

TÀI LIỆU HƯỚNG DẪN NGƯỜI DÙNG

THIẾT LẬP XÁC THỰC 2 YẾU TỐ (2FA) QUA ỨNG DỤNG XÁC THỰC

Quy trình liên kết ứng dụng Authenticator, quét mã QR, quản lý khóa bảo mật và
hủy kích hoạt

Mã tài liệu:	ITMS-UG-AUTH-07	Phiên bản:	1.0
Ngày ban hành:	22/09/2026	Đơn vị thực hiện:	Đội ngũ Phát triển Phần mềm ITMS
Đối tượng áp dụng:	Người dùng được phân quyền thao tác tính năng này trên hệ thống		

MỤC LỤC TÀI LIỆU

1. Giới thiệu tổng quan

2. Điều kiện tiên quyết & Chuẩn bị ứng dụng

3. Giao diện mở thiết lập 2FA

4. Hướng dẫn quy trình kích hoạt từng bước

- 4.1 Bước 1: Bật công tắc Ứng dụng xác thực
- 4.2 Bước 2: Quét mã QR hoặc Nhập khóa bí mật
- 4.3 Bước 3: Nhập mã xác minh từ ứng dụng
- 4.4 Bước 4: Xác nhận kết nối thành công
- 4.5 Bước 5: Kiểm tra trạng thái hoạt động trong Cài đặt 2FA

5. Hướng dẫn quy trình tắt hoặc xóa liên kết Ứng dụng xác thực

- 5.1 Bước 1: Gạt tắt công tắc Ứng dụng xác thực
- 5.2 Bước 2: Xác nhận cảnh báo xóa liên kết

6. Hoạt động của Ứng dụng xác thực trong quá trình đăng nhập

7. Bảng câu hỏi thường gặp & Khắc phục sự cố

8. Kênh hỗ trợ kỹ thuật

PHỤ LỤC TÀI LIỆU

- Phụ lục A: Bảng mã trạng thái & Mã lỗi thiết lập 2FA App
- Phụ lục B: Danh mục phím tắt & Thao tác nhanh
- Phụ lục C: Danh sách ứng dụng Authenticator tương thích & Khuyến nghị bảo mật
- Phụ lục D: Lịch sử cập nhật tài liệu

1. Giới thiệu tổng quan

Tính năng **Xác thực 2 yếu tố qua Ứng dụng xác thực (Authenticator App 2FA)** là phương thức gia tăng lớp bảo mật tiêu chuẩn cao cho tài khoản trên hệ thống ITMS.

Khi tính năng này được kích hoạt:

- **Bảo vệ tài khoản đa tầng:** Ngoài tên đăng nhập và mật khẩu, hệ thống sẽ yêu cầu thêm một mã số xác thực gồm 6 chữ số sinh tự động từ ứng dụng Authenticator trên thiết bị của bạn khi phát hiện truy cập từ thiết bị hoặc trình duyệt lạ.
 - **Hoạt động độc lập và bảo mật cao:** Ứng dụng sinh mã hoạt động hoàn toàn độc lập, không phụ thuộc vào sóng viễn thông di động, giúp người dùng luôn đăng nhập được ngay cả khi di chuyển đến khu vực sóng yếu hoặc khi ở nước ngoài.
 - **Chống nghe lén và đánh cắp tài khoản:** Ngăn chặn tuyệt đối các cuộc tấn công lừa đảo, tấn công chuyển hướng tin nhắn hoặc lộ lọt mật khẩu.
-

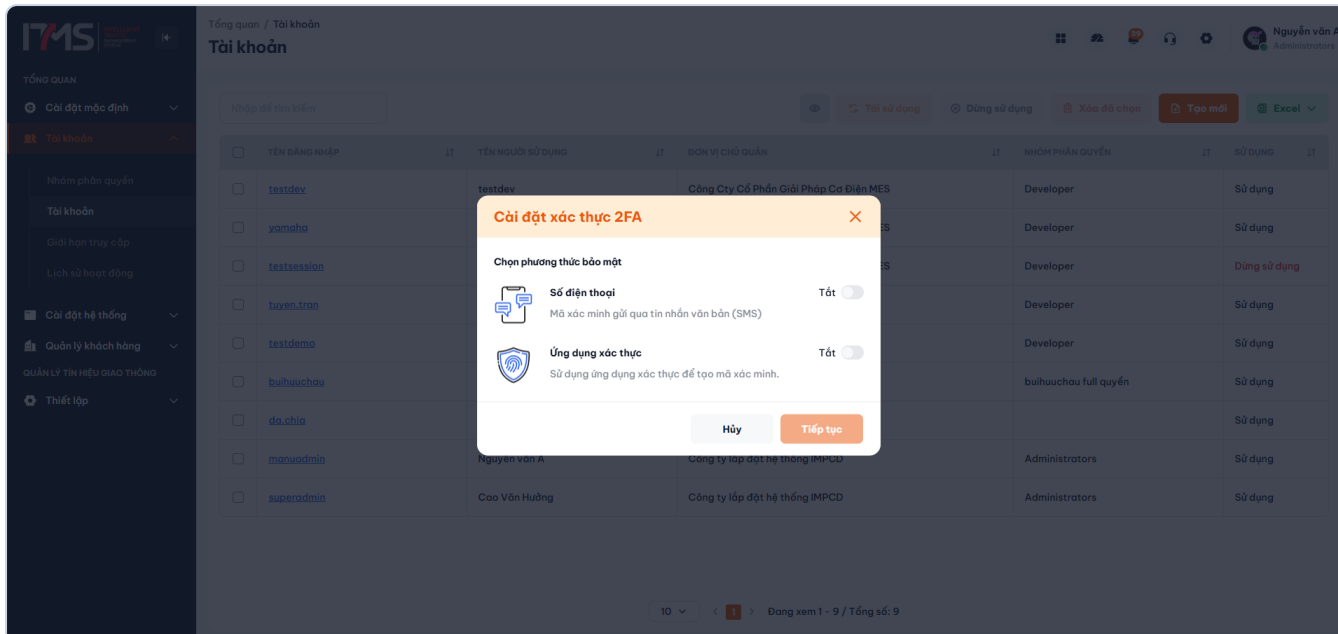
2. Điều kiện tiên quyết & Chuẩn bị ứng dụng

Trước khi tiến hành thiết lập, người dùng cần chuẩn bị:

1. **Tài khoản hệ thống:** Đã đăng nhập thành công vào hệ thống ITMS với tài khoản hợp lệ.
 2. **Thiết bị cài đặt ứng dụng:** Điện thoại thông minh, máy tính bảng hoặc tiện ích trình duyệt đã cài sẵn một trong các ứng dụng Authenticator phổ biến:
 - **Google Authenticator**
 - **Microsoft Authenticator**
 - **Duo Mobile**
 - Hoặc các ứng dụng hỗ trợ quét mã OTP tương đương.
-

3. Giao diện mở thiết lập 2FA

Tại menu quản lý tài khoản cá nhân, người dùng mở hộp thoại **Cài đặt xác thực 2FA**. Giao diện ban đầu hiển thị danh sách các phương thức bảo mật đang có trên hệ thống:



Hộp thoại bao gồm:

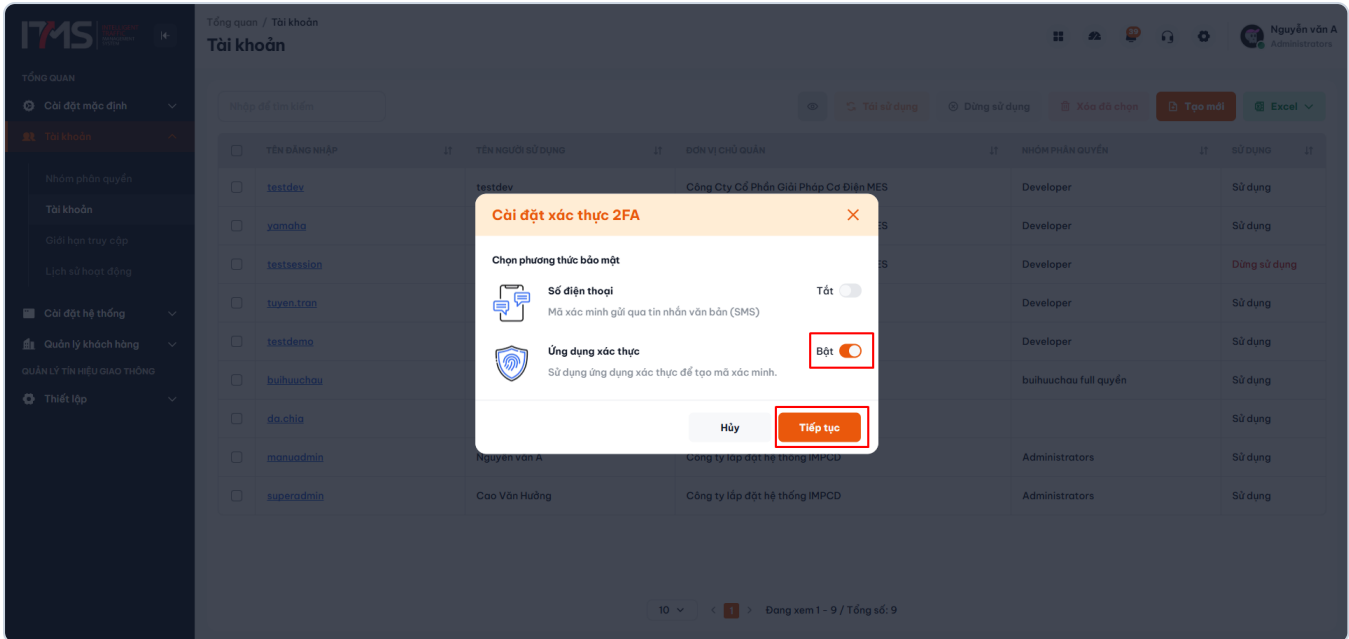
- **Số điện thoại (Mã xác minh gửi qua tin nhắn văn bản - SMS):** Tùy chọn 2FA qua tin nhắn SMS.
- **Ứng dụng xác thực (Sử dụng ứng dụng xác thực để tạo mã xác minh):** Tùy chọn 2FA qua ứng dụng tạo mã OTP.
- **Nút điều hướng:** Nút **Hủy** và nút **Tiếp tục**.

4. Hướng dẫn quy trình kích hoạt từng bước

[1. Bật công tắc App] → [2. Quét mã QR/Nhập Key] → [3. Nhập mã OTP] → [4. Hoàn tất kết nối]

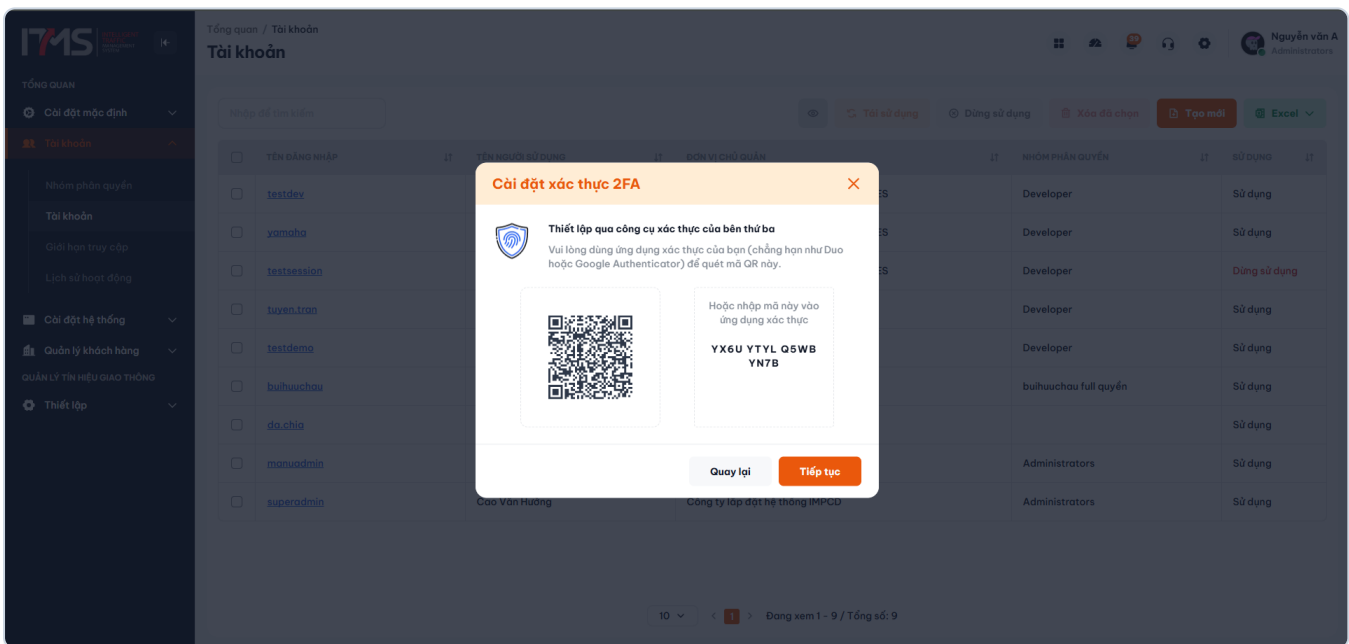
4.1 Bước 1: Bật công tắc Ứng dụng xác thực

1. Tại hộp thoại **Cài đặt xác thực 2FA**, tìm đến dòng **Ứng dụng xác thực**.
2. Nhấp vào công tắc gạt (toggle switch) để chuyển trạng thái sang **Bật** (nút gạt chuyển sang màu cam).
3. Nút **Tiếp tục** ở góc dưới bên phải sẽ sáng lên, sẵn sàng cho bước thiết lập.
4. Nhấn nút **Tiếp tục**.



4.2 Bước 2: Quét mã QR hoặc Nhập khóa bí mật

Hệ thống chuyển sang màn hình **Thiết lập qua công cụ xác thực của bên thứ ba**:



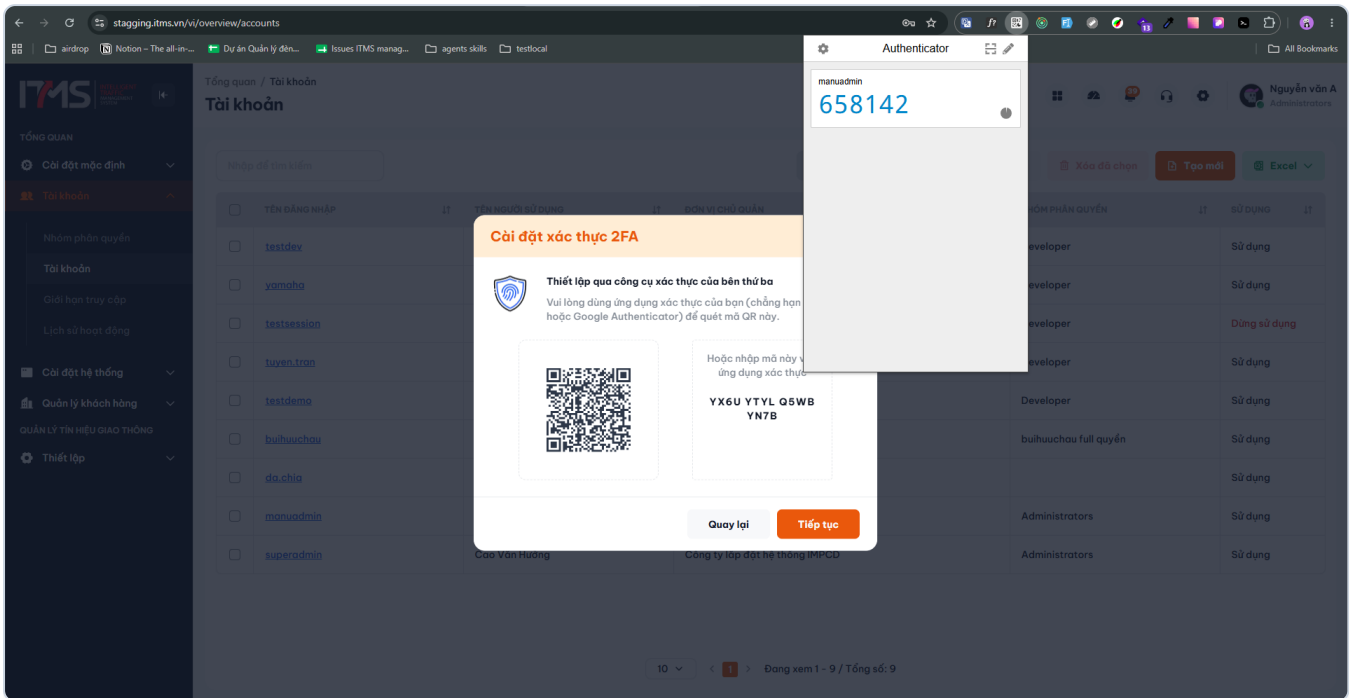
Người dùng thực hiện liên kết ứng dụng bằng một trong hai cách:

- **Cách 1 - Quét mã QR (Khuyến dùng):**
 1. Mở ứng dụng Authenticator trên điện thoại của bạn.
 2. Chọn tính năng quét mã QR (biểu tượng dấu **+** hoặc Camera trong ứng dụng).
 3. Hướng camera về phía **Mã QR** hiển thị trên màn hình máy tính để quét.
- **Cách 2 - Nhập khóa bí mật thủ công:**
 1. Nếu thiết bị không có camera hoặc sử dụng tiện ích Authenticator trên máy tính, sao chép chuỗi ký tự bên

dưới dòng "Hoặc nhập mã này vào ứng dụng xác thực" (ví dụ: `YX6U YTYL Q5WB YN7B`).

2. Dán chuỗi ký tự này vào mục thêm khóa thủ công trong ứng dụng Authenticator.

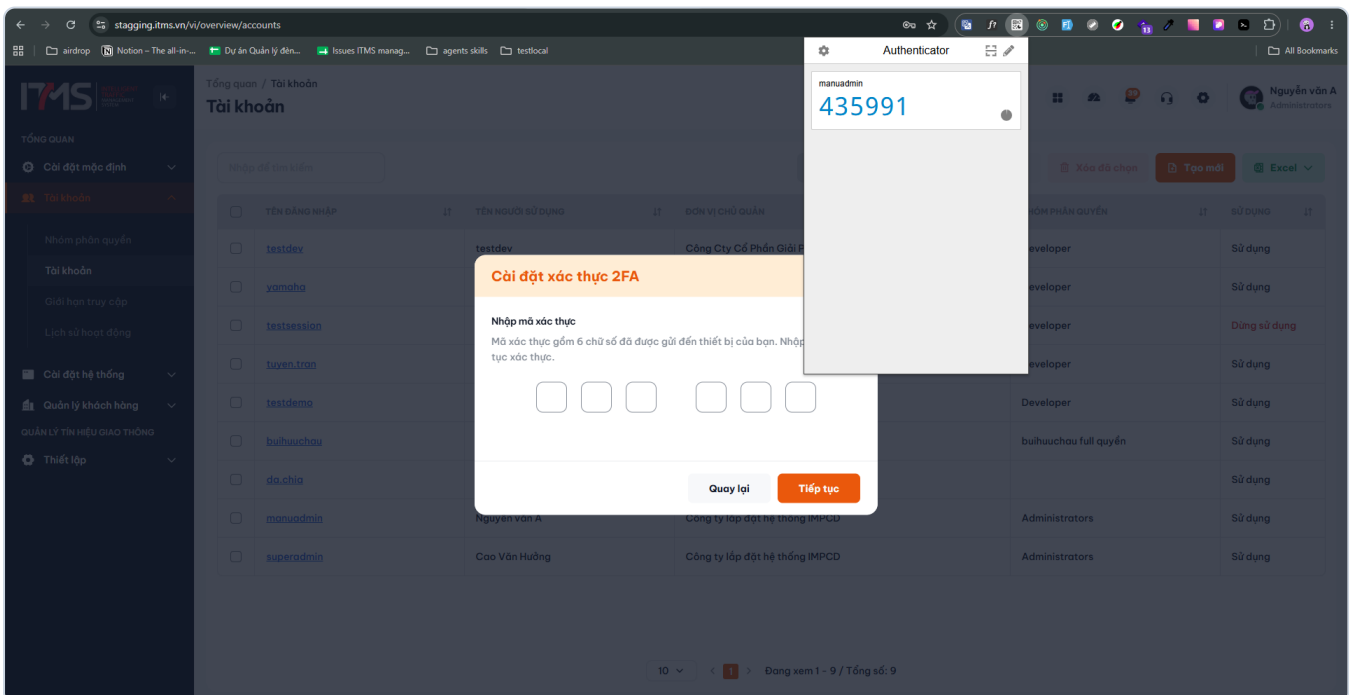
Sau khi quét hoặc nhập khóa thành công, ứng dụng Authenticator sẽ tự động thêm một tài khoản mới và hiển thị mã xác nhận:



3. Nhấn nút **Tiếp tục** màu cam trên hệ thống ITMS để chuyển sang bước kiểm tra mã.

4.3 Bước 3: Nhập mã xác minh từ ứng dụng

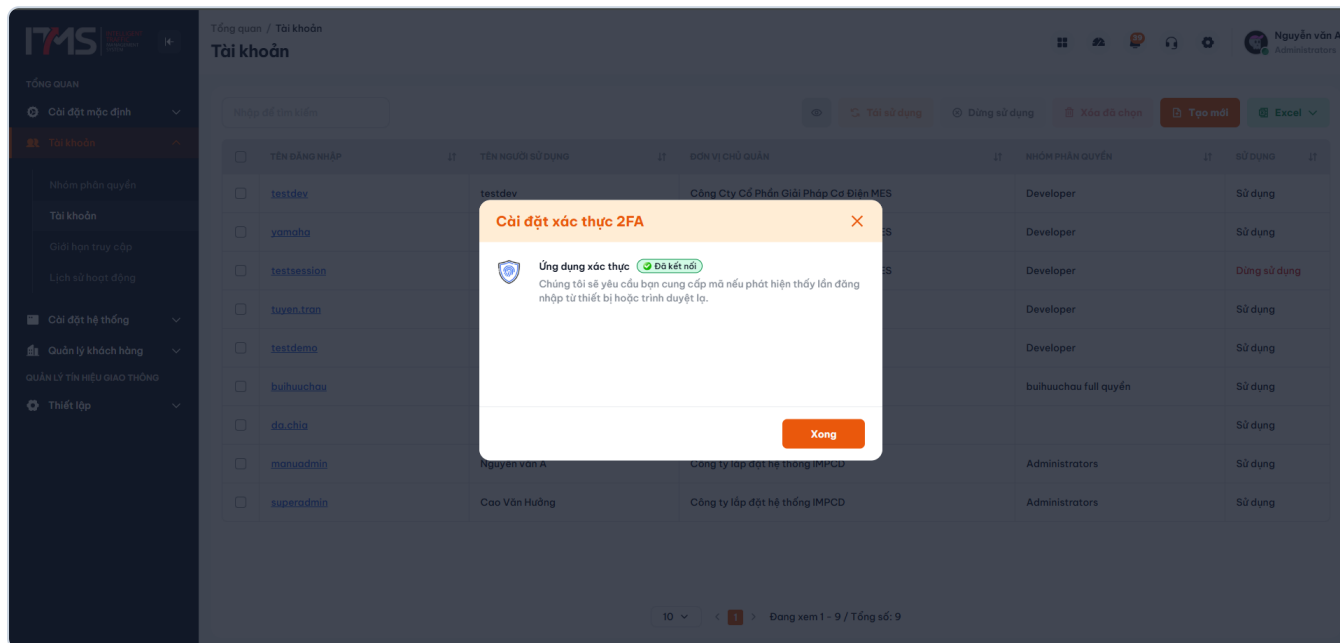
Hệ thống hiển thị màn hình **Nhập mã xác thực** gồm 6 ô trống:



1. Mở ứng dụng Authenticator và xem mã 6 chữ số đang hiển thị cho tài khoản ITMS (ví dụ: 435991).
2. Nhập lần lượt 6 chữ số này vào 6 ô trên màn hình hệ thống ITMS.
3. Sau khi nhập đủ 6 chữ số hợp lệ, nhấn nút **Tiếp tục** màu cam.

4.4 Bước 4: Xác nhận kết nối thành công

Khi mã xác thực được kiểm tra hợp lệ, màn hình hiển thị thông báo kết nối hoàn tất:



- Biểu tượng khiên bảo vệ kèm huy hiệu màu xanh lá **[Đã kết nối]**.
- Lời nhắc an toàn từ hệ thống:

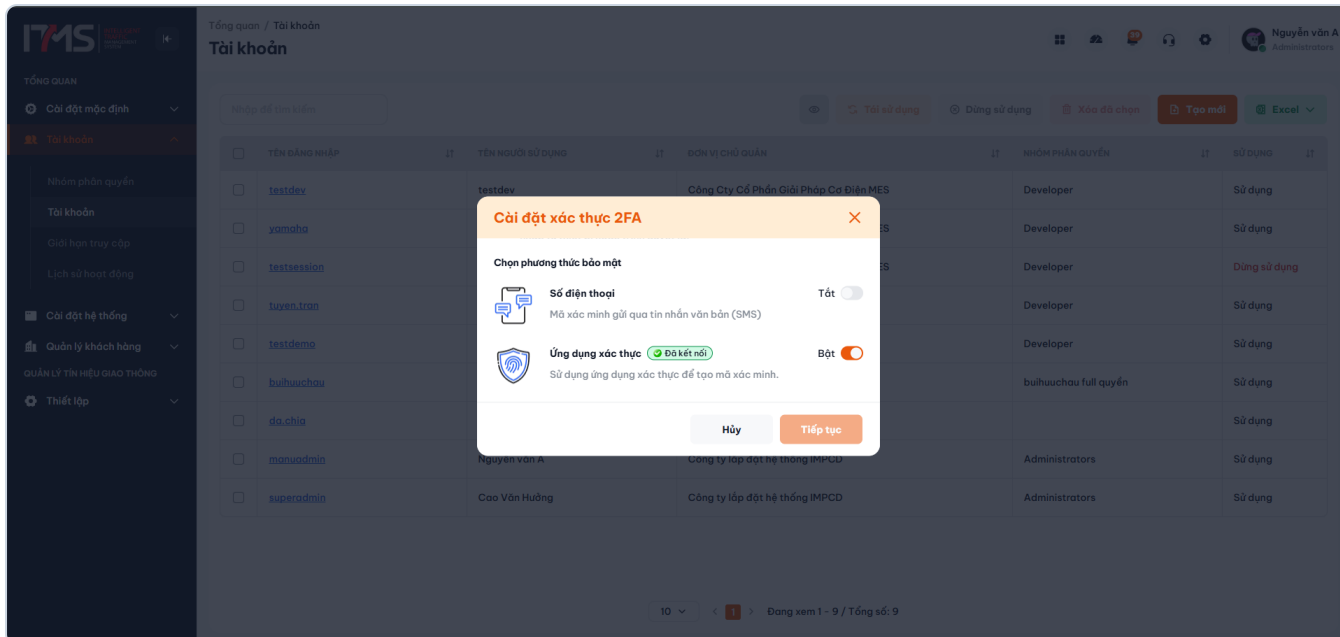
"Chúng tôi sẽ yêu cầu bạn cung cấp mã nếu phát hiện thấy lần đăng nhập từ thiết bị hoặc trình duyệt lạ."

- Nhấn nút **Xong** màu cam để đóng hộp thoại và hoàn thành thiết lập.

4.5 Bước 5: Kiểm tra trạng thái hoạt động trong Cài đặt 2FA

Sau khi nhấn **Xong**, hệ thống đưa bạn trở lại màn hình danh mục **Cài đặt xác thực 2FA**:

- Phương thức **Ứng dụng xác thực** hiển thị huy hiệu **[Đã kết nối]** màu xanh lá.
- Công tắc trạng thái hiển thị rõ ràng là **Bật** (màu cam).
- Tài khoản của bạn đã được bảo vệ an toàn bằng phương thức Ứng dụng xác thực.

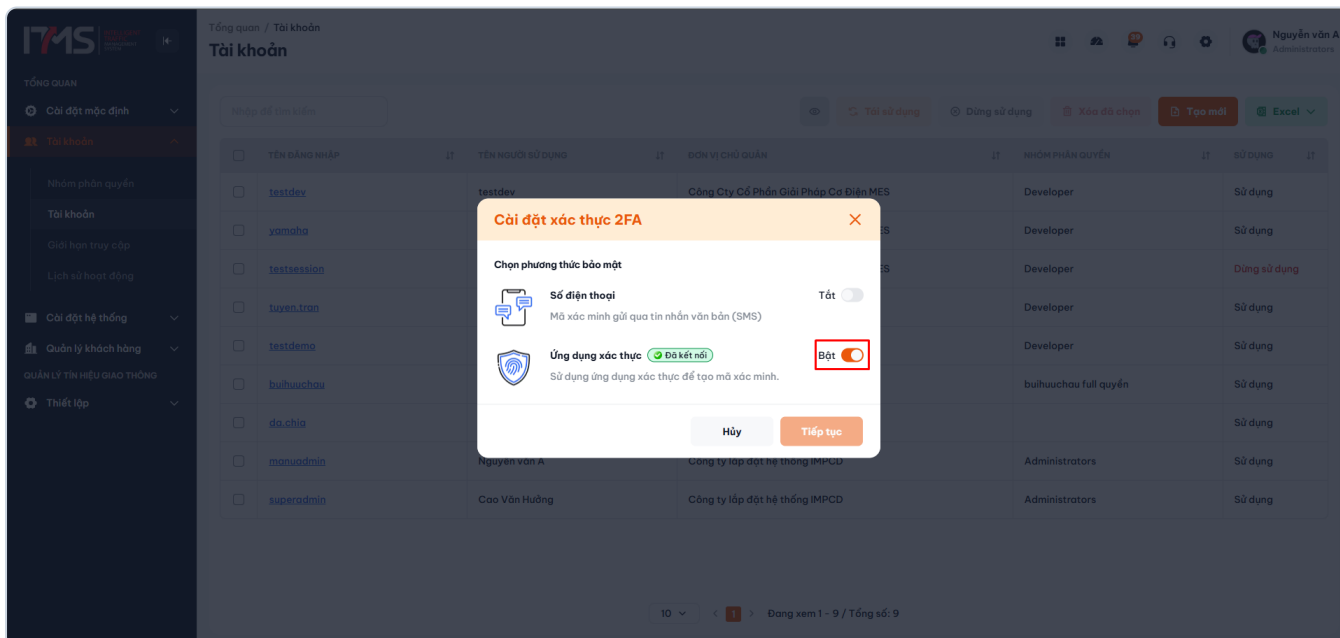


5. Hướng dẫn quy trình tắt hoặc xóa liên kết Ứng dụng xác thực

Khi bạn đổi điện thoại mới hoặc muốn tạm thời ngừng sử dụng phương thức này, thực hiện theo các bước sau:

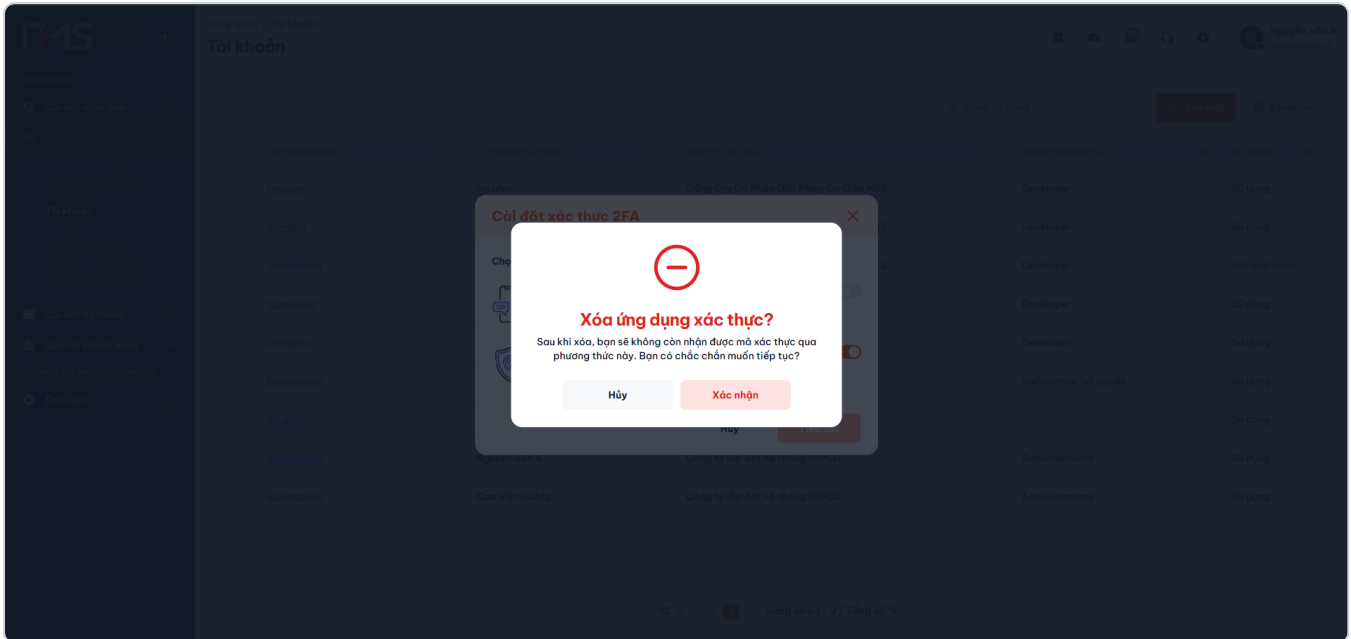
5.1 Bước 1: Gạt tắt công tắc Ứng dụng xác thực

- Mở hộp thoại **Cài đặt xác thực 2FA**.
- Tại dòng **Ứng dụng xác thực**, nhấp vào công tắc gạt đang ở trạng thái **Bật** để chuyển sang **Tắt**.



5.2 Bước 2: Xác nhận cảnh báo xóa liên kết

Hệ thống sẽ hiển thị hộp thoại cảnh báo bảo mật **Xóa ứng dụng xác thực?**:



- Nội dung cảnh báo:

"Sau khi xóa, bạn sẽ không còn nhận được mã xác thực qua phương thức này. Bạn có chắc chắn muốn tiếp tục?"

- Nếu chắc chắn muốn gỡ bỏ, nhấn nút **Xác nhận** (màu đỏ).
- Nếu không muốn thay đổi, nhấn nút **Hủy** (màu xám) để giữ nguyên cài đặt 2FA hiện tại.

6. Hoạt động của Ứng dụng xác thực trong quá trình đăng nhập

Sau khi kích hoạt phương thức Ứng dụng xác thực:

1. **Đăng nhập trên thiết bị quen thuộc:** Người dùng đăng nhập bình thường bằng Tên đăng nhập và Mật khẩu.
2. **Đăng nhập trên thiết bị / trình duyệt mới:**
 - Hệ thống chuyển sang màn hình yêu cầu mã xác thực 2 bước.
 - Người dùng mở ứng dụng Authenticator trên điện thoại, lấy mã 6 chữ số và nhập vào màn hình để hoàn tất đăng nhập.

7. Bảng câu hỏi thường gặp & Khắc phục sự cố

Hiện tượng / Vấn đề	Nguyên nhân có thể	Hướng dẫn xử lý
Báo lỗi "Mã xác thực không hợp lệ" liên tục	Thời gian trên điện thoại bị lệch so với giờ chuẩn máy chủ	Vào Cài đặt trên điện thoại → Bật tính năng "Ngày & giờ tự động" (Network Time). Trên Google Authenticator: Chọn Cài đặt → Đồng bộ thời gian.
Không quét được mã QR	Ống kính camera mờ hoặc độ sáng màn hình quá chói	Làm sạch ống kính hoặc sử dụng Cách 2: Sao chép và dán khóa bí mật dạng văn bản hiển thị bên cạnh mã QR vào ứng dụng.
Làm mất điện thoại chứa ứng dụng Authenticator	Người dùng không thể tự lấy mã OTP để đăng nhập	Nếu tài khoản có bật thêm kênh SMS , chọn chuyển sang nhận mã qua SMS. Nếu không, liên hệ Quản trị viên Tenant để được hỗ trợ mở khóa tài khoản.
Muốn chuyển ứng dụng sang điện thoại mới	Đổi thiết bị làm việc mới	Truy cập Cài đặt 2FA trên máy tính, thực hiện tắt phương thức cũ và tiến hành bật lại để quét mã QR mới trên điện thoại mới.

8. Kênh hỗ trợ kỹ thuật

Trong trường hợp người dùng gặp sự cố liên quan đến thiết lập 2FA hoặc mất thiết bị chứa ứng dụng xác thực:

- **Đầu mối nội bộ:** Liên hệ Quản trị viên Tenant của cơ quan/tổ chức bạn để được hỗ trợ tạm thời thiết lập lại phương thức xác thực.
- **Tổng đài hỗ trợ kỹ thuật ITMS:** 1900 xxxx (Nhánh 1 - Vận hành hệ thống)
- **Email hỗ trợ:** support@itms.vn
- **Cổng tiếp nhận hỗ trợ:** https://helpdesk.itms.vn
- **Thời gian làm việc:** 24/7 đối với hệ thống giám sát và quản lý giao thông thông minh.

PHỤ LỤC TÀI LIỆU

Phụ lục A: Bảng mã trạng thái & Mã lỗi thiết lập 2FA App

Bảng tổng hợp các mã phản hồi từ hệ thống khi kích hoạt và xác thực phương thức qua Ứng dụng xác thực:

Mã phản hồi (HTTP/Status)	Thông báo hiển thị trên giao diện	Nguyên nhân kỹ thuật & Nghiệp vụ	Hướng khắc phục
400 Bad Request	<i>Yêu cầu thiết lập không hợp lệ</i>	Dữ liệu mã xác thực gửi lên trống hoặc thiếu trường thông tin cần thiết.	Kiểm tra lại việc nhập đủ 6 chữ số mã xác minh trước khi nhấn Tiếp tục.
401 Unauthorized	<i>Phiên làm việc đã hết hạn</i>	Phiên đăng nhập của tài khoản kết thúc trong quá trình thao tác.	Đăng nhập lại vào hệ thống và mở lại hộp thoại Cài đặt xác thực 2FA.
403 Forbidden	<i>Tài khoản không được phép thay đổi cấu hình 2FA</i>	Chính sách của tổ chức hoặc phân quyền quản trị hạn chế việc tự chỉnh sửa phương thức xác thực.	Liên hệ Quản trị viên hệ thống để kiểm tra phân quyền tài khoản của bạn.
422 Unprocessable	<i>Mã xác thực không chính xác</i>	Người dùng nhập sai mã 6 chữ số hoặc mã đã hết hiệu lực do đồng hồ thiết bị bị lệch thời gian.	Kiểm tra lại mã mới nhất trên ứng dụng hoặc đồng bộ lại thời gian trên thiết bị di động.
500 Internal Server Error	<i>Lỗi hệ thống máy chủ xác thực</i>	Sự cố kết nối cơ sở dữ liệu xác thực nội bộ của hệ thống.	Chờ trong giây lát rồi thử lại hoặc liên hệ bộ phận kỹ thuật ITMS.

Phụ lục B: Danh mục phím tắt & Thao tác nhanh

Nhằm hỗ trợ thao tác nhanh chóng và thuận tiện trên hộp thoại cài đặt:

Phím tắt / Thao tác	Vị trí áp dụng	Chức năng thực thi
Enter	Tại ô nhập mã xác thực 6 số	Xác nhận mã OTP ngay lập tức mà không cần nhấp chuột vào nút Tiếp tục .
Tab	Toàn bộ hộp thoại	Di chuyển con trỏ lần lượt qua switch bật/tắt, nút Hủy, nút Quay lại và nút Tiếp tục.
Shift + Tab	Toàn bộ hộp thoại	Di chuyển con trỏ ngược lại thành phần giao diện liền trước.
Esc	Khi hộp thoại cài đặt 2FA đang mở	Đóng nhanh hộp thoại (tương đương bấm nút Hủy hoặc biểu tượng đóng).
Nhập phím số (0-9)	Tại các ô nhập mã OTP 6 số	Tự động điền số vào ô hiện tại và chuyển con trỏ ngay sang ô tiếp theo.
Backspace	Tại các ô nhập mã OTP 6 số	Xóa số tại vị trí con trỏ và tự động lùi về ô liền trước.

Phụ lục C: Danh sách ứng dụng Authenticator tương thích & Khuyến nghị bảo mật

Để đảm bảo quá trình xác thực luôn diễn ra ổn định và bảo mật cao nhất:

1. Các ứng dụng xác thực được khuyến nghị sử dụng

- **Google Authenticator:** Ứng dụng phổ biến, gọn nhẹ, hỗ trợ đồng bộ mã qua tài khoản Google Cloud Sync.
- **Microsoft Authenticator:** Hỗ trợ sao lưu đám mây (Cloud Backup) an toàn, phù hợp môi trường doanh nghiệp.
- **Duo Mobile:** Hỗ trợ giao diện trực quan và quản lý nhiều tài khoản bảo mật.
- **1Password / Bitwarden:** Các trình quản lý mật khẩu có tích hợp sẵn tính năng tự động điền mã xác thực 2 bước.

2. Khuyến nghị an toàn khi sử dụng Ứng dụng xác thực

- **Lưu giữ an toàn khóa bí mật:** Khi quét mã QR, nên ghi lại chuỗi khóa bí mật (Secret Key) tại nơi an toàn để có thể khôi phục lại khi cần đổi máy.
- **Đồng bộ thời gian chính xác:** Ứng dụng tạo mã hoạt động dựa trên thuật toán thời gian thực, do đó thiết bị di động cần bật tính năng cập nhật giờ tự động qua mạng để tránh tình trạng mã bị báo không hợp lệ.
- **Kích hoạt đồng thời kênh dự phòng:** Khuyến nghị người dùng nên kích hoạt thêm phương thức **Xác thực qua tin nhắn SMS** để có kênh chuyển đổi linh hoạt khi không mang theo thiết bị cài ứng dụng.

Phụ lục D: Lịch sử cập nhật tài liệu (Document Revision History)

Phiên bản	Ngày cập nhật	Người thực hiện	Nội dung thay đổi
1.0	22/09/2026	ITMS Frontend Team	Khởi tạo tài liệu hướng dẫn thiết lập 2FA qua Ứng dụng xác thực, tích hợp 9 màn hình thực tế (quét QR, nhập OTP, bật/tắt 2FA), Trang bìa chuẩn in ấn A4, Mục lục riêng 1 trang và Phụ lục A-D.