Triển khai xác thực 2 lớp (2FA) cho máy chủ và client

Cấu hình OTP cho User

\*\* Chuẩn bị:

* Tool Rohos Logon Key hoặc các tính năng Authentication (VD: Google Authenticator) để nhận mã xác minh 2 lớp

Phần mềm authenticator sẽ được cài đặt trên điện thoại

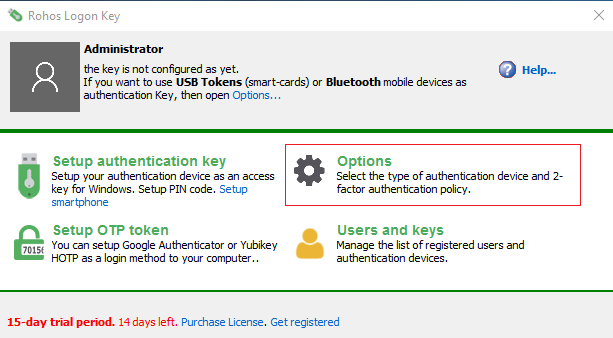
* Máy chủ DC đã lên miền (Cũng có thể để chế độ WORKGROUP)

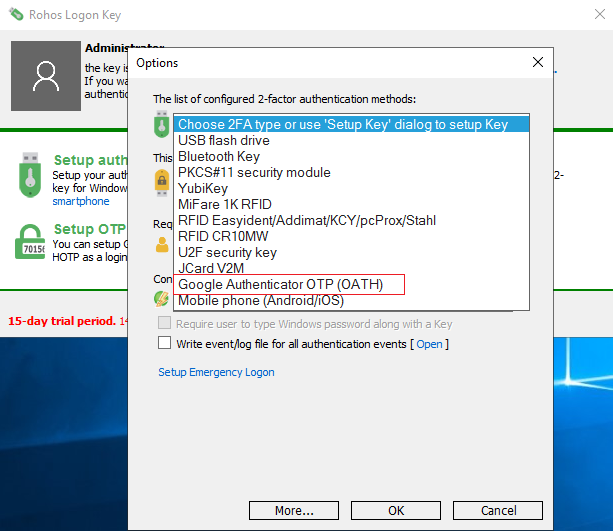
\*\* Triển khai

* Cài đặt phần mềm Rohos Logon Key cho máy chủ DC

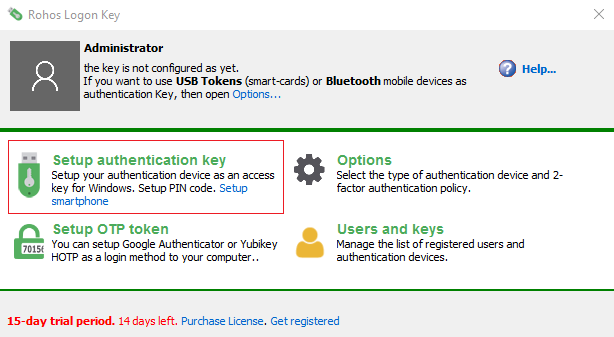


Sau khi đã cài đặt và Active xong, ta vào phần option để mở tính năng google authenticator

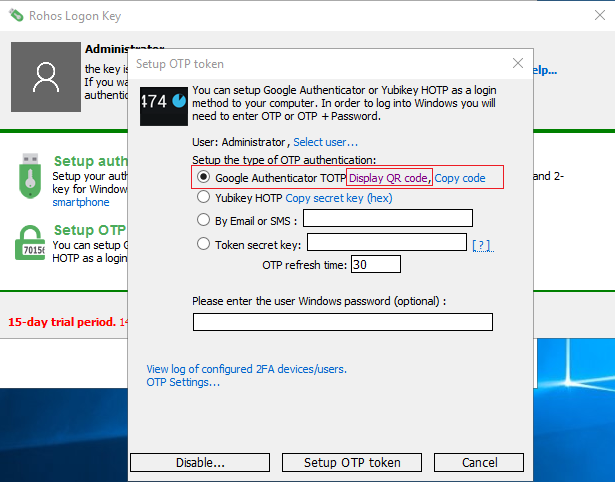




Sau đó tiền hành setup cho việc xác thực key



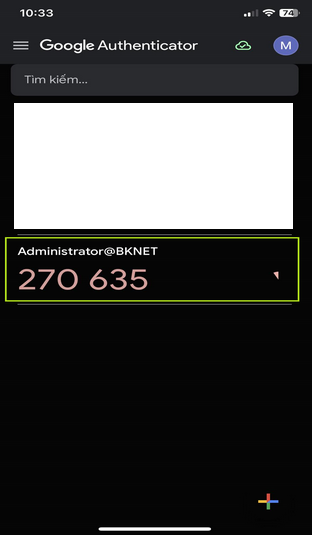
Setup OTP token sau đó chọn Google Authenticator TOTP



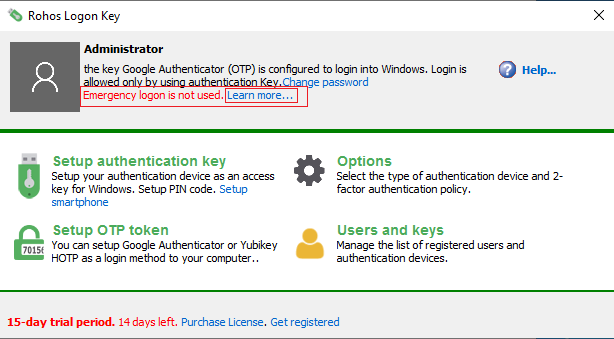
\*\* Lưu ý: Trong phần này có phần Display QR Code, ta click vào để lấy mã QR và lưu lại phòng trong trường hợp thiết bị sử dụng google authenticator gặp sự cố (mất, hỏng không thể khôi phục) thì vẫn còn mã QR để mở lại thay cho mã pin



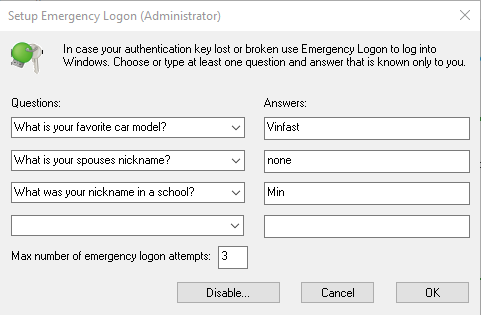
Sau đó ta mở điện thoại vào app authenticator có trên điện thoại mà quét mã QR vừa tạo để tạo 1 mã mới



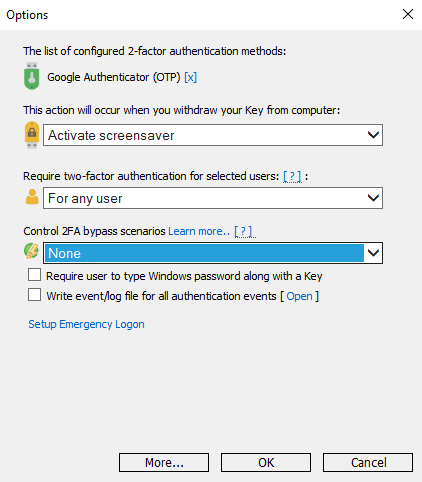
Sau khi quét QR xong ta click Setup OTP token trên phần mềm Rohos để lưu lại. Tiếp tục ta ta đặt mật khẩu cho phần mềm rohos để bảo mật



Tiến hành đặt 3 câu hỏi bảo mật cho phần mềm



Sau đó ta quay lại phần Option và tiến hành setup 1 số mục như sau:



Rồi ấn OK

Kết quả sau khi setup thành công Key Logon

