



### Comodo IT and Security Manager

Software Version 6.14

### Quick Start Guide

Guide Version 6.14.121217

Comodo Security Solutions 1255 Broad Street Clifton, NJ 07013

COMODO Creating Trust Online

## Comodo IT and Security Manager - Quick Start

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

- Step 1 Enrollment and Configuration
- Step 2 Configure ITSM Communications
- Step 3 Add Users
- Step 4 Enroll Users' Devices
- Step 5 Create Groups of Devices (optional)
- Step 6 Create Configuration Profiles
- Step 7 Applying profiles to devices or device groups

**Note** - ITSM communicates with Comodo servers and agents on devices in order to update data, deploy profiles, submit files for analysis and so on. You need to configure your firewall accordingly to allow these connections. The details of IPs, hostnames and ports are provided in **Appendix 1**.

#### Step 1 - Enrollment and Configuration

- Note: This step explains how to enroll to ITSM as a new customer.
- Existing Comodo One users can access ITSM by logging in at <a href="https://one.comodo.com/app/login">https://one.comodo.com/app/login</a> then clicking 'Licensed Applications' > 'IT and Security Manager'.
- For more details on Comodo One services, see the online guide at <a href="https://help.comodo.com/topic-289-1-716-8478-Introduction-to-Comodo-One-MSP.html">https://help.comodo.com/topic-289-1-716-8478-Introduction-to-Comodo-One-MSP.html</a>

Getting a new Comodo ITSM subscription is very easy and can be completed in a few steps.

- Visit https://one.comodo.com/
- Click 'Sign up Now' at the top right

сомодо

# ONE (972) 649-9012

You will be taken to the Comodo One enrollment wizard:



- Enter your email address and click 'Submit'
- Next, complete the short registration form:

COMODO Creating Trust Online\*

NEW COMODO	DNE USER
Email *	
Sough Schemeny come	
Password *	
Telephone Number *	
04422592016	
I have read <u>EULA</u> and acc	cept it.
binnacle	
	Click here to reload above text.
GET NOW FO	R FREE!

- Email This will be pre-populated with the address you provided in the previous step. Enter a new email address if you wish to change it. You will receive the verification link to this email address.
- Password Create a password for your C1 account. Password rules:
  - At least eight characters long
  - Contain a mix off lower case and upper case letters
  - Contain at least one numeral - Contain at least one of the following special characters - '("!#\$%^&\*")'
- Telephone Number Primary contact number
- End User License Agreement: Read the EULA fully by clicking the 'EULA' link and select the 'I have read EULA and accept it' check box.
- **Captcha**: Type the randomly generated value to verify your application
- Click the 'Get Now for Free' button.
- A verification email will be sent to your email address. Click the link in the mail to activate your account:

COMODO Creating Trust Online\*



Hello,

Thank you for signing up to Comodo One. Please click on the link below to verify your email address and activate your account.

Verify my email

Thank you for joining The Comodo One Community!

The Comodo One Team

Please do not reply to this email as this email address is not monitored.

Comodo One Technical Support Call: 973-396-1232 (24/7) Email: <u>c1-support@comodo.com</u> MSP Forum: <u>https://forum.mspconsortium.com</u> Enterprise Forum: <u>https://forum1.comodo.com</u>

You will be taken to the C1 login page after successful verification:

COMODO ONE					
<ul> <li>Welcome to Comodo Ol with your email ar</li> </ul>	NE. You can now login nd password.				
Email or Login					
Password					
Remember Me	Forgot password?				
LOGII	N				
Available on the Apple Store	Android App an GOOGLE PLAY				
I don't have an acc	ount > Sign Up				

- Enter your email address and password and click 'Login'.
- You need to complete account registration after first-login:

#### COMODO Creating Trust Online\*

Setup Account Details	€ <u>+ Logout</u>
Email	•
anomina all'annan and counter	
Business Type *	Compare Business Types
<ul> <li>Managed Service Provider (MSP)</li> </ul>	⊖ Enterprise
Company Name *	
Subdomain * 🕖	
	Your custom support URL for your end-users: ACME.servicedesk.comodo.com
Phone Number *	
04422592016	
Country	
	\$
State	Postal Code 👻
	SUBMIT

- Complete the form with your company, location and sub-domain details to finalize account setup.
  - **Email** This field will be pre-populated with the email address entered during account creation. You cannot edit this field.
  - **Business Type** This will determine your version of Comodo One (either 'MSP' or 'Enterprise'). The modules offered with each version are as follows:

COMODO Creating Trust Online\*

Comodo One MSP	Comodo One Enterprise				
Modules included in the Comodo One Base package					
Service Desk	Service Desk				
IT and Security Manager (ITSM)	IT and Security Manager (ITSM)				
Dome Shield	Dome Shield				
Modules that can be subscribed	and added to base Comodo One				
Stand-alone Patch Management	Acronis Backup				
Acronis Backup	Comodo Quote Manager				
Comodo Quote Manager	cWatch				
cWatch	Comodo Dome Standard				
Comodo Dome Standard	Comodo CRM				
Comodo CRM	Comodo Dome Firewall Cloud				
Comodo Dome Antispam MSP	Comodo Dome Firewall Virtual Appliance				
Comodo Dome Firewall Virtual Appliance	Comodo Dome Data Protection				
	Comodo Dome Antispam				

For more details on C1 modules, see https://help.comodo.com/topic-289-1-716-8478-Introduction-to-Comodo-One-MSP.html.

- Company Name Enter the name of the business entity that you want to enroll for Comodo One.
- Subdomain The sub-domain will form part of the unique URL you use to access the standalone ITSM.
   For example, if you enter the sub-domain 'dithers' then you will access ITSM at
  - https://dithers.cmdm.comodo.com
- Phone Number Primary contact number of your company
- Country The country in which your company is located
- State The state or county in which your company is located (if applicable)
- Postal Code Your company's post or zip code (if applicable)
- Time Zone Time zone in your region. The zone you select here will be used in the ITSM console.
- Daylight Saving Time Select if applicable.
- Click 'Submit'

The next screen shows a summary of your active services:

COMODO Creating Trust Online\*

Co Fre	modo ONE MSP ee Services Out of Box	€ <u>Lo</u>	gou	t
0	IT and Security Manager	READY	^	-
	Full Mobile Device Management Full Mobile Application Management Full Mobile Security Management Bring Your Own Device Support Endpoint Security Management for Windows Devices including World Best Cont Technology (For the first month.) Community support	tainmen	t	
0	Dome Shield	READY	^	
0 0 0	DNS Based Security Domain Filtering Malware, Phishing and Botnet Protection Service Desk	READY	~	
0 0 0	Service Automation Ticketing System Multi-Site Help Desk Management Fully Integrated / One View Dashboard for all 3 Free Tools			
	Comodo One MSP Forum Subscription for FREE You are now a member of our MSP Forum partnership community v	vhere		•
		ОК		

- Click 'OK' to finish setup. You will be taken to the Comodo One Dashboard.
- Click 'Licensed Applications' > 'ITSM' to open the ITSM console
- This account will be given master 'Account Admin' privileges and cannot be deleted. You will be able to create administrators and staff under this account.
- Admins/users who enrolled via C1 can login at https://one.comodo.com/app/login
- Admins/users created in ITSM can login at https://company name>.cmdm.comodo.com/

COMODO Creating Trust Online\*

#### Step 2 - Configure ITSM Communications

In order for your ITSM server to communicate with enrolled devices, you need to install an Apple Push Notification (APN) certificate and/or a Google Cloud Messaging (GSM) Token on your portal. The following sections explain more about:

- Adding APN Certificate
- Adding GCM Token

#### Adding Apple Push Notification Certificate

Apple requires an Apple Push Notification (APN) certificate installed on your ITSM portal to facilitate communication with managed iOS devices and Mac OS devices. To obtain and implement an APN certificate and corresponding private key, please follow the steps given below:

- Step 1- Generate your PLIST
  - Click 'Settings' on the left and select 'Portal Set-Up'
  - Click 'APNs Certificate' from the top.

IT & Security Manager	
DASHBOARD >	
DEVICES	Active Directory APNs Certificate Android Client Configuration
<u>A</u> users >	
APPLICATION STORE	APNs certificate is not installed.
APPLICATIONS >	Click "Create APNs Certificate" to proceed.
SECURITY SUB-SYSTEMS	Create APNS Certificate
CERTIFICATES >	
SETTINGS V	
System Templates	
Portal Set-Up	
Subscriptions	
Support	

• Click the 'Create APNs Certificate' button to open the APNs application form.

The fields on this form are for generating a Certificate Signing Request (CSR):

COMODO Creating Trust Online\*

Generation of APNs Certificate	×
Country name *	
Select country name	~
Email address *	
Email address	
State or province name *	
State or province name	
Locality name (eg, city) *	
Locality name (eg, city)	
Organization name *	
Organization name	
Organizational unit *	
Organizational unit	
Organizational Unit Name (eg, section)	
Common name *	
Common name	
(e.g. server FQDN or YOUR name)	
	Create Reset

 Complete all fields marked with an asterisk and click 'Create'. This will send a request to Comodo to sign the CSR and generate an Apple PLIST. You will need to submit this to Apple in order to obtain your APN certificate. Usually your request will be fulfilled within seconds and you will be taken to a page which allows you to download the PLIST:

COMODO Creating Trust Online\*

Active Directory	APNs Certificate	Android Client Configuration	Windows Client Configuration	Extensions Management
Upload AF	PNs Certificate			🕞 Save
To get the o and Apple o	certificate for commu levices you need to:	nication between server		
1. Down 2. Login regul 3. Uplos Apple 4. Down .PEM 5. Click to up	nload: <u>The Apple PLIS</u> n to the <u>Apple Push Ca</u> ar Apple ID (free acco ad the PLIST from ste e will use this to gene nload your certificate I format. 'Browse', select your load it to ITSM	T Signed by Comodo ertificate Portal with your ount is enough). p 1 to the Apple portal. rate your certificate. from Apple. It will be in certificate, and click 'Save'		
Select .PE	M file Browse			

- Download your Apple PLIST from the link in step 1 on this screen. This will be a file with a name similar to 'COMODO\_Apple\_CSR.csr'. Please save this to your local drive.
- Step 2 -Obtain Your Certificate From Apple
  - Login to the 'Apple Push Certificates Portal' with your Apple ID at https://identity.apple.com/pushcert/.
  - If you do not have an Apple account then please create one at https://appleid.apple.com.
  - Once logged in, click 'Create a Certificate'.

<b>Ś</b>	Store	Мас	iPod	iPhone	iPad	iTunes	Support	٩	
Apple	Push Ce	rtificates	Portal				coyoteew	ile@yahoo.com	Sign out
Get	Started								
Create a Notificat	push certificate t tion Service and y	that enables your our Apple device	third-party se 5.	rver to work wit	h the Apple Push		1.		
Create	a Certificate						G.	th	
FAQ							PH	Ø1	>
Learn m What ab	ore about Mobile out OS X Server?	Device Managem	ent				H		
Shop the Apple Onl	ine Store (1-800-MY-/	APPLE), visit an <b>Apple F</b>	tetail Store, or find	a reseller.	Apple Info	Site Map	Hot News RSS	Feeds Conta	ct Us   🍚
Copyright © 2014	Apple Inc. All rights res	served. Terms of Use	Privacy Polic	Fγ					

You will need to agree to Apple's EULA to proceed.

#### COMODO Creating Trust Online



 On the next page, click 'Choose File', navigate to the location where you stored 'COMODO\_Apple\_CSR.csr' and click 'Upload'.

	<b>É</b>	Store	Мас	iPod	iPhone	iPad	iTunes	Support	٩	}
Ap	ople Pu	ish Cert	tificates	Portal				coyoteew	ile@yahoo.com	Sign out
	Create	a New P	oush Cert	ificate						
	Upload your vendor to cre	Certificate Sigr eate a new pusl	ning Request sig h certificate.	ned by your th	nird-party server					
	Notes									
	Vendor-Sign Choose File	ed Certificate S	Signing Request	Cancel	Upload					

Apple servers will process your request and generate your push certificate. You can download your certificate from the confirmation screen:

COMODO Creating Trust Online\*



- Click the 'Download' button and save the certificate to a secure location. It will be a .pem file with a name similar to 'MDM\_COMODO GROUP LTD.\_Certificate.pem'
- Step 3 Upload your certificate to ITSM
  - Next, return to the ITSM interface and open the 'APNs Certificate' interface by clicking Settings > Portal Set-Up > APNs Certificate.
  - Click the 'Browse' button, locate your certificate file and select it.

Active Directory	APNs Certificate	Android Client Configuration	Windows Client Configuration	Extensions Management	Þ
Upload AF	PNs Certificate			🕞 Save	
To get the c and Apple d	certificate for commu levices you need to:	nication between server			
1. Dowr 2. Logir regul 3. Uploa Apple 4. Dowr .PEM 5. Click to up Select .PEM	hload: <u>The Apple PLIS</u> in to the <u>Apple Push C</u> ar Apple ID (free acco ad the PLIST from ste e will use this to gene hload your certificate I format. 'Browse', select your load it to ITSM M file	T Signed by Comodo ertificate Portal with your ount is enough). p 1 to the Apple portal. rate your certificate. from Apple. It will be in certificate, and click 'Save'			

Click 'Save' to upload your certificate.

The APNs Certificate details interface will open:

#### COMODO Creating Trust Online\*

Active Directory APNs Certificate	Android Client Configuration	Windows Client Configuration	Extensions Management	Þ
APNs Certificate				
Certificate Details	Renew Delete	Additional Info		
Country Name India		<b>Activation Date</b> Oct 19, 2016, 6:39:37 AM		
Locality Name Madras		Expiry Date Oct 19, 2017, 6:39:37 AM		
Organization Name Coyote				
Organization Unit Name ITSM				
Common Name coyoteewile@yahoo.com				
Email coyoteewile@yahoo.com				

Your ITSM Portal will be now be able to communicate with iOS devices. You can enroll iOS devices and Mac OS devices for management.

The certificate is valid for 365 days. We advise you renew your certificate at least 1 week before expiry. If it is allowed to expire, you will need to re-enroll all your iOS devices to enable the server to communicate with them.

• To renew your APN Certificate, click 'Renew' from the iOS APNs Certificate details interface.

Active Directory	APNs Certificate	Android Client Configuration	Windows Client Configuration	Exte:
APNs Certific	ate			
Certificate D	etails	Renew	Additional Info	
Country Name India		$\smile$	Activation Date Oct 19, 2016, 6:39:37 AM	
<b>Locality Name</b> Madras			Expiry Date Oct 19, 2017, 6:39:37 AM	
Organization Nam Coyote	ne			
Organization Unit	t Name			
Common Name				

Click 'Delete' only if you wish to remove the certificate so you can generate a new APNs certificate

#### Adding Google Cloud Messaging (GCM) Token

Comodo IT and Security Manager requires a Google Cloud Messaging (GCM) token in order to communicate with Android devices. ITSM ships with a default API token. However, you can also generate a unique Android GCM token for your ITSM portal. To get a token, you must first create a project in the Google Developers console.

Please follow the steps given below to create a project and upload a token.

Step 1 - Create a New Project

Login to the Google Firebase API Console at https://console.firebase.google.com, using your • Google account. Firebase Welcome to Firebase Tools from Google for developing great apps, engaging with your users, and earning more through mobile ads. Learn more CREATE NEW PROJECT Create a project Х Project name Coyote ITSM Country/region (?) United States By default, your Firebase Analytics data will enhance other Firebase features and Google products. You can control how your Firebase Analytics data is shared in your settings at anytime. Learn more By proceeding and clicking the button below, you agree that you are using Firebase services in your app and agree to the applicable terms. CANCEL CREATE PROJECT

- Click 'Create Project'
- Type a name for the new project in the 'Project Name' field
- Select your country from the 'Country/region' drop-down
- Click 'Create Project'.

Your project will be created and the project dashboard will be displayed.

COMODO Creating Trust Online

#### COMODO Creating Trust Online\*

-	Firebase			Coyote ITSM 👻 G	io to docs
A	Coyote ITSM	Overview			?
9	Analytics				
DEV	ELOP	Welcom	ne to Firebasel Get start	ed here	
	Authentication	Welcoll			
	Database				
	Storage	i05			
$\bigcirc$	Hosting				
Ľ	Test Lab	Add Firebase to your iOS app	Add Firebase to your Android app	Add Firebase to your web app	
ŧ	Crash Reporting				
	W				

- Step 2 Obtain GCM Token and Project number
  - Click the gear icon beside the project name at the left and choose Project Settings from the
    options.



The 'Settings' screen for the project will appear.

Click the 'Cloud Messaging' tab from the top.

COMODO Creating Trust Online\*

Settings			<b>?</b>
GENERAL CLOUD MESS	AGING	ACCOUNT LINKING	SERVICE ACCOUNTS
Project credentials			
			ADD SERVER KEY
Key	Token		
Server key	AAAA5smXzi4:APA91bFl54R LNiyORVq0tJnf4A1t8ZvF0i0g MBvpVfN8_Smu2Aw3pmXZ_	H7fgZQ8TjkZSVNiWd5YsbK jMmwQHT9C2KZGyO3XxFN: ZpsVXpk6jcOj3RBtRR0Fs0	YdXSWNE9oh ZiD4wwPPpW
Legacy server key 🕥	AlzaSyAVKUfE95XhfEjDiMZL	H4yg1Kq7WXzWtLg	
Sender ID ⑦			
991224647214			
iOS app configuration			
	Y	ou don't have an iOS ap	p.

- Note down the Server key and Sender ID in a safe place
- Step 3 Enter GCM Token and Project number
  - Login to ITSM.
  - Click 'Settings' > 'Portal Set-Up' > 'Android Client Configuration' and choose 'Android Cloud Messaging' tab

#### COMODO Creating Trust Online\*



Click on the edit button concernent at the top right of the 'view the GCM token and project number fields

at the top right of the 'Cloud Messaging Token' column, to

ud Mea	ssaging Token	Info
wid (GCN A5smXzi ZvF0i0gi k6jc0j3Ri wid (GCN 2454721	(I) token (API key) 4:24PA91bFI54RH7fg2Q8Tjk25VNWd5YsbKYdX5WNE9ohLNiyORVq0tJnf4 MmwQHT9C2K2GyO3XxFNZiD4wwPPpWMBvpVIN8_Smu2Aw3pmX7_Zps BiRR0Fs0 (I) project number I4	You need to obtain Google Cloud Messaging (GCM) token in orde (IT and Security Manager) to communicate with Android devices, token, you must first create a project in the Google Developers co Please complete the following steps to get a GCM token: 1. Login to the Google Firebase API Console and click «Create 2. After choosing a project name and country/region, click the
I	Cloud Messaging Token	😵 Cancel 📔 Save
Г	Android (GCM) token (API key)	
	Android (GCM) token (API key) AAAA5smXzi4:APA91bFl54RH7fgZQ8Tjkz LNiyORVq0tJnf4A1t8ZvF0i0gMmwQHT90 MBvpVfN8_Smu2Aw3pmXZ_ZpsVXpk6jc0	ZSVNiWd5YsbKYdXSWNE9oh C2KZGyO3XxFNZiD4wwPPpW Oj3RBtRR0Fs0 :
	Android (GCM) token (API key) AAAA5smXzi4:APA91bFl54RH7fgZQ8Tjk2 LNiyORVq0tJnf4A1t8ZvF0i0gMmwQHT90 MBvpVfN8_Smu2Aw3pmXZ_ZpsVXpk6jc0 Android (GCM) project number	ZSVNiWd5YsbKYdXSWNE9oh C2KZGyO3XxFNZiD4wwPPpW Oj3RBtRR0Fs0 :

- Paste the 'Server key' into 'Android (GCM) Token' field.
- Paste the Sender ID into 'Android (GCM) Project Number' field.

СОМОДО

Cloud Messaging Token	😢 Cancel 🖺 Save
Android (GCM) token (API key)	
AAAA5smXzi4:APA91bFl54RH7fgZQ LNiyORVq0tJnf4A1t8ZvF0i0gMmwQ MBvpVfN8_Smu2Aw3pmXZ_ZpsVXp	28TjkZSVNiWd5YsbKYdXSWNE9oh 2HT9C2KZGyO3XxFNZiD4wwPPpW pk6jcOj3RBtRR0Fs0
Android (GCM) project number	

• Click 'Save'.

Your settings will be updated and the token/project number will be displayed in the same interface.

Your ITSM Portal will be now be able to communicate with Android devices using the unique token generated for your ITSM portal.

#### Step 3 - Add User

- Comodo One Staff Staff created by C1 enterprise customers will be automatically added as users/staff to ITSM. Staff created by C1 MSP customers will automatically be added to ITSM and will be available as users/staff for all companies.
- ITSM Users C1 enterprise and ITSM stand-alone customers can add users with appropriate role for a single company via ITSM. C1 MSP customers can create multiple companies and add users/staff to them accordingly. You can group users/devices under different companies (for C1 MSP customers) as explained in Step 5 - Create Groups of Devices.

#### To add a user

- Click 'Users' on the left then 'User List', then click the 'Create User' button
   or
- Click the 'Add' button
   at the menu bar and choose 'Create User'.

IT & Security Manager	≡ User List	License Options 🔁 🛈
DASHBOARD >		🛔 Create User
DEVICES >		<ul> <li>Enroll Device</li> </ul>
	Enroll Device Create User Manage Profiles Send Password Recovery Email	
User List		
User Groups	🗋 💿 Dyanora dyanor	
Role Management	Samsung avant	
CONFIGURATION TEMPLATES >	💼 🕘 Tab user impair	

The 'Create new user' form will open.

#### COMODO Creating Trust Online\*

Create new User	Close
Username *	
avantistude	
Email *	
avantistude@gmail.com	
Phone number	
0123456	
Company *	
Dithers Company	-
Assign role	
Administrators	-
Su	bmit

- Type a login username (mandatory), email address (mandatory) and phone number for the user
- Choose user's company (mandatory)
  - Comodo One MSP Users The drop-down will list companies added to C1. Choose which company the user should be enrolled under.
  - Comodo One Enterprise and stand-alone ITSM users Leave the selection as 'Default Company'.
- Choose user role. A 'role' determines user permissions within the ITSM console itself. ITSM ships with four default roles:
  - Account Admin Can login to the ITSM administrative interface and access all management interfaces. This will not be listed here since it will be automatically assigned only to the person who opens a C1 account. This role is not editable.
  - Administrators Can login to the ITSM administrative interface and access all management interfaces. This role can be edited according to your requirements.
  - Technician Can login to the ITSM administrative interface and access all management interfaces. This role can be edited according to your requirements.
  - Users Can login to the ITSM interface and view only the dashboard part of the application. This
    role can be edited according to your requirements.

You can create roles with different permission levels via the 'Role Management' screen (click 'User' > 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.



• Click 'Submit' to add the user to ITSM.

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

• Repeat the process to add more users.

If you create an administrator then an account activation mail will be sent to their registered email address.

Tip: ITSM also allows you to import users/user groups from Active Directory using LDAP. Imported users will be placed into ITSM with the same group structure as used in AD. ITSM will periodically synchronize with AD to ensure any changes to AD users are mirrored in the ITSM database. See Importing User Groups from LDAP for more details.

#### Step 4 - Enroll Users' devices

The next step is to enroll user devices for management.

- Each license allows you to enroll up to five mobile devices or one Windows endpoint per user. So 1 user license will be consumed by 5 mobile devices and 1 license will 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.

#### To enroll devices

- Click 'Users' then 'User List'
- Select the user(s) whose devices you wish to enroll then click the 'Enroll Device' button above the table Or





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

#### COMODO Creating Trust Online\*

Enroll Devices	Close
Please choose the device owner(s) * mmoxford@yahoo.com	
Show Enrollment Instructions	Email Enrollment Instructions

The 'Please choose the device owner(s)' field is pre-populated with any users you selected in the previous step.

- To add more users, start typing first few letters of the username and choose from the results
- If you want enrollment instructions to be displayed in the ITSM interface, click 'Show Enrollment Instructions'. This is useful for administrators attempting to enroll their own devices.
- If you want the enrollment instructions to be sent as an email to users, click 'Email Enrollment Instructions'.
- A confirmation dialog will be displayed.

Enroll Devices Cl	ose
Instruction e-mail has been sent to selected user(s). The user should navigate to the lin on a device that is going to be enrolled.	k
Show Enrollment Instructions Ok	

A device enrollment email will be sent to each user. The email contains instructions that will allow them to enroll their device. An example mail is shown below.

COMODO Creating Trust Online

COMODO

### Welcome to IT and Security Manager!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet, Mac or Windows device into the IT and Security Manager 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:

ITSM

 Please make sure you follow the correct procedure for your type of device - Mac, Windows, iOS or Android.

- 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 - <u>https://demoq3-</u> <u>msp.dmdemo.comodo.com:443/enroll/device/by/token/ae7d8e58f5af4a2b277135d132bdb31</u> 0

Sincerely, IT and Security Manager team.

Clicking the link will take the user to the enrollment page containing the agent/profile download and configuration links.

COMODO Creating Trust Online

#### Welcome to IT and Security Manager!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet or Windows device into the IT and Security Manager 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 - Mac, Windows, iOS or Android.
- 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.

#### FOR LINUX DEVICES

Download and install Comodo Client application by tapping the following link:

https://demoq3-msp.dmdemo.comodo.com:443/enroll/linux/run/to ken/370522bb23b6fb954dc2b64ce199183a Use the same link for manual enrollment if required.

1) Change installer mode to executable:

\$ chmod +x {\$installation file\$}

#### 2) Run installer with root privileges:

\$ sudo ./{\$installation file\$}

#### **FOR APPLE DEVICES**

 Enroll opening the following link with any browser on your device:

https://demoq3-msp.dmdemo.comodo.com:443/enroll/apple/index /token/370522bb23b6fb954dc2b64ce199183a

2.a) [ONLY for Mac OS X Devices] When you have installed *itsm.mobileconfig* file, use this link to download and install Comodo Client application: https://static.dmdemo.comodo.com/download/itsmagent-installer.p kg

#### 2.b) [ONLY for iOS Devices]

When your profile has been enrolled, you will be requested to install Comodo Client application. Upon completion of the installation, tap the green icon labeled "Run after installation" and follow on-screen instructions to complete enrollment process.

#### FOR ANDROID DEVICES

Download and install Comodo Client application by tapping the following link:

https://play.google.com/store/apps/details?id=com.comodo.mdm

Upon completion of the installation, enroll using this link: https://demoq3-msp.dmdemo.comodo.com:443/enroll/android/ind ex/token/370522bb23b6fb954dc2b64ce199183a

#### FOR WINDOWS DEVICES

Enroll using this link: https://demoq3-msp.dmdemo.comodo.com:443/enroll/windows/m si/token/370522bb23b6fb954dc2b64ce199183a

### Use the following settings:

Host: demoq3-msp.dmdemo.comodo.com Port: 443 Token: 370522bb23b6fb954dc2b64ce199183a

Sincerely, IT and Security Manager team,

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.



#### **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:

emenment.
FOR ANDROID DEVICES
Download and install the Comodo ONE Client app by tapping the following link: https://play.google.com/store/apps/details?id=com.comodo.mdm
After installation, enroll by this link: https://dithers_construction_company-coyote-msp.cmdm.comodo.c om:443/enroll/android/index/token/554fd18d57eef662e8b908a9a1 86f811
MANUAL ENROLLMENT

- 1. User opens the enrollment page on the target device and taps the 1st link to install the ITSM app.
- 2. After the app has been installed, the user clicks the 2nd link to enroll their device to ITSM. The app will connect to ITSM then request the user to tap 'Activate' to enroll the device.

#### Enroll iPhones, iPods and iPads

The device enrollment page contains an enrollment link under 'FOR APPLE DEVICES'. Users should tap this link to install the ITSM client authentication certificate and ITSM profile.

COMODO Creating Trust Online\*



**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.

- After the profile has been installed, the client app installation will begin.
- The app is required so that ITSM can manage the remote device:



• The app will be downloaded and installed from the iTunes store. End-users may need to login with their

COMODO Creating Trust Online\*

#### Apple ID.

 After installation, users should tap the green 'Run After Install' icon on the home screen to complete registration:



The device will be enrolled and connected to ITSM.

#### **Enroll Mac OS X Devices**

#### Step 1 - Install the ITSM Configuration Profile

The device enrollment page contains an enrollment link under 'FOR APPLE DEVICES'. The user clicks this link to download the ITSM profile and install it.

COMODO Creating Trust Online



On completion of installation, the profile will be added to the Device Profiles list in the Mac OS X device.

Device Profiles	Oomodo IT	
Comodo ITSM 2 settings	COMODO GROUP LT	<b>SM</b> D. Verified
	Description Configuration	T and Security Manager
	Signed *.cmdm.comod	lo.com
	Installed 08-Jul-2016, 2	2:11 PM
	Settings SCEP Enrollme	nt Request
	Mobile Device	Management
	DETAILS	
	Mobile Device Management	
	Description COMODO GRO	OUP LTD. ITSM
	Remuer https://covote.	

The next step is to install the ITSM agent for connection to the ITSM server and complete the enrollment.

#### Step 2 - Install ITSM Agent

• Next the user click the link under 'Only For Mac OS X Devices' to download the ITSM agent for Mac.

61811
FOR APPLE DEVICES
1) Enroll by opening this link on your device: https://dithers_construction_company-coyote-msp.cmdm.comodo.c om:443/enroll/apple/index/token/554fd18d57eef662e8b908a9a18 6f811
2.a) [ONLY For Mac OS X Devices] After <i>itsm.mobileconfig</i> file has been installed, please download and install the Comodo Client from: https://dl.cmdm.comodo.com/download/itsmagent-installer.pkg
2.b) [ONLY For iOS Devices] After profile enrollment, you will be asked to install the Comodo Client. After installation, tap the green icon labelled "Run after installation" then follow the on-screen installations to finish enrollment.

The agent setup package will be downloaded and the installation wizard will start.

You wil softwar	be guided , version	through the 5.3.0.122.	steps neces	sary to install	this

The user follows the wizard and completes the installation.

Once installation is complete, the agent will start communicating with the ITSM server.

COMODO

•••	Install Comodo Client - Communication	
	The installation was completed successfully.	
<ul> <li>Introduction</li> <li>License</li> <li>Destination Select</li> </ul>		
<ul> <li>Installation Type</li> <li>Installation</li> <li>Summary</li> </ul>	The installation was successful. The software was installed.	
	Go Back Close	

#### **Enroll Windows PCs**

The device enrollment page contains a single enrollment link under 'For Windows Devices'.

ана тападе apps, and егазе ааа
Enroll by this link: https://dithers_construction_company-coyote-msp.cmdm.comodo.c om:443/enroll/windows/msi/token/554fd18d57eef662e8b908a9a18 6f811

The user clicks this link to download the ITSM client app. Once installed, the app will enroll the device into ITSM.

[ Enrol	→ Device	Manage Profiles	 Takeover	Install MSI/Packages	Install OSX Packages	Siren Off	ा अ Siren On	Send Message	More
	<b>0</b> S	NAME	ACTIVE	COMPONENTS	PATCH STATUS	COMP	ANY	OWNER	LAST ACTIVITY
		DESKTOP-8	AG	AV FW SB	<b>A</b> 1	Dithers	s Constru	Dagwood	2016/09/02 09:03:1
		• DESKTOP-T	AG	AV FW SB	<b>A</b> 1	Dithers	s Constru	Angel Snow	2016/09/02 08:42:3
	_, <u>``</u> ,	LENOVO Le	an the start			Dither	Constru-	boo	Q0/02.05

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

The 'Device List' interface contains a list of all enrolled devices with columns that indicate the device IMEI, owner,

COMODO

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.

#### **Enroll Linux Devices**

The device enrollment page contains a single enrollment link under 'For Linux Devices'.

and manage apps, and remotely erase data on your device.
FOR LINUX DEVICES
Download and install Comodo Client application by tapping the
following link: https://demoq3-msp.dmdemo.comodo.com:443/enroll/linux/run/to ken/370522bb23b6fb954dc2b64ce199183a
Use the same link for manual enrollment if required.
1) Change installer mode to executable:
1) Change installer mode to executable: \$ chmod +x {\$installation file\$}
<ol> <li>Change installer mode to executable:</li> <li>\$ chmod +x {\$installation file\$}</li> <li>2) Run installer with root privileges:</li> </ol>

• Click on the enrollment link under 'For Linux Devices' and save the file.

The ITSM agent setup file will be downloaded.

You can install the ITSM agent in your Linux device by first changing installer mode to executable and running the installer with root privileges in the command terminal:

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

\$ chmod +x {\$installation file\$}

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

\$ sudo ./{\$installation file\$}

For example:

chmod +x itsm\_cTjlw6gG\_installer.run sudo./itsm\_cTjlw6gG\_installer.run

COMODO Creating Trust Online\*



That's it. The Linux device will be enrolled and displayed in the devices list. Currently you can view the device status and online status. Other features such as security client, patch management, procedures and so on will be supported in future ITSM versions.

#### Step 5 - 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 each group. OS specific profiles which are applied to a group will be deployed appropriately to devices.

- C1 MSP customers can create separate device groups for each Company/Organization enrolled in their Comodo One account.
- C1 Enterprise and ITSM stand-alone customers can only create groups under the 'Default Company'.

Refer to Managing Companies if you need more help with this.

#### To create a device group

- · Click the 'Devices' tab on the left and choose 'Device List'
- Click the 'Group Management' tab
- C1 MSP customers should choose the company whose devices they wish to manage on the left
- Click 'Create Group' on the top right pane
- · Alternatively move the mouse over the company name and click the '+' sign that appears at the right

COMODO Creating Trust Online\*

Search group name     Group Management     Search group name	<b>、</b> ¦¦;
C All Devices	
→ ▲ ABC TV Services     ▲ Create Group     Manage Profiles     → ▲ ABC TV Services     ▲	Crea
+ 🖶 Chennai IT Services	
- 🖶 Coyote NAME - 🖶 Coyote	
- 🔁 Default Group - Coyote	
- 🔁 Default Group	
Sales	
- B Deer Company	
Results per page: 20 - Default Group - Deer	Resul
— 🔁 Default Group	

The 'Add Group' interface will open:

Add Group	Close
Name * Running Staff	
Company * Deer Company	
Devices	
Type device name to search among devices	
	Add

- 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 'OK'. Repeat the process to create more groups.

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

#### Step 6 - Create Configuration Profiles

A configuration profile is a collection of settings which can be applied to mobile devices and PCs and Mac OS X devices that have been enrolled to Comodo IT and Security 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 ITSM app is uninstalled from the device or the profile itself is modified/removed/disabled by the administrator.

Profile specifications differ between Android, iOS, Mac OS X and Windows Devices:

- Android profiles
- iOS profiles
- Mac OS X profiles
- Windows Profiles

#### To create an Android Profile

- · Click the 'Configuration Templates' tab on the left and choose 'Profiles'.
- Click 'Create' drop-down above the table and then choose 'Create Android Profile'.

IT & Security Manager	■ Profiles	License Options
DASHBOARD >		
DEVICES >	Profiles Default Profiles	
Susers >		di Eò
CONFIGURATION TEMPLATES V	Create Import Export Profile	e Clone Profile Delete Profile
Profiles	Create Android Profile	CREATED BY
Alerts	Create iOS Profile	coyoteewile@yahoo.c 25.
APPLICATION STORE	Create OS X Profile Create Windows Profile	ne coyoteewile@yahoo.c 20
	Certificate Optimise	coyoteewile@yahoo.c
Create Android Profile		×
Name *		
Name		
Description		
Description		
		Create

• 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.

🗭 Androi	d Devices in	Purchase	Dept.		
Add Profile Section	Export Profile	Clone Profile	Delete Profile	Kake Default	
General	Settings	_	_	_	₩ Edit
Name * Android De Display nam Is Default Disabled	evices in Purchase ne of the profile (sh	Dept. own on the device)	).		
Descriptio For Androi Brief explar	n Id phones and taba hation of the conten	s used by purcha ts or purpose of th	se dept. staff e profile		

If you want this profile to be a default policy, click the 'make default' button at the top. Alternatively, click the

'Edit' button Edit on the top right of the 'General' settings screen and enable the 'Is Default' check box.

• Click 'Save'.

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

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

COMODO

Android Devices	in Purchase	Dept.	
Add Profile Section	e Clone Profile	Delete Profile	ES Make Defaul
Antivirus Settings			
Bluetooth Restrictions	/PN Wi-Fi		
Browser Restrictions			
Certificate			
CCM Certificates			
Email	se Dept.		
ActiveSync Settings	shown on the device	).	
Kiosk			
Native App Restrictions			
Network Restrictions	ents or purpose of the	ise dept. staff he profile	
Passcode			Same .
Restrictions			
VPN			
Wi-Fi			
Other Restrictions			

The settings screen for the selected component will be displayed and, after saving, the new section will become available as a link. 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 ITSM profile.

- Click 'Save' in each configuration screen for the parameters and options selected in that screen to be added to the profile.
- **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.
- Antivirus Settings Schedule antivirus scans on the device and specify trusted Apps to be excluded from AV scans.
- 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.
- Browser Restrictions Configure browser restrictions such as to allow pop-ups, javascript and cookies. This profile is supported for SAFE devices only.
- 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.
- CCM Certificates Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Note - The 'CCM Certificates' section will appear only if you have integrated your ITSM server with your CCM account. For more details, see the online help page Integrating with Comodo Certificate Manager in the ITSM online help guide.
- 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.
- Active Sync Settings 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.

COMODO

### Comodo IT and Security Manager - Quick Start Guide

- Kiosk Enable and configure Kiosk Mode for SAFE devices like 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.
- 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.
- 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.
- 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'.
- **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.

#### To create an iOS Profile

- Click the 'Configuration Templates' tab on the left and choose 'Profiles'.
- Click the 'Create' drop-down above the table and then choose 'Create iOS Profile' from the profiles.

COMODO Creating Trust Online\*

IT & Security Manager		License Options
DASHBOARD >		
DEVICES	Profiles Default Profiles	
Q USERS >		e" Eô
CONFIGURATION TEMPLATES	Create Import Export Pr	ofile Clone Profile Delete Profile
Profiles	Create Android Profile	CREATED BY
Alerts Procedures	Create iOS Profile Preate OS X Profile Create Windows Profile	coyoteewile@yahoo.c
Create iOS Profile		×
Name *		
Name		
Description		
Description		
		Create

- 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.

COMODO Creating Trust Online\*

iOS Pro	ofile for Pure	chase Dept						
Add Profile Section	Export Profile	Clone Profile	Delete Profile	Kake Default				
General	Settings			_				₹ Edi
Name * IOS Profile Display nam	e for Purchase Dep ne of the profile (sh	ot. own on the device)					L	
<b>is Default</b> Disabled								
Descriptio For iPhone Brief explar	n es and iPads used nation of the conten	by purchase dep its or purpose of th	artment staff e profile					

• If you want this profile to be a default policy, click the 'Make default' button at the top. Alternatively, click the

'Edit' button Edit on the right of the 'General' settings screen and enable the 'Is Default' check box.

• Click 'Save'.

The next step is to add components for the profile.

COMODO Creating Trust Online

5		63	1 into	ഭ	
Add Profile Section	Export Profile	Clone Profile	Delete Profile	Make Default	
Air Play					
Air Print					
APN					
Calendar					
Cellular Netw	orks				
Certificate					
CCM Certifica	ntes <sup>no</sup>	wn on the device	.).		
Contacts					
ActiveSync Se	ettings				
Global Proxy I	HTTP nt	by purchase dep s or purpose of t	ot staff he profile		
LDAP					
Email					
Passcode					
Proxy					
Restrictions					
Single Sign-O	n				
Subscribed C	alendars				
VPN					
Per-App VPN					
Web Clip					
Wi-Fi					
App Lock					

 Click the 'Add Profile Section' drop-down 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 new section will become available as a link. 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 ITSM profile.

- Click 'Save' in each configuration screen for the parameters and options selected in that screen to be added to the profile.
- **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.
- Airplay Allows you to whitelist devices so they can take advantage of Apple Airplay functionality (iOS 7 +)
- Airprint Specify the location of Airprint printers so they can be reached by devices under this profile (iOS 7 +)
- **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 poxy host server. The APN setting is replaced by the 'Cellulars' setting in iOS7 and over.
- **Calendar** Configure CalDAV server and connection settings which will allow device integration with corporate scheduling and calendar services.
- **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.
- **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.
- CCM Certificates Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Note - The 'CCM Certificates' section will appear only if you have integrated your ITSM server with your CCM account. For more details, see the online help page Integrating with Comodo Certificate Manager in the ITSM online help guide.
- **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).
- Active Sync Settings- Specify account name, host, domain and other settings to facilitate connections from devices under this profile to Microsoft Exchange Active Sync servers.
- **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.
- LDAP Configure LDAP account settings for devices under this profile so users can connect to company address books and contact lists.
- **E-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.
- **Proxy** Allows you to specify the proxy server, and their credentials, to be used by the device for network connections.
- **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.
- 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.
- Subscribed Calendars Specify one or more calendar services which you wish to push notifications to devices under this profile.
- 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. This profile is supported for iOS 7 and above.

- VPN Per App Configure VPN as above but on a per-application basis. This profile is supported for iOS 7 and above.
- 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.
- 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.
- App Lock Configure restrictions on usage of device resources for selected applications.

#### To create Mac OS X Profile

- Click the 'Configuration Templates' tab on the left and choose 'Profiles'.
- Click 'Create' drop-down above the table and then click 'Create OS X Profile'

		≡	Profiles				
DASHBOARD	>						
DEVICES	>		Profiles	Default	Profiles		
USERS	>		ĽЦ	LT			
CONFIGURATION TEMPLATES	~		Create	Import	Export Profile	Clone Profile	Delete Profile
Profiles			Create Ar	ndroid Pro	file		CREATED
Alerts			Create iO	S Profile	for Win	dows Devices	covoteoui
Procedures	<b>(</b> )	0	Create OS	S X Profile		dows Devices	Coyoteewa
			Create W	indows Pr	ofile		
Create US X Profile							×
Name *							
Name *							
Name * Name Description							
Name * Name Description Description							
Name * Name Description Description							
Name *          Name         Description         Description							

- Enter a name and description for the profile (for example, 'Sales Dept Mac machines', 'Mac Air Books' or 'Field Executives Laptops') and click 'Create'.
- The profile will be created and the 'General Settings' for the profile will be displayed.

COMODO Creating Trust Online\*

Mac (	OS Profile fo	r Stores De	pt		
Add Profile Section	Export Profile	Clone Profile	Delete Profile	📙 Make Default	
General General	Settings	_			₹ Edit
Name * Mac OS P Display nar Is Default Disabled	rofile for Stores De me of the profile (sh	pt own on the device	).		
Descriptio Profiles fo Brief explai	n Ir Mac devices in s nation of the conten	tores ts or purpose of th	e profile		

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

The next step is to add components for the profile.

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



- 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.
- **Certificates** Upload certificates and this will act as a certificate store from which the certificates can be selected for use in other settings like 'Wi-Fi and 'VPN'.
- CCM Certificates Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Note - The 'CCM Certificates' section will appear only if you have integrated your ITSM server with your CCM account. For more details, see the online help page Integrating with Comodo Certificate Manager in the ITSM online help guide.
- Restrictions Configure restrictions on device functionality and features, iCloud access and so on.
- 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 and more.
- 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.

#### To create a Windows profile

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

IT & Security Manager		■ Profiles			License Optio	ns 🔁 🕯
DASHBOARD >						
DEVICES		Profiles	Default	Profiles		
<u>A</u> USERS >		Щ.	Ę			
		Create	Import	Export Profile	Clone Profile	Delete Profile
Profiles		Create Ar	ndroid Pro	ofile	CREATED B	
Alerts Procedures (i)		Create iO Create O	S Profile	e	coyoteewile	
	<	Create W	indows P	rofile		
Create Windows Profile	Ľ					×
Name						
Description						
Description						
					Crea	ate

- 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.

Financ	e Departme	ent Window	s Computer	'S		
Add Profile Section	Export Profile	Clone Profile	Delete Profile	📙 Make Default		
General						
General	Settings					
Name * Finance De	epartment Windov	vs Computers				
<b>Is Default</b> Disabled						
Descriptio Profile for	<b>n</b> Windows devices	in finance dept.				

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

The next step is to add components for the profile.

• Click the 'Add Profile Section' drop-down and select the component that you want to include in the profile.

The settings screen for the selected component will be displayed and, after saving, the new section will become available as a link in this interface. You can configure Antivirus, Firewall, Containment, File Rating, Valkyrie, HIPS, VirusScope and Update settings. In addition, you can configure the Proxy and Agent Discovery Settings 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 ITSM profile.

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

COMODO Creating Trust Online\*

### Comodo IT and Security Manager - Quick Start Guide



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.
- CCS Update Rule Set the conditions for Comodo Client Security (CCS) to automatically download and install program and virus database updates.
- 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 CCS, refer to the help page explaining File rating Settings in CCS 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 CCS, refer to the help page explaining Firewall Settings in CCS 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 CCS, refer to the help page explaining
  HIPS Settings in CCS online help guide

COMODO Creating Trust Online\*

- Containment Enable Auto-containment of unknown files, add exclusions, and configure containment behavior and alert options and view and manage Containment Rules for auto-containing applications. For more details on Containment in CCS, refer to the help page explaining Containment in CCS online help guide.
- VirusScope Enable VirusScope 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 VirusScope in CCS, refer to the help page explaining VirusScope in CCS 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.
- Proxy Allows you to specify a proxy server to be used by the device for network connections.
- Agent Discovery Settings Allows you to specify whether or not Comodo Client should send logs to ITSM above antivirus and containment events.
- CCS UI Settings Allows you to to specify Comodo Client Security user interface settings.
- Logging Settings Allows you to enable logging events from CCS, the maximum size of the log file and configure behavior once log file reaches the maximum file size.
- **Monitoring Settings** Allows you to configure performance and availability conditions for various events and services. An alert will be triggered if the conditions are breached. For example, you can monitor free disk space, service and web page availability, CPU/RAM usage, device online status and more.
- CCM Certificates Allows you to add requests for client and device authentication certificates to be issued by Comodo Certificate Manager (CCM). Note - The 'CCM Certificates' section will appear only if you have integrated your ITSM server with your CCM account. For more details, see the online help page Integrating with Comodo Certificate Manager in the ITSM online help guide.
- Procedures Allows you to add, view, delete and prioritize procedures which have been added to a profile.
- **Remote Control** Allows you to configure notifications which are shown to end-users before and during a remote control session.

#### Step 7 - Apply profiles to devices or device groups

- Click the 'Devices' link on the left then choose 'Device List'
- · Click the 'Device Management' tab at the top of the main configuration pane
  - Select a Company and choose a group under it to view the list of devices in that group Or
  - Select 'All Devices' to view every device enrolled to ITSM
- Select the device to be managed and click 'Manage Profiles' from the options at the top

COMODO Creating Trust Online\*



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

• 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.

COMODO Creating Trust Online\*

Manag	e Profile	es of DESKTOP-TTPO9PR	
Add Profiles	)		
Remo	ove Profiles		T
🗆 os	ТҮРЕ Р	PROFILE NAME	OWNER
	## \$31	PC with 1TB hard drive	coyoteewile@yahoo.com
	e P	Purchase Dept Computers	coyoteewile@yahoo.com
Results per	r page: 2		Displaying 1-2 of 2 results.
Results per	ofiles to	DESKTOP-TTPO9PR	Displaying 1-2 of 2 results.
Results per Add Pro	r page: 2	DESKTOP-TTPO9PR	Displaying 1-2 of 2 results.
Results per Add Pro	ofiles to	DESKTOP-TTPO9PR	Displaying 1-2 of 2 results.
Results per Add Pro	ofiles to	DESKTOP-TTPO9PR	Displaying 1-2 of 2 results.           Visit Comparison           OWNER           coyoteewile@yahoo.com
Results per Add Pro	ofiles to	DESKTOP-TTPO9PR	Displaying 1-2 of 2 results.
Add Pro	TYPE P F	DESKTOP-TTPO9PR	Displaying 1-2 of 2 results.
Results per Add Pro	TYPE P F F S S S S S S S S S S	DESKTOP-TTPO9PR PROFILE NAME For Bobs PC For Coyote Cert Vindows Profile for local desktops Stores Test Components disabled	Displaying 1-2 of 2 results.
Results per Add Pro	TYPE P F F F F F F F F F F	DESKTOP-TTPO9PR  PROFILE NAME For Bobs PC For Coyote Cert Windows Profile for local desktops Stores Test Components disabled Sales Team PCs	Displaying 1-2 of 2 results.

- Select the profile(s) to be applied to the device
- 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 on the left and choose 'Device List ' from the options.
- 2. Click the 'Group Management' tab
- 3. Choose the Company to view the list of groups in the right pane (for C1 MSP customers)
- 4. Click the name of the device group
- 5. Click 'Manage Profiles'
- 6. Select the profile(s) to be applied to the devices in the group
- 7. Click 'Add Selected' on the top left to add the selected profile(s) to the device group

COMODO Creating Trust Online

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.

### **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.

The Comodo Threat Research Labs is a global team of IT security professionals, ethical hackers, computer scientists and engineers analyzing and filtering input from across the globe. The team analyzes millions of potential pieces of malware, phishing, spam or other malicious/unwanted files and emails every day, using the insights and findings to secure and protect its current customer base and the at-large public, enterprise and internet community.

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. With offices in the US, China, Turkey, India, Romania and Ukraine, Comodo secures the online and offline eco-systems of thousands of clients worldwide.

#### Comodo Security Solutions, Inc.

Comodo Security Solutions, Inc 1255 Broad Street. Clifton, NJ 07013 United States Tel : +1.888.266.6361 Tel : +1.703.581.6361 Email: EnterpriseSolutions@Comodo.com

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