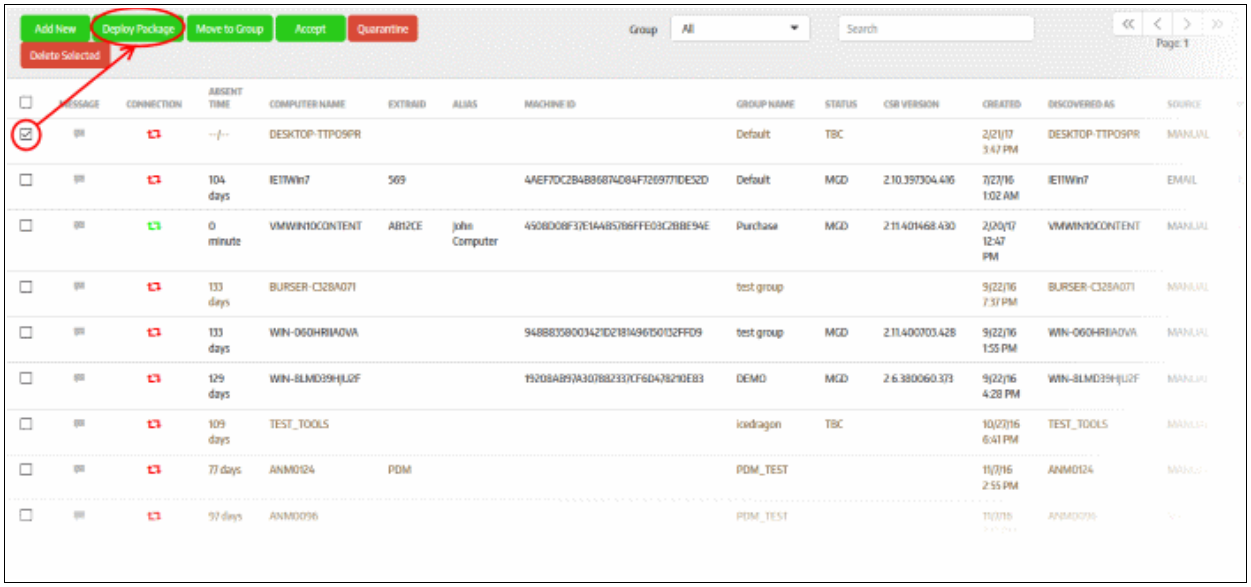


- Select your desired endpoint group from the drop-down and click the 'Add' button.

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

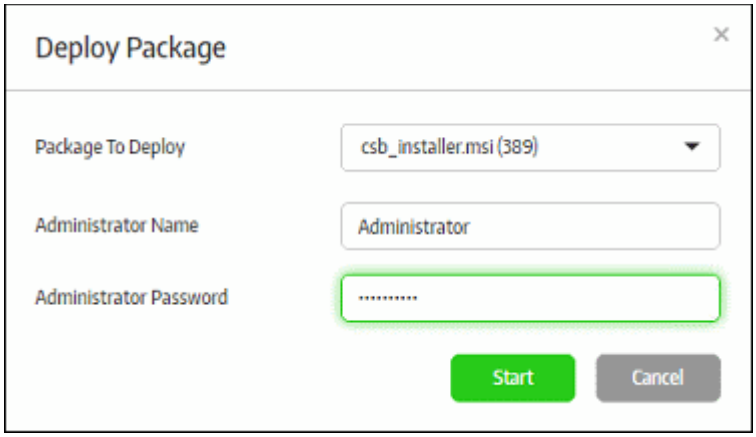


The next step is to deploy the CSB package that should be installed on the endpoints. Installing a package will allow you to assign policies and manage the endpoint.



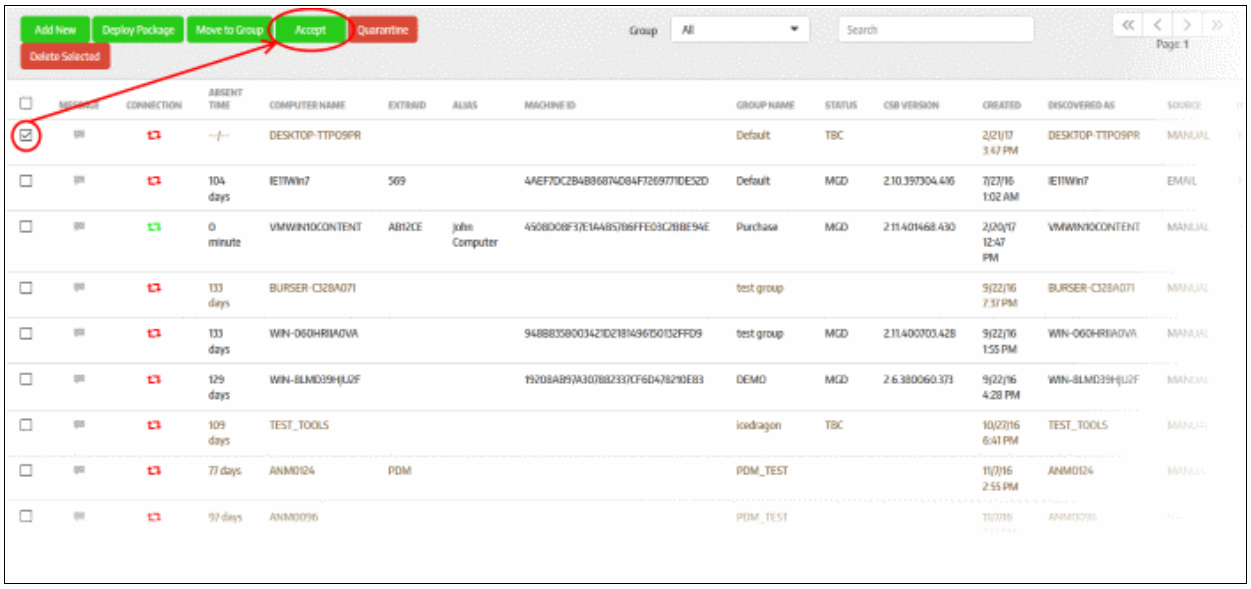
- Click the 'Deploy Package' button after selecting the endpoint

The 'Deploy Package' dialog will be displayed.



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

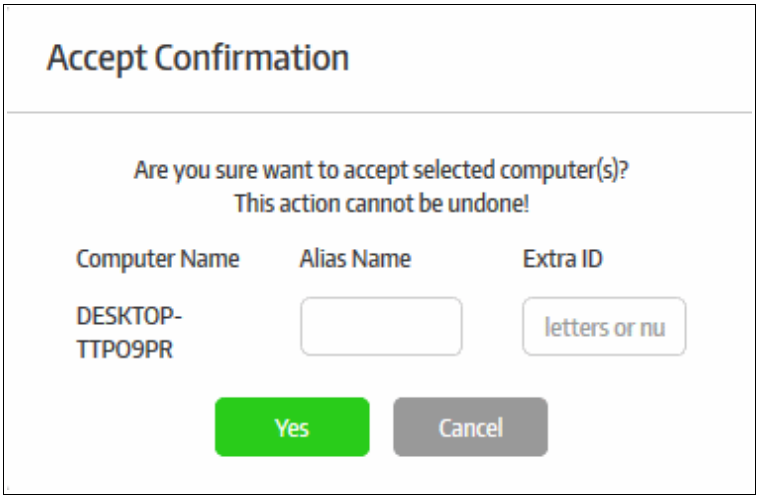
The selected package will be deployed and the status of the endpoint will change to 'MGD TBC' - meaning it has to be accepted by the administrator. If the 'Auto accept' option was enabled while adding the organization, then enrolled endpoints will be automatically accepted. Refer to the section '**Adding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



- Select the endpoint and click 'Accept'

The 'Accept Confirmation' dialog will be displayed.

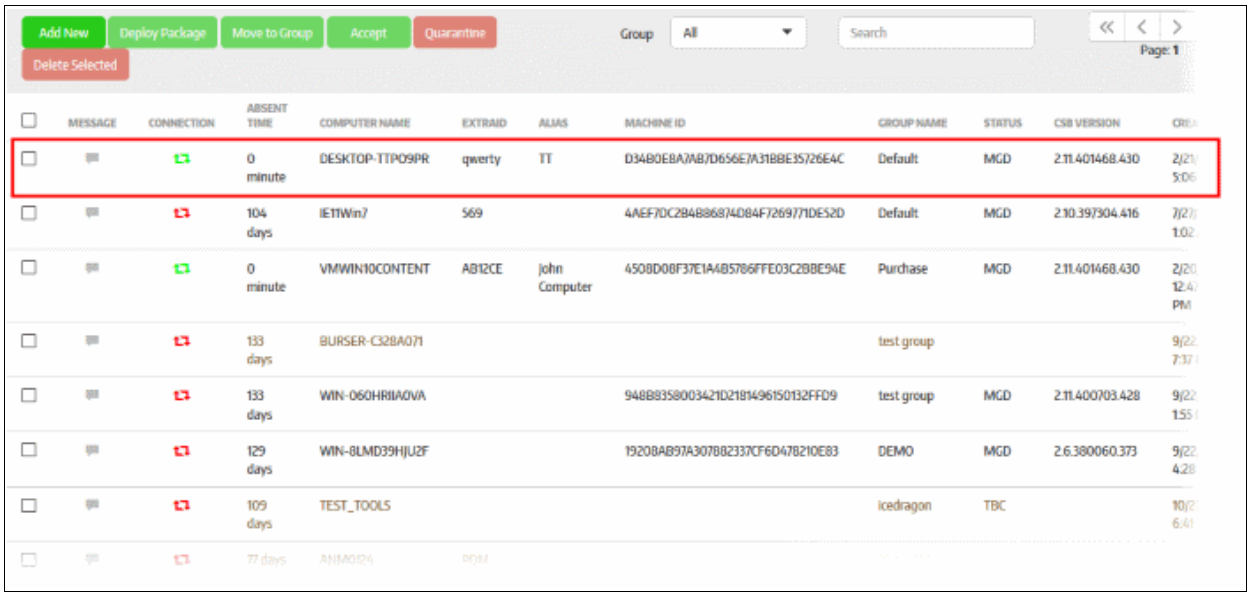
- **Alias Name** (Optional) - Specify an alternative name for the endpoint so you can easily track it in the console.



- **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'

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

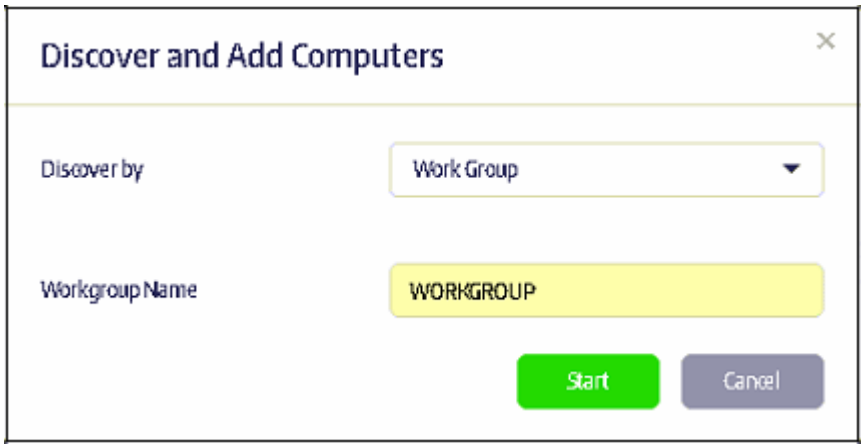


Refer to the sections **Endpoints and Endpoints Groups** and **Policies** to find out how to manage endpoints and deploy polices.

Enrollment via Work Group

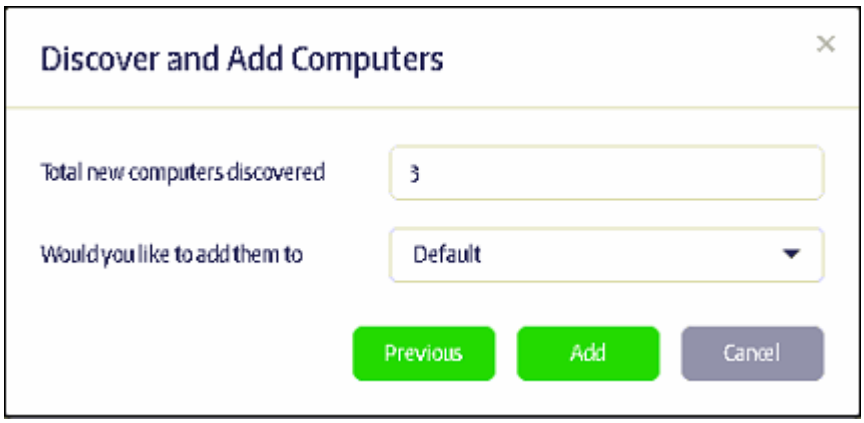
Please note endpoint enrollment via WG will work only if CMC is not added to the domain during premise installation. Refer to the section **Initial Setup** for more details.

- Select the 'Work Group' option from the drop-down



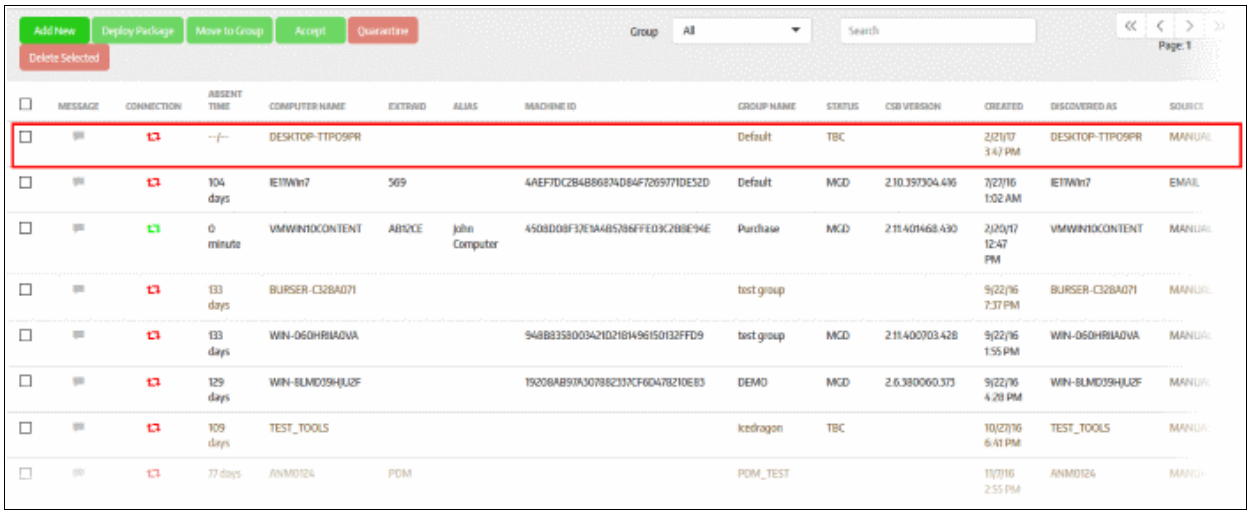
- Enter the Workgroup name and click the 'Start' button

The management console will run a scan to discover endpoints. You then have the option to add discovered endpoints to an endpoint group. Refer to the sections '**Creating a New Endpoint Group**' and '**Assigning Endpoints to Groups**' for more details.

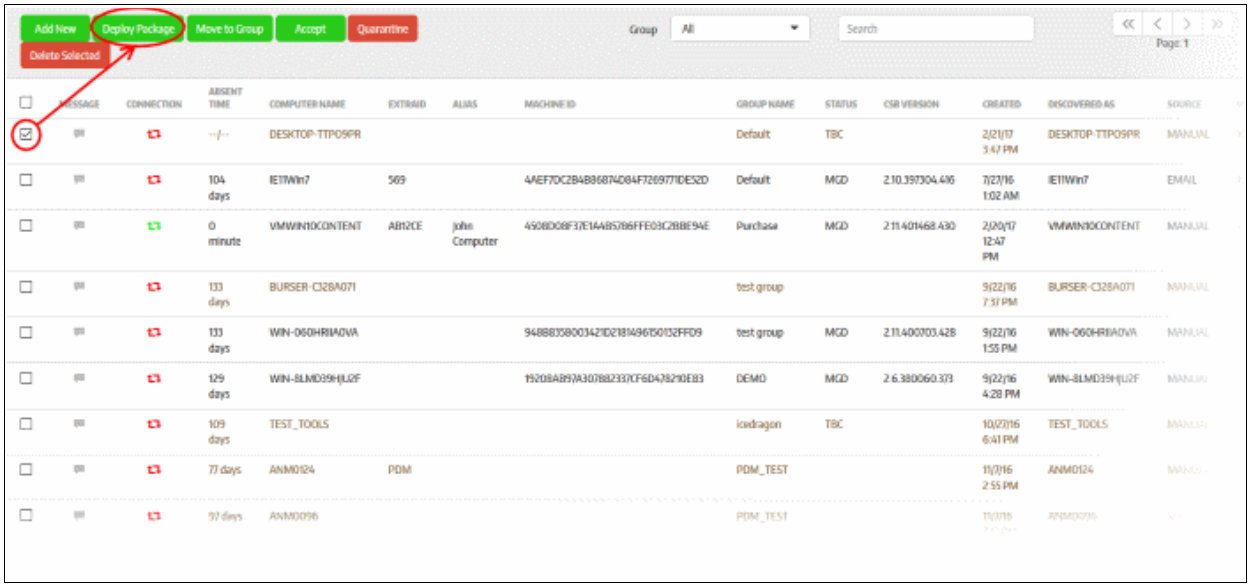


- Select the endpoint group from the 'Would you like to add them to' drop-down and click the 'Add' button.

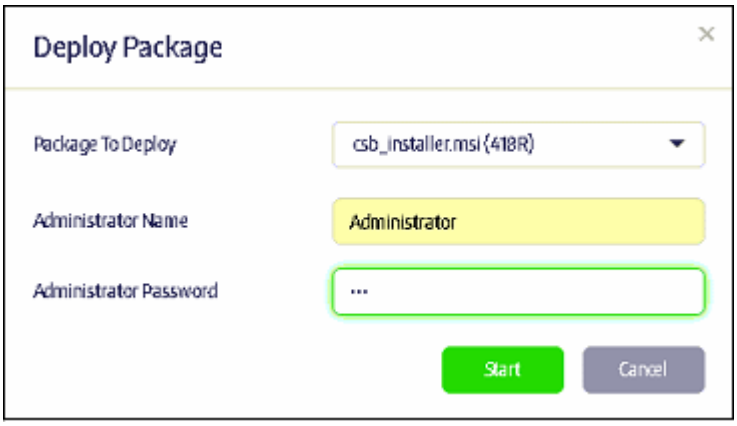
The newly enrolled endpoints will be added to the 'Computers' screen:



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.

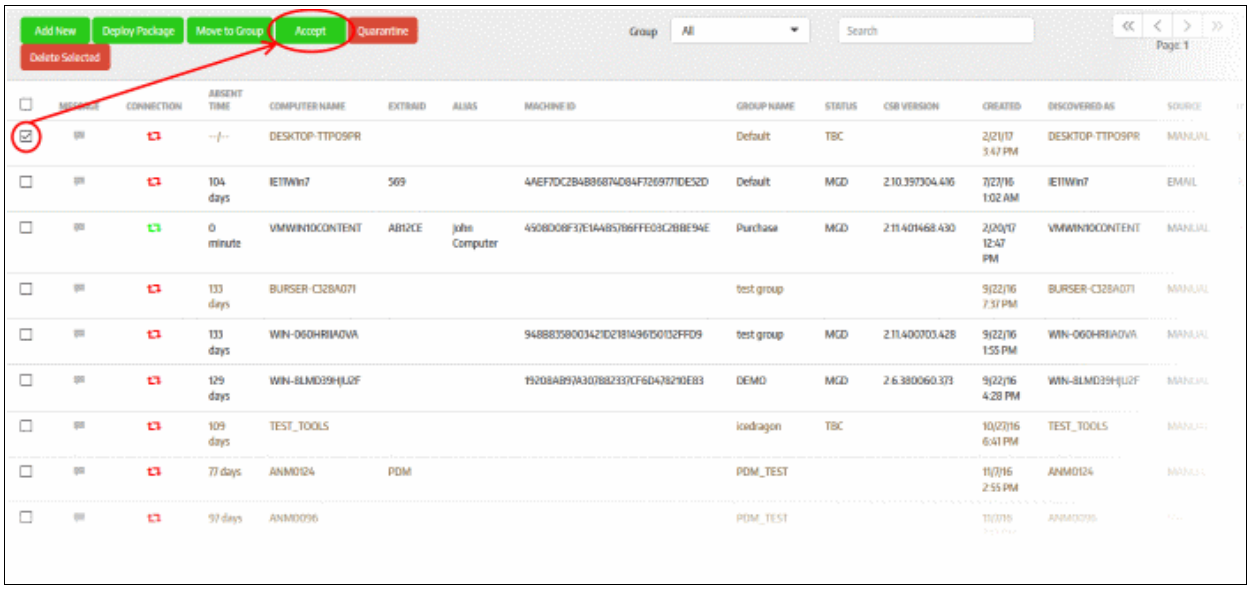


The 'Deploy Package' dialog will be displayed.

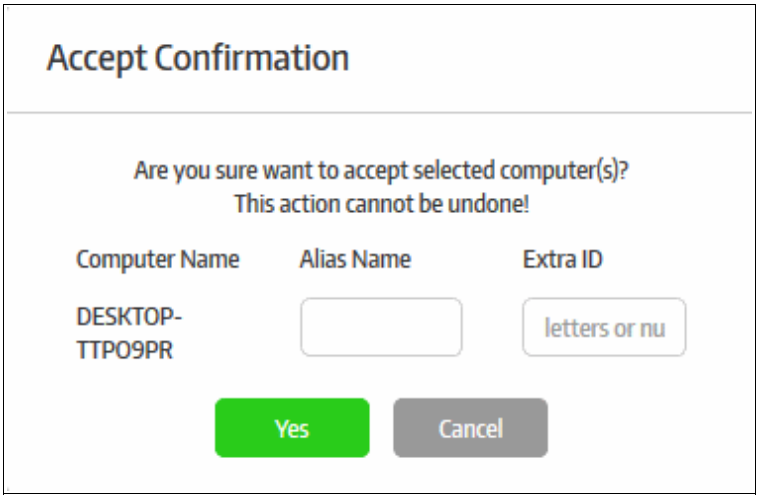


- Select the package to deploy to the selected endpoint(s) from the first field.
- Provide the credentials of the network and click the 'Start' button

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'

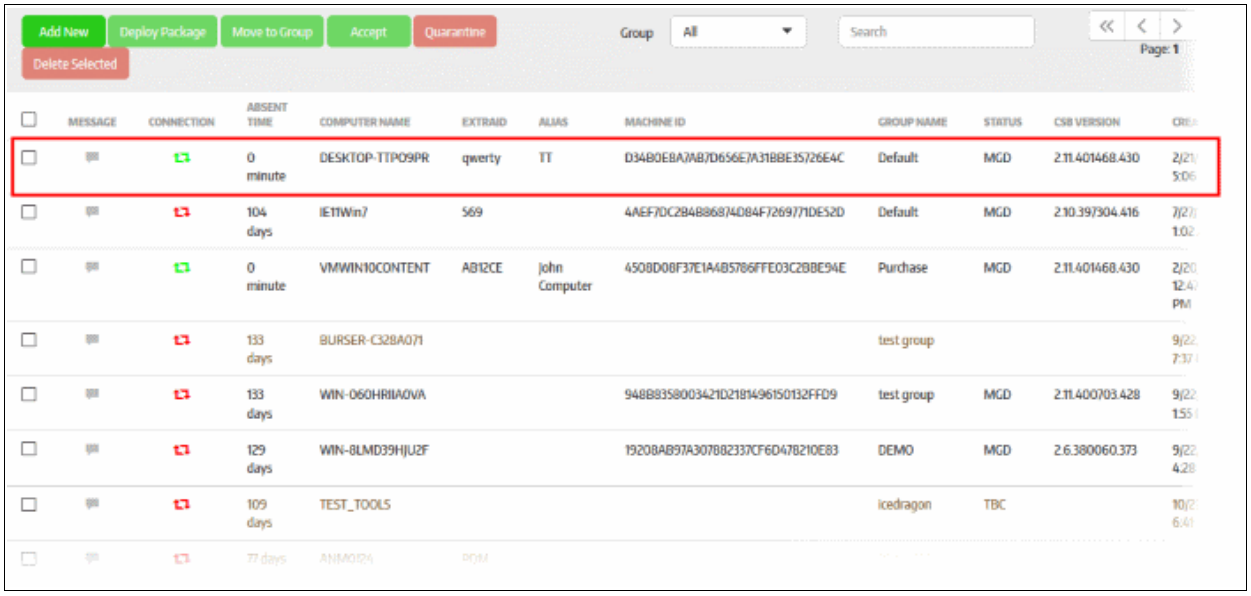


The 'Accept Confirmation' dialog will be displayed.

- **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'

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

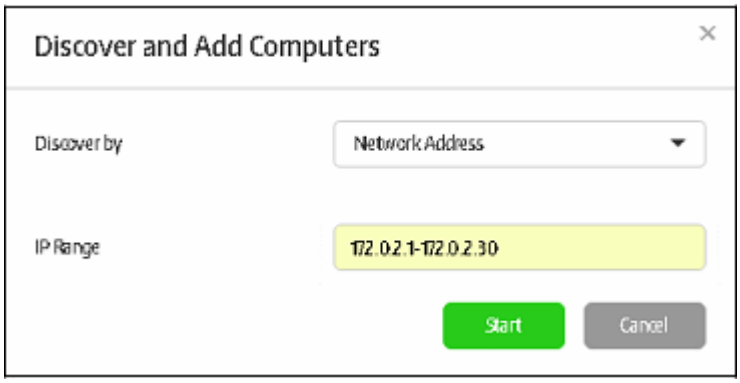


Refer to the sections **Endpoints and Endpoints Groups** and **Policies** to find out how to manage endpoints and deploy polices.

Enrollment via Network Address

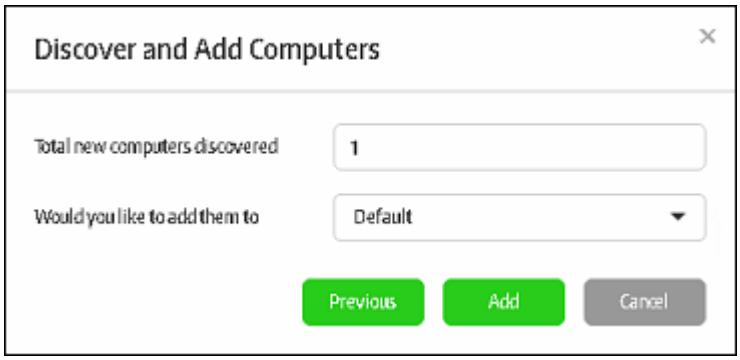
Please note endpoint enrollment via Network Address will work only if CMC is not added to the domain during premise installation. Refer to the section **Initial Setup** for more details.

- Select the 'Network Address' option from the drop-down



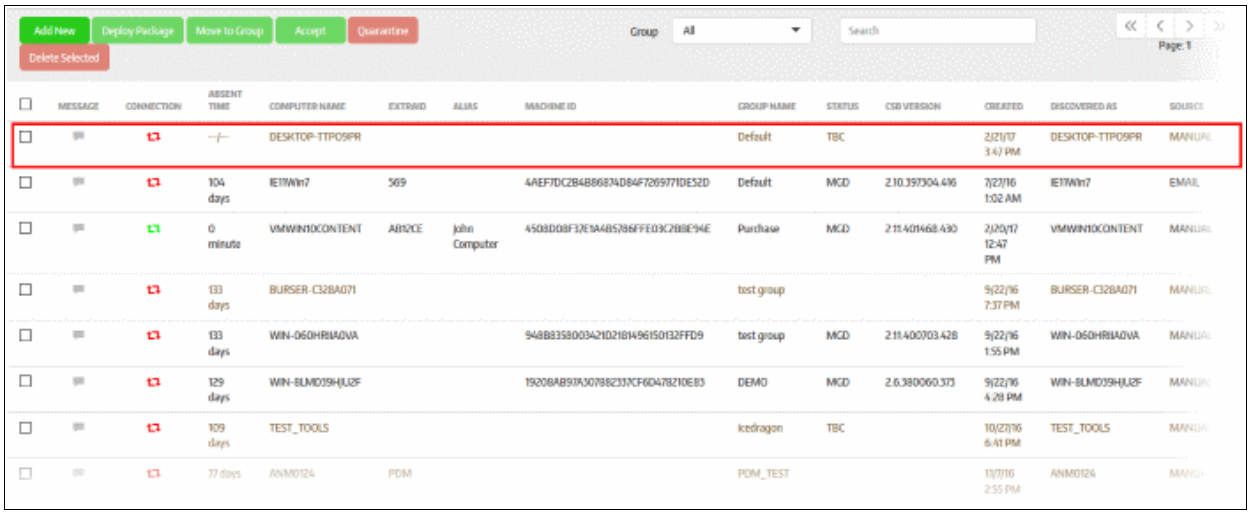
- Enter the IP range and click the 'Start' button

The management console will run a scan to discover endpoints. You will see the number of endpoints discovered and will have the opportunity to add them to an endpoint group. Refer to the sections **'Creating a New Endpoint Group'** and **'Assigning Endpoints to Groups'** for more details.

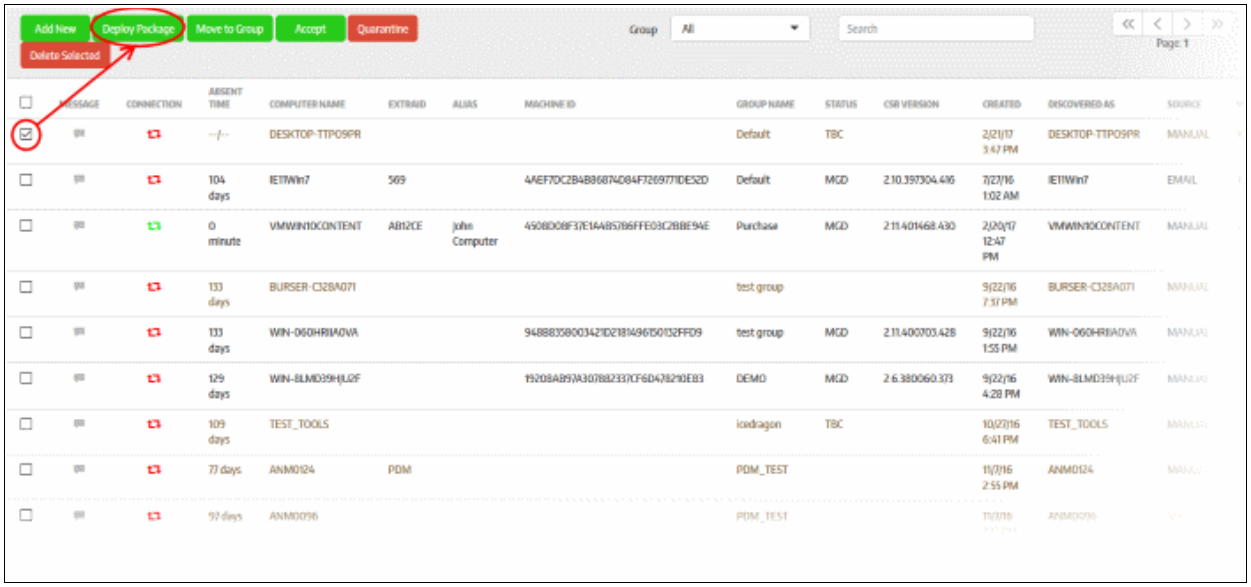


- Select the destination endpoint group from the drop-down and click the 'Add' button.

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



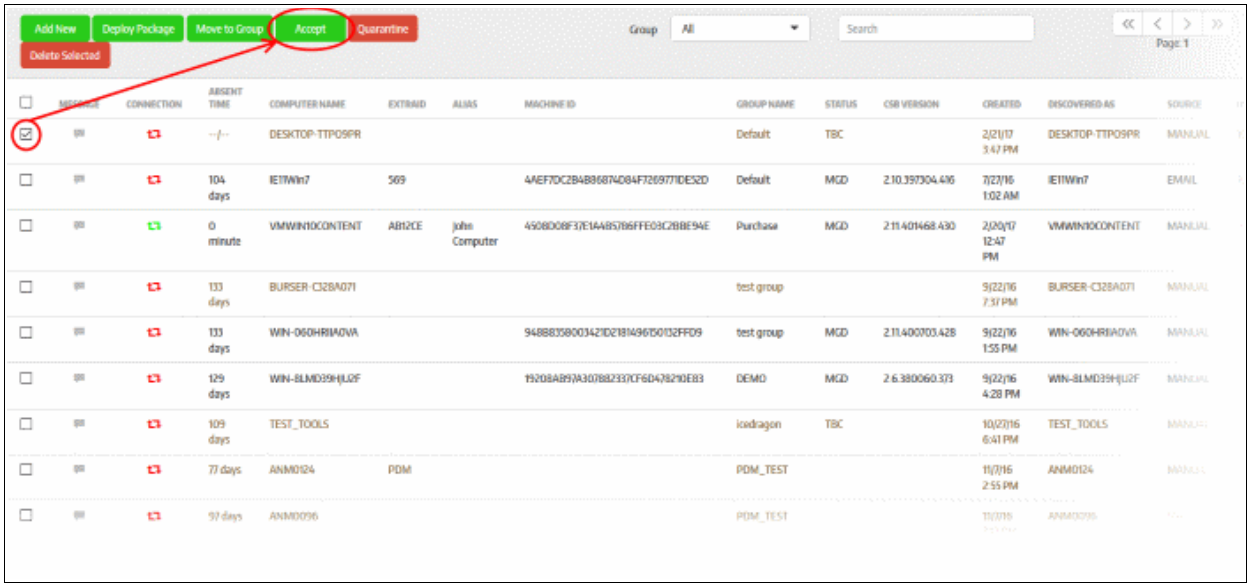
The next step is to deploy the CSB package that should be installed on the endpoints. Installing a package will allow you to assign policies and manage the endpoint.



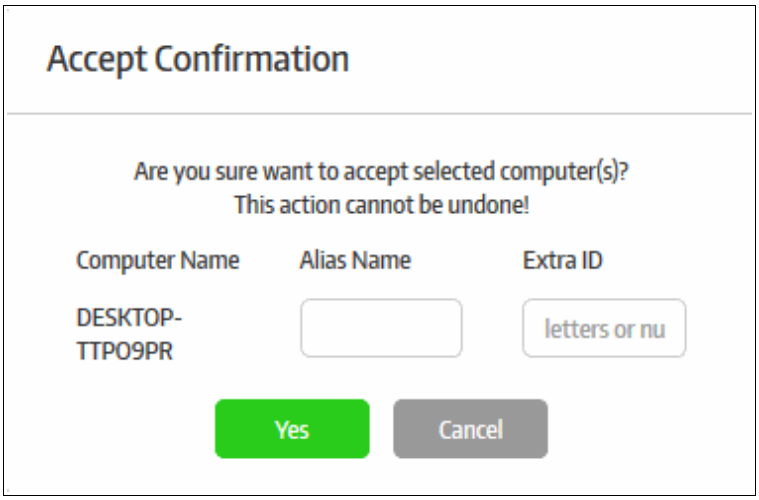
The 'Deploy Package' dialog will be displayed.

- Select the package to deploy to the selected endpoint(s) from the first field.
- Provide the credentials of the network 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'



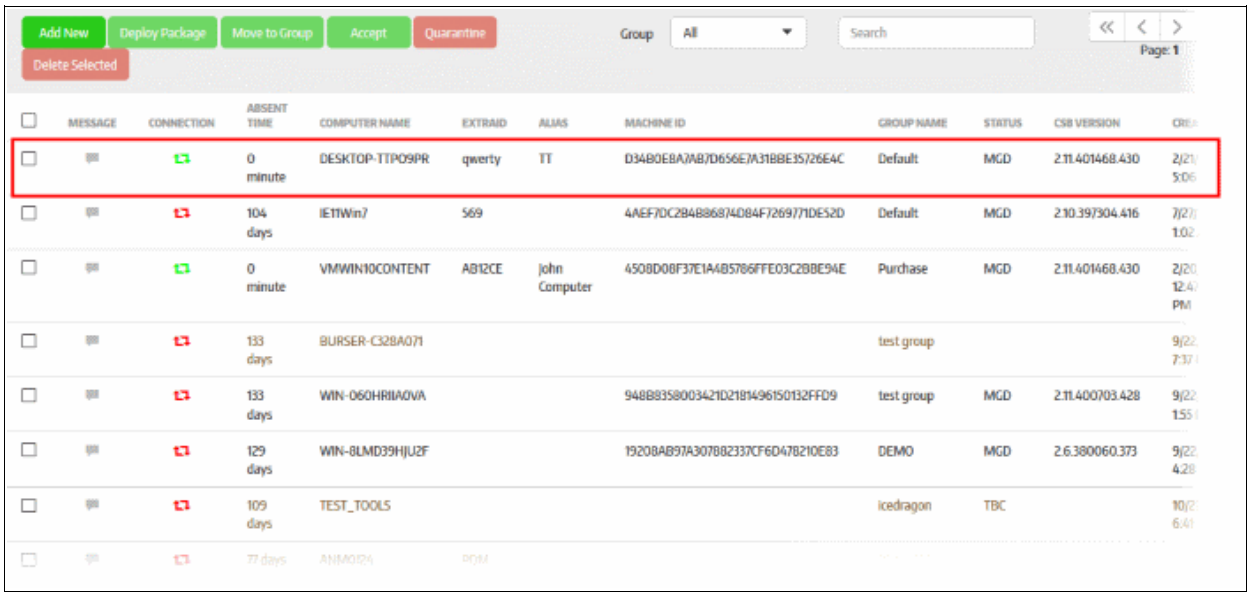
The 'Accept Confirmation' dialog will be displayed.:

- **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'

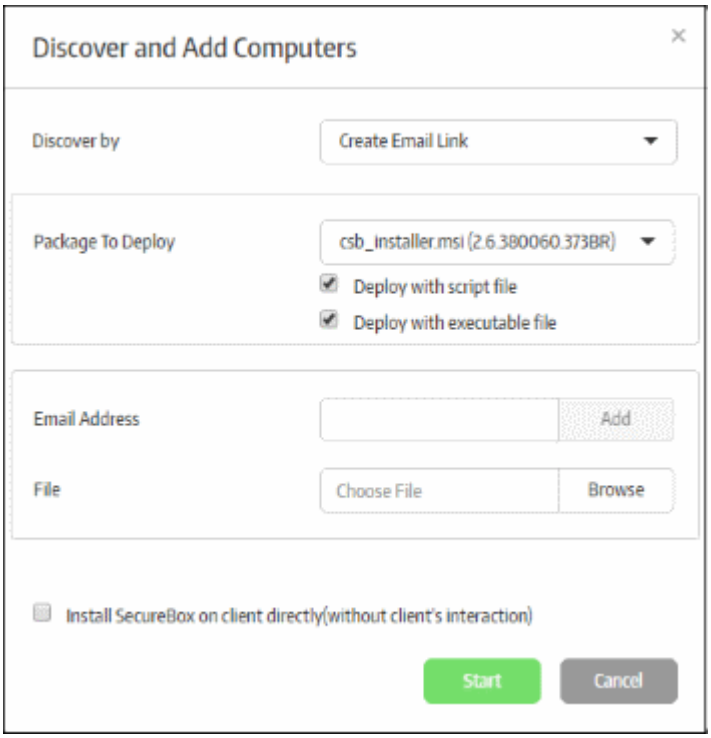
The endpoint will be shown as connected and managed in the 'Computers' screen.

Refer to the sections **Endpoints and Endpoints Groups** and **Policies** to find out how to manage endpoints and deploy polices.



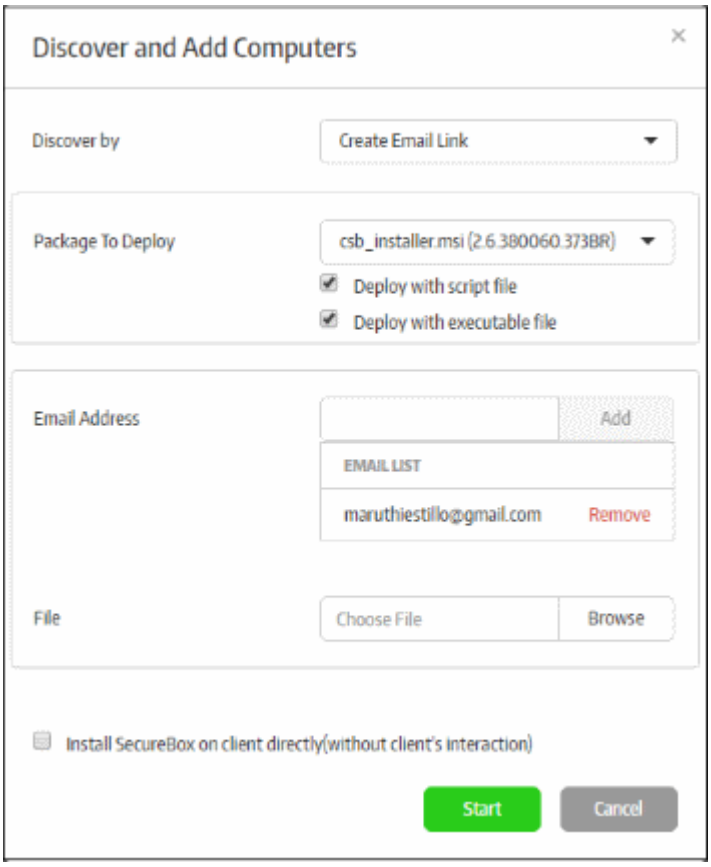
Enrollment via Email Link

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

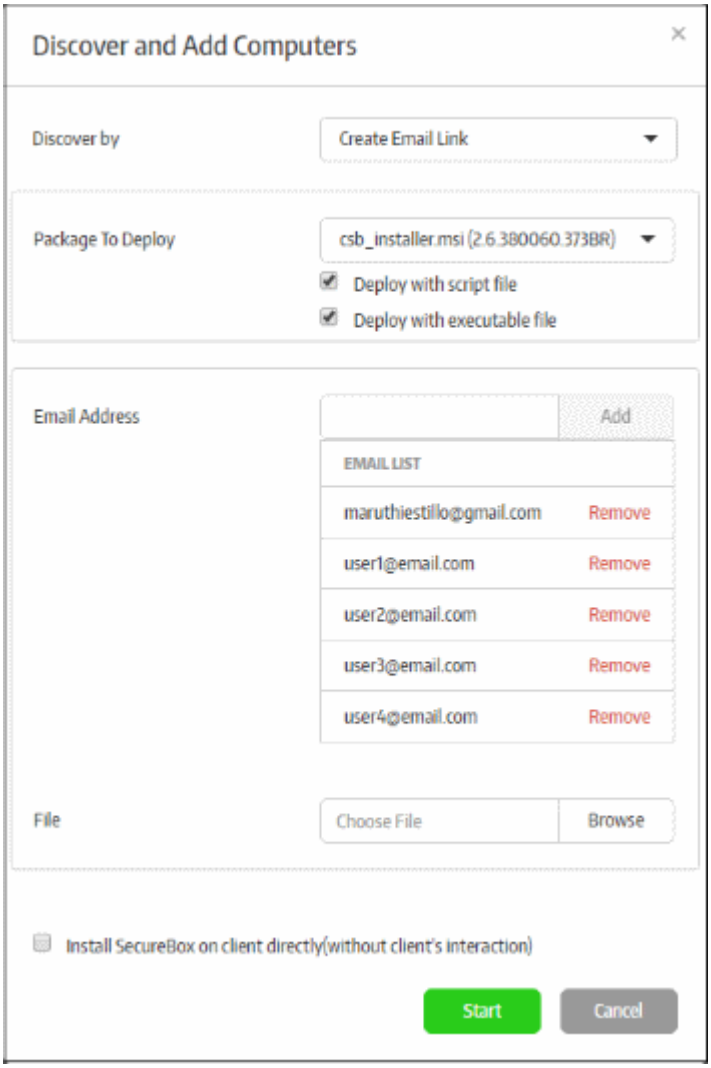


The 'Package to Deploy' drop-down displays all CSB applications uploaded by the administrator.

- 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.

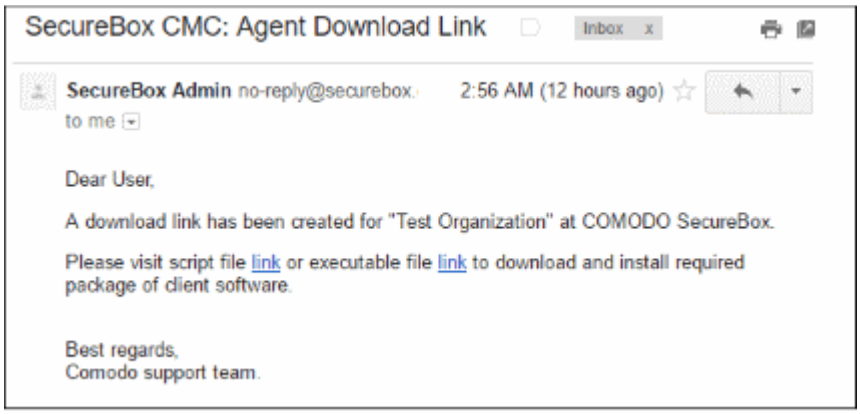


- For bulk enrollment, you can use the 'File' option. Recipient email addresses should be entered on each line of a .txt file. Click 'Browse', navigate to your file and click the 'Open' button. All imported recipients will be listed in the dialog:

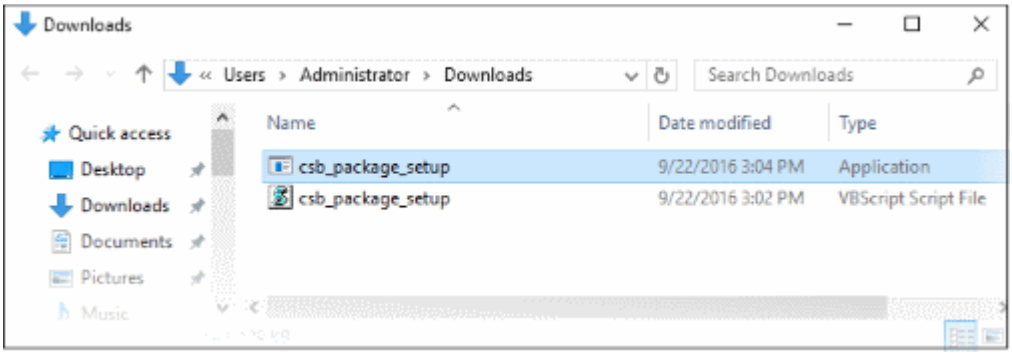


- To remove a recipient, click the 'Remove' link.
- 'Install Secure Box on client directly (without client's interaction)' - If selected, the endpoint user will only see the installation progress bar. They will not be shown the EULA or the configuration page.
- Click the 'Start' button

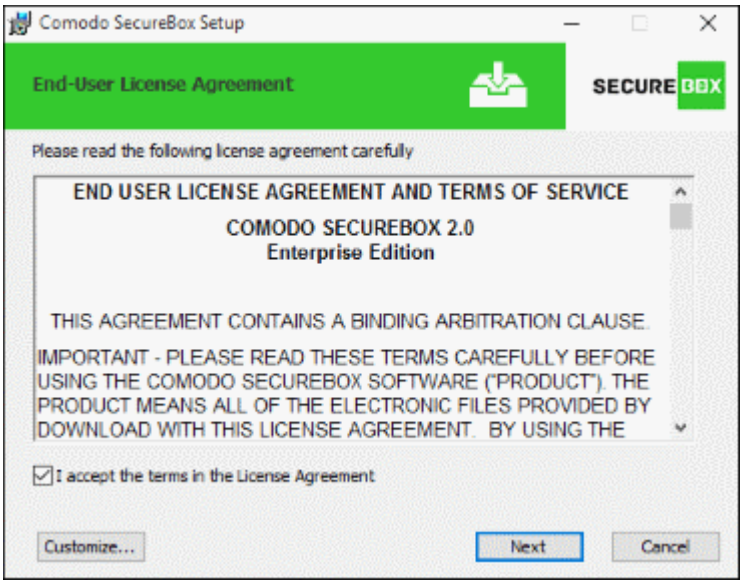
The endpoint user(s) will receive an email from Comodo containing the CSB app download link(s).



The user should click any of the links to download the CSB installer package and save it on the endpoint.



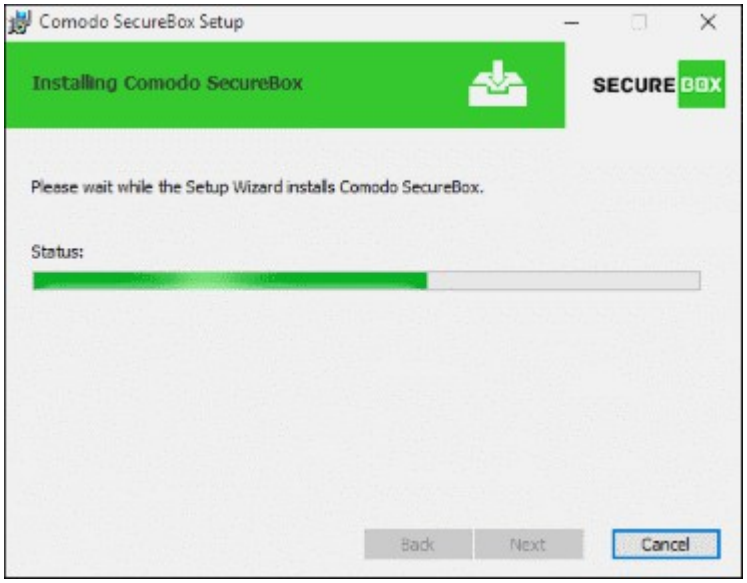
- Double-clicking on any package will start the installation on the endpoint:



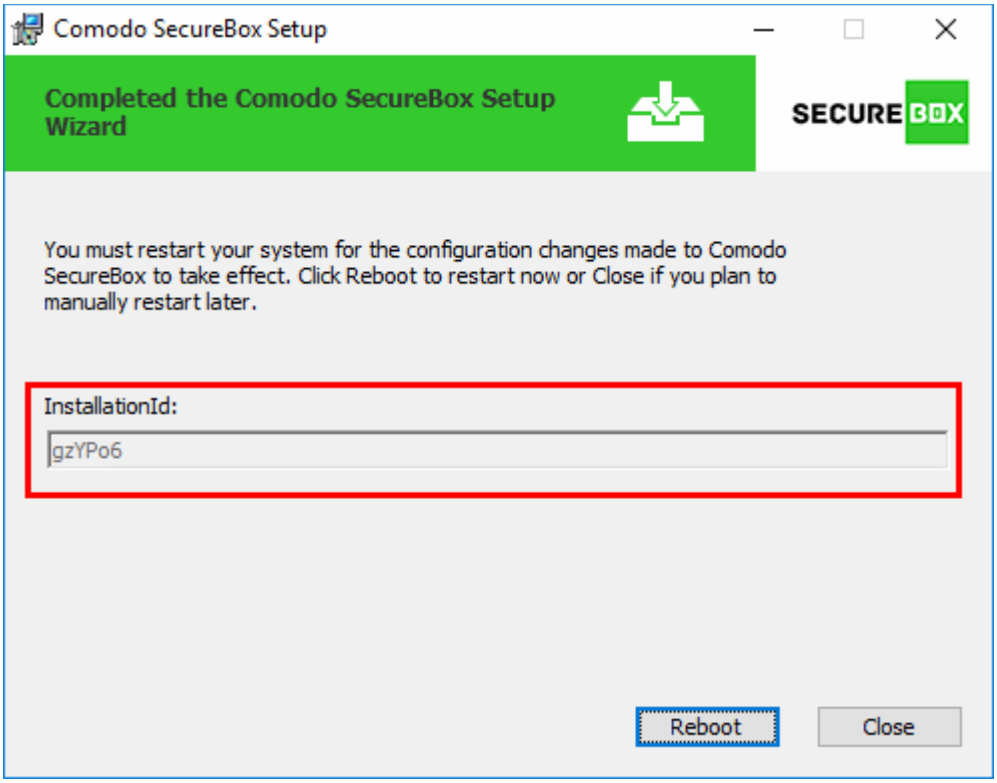
- Click the 'Customize' button to change CSB installation path. The default installation path is C:\Program Files (x86)\COMODO\Comodo SecureBox.

- The CMC server address and CMC customer ID are auto-populated and are required to apply policies configured in the management console. Administrators should complete the 'LDAP' and 'External IP address' fields if you have an 'on-premise' CMC installation.
- Next, read and agree to the license agreement then click the 'Next' button.

The installation will begin:

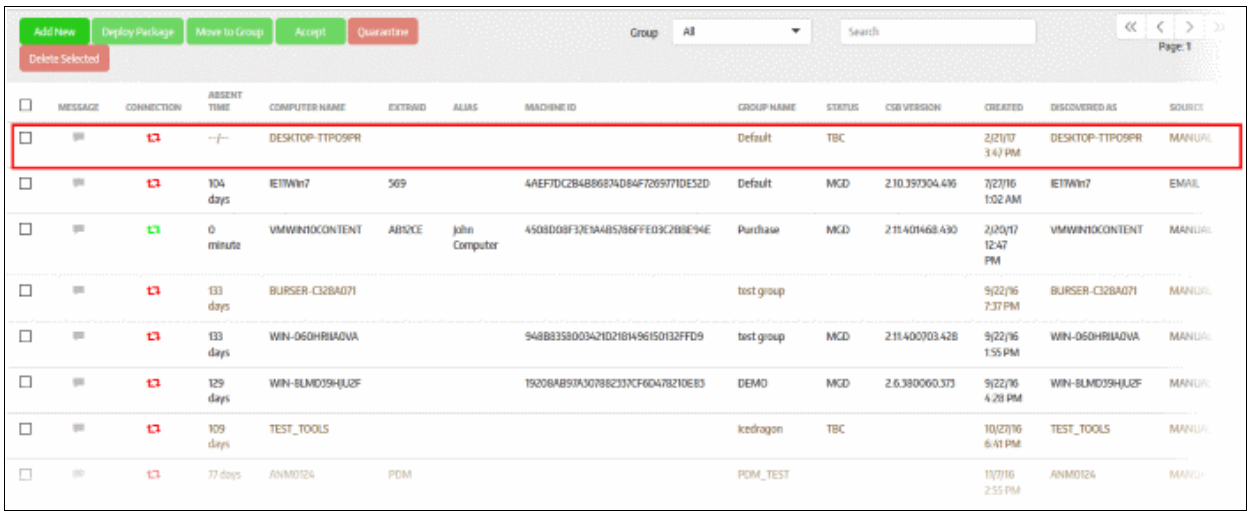


After setup is complete, an installation ID will be generated. End users can communicate the installation ID to administrators to identify their endpoint should the need arise.

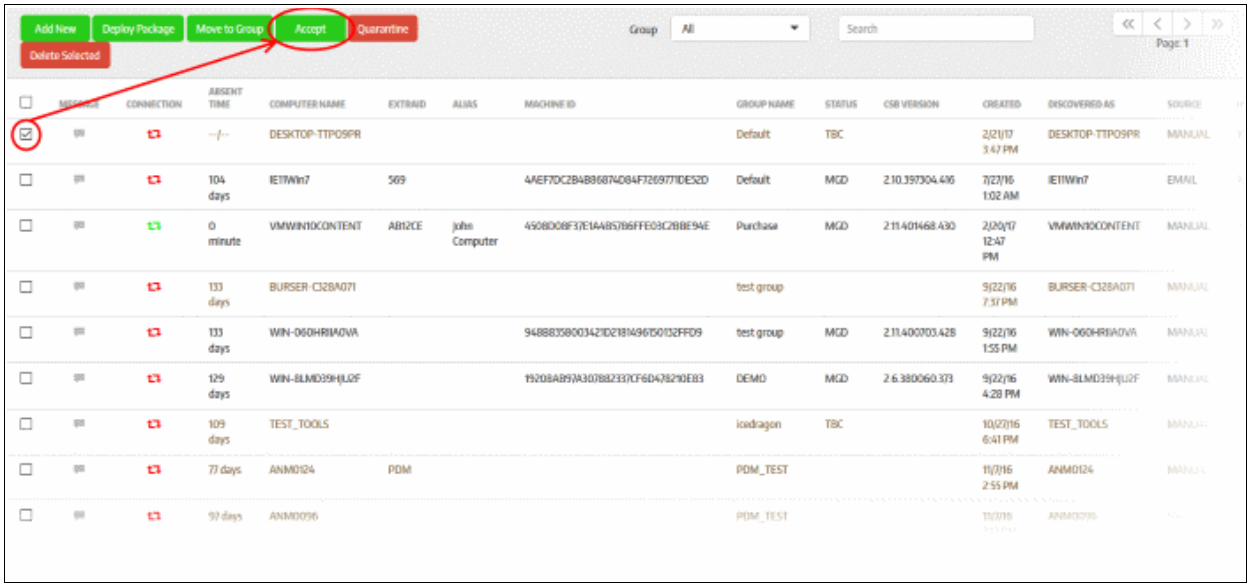


The endpoint needs to be restarted to complete the installation. After rebooting, the endpoint will appear on the 'Computers' screen as 'MGD TBC' - meaning it needs to be approved by an administrator. The installation ID generated at the endpoint will be displayed in the 'Status' column of the 'Computers' interface.

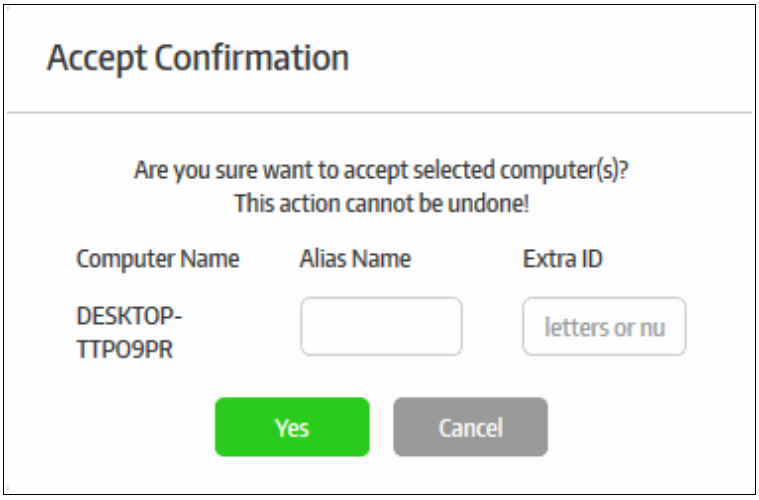
If the 'Auto accept' option was enabled while adding the organization, then enrolled endpoints will be automatically accepted. Refer to the section '**Adding a New Organization**' for more details.



- Select the endpoint and click 'Accept'



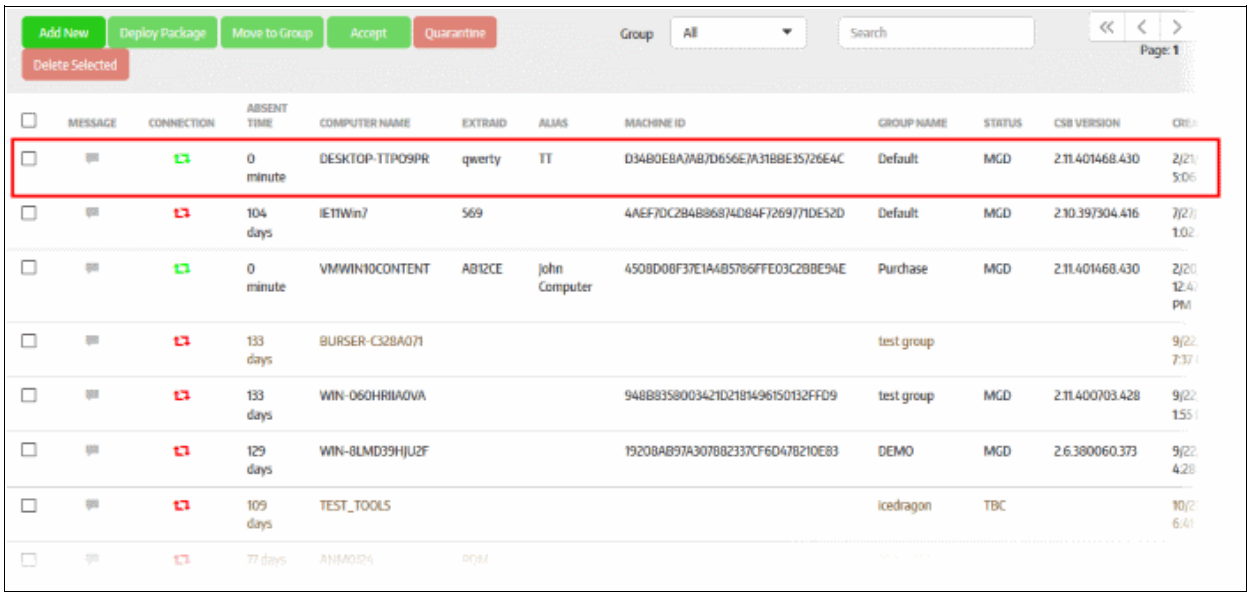
The 'Accept Confirmation' dialog will be displayed.



- **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'

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.

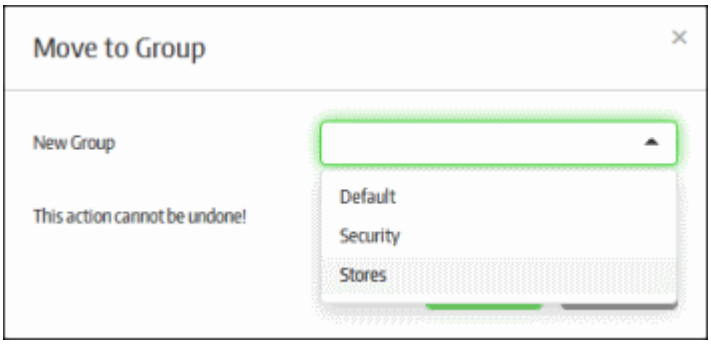
6.1.2. Assign Endpoints to Groups

Computer groups are created in order to assign policies and schedule a quarantine period for endpoints in the group. The endpoints in the 'Computers' screen can be moved to a desired group according to the organizational requirement. When a new endpoint is enrolled in to the management console, they are automatically placed under the 'Default' group and applied the policy in the group. Refer to the section '**Managing Endpoint Groups**' for more details about creating and managing endpoint groups.

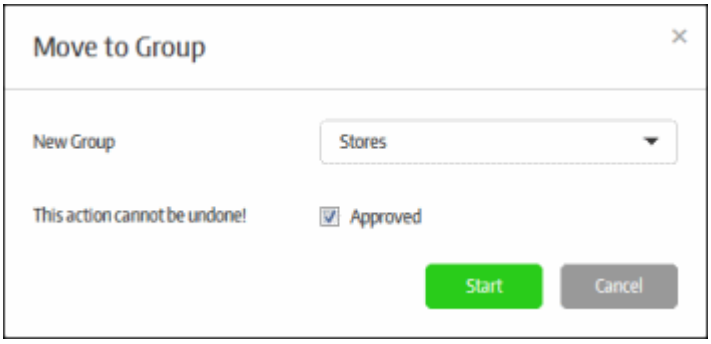
To move an endpoint to a group, select it and click the 'Move to Group' button in the 'Computers' interface

The 'Move to Group' dialog will be displayed:

The 'New Group' drop-down displays the 'Computer Groups' that are added from the 'Groups' section. Refer to the '**Managing Endpoint Groups**' for more details.

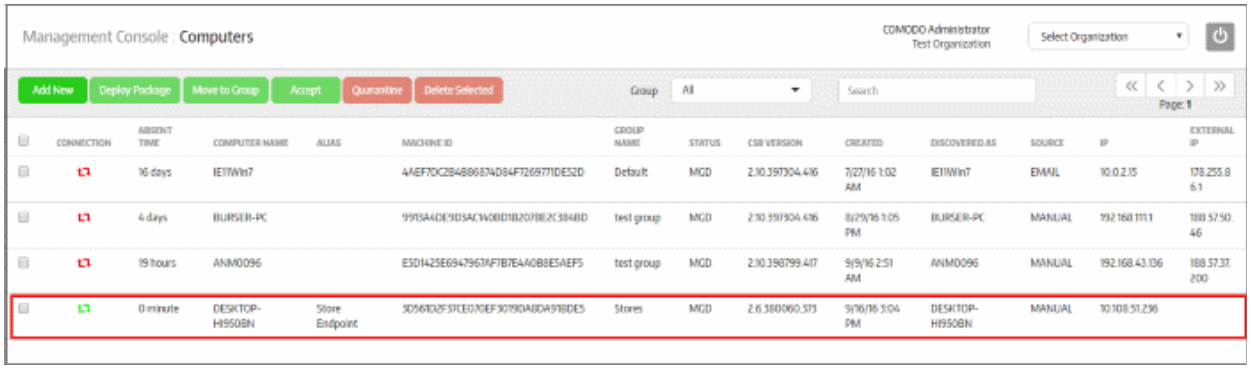


- Select the group the from the drop-down
- Select the 'Approved' check box



- Click the 'Start' button

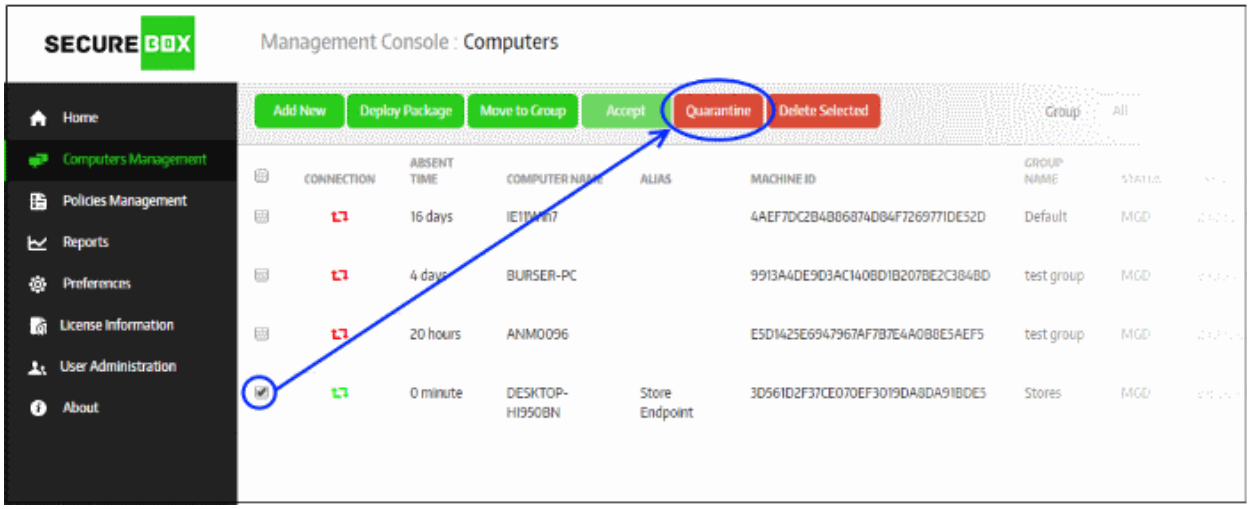
The selected endpoint will be moved to the group and its policy will be automatically be applied to it. Refer to the section '**Policies**' for more details about polices.



6.1.3. Quarantine Endpoints

Quarantining an endpoint blocks the secured items on the endpoint from starting. The 'Computers' screen allows administrators with appropriate privileges to quarantine specific endpoints in a group. The quarantine settings also can be configured for an endpoint group that will apply to all the endpoints in the group. Refer to the '**Managing Endpoint Groups**' for more details. The 'Quarantine' button toggles the quarantine setting meaning the same button is used for quarantining endpoints as well as releasing them from quarantine.

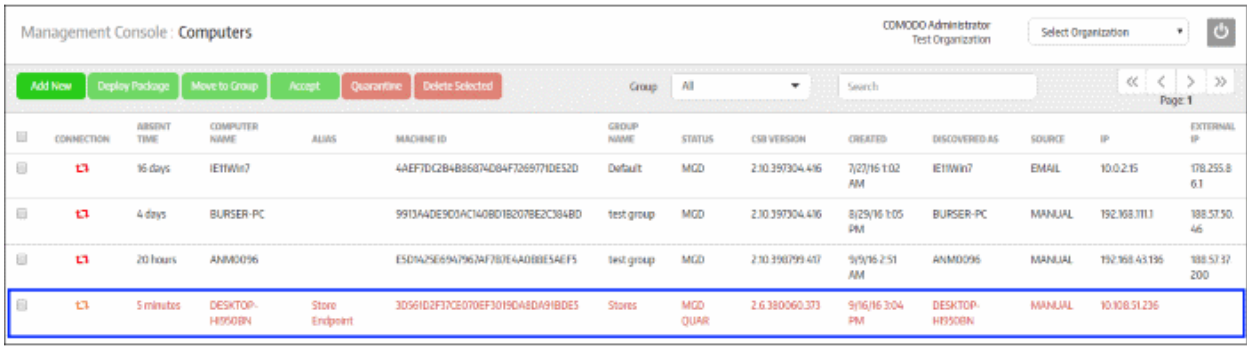
To quarantine an endpoint, select it and click the 'Quarantine' button in the 'Computers' interface.



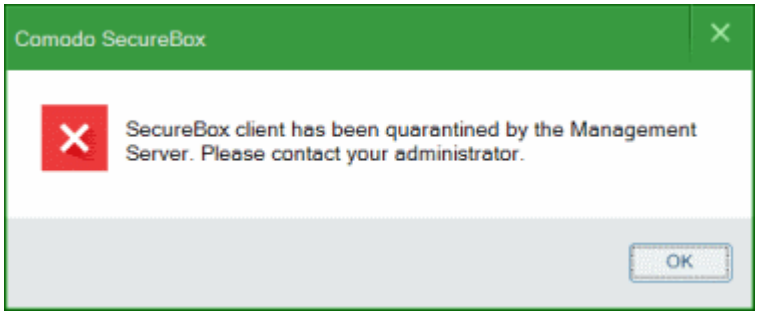
A confirmation dialog will be displayed.

- Click 'Yes' to confirm blocking the secure apps from starting on the selected endpoint(s)

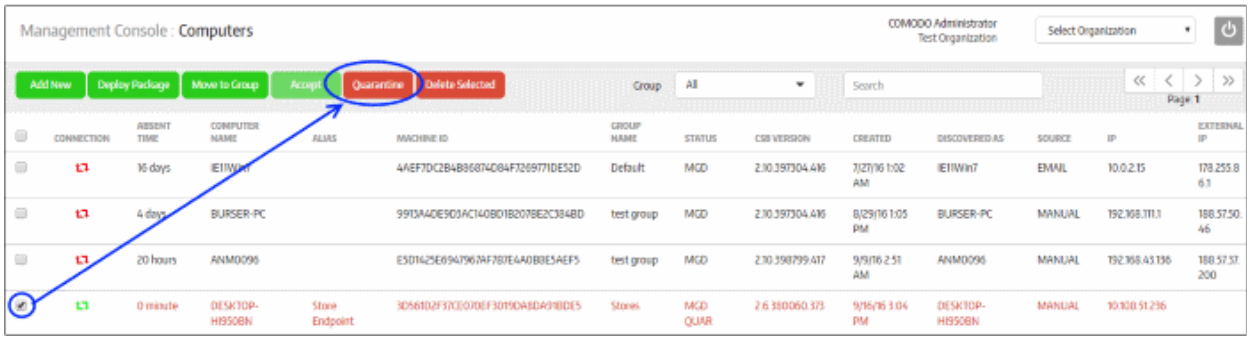
The status of the endpoint will display as 'MGD QUAR' meaning it is managed but quarantined.



When an end user opens a secured app on an quarantined endpoint, the following message will be displayed:



To release the endpoints from quarantine, select it from the list and click the 'Quarantine' button



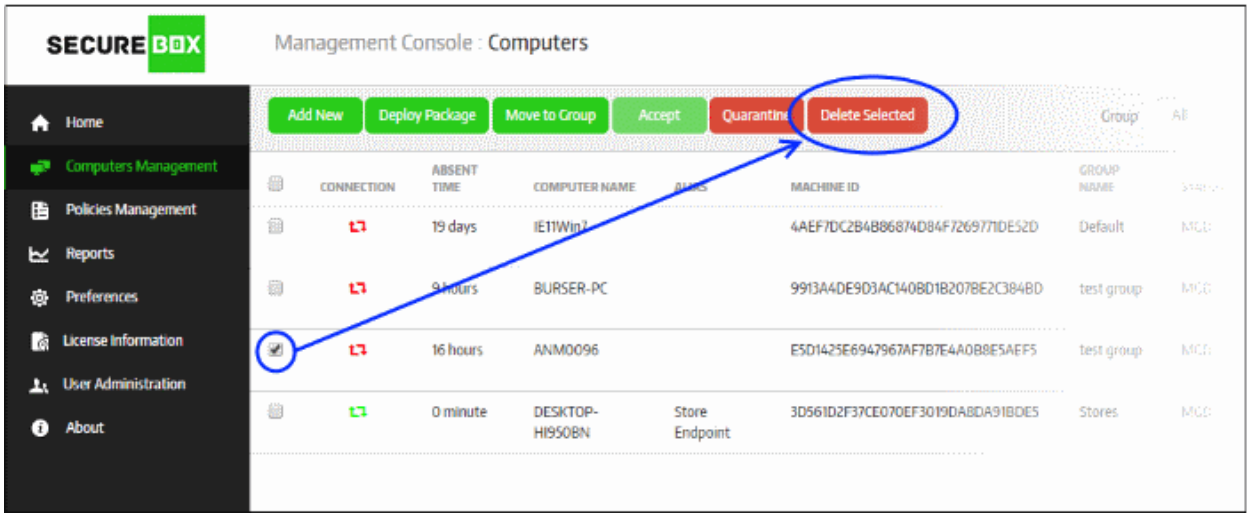
- Click 'Yes' in the confirmation dialog

The quarantine will be released and the user can start the secured apps on the endpoint.

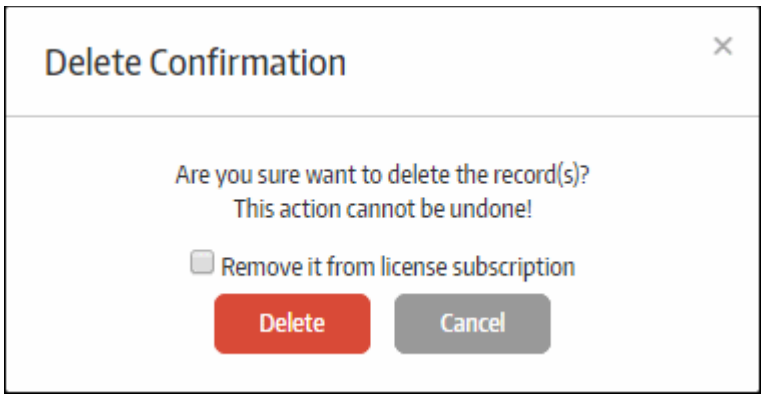
6.1.4. Delete Endpoints

The Secure Box Central Management Console allows administrators to remove enrolled endpoints from the list if required. Once removed from the CMC, the secured apps on the endpoints will also be removed from them.

To remove an endpoint, select it and click the 'Delete Selected' button in the 'Computers' interface



A confirmation dialog will be displayed.



- Remove it from license subscription - If this option is not selected, then the endpoint record will be removed from the list but the machine ID will remain stored in CMC server and the number of 'Used' endpoints in license will not reduce. These endpoints can be added again to CMC for management. If the option is selected, the number of endpoints that are used from the license will be reduced. For example, if you have subscribed for 1000 endpoints and used 600 and if this option is selected the number of used endpoints in the license will display 599. The endpoint details will remain in the list but will be displayed with a strike through. You cannot add this endpoint again with the same license since its machine ID will be disabled in CAM server and you have to enable it again to add it. Please contact your Comodo administrator if you need more help regarding this.
- Click 'Delete' to confirm the removal of the endpoint

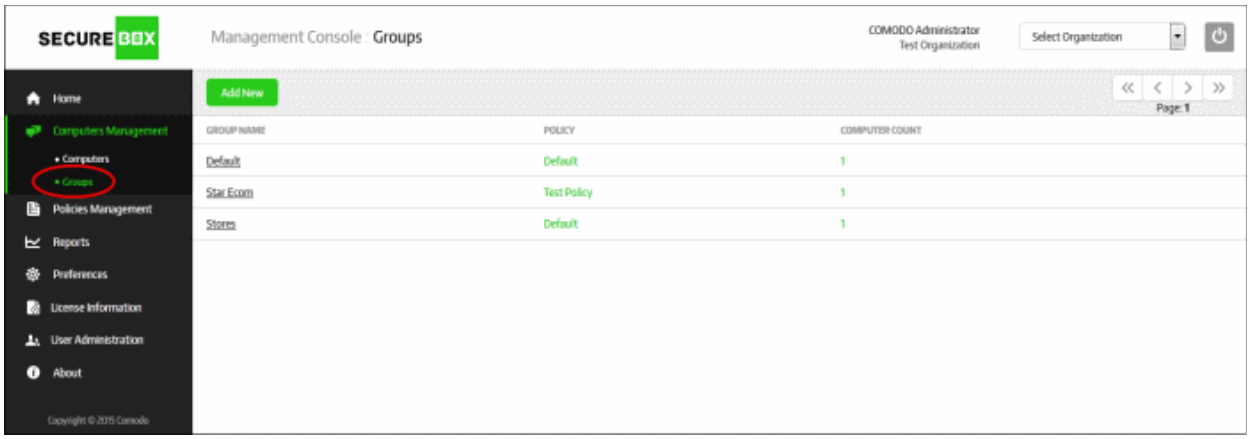
6.2. Manage Endpoint Groups

All enrolled endpoints must be placed in an endpoint group. After creating an endpoint group you can apply security policies to them and schedule quarantine periods according to your requirements. All newly enrolled endpoints are placed in the default group. You can move them to different groups at any time. Refer to '**Assigning Endpoints to Groups**' if you need help with this.

The policy to be applied to a group is selected while creating the group. You can change the policy at any time by editing the group. Only one policy can be applied to a group at a time.

The 'default' group also can be edited so it applies a policy to newly enrolled endpoints.

To manage endpoint groups, click 'Computers Management' on the left and then 'Groups' below it:



Computer Groups - Table of Column Description	
Column	**Description**
Group Name	The name of the endpoint group provided\edited while creating\editing it. Clicking on a name will display the 'Group Properties' screen. Refer to the section '**Creating a New Endpoint Group**' and '**Editing Endpoint Groups**' for more details.
Policy	The name of the policy assigned to the endpoint group. A 'Default' policy will be assigned to the default endpoint group. Clicking on a policy name will open the 'Policy Management' interface. Refer to the section '**Polices**' for more details about managing policies.
Computer Count	The number of endpoints that are assigned to the group. Refer to the section '**Assigning Endpoints to Groups**' for more details. Clicking on a number will open the 'Computers' interface with list of computers in that group. Refer to the section '**Managing Endpoints**' for more details.

Sorting option

Sorting the entries

Clicking on the 'Group Name' column heading sorts the entries based on the ascending/descending order of the entries as per the information displayed in the column.

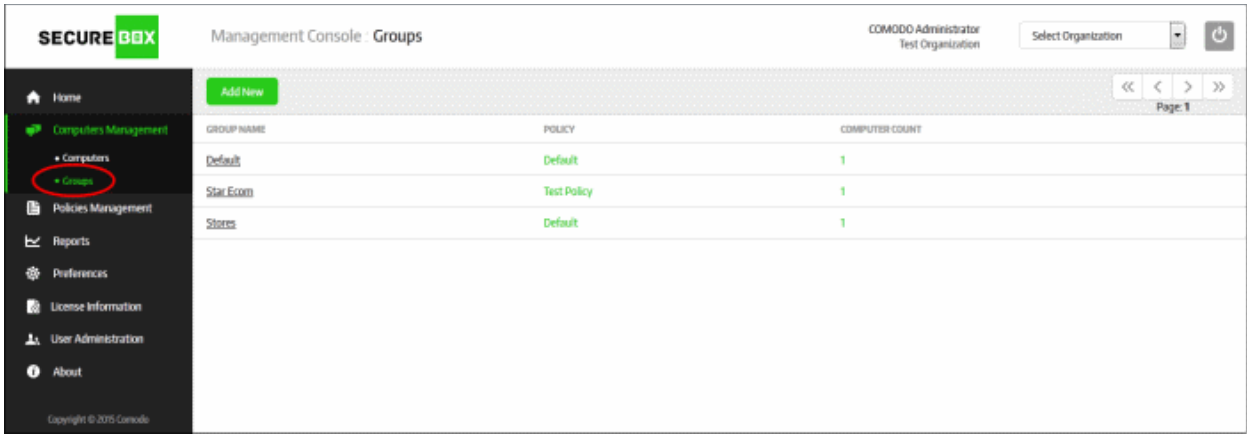
The interface allows an administrator with appropriate privileges to:

- **Create a new endpoint group**
- **Edit endpoint groups**

6.2.1. Create a New Endpoint Group

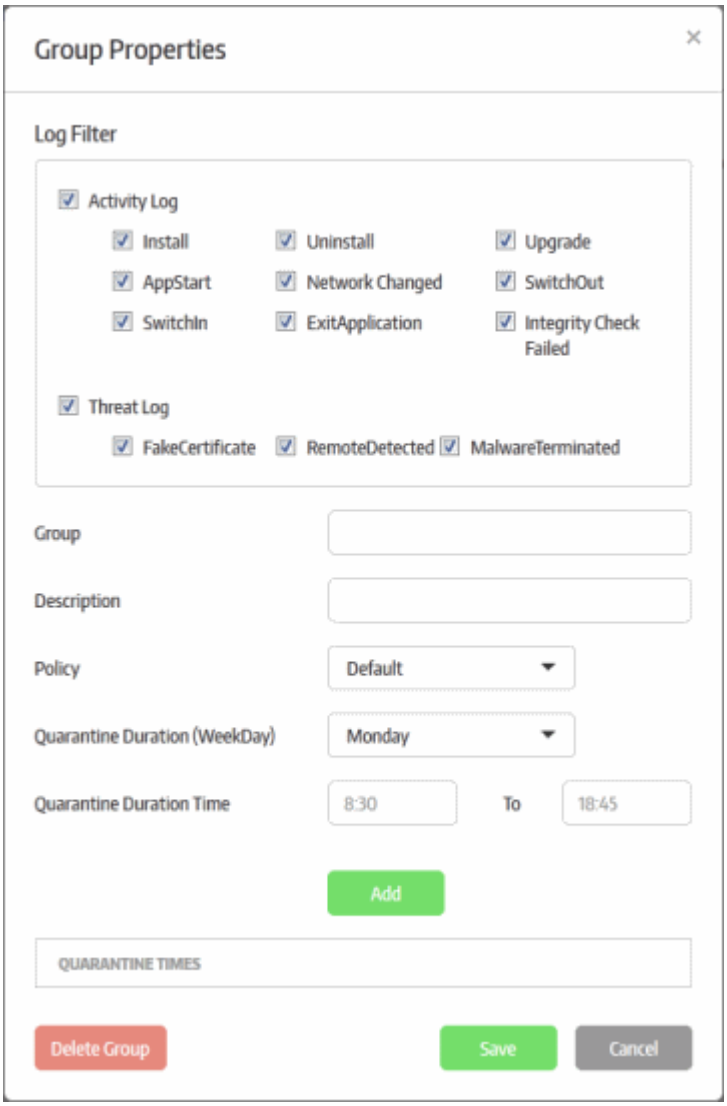
The Secure Box Central Management Console allows administrators with appropriate privileges to create new endpoint groups according to your organization's requirements. The newly enrolled endpoints are automatically placed in the default group and administrators can move them to other groups later on for assigning appropriate policies. Refer to the section '**Assigning Endpoints to Groups**' for more details about moving endpoints to other groups.

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

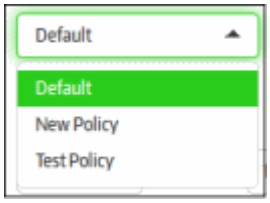


- Click the 'Add New' button

The 'Group Properties' screen will be displayed.



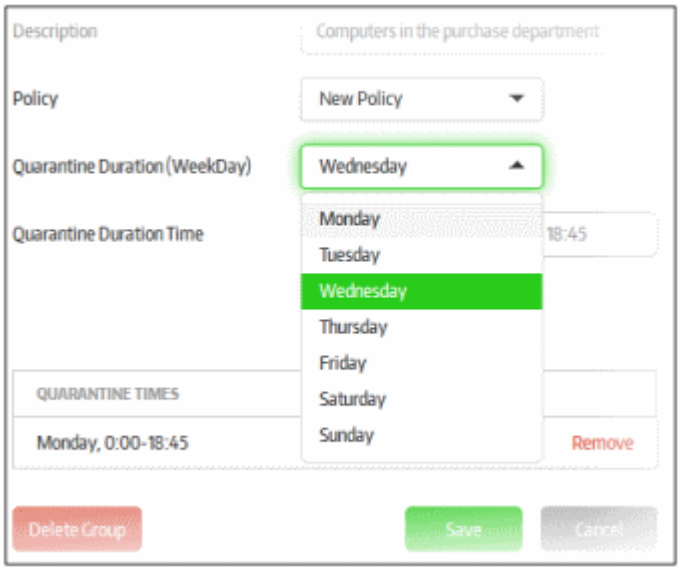
Group Properties - Form Parameters	
Form Element	**Description**
Log Filter	Select which events should be recorded in logs for the group. Log filter selection determines what notifications can be sent and impacts reports. • Notifications - Email notifications for threat category and activity action depends on the items selected. Notifications will be sent only for the selected items here. Refer to **Threat Notifications** and **Activity Notifications** in the section **Configuring the Management Console** for more details. • Reports - The logs for the selected events will be received by the management console and saved into database. Reports can be generated for different time periods and the data will be fetched from the database. Report

	data will be empty if a threat category / activity action was disabled for the selected report generation period. Refer to the sections **Threat Report** and **Activity Report** for more details.
Group	Enter the name of the endpoint group
Description	Enter an appropriate description for the group
Policy	Select the policy to be applied to the endpoints in the from the drop-down.  The policies available from drop-down are configured from the 'Policies Management' section. Refer to the section **Policies** for more details about creating and managing policies.
Quarantine Duration (Week Day)	Allows you to select the week day the quarantine for the endpoint group should be applied. Refer to '**To schedule quarantine period for the endpoint group**' for more details.
Quarantine Duration Time	Allows you to 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.

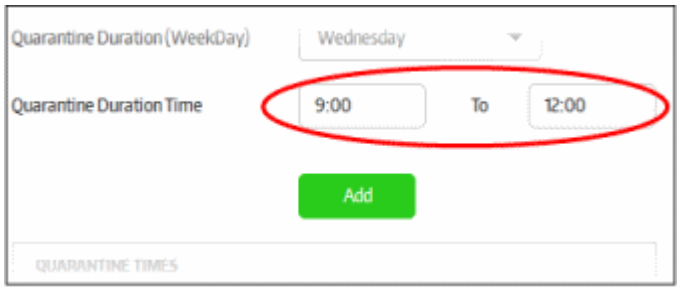
To schedule quarantine period for the endpoint group

Quarantining blocks the secured items on the endpoints in the group 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

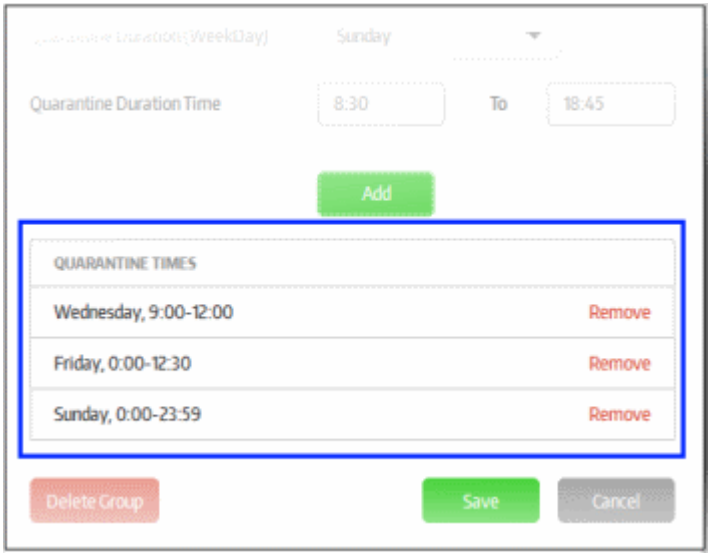


- Enter the quarantine time duration time the selected quarantine day in the 'Quarantine Duration Time' fields



- Click the 'Add' button below

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



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.

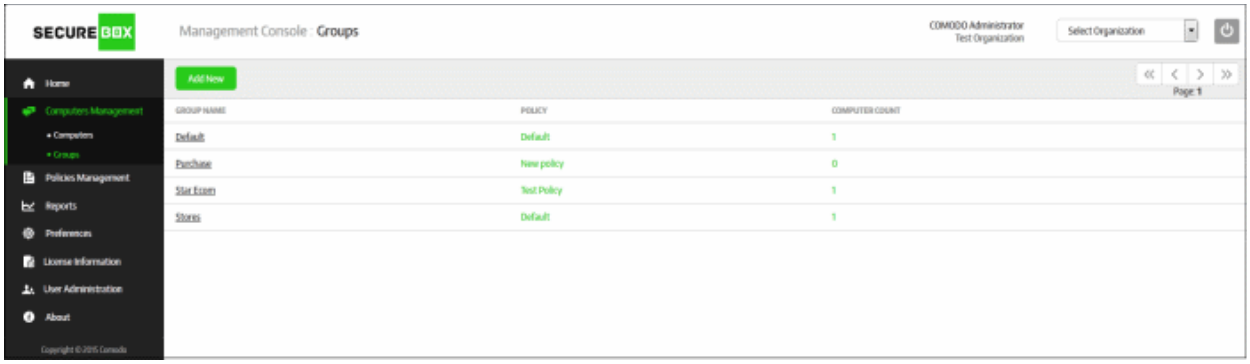
The added endpoint group will now be available for adding endpoints into it. Refer to the section '**Assigning Endpoints to Groups**' for more details.

6.2.2. Edit Endpoint Groups

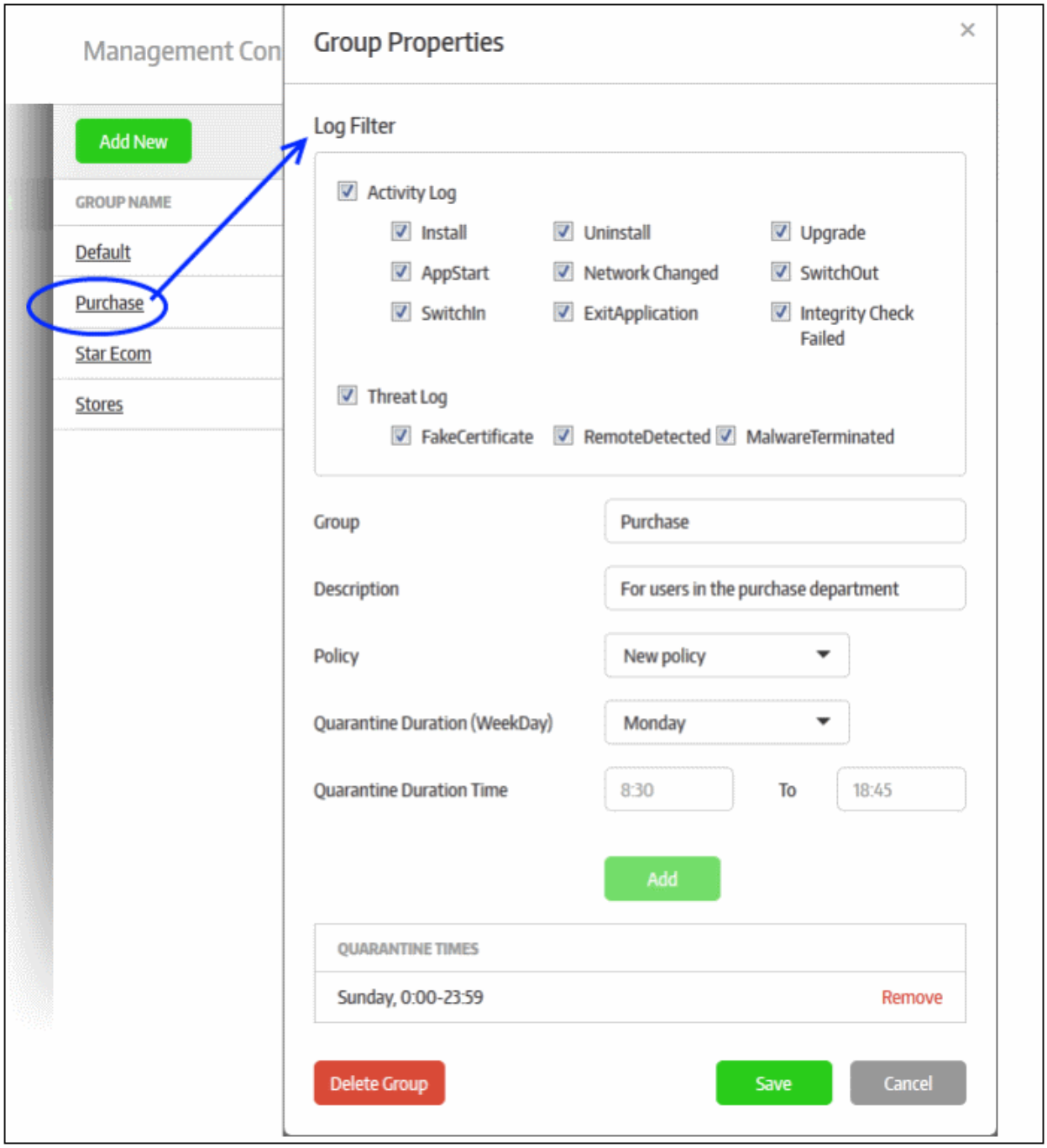
The Central Management Console allows administrators with appropriate privileges to edit or delete endpoint groups. Please note that you cannot delete a group which contains endpoints. To delete an endpoint group, you have to first move the endpoints to another group or delete them from the list. You can only delete a group that has

no endpoints in it.

To edit an endpoint group, click 'Computers Management' on the left and then 'Groups' below it:



- Click on the name of the endpoint group that you want to edit



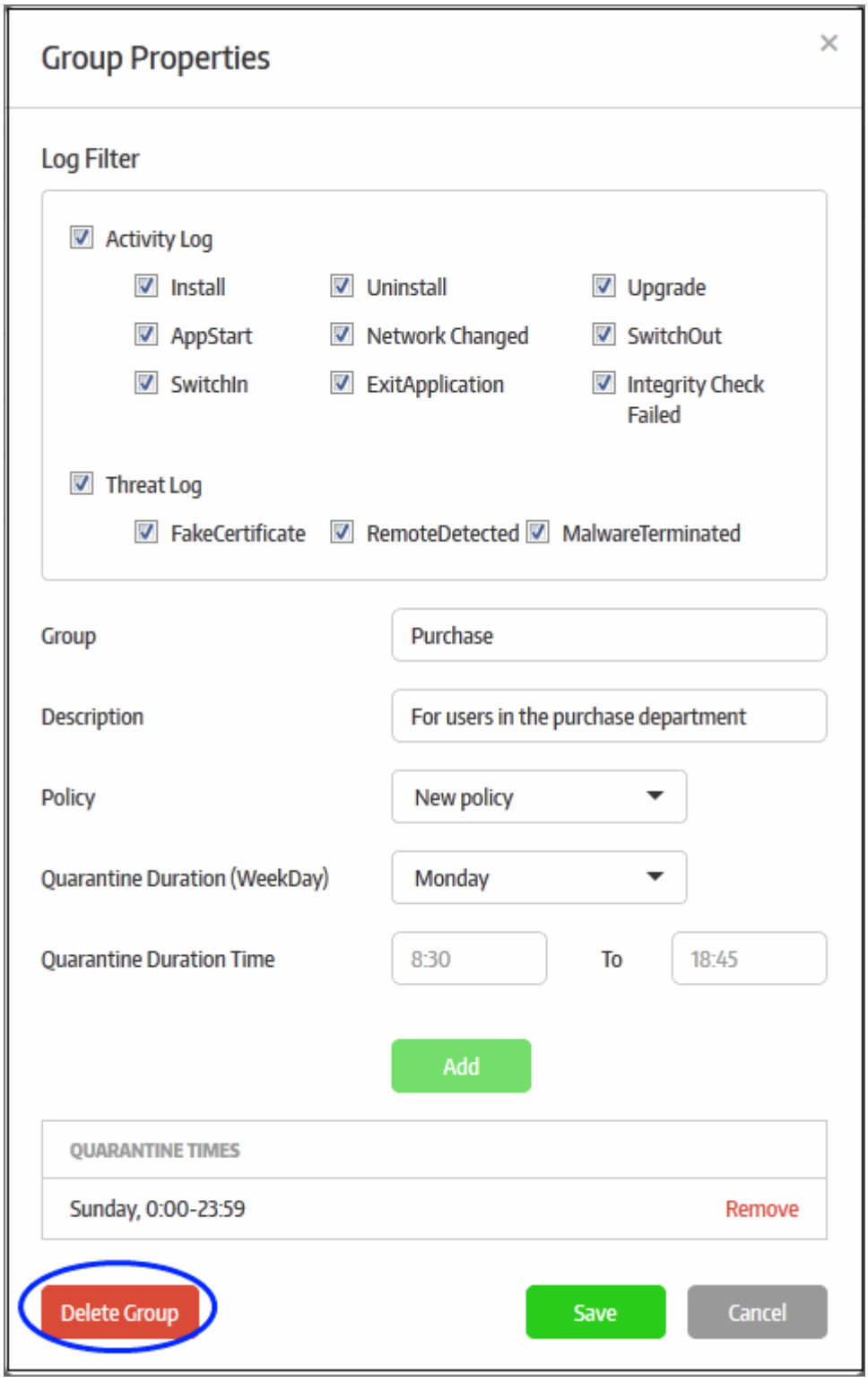
The 'Group Properties' screen of the selected screen will be displayed.

- Edit the details as required. The 'Group Properties' screen is the same screen displayed for creating a new endpoint group. Refer to the section '**Creating a New Endpoint Group**' for more details.
- Click the 'Save' button to apply your changes.

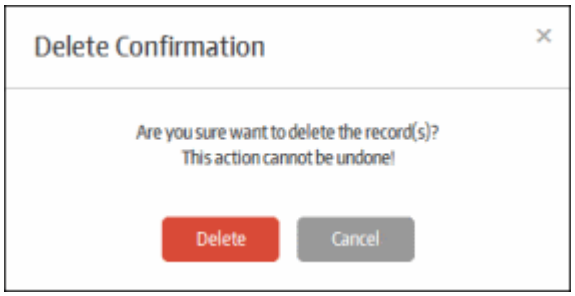
To delete an endpoint group

You cannot delete a group in which endpoints are available. To delete an endpoint group, you have to first move the endpoints to another group or delete them from the list. You can only delete a group that has no endpoints in it.

- Click on the name of the endpoint group that you want to delete from the list
- Click the 'Delete Group' button at the bottom of the 'Group Properties' screen



A confirmation dialog will be displayed.



- Click 'Delete' to confirm removal of the endpoint group

The endpoint group will be removed from the list.

7.Policies

The 'Policy Management' interface allows administrators to configure security policies that can be deployed to endpoint groups. Each policy consists of a set of secure apps that run inside the Secure Box environment on the target endpoints. Additional settings such as root certificate checks, keyboard protection and desktop isolation can be applied to each app. You can add multiple secure apps to a policy in three different modes:

- **URL Mode** - The specified URL will be run inside the Secure Box environment. For example, you can specify a bank website that is used by your customers or endpoint users.
- **APP Mode** - The specified endpoint application will be protected by Secure Box. For example, you could specify a payment processing application on a POS terminal.
- **Folder Mode** - Specific folders or even entire drive partitions can be protected. Items located inside the protected folder or drive will be run inside the secure environment.

Each policy can be applied to different endpoint groups, but each group can only have one policy at a time. If you want a policy to be applied to a single endpoint, you must still create a group for it.

A policy can be applied to a group during group creation or by editing it. Refer to the section **Managing Endpoint Groups** for more details on selection of policy to be applied to a group while creating it.

Once a policy is applied to a group, all secure apps configured in that policy will be pushed to all endpoints in the group. If a policy is edited, for example to add new secure apps, the changes will be pushed to all endpoints in the groups to which the policy is applied during the next polling cycle.

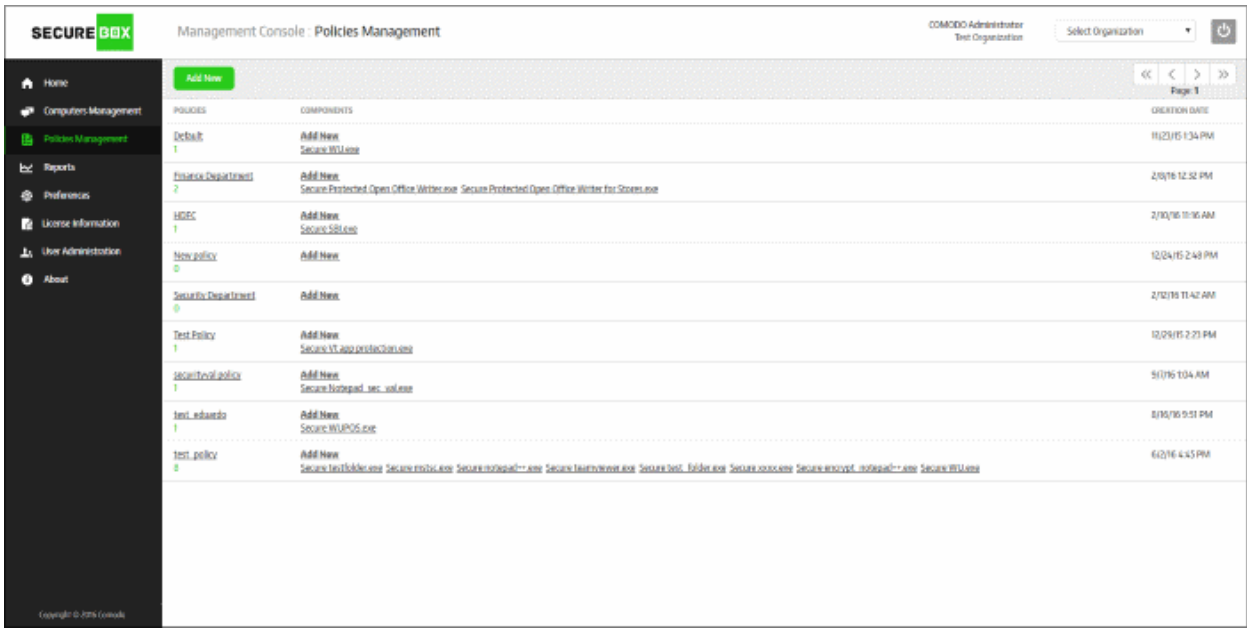
Click the following link for more details:

- **Managing Policies**

7.1.Manage Policies

The Secure Box Central Management Console allows administrators with appropriate privileges to configure policies as per organization requirements. The polices then can be assigned to endpoint groups. Please note that for an endpoint group only one policy can be assigned at a time. However, you can add multiple secure applications for a policy, such as multiple URLs, applications and folders. Refer to the section '**Creating a New Policy**' for more details.

To manage polices, click 'Polices Management' on the left:



Policies Management - Table of Column Description	
Column	**Description**
Policies	The name of the policy. You can edit the name and description of the policy by clicking on the name. The number below the name of the policy indicates the number of components added to the policy. Refer to the section '**Editing a Policy**' for more details.
Components	Displays the secured items available for a policy. You can edit a secure application of the policy by clicking on the name. Refer to the section '**Editing a Policy**' for more details. The 'Add New' link allows you to add a new secure application for the policy. Refer to the section '**Creating a New Policy**' for more details.
Creation Date	The date and time of policy creation by the administrator

Sorting option

Sorting the entries

Clicking on the 'Policies' and 'Creation Date' column headings sorts the entries based on the ascending/descending order of the entries as per the information displayed in the column.

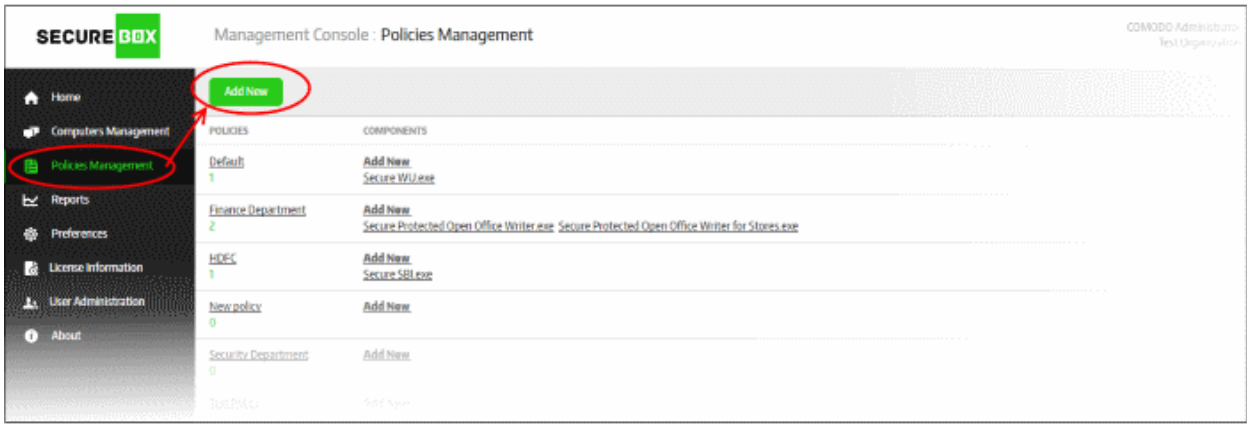
The interface allows an administrator with appropriate privileges to:

- **Create a new policy and add secure applications**
- **Edit a policy and its secure applications**

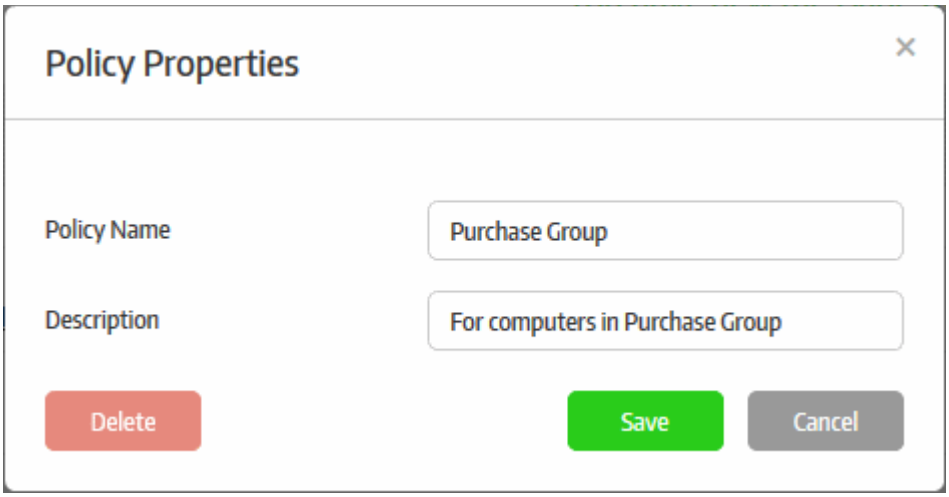
7.1.1. Create a New Policy

The 'Policies Management' section allows administrators to configure new polices and add secure applications to them as per organizational requirements. Though you can assign only one policy at a time to an endpoint group, you can add multiple components (secure applications) to a policy, each of which will be added to all endpoints in a group.

To create a new policy, click 'Polices Management' on the left and then the 'Add New' button

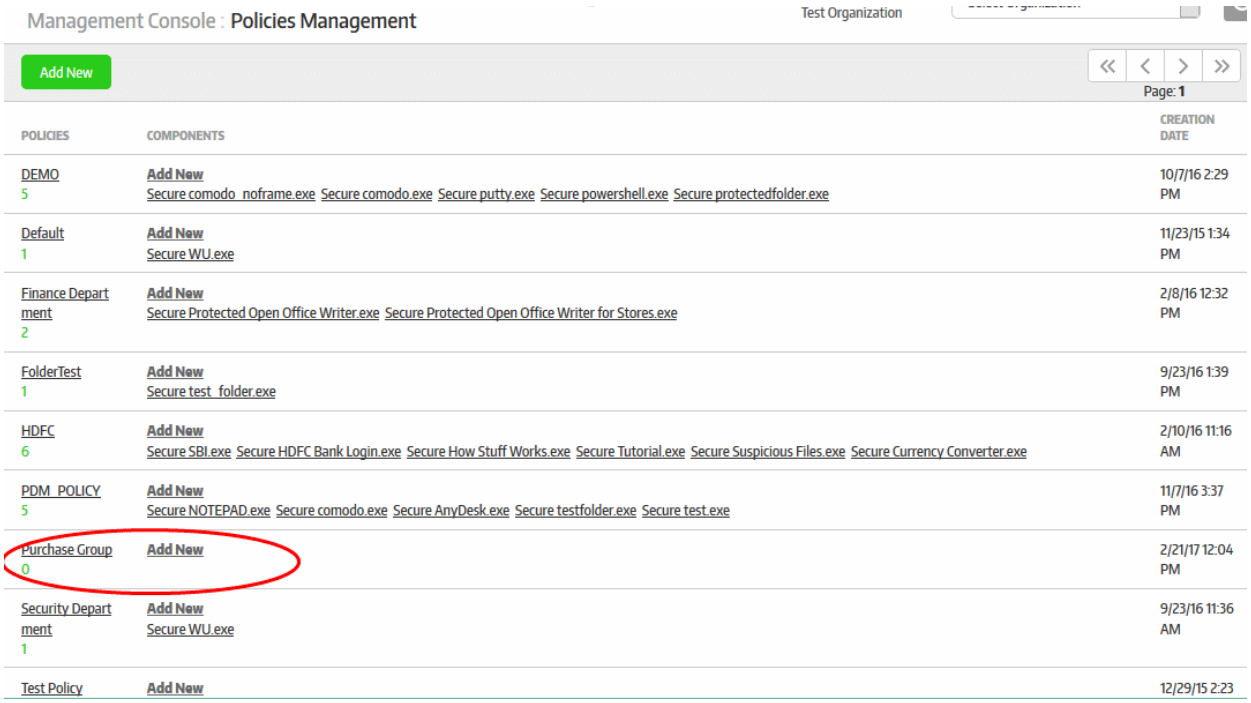


The 'Policy Properties' screen will be displayed:



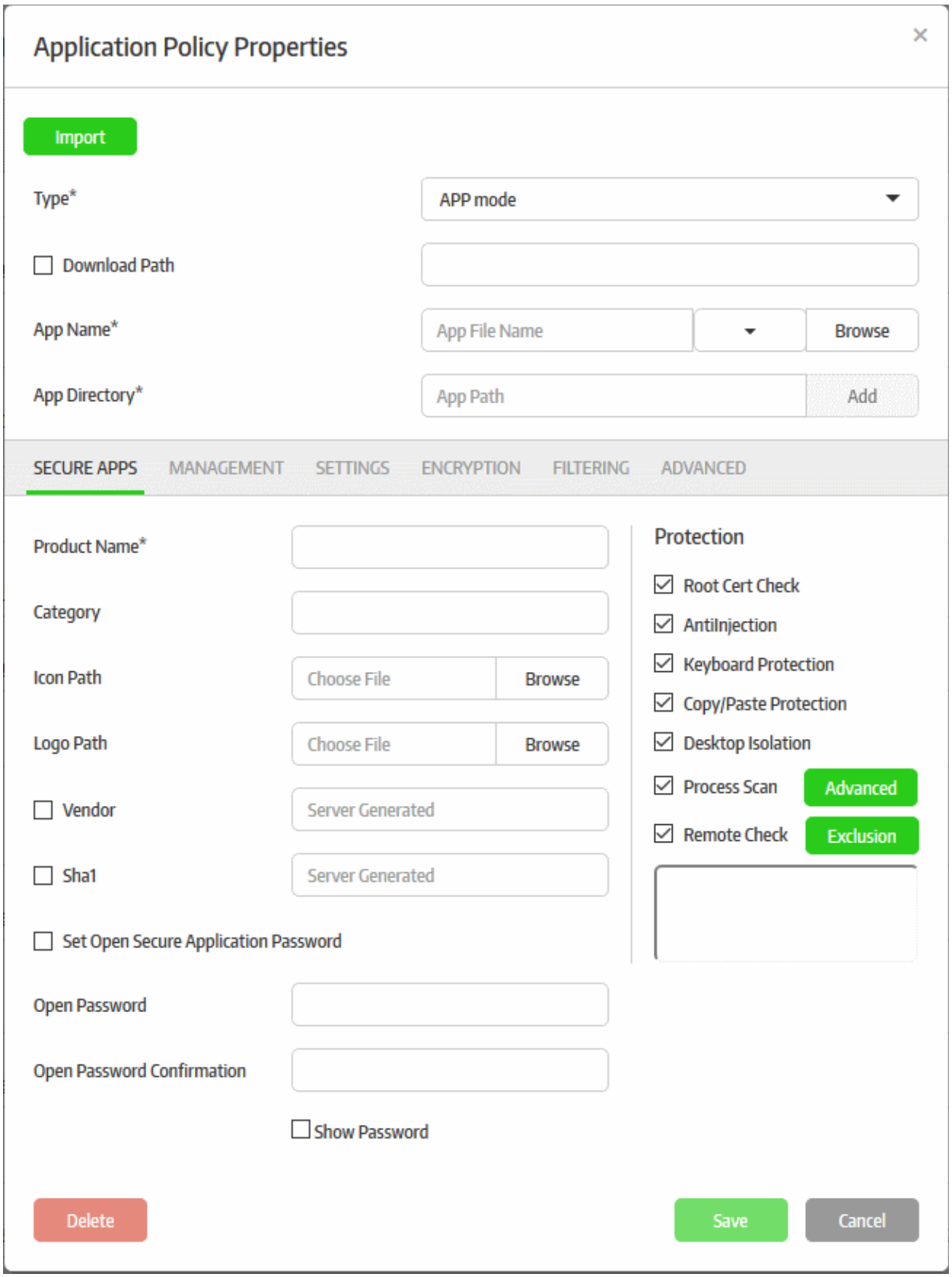
- Enter the name for the policy in the 'Policy Name' field
- Enter an appropriate description for the policy in the 'Description' field
- Click the 'Save' button

The policy will be added and listed in the screen.



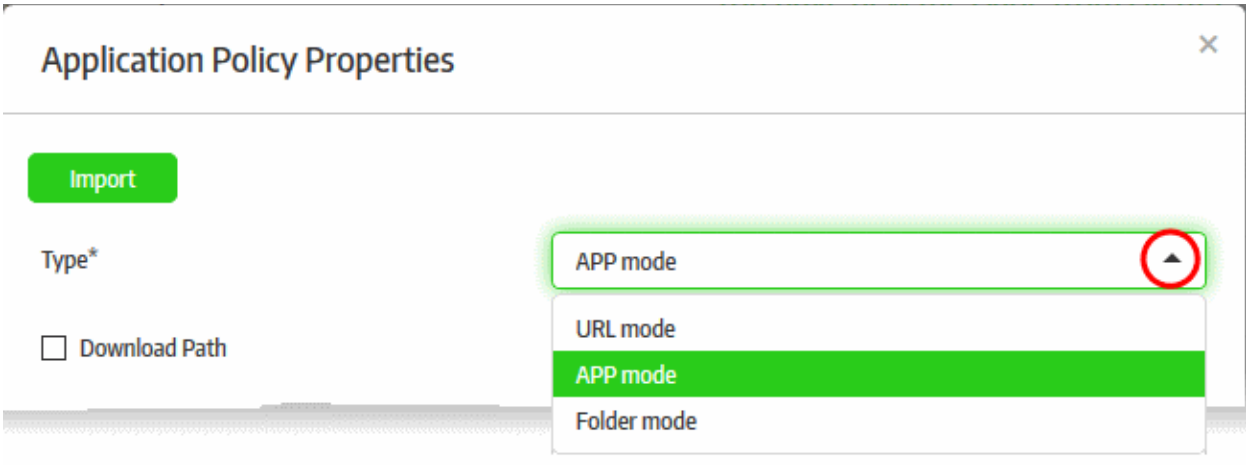
The next step is to and configure the secure application(s) for the policy. Click the 'Add New' link under the 'Components' column.

The 'Application Policy Properties' screen will be displayed:



You have the option to use an existing policy as a base to create a new policy. Refer to the section '**To create a new policy using an existing policy as a base**' for more details. The following steps explain how to create a new policy.

- Select the type of secure application that you want to add from the 'Type' drop-down

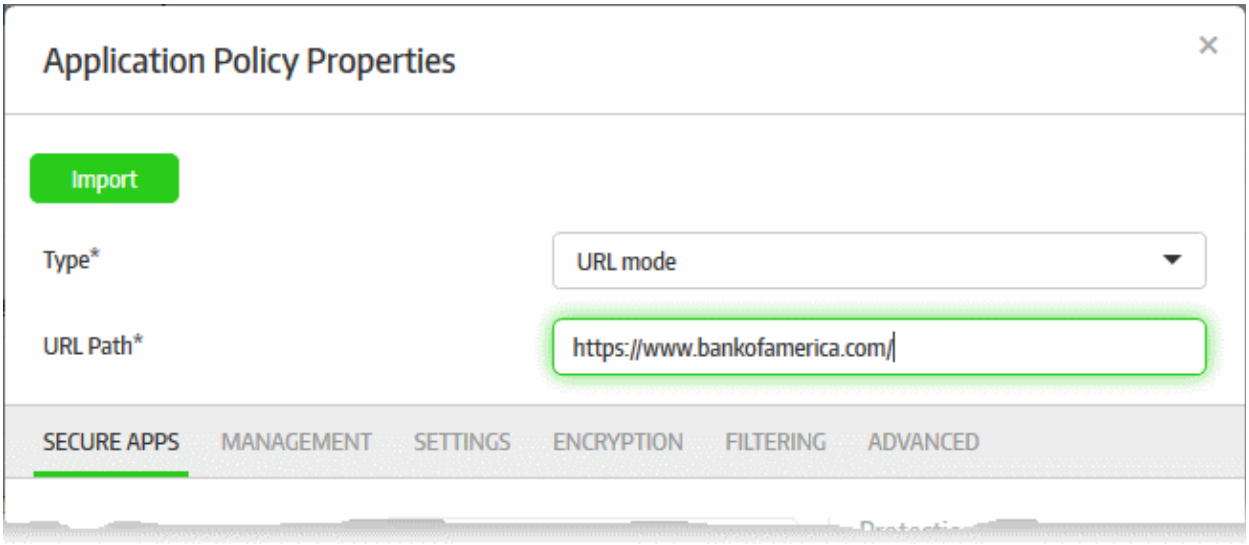


There are three types of secure applications:

- **URL Mode** - The specified URL will be run inside the secure box environment via the configured browser automatically when the secured application is launched. Refer to '**Configuring a Secure URL**' for more details.
- **APP Mode** - The specified application on the Windows endpoints will be protected by Secure Box. The secured application can be configured to open only in the SB environment. Refer to '**Configuring a Secure APP**' for more details.
- **Folder Mode** - A specified folder or an entire partition in the drive can be protected. The items opened inside the protected folder or drive will be run inside the secured environment. The secured item can be configured not to run outside of CSB. Refer to '**Configuring a Secure Folder**' 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



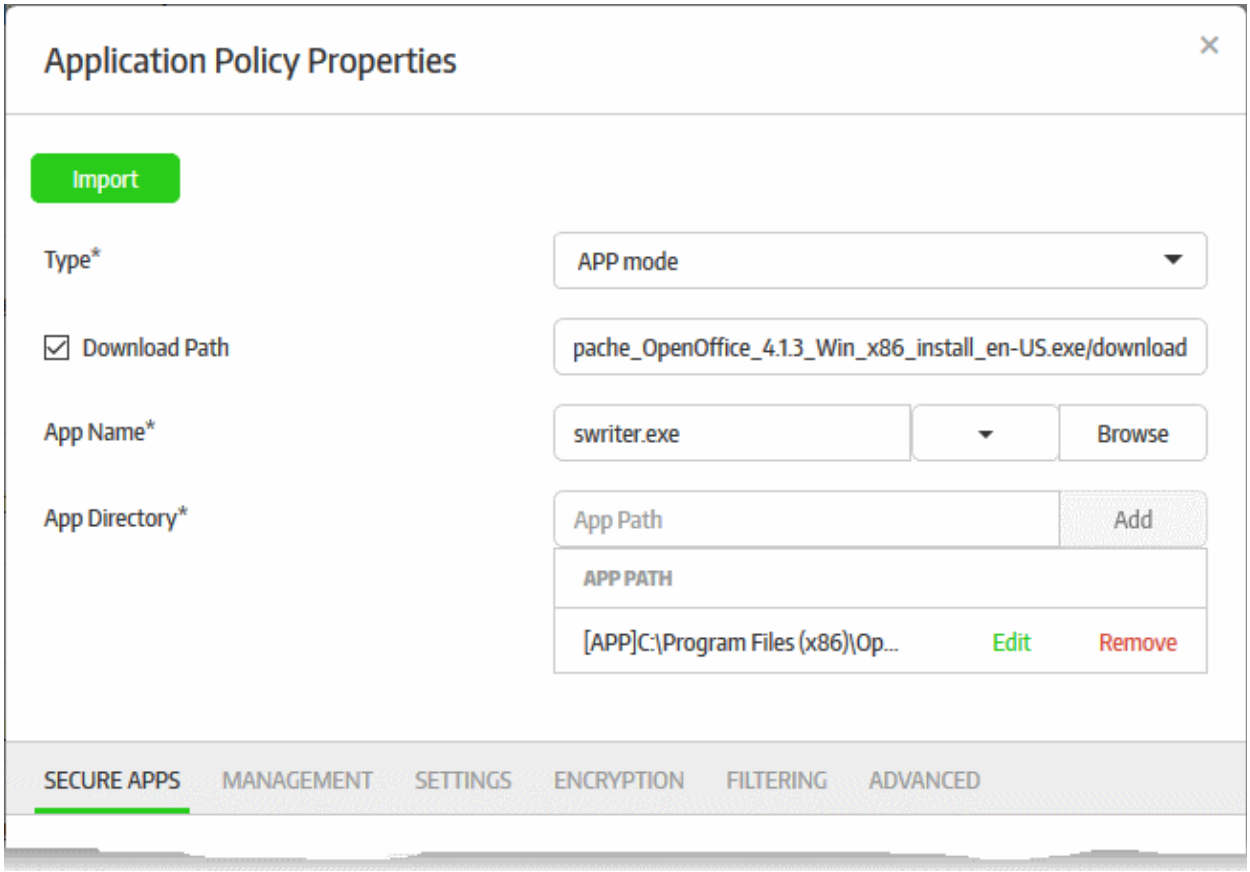
Each secure application allows for a more granular configuration through the sections below it. The parameters in the sections differ depending on the 'Type' of mode selected. Refer to '**Configuring Granular Secure Box Application Settings**' for more details.

Configuring a Secure APP

- Select 'APP mode' from the 'Type' drop-down
- Enter your app'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. Please note that the

'Vendor' and 'SHA1' fields (should be selected) 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 enter the app name. 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 in the field allows you to select Word, Excel or Powerpoint apps. If any of this selected, then there is no need to enter app name and app directory below, since they 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. The path of applications support system variables. For example, C:\Users\%username %\app\app.exe. Click 'Add'. Repeat the process to add more paths if the application might be installed on different locations on different endpoints.
- 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.

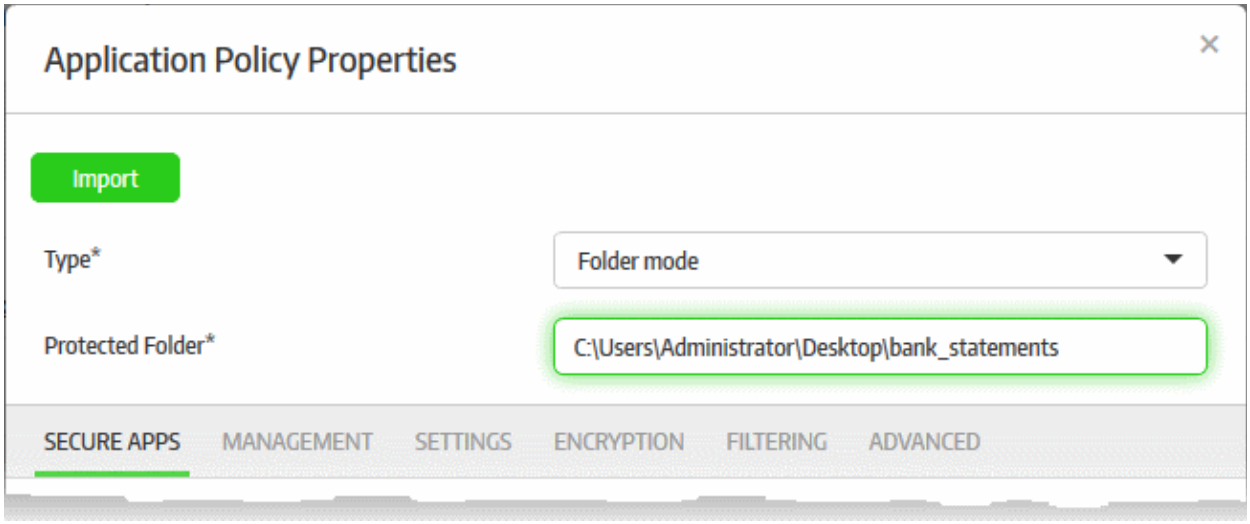


The app (bundled with vendor name and SHA1 values, if selected) with its path will be added and listed below it. Repeat the process to add multiple apps for the secure application. To remove an application path, click the 'Remove' link beside it. Each secure application allows for a more granular configuration through the sections below it. The parameters in the sections differ depending on the 'Type' of mode selected. Refer to '**Configuring Granular Secure Box Application Settings**' for more details.

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



Each secure application allows for a more granular configuration through the sections below it. The parameters in the sections differ depending on the 'Type' of mode selected. Refer to '**Configuring Granular Secure Box Application Settings**' for more details.

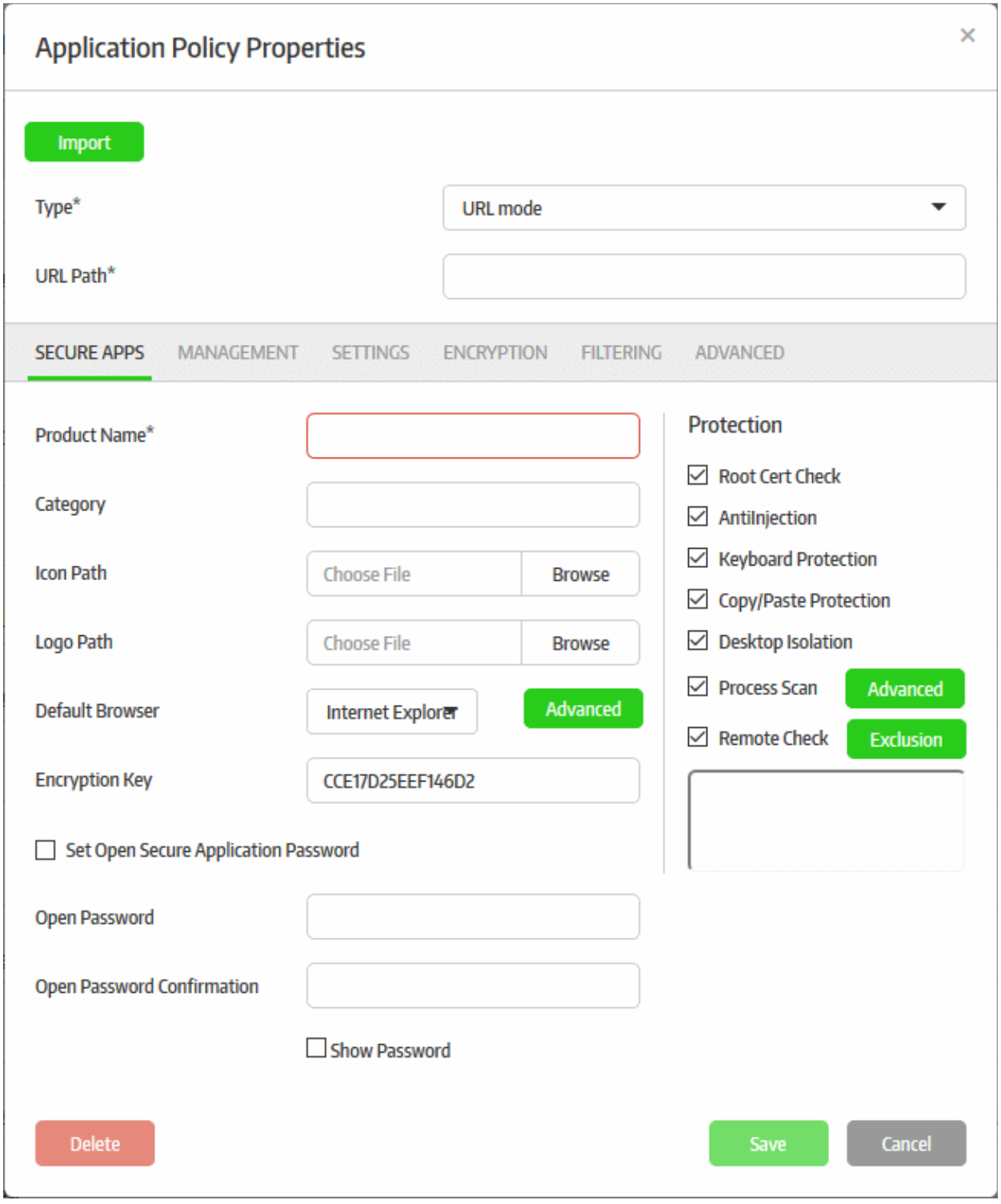
Configuring Granular Secure Box Application Settings

By default, the 'Secure Apps' tab will be selected. Click the links below to go straight to the required settings tab:

- **Secure Apps**
- **Management**
- **Settings**
- **Encryption**
- **Filtering**
- **Advanced**

Secure Apps Tab

The 'Secure Apps' tab allows you to configure basic information and protection settings for the secure application.



Policies - 'Secure Apps' Tab - Table of Parameters	
Parameter	**Description**
Product Name	Enter the name of the secure application.
Category	Enter an appropriate category name for the application.
Icon Path	The icon is used: • As the symbol of the secure application • On the splash screen when the secure application starts

	• As the start menu image for the secure application when a logo is not configured Supported format for the icon is .ico. Click the 'Browse' button, navigate to the location where the icon is stored and click 'Open'.
Logo Path	The logo is used: • On the 'blocked page' dialog • On the 'remote connection' warning dialog • As the start menu image for the secure application. If a logo is not configured then the icon will be shown instead. Supported format for the log is .png. Click the 'Browse' button, navigate to the location where the logo is stored and click 'Open'.
Default Browser	This will be available only for 'URL mode'. Select the browser from the drop-down which will be used to open the secured URL. The options available are Internet Explorer (IE), Comodo Dragon, Portable IE8/9 and Comodo Ice Dragon browsers. If you choose Internet Explorer, you can configure advanced settings for IE-based secure applications. You can also add a pre-installed website certificate for the URL specified in the secure app, in order to compare it with the certificate obtained from the website. For more details, Refer to the explanation of **Configuring Advanced Settings for IE Based Applications**, under this table.
Encryption Key	This will be available only for 'URL mode'. This is used for validating an endpoint that is connected with CMC. The validation process includes sending encrypted values from the endpoint such as CMC generated machine ID, time stamp, Extra ID of the machine and so on. The values are encrypted using the encryption key and sent to the CMC via X token parameter in the http header. CMC decrypts the value and if found they are from a validated endpoint and coming from CSB, CMC allows it to connect to the configured URL. By default, an encryption key, which is 16 bytes in length, comes built-in with CMC. However it is advisable to change the encryption key in frequent intervals for safety.
Vendor	Applicable for 'App mode' only. If this is enabled and details filled, then only application produced by this vendor is allowed to run in the secure applications. If 'Browse' option is used to fill the 'App Name', then the vendor name, if available, will be auto-populated. You can also enter the details manually. CSB will check the vendor details when the app is run, and only when this matches with defined value, the application will be allowed to run. To get the vendor information of an executable file, check its properties -> Digital signature -> Details -> Singer information -> Name.
SHA1	Applicable for 'App mode' only. If 'Browse' option is used to fill the 'App Name', then the SHA1 values, will be auto-populated. You can also enter the details manually. CSB will check the hash values when the app is run, and only when this matches with the defined value, the application will be allowed to run.
Folder Advanced	Applicable for 'Folder mode' only. Click this to configure advanced settings for the protected folder.

	
	• Only run signed applications - If enabled, applications signed by code signing certificates by vendors only will be allowed to run.
	• Block outside process from access file in protected folder - If enabled, outside processes will be denied access to files in the protected folder. This is enabled by default.
	• Allowed Files - Allows you to configure to open files with the set extensions only. Enter the file name with the extension. You can also add extension with wildcard so as to allow opening all files with the configured extension. If no file is specified, then all the files in the secured folder will be allowed to open.
	  • Click the 'Add' button to add the files to the 'Allowed Files' list.
	  • To delete a file, click the 'Remove' link beside it.
	  • Click the 'Save' button to apply your changes.

Set Open Secure Application Password	If selected, administrators can configure a password to open the secured item.
Open Password	Enter the password that should be used to open the secured item.
Open Password Confirmation	Enter the same password to confirm.
Show Password	If selected, the password will be displayed in the 'Open Password' field.
Protection Settings	
Root Cert Check	If enabled, the secured application will check for the root certificate. By default, CSB will compare with the Microsoft Trusted Certificate list. If required, the root certificate list can also be customized from the '**Management**' tab.
Anti-Injection	If enabled, the secured application will be protected from malware injection.
Keyboard Protection	If enabled, the secured application will be protected against keyboard sniffing
Copy/Paste Protection	If enabled, the copy/paste operation cannot be done between the secured item and Windows desktop application
Desktop Isolation	If enabled, the normal Windows desktop will be isolated when the secured item is in operation. The user can switch between the desktop and the SB environment, by clicking the 'Switch to' button in the task bar.
Process Scan	If enabled, Comodo Secure Box will check all running processes with Comodo's File Look-Up Server (FLS) before the secure application starts. The FLS database contains the latest virus signatures. You have the option to automatically terminate any malicious processes which are discovered. Click 'Advanced' to view the scan options:

	 • Scan in Background - Process scan will be done in the background during secure application launch. • Detect unsafe process - Unsafe processes will be detected and a warning message will be displayed before the secure application launches. • Detect and terminate unsafe process - Unsafe processes will be detected and terminated before the secure application launches.
Remote Check	If enabled, remote control applications will be detected and blocked for the secured item. You can exclude some remote applications by clicking the 'Exclusion' button.  • Select the remote application that should be excluded • Click the 'Save' button.

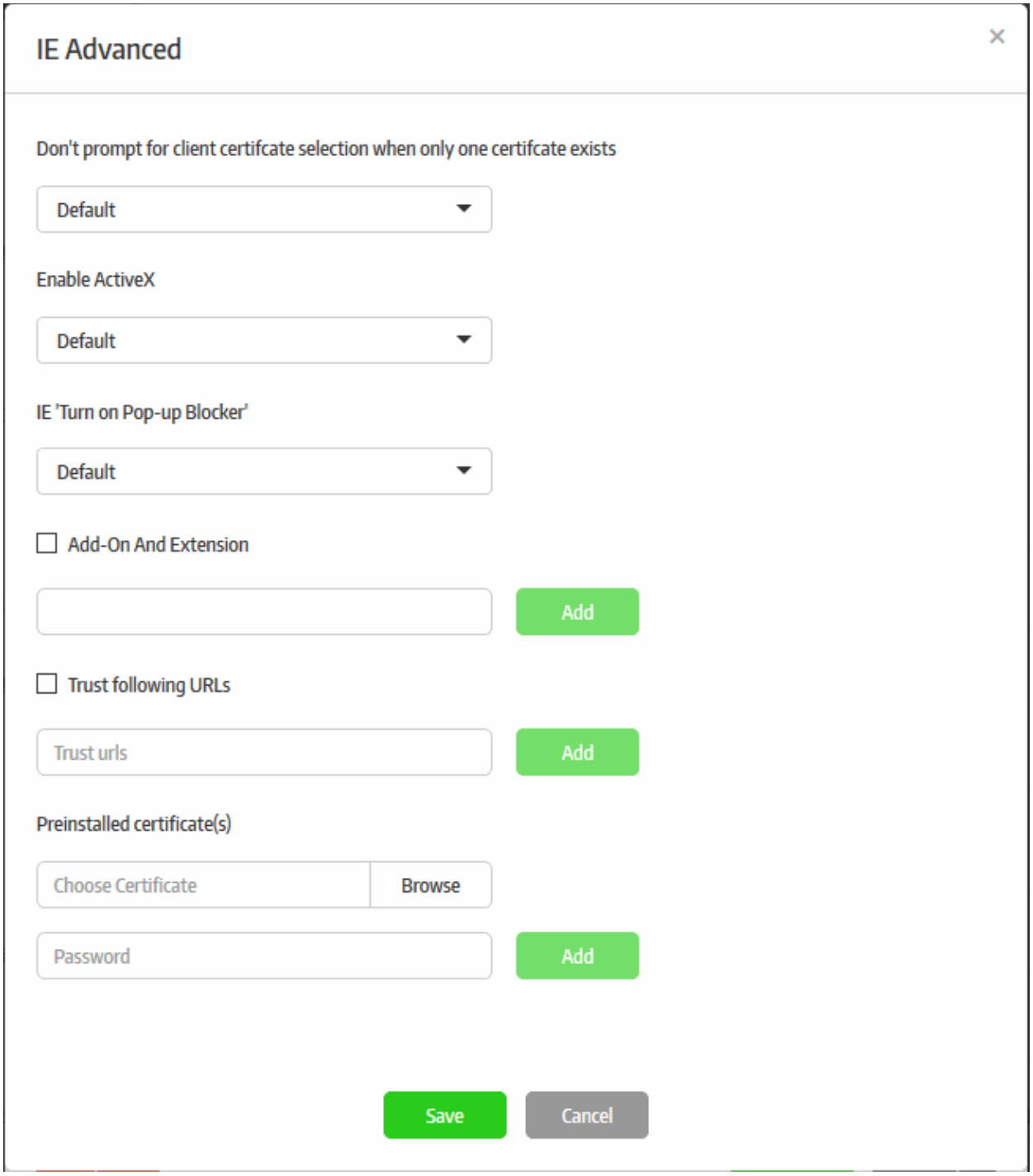
- Click 'Save' for your settings to take effect

Configuring Advanced Settings for IE Based Applications

Administrators can configure additional security settings for URL Mode applications that are set to open in Internet Explorer (IE).

- Click the 'Advanced' button that appears beside the 'Default Browser' field after selecting 'Internet Explorer' from the drop-down

The IE Advanced Settings interface will open:



'Advanced IE Settings' - Table of Parameters	
Parameter	**Description**
Don't prompt for client certificate selection when only one certificate exists	If the secure app requires client authentication to access a site, Internet Explorer will ordinarily ask the user to choose the client certificate they want to use - even if only one certificate exists. You can change this behavior to the following: • Default - The default setting in IE will apply • Enable - If only one client certificate exists, IE will automatically select it and will not show a prompt to the user. • Disable - IE will always prompt users to choose the client certificate they wish to use - even if only one certificate exists.

Enable ActiveX	Allows you to enable or disable ActiveX controls on the website accessed through the secure app. The available options are: • Default - The default setting in IE will apply • Enable - ActiveX controls will be forcibly enabled for the website • Disable - ActiveX controls will be forcibly disabled for the website
IE 'Turn on Pop-up Blocker'	Choose whether to allow or block pop-up windows displayed by the website. The available options are: • Default - The default setting in IE will apply • Enable - Pop-up windows will be forcibly blocked • Disable - Pop-up windows will be allowed irrespective of the The default setting in IE
Add-on and Extension	By default, Secure Box disables all add-on and extensions in IE. To enable them, you have to add their GUID in the field below. The GUID of an add-on can be found in its properties (IE > Manage add-ons > right click on the add-on > select 'more information'). GUID = CLASS ID. **To selectively allow Add-ons and Extensions** • Enable the 'Add-on And Extension' checkbox • Enter the CLASS ID of the extension you wish to allow and click 'Add':  • Repeat the process to add more allowed extensions/add-ons • To delete an item from the list, click the 'Remove' link beside it.
Trust following URLs	Add a list of trusted websites to the secure application. If the security level setting of IE ('Tools' > 'Internet Options' > 'Security' Tab) at an endpoint is set to 'High', IE will block all websites other than those in its trusted websites list. If you want some websites to be accessed by the IE based secure app, even if the IE is set to 'High' Security level at the endpoint, then add the URLs of the websites to 'Trusted URLs' field. **To add trusted websites** • Select the 'Trust following URLs' check box.

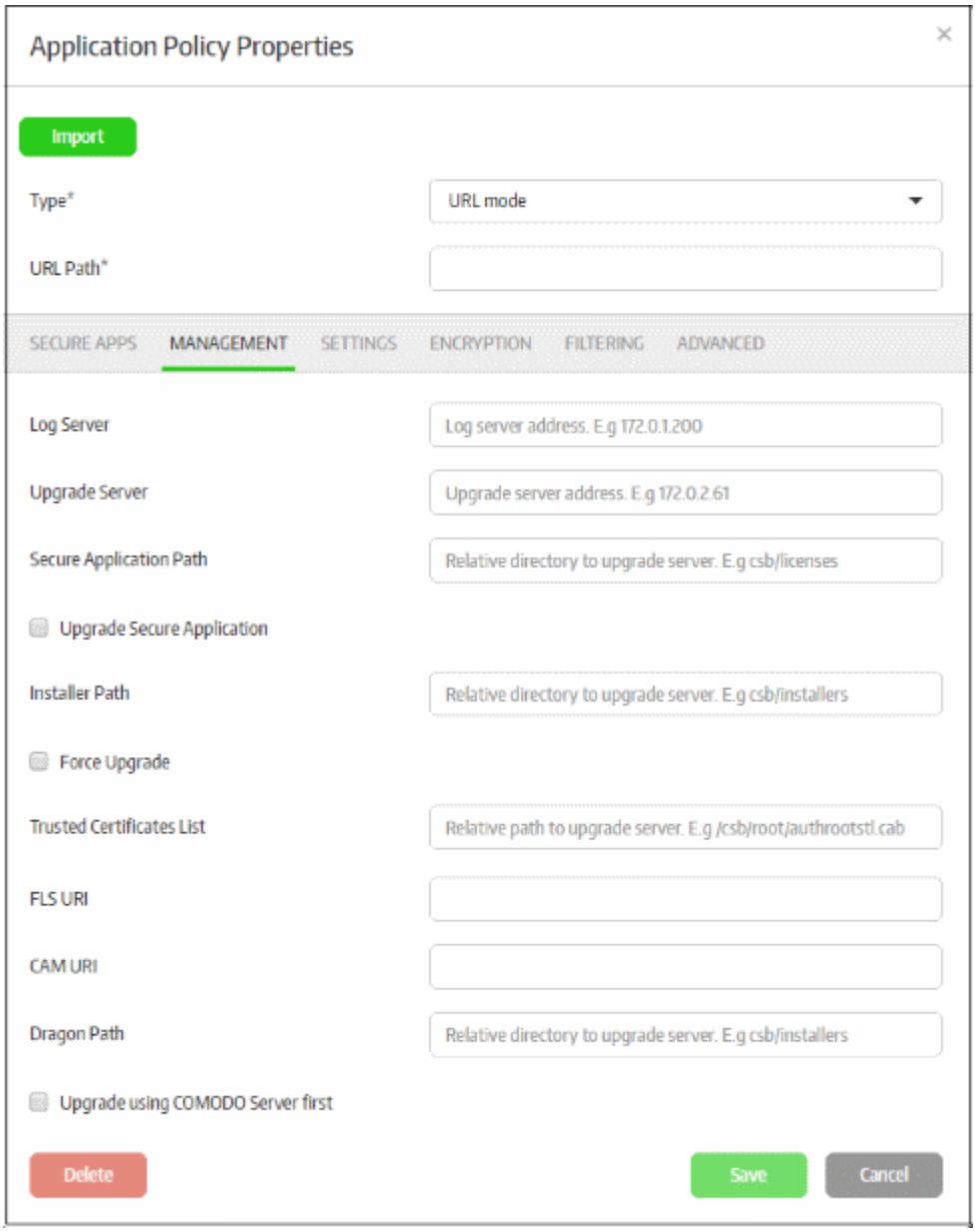
	 • Enter the URL/domain name and click the 'Add' button. • Repeat the process to add more trusted URLs • To delete a URL from the list, click the 'Remove' link beside.
Pre-installed certificates	Allows you to install existing client certificates into the IE certificate store. This allows users to continue to authenticate themselves to websites when accessing via a Secure Box app. Some websites, for example banking websites and online shopping websites, require a client certificate to be installed on the user's browser for two-factor authentication. The client certificate is usually provided by the website operator. A user's client certificate can also be obtained by exporting it from their browser's certificate store and saving in .cer format. Administrators can add these certificates to the IE Advanced Settings component of the secure app configuration. Once the secure app is pushed to the endpoint, the certificate(s) will be installed, allowing the user to access the website from within the secure app. Once installed, the certificate also serves for authentication when the website is accessed outside the secure app. To add a pre-installed certificate • Download the certificate from the website and save it in .cer format • Click 'Browse', navigate to the location of the certificate file, select the certificate and click 'Open' The certificate file will be added • Enter the password to be used for installation of the certificate in the 'Password' field and click 'Add' • Repeat the process for adding more certificates

- Click 'Save' for your settings to take effect.

Management Tab

The administrators can upgrade CSB to latest versions using the Central Management Console, which is convenient and easy. However, if the organization has a strict network environment or if the CMC is down, the admins can configure the local server and upload the latest CSB versions here so that the endpoints can upgrade to latest versions from the local server.

- Click the 'Management' tab.



Policies - 'Management' Tab - Table of Parameters	
Parameter	**Description**
Log Server	Enter the IP of the log server address where the CSB logs will be stored. This will be auto-filled if the global log server setting is configured in the 'Preferences' section. Refer to the section 'Configuring the Management Console' for more details.
Upgrade Server	Enter the IP address of the local server in which the latest CSB versions must be uploaded by the admins. For example, 172.0.2.61. This will be auto-filled if the global upgrade server setting is configured in the 'Preferences' section. Refer to the section 'Configuring the Management Console' for more details.
Secure Application Path	Enter the path of the secure apps in the upgrade server, for example, csb/secureapps or csb/licenses. Secure applications will be updated from this path if CMC is not available or down.
Upgrade Secure Application	If this option is enabled and if there is a new version of secure application is available provided in the 'Secure Application Path' field, then the secure application will be updated when it is opened. If it is disabled, the secure app will not be updated.

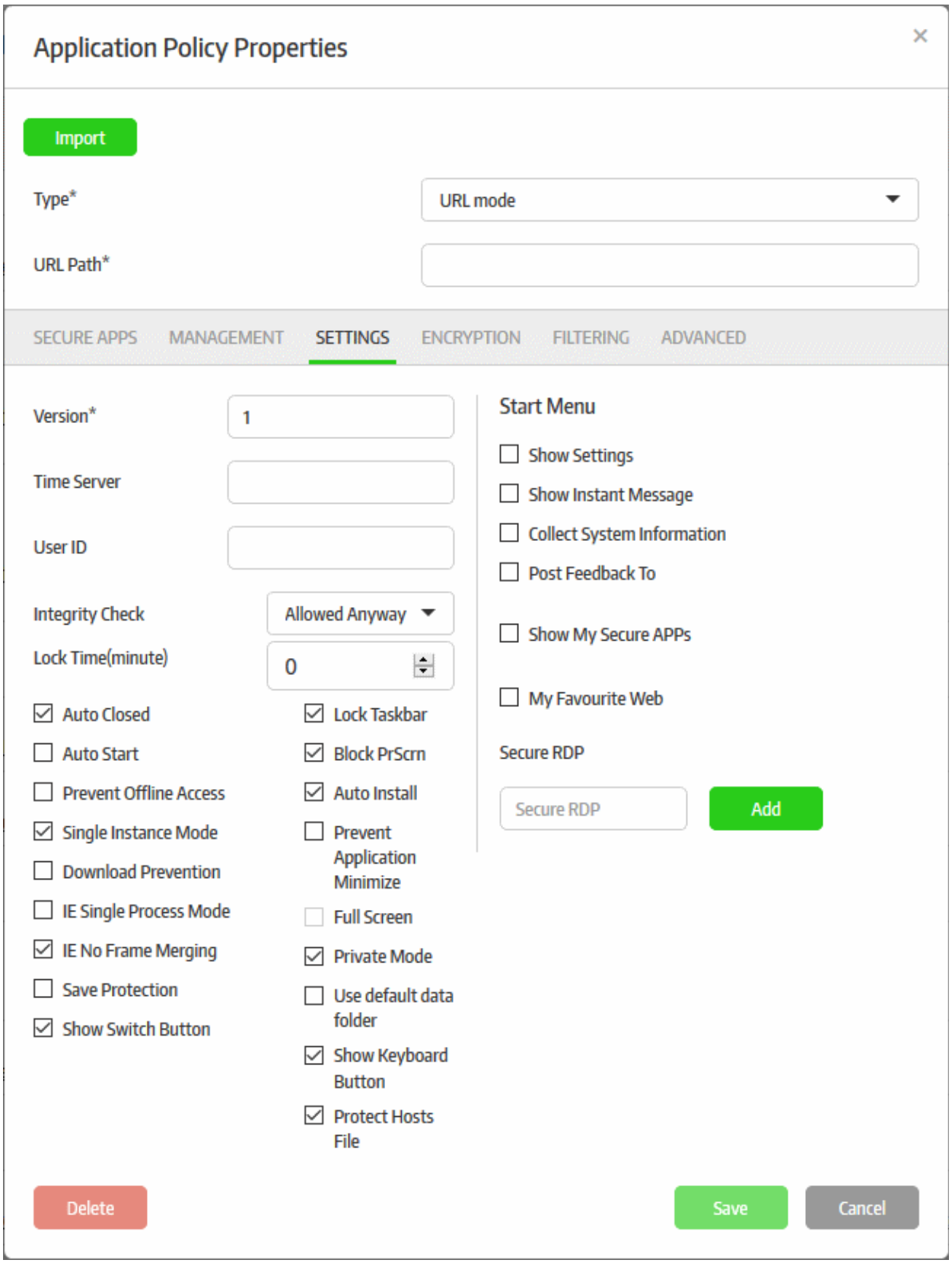
Installer Path	Enter the path of the CSB installation files in the upgrade server, for example, csb/installers.
Force Upgrade	If a new version of CSB available and the path is specified in the 'Installer Path', CSB will be updated automatically when any secure application is run. If disabled, users will get a prompt dialogue when running a secure app that a CSB update is available.
Trusted Certificates List	CSB verifies the root certificates using the Microsoft Root Certificate list. You can customize the root certificate list for verification. Enter the path of the root certificates stored in the upgrade server. For example, csb/root/authrootstl.cab
FLS URI	Enter the URL of the FLS. The FLS scan is performed in this redirected location, which mostly is pointed to Comodo's FLS servers.
CAM URI	Enter the URL of the CAM. The CAM license check scan is performed in this redirected location, which mostly is pointed to Comodo's CAM servers.
Dragon Path	Applicable for 'URL mode' only. The Dragon browser is customized for CSB. If a newer Dragon version is available, it can be updated by client. Enter the path of new versions of Dragon installation files in the upgrade server, for example, csb/dragon
Upgrade using COMODO Server first	If enabled, Comodo servers will be the first option for upgrading irrespective of the settings done above.

- Click the 'Save' button for your changes to take effect.

Settings Tab

The 'Settings' tab allows administrators to configure basic settings for the secured item.

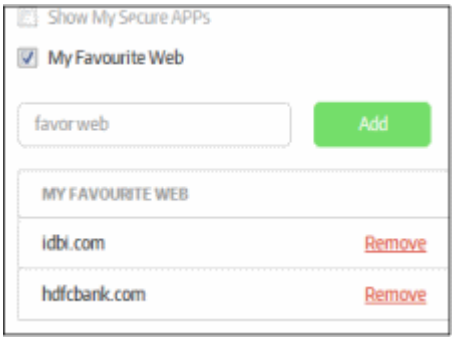
- Click the 'Settings' tab.



Policies - 'Settings' Tab - Table of Parameters	
Parameter	**Description**
Version	Enter the version number for the secure application. This determines the whether the

	secure app is up-to-date or not. The secure app on the endpoints will the check the upgrade server for the latest version and update accordingly. This is applicable only when the upgrade server details are configured in the 'Management' tab.
Time Server	Enter the time server details for synchronizing the time among the systems, which is used for HTTP authentication time stamp. This will be auto-filled if the global time server setting is configured in the 'Preferences' section. Refer to the section '**Configuring the Management Console**' for more details.
User ID	The 'Customer ID' that can be found in the 'About' page. This is applicable only when the upgrade server details are configured in the 'Management' tab.
Integrity Check	When a secure application is started, CSB will check the system environment for running the secure application safely. For example, CSB keyboard filter priority in the filter list. If the integrity check is failed, that CSB keyboard filter is not in the first priority, CSB will act per the option chosen. There are three options available: • Allowed Anyway - The secure app will be allowed to start • Block - The secure app will not be allowed to start • Prompt to user - A warning message will be displayed for the user to decide whether to allow or block
Lock Time (minute)	This field specifies the timeout in minutes to lock the Windows desktop if there is no user action. Enter '0' to disable this option.
Auto Closed	If enabled, the secure application will be closed automatically if the last window in it is closed.
Auto Start	If enabled, secure application will be launched during the Windows OS start.
Always Open it in CSB	Applicable for 'APP mode' only. If enabled, the secure application will always run in CSB only irrespective of whether the application is opened directly or a file that opens through the application. For example, if you create MS Word application as a secure app and deploy it, all the word files will open in Secure Box only whether opened via MS Word or double clicked on a word file.
Prevent Offline Access	If enabled, the secure application is not allowed to start if network connection is not available.
Single Instance Mode	If enabled, only one instance of the secured application will open. If opened again, the secure application will show the already opened application.
Download Prevention	Applicable for 'URL mode' only. If enabled, files cannot be downloaded from the Internet.
IE Single Process Mode	Applicable for 'URL mode' only. If enabled, IE runs at single process mode in CSB.
IE No Frame Merging	Applicable for 'URL mode' only. If enabled, IE can run both inside and outside the secure app at the same time. The user will be able to run IE outside the app separately, even if the browser is running inside the secure app.
Save Protection	If enabled, users cannot save the content of the web pages to their local machines. Currently only IE is supported for this feature.
Show Switch Button	If enabled, the button to switch between secure application and desktop will be displayed inside the Secure App window.
Lock Taskbar	If enabled, the task bar is locked when the secure application is run.
Block PrScrn	If enabled, no print screen is allowed in CSB.

Auto Install	If enabled, when the secure application is run on a system without CSB, the CSB will be automatically downloaded and installed.
Prevent Application Minimize	If enabled, the secure application window cannot be be minimized.
Full Screen	Applicable for 'URL mode' only. If enabled, the secure application will open in full screen mode.
Close Running Application	Applicable for 'App mode'. If enabled, a warning will be displayed if you open an secure application that is already open before it was made secure. For example, some endpoints will have notepads already running and you create a secure application to run notepad.exe and deploy it. If the users try to open the secure application, a warning will be displayed to close the already running application.
Private Mode	Applicable for 'URL mode' only. If enabled, the secure application will open in private mode.
Use default data folder	Applicable for 'URL mode'. If enabled, Comodo Dragon and IE browsers can use profile data saved in their respective default data folders (running outside SecureBox). If this not enabled, these browsers will create their own profile data. Username and password saved outside of SB cannot be auto used in SB.
Show Keyboard Button	If enabled, the keyboard button will be displayed in secure application desktop.
Protect Hosts File	If this option is selected, the hosts file will not be used in secure applications. This means secure applications will be protected from host file poisoning attacks.
App Filter Behavior	The settings done here determine the action for the 'Allow following applications only' settings done in the 'Filtering' tab. There are three options available: • Allowed Anyway - The configured app will be allowed to start • Block - The configured app will not be allowed to start • Prompt to user - A warning message will be displayed for the user to decide whether to allow or block
Start Menu Settings	
Show Settings	If selected, the 'Show Settings' menu item will be available from the CSB start menu on the endpoints. On clicking it, the 'View Settings' dialog will be displayed providing details such as 'Protected Data, Allowed URLs, 'Allowed Applications', Terminated Process and About'.
Show Instant Message	If selected, the 'Send Instant Message' option will be available on the endpoint from the start menu for the secure application. The end-user can use this option to send instant messages to administrators. When an end-user sends a message, a notification will be displayed at the top of the management console, and the message icon beside the endpoint name will turn green in the 'Computer' > 'Computer Management' interface. By clicking the icon, the currently logged-in administrator can view the message. Refer to the **Managing Endpoints** section for more details.
Collect System Information	If selected, the 'Collect System Information' menu item will be available from the CSB start menu on the endpoints. On clicking it, CSB collects the basic system information for troubleshooting to help CSB support team.
Post Feedback To	If selected, the 'Post Feedback To' menu item will be available from the CSB start menu on the endpoints. On clicking it, CSB will send feed back information to a

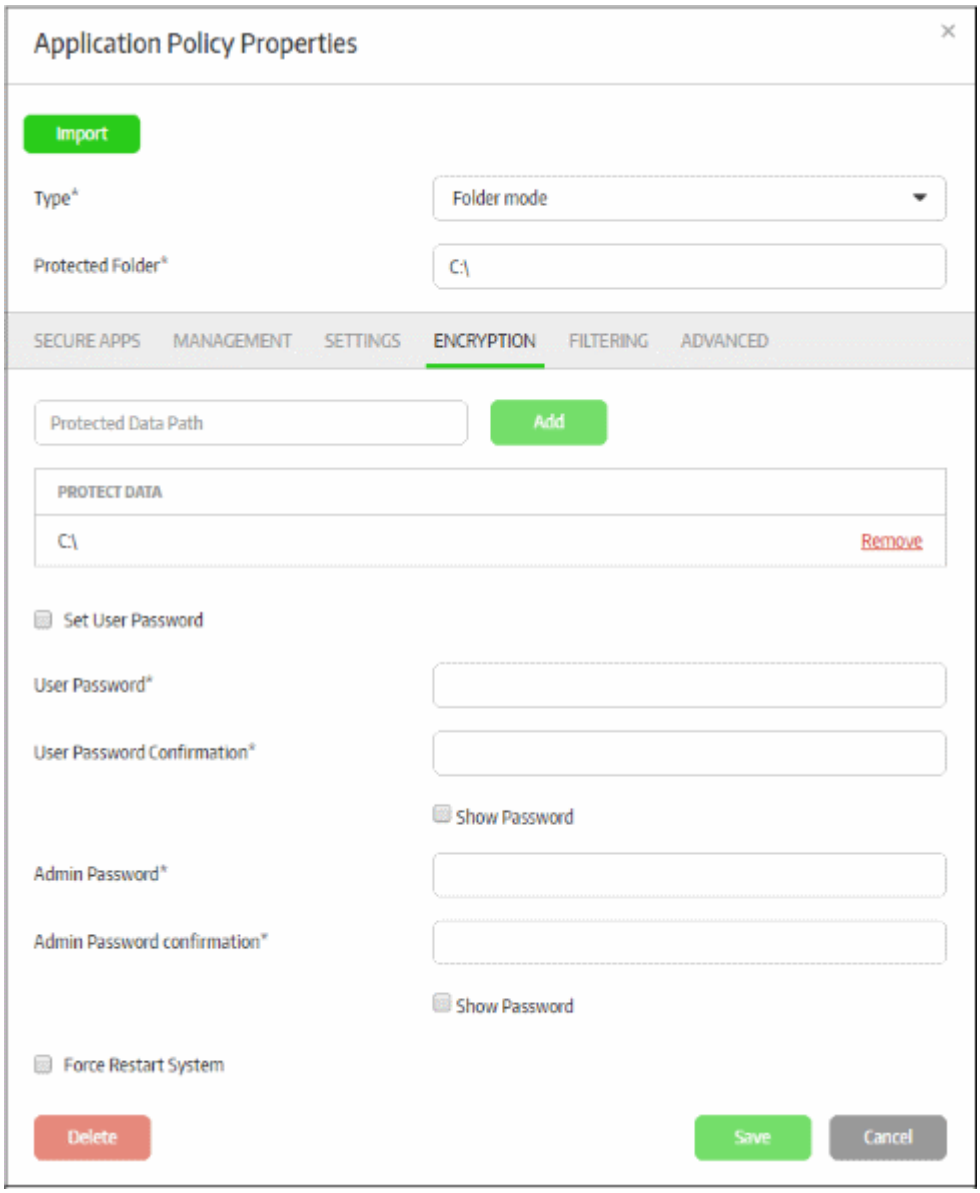
	specified email address. By default, the information is sent to **secureboxsupport@omodo.com**. You can change the email address in the field.
Show My Secure APPs	If selected, all the secure applications that have run before will be available from the CSB start menu as 'Recent Secure Applications'
My Favourite Web	Applicable for 'URL mode' only. If selected, the 'My Favorite Websites' menu item will be available from the CSB start menu on the endpoints. • Enter the website address and click the 'Add' button. Repeat the process to add more websites.  • To delete a website from the list, click the 'Remove' link beside. The added websites will be listed under 'My Favorite Websites'
Secure RDP	Computers that are using secure RDP application will allow RDP connections to it only via secure applications from other endpoints. You can add IPs of machines that are installed secure RDP application. • Enter the IPs of remote machines with secure RDP application that should be allowed to taken remotely and click 'Add'.  • Repeat the process to add more computers with secure RDP application. • To delete an IP from the list, click 'Remove' beside it.

- Click the 'Save' button for your changes to take effect.

Encryption Tab

The 'Encryption' tab allows administrators to configure the data folders that will be be protected with 'Transparent Data Encryption'. Files created by secure applications and stored in the configured folder will also be encrypted and can be accessed by the secure applications with read/write permissions. Non secure applications that access the encrypted folders have only read permissions. One secure app can secure multiple folders and one folder can be secured by multiple secure apps as well. Make sure to specify predefined generic names, for example, appdata and userhome, to work with all Windows accounts.

- Click the 'Encryption' tab.



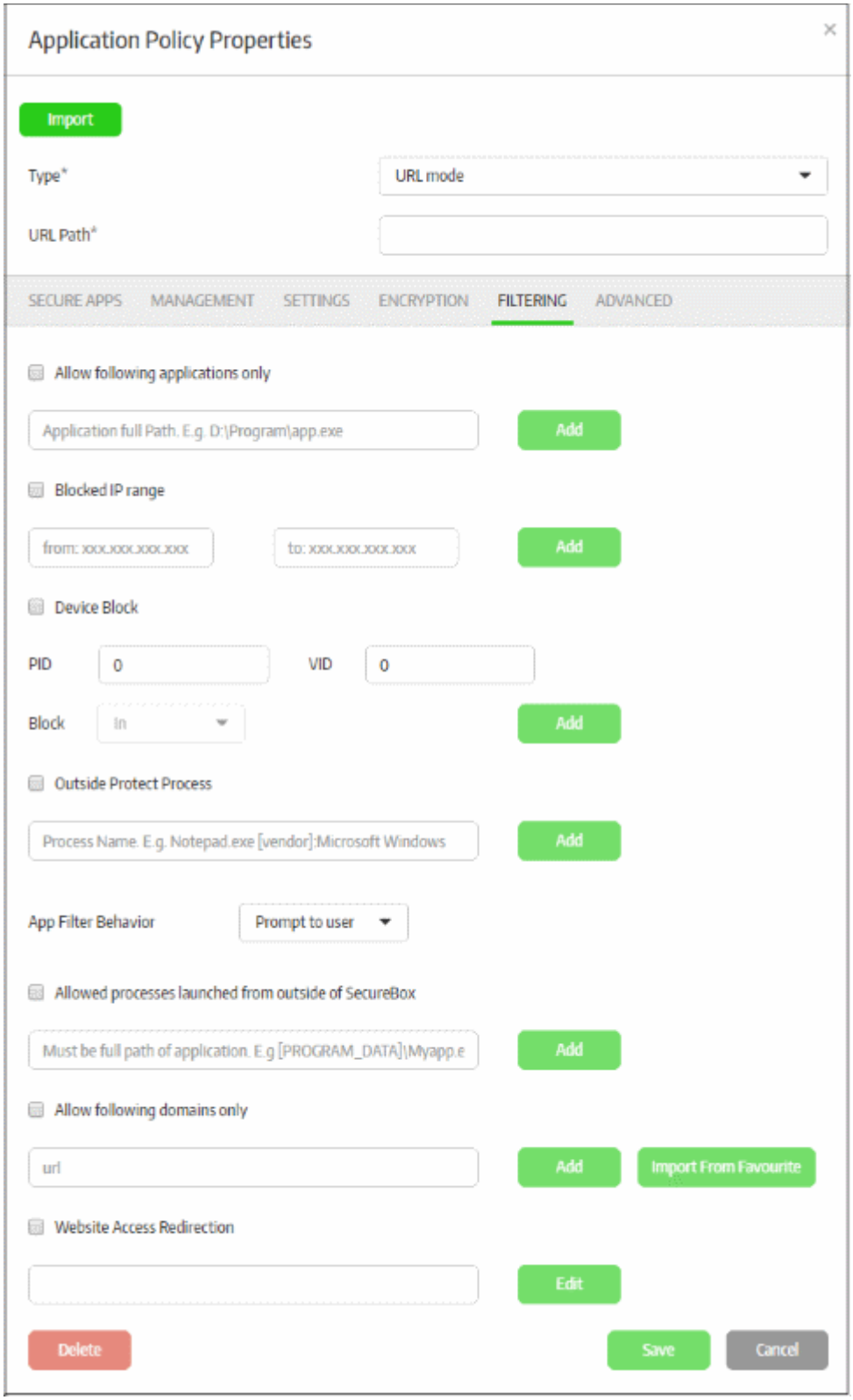
Policies - 'Encryption' Tab - Table of Parameters	
Parameter	**Description**
Protected Data Path	Enter the full path of the folder or drive that should be encrypted and click the 'Add' button. Repeat the process to add more folders. To remove a folder from the list, click the 'Remove' link beside it.
Set User Password	If selected, you can configure the user and admin password to open the encrypted folders
User Password	Enter the password for the user to open the folder
User Password Confirmation	Confirm the user password
Show Password	If selected, you can see the password details while entering
Admin Password	Enter the password for the administrator to open the folder
Admin Password Confirmation	Confirm the admin password

Show Password	If selected, you can see the password details while entering
Force Restart	When encryption is enabled, computer should be restarted to enable the encryption property in the endpoints. If this option is checked, user will not be able to use the secure application without restarting the endpoint.

Filtering Tab

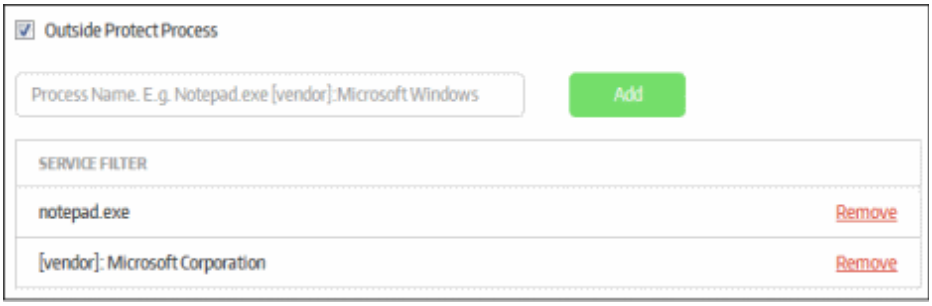
It is possible to open other programs, visit other URLs and so on from the secured environment. The 'Filtering' tab allows administrators to define filtering checks when creating a secured application, such as configuring to allow only certain applications, URLs to open in the secured environment. You can also configure to allow or not allow USB devices from accessing the secured application.

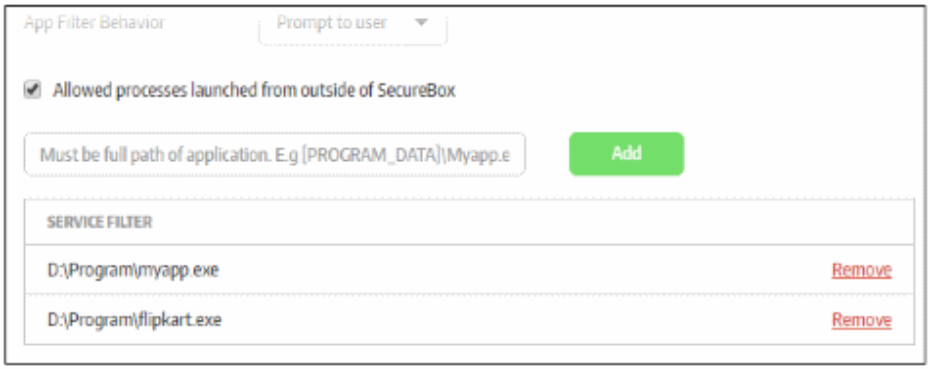
- Click the 'Filtering' tab.



Policies - 'Filtering' Tab - Table of Parameters	
Parameter	**Description**
Allow following applications only	If selected, only the added applications will be allowed to open in the secured environment for the secure application. Depending on the setting configured in 'App Filter Behavior', the opening of other applications will be blocked, allowed or displayed a warning to the user.

	• Enter the full path of the application that should allowed to run and click the 'Add' button. Repeat the process to add more applications.  • To delete an application from the list, click the 'Remove' link beside.
Blocked IP Range	If selected, the secure application prevents access to the sites with IP in the defined range. • Enter the IP range in the 'From' and 'To' fields and click the 'Add' button. Repeat the process to add more applications.  • To delete an IP range from the list, click the 'Remove' link beside.
Device Block	If selected, the secure application can be defined to block or allow devices based on their product ID (PID) and vendor ID (VID) numbers. • Enter the PID and VID numbers of the device in the respective fields • In the 'Block' drop down, select from the options: • In - The devices will not work inside the secure application, but will work in the host system.

	• Out - The devices will work inside the secure application, but will not work in the host system. • In & Out - The devices will not work for both the secure application and the host system. • Repeat the process to add more devices.  • To delete a device from the list, click the 'Remove' link beside. Please note that in order to make the blocked out device to work again in the host system, the configuration in the secure application should be changed or the CSB should be uninstalled.
Outside Protect Process	In addition to the protection for processes invoked by the secure application, you can configure protection for processes for applications running outside the secure application. This can be configured to protect a specific application or applications produced by a vendor. If an executable file name is entered, the specified program will be protected by CSB even when it's run outside of secure application. If a vendor name is entered, all the programs that are produced by this vendor will be protected even when they run outside of secure application. • Select the 'Outside Protect Process' check box • Enter the name of the application that you want to protect, for example, notepad.exe or enter the name of the vendor whose applications that you want to protect, for example, [vendor]: Microsoft Corporation, and click the 'Add' button. • Repeat the process to add more applications.  • To delete an entry from the list, click the 'Remove' link beside.
App Filter Behavior	The settings done here determine the action for the 'Allow following applications only' settings done above. There are three options available: • Allowed Anyway - Apps not configured in 'Allow following applications only'

	will be allowed to start • Block - Apps not configured will not be allowed to start • Prompt to user - A warning message will be displayed for the user to decide whether to allow or block apps that are not configured.
Allowed process launched from outside of Secure Box	Secure applications prevent outside process to start another process into secure application. For example, Windows Explorer may start another application(assume notepad.exe) into secure application. If it's not configured here, secure application will block this. To add applications that can be started outside SB, enter the full path of the application and click 'Add'.  • To delete an application from the list, click the 'Remove' link beside.
Allow following domains only	Available for 'URL mode' only. The user can open multiple sites from the configured browser. You can configure the websites that can be opened from the secured application. Select the 'Allow following domains only' check box. • Enter the website URL that you want allow from the secure application and click the 'Add' button. Repeat the process to add more domains.  • Click the 'Import From Favorite' button to add your favorite websites to the list. • To delete a domain from the list, click the 'Remove' link beside.
Website Access Redirection	Available for 'URL mode' only. You can configure to redirect websites that are opened in the secure URL app browser to other websites. • Select the 'Website Access Redirection' check box

- Click the 'Edit' button

- Enter the website that you want the user to be redirected from in the first field, for example, **www.badsite.com**
- Enter the website that you want the user to be redirected to in the second field, for example, **www.goodsite.com**
- Click the 'Add' button
- Repeat the process to add more websites

- To delete an entry from the list, click the 'Remove' link beside.
- Click the 'Save' button

The redirect details will be listed in the screen.

- To remove the redirect websites list, uncheck the 'Website Access Redirection' check box.

- Click the 'Save' button for your changes to take effect.

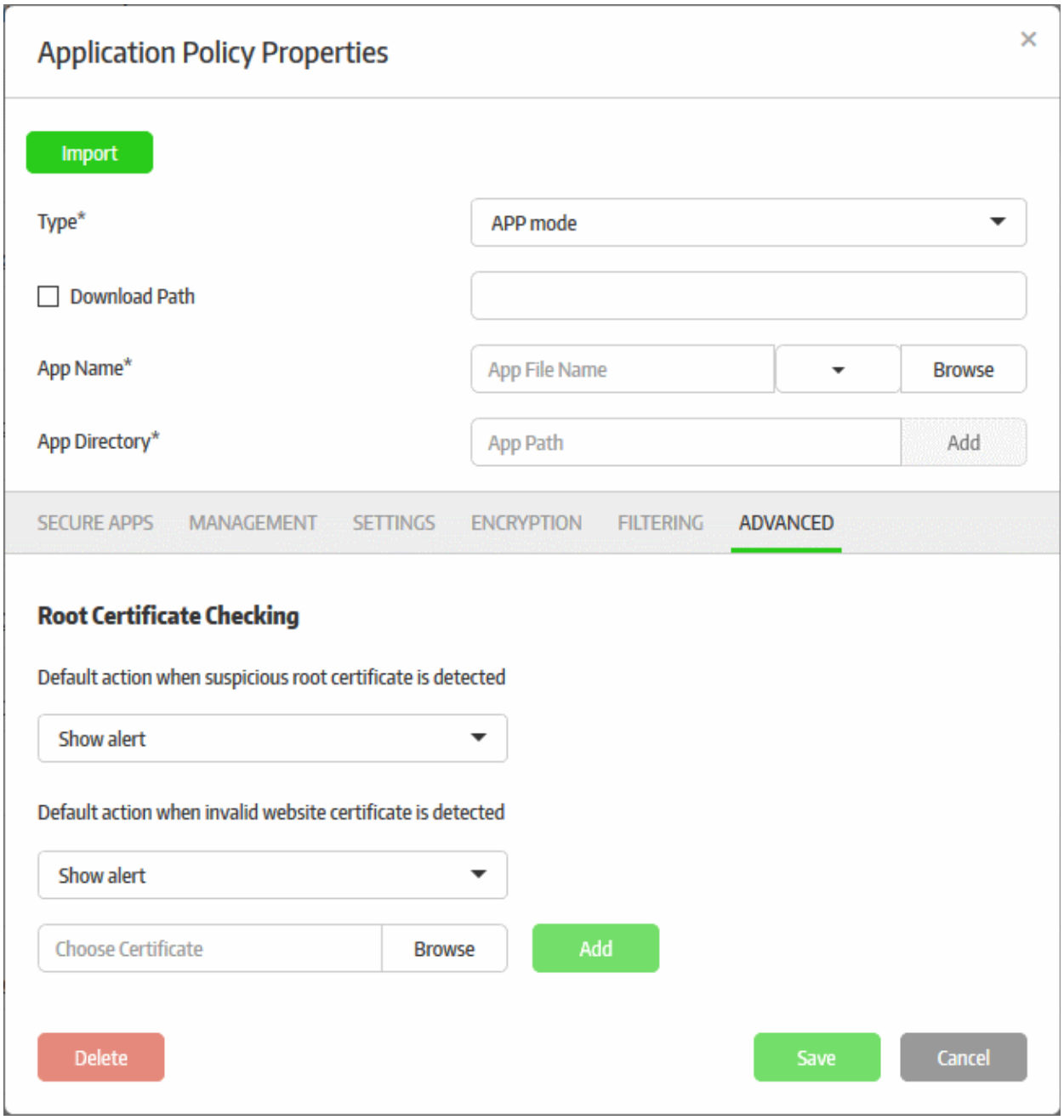
Advanced Tab

The 'Advanced' tab allows administrators to define actions to be taken for 'Root Cert Check' feature. Root certificate of all SSL connection in the protected application will be verified using a trusted root certificate list added to the management console. You can also add website certificates here in order to compare it with the certificate in the secure application. This is similar to certificate pinning that associates a host with their expected certificate or public key.

Please note that root certificate check and certificate checks are different. Root certificate check is for checking if the root certificate is in the trusted list and by default it checks the Microsoft Trust Certificate list. You can also configure

to check against a customized root certificate list from the 'Management' tab > Trusted Certificates List. The certificate check is used to compare the website information in the added certificate with the secure application website's certificate and ascertain if they are the same or not.

- Click the 'Advanced' tab.



Policies - 'Advanced' Tab - Table of Parameters	
Parameter	**Description**
Root Certificate Checking	
Default action when suspicious root certificate is detected	The setting done here determines the action for the 'Root Cert Check' feature in SECURE APPS tab > Protection. The options available are: • Show alert - An alert will be displayed to the user • Use Tor to bypass sniffers - Switches to Tor network to prevent the endpoint from malicious attack

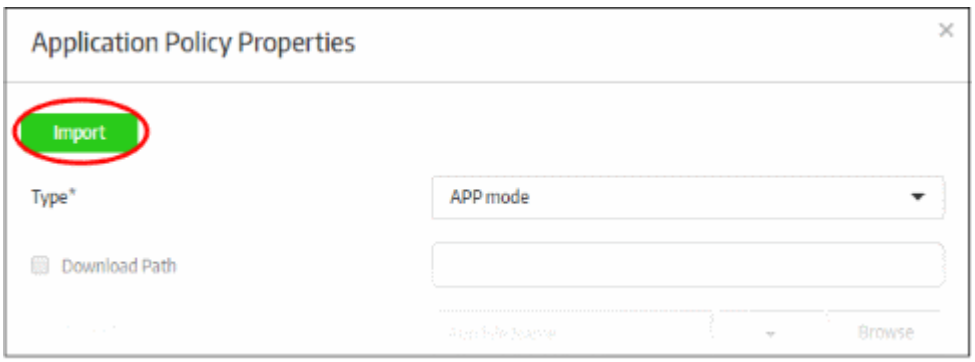
	• Ignore - The suspicious detection will be ignored • Block - The website will be blocked
Default action when invalid website certificate is detected	Allows you to configure the action for an invalid website certificate detection after comparing with website certificates added in the next field 'Choose Certificate'. The options are: • Show alert - An alert will be displayed to the user • Block - The website will be blocked
Add Website Certificates	The 'Choose Certificate' field allows you to add website certificates in order to compare and check with the secure application website's certificate. • Click 'Browse', navigate to the location where the website certificate is stored and click 'Open'. • Click 'Add'  • Repeat the process to add more website certificates • To delete a certificate from the list, click the 'Remove' link beside.

- Click the 'Save' button for your changes to take effect.

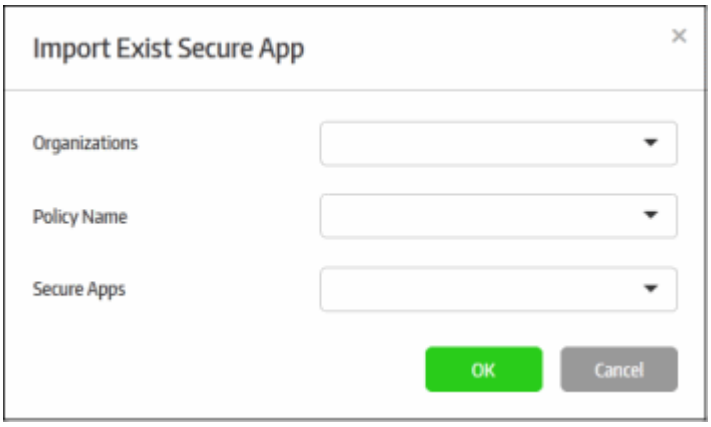
To create a new policy using an existing policy as a base

CMC allows administrators to create a new policy using the configuration of an existing secure app from a policy. This feature will be useful to roll out the policy with or without modifications to other endpoints groups per the organization's requirement.

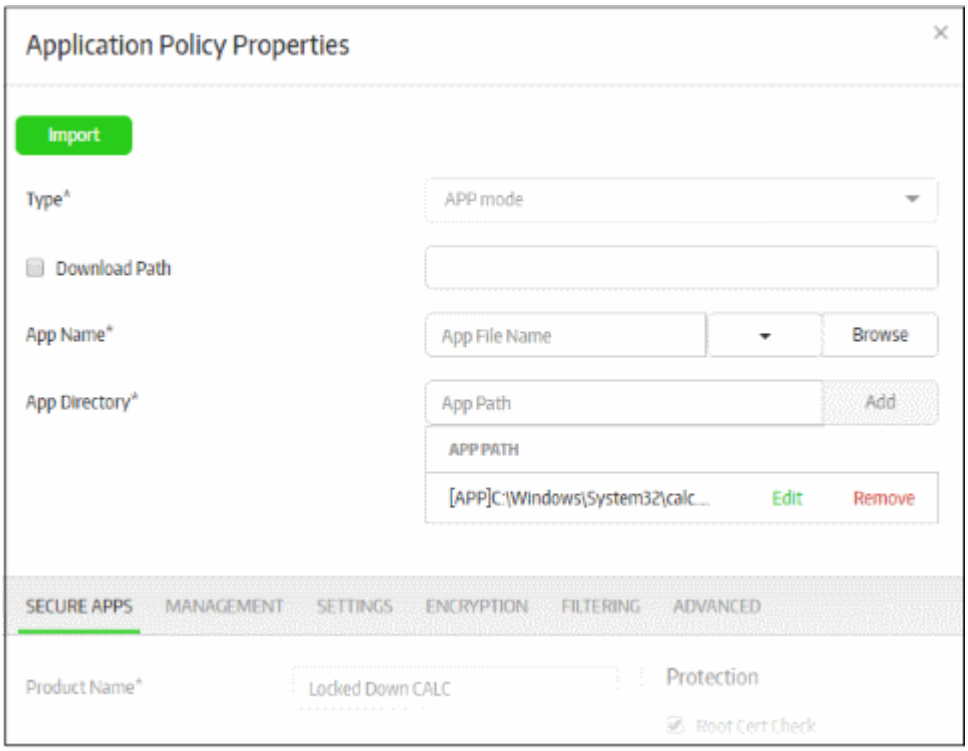
To import the settings of an existing policy, click the 'Add New' link or on the name of a secure app under 'Components' and click the 'Import' button at the top.



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'.

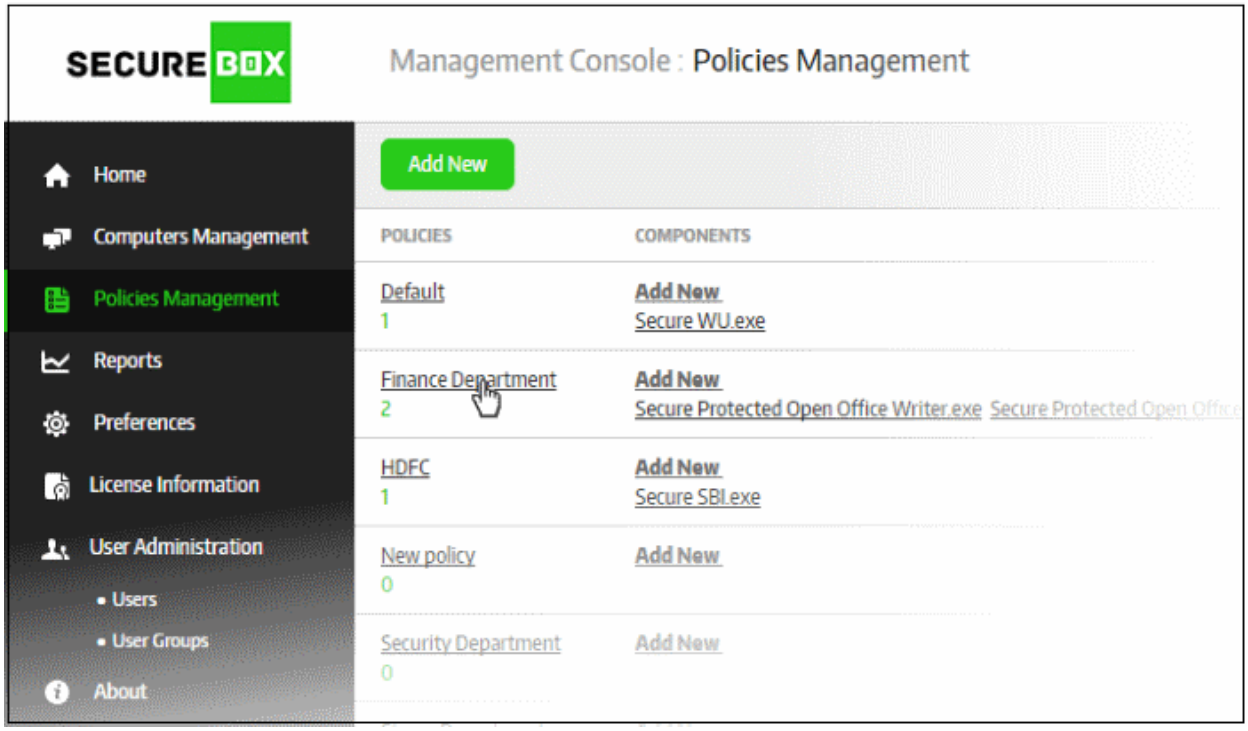


The secured item will be imported with all its settings including the product name. You can save it with the same settings or modify them according to the requirement. This is similar to the process explained for creating a new policy. **Click here** to know more about how to configure the settings in the imported policy.

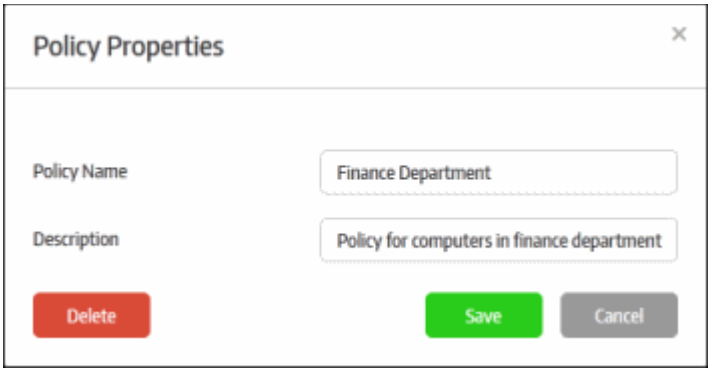
7.1.2. Edit a Policy

The management console allows you to edit a secure application policy so that changes will be applied to the endpoints in the next polling cycle. Endpoints will contact the management console at the time interval specified in '**Preferences**' to check for any policy updates.

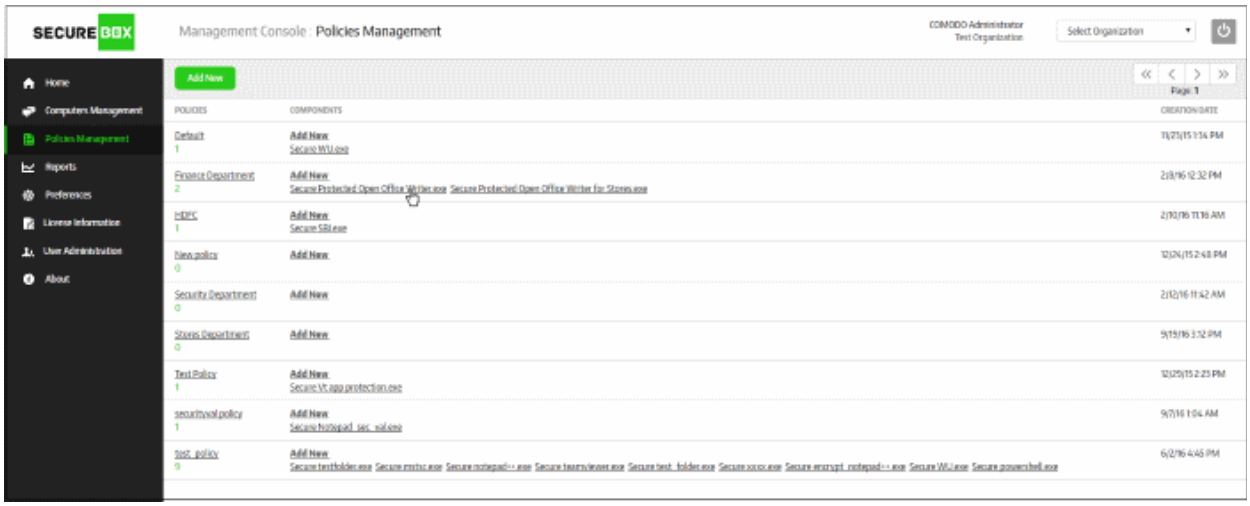
To edit a secure application policy name, click 'Polices Management' on the left and then the policy name that you want to edit.



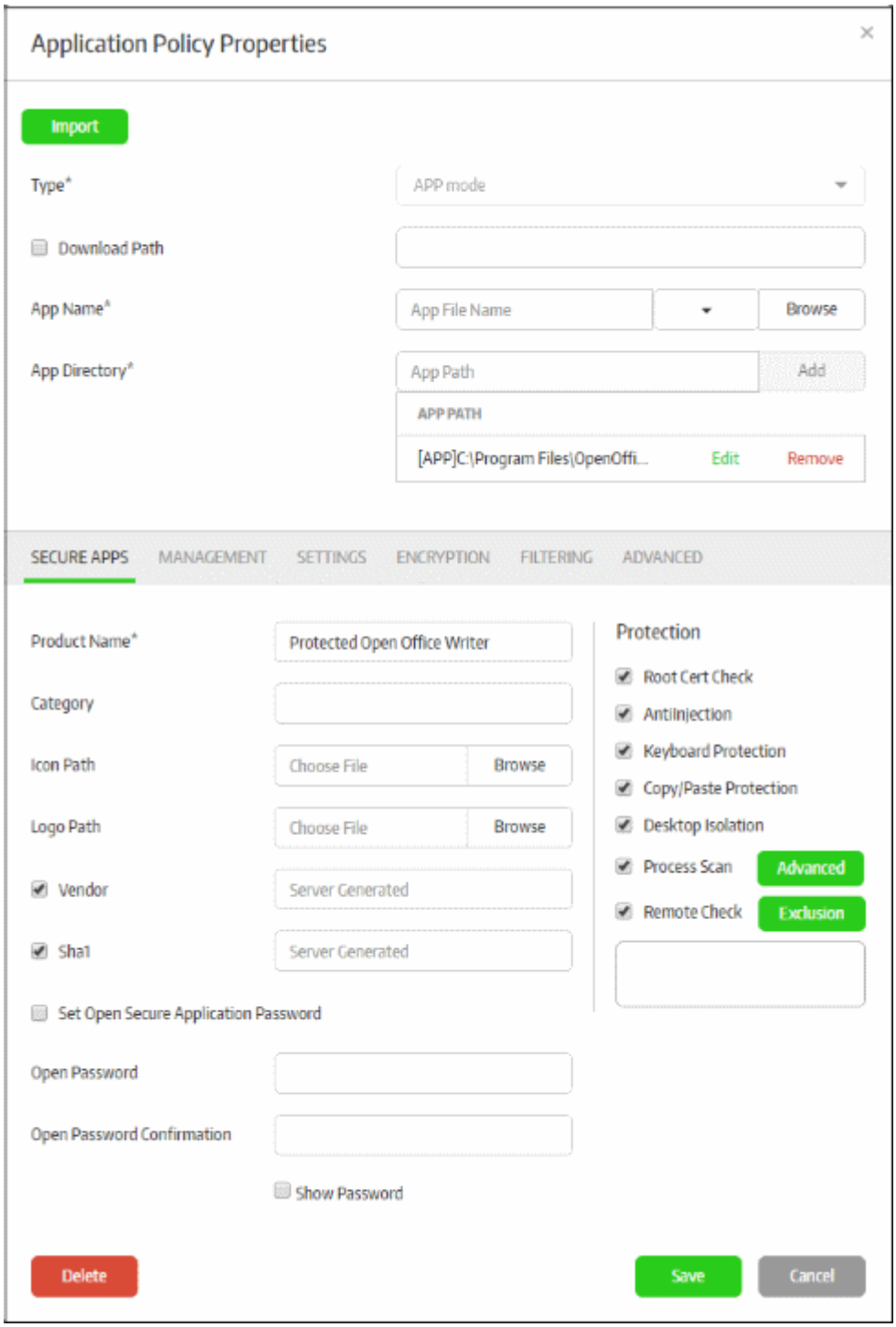
The 'Policy Properties' screen will be displayed.



- If required, edit the policy name and description and click 'Save'. Please note that you can edit the name and description of the default policies but cannot delete them.
- Next, click the name of the secure application whose settings you wish to edit:



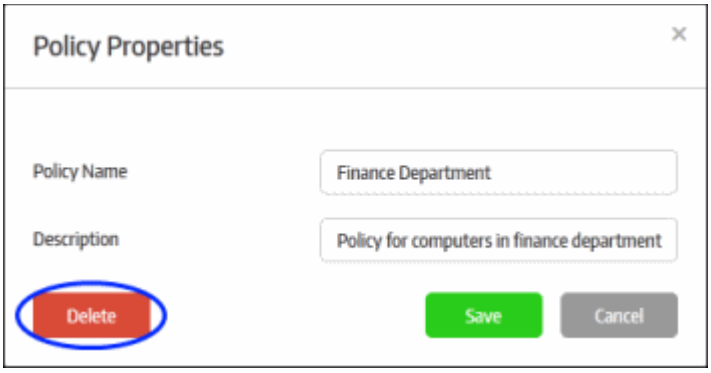
The 'Application Policy Properties' screen of the application will be displayed:



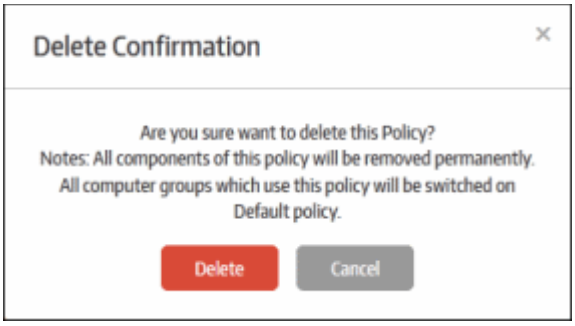
- If you change the protected item's settings details, then the 'Product Name' will remain the same, but CSB will update the secure application for the edited protected item.
- If you change the 'Product Name', then a new security application with the changed name will be created for the protected item with the same settings.
- The policy properties screen is the same as that which appears when creating a new secure application for a policy. Refer to '**Configuring Granular Secure Box Application Settings**' for more details about editing the settings under the configuration tabs.

To delete a policy

- Click on the policy name and then the 'Delete' button in the 'Policy Properties' dialog. Please note that you cannot delete the default policy.



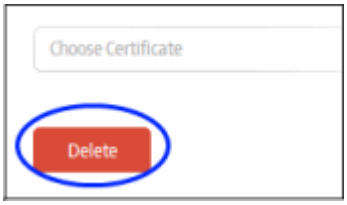
A confirmation dialog will be displayed.



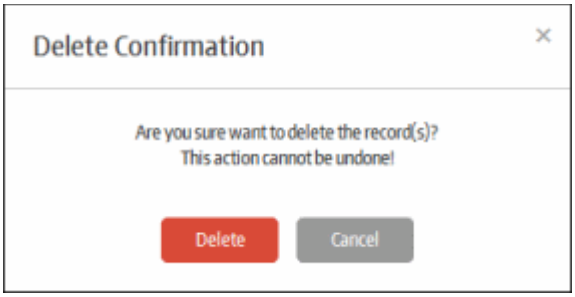
- Click 'Delete' to confirm removal of the policy. Please note the endpoints which used this policy will be given the default policy as replacement.

To delete a secure application in a policy

- Click the 'Delete' button that is available under all the tabs in the 'Application Policy Properties' screen



A confirmation dialog will be displayed.

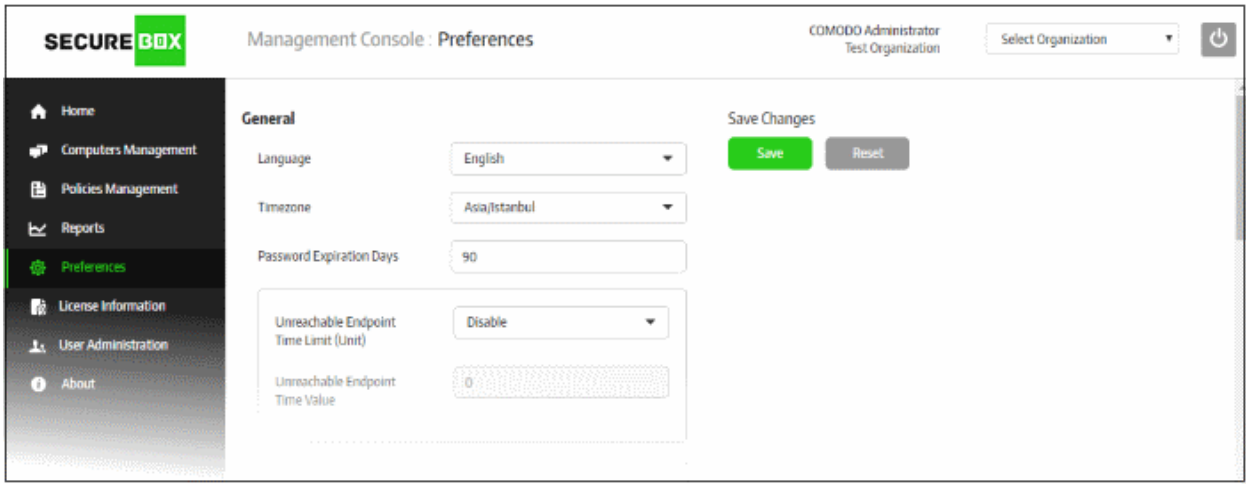


- Click 'Delete' to confirm removal of the security application

8. Configure the Management Console

The 'Preferences' section allows administrators to configure language, timezone, password expiry intervals, endpoint settings, reports, notifications and more.

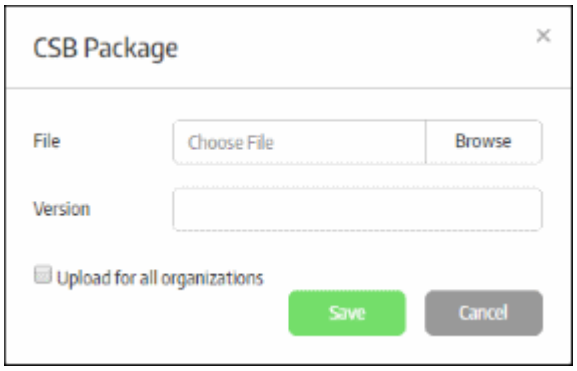
To configure preferences, click 'Preferences' on the left:



Preferences Settings - Table of Parameters	
Parameter	**Description**
General	
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	Set whether or not Secure Box protection should be disabled on an endpoint if it does not contact the management console for a certain period of time. For example, if this value is set to '1 Day', then applications will no longer launch in the CSB container if the endpoint does not communicate for a period of 24 hours. Protection will resume immediately after communications are restored. Endpoint installations regularly receive updates from the management console, so administrators may not want the CSB application to launch if it has not been updated for some time. If you select 'Disabled' in the drop-down, CSB will continue to operate on endpoints regardless of connection status to the management console.
Absent Time (Unit) 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 computer screen for endpoints

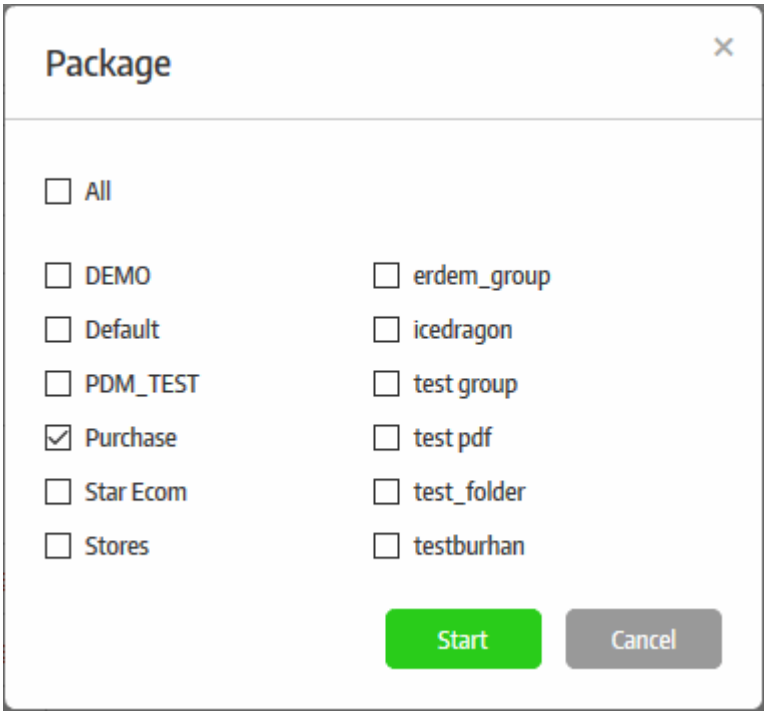
	that are not connected to CMC for more than a day, then select 'Days' from the Absent Time (unit) drop-down in the first box. Then, select '1' from the 'Absent Time Value' drop-down.
CMC Secure App Only	If selected, only secure applications from CMC can be run on endpoints. Secure applications copied from another policy or created with SAW (Secure Application Wizard) tool will not be allowed to run on endpoints.
Endpoint Settings	
Administrator Password for Open Secure App	Enter the password for administrators to open a secure application 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	If enabled, users will have to enter a password before they can uninstall CSB from an endpoint.
Administrator Password for Uninstall Secure App	Specify the password required for uninstalling CSB on endpoints.
Report Settings	
Remove Reports Older Than	The threat and activity reports for the account will be removed from the server as per the period set here. Select the period from the drop-down after which the reports will be removed.
Polling Interval Settings	
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	
Log Server	Global Log Server setting, used for the endpoint to send logs to. If it's set, the 'Log Server' on 'Management' tab will be filled with the global setting when creating a secure application.
Time Server	Global Time Server setting, used for the endpoints to sync-up their system time. If it's set, the 'Time Server' on 'Settings' tab will be filled with the global setting when creating a secure application.
Secure Box Installer Upgrade Server	Global Upgrade Server setting, used for uploading latest CSB installation files. If it's set, the 'Upgrade Server' on the 'Management' tab will be filled with the global setting when creating a secure application.
Packages	
Available Secure Box Versions	Displays the CSB installer versions that has been uploaded to the server. When enrolling endpoints, the uploaded installers will be available from the drop-down. Refer to the section '**Enrolling Endpoints for Management**' for more details.

- To upload the latest CSB installer package, click the 'Manual Upload' button



- 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 beside it.
- To upgrade CSB endpoints, select the package to be installed and click the 'Upgrade' button.

The 'Package' dialog will appear

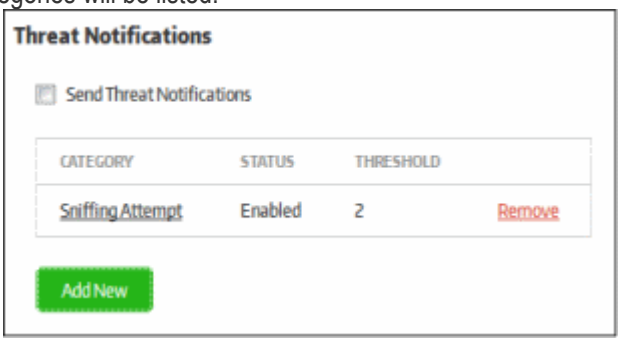
	 • Select the organization whose endpoints required the upgrade and click 'Start' A schedule will be created for the update. • If there was a problem during installation, or if the application is corrupted or malfunctioning, select the relevant package(s) and click the 'Repair' button. The 'Package' dialog will appear • Select the organization whose endpoints require the repair and click 'Start' A schedule will be created for upgrading all endpoints enrolled to the organization for diagnosis and repair.
E-Mail Notifications	
Send E-Mail Notifications	If selected, email notifications to the configured addresses will be sent for the enabled categories such as threat, activities and licenses.
E-Mail Address(es)	Enter the email addresses of the administrators to whom the configured notifications should be sent.
Threat Notifications	
Send Threat Notifications	If selected, the threat notifications will be sent to the subscribed administrators. Please note that 'Send E-Mail Notifications' should be enabled for the alerts to be sent.
Configure Threat Notifications	You can configure the threat notifications by clicking the 'Add New' button in the 'Threat Notifications' section.

- Category - The name of the threat category. The available categories are:
  - Fake Certificate
  - Remote Detected
  - Malware Terminated

Enter the threat category name in the field. Please note the **logs** for these threat categories should be enabled in the endpoint **Group Properties** dialog.

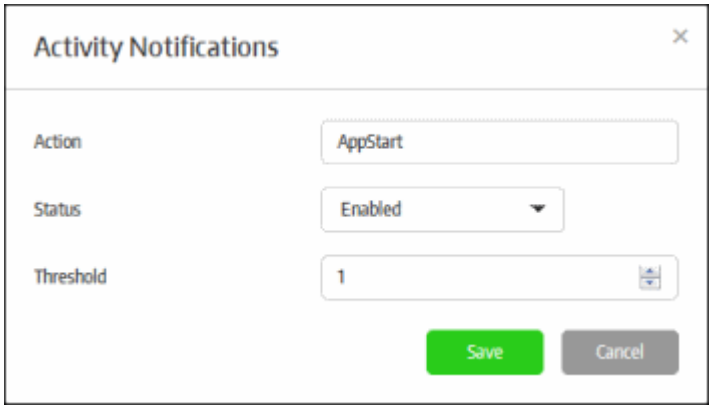
- Status - Select whether you want to enable or the disable the notification to be sent.
- Threshold - Enter the threshold number of threats or increase/decrease the value from the combo box for sending the notifications.
- Click the 'Save' button.

The threat categories will be listed.



- To edit a threat category, click on the name and edit as required.
- To remove a threat category from the list, click the 'Remove' link beside it.

Activity Notifications	
Send Activity Notifications	If selected, the activity notifications will be sent to the subscribed administrators. Please note that 'Send E-Mail Notifications' should be enabled for the alerts to be sent.
Configure Activity Notifications	You can configure the activity notifications by clicking the 'Add New' button in the 'Activity Notifications' section.

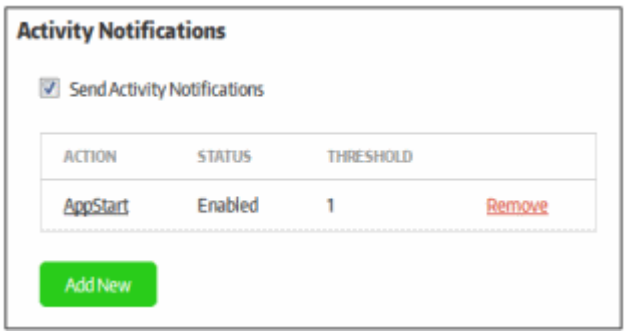


- Action - The name of the action category. The available actions are:
  - Install
  - Uninstall
  - Upgrade
  - App Start
  - Network Changed
  - Switch Out
  - Switch In
  - Exit Application
  - Integrity Check Failed

Enter the activity action name in the field. Please note the **logs** for these events should be enabled in the endpoint **Group Properties** dialog.

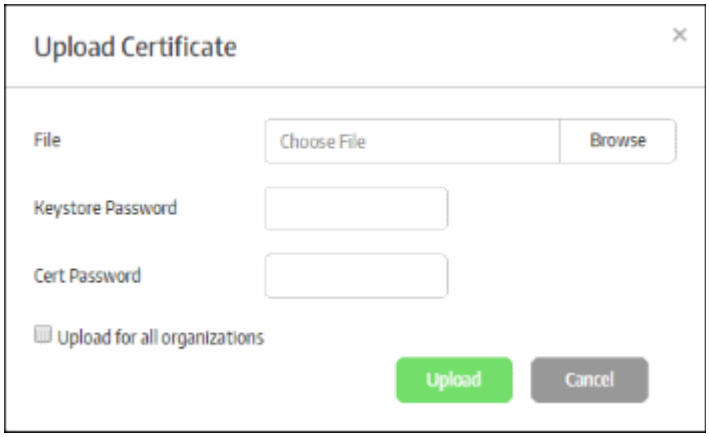
- Status - Select whether you want to enable or the disable the notification to be sent.
- Threshold - Enter the threshold number of actions or increase/decrease the value from the combo box for sending the notifications.
- Click the 'Save' button.

The action categories will be listed



- To edit an action category, click on the name and edit as required.
- To remove an action category from the list, click the 'Remove' link beside it.

License Notifications	
Send License Notifications	If selected, a license notification will be sent to the subscribed administrators if the number of enrolled endpoints in percentage with respect to the purchased license satisfies the condition in the 'Inform after 'N%' licenses are used'.

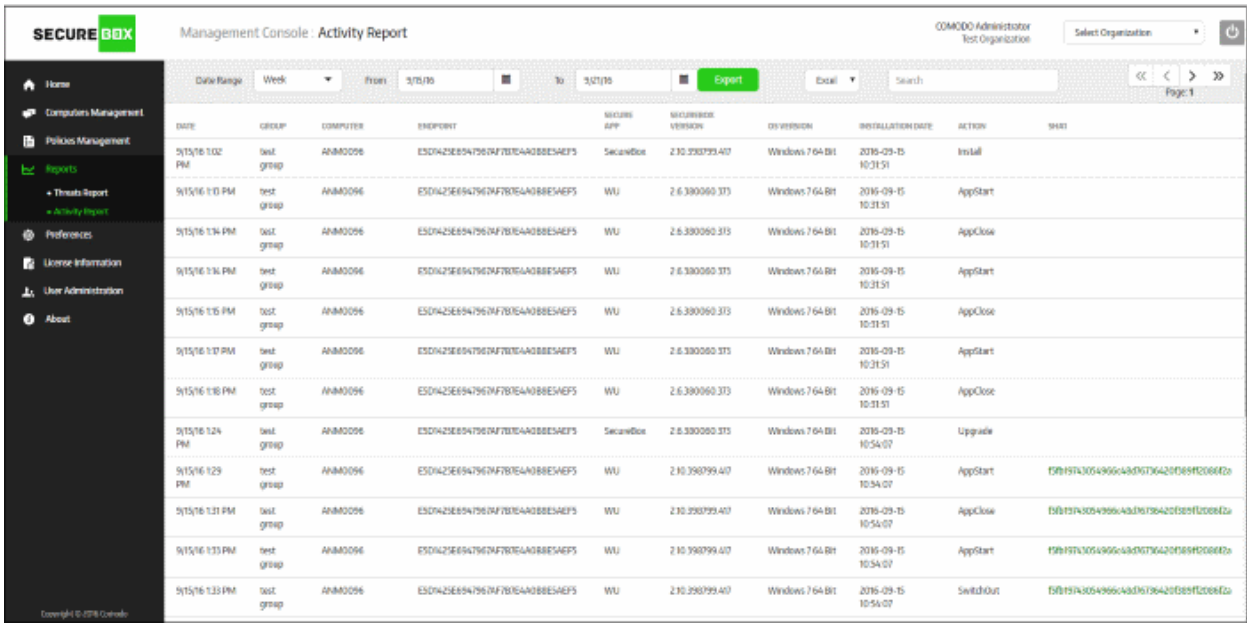
	• Select the percentage of enrolled endpoints from the 'Inform after 'N%' license are used' drop-down.
SMTP Settings - Allows to configure the mail server for sending out notifications	
Email Host	Enter the SMTP server from which the notification mails are to be sent
Email Port	Enter the outgoing port 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 to configure 'Active Directory' and 'Workgroup' in order to enroll endpoints within a network	
Discovery From	The options available are 'Active Directory' and 'Workgroup' If 'Active Directory is selected, provide the following details: • Domain to scan - Enter the domain name of the AD • Host - The host name or IP address of the AD server • Username - The username of an administrative account to access the AD server • Password - The password for the account If 'Workgroup' is selected, provide the following details: • Workgroup Name - Enter the name of the workgroup in the network
Discovery Period	Determines the scanning intervals by the management console for auto-discovery in the network. Select the scanning interval from the drop-down. If 'Disabled' is selected, then no scanning will be performed.
Code Signing Certificate	
	The certificate used to sign the created secure applications, so that the secure application can be authorized to run on endpoints. CSB will check the certificate. Code signing certificate part is divided into 2 parts: SHA2 and SHA1 certificate. Secure applications will be signed with both of the certificates if they are configured. SHA1 certificate is needed for secure applications to be used in Win XP. • To upload a certificate, click the 'Upload' button  • 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 the details will be displayed under the 'Code Signing Certificate' section. This certificate will be used for creating a new secure app each time. • To revoke the existing code signing certificate, click the 'Revoke' button. Please note a valid code signing certificate should be uploaded in order to sign the secure applications.

- Click the 'Save' button to apply your changes.

9. Reports

The 'Reports' section provides administrators the details of threats detected and the activity on the endpoints while running the secure apps. The 'Threats' reports provides the details of threats detected such as malware, fake certificate and remote attempt. The 'Activity' reports provides the details of 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 following sections for more details:

- **Threats Report**
- **Activity Report**

9.1. Threats Report

The 'Threats Report' interface provides a comprehensive report of threats that were encountered by the secure applications. The details include the name of the endpoint and its ID assigned by the management console, the details of secure applications, when the CSB was installed and more. The report for the threat categories generated

here for the computer groups depends on the settings configured in the **log filter** section of the **computer group properties** dialog. The available threat categories are:

- Fake Certificate
- Remote Detected
- Malware Terminated

The logs for the selected threat categories will be received by the management console and saved into database. Reports can be generated for different time periods and the data will be fetched from the database. Report data will be empty if a threat category was disabled in **log filter** for the selected report generation period. For example, if you had disabled 'Fake Certificate' last week, no data for this category will be available in the generated report for the period last week. However, data will available in the generated reports for other time periods when the category was in enabled status.

To view the threat report, click 'Reports' on the left and then 'Threats Report' below it:

Threat Report - Table of Column Description	
Column	**Description**
Date	The date and time of threat recorded on the endpoint
Group	The computer group to which the endpoint belongs. Refer to the section '**Managing Endpoint Groups**' for more details.
Computer	The name of the endpoint that was detected by CSB on enrollment. Refer to the section '**Enrolling Endpoints for Management**' for more details.
Endpoint	The ID for the endpoint assigned by CSB on enrollment.
Threat Name	The application name which is detected as a threat, for example, AKLT.exe, Windows Remote Desktop and so on.
Malware Name	The malware name, which is the result of FLS scan. But not every threat log has the Malware name, for example, remote detect is a threat log but it has no malware name.
Threat Category	The category of the threat that was recorded on the enrolled endpoints: • Malware Terminated - A malware was detected and terminated by CSB • Remote Detected - Remote attempt was detected on the endpoint • Fake Certificate - An invalid certificate is detected when endpoint browses a website For configuring the threat email notifications, the name of the threat category should be provided in the 'Category' row in the 'Preferences' interface > 'Threat Notifications' > 'Add New' button. Refer to the section '**Configuring the Management Console**' for more details.
SecureBox Version	The details of the CSB version that is installed on the endpoints.

Installation Date	The date and time when the CSB was installed on the endpoints
Secure App	The name of the secure application for which the threat was recorded.
OS Version	The details of the endpoint's operating system.
SHA1	The SHA1 value of the secure application.

Sorting, filtering and searching options

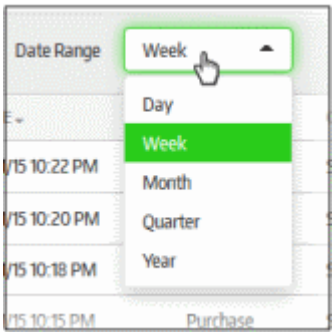
Sorting the entries

Clicking any column heading sorts the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using the filter option

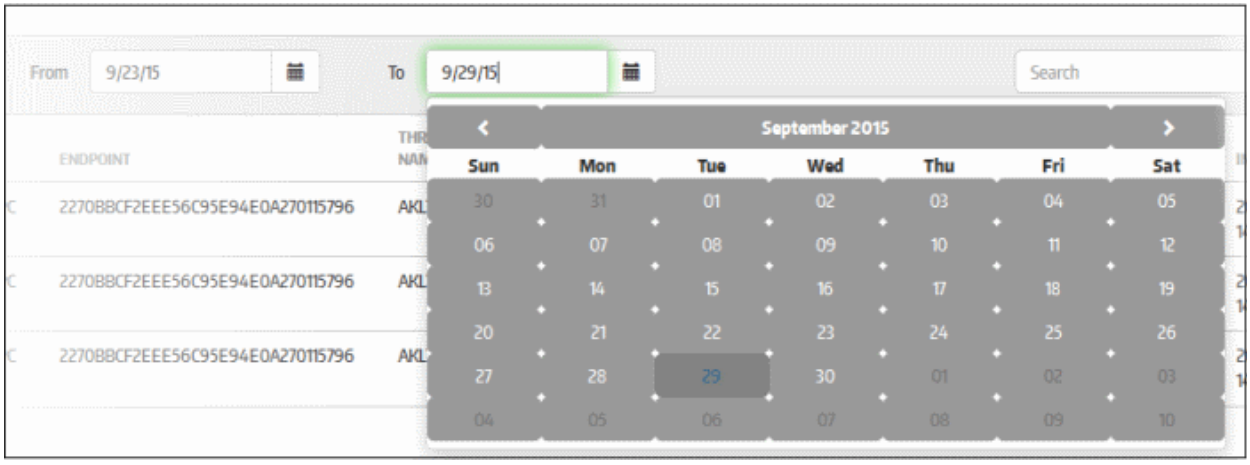
The threat report can be filtered using the date range and can be further filtered by providing the 'From' and 'To' dates. Please note the availability of past reports (up to one year) depends on the settings configured in 'Report Settings' from the '**Preferences**' screen.

- Click the 'Date Range' drop-down box.



By default, 'Week' will be selected for the date range and the dates in the 'From' and 'To' will be for the last 7 days and the results displayed.

- To refine the search further, provide the 'From' and 'To' dates by clicking on the combo boxes and selecting the dates from the calendar.

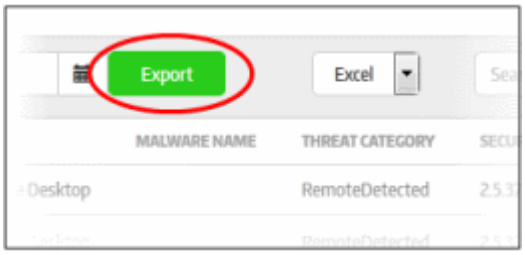


The results will be displayed per the dates and the date range selected. For example, if the selected date range is 'Week', the results will be displayed for 7 days or less according to the dates selected.

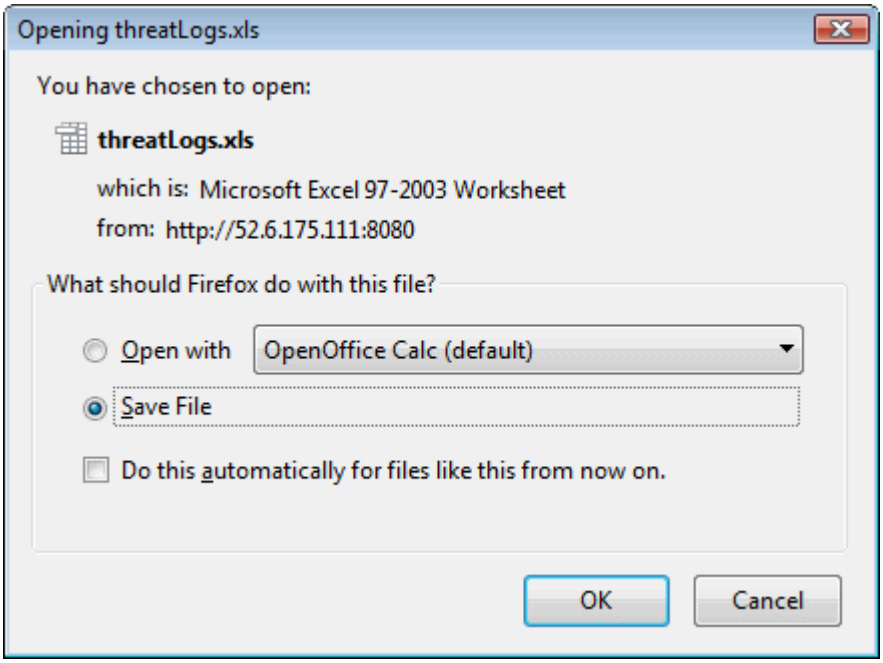
To export the report

CMC allows administrators to save the generated threat report to your system.

- Click the 'Export' button (currently only .xls format is supported)



You can choose to save the file or open with any spreadsheet application.



- Click 'OK'

The file will be saved in your default download location.

Using the search option

- Enter the search details of items under any of the columns in the box fully or partially.

The search will begin automatically and results displayed.

9.2. Activity Report

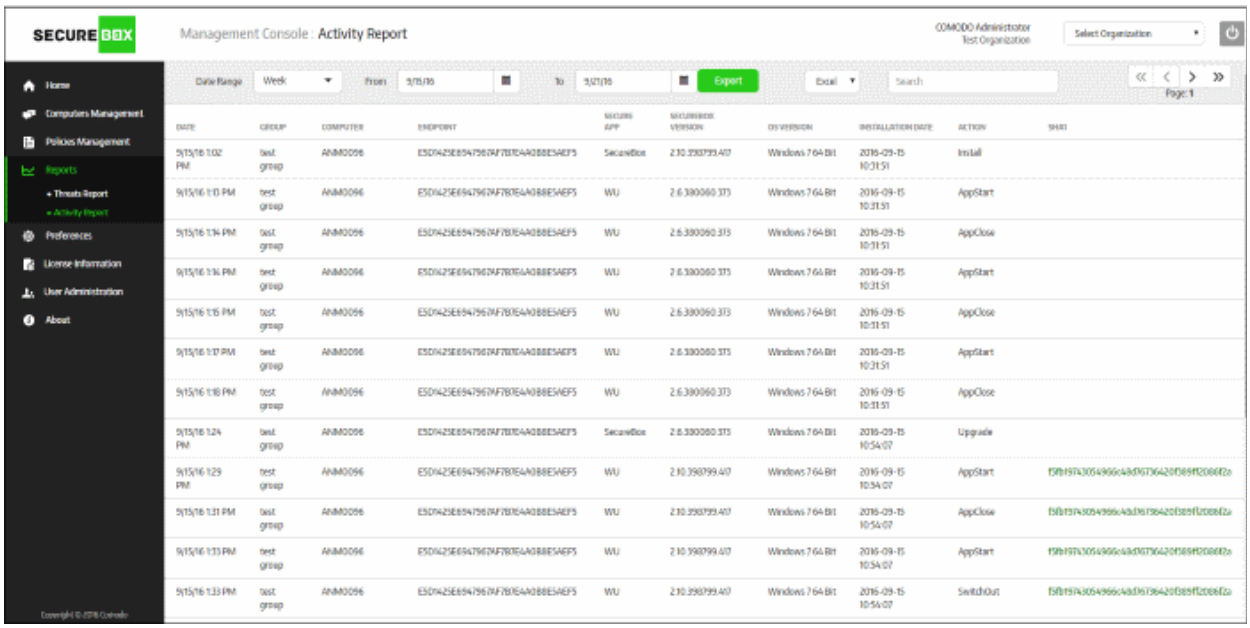
The 'Activity Report' interface provides a comprehensive report of actions that have taken place on enrolled points for an account. The details include the name of the endpoint and its ID assigned by the management console, the details of secure applications, when the CSB was installed and more. The report for the activities generated here for the computer groups depends on the settings configured in the **log filter** section of the **computer group properties** dialog. The available activities are:

- App Start - Indicates a secure application is started
- Exit Application - Indicates a secure application is closed
- Network Changed - Indicates the endpoint IP address changed to another subnet.
- Switch In - Indicates the switching in from Windows desktop to the CSB environment
- Switch Out - Indicates the switching out from CSB environment to Windows desktop
- Install - The CSB was installed
- Uninstall - The CSB was uninstalled

- Upgrade - The CSB is updated to the latest version
- Integrity Check Failed - Indicates the failure of integrity check when a secure app was launched. When a secure app is started, CSB will check the secure environment and will produce a log if the check fails.

The logs for the selected activities will be received by the management console and saved into database. Reports can be generated for different time periods and the data will be fetched from the database. Report data will be empty if an activity log was disabled in **log filter** for the selected report generation period. For example, if you had disabled 'Network Changed' last week, no data for this activity will be available in the generated report for the period last week. However, data will available in the generated reports for other time periods when the activity log was in enabled status.

To view the activity report, click 'Reports' on the left and then 'Activity Report' below it:



Activity Report - Table of Column Description	
Column	**Description**
Date	The date and time of activity on the endpoint
Group	The computer group to which the endpoint belongs. Refer to the section '**Managing Endpoint Groups**' for more details.
Computer	The name of the endpoint that was detected by CSB on enrollment. Refer to the section '**Enrolling Endpoints for Management**' for more details.
Endpoint	The ID for the endpoint assigned by CSB on enrollment.
Secure App	The name of the secure application for which the activity is recorded.
SecureBox Version	The details of the CSB version that is installed on the endpoints.
OS Version	The details of the endpoint's operating system
Installation Date	The date and time when the CSB was installed on the endpoints
Action	The name of the activity that was recorded on the enrolled endpoints: • AppStart - Indicates a secure application is started • ExitApplication - Indicates a secure application is closed • Network Changed - Indicates the endpoint IP address changed to another subnet.

	• SwitchIn - Indicates the switching in from Windows desktop to the CSB environment • SwitchOut - Indicates the switching out from CSB environment to Windows desktop • Install - The CSB was installed • Uninstall - The CSB was uninstalled • Upgrade - The CSB is updated to the latest version • Integrity Check Failed - Indicates the failure of integrity check when a secure app was launched. When a secure app is started, CSB will check the secure environment and will produce a log if the check fails. For configuring the activity email notifications, the name of the activity should be provided in the 'Action' column in the 'Preferences' interface > 'Activity Notifications' > 'Add New' button. Refer to the section '**Configuring the Management Console**' for more details.
SHA1	The SHA1 value of the secure application.

Sorting, filtering and searching options

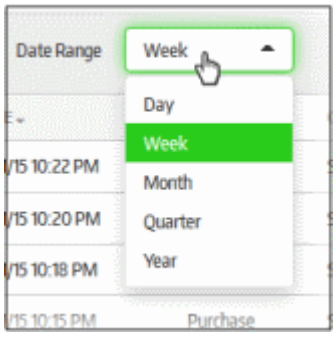
Sorting the entries

Clicking any column heading sorts the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using the filter option

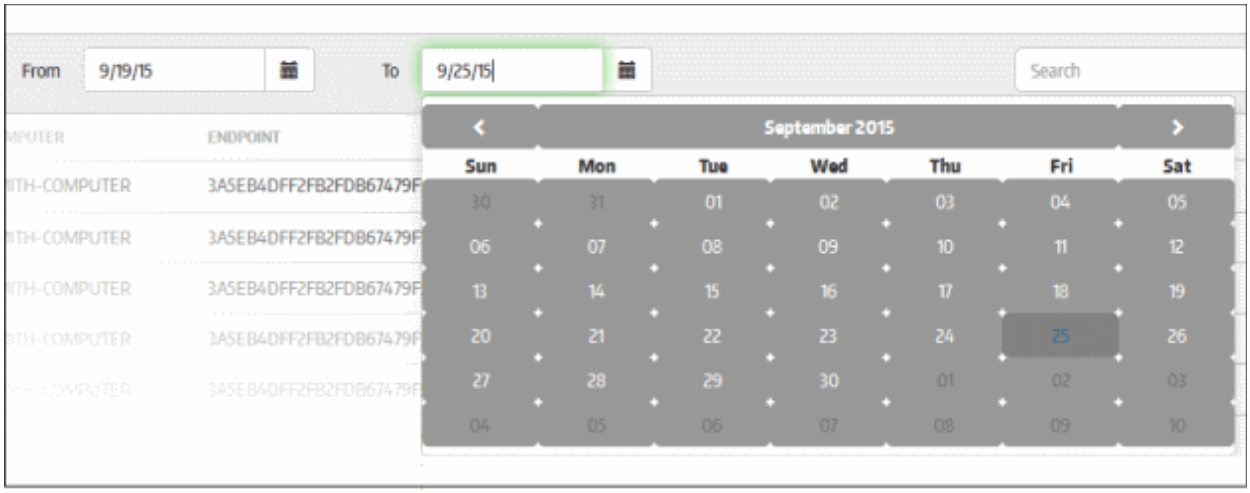
The activity report can be filtered using the date range and can be further filtered by providing the 'From' and 'To' dates. Please note the availability of past reports (up to one year) depends on the settings configured in 'Report Settings' from the '**Preferences**' screen.

- Click the 'Date Range' drop-down box.



By default, 'Week' will be selected for the date range and the dates in the 'From' and 'To' will be for the last 7 days and the results displayed.

- To refine the search further, provide the 'From' and 'To' dates by clicking on the combo boxes and selecting the dates from the calendar.

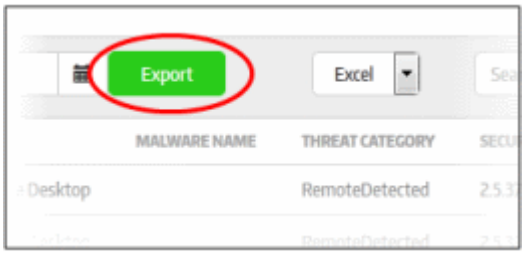


The results will be displayed per the dates and the date range selected. For example, if the selected date range is 'Week', the results will be displayed for 7 days or less according to the dates selected.

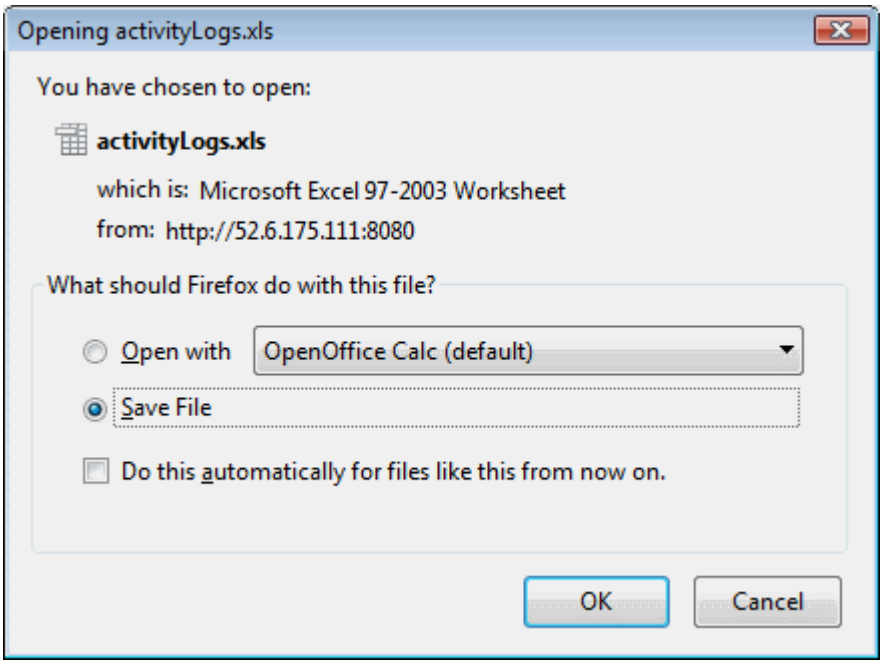
To export the report

CMC allows administrators to save the generated threat report to your system.

- Click the 'Export' button (currently only .xls format is supported)



You can choose to save the file or open with any spreadsheet application.



- Click 'OK'

The file will be saved in your default download location.

Using the search option

- Enter the search details of items under any of the columns in the box fully or partially.

The search will begin automatically and results displayed.

10. License Information

In order to use the CSB, enroll endpoints, assign polices so as to add secure applications, the organization must have a subscribed license from Comodo. Administrators can add multiple licenses for an account if the need arises such as an increase in the number of endpoints to be added. 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 open the 'License Information' page, click 'License Information' on the left:

License Information - Table of Column Description	
Column	**Description**
License Key	Displays the details of the subscribed license key. Clicking the link will display the full details. Refer to '**View the details of current license**' for more information.
Used	The number of endpoints that are installed the CSB.
Total	The total number of endpoints that are subscribed for the current license.
Starts	Indicates the start period of the license.
Expires	Indicates the expiry date of the license.
Status	Indicates whether the license is valid or expired.
Warranty	The link 'Active' is used to activate a license key. Please note currently this feature is not supported and will be available in the next version.
Control Buttons	
Buy License(s) Online	Allows to purchase CSB licenses from Comodo via their website. Refer to '**Buy a new license**' for more information.
Add License	Allows administrators to add license(s). Refer to '**Add a license**' for more information.

Sorting option

Sorting the entries

Clicking any column heading sorts the entries based on the ascending/descending order of the entries as per the

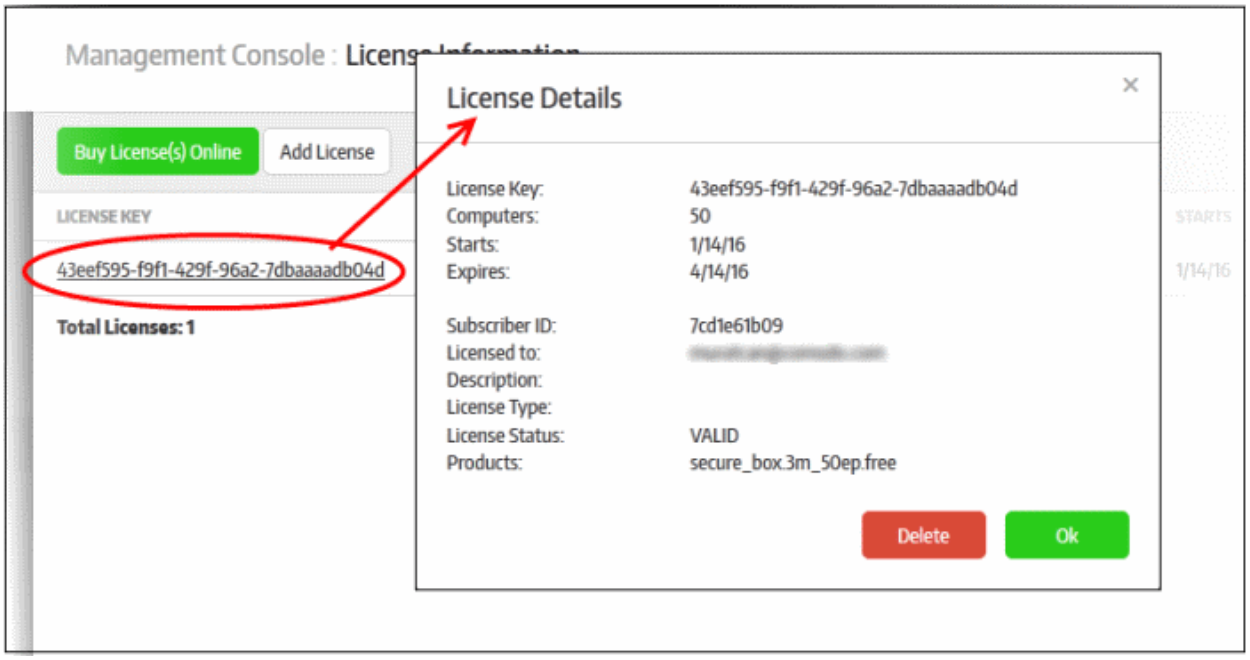
information displayed in the respective column.

The 'License Information' interface allows administrators to:

- **View the details of current license**
- **Add a license**
- **Buy a new license**

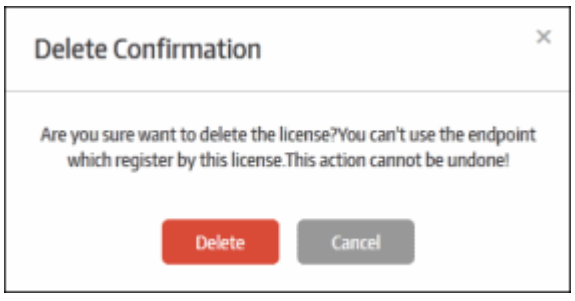
Viewing your Current License

- Clicking on the license key link in the screen will display the details dialog



The 'License Details' provides more additional information such as 'Subscriber ID', the email address of the account, 'License Type', 'Products' and more.

- Click 'Ok' to close the dialog and return to 'License Information' screen.
- To delete the license, click the 'Delete' button. Please note a valid license should be available for the continued CMC management.

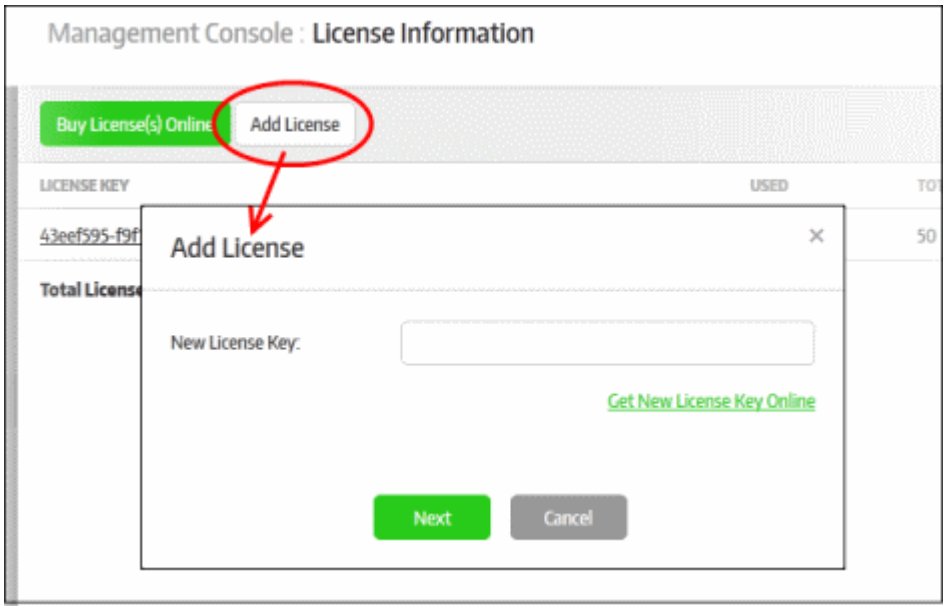


- Click 'Delete' to remove the license from the list.

Adding a License

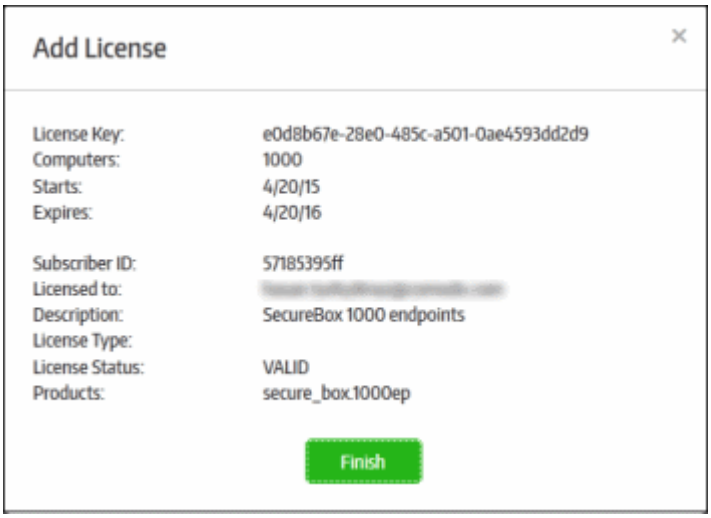
Administrators can add multiple CSB license for the same account if required to enroll more endpoints or renew the subscription that is expired.

- Click the 'Add License' button at the top



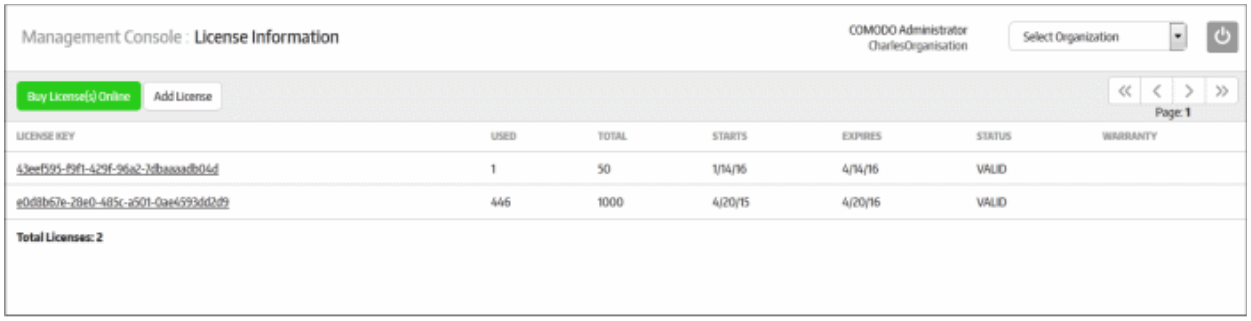
- Enter the license key that you would have received in the registered email address and click the 'Next' button.

The license key will be verified and if found valid, the 'Add License' dialog will be displayed.



- Click the 'Finish' button

The new license key will be added and displayed:



Buying New Licenses

The interface allows administrators to buy new licenses.

- Click the 'Buy License(s) Online' button at the top

You will be taken to the purchase page at **https://accounts.comodo.com/secure_box/management/signup**

- Select the product from the drop-down, provide the customer information and complete the payment procedure.

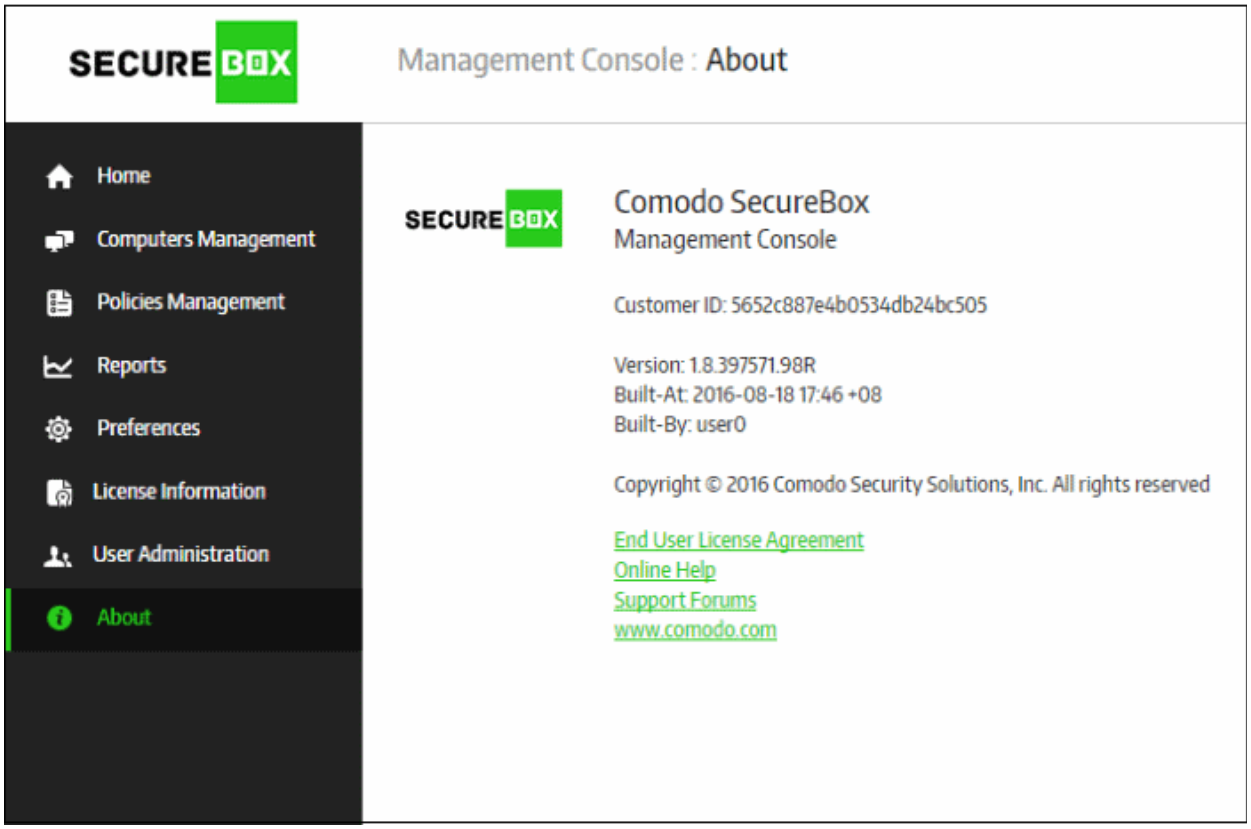
The license key will be mailed to your registered email address and you can also view the details from your account at **https://accounts.comodo.com**

The license key has to be entered in the 'License Information' page as explained above.

11. Management Console Details and Support

The 'About' screen displays the details of the management console including its version number, customer ID and also allows administrators to read the End User License Agreement (EULA). It has links to online help guides and support forums for product support.

To view details of the management console, click 'About' on the left:



The lower section of the screen allows to read the EULA, open online help guide and post your queries in the support forums:

End User License Agreement

- Click the link and read the EULA fully

Online Help Guides

Comodo's online help guides available at help.comodo.com contains guides for all its products. You can navigate to the required guide from the main page. To open the CSB help guides from this interface, click the 'Online Help' link.

Support Forums

Find the answers to your questions online at http://forums.comodo.com.

Register at Comodo Forums and join thousands of other users discussing all aspects of our products.

You'll benefit from the expert contributions of developers and fellow users alike and can find answers to any questions you may have. **Join the forums now**.

If you are an enterprise, then visit, **https://forum1.comodo.com**

Email Support

If you are unable to find a solution in either the help guide or the forums, then please email support at **techsupport@comodo.com**

Submit a Ticket

You can also submit a ticket by visiting **https://support.comodo.com/**, the Comodo support web page, an online knowledge-base and support ticketing system. The fastest way to get further assistance in case you find any problem using CSB management console.

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**