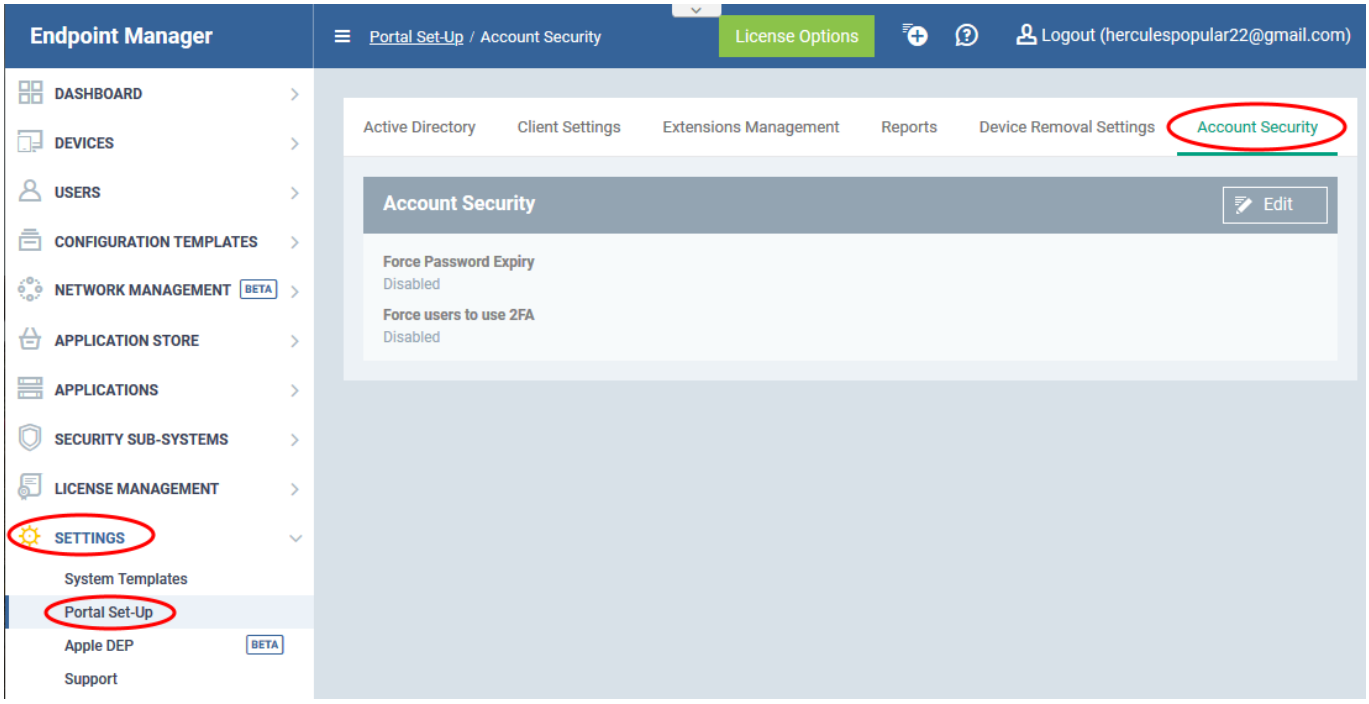
Click 'Settings' > 'Portal Set-Up' > 'Account Security'

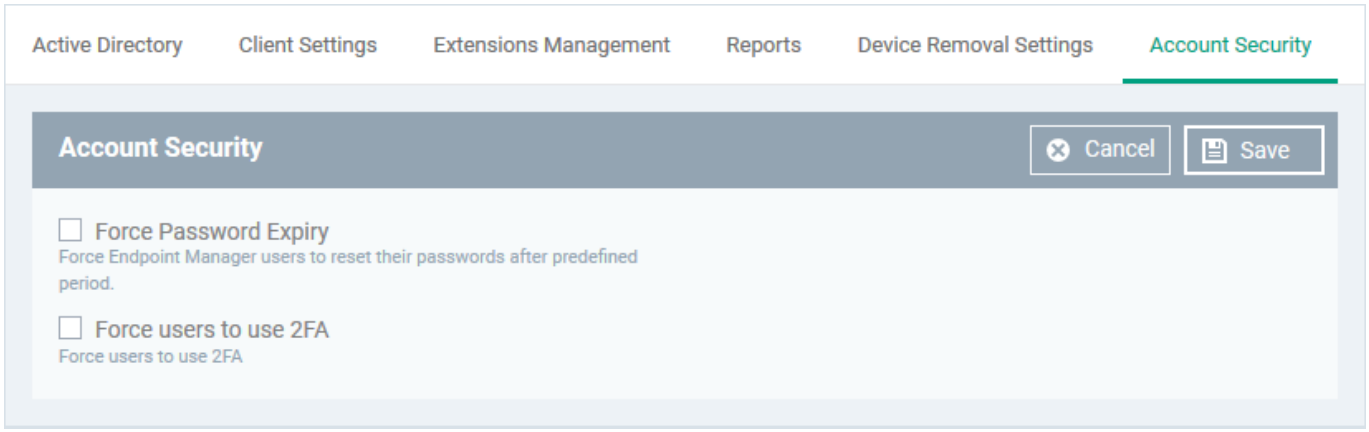
- The 'Account Security' interface lets you enforce two-factor authentication and set password expiry term for admins, staff and technicians who login to Endpoint Manager
- The settings configured in this interface is only for login access to the EM console

Set the account security options in EM

- Login to ITarian
- Click 'Applications' > 'Endpoint Manager'
- Click 'Settings' on the left then 'Portal Set-Up'
- Click the 'Account Security' tab



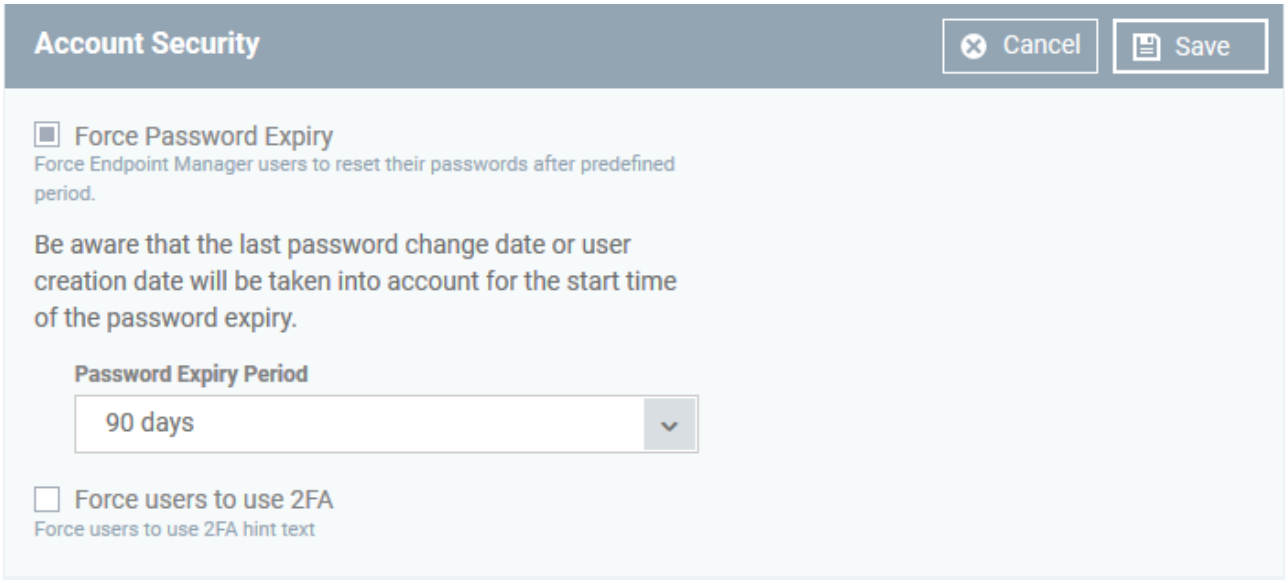
- Click 'Edit'



The interface lets you:

- Set a password expiry term
- Enforce two factor authentication for login

  Force Password Expiry – Set a life term for login passwords of admins, staff and technicians, who log-in to the EM console.



  - **Password Expiry Period** – Choose the maximum length of time a user can keep the same password before they need to change it. Options are 45 days, 90 days, 180 days, 365 days and 3 years. (3 years default). The password expiry period options for reseller account are 45 days and 90 days (90 days default).

- The password expiry counter starts from the day the user was created (new users) or the day of most recent password change (existing users)
- The users will be forced to change their password on lapse of the expiry period to login to EM
- The setting applies to all admins, staff, technicians and other users with administrative roles, who login to Endpoint Manager.

See this wiki to read more about roles and assigning roles to users.

- The setting also applies to technicians logging-in to the Remote Control tool to remotely take-over managed devices for solving issues. The remote control tool users are notified from 7 days in advance of the password expiry. They should login to Endpoint Manager console to change their password.

See this wiki to read more about logging-in to the remote control tool and remote take-over of managed devices

- The setting does not apply to users logging-in to ITarian portal. If you created your admins in the ITarian portal, then please configure password policy in ITarian. ('Settings' > 'Password and Account Policies'). See this wiki if you need help to configure password policy in ITarian.

Force users to use 2FA - If enabled, admin users will need to set-up 2FA on their next login to the EM console. Setup involves installing the Google Authenticator app on their device. This app generates the codes that form the 2nd layer of authentication. See Activate two-factor authentication if you need help on how admin users set up and use their authenticator app.

- Two-factor authentication adds additional security by requiring admins to present two forms of authentication before they can login to endpoint manager. They will need to enter their regular UN/PW + a unique code generated on their mobile device.

- This setting applies only to admins and users with administrative roles who were created in Endpoint Manager itself ('Users' > 'User List' > 'Create User').

  See this wiki to read more about roles and assigning roles to users.

- This setting does not implement 2FA for ITarian logins. If you created your admins in the ITarian portal, then please enable 2FA in ITarian ('Management' > 'Account' > 'Account Security Details').

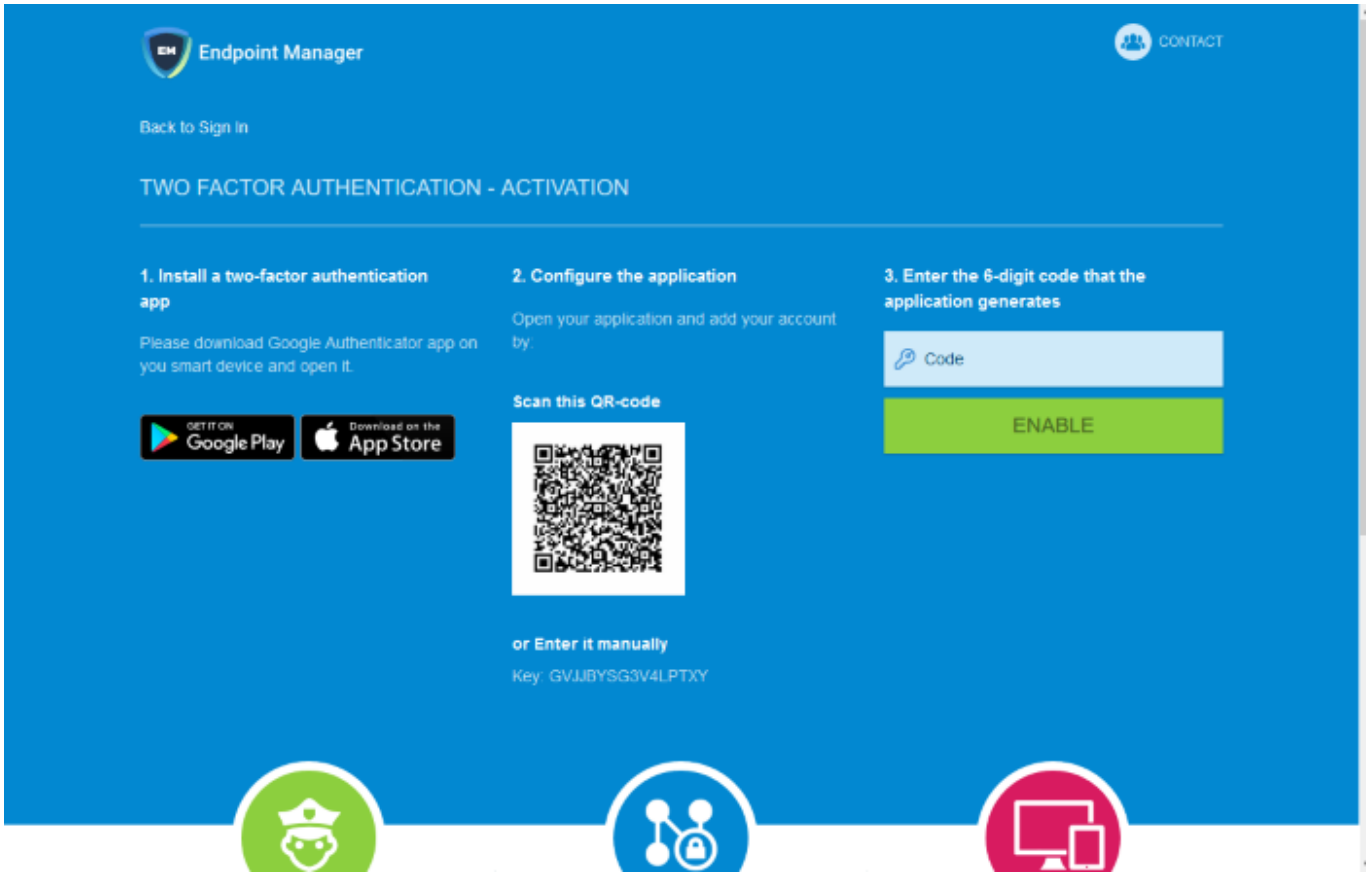
Click 'Save' to apply your changes.

Activate two-factor authentication

The following explains the admin's user-experience to configure 2FA at their first login:

- Admin enters his UN/PW in the EM login screen and clicks 'Login':

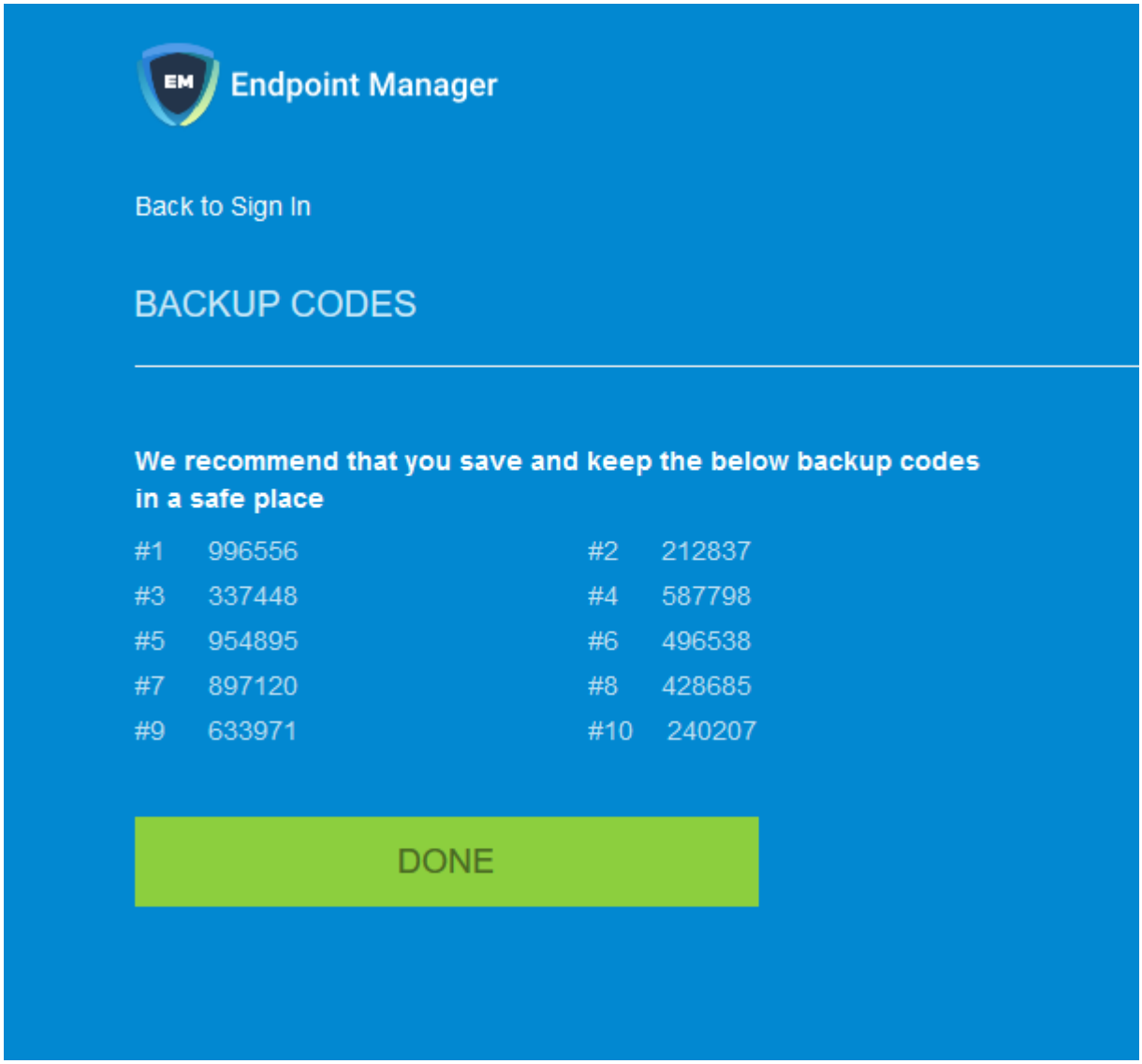
The two factor authentication activation screen is shown:



- **Step 1** - Download the 'Google Authenticator' app and install it on your iOS or Android device
    - Open the 'Authenticator' app and tap the '+' icon

- **Step 2** - Scan the QR code with the device camera. This will cause the Google app to generate the six digit code you need to complete pairing.
    - Alternatively, enter the key shown below the QR code in the Google Authenticator app.
- **Step 3** - After completing steps 1 and 2, a six digit authentication code is generated in the Google app. This code changes frequently and is unique to your account.
    - Enter the verification code in the field provided
- Click 'Enable'

A success message is shown along with 10 backup codes



You can use the backup codes to complete two-factor authentication if you do have the authentication device with you. Please make a copy of the codes. Each code can only be used once.

- Click 'Done'. You will be logged in to your account.

Two-factor authentication is now configured.

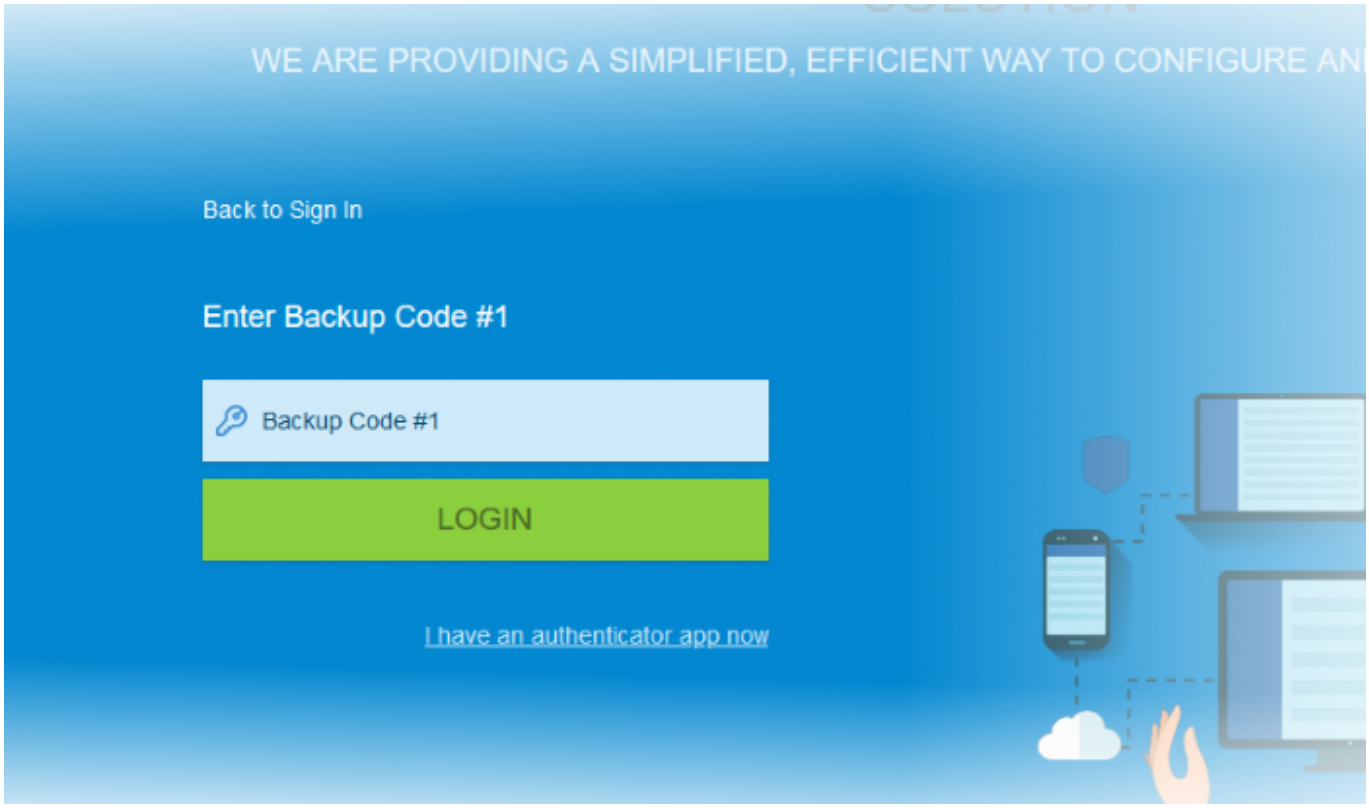
During next login to EM console, the two-factor authentication screen is shown after entering your username and password

- **Code** - Open the Google Authenticator app on your paired device and enter the displayed code. Please note the code changes frequently.
- Click 'Login'

Use Backup Codes

Endpoint Manager two-factor authentication allows you to use your backup codes in case you do not have your paired device with you during a login attempt.

- Click 'I don't have an authenticator app now' link



- Enter backup code 1 from the saved backup codes when you paired your device
- Click 'Login'