

How to manage users and their devices

Click 'Users' > 'User List'

- The user list shows all users and staff you have enrolled to Endpoint Manager.
- From here, you can add and manage users, enroll user devices, apply profiles to devices, run procedures, and more.
 - See [this wiki](#) if you need help to add users
 - See [this wiki](#) if you need help to add user devices

See the following links for further help:

- [The user list interface](#)
- [Manage users and their devices](#)
 - [User information](#)
 - [View devices associated with a user](#)
 - [View user device enrollment tokens](#)
 - [View and manage a user's group membership](#)
 - [Apply profiles to user devices](#)
 - [Send a password recovery mail to a user](#)
 - [Reset password for a user](#)
 - [Reset two-factor authentication token for a user](#)
 - [Run procedure on user devices](#)

The user list interface

- Login to Comodo One / Dragon
- Click 'Applications' > 'Endpoint Manager'
- Click 'Users' > 'User List':



	NAME	EMAIL	PHONE NUMBER	# OF DEVICES	2FA STATUS	LAST LOGIN
<input type="checkbox"/>	Oxford	mmoxford@yahoo.com	9876543210	0	Not active	Not logged in yet
<input type="checkbox"/>	bsachamp@yop...	bsachamp@yopmail.co	N/A	0	Not available	2020/04/01 11:41:0...
<input type="checkbox"/>	John	fiatlina@gmail.com	9876543210	1	Not active	Not logged in yet
<input type="checkbox"/>	John Duncan	maruthicelerio@gmail.c	N/A	0	Not active	Not logged in yet
<input type="checkbox"/>	Alice	aliceroadster@gmail.cc	9876543210	2	Not active	Not logged in yet
<input type="checkbox"/>	joesmith	coyoteewile@yopmail.c	N/A	0	Not active	Not logged in yet
<input type="checkbox"/>	ssgalia@yahoo...	ssgalia@yahoo.com	N/A	0	Not available	2019/08/12 10:46:1...
<input type="checkbox"/>	fsregionaltrans...	fsregionaltransport@gr	N/A	0	Not available	Not logged in yet
<input type="checkbox"/>	Herald	hertriumph@gmail.com	1234567890	1	Not active	Not logged in yet

Name - First and last name of the user.

- Click the name of a user to view and edit their details.
- See [manage users and their devices](#) later in this wiki for more info.

Email - The registered email address of the user. Account activation and device enrollment mails are sent to this address.

Phone Number - The registered contact number of the user.

Number of Devices - The total count of devices enrolled for the user.

2FA Status - States whether two-factor authentication (2FA) is enabled for the user.

- **Active** - 2FA is enabled and the user has completed the setup process.
- **Not active** - The user has not yet completed the 2FA setup process. 2FA may or may not be enabled in the portal.
- **Not configured** - 2FA was reset by an admin and the user is yet to re-configure it.
- **Not available** - Indicates the user was added via the Comodo One / Dragon portal. For these users, 2FA is configured in Comodo One / Dragon.

Setup 2FA in Comodo One / Dragon– Login to Comodo One / Dragon > Click 'Management' > 'Account' > 'Account Security Details' > 'Enable Two factor Authentication'. See [this help page](#) for more.

Setup 2FA in Endpoint Manager – Open Endpoint Manager > Click 'Settings' > 'Portal Management' > 'Account Security' > 'Force users to use 2FA'. See [this help page](#) for more.

- The preferred option is to setup in Comodo One / Dragon. Doing so enables 2FA for the Comodo One / Dragon portal AND Endpoint Manager AND other Comodo One / Dragon modules such as Service Desk.

Last Login - Date and time that the user most recently accessed EM.

The controls on the top lets you perform various actions:

Enroll Device - Add user devices for management by EM. You can enroll Android, iOS, Mac, Windows and Linux devices.

- See [this wiki](#) if you need help to enroll user devices

Create User - Manually add users to EM.

- You can only add devices for users after you have enrolled the users themselves. See [this wiki](#) if you need help to add new users.
- You can convert a user into an admin by assigning them an appropriate role. See [this wiki](#) for help to assign roles.

Manage Profiles - A profile determines the security configuration and network access rights of a device.

- See [apply profiles to user devices](#) for help to assign profiles to a user devices.

Send Password Recovery Email - Reset the password of users who have admin privileges. The password allows them to login to the EM console.

- See [send password recovery email to a user](#) for more details.

Change Password - Generate new password for a user.

- See [reset password for a user](#) if you need help.

Delete User - Terminate selected user accounts.

Import User - Bulk add new users by importing them from a comma separated values (CSV) file.

- See [this wiki](#) if you need help to import users from a .csv file

Export - Save a copy of the current user list as a comma separated values (.csv) file.

- The exported .csv is available at 'Dashboard' > 'Reports'

Reset 2FA Token - Force users to configure new two-factor authentication codes.

- See [Reset Two Factor Authentication Token](#) for more help on this.

Run Procedure - Execute stand-alone instruction scripts and patches on all Windows devices belonging to a user.

- See [Run Procedures on User Devices](#) for more help with this.

Manage users and their devices

- Click 'Users' > 'User List'
- Click on the name of a user

The user details screen opens:

☰ User List + ? 👤

Enroll Device
Create User
Manage Profiles
Send Password Recovery Email
Change Password
Delete User
Import User
Run Procedure

<input type="checkbox"/>	NAME	EMAIL	PHONE NUMBER	# OF DEVICES	2FA
<input checked="" type="checkbox"/>	Oxford	mmoxford@yahoo.com	9876543210	2	Not
<input type="checkbox"/>	bsachamp@yo...	bsachamp@yopmail.cc	N/A	0	Not
<input type="checkbox"/>	John	fiatliena@gmail.com	9876543210	1	Not
<input type="checkbox"/>	John Duncan	maruthicelerio@gmail.c	N/A	0	Not

☰ [User List](#) / [Oxford](#) / User Info

Oxford

Enroll Device
Manage Profiles
Send Password Recovery Email
Delete User
Run Procedure
Reset 2FA Token

User Info
Associated Devices
User Tokens
Groups

Personal
Edit

Username
Oxford

Email
mmoxford@yahoo.com

Phone number
9876543210

Roles
[Administrators](#)

Customer
Default Customer

Change password time
Not changed yet

Time add
2020/04/01 03:52:39 PM

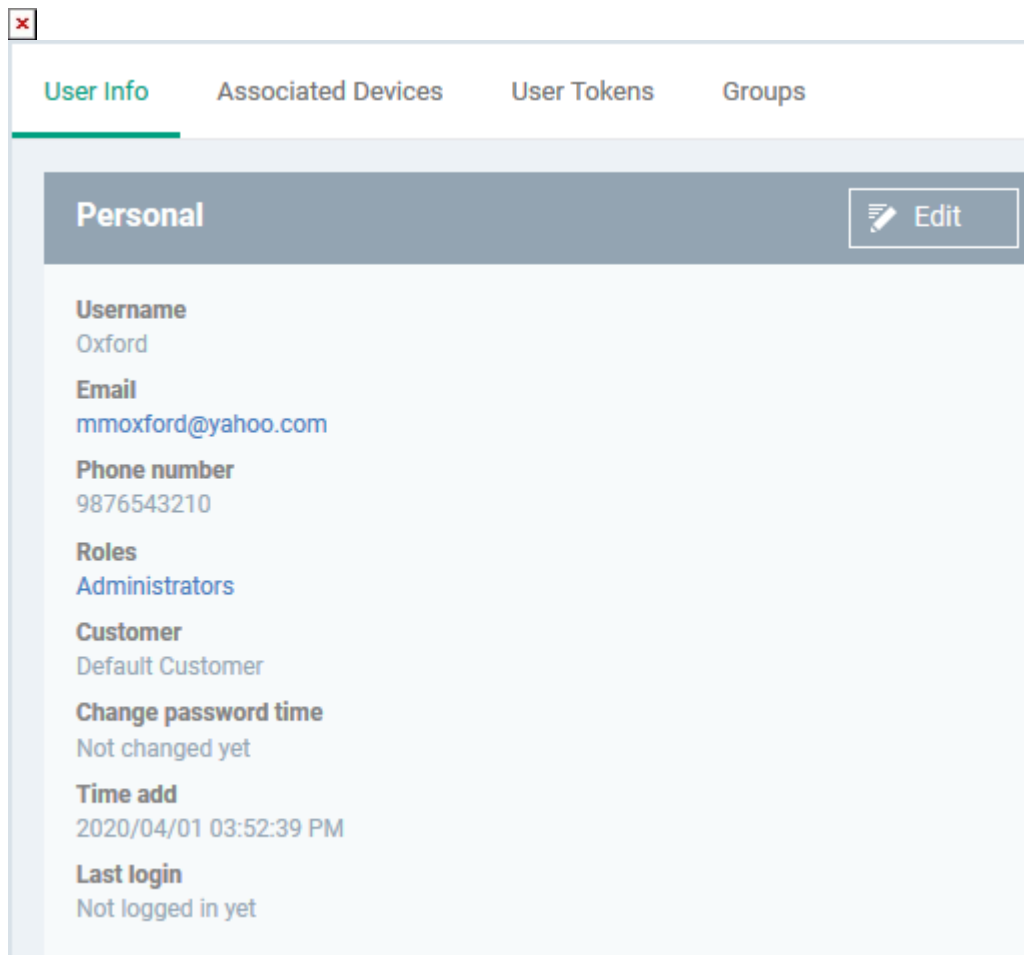
Last login
Not logged in yet

The details screen has four tabs:

- [User Info](#) – View and edit user contact details and their Endpoint Manager role.
- [Associated Devices](#) - Shows devices owned by the user.
- [User Tokens](#) - Shows the device enrollment tokens generated for the user.
- [Groups](#) - Shows the user groups of which the user is a member. You can add the user to new groups or remove the from groups.

View and update user information

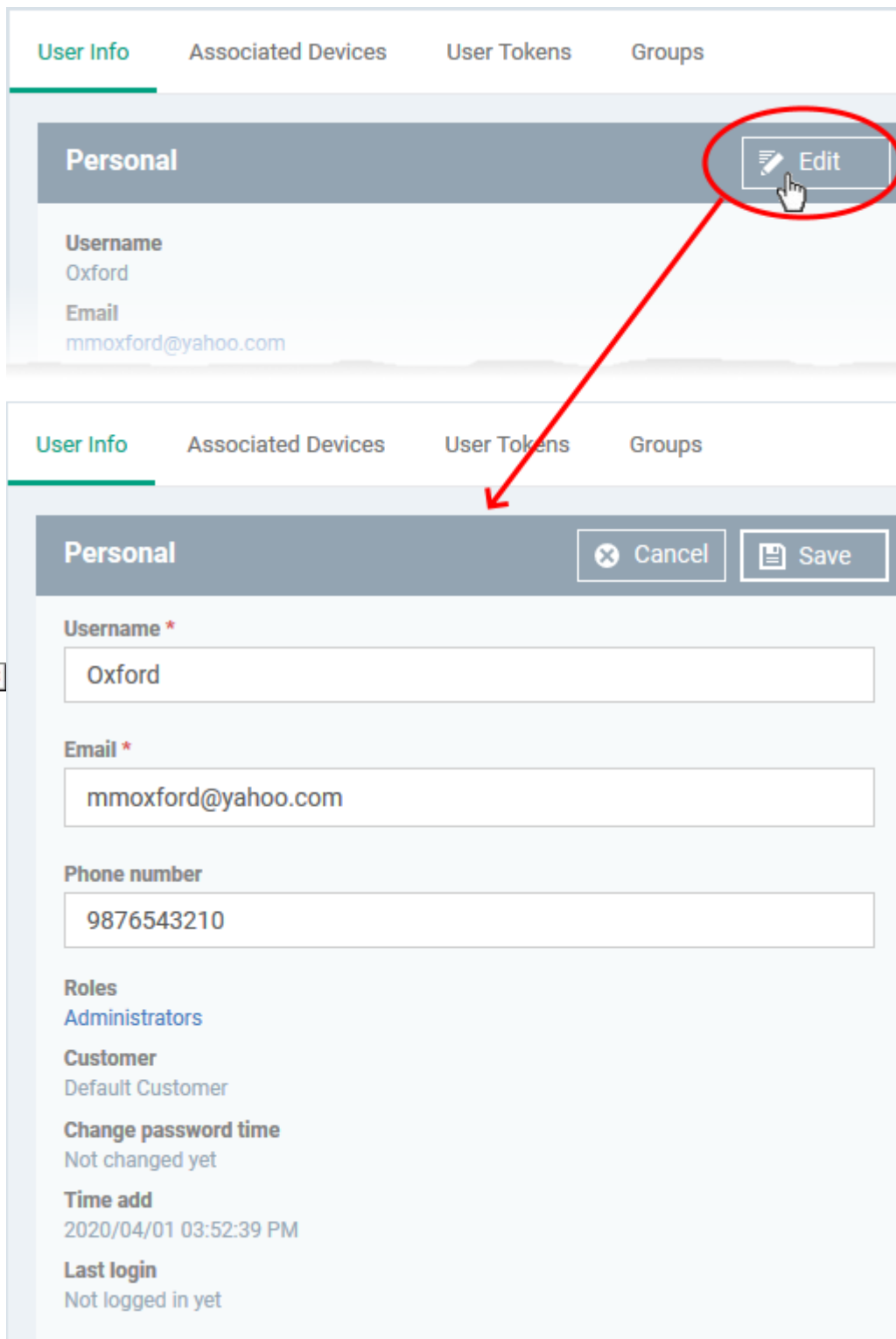
- Click 'Users' > 'User List'
- Click the name of a user
- Click the 'User Info' tab , if not already open.



The screenshot shows a web interface with four tabs: 'User Info', 'Associated Devices', 'User Tokens', and 'Groups'. The 'User Info' tab is selected and highlighted. Below the tabs is a 'Personal' section with an 'Edit' button. The details listed are:

- Username**: Oxford
- Email**: mmoxford@yahoo.com
- Phone number**: 9876543210
- Roles**: [Administrators](#)
- Customer**: Default Customer
- Change password time**: Not changed yet
- Time add**: 2020/04/01 03:52:39 PM
- Last login**: Not logged in yet

- The tab shows user contact details, the role of the user, and more
- Click the 'Edit' button to update their details



- Update the username, email and phone number as required.
- Click the role name to change their role if required. See [this wiki](#) to read more about roles.
- Click 'Save' at the top for your changes to take effect


View devices associated with a user


- Click 'Users' > 'User List'
- Click the name of a user


- Click the 'Associated Devices' link


This tab shows all devices enrolled for the user:


Herald



Enroll Device


Manage Profiles






Send Password Recovery Email


Delete User


Run Procedure


Reset 2FA Token

User Info
Associated Devices
User Tokens
Groups

OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	CUSTOMER	LAST ACTIVITY
	 Redmi	AG AV		Saddle and Pedals	2020/04/02 03:47:49 ...
	 TECHMON...	AG AV FW CO	1	Saddle and Pedals	2020/04/02 03:45:35 ...

OS - The operating system of the device.

Name - The label of the device as assigned by the user or local admin.

- If no name exists, the model number is used as the device name.
- Click the name of a device to view its details. See '[View summary information](#)' if you need more info on the details screen.

Active Components - The endpoint security modules running on the device. Possible components are 'Agent' (AG), 'Antivirus' (AV), 'Firewall' (FW) and 'Containment' (CO). See [this page](#) for a more detailed explanation of the icons in this table.

Patch Status - How many OS patches and updates are ready to install on the endpoint. Patch status is only available for Windows devices.

- Click the number to open the 'Patch Management' tab of the 'Device Details' interface. You can initiate installation of the missing patches.
- See [this wiki](#) to read more about managing patches on individual devices.

Customer - The customer organization to which the device is registered.

Last Activity - The date and time at which the device last communicated with the EM server.

View user device enrollment tokens

- Endpoint Manager generates a unique token for each user when you enroll a device for them.
- This token is used by the client on the device to verify the enrollment request.

- A single token can be used to enroll multiple devices for the same user. A token is valid for 720 days.
- The user tokens screen lists all tokens generated for the user. You can use these tokens to manually enroll devices for the user.

View user tokens

- Click 'Users' > 'User List'
- Click the name of a user
- Click the 'User Tokens' link

TOKEN	EXPIRATION DATE	DAYS LEFT
4bad349ea56dea78c2c4e745f818d05c	2022/03/23 12:21:04 PM	720
63b7d584e6b472f39b9fe6f9daf6e643	2021/12/01 12:28:50 PM	608
876ccf4f65f06b5541fbffc5adfa0a12	2021/12/01 12:28:42 PM	608
26463a8d4b298761a5c0739ab0285514	2021/12/01 12:26:58 PM	608
c2795e966011b35511dcc7c56332a421	2021/11/02 05:38:39 AM	579
f173a725da08de19458a1e0c395e49f1	2021/11/02 05:33:37 AM	579

Token - The unique serial number of the token.

Expiration Date - Date till which the token is valid. Users can enroll devices using the same token until expiry.

Days left - How many days remain until the token expires.

View and manage a user's group membership

- Click 'Users' > 'User List'
- Click the name of a user

- Click the 'Groups' tab to view all groups to which the user belongs:

✖

Herald

Enroll Device

Manage Profiles

Send Password Recovery Email

Delete User

Run Procedure

Reset 2FA Token

User Info Associated Devices User Tokens Groups

Add to Group
 Remove from Group

<input type="checkbox"/>	GROUP NAME	# OF USERS	CREATED BY	CREATED
<input checked="" type="checkbox"/>	Flying Squad	3	herculespopular22@gmail...	2018/10/31 12:03:35 PM
<input type="checkbox"/>	Marketing Staff	5	herculespopular22@gmail...	2018/08/02 10:14:01 AM





- **Group Name** - The group label. Click the group name to view and edit group details, manage configuration profiles and more.
- **Number of Users** - The total count of users in the group.
- **Created By** - The admin who added the group.
- **Created** - Date and time the group was added.

Add the user to a new group

- Click 'Add to group'
- Start typing the name of the group to which you want to add the user and select from the suggestions:



User Info Associated Devices User Tokens **Groups**

 Add to Group  Remove from Group  

<input type="checkbox"/>	GROUP NAME	# OF USERS	CREATED BY	CREATED
<input checked="" type="checkbox"/>	Flying Squad	3	herculespopular22@gmail...	2018/10/31 12:03:35 PM

Add User to Group ✕

Choose group(s)

To add groups, start typing their names





- Click 'Add'

The user is added to the group. All group profiles are applied to the user's devices.

Remove the user from a group

- Select the group from the list and click 'Remove from Group'

User Info Associated Devices User Tokens **Groups**

 Add to Group  Remove from Group  

<input type="checkbox"/>	GROUP NAME	# OF USERS	CREATED BY	CREATED
<input checked="" type="checkbox"/>	Flying Squad	3	herculespopular22@gmail...	2018/10/31 12:03:35 PM

Remove from Group ✕

Do you really want to remove this user from user group?

- Click 'Confirm' to remove the user's membership from the group.

Any group configuration profiles are automatically removed from the user's devices.

Apply profiles to user devices

Profiles assigned to a user apply to all devices owned by the user.

You can apply multiple profiles for different operating systems to a user. Endpoint Manager will apply the appropriate profile to a device depending on its OS.

See [this wiki](#) for help to apply profiles to a user.

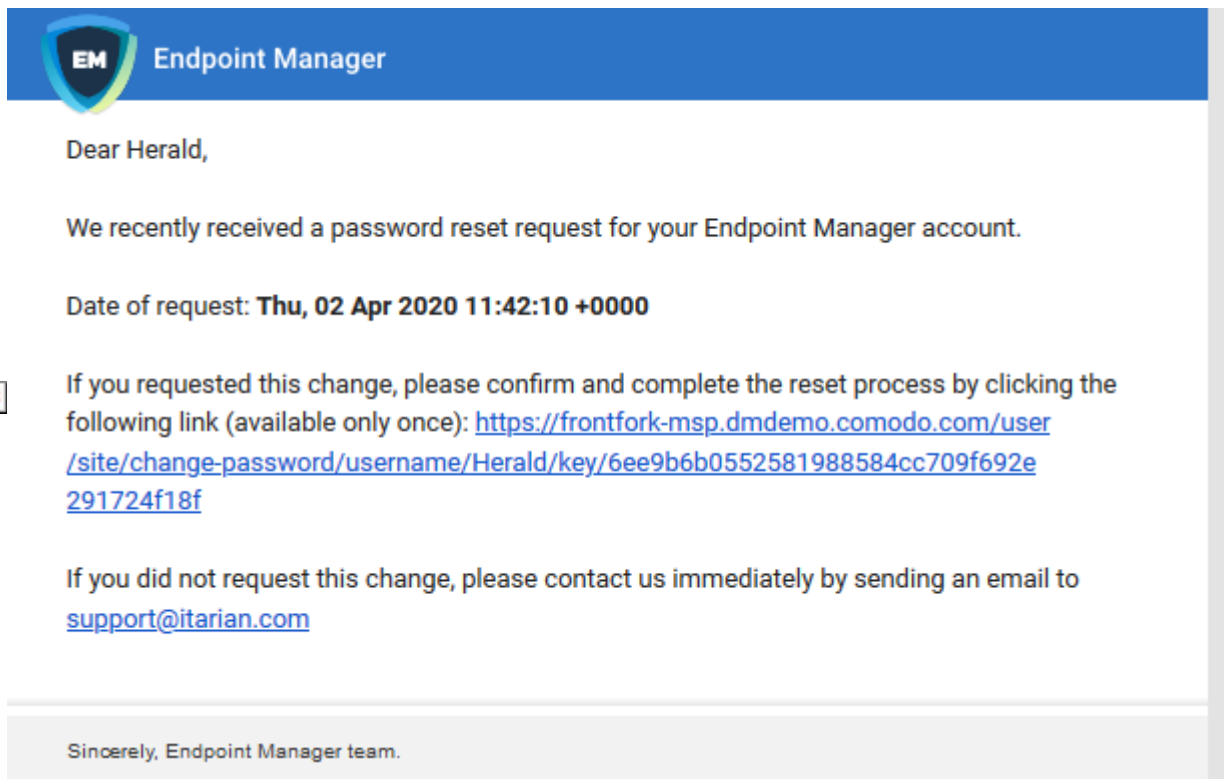
Send a password recovery mail to a user

Users with admin roles can login to the Endpoint Manager console. An account activation mail is sent to such users when they are first given the admin role. The mail lets them create a password to login to Endpoint Manager. You can send them a password reset mail if, for example, they have forgotten their password.

- Click 'Users' > 'User List'
- Select the user for whom you want to send password reset email
- Click 'Send Password Recovery Email'

Note - you can only send reset mails to users that were directly added to Endpoint Manager. This option is not available for users added via the Comodo One / Dragon portal.

The email contains a link which lets the user change their password:



Reset password for a user

You can manually set a new password for a user instead of letting them [reset it for themselves](#).

- Click 'Users' > 'User List'

- Select the user for whom you want to set a new password
- Click 'Change Password':

The screenshot shows a 'User List' interface with a table of users. The 'Change Password' button is circled in red, and a red arrow points to the 'Change Password' modal dialog. The modal dialog is titled 'Change Password' and contains the following elements:

- A text input field for the new password, labeled 'New Password for Herald *'.
- A green button labeled 'Generate New Password'.
- Two checkboxes:
 - Ask for a password change at the next Sign-in
 - Notify user about changing password on email
- Two buttons at the bottom: 'Cancel' and 'Change'.

	NAME	EMAIL	PHONE NUMBER ▲	# OF DEVICES	2FA STATUS	LAST LOGIN
<input checked="" type="checkbox"/>	Herald	hertriumph@gmail	1234567890	1	Not active	Not logged in y...
<input type="checkbox"/>	Dyanora	dyanorat481@gma	9876543210	1	Not active	Not logged in y...
<input type="checkbox"/>	Alice					

- Type a new password for the user in the box provided. Alternatively, click 'Generate New Password' to have Endpoint Manager create a random password.
- **Ask for a password change at the next Sign-in** - After logging in with the new password you provide, users will be forced to change their password again. This improves privacy by ensuring only the user knows their own password.
- **Notify user about changing password on email** - Will send an email to users that informs them their password has been reset.

Click 'Change'.

Reset two-factor authentication token for a user

- You can force admin users to reset their two-factor authentication (2FA) on their next login.
 - See '[Configure two-factor authentication settings](#)' if you want to know how to setup 2FA in

Endpoint Manager.

- Note: This action does not reset 2FA on Comodo One / Dragon logins. It only affects 2FA for admins who were created in Endpoint Manager itself.

Reset two factor authentication

- Click 'Users' > 'User List'
- Select the user for whom you want reset two-factor authentication
- Click 'Reset 2FA Token'
- Alternatively, click 'Users' > 'User List' > click on a username > 'Reset 2FA Token'.

The screenshot shows the 'User List' page in Endpoint Manager. The top navigation bar includes 'User List', 'License Options', and a 'Logout' button for 'herculespopular22@gmail.com'. Below the navigation bar is a toolbar with various actions: 'Enroll Device', 'Create User', 'Manage Profiles', 'Send Password Recovery Email', 'Change Password', 'Delete User', 'Import User', 'Run Procedure', 'Export', and 'Reset 2FA Token'. The 'Reset 2FA Token' button is circled in red. Below the toolbar is a table with columns: 'NAME', 'EMAIL', 'PHONE NUMBER', '# OF DEVICES', '2FA STATUS', and 'LAST LOGIN'. The first row, for user 'Oxford', has a checkbox circled in red. A red arrow points from the 'Reset 2FA Token' button to a confirmation dialog box titled 'Reset Two-Factor Authentication Token' with the question 'Do you want to reset 2FA for User «Oxford?»' and 'Confirm' and 'Cancel' buttons.

	NAME	EMAIL	PHONE NUMBER	# OF DEVICES	2FA STATUS	LAST LOGIN
<input checked="" type="checkbox"/>	Oxford	mmoxford@yahoo.com	9876543210	0	Active	2020/04/03 08:46:0...
<input type="checkbox"/>	Patrick	remotedesktop@yopm	N/A	0	Not active	2020/03/16 03:27:3...
<input type="checkbox"/>	fsregionaltrans...	fsregionaltransport@gn	N/A	0	Not available	Not logged in yet

- Click 'Confirm'
- The admin will go through the 2FA setup process after their next login.

[Back to Sign In](#)

TWO FACTOR AUTHENTICATION - ACTIVATION

1. Install a two-factor authentication app

Please download Google Authenticator app on your smart device and open it.



2. Configure the application

Open your application and add your account by:

Scan this QR-code



or Enter it manually

Key: 2MYIXYT7RSDAZ7NI

3. Enter the 6-digit code that the application generates

 Code

ENABLE

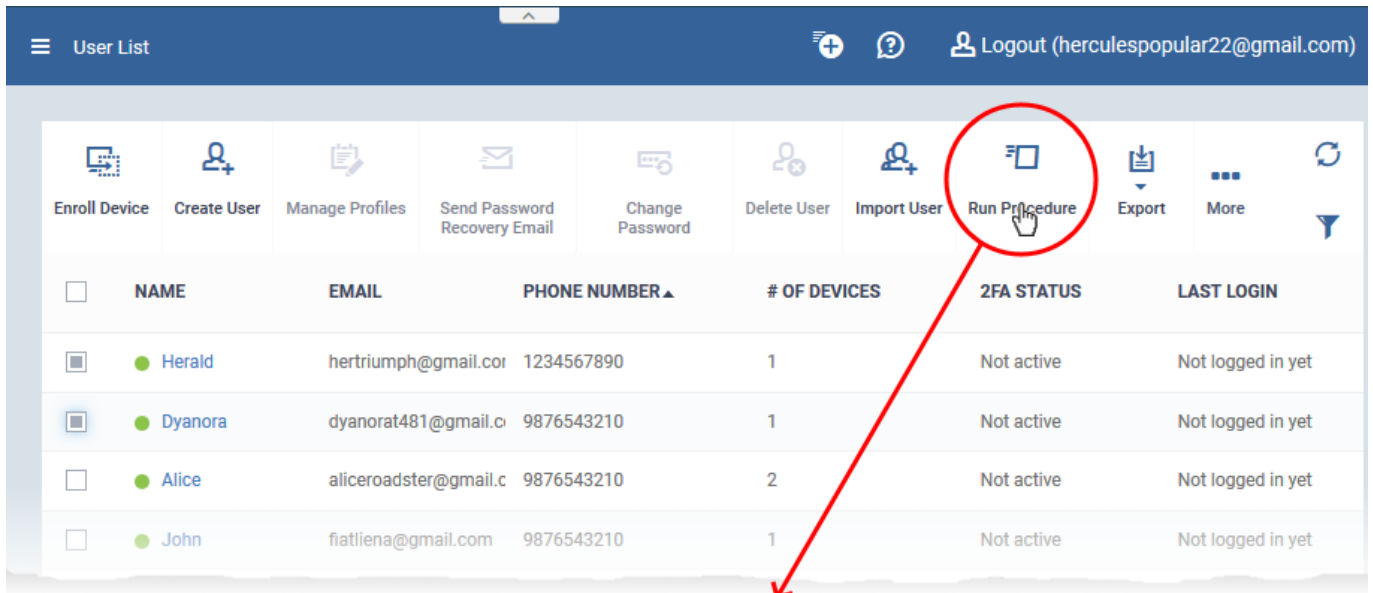
Run procedure on user devices

Procedures are standalone instruction scripts and patches for Windows devices.

There are various ways you can execute procedures on devices. See [this wiki](#) for more in-depth info on procedures.

- Click 'Users' > 'User List'
- Select the target users then click 'Run Procedure'
- Alternatively, click on a user's name then click 'Run Procedure' in their details screen.
- Next, choose the script you want to run and other options:





Run Procedure ✕

Type approved procedure name to search among procedures

Run as LocalSystem User
 Run as Logged in User

Cancel
Run

- Procedure Name - Type the name of the procedure that you want to add (make sure you have approved the procedure).
- Run as Local System User / Run as Logged in user - Choose the user account under which the procedure should run. This option is not available for patch procedures.
- Send the resulting logs by email - Script procedures only.
 - **Send to current user** - Procedure results are sent to the admin who is currently logged into Endpoint Manager.
 - **Send to the following email addresses** - Add email addresses to whom procedure results should be sent.

Click 'Run'

Endpoint Manager runs the procedure on the users' devices.

You can also view the results of the procedure in 'Device Details' > 'Logs'.

See [this wiki](#) if you want to read more about logs.

Further reading:

[How to create new user accounts and user groups in Endpoint Manager](#)

[How to add staff and assign or reassign them to roles](#)

[How to create a new role with custom permissions and assign it to users](#)

[How to enroll devices using the on-boarding wizard](#)