

How to set up Remote Control for End-User

Introduction

MSP customers can configure Endpoint Manager settings to allow end-user to access their computer remotely while working from home. This wiki helps you to achieve it.

Process In Detail

- Login to the Xcitium
- Create a profile and configure it
- Set the profile as “default” so that newly enrolled devices get the profile automatically
- Create a separate device group for each user
- Create a separate role?for each user
- Configure the role permission
- Create user accounts with an associated role for end-user
- Instructions for end-user

Create a profile and configure it

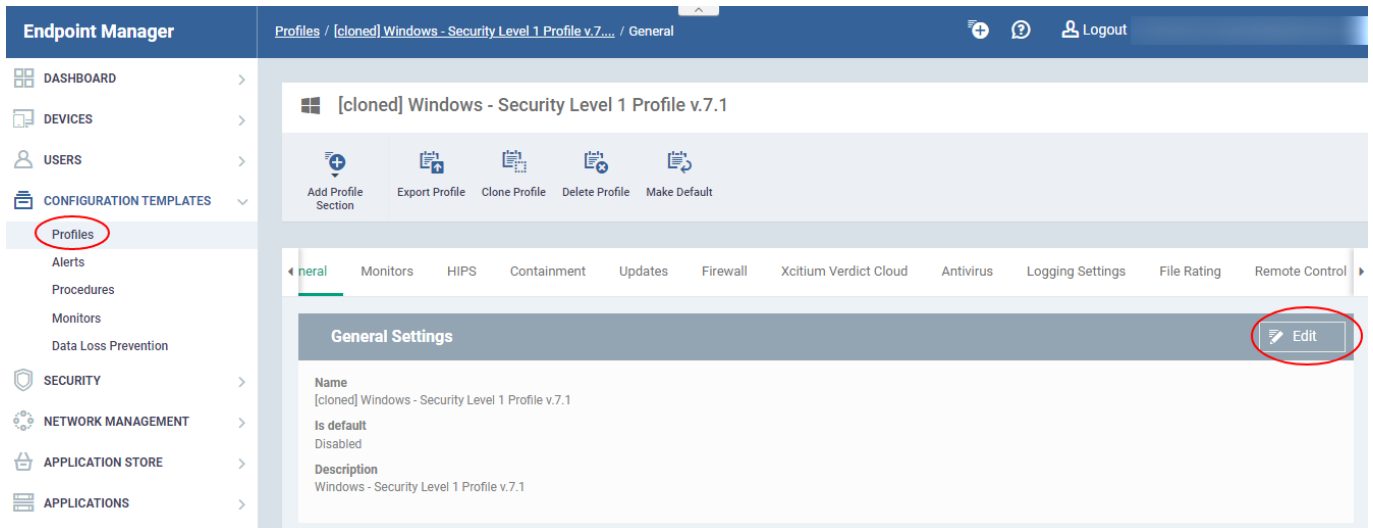
- Go to?Configuration Templates - > Profiles
- Click the name of the Windows or MAC profile that you want to work on
- Select the Profile you want to apply changes

Select a profile...

The screenshot displays the Endpoint Manager interface. On the left, the 'CONFIGURATION TEMPLATES' menu is expanded, and 'Profiles' is highlighted with a red circle. The main area shows a table of profiles. The table has the following data:

<input type="checkbox"/>	OS	NAME	CREATED BY	CREATED	UPDATED AT
<input type="checkbox"/>	Windows	Windows - Containment Only Profile ...	admin	2022/07/22 10:43:11 AM	Not updated
<input checked="" type="checkbox"/>	Windows	[cloned] Windows - Security Level 1 P...	comodo-pm-support@yopmail.com	2022/06/28 11:15:44 AM	2022/06/28 05:25:44 PM
<input type="checkbox"/>	Windows	cloned[cloned] [cloned] Windows - Se...	comodo-pm-support@yopmail.com	2022/05/27 04:20:19 PM	Not updated
<input type="checkbox"/>	Windows	[cloned] Windows - Security Level 1 P...	comodo-pm-support@yopmail.com	2022/05/11 12:20:19 PM	2022/05/27 05:32:19 PM
<input type="checkbox"/>	Windows	[cloned] Windows - Security Level 1 P...	comodo-pm-support@yopmail.com	2022/03/01 08:18:14 AM	Not updated
<input type="checkbox"/>	Windows	[cloned] Windows - Security Level 1 P...	comodo-pm-support@yopmail.com	2021/09/16 11:57:30 AM	2021/09/16 12:29:08 PM
<input type="checkbox"/>	Windows	TNS Monitors	comodo-pm-support@yopmail.com	2021/06/23 02:45:20 PM	2021/06/23 02:45:44 PM
<input type="checkbox"/>	Windows	sample_prof_without_default	comodo-pm-support@yopmail.com	2021/06/15 05:40:15 PM	2021/06/15 05:41:21 PM

- Click Edit and check Is default to set the profile as the default



- Click Save.
- Click the Remote Control tab?(or click Add Profile Section > Remote Control)
- Click Edit
- Enable Device Takeover gives you full control of the remote device'.?Use the On/Off button to enable the device to take over the session
- Select the ' Establish Remote Control sessions without asking user permission ' option.

'Establish Remote Control sessions without asking user permission'...



Device Takeover

File Transfer

Device Takeover Options

Apply to all

ON

NAME	DESCRIPTION	STATE
Device Takeover	Enable/disable device takeover session using Remote Control application	ON

Establish Remote Control sessions without asking user permission

Ask user, wait and allow access (waiting time is shown below) (seconds) ⚠

30

If the user is logged in: ask permission and connect if the user allows it or doesn't respond within the specified time

If the user is not logged in: proceed with Remote Control session

Ask user, wait and deny access (waiting time is shown below) (seconds) ⚠

60

If the user is logged in: ask permission and connect only upon user approval

If the user is not logged in: proceed with Remote Control session

Message to Device User

Your IT administrator would like to view and control your desktop. Please click "Allow" to start remote session.

Client Notification Options

- Show notification to device user about who connected to his/her workstation
- Allow endpoint user to terminate the connection
- Keep notification windows open upon remote session termination

Protocol Options

Ports that will be applied are UDP ports only, please make sure your firewall configurations are compatible with the UDP settings

Use WebRTC ⚠ **CC 6.17+**

Allow multiple connections **CC 6.42+**

Set at least 1 port

Port(s)

WinXP : 1025 - 5000 range by default

Win7+ : 49152 - 65535 range by default

Use Chromoting **CC 6.17+**

Set at least 4 ports

Ports

49152 - 65535 range by default

- Go to 'File Transfer' Tab
- Use the On/Off button to enable the permissions

- **Establish File Transfer sessions without asking user permission?**- Connects without the user permission
- **Select the Ask user, wait and allow access (waiting time is shown below) (seconds)**-?If the user is logged in they ask permission and connect if the user allows it or doesn't respond within the specified given time
- **Ask user, wait and deny access (waiting time is shown below) (seconds)** -?If the user is logged in ask permission and connect only upon user approval, If the user is not logged in it will proceed with Remote Control session

'Establish File Transfer sessions without asking user permission '...



Remote Control Cancel Save

Device Takeover **File Transfer**

File Transfer Options **CC 6.29+**

Apply to all **ON**

NAME	DESCRIPTION	STATE
File Transfer	Enables read-only access to remote devices (parent permission for other permissions allowing for extended capabilities)	ON
Send & Receive Folders & Files	Download and upload files/folders to/from the local device using Remote Control application	ON
Create, Delete, Rename actions	Create, delete and rename files/folders using Remote Control application at the local device	ON

Establish File Transfer sessions without asking user permission
 Ask user, wait and allow access (waiting time is shown below) (seconds)

If the user is logged in: ask permission and connect if the user allows it or doesn't respond within the specified time
If the user is not logged in: proceed with Remote Control session
 Ask user, wait and deny access (waiting time is shown below) (seconds)

If the user is logged in: ask permission and connect only upon user approval
If the user is not logged in: proceed with Remote Control session

Message to Device User

Your administrator needs to remotely access your device to perform routine security maintenance which will not interfere with your work.

Client Notification Options

Show notification to device user about who connected to his/her workstation
 Allow endpoint user to terminate the connection
 Keep notification windows open upon remote session termination

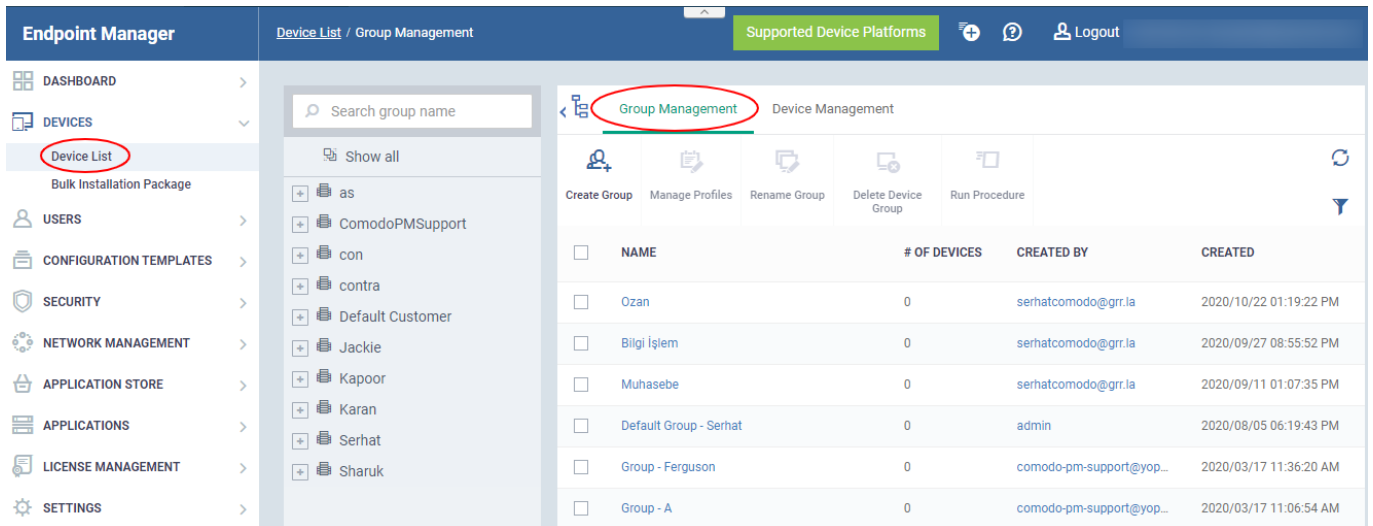
- Click Save

Create Separate Device Groups for Each Employee

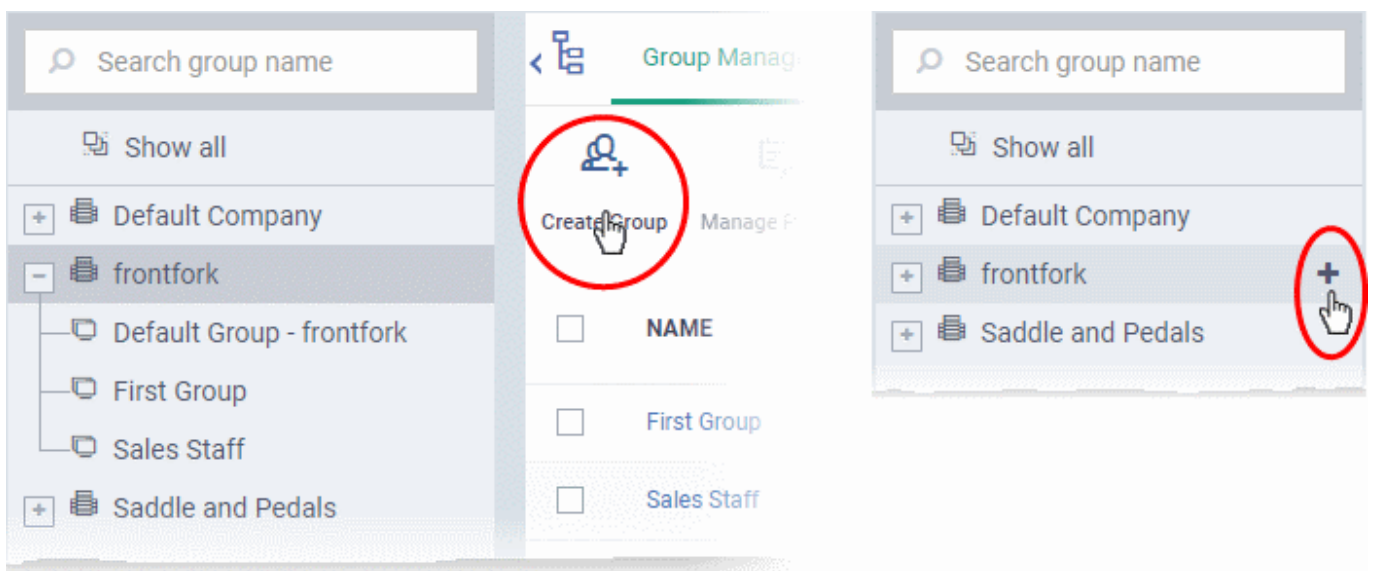
- Click Devices > Device List > Group Management

Create Separate Device Groups...





- Click the Create Group button



×

Add Group

Name *

Customer *

Devices

Add

- Fill Name and Company sections and click Add.
- Repeat the process to add separate groups for each employee.

Create Separate User Roles for Each Employee

- Click Users > Role Management

×
+ ? Logout

Endpoint Manager

Roles Users

+ Add role
Export ▾
↻
⏮

NAME	DESCRIPTION	# OF USERS
Login Permission	Users with only login permission	0
admin	control	1
serhat	serhat	0
Role_S [default]	Role assigned for staff_technician	0
Role_Std	Only permitted user can access	0
Users	Users of the system	2
Account Admin	Account Admin of the system	3

- Create a role by clicking Add Role
- Create a name for the role for example? employee_device_management



Endpoint Manager		Role Management / Roles		Logout
DASHBOARD	>	Roles Users		
DEVICES	>	Add role Export		
USERS	>	Refresh Filter		
User List				
User Groups				
Role Management				
CONFIGURATION TEMPLATES	>			
SECURITY	>			
NETWORK MANAGEMENT	>			
APPLICATION STORE	>			
APPLICATIONS	>			
NAME	DESCRIPTION	# OF USERS		
serviceeee	test	0		
userss	test	0		
adminis1	test	0		
employee_device_management	employee-device-management is to assign this role for the user Ferguson	2		
Technician	Technician of the system	8		
Administrators	This is the super administrator role that has maximum privilege and needs to contain at least one user.	6		

- Add a description to the role?
 - The created new role will be displayed in the Roles section
 - Click the created role to assign the role and permission for that.

Role Permissions?- Explains the access rights and privileges to the users

Assign Users?- Select the users to assign a role

Access Scope?- Select which companies or groups can be accessed by the members

Role permissions

- Click the Role permission tab?

Each item in the list lets you choose permissions for a specific area.

- Click the down arrow next to a module name to view its permissions

OR

- Click 'Expand' at the top to view all permissions
- Use the switches on the right to enable or disable specific permissions
- Enable “users.allow-portal-login” permission for the user to be able to login to Remote Control Application.
- Enable the Remote Control tab to access the device for remote
- Click 'Save' for your settings to take effect

Set up the Role Permissions...



employee_device_management

Make Default

Delete Role Edit

Role Permissions Assign Users Access Scope

Save Expand Apply to all OFF

Read Only Portal Access to portal elements in read only mode. OFF

PERMISSION	DESCRIPTION	ACTION
users.allow-portal-login	Ability to login to portal, access to 'User Settings' and 'Support' pages.	ON <input type="checkbox"/>
Dashboard		
Devices		
Remote Control		
remote-control	Allows access to Remote Control functionality and list devices on Remote Control tool. Parent permission is 'users.allow-portal-login'	ON <input type="checkbox"/>
remote-control.takeover	Allows to establish Remote Control session. Parent permission is 'remote-control'.	ON <input type="checkbox"/>
remote-control.file-transfer	Allows to view files at the remote device. Parent permission is 'remote-control'.	ON <input type="checkbox"/>
remote-control.file-transfer.crud	Allows to view and copy/read/update/delete (CRUD) files at the remote device. Parent permission is 'remote-control.file-transfer'.	ON <input type="checkbox"/>
remote-control.file-transfer.download	Allows to download files from the remote device. Parent permission is 'remote-control.file-transfer'.	ON <input type="checkbox"/>
remote-control.file-transfer.upload	Allows to upload files to the remote device. Parent permission is 'remote-control.file-transfer'.	ON <input type="checkbox"/>
User		
Configuration templates		
Network management		
App store		
Applications		
Security sub-systems		
Licence management		
Settings (Templates)		
Settings (Portal Set-Up)		
Settings (Apple DEP)		

Access Scope

- Click the 'Access Scope' tab

This shows the list of which companies or groups can be accessed by the members of the Endpoint manager

Role Permissions Assign Users Access Scope

 Save


Apply to all ON

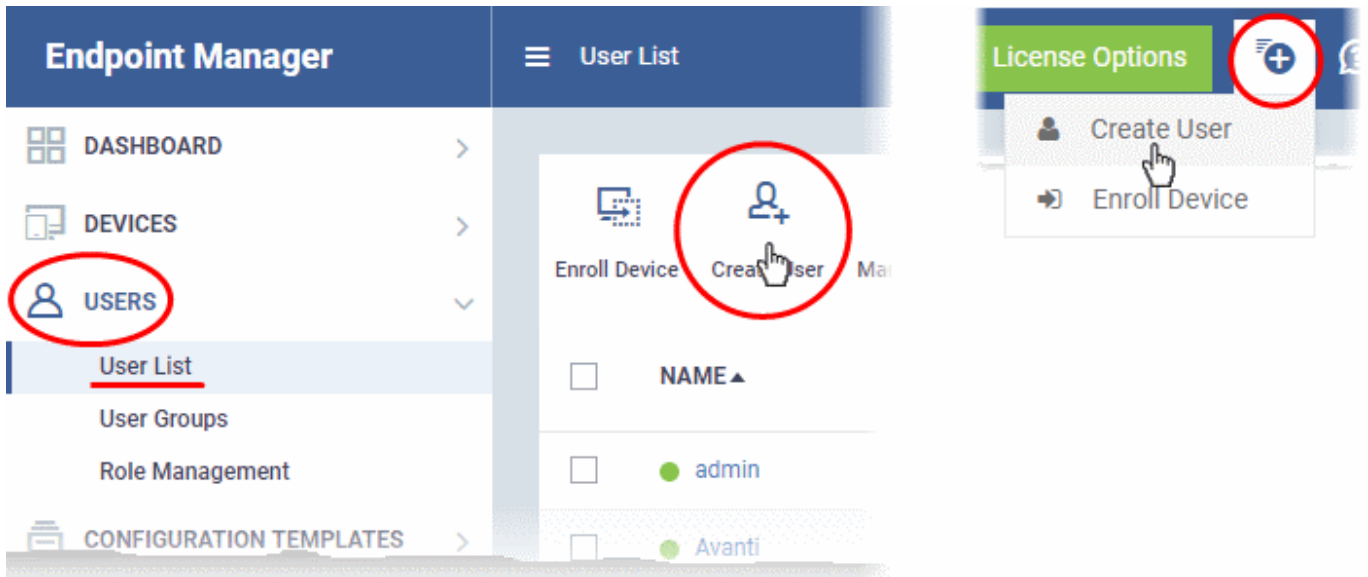
CUSTOMER	GROUP	ACTION
ComodoPMSupport	varun	<input type="checkbox"/> OFF
ComodoPMSupport	Ashny	<input type="checkbox"/> OFF
Sharuk		<input type="checkbox"/> OFF
Sharuk	Default Group - Sharuk	<input type="checkbox"/> OFF
Kapoor		<input type="checkbox"/> OFF
Kapoor	Default Group - Kapoor	<input type="checkbox"/> OFF
Jackie		<input type="checkbox"/> OFF
Jackie	Default Group - Jackie	<input type="checkbox"/> OFF
Karan		<input checked="" type="checkbox"/> ON
Karan	Default Group - Karan	<input type="checkbox"/> OFF
Karan	Group - B	<input type="checkbox"/> OFF
Karan	Group - A	<input type="checkbox"/> OFF
Karan	Group - Ferguson	<input checked="" type="checkbox"/> ON

You can configure the company by clicking the *enable/disable* button under the company name.

- Choose a related Company and Device Group
- Click 'Apply To All' to access all the companies and groups
- Click the Save button to make the changes take effect.

Create Users

- Click 'Users' > 'User List'
- Click the 'Create User' button or Click the “Add” button  at the menu bar and choose 'Create User'.



The 'Create New User' appears:

Create New User ✕

User Name *

Email *

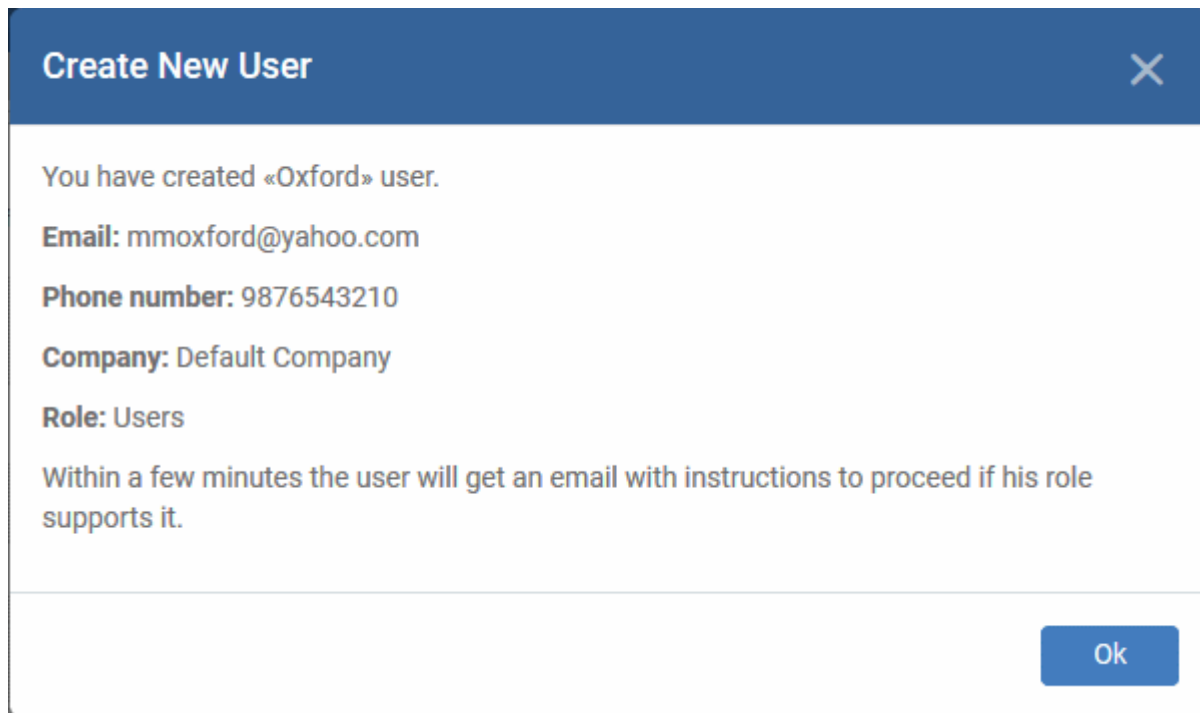
Phone Number

Customer *

Assign Role

- Enter the details, select the role for the new user and click the 'Submit' button.

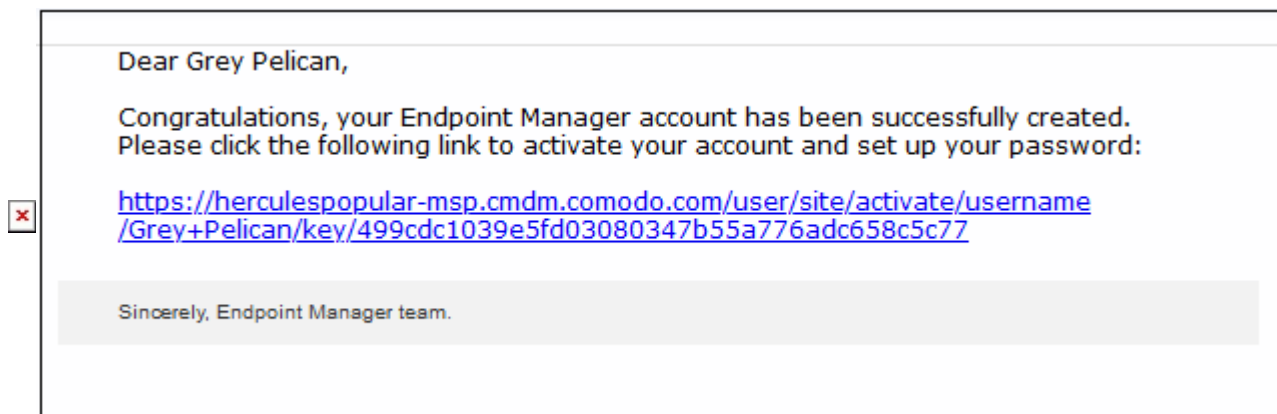
A confirmation will be displayed:



- Repeat the process to add more users.

Successfully added users will be listed in the 'Users' interface. The user's devices can now be enrolled to EM.

Endpoint Manager will send account activation mails to the newly added users. They can activate their account and set their login password by clicking the link in the email. An example of mail is shown below:



- User clicks the link and activates his EM account
- Upon activation, the user will be able to login to EM with his user-name and password. Log in at: [https://\[your company name\]-msp.cmdm.comodo.com/](https://[your company name]-msp.cmdm.comodo.com/) as shown in the mail link
- Users added via EM can log in to EM console only and cannot log in to Dragon / C1 portal
- If the portal administrator has configured two-factor authentication, then the user has to follow the on-screen instructions to set up this during login.

Endpoint Manager will send device enrollment link to the user email. They can click to the link on the email to enrol their devices.

Welcome to Endpoint Manager!

You are receiving this mail because your administrator wishes to enroll your smartphone, tablet, macOS, Linux or Windows device into the Endpoint 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:

- Make sure that you selected the operating system of the device that you want to enroll.

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.

Device Enrollment:

[Click this link to enroll your device](#)

Move Devices to Related Device Groups after Enrollment is Complete

- Click 'Devices' > 'Device List'
- Click the name of a device then select the 'Groups' tab:



Select Groups tab...



	GROUP NAME	CUSTOMER	# OF DEVICES	CREATED BY	CREATED
<input type="checkbox"/>	Flying Squad Devices	Default Customer	1	herculespopular22...	2018/10/26 05:18...
<input checked="" type="checkbox"/>	First Group	Default Customer	4	herculespopular22...	2018/10/26 05:19...

- Click 'Add to Group'

File List Exported Configurations MSI Installation State Patch Management Antivirus Scan History

 Add to Group  Remove from Group

<input type="checkbox"/>	GROUP NAME	COMPANY	NUMBER OF DEVICES	CREATED BY
<input type="checkbox"/>	Default Group	Deer Company	3	Impala
<input checked="" type="checkbox"/>	Innotek PCs	Deer Company	1	coyoteewile@yahoo.com
<input type="checkbox"/>	Running Staff	Deer Company	4	coyoteewile@yahoo.com

Results per page: 20

Add Device to Group Close

Choose group(s)

To add groups, start typing their names

The 'Add Device to Group' dialog will appear.

- Start typing the name of the group which you want the endpoint to join. Select the correct group from the list of suggestions.
- Click 'Add'.

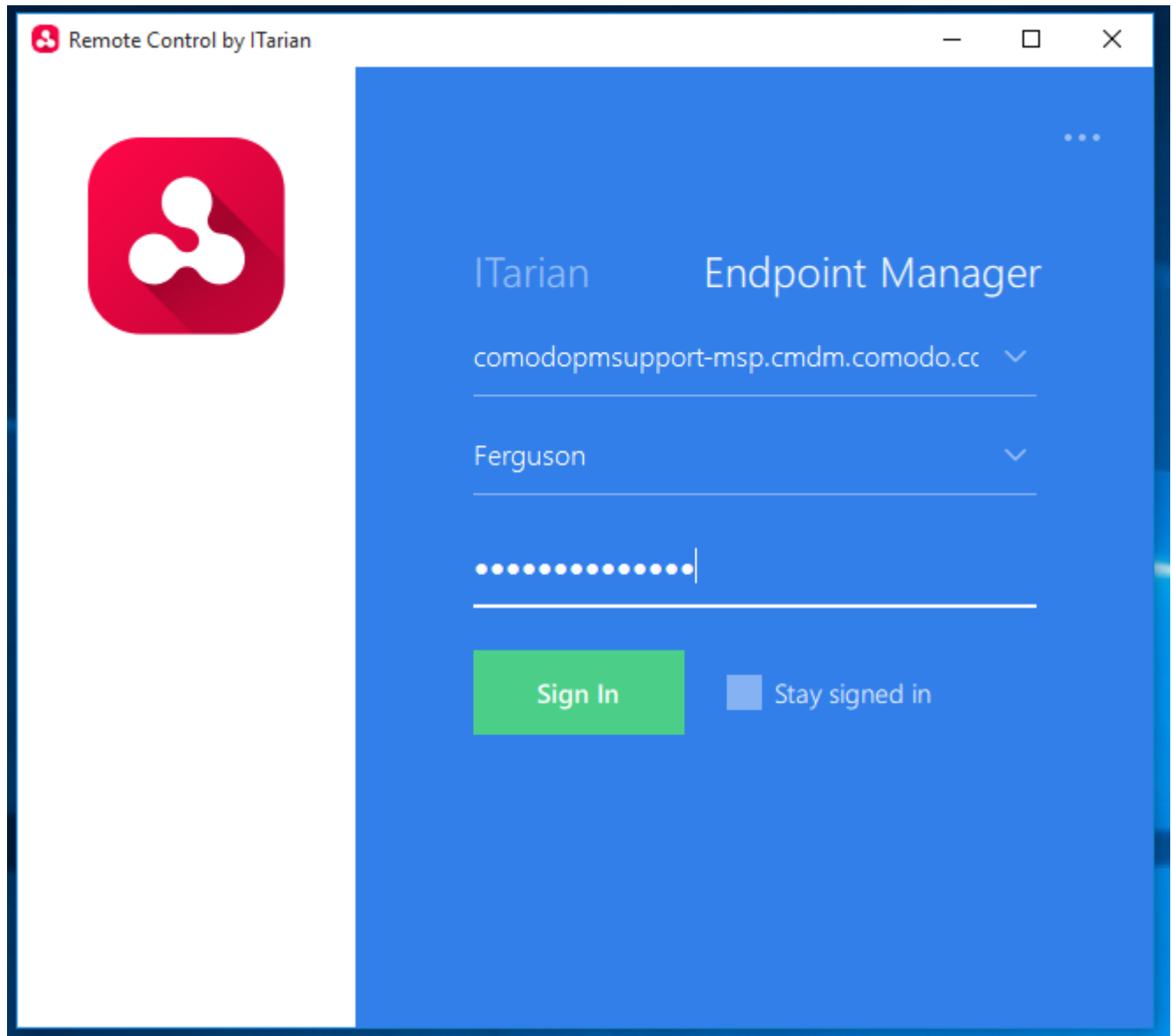
The device will be added to the group or groups.

- Repeat the process for all enrolled devices.

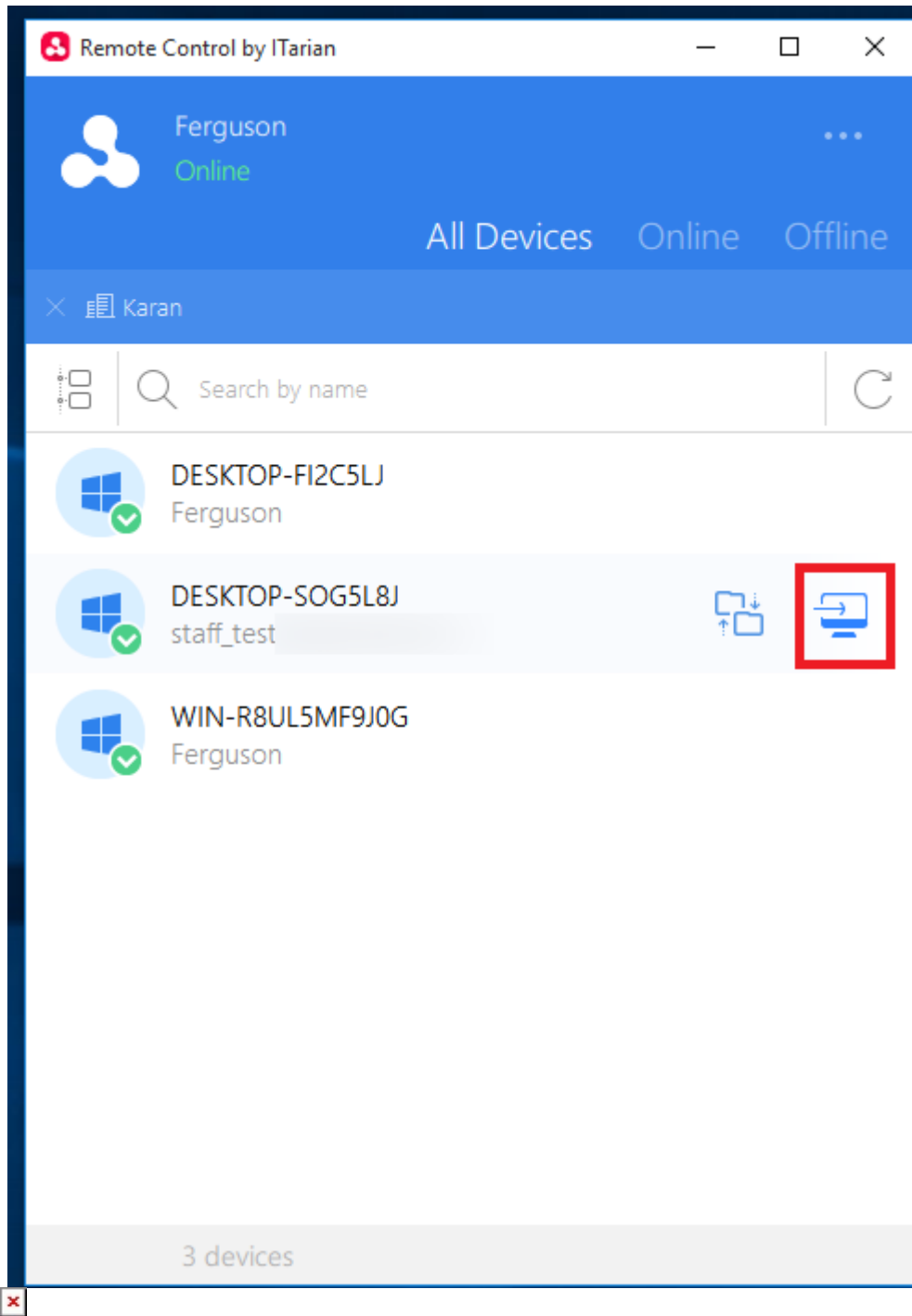
Instruction for the End-User Settings

Login into the remote Device

- Click the invitation link that sends to your default mail id
- Set up the Password as per the standards
- Download the Remote Control App from the Comodo One/ Dragon site
- Log in with the Domain name, Username and password that you applied



- After login, you can view the applied device to your remote environment
- You can view the enrolled devices here
- Select the devices to start the remote control



After that, the window will open like this...

