

**COMODO**  
Creating Trust Online®



# Comodo Device Manager

Software Version 5.0

## Quick Start Guide

Guide Version 5.0.010516

Comodo Security Solutions  
1255 Broad Street  
Clifton, NJ 07013

# Comodo Device Manager - Quick Start

This tutorial explains how to use Comodo Device Manager (CDM) to add users, enroll devices, create device groups and create/deploy device configuration profiles:

**Step 1 - Login to the Admin Console**

**Step 2 - Add Users**

**Step 3 - Enroll Users' Devices**

**Step 4 - Create Groups of Devices (optional)**

**Step 5 - Create Configuration Profiles**

**Step 6 - Applying profiles to devices or device groups**

**Note:** This guide assumes you have already completed Comodo Device Manager set up and activation, and have acquired an Apple Push Notification (APN) certificate (iOS devices) and/or Google Cloud Messaging (GCM) token (Android devices). Refer to the online guide at <https://help.comodo.com/topic-214-1-633-8155-Comodo-Device-Manager---Cloud-Portal-Setup-Guide.html> if you need to find out more about adding APN certificates and GCM tokens.

## Step 1 - Login to the Admin Console

The Comodo Device Manager (CDM) console can be viewed in any Internet browser.

- Enter the URL of your portal and the login credentials received through your Portal creation confirmation mail.



## Step 2 – Add User

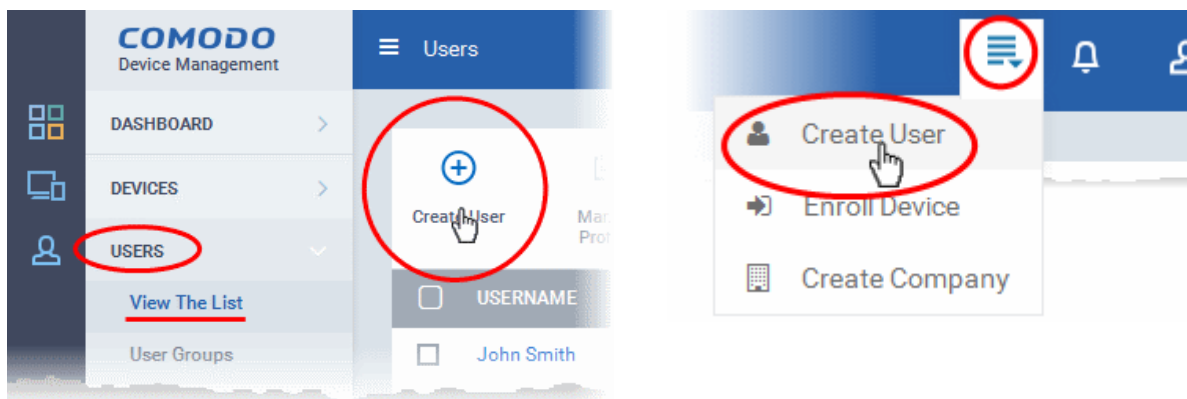
The next step is to add users. Users' devices can be enrolled for management by CDM only after adding them to the console.

- **Comodo One users** - if you created only one company in C1, then any users you enroll here will be automatically assigned to that company. If you created more than one company in C1, the 'Enroll User' dialog will allow you to choose the company to which you want to assign the user.

- **CDM Users** – You can add users and enroll their devices without selecting any company. However, If you need the users/devices to be grouped under different companies, you can create companies in CDM and add device groups under them as explained in **Step 4 - Create Groups of Devices**.

### To add a user

- Open the 'Users' interface by clicking the 'Users' tab from the left hand side and choosing 'View The List' from the options and click the 'Create User' above the table.
- or
- Choose 'Create User' from the drop-down at the top right:



The 'Create new user' form will open.

### Create new User Close

**Username \***

**Email \***

**Phone number**

**Company \***

**Assign role**

- Type a login username (mandatory), email address (mandatory) and phone number of the user to be added.
- Choose the company (mandatory), from the 'Company' drop-down.
  - Comodo One Users – The drop-down will display the companies added to C1. You can choose the company to which the user belongs. The user will be enrolled under the chosen company.
  - CDM users – Leave the selection as 'Default Company'.
- Choose a role for the user. A 'role' determines user permissions within the CDM console itself. CDM ships with two default roles:
  - **Administrators** - Full administrative privileges in the CDM console. The permissions for this role are not editable.
  - **Users** - In most cases, a 'user' will simply be an owner of a managed device who should not require elevated privileges in the management system. Under default settings, 'Users' cannot login to CDM.

You can create roles with different permission levels via the 'Role Management' screen (click 'Settings > Role Management'). You can edit the permissions of existing roles by clicking on the role in the list and add or remove permissions as required. Any new roles you create will become available for selection in the 'Roles' drop-down when creating a new user. See [Configuring the Role-Based Access Control for Users](#) and [Managing Roles assigned to a User](#) for more details.

- Click 'Submit' to add the user to CDM.

The user will be added to list in the 'Users' interface. The user's devices can be enrolled to CDM for management.

- Repeat the process to add more number of users.

If an administrator is added, an activation mail will be sent to their registered email address. The new administrator needs to activate their account and set the login password by clicking the activation link in the email.

Upon activation, the administrator will be able to login to CDM with their user-name and password.

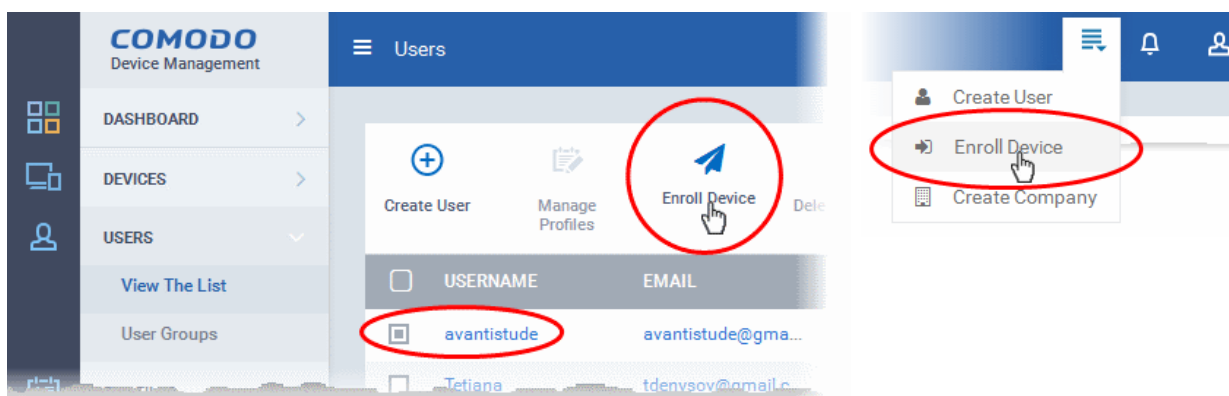
## Step 3 - Enroll Users' devices

The next step is to enroll users' devices for management.

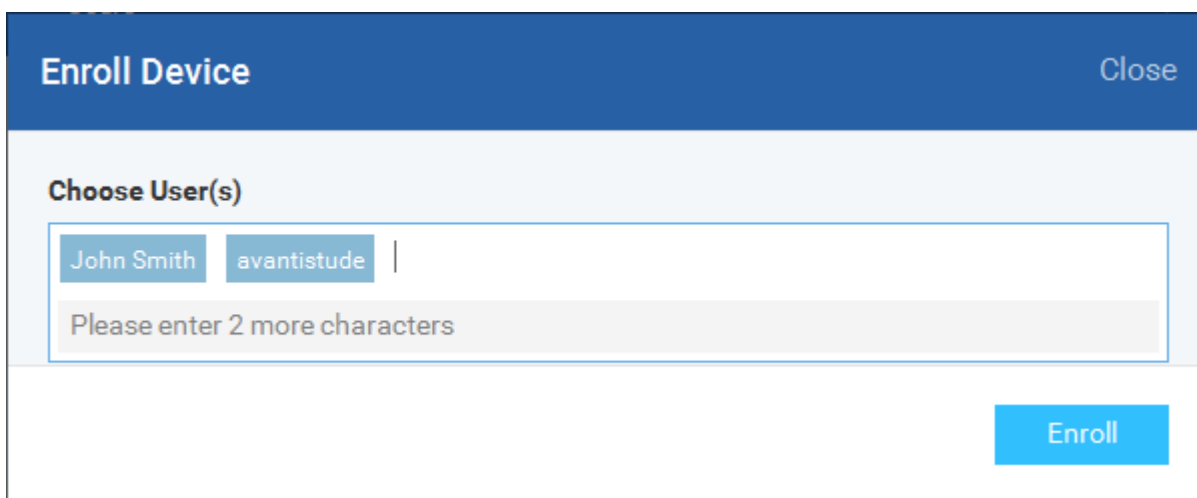
Each user license enables to enroll a maximum of five mobile devices or one Windows endpoint for a single user. (1 license will be consumed by 5 mobile devices. 1 license could also be consumed by a single Windows endpoint). If more than 5 devices or 1 endpoint are added for the same user, then an additional user license will be consumed. Administrators can purchase additional licenses from the Comodo website if required.

### To enroll devices

- Click the 'Users' tab from the left and choose 'View The List' to open the 'Users' interface
  - Select the user(s) whose devices are to be enrolled and click the 'Enroll Device' button above the table in the 'Users interface'.
- Or
- Choose 'Enroll Device' from the drop-down at the top right



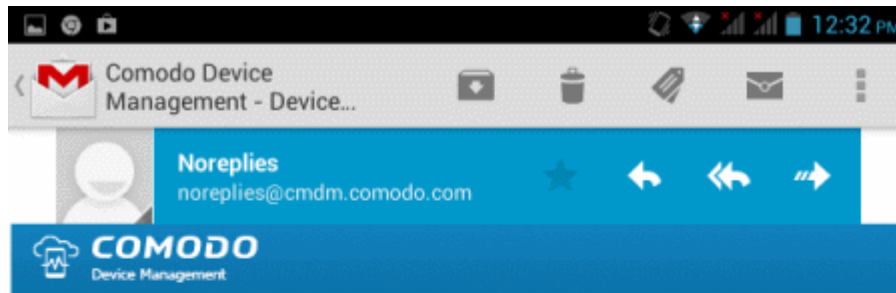
The 'Enroll Device' dialog will open for the chosen users.



The 'Choose Users' field is pre-populated with the users chosen from the 'Users' interface, if you have chosen the users from the 'Users' interface before clicking 'Enroll Device' button.

- To add more users, start typing first few letters of the username and choose the user from the search results drop-down.
- Click 'Enroll'

A device enrollment email will be sent to each user. The email will contain a link to the enrollment page containing the instructions and links to download the DM agent/profile for the device to be enrolled and configuring them. An example mail is shown below.



## Welcome to Comodo Device Management!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet or Windows device into the Comodo Device Management system. Doing so will make it easier and more secure to connect your personal devices to company networks. This mail explains how you can complete the enrollment process in a few short steps.

### Note:

- Please make sure you follow the correct procedure for your type of device - iOS, Android or Windows.
- Please make sure you complete these steps from the phone or tablet or desktop machine.

This product allows the system administrator to collect device and application data, add/remove accounts and restrictions, list, install and manage apps, and remotely erase data on your device.

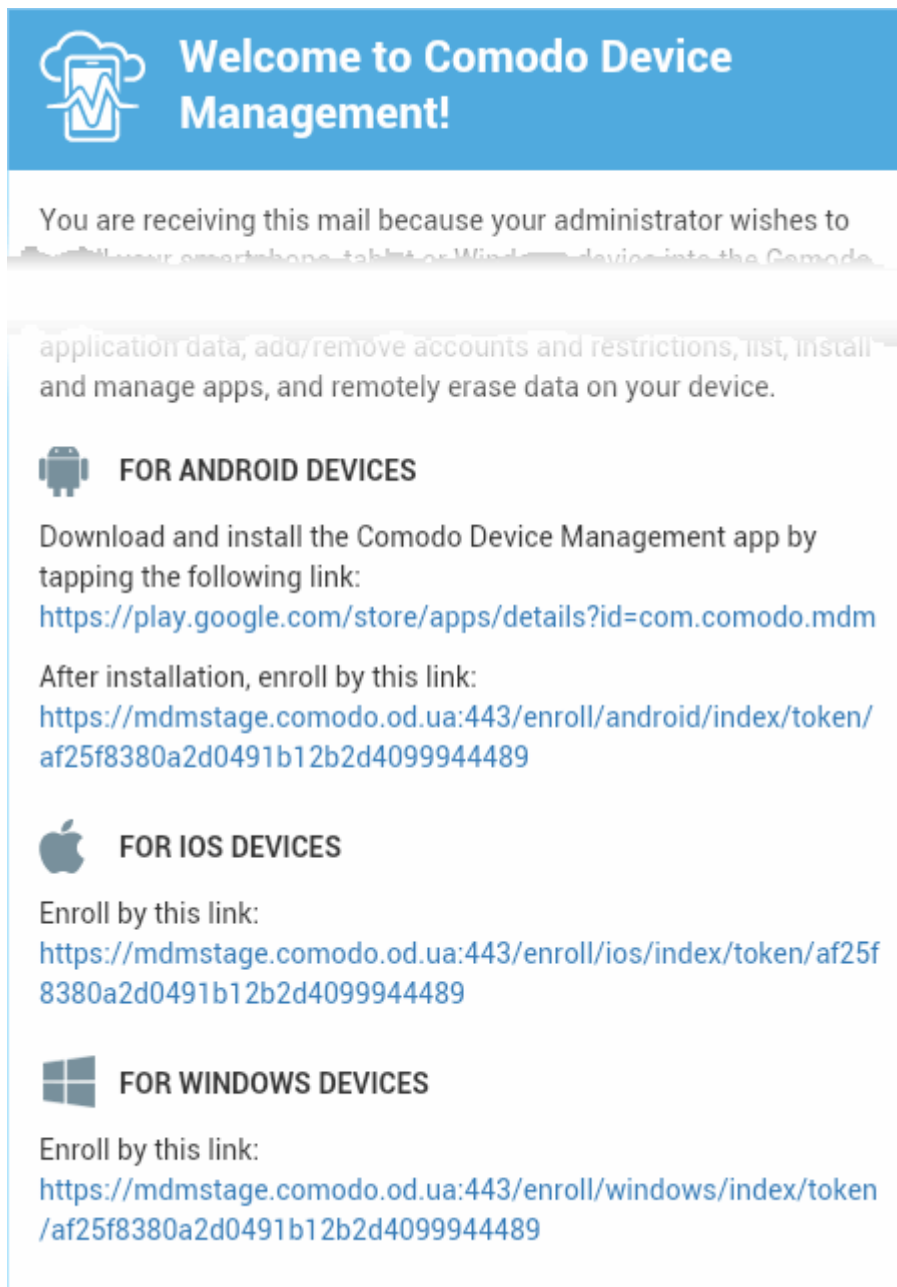
### Enrollment device:

Please click the following link to enroll your device - <https://mdmstage.comodo.od.ua:443/enroll/device/by/token/af25f8380a2d0491b12b2d4099944489>



- Clicking the link will take the user to the enrollment page containing the links to download and configure agent/profile for Android, iOS and Windows devices.


The end-user should open the mail in the device to be enrolled and tap/click the link to view the device enrollment page in the same device.



**Welcome to Comodo Device Management!**


You are receiving this mail because your administrator wishes to enroll your smartphone, tablet or Windows device into the Comodo Device Manager.

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


 **FOR ANDROID DEVICES**

Download and install the Comodo Device Management app by tapping the following link:  
<https://play.google.com/store/apps/details?id=com.comodo.mdm>

After installation, enroll by this link:  
<https://mdmstage.comodo.od.ua:443/enroll/android/index/token/af25f8380a2d0491b12b2d4099944489>

 **FOR IOS DEVICES**

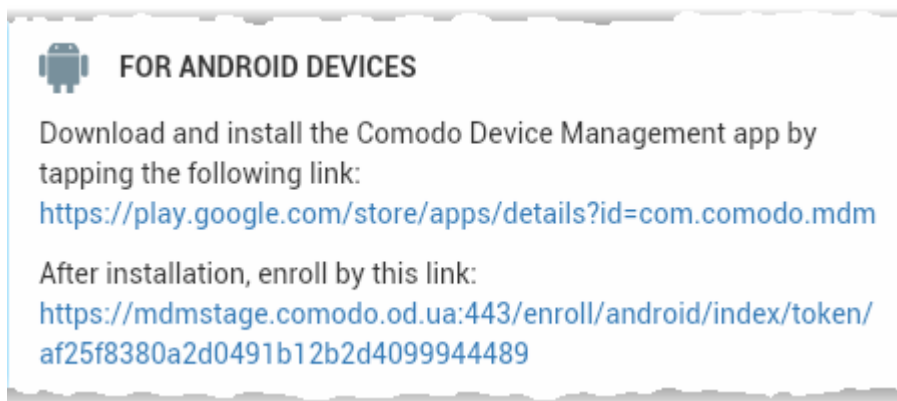
Enroll by this link:  
<https://mdmstage.comodo.od.ua:443/enroll/ios/index/token/af25f8380a2d0491b12b2d4099944489>


 **FOR WINDOWS DEVICES**

Enroll by this link:  
<https://mdmstage.comodo.od.ua:443/enroll/windows/index/token/af25f8380a2d0491b12b2d4099944489>

## Enroll Android Devices

The device enrollment page contains two links under 'FOR ANDROID DEVICES'. The first to download the Android app and the second to enroll the device:



 **FOR ANDROID DEVICES**

Download and install the Comodo Device Management app by tapping the following link:  
<https://play.google.com/store/apps/details?id=com.comodo.mdm>

After installation, enroll by this link:  
<https://mdmstage.comodo.od.ua:443/enroll/android/index/token/af25f8380a2d0491b12b2d4099944489>

1. User opens the enrollment page on the target device and clicks the 1st link to install the CDM app.
2. After app installation is complete, user clicks the 2nd link to enroll their device. The app will connect to CDM and then the user needs to tap 'Activate' in the next screen. The app will automatically enroll the device with CDM.

## Enroll iPhones, iPods and iPads

The device enrollment email contains a single enrollment link under 'FOR IOS DEVICES'. The user clicks this link to download the CDM client authentication certificate and CDM profile. Once installed, the authentication certificate will be used to verify the user and the device when he or she attempts to connect to your network.



**Note:** The user must keep their iOS device switched on at all times during enrollment. Enrollment may fail if the device auto-locks/ enters standby mode during the certificate installation or enrollment procedures.

## Enroll Windows PCs

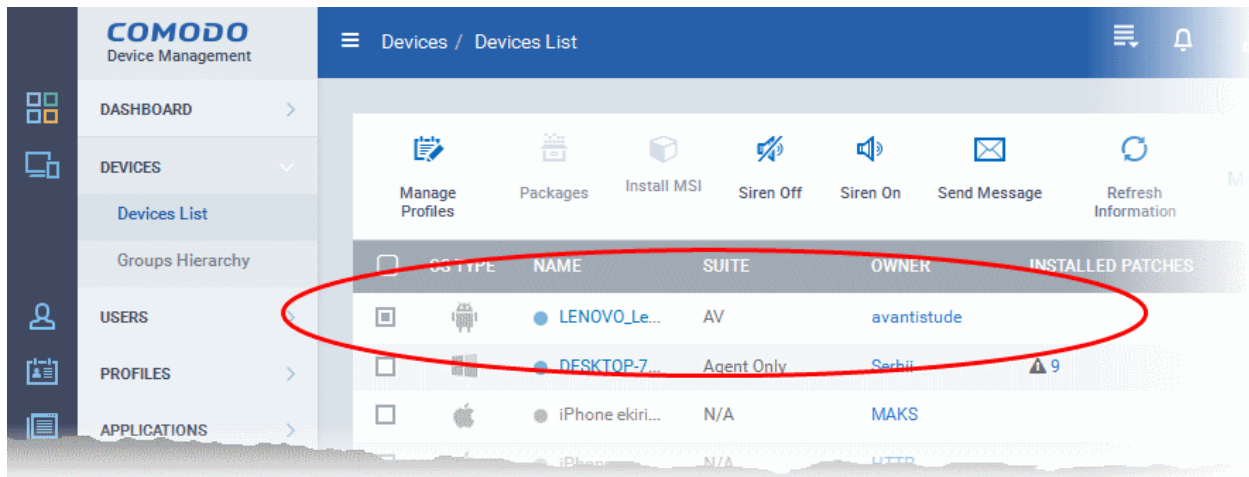
The device enrollment page contains a single enrollment link under 'FOR WINDOWS DEVICES'.



The user clicks this link to download the Comodo Device Management client app. Once installed, the app will enroll the device into CDM . Upon successful enrollment, CDM will remotely install the endpoint security software Comodo Endpoint Security (CES) on to the device.

You can check whether the devices are successfully enrolled from the 'Devices/Devices List' interface.





The 'Devices List' interface contains a list of all enrolled devices with columns that indicate the device IMEI, owner, platform and more. The interface allows you to quickly perform remote tasks on selected devices, including device wipe/lock/unlock/shutdown, siren on/off, install apps, password set/reset and more.

See [The Devices Interface](#) for more details.

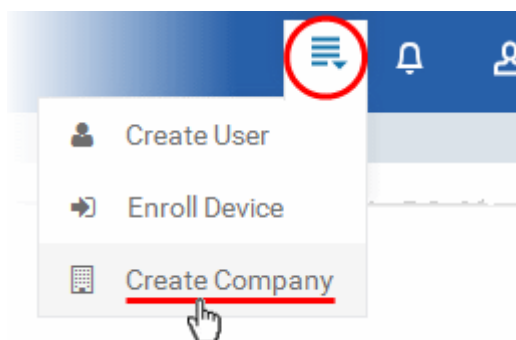
## Step 4 - Create Groups of Devices (optional)

Administrators can create groups of Android, iOS and Windows devices that will allow them to view, manage and apply policies to large numbers of devices. Each group can contain devices of different OS types. Once created, the administrator can manage all devices belonging to that group together. Dedicated configuration profiles can be created for and applied for each group as per their requirements and the allowable user privileges and applied appropriately to the device groups. The profiles for different OS types applied to a group will be deployed on the devices of respective OS types.

- **Comodo One Users** - Device Groups can be created under respective companies to which their users belong, if the companies are already defined in Comodo One.
- **CDM Users** - If no companies are added yet or if you want a group to be created under a new company, you can create a new company in CDM.

### To create a company

- Choose 'Create Company' from the drop-down at the top right:



The 'Create new Company' dialog will appear.

### Create new Company Close

**Name \***

**Subdomain \***

**Email \***

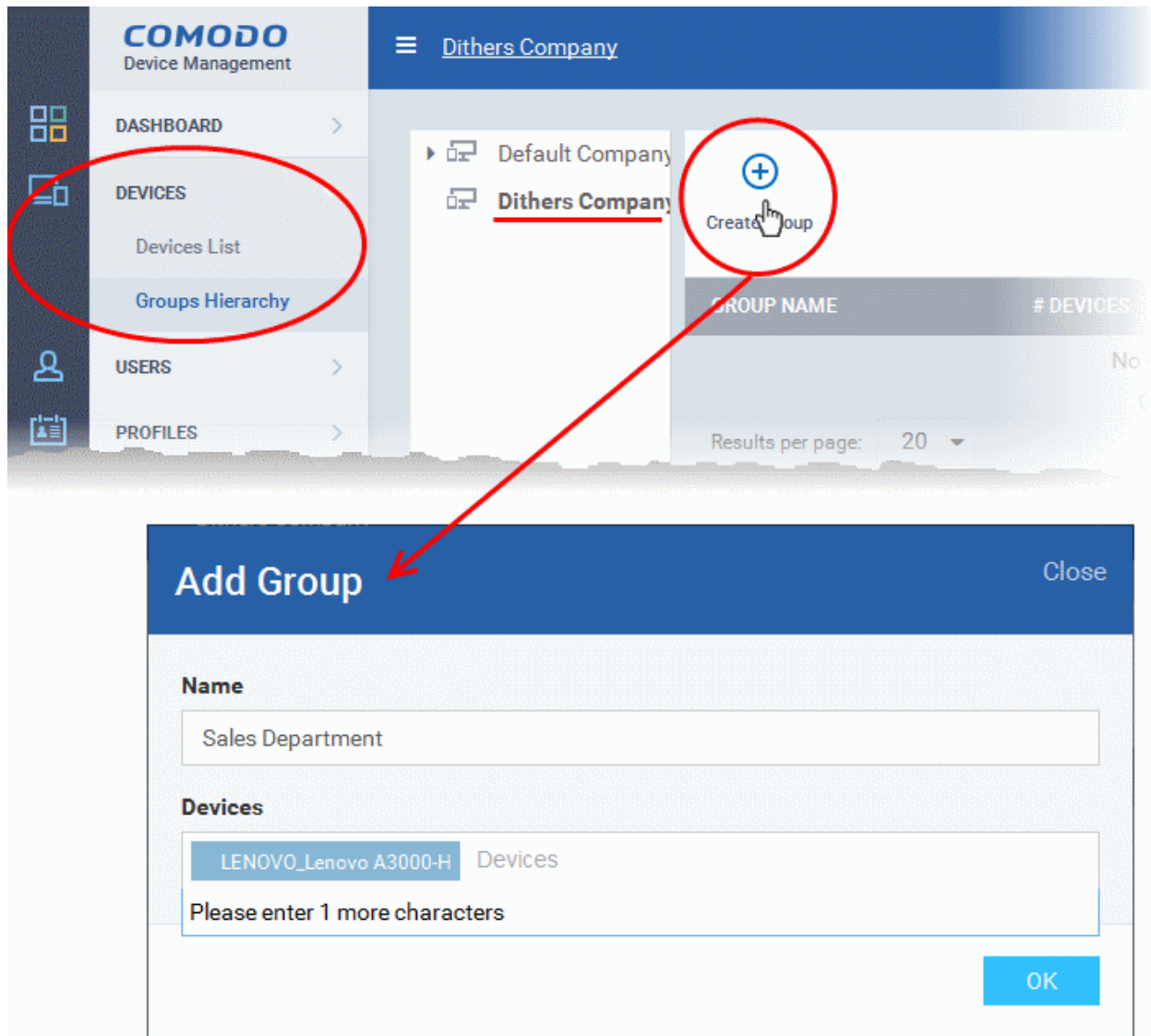
- Enter the company name (mandatory), the sub domain (mandatory) to be added to the URL to access the MDM interface for the company and the administrator email address (mandatory) for the company in the respective fields and click 'Submit'.

The company will be created.

- Repeat the process to add more companies.

#### To create a device group

- Click the 'Devices' tab from the left and choose 'Groups Hierarchy'
- Choose the Company under which you wish to create a new group from the left (optional)



- Click 'Create Group' from the top of the right pane

The 'Create/Edit Device Group' interface will open.

- You now have to name the group and choose the device(s). Enter a name in the 'Name' field. Type the first few letters of the device name in the Devices field and choose the device from the drop-down that appears. Repeat the process for adding more devices. You can also add devices after the group is created by clicking on the group name from the same screen > 'Add to Group' button and selecting the devices from the list.
- Click 'Save'. Repeat the process to create more groups. Refer to the section **Managing Device Groups** for more details.

The next step is to create profiles, which is **explained in the next section**.

## Step 5 - Create Configuration Profiles

A configuration profile is a collection of settings which can be applied to mobile devices and PCs that have been enrolled into Comodo Device Manager. Each profile allows an administrator to specify a device's network access rights, overall security policy, antivirus scan schedule and general device settings.

If you designate a profile as 'Default', then it will be auto-applied to a device upon enrollment. Multiple profiles can be created to cater to the different security and access requirements of devices connecting to your network.

Profiles are applied at the time a device connects to the network. Profile settings will remain in effect until such time as the CDM app is uninstalled from the device or the profile itself is modified/removed/disabled by the administrator.

Profile specifications differ between iOS, Android and Windows Devices:

- **Android profiles**
- **iOS profiles**
- **Windows Profiles**

## To create an Android Profile

- Click the 'Profiles' tab from the left and choose 'View The List'.
- Click 'Create' drop-down above the table and then choose 'Create Android Profile'.

The screenshot shows the Comodo Device Manager interface. On the left sidebar, the 'PROFILES' tab is selected and circled in red. Below it, the 'View The List' option is also circled. In the main content area, the 'Profiles' section is visible. The 'Create' button (a green circle with a plus sign) is circled in red, and a dropdown menu is open showing the following options: 'Create Android Profile', 'Create iOS Profile', 'Create Windows Profile', 'Import from CES Config file', and 'Import from CDM Exported Profile'. A red arrow points from the 'Create Android Profile' option in the dropdown to the 'Create Android Profile' dialog box below. The dialog box has a blue header with the title 'Create Android Profile' and a 'Close' button. It contains two text input fields: 'Name \*' with the value 'Sales Team Android Devices' and 'Description' with the value 'Security Profile for Android devices used by sales staff'. A blue 'Create' button is located at the bottom right of the dialog.

- Enter a name and description for the profile and click 'Create'.

The profile will be created and the 'General Settings' for the profile will be displayed.

Profiles / Sales Team Android Devices

Logout (John Smith)

## Sales Team Android Devices

Add Export Profile Clone Profile Delete Profile

### General


#### General Settings

Edit

**Name \***  
Sales Team Android Devices  
Display name of the profile (shown on the device).

**Is Default**  
Disabled

**Description**  
Security Profile for Android devices used by sales staff  
Brief explanation of the contents or purpose of the profile

- If you want this profile to be a default policy, click on the 'Edit' button  at the top right of the 'General' settings screen and select the check box beside 'Is Default'.
- Click 'Save'.

The next step is to add the components for the profile.

- Click 'Add' drop-down button and select the component from the list that you want to include for the profile

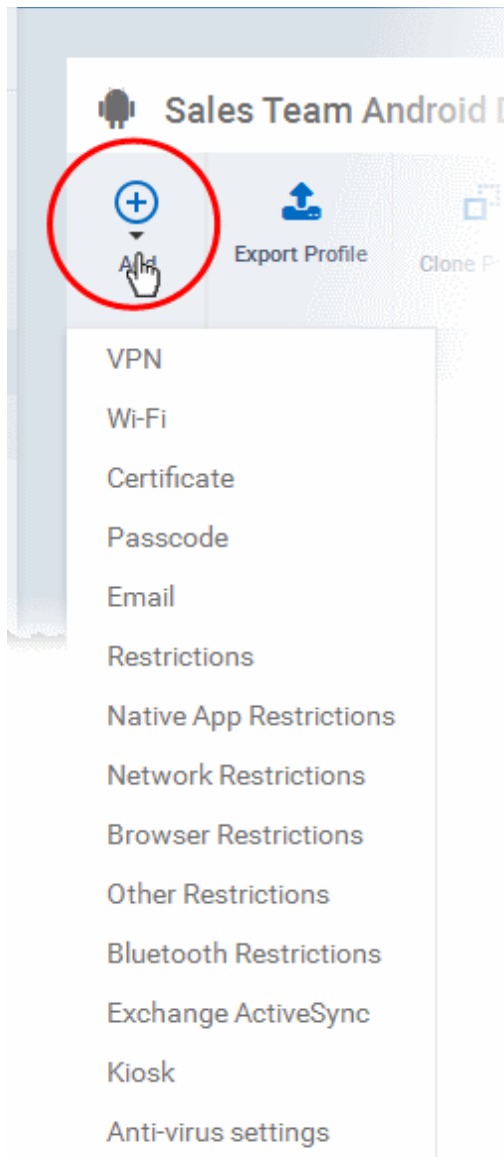
The settings screen for the selected component will be displayed and after saving the settings, it will be available as links at the top. You can configure passcode settings, feature restrictions, antivirus settings Wi-Fi settings and more. If a component is not configured, the device will continue to use existing, user-defined settings or settings that have been applied by another CDM profile.

- Click 'Save' in each configuration screen for the parameters and options selected in that screen to be added to the profile

See **Profiles for Android Devices** in the full guide for more information on these settings. In brief:

- **General** - Profile name, description and whether or not this is a default profile. These were configured in the previous step. Default profiles are automatically applied upon device enrollment.
- **VPN** - Configure directory user-name, VPN host, connection type and method of authentication for users wishing to connect to your internal network from an external location, whether to forcibly maintain VPN connection and more. This profile is supported for SAFE devices only.

- **Wi-Fi** - Specify the name (SSID), security configuration type and password (if required) of your wireless network to which the devices are to be connected. You can add other wireless networks by clicking 'Add new Wi-Fi section'.
- **Certificate** - Upload certificates and this will act as a certificate store from which the certificates can be selected for use in other settings such as 'Wi-Fi', 'Exchange Active Sync', 'VPN' and so on.
- **Passcode** - Specify passcode complexity, minimum length, timeout-before-lock, failed logins before wipe (0=unlimited/never wipe), failed logins before capturing the photo of the possessor and location to recover lost or mislaid device, maximum lifetime of passcode in days and number of previous passcodes from which the new passcode should be unique.
- **Email** - Configure email account, connection and security details for users accessing incoming and outgoing mails from their devices. This profile is supported for SAFE devices only.



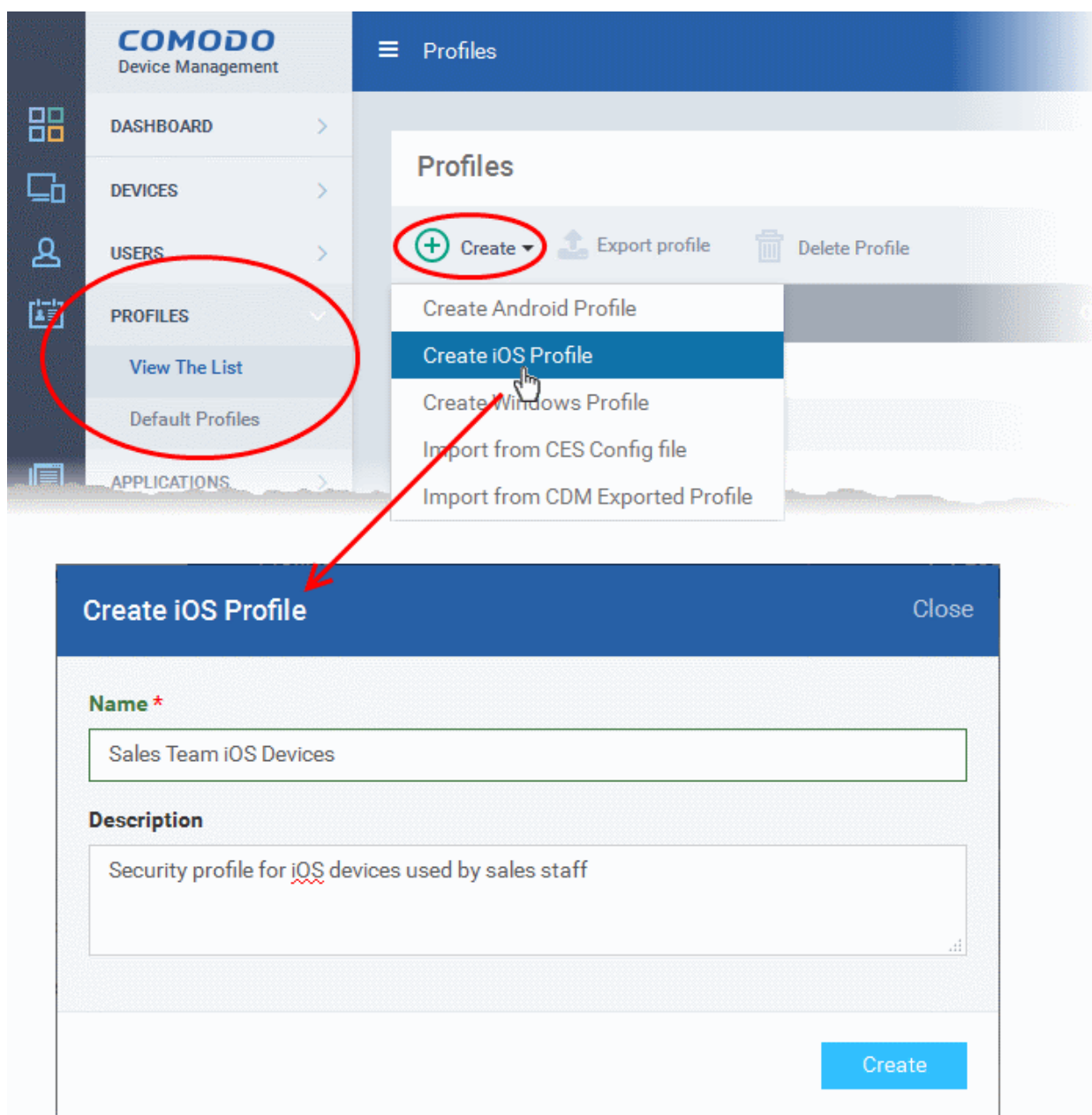
- **Restrictions** - Configure default device settings for Wi-Fi connection and cellular network connection, whether users should be able to disable app verification, background traffic, bluetooth on/off, whether camera use is allowed, whether the user is allowed to encrypt data stored on the device and whether or not they are allowed to install applications from unknown sources.
- **Native App Restrictions** - Configure which native applications should be accessible to users. Native applications are those that ship with the device OS and include apps like Gmail, YouTube, the default Email client and the Gallery. This feature is supported for Android 4.0+ and Samsung for Enterprise (SAFE) devices such as Galaxy smartphones, Galaxy Note devices and Galaxy tablets.
- **Network Restrictions** - Specify network permissions such as minimum level of Wi-Fi security required to access that Wi-Fi network, allow user to add more Wi-Fi networks in their devices, type of text and multimedia messages to be allowed and configure whitelist/blacklisted Wi-Fi networks. This profile is supported for SAFE devices only.
- **Browser Restrictions** - Configure browser restrictions such as to allow pop-ups, javascript and cookies. This profile is supported for SAFE devices only.
- **Other Restrictions** - Configure a host of other permissions such as use of microphone, SD card, allow screen capture and more. This profile is supported for SAFE devices only.
- **Bluetooth Restrictions** - Specify Bluetooth restrictions such as to allow device discovery via Bluetooth, allow outgoing calls and more. This profile is supported for SAFE devices only.
- **Exchange Active Sync** - Specify account name, host, domain and other settings to facilitate connections from devices under this profile to Microsoft Exchange Active Sync servers. This profile is supported for SAFE devices only.

the Samsung Galaxy range. Kiosk Mode allows administrators to control how applications run on managed devices and whether SMS/MMS are allowed. This profile is supported for SAFE devices only.

- **Antivirus Settings** - Schedule antivirus scans on the device and specify trusted Apps to be excluded from AV scans.

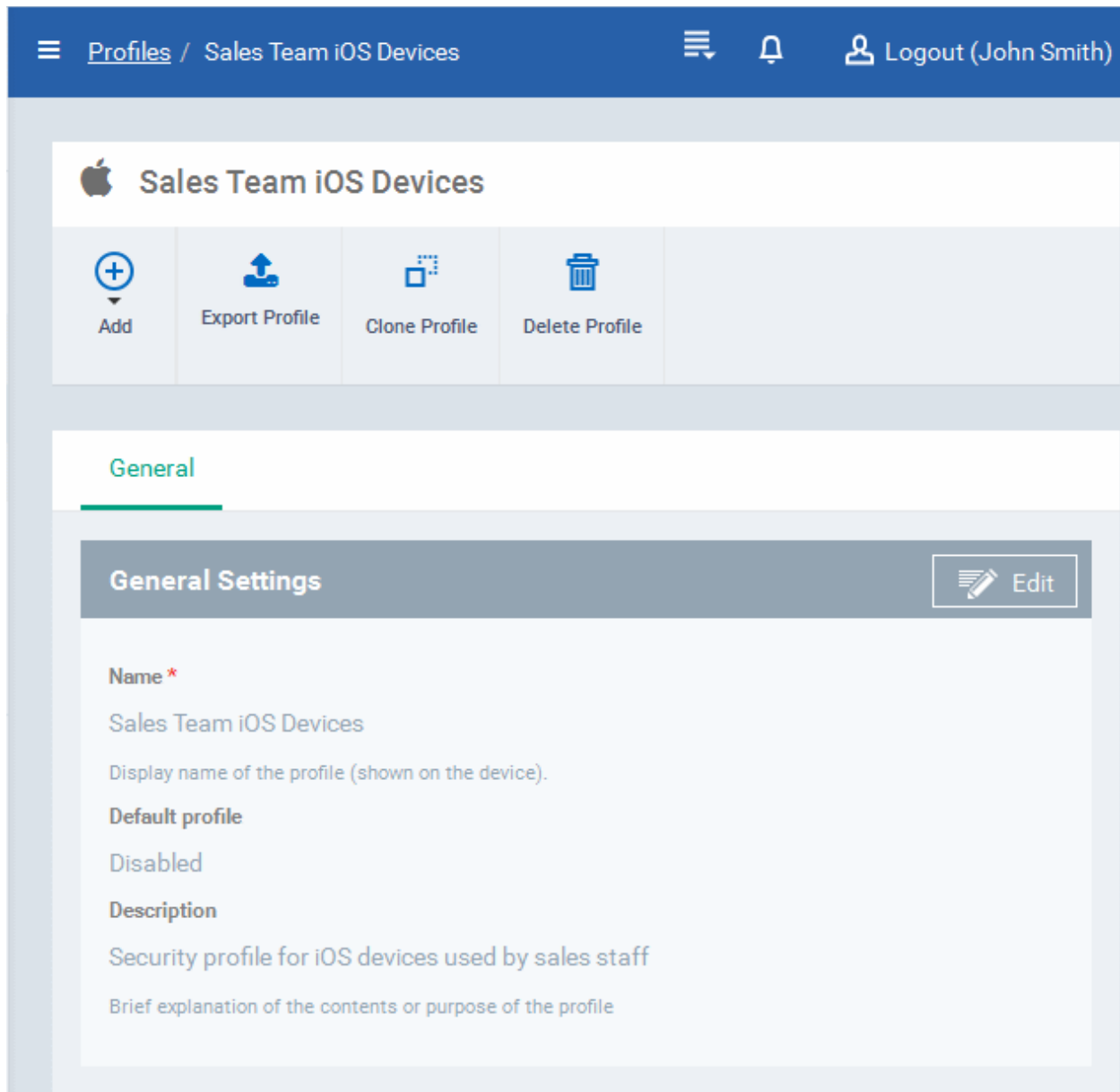
## To create an iOS Profile

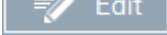
- Click the 'Profiles' tab from the left and choose 'Profile List'.
- Click 'Create' drop-down above the table and then click 'Create iOS Profile'.



- Enter a name and description for the profile and click 'Create'.

The profile will be created and the 'General Settings' for the profile will be displayed.



- If you want this profile to be a default policy, click on the 'Edit' button  at the top right of the 'General' settings screen and select the check box beside 'Is Default'.
- Click 'Save'.

The next step is to add the components for the profile.

- Click 'Add' drop-down button and select the component from the list that you want to include for the profile

The settings screen for the selected component will be displayed and after saving the settings, it will be available as links at the top. You can configure passcode settings, feature restrictions, VPN settings Wi-Fi settings and more. If a component is not configured, the device will continue to use existing, user-defined settings or settings that have been applied by another CDM profile.

- Click 'Save' in each configuration screen for the parameters and options selected in that screen to be added to the profile.

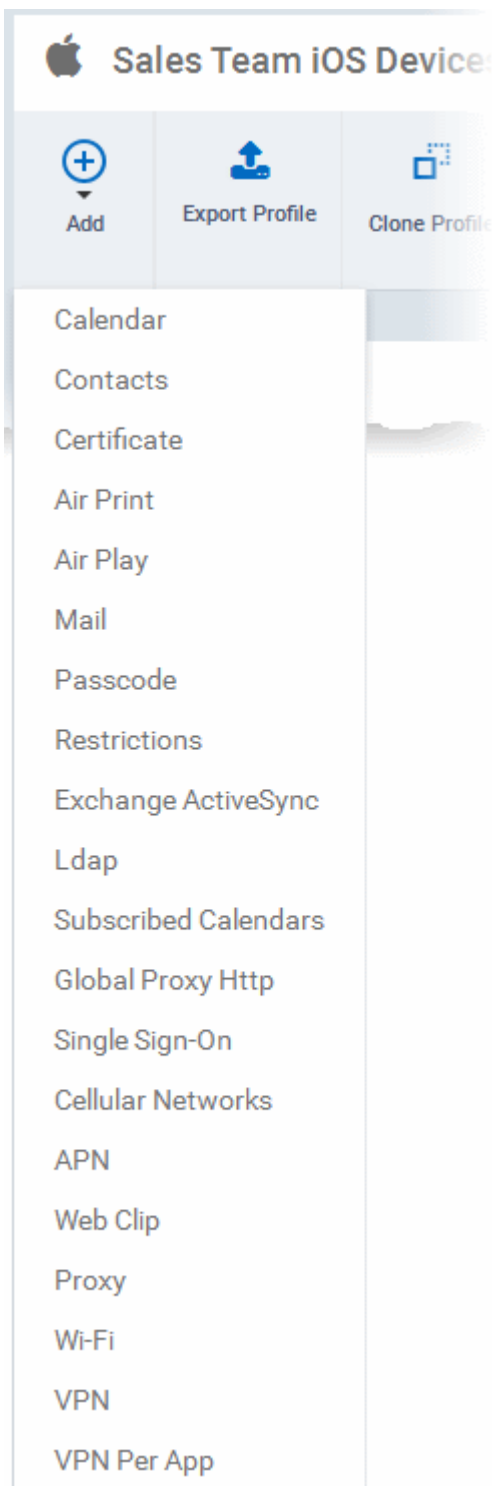
See **Profiles for iOS Devices** in the main guide for more details on this area. In brief, iOS device profiles are more detailed than Android profiles:

- **General** - Profile name, description and whether or not this is a default profile. These were configured in the previous step. Default profiles are automatically applied upon device enrollment.
- **Calendar** - Configure CalDAV server and connection settings which will allow device integration with corporate



scheduling and calendar services.

- **Contacts** - Configure CardDAV account, host and user-settings to enable contact synchronization between different address book providers (for example, to synchronize iOS contacts and Google contacts).



- **Certificate** - Upload certificates and this will act as a certificate store from which the certificates can be selected for use in other settings such as 'Wi-Fi', 'Exchange Active Sync', 'VPN' and so on.
- **Airprint** - Specify the location of Airprint printers so they can be reached by devices under this profile (iOS 7 +)
- **Airplay** - Allows you to whitelist devices so they can take advantage of Apple Airplay functionality (iOS 7 +)
- **Mail** - Configure general mail server settings including incoming and outgoing servers, connection protocol (IMAP/POP), user-name/password and SMIME/SSL preferences.
- **Passcode** - Specify passcode complexity, minimum length, timeout-before-lock, failed logins before wipe (0=unlimited/never wipe), failed logins before capturing the photo of the possessor and location to recover lost or mislaid device, maximum lifetime of passcode in days and number of previous passcodes from which the new passcode should be unique.
- **Restrictions** - Configure default device settings for Wi-Fi connection and cellular network connection, whether users should be able to disable app verification, background traffic, bluetooth on/off, whether camera use is allowed, whether the user is allowed to encrypt data stored on the device and whether or not they are allowed to install applications from unknown sources.
- **Exchange Active Sync** - Specify account name, host, domain and other settings to facilitate connections from devices under this profile to Microsoft Exchange Active Sync servers.
- **VPN** - Configure directory user-name, VPN host, connection type and method of authentication for users wishing to connect to your internal network from an external location.
- **VPN Per APP**- Instead of forcing all BYOD traffic over the corporate VPN tunnel, 'Per-app VPN' functionality allows admins to choose specific 'managed apps' which should always connect via VPN. This improves user privacy and network performance by keeping all private browsing and emails off the corporate VPN. This section allows you to configure the VPN service that those managed apps will connect to.
- **LDAP** - Configure LDAP account settings for devices under this profile so users can connect to company address books and contact lists.
- **Subscribed Calendars** - Specify one or more calendar services which you wish to push notifications to devices under this profile.
- **Global HTTP Proxy** - Global HTTP proxies are used to ensure

that all traffic going to and coming from an iOS device is routed through a specific proxy server. This, for example, allows the traffic to be packet-filtered regardless of the network that the user is connected through.

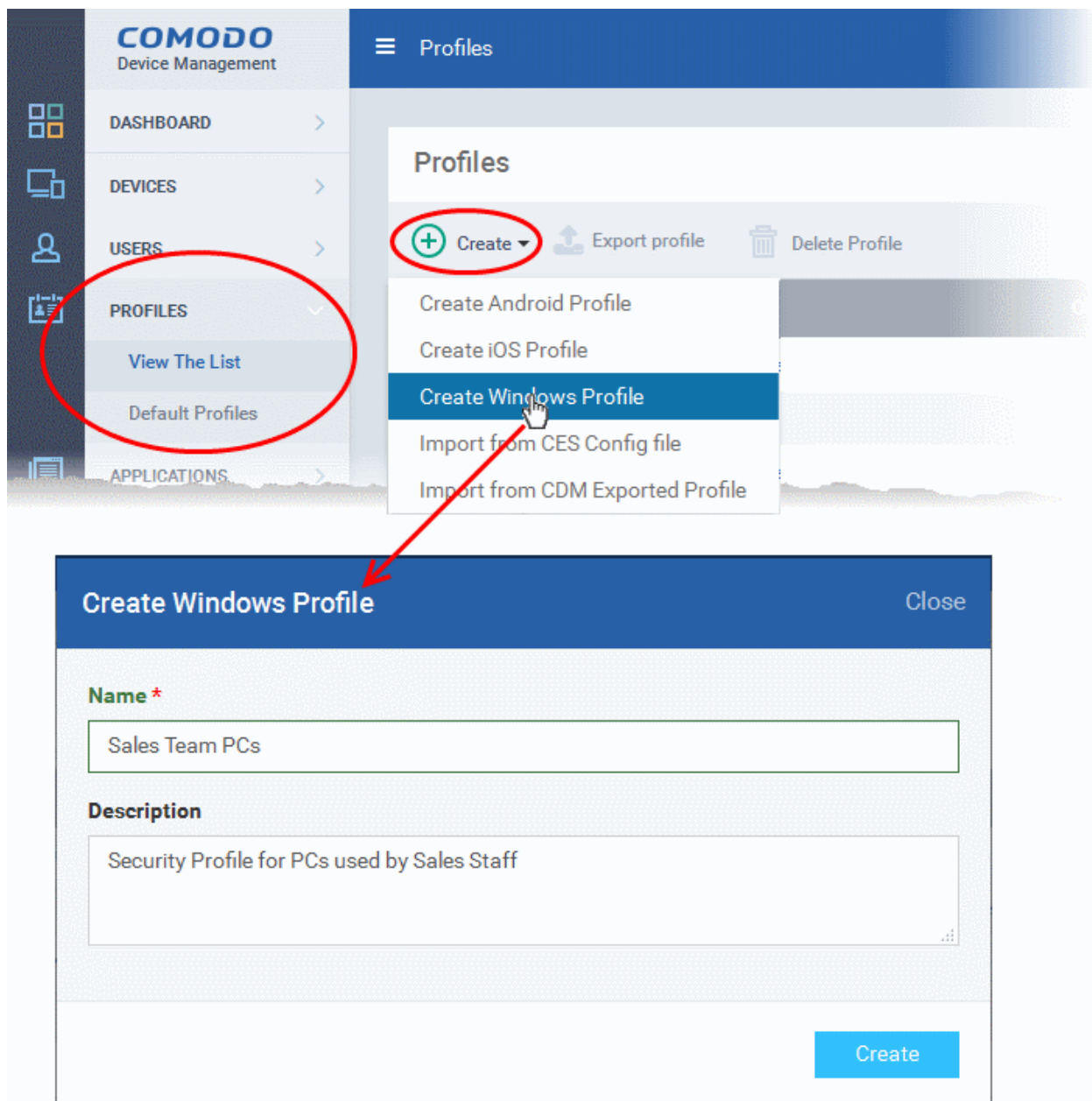
- **Single Sign-On** - iOS 7 +. Configure user credentials that can be used to authenticate user permissions for multiple enterprise resources. This removes the need for a user to re-enter passwords. In this area, you will configure Kerberos principal name, realm and the URLs and apps that are permitted to use Kerberos credentials for authentication.
- **Cellular Networks** - Configure cellular network settings. The 'cellulars' setting performs fulfills a similar role to the APN setting and actually replaces it in iOS 7 and above.
- **APN** - Specify an Access Point Name for devices on this profile. APN settings define the network path for all cellular

data. This area allows you to configure a new APN name (GPRS access point), username/password and the address/port of the proxy host server. The APN setting is replaced by the 'Cellulars' setting in iOS7 and over.

- **Web Clip** - Allows you to push a shortcut to a website onto the home-screen of target devices. This section allows you to choose an icon, label and target URL for the web-clip.
- **Proxy** – Allows you to specify the proxy server, and their credentials, to be used by the device for network connections.
- **Wi-Fi** - Specify the name (SSID), security configuration type and password (if required) of your wireless network to which the devices are to be connected.
- **VPN** - Configure directory user-name, VPN host, connection type and method of authentication for users wishing to connect to your internal network from an external location, whether to forcibly maintain VPN connection and more. This profile is supported for iOS 7 and above.
- **VPN Per App** - Configure directory user-name, VPN host, connection type and method of authentication for users wishing to connect to your internal network from an external location, whether to forcibly maintain VPN connection and more exclusively for Safari domains. This profile is supported for iOS 7 and above.

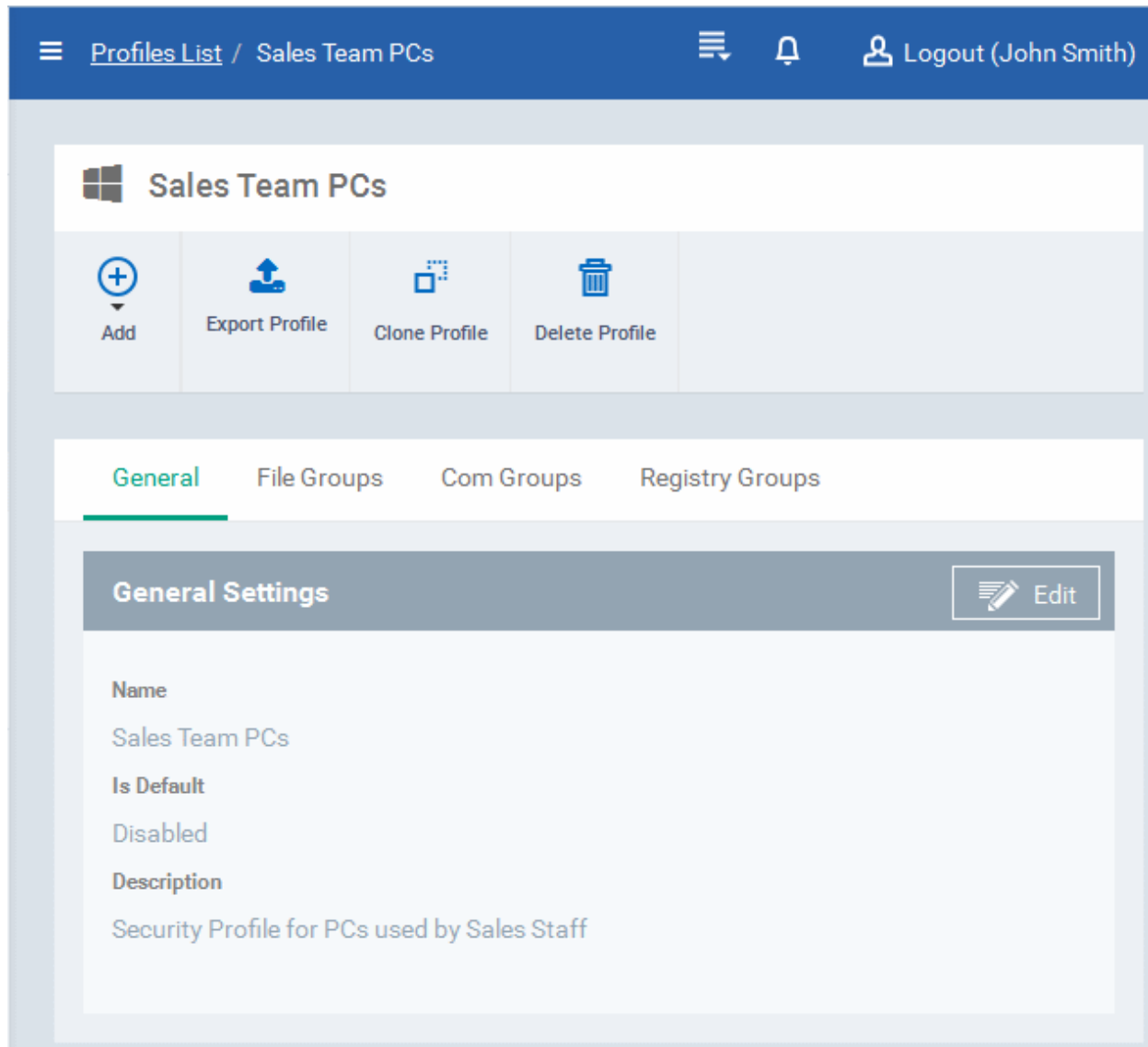
### To create a Windows profile


- Click the 'Profiles' tab from the left and choose 'Profiles List'.
- Click 'Create' drop-down above the table and then click 'Create Windows Profile'



- Enter a name and description for the profile (for example, 'Sales Dept endpoints', 'Win7 Machines' or 'Field Executives Laptops') and click 'Create'.

The profile will be created and the 'General Settings' for the profile will be displayed.



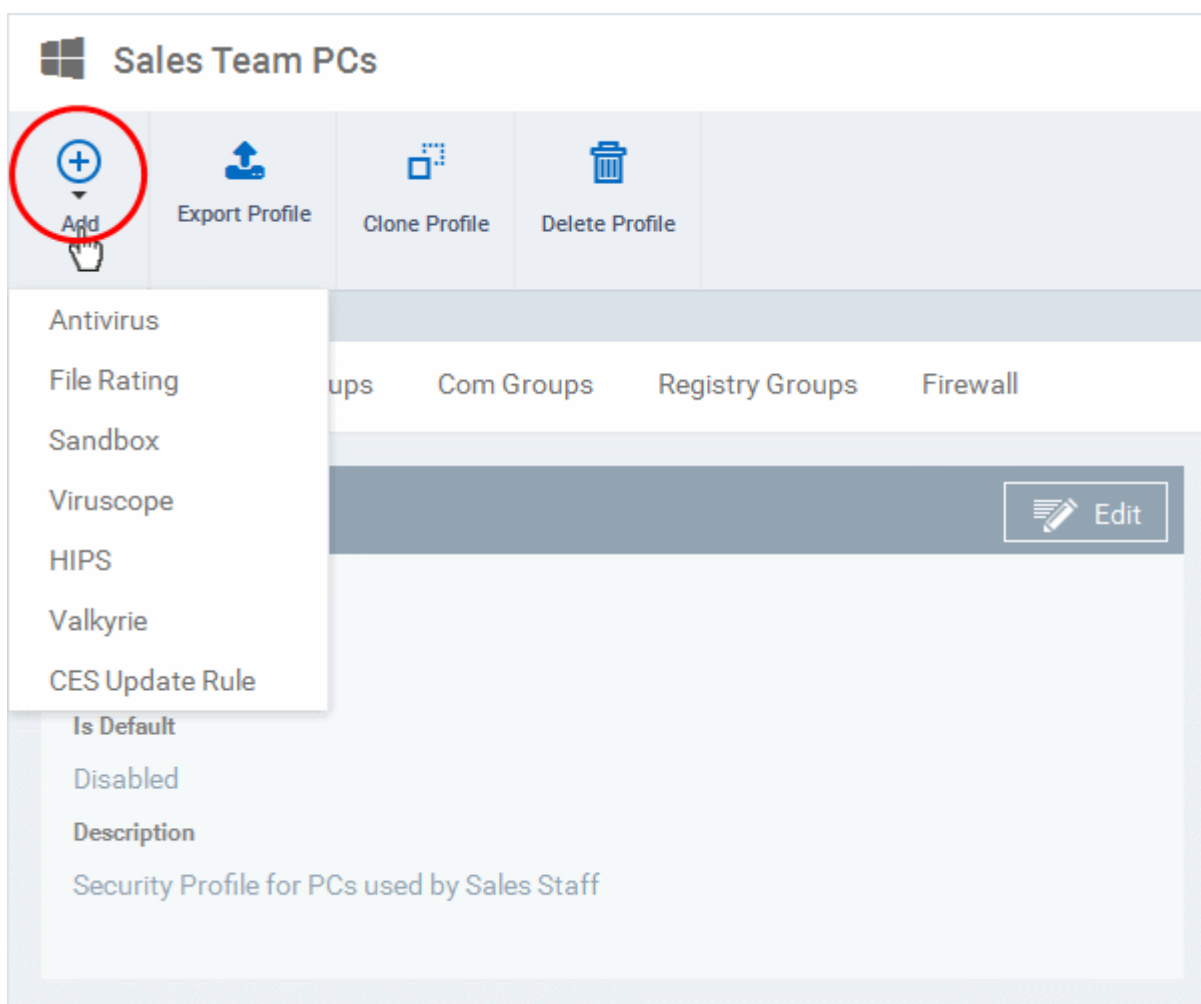
- If you want this profile to be a default policy, click on the 'Edit' button  at the top right of the 'General' settings screen and select the check box beside 'Is Default'.
- Click 'Save'.

The next step is to add the components for the profile.

- Click 'Add' drop-down button and select the component from the list that you want to include for the profile

The settings screen for the selected component will be displayed and after saving the settings, it will be available as links at the top. You can configure Antivirus, Firewall, Sandbox, File Rating, Valkyrie, HIPS, Viruscope and Update settings. In addition, you can configure the File Groups, COM Groups and Registry Groups for each profile, for use in Firewall and HIPS rules configured for the profile.

If a component is not configured, the device will continue to use existing, user-defined settings or settings that have been applied by another CDM profile.



- Click 'Save' in each configuration screen for the parameters and options selected in that screen to be added to the profile.

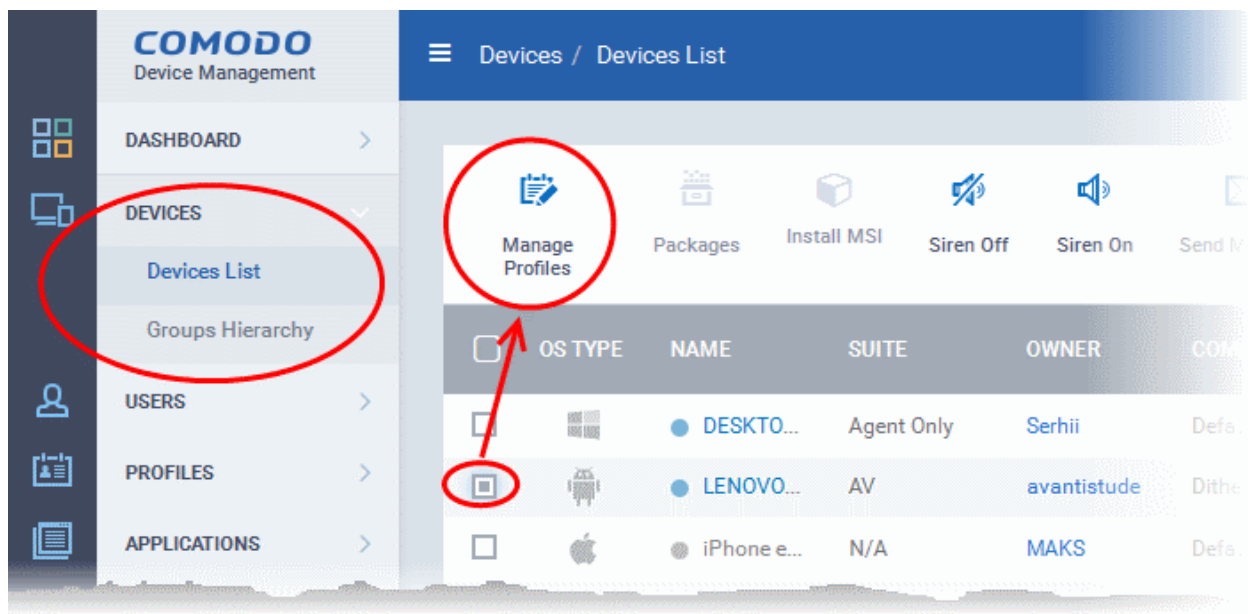
See **Profiles for Windows Devices** in the full guide for more information on these settings. In brief:

- **Antivirus** - Enable on-access scanning of files, configure scan and alert options, set alert time out period, maximum size for files to be scanned, files to be excluded and more.
- **File Rating** - Enable cloud lookup for checking reputation of files accessed in real-time, configure options for files to be trusted and detecting potentially unwanted applications. For more details on File Rating in CES, refer to the [help page explaining File rating Settings](#) in [CES online help guide](#).
- **Firewall** - Enable/Disable the Firewall component, configure Firewall behavior, add and manage Application and Global Firewall rules and more. For more details on Firewall in CES, refer to the [help page explaining Firewall Settings](#) in [CES online help guide](#).
- **Sandbox** - Enable Auto-Sandboxing of unknown files, add exclusions, and configure sandbox behavior and alert options and view and manage Sandbox Rules for auto-sandboxing applications.
- **Viruscope** - Enable Viruscope that monitors the activities of processes running at the endpoints and generates alerts if they take actions that could potentially threaten your privacy and/or security and configure options for alert generation. For more details on Viruscope in CES, refer to the [help page explaining Viruscope](#) in [CES online help guide](#).
- **HIPS** - Enable Host Intrusion Prevention System (HIPS) and its behavior, configure HIPS rules and define Protected Objects at the endpoints. For more details on HIPS in CES, refer to the [help page explaining HIPS Settings](#) in [CES online help guide](#).
- **Valkyrie** – Valkyrie is a cloud based file analysis system. look-up system. It uses a range of static and dynamic detectors including heuristics, file look-up, real-time behavior analysis and human expert to analyze the submitted files and determine if the file is good or bad (malicious). You can enable Valkyrie and its components and set a schedule for submitting unknown files identified from the endpoints.

- **CES Update Rule** – Set the conditions for the CES installations at the endpoints to automatically download and install the program and virus database updates.
- **File Groups** - File Groups are handy, predefined groupings of one or more file types, which makes it easy to add them for various CES functions such as adding them to Exclusions, HIPS Rules, Auto-Sandbox and so on. You can view pre-defined file groups, define and manage new groups of files for use in Sandbox and HIPS rules in the profile. For more details on File Groups, refer to the [help page explaining the File Groups](#) in [CES online help guide](#).
- **COM Groups** - COM groups are handy, predefined groupings of COM interfaces. You can view pre-defined COM groups, define and manage new groups for use in Sandbox and HIPS rules in the profile. For more details on COM Groups, refer to the [help page explaining the COM Groups](#) in [CES online help guide](#).
- **Registry Groups** - Registry groups are handy, predefined groupings of Registry keys and values. You can view pre-defined Registry groups, define and manage new groups for use in Sandbox and HIPS rules in the profile. For more details on Registry Groups, refer to the [help page explaining Registry Groups](#) in [CES online help guide](#).

## Step 6 - Apply profiles to devices or device groups

1. Click the 'Devices' tab from the left and choose 'Devices List' from the options.
2. Select the device to be managed and click 'Manage Profiles' from the options at the top .



The list of profiles currently active on the device will be displayed.

Manage Profiles of LENOVO\_Lenovo A3000-H

Add Profiles

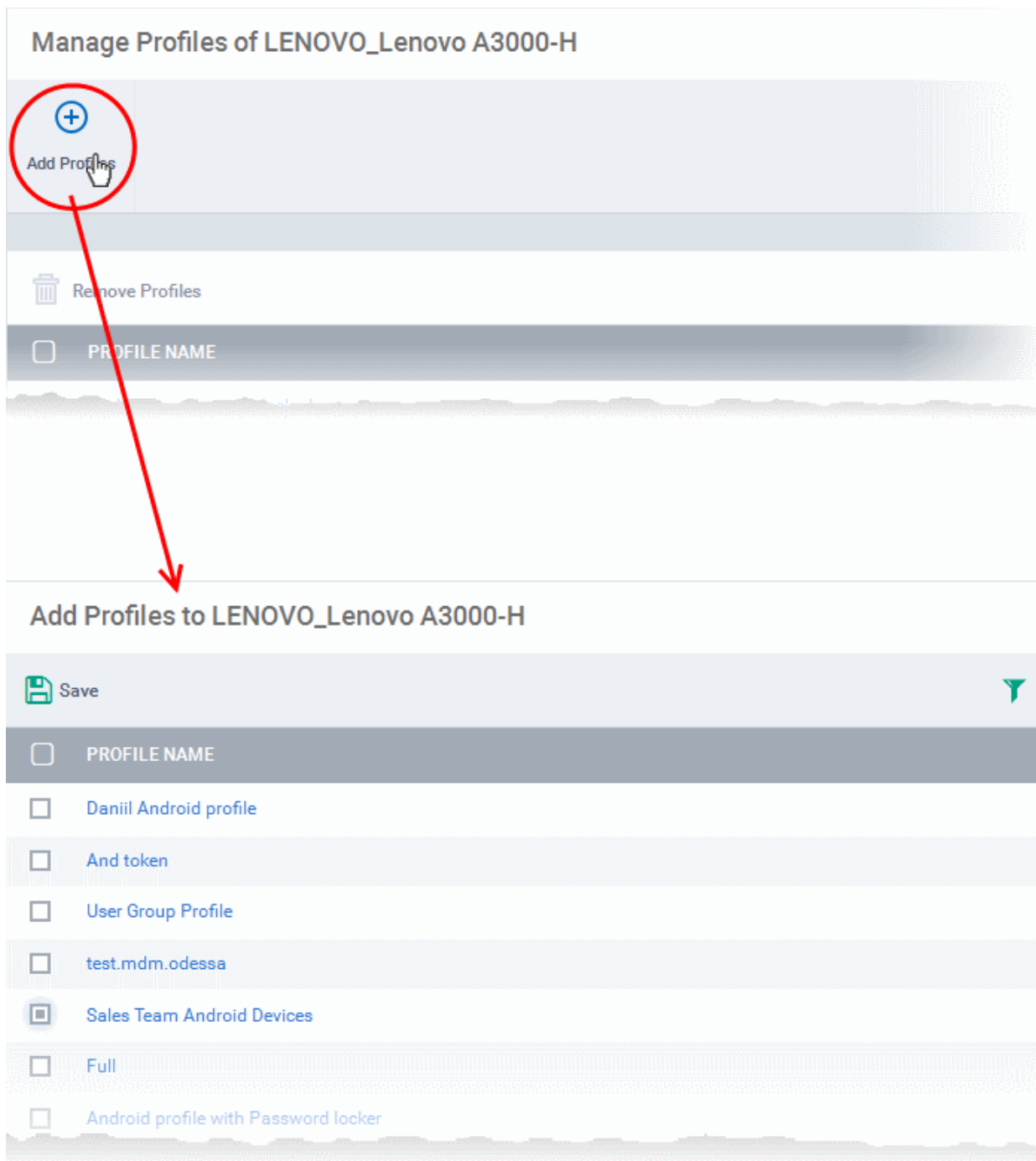
Remove Profiles

<input type="checkbox"/>	PROFILE NAME
<input type="checkbox"/>	Android profile with blocked camera

Results per page: 20

Displaying 1-1 of 1 result.

3. To add a profile to the device, click 'Add Profiles' from the top left.



A list of all profiles applicable to the chosen device, excluding those that are already applied to the device will be displayed.

4. Select the profile(s) to be applied to the device
5. Click 'Save' at the top left to add the selected profile(s) to the device.

### To apply profiles to a *group* of devices

The procedure is similar to adding profile(s) to a device except for the second step.

1. Click the 'Devices' tab from the left and choose 'Groups Hierarchy' from the options.
2. Choose the Company to view the list of groups in the right pane
3. Click on the name of the device group
4. Click 'Manage Profiles'
5. Select the profile(s) to be applied to the devices in the group

6. Click 'Save' at the top left to add the selected profile(s) to the device group

If you have successfully followed all 7 steps of this quick start guide then you should have a created a basic working environment from which more detailed strategies can be developed. Should you need further assistance, each topic is covered in more granular detail in the full administrator guide. If you have problems that you feel have not been addressed, then please contact [mdmsupport@comodo.com](mailto:mdmsupport@comodo.com).



## About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

### **Comodo Security Solutions, Inc.**

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: [EnterpriseSolutions@Comodo.com](mailto:EnterpriseSolutions@Comodo.com)

For additional information on Comodo - visit <http://www.comodo.com>.