

TÀI LIỆU HƯỚNG DẪN NGƯỜI DÙNG

THIẾT LẬP XÁC THỰC 2 YẾU TỐ (2FA) QUA TIN NHẮN SMS

Quy trình kích hoạt, liên kết số điện thoại bảo mật và xác thực đăng nhập hai lớp

Mã tài liệu:	ITMS-UG-AUTH-04	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

3. Giao diện mở thiết lập 2FA

4. Hướng dẫn quy trình thiết lập từng bước

- 4.1 Bước 1: Kích hoạt phương thức Số điện thoại
- 4.2 Bước 2: Nhập số điện thoại nhận mã xác minh
- 4.3 Bước 3: Nhập mã xác minh (OTP) gửi về tin nhắn
- 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. Hoạt động của 2FA SMS trong quá trình đăng nhập

6. Lưu ý quan trọng & Khắc phục sự cố

7. Kênh hỗ trợ kỹ thuật

PHỤ LỤC TÀI LIỆU

- Phụ lục A: Bảng mã trạng thái & Mã lỗi thiết lập 2FA SMS
- Phụ lục B: Danh mục phím tắt & Thao tác nhanh
- Phụ lục C: Cơ chế an toàn & Khóa đặt lại mật khẩu khi bật 2FA
- Phụ lục D: Lịch sử cập nhật tài liệu

1. Giới thiệu tổng quan

Tính năng **Xác thực 2 yếu tố qua tin nhắn văn bản (SMS 2FA)** là phương thức gia tăng lớp bảo vệ thứ hai cho tài khoản người dùng trên hệ thống ITMS.

Khi tính năng này được kích hoạt:

- **Bảo vệ đăng nhập đa lớp:** Ngoài tên đăng nhập và mật khẩu, hệ thống sẽ yêu cầu thêm một mã số xác thực dùng một lần (OTP) gồm 6 chữ số gửi trực tiếp qua SMS đến số điện thoại di động của bạn khi phát hiện truy cập từ thiết bị hoặc trình duyệt lạ.
 - **Chống truy cập trái phép:** Ngăn chặn tuyệt đối các nguy cơ lộ lọt mật khẩu, truy cập trái phép từ bên ngoài hoặc các cuộc tấn công đánh cắp phiên đăng nhập.
-

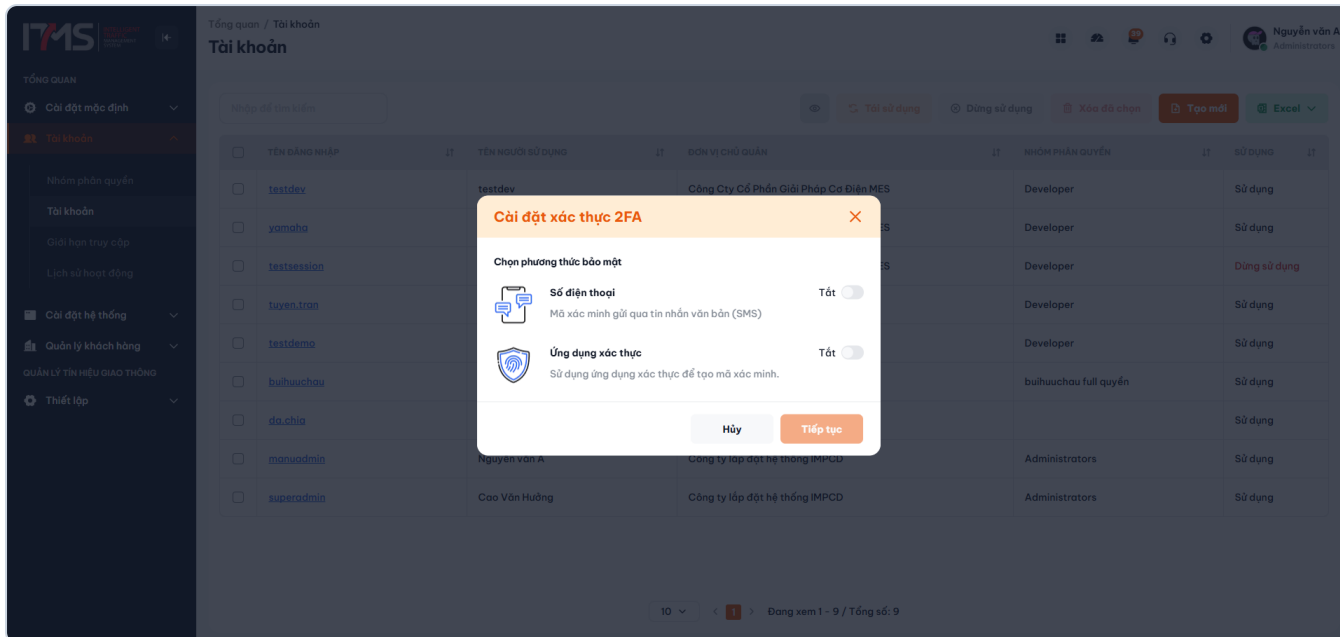
2. Điều kiện tiên quyết

Trước khi bắt đầu thiết lập, người dùng cần chuẩn bị:

1. **Tài khoản đăng nhập:** Đã đăng nhập vào hệ thống ITMS với thông tin hợp lệ.
 2. **Thiết bị di động:** Có sẵn điện thoại đang hoạt động với SIM còn nhận được tin nhắn SMS bình thường, sóng viễn thông ổn định.
 3. **Số điện thoại:** Đã cập nhật số điện thoại cá nhân trong hồ sơ tài khoản hoặc chuẩn bị số điện thoại hợp lệ để nhập vào hệ thống.
-

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:

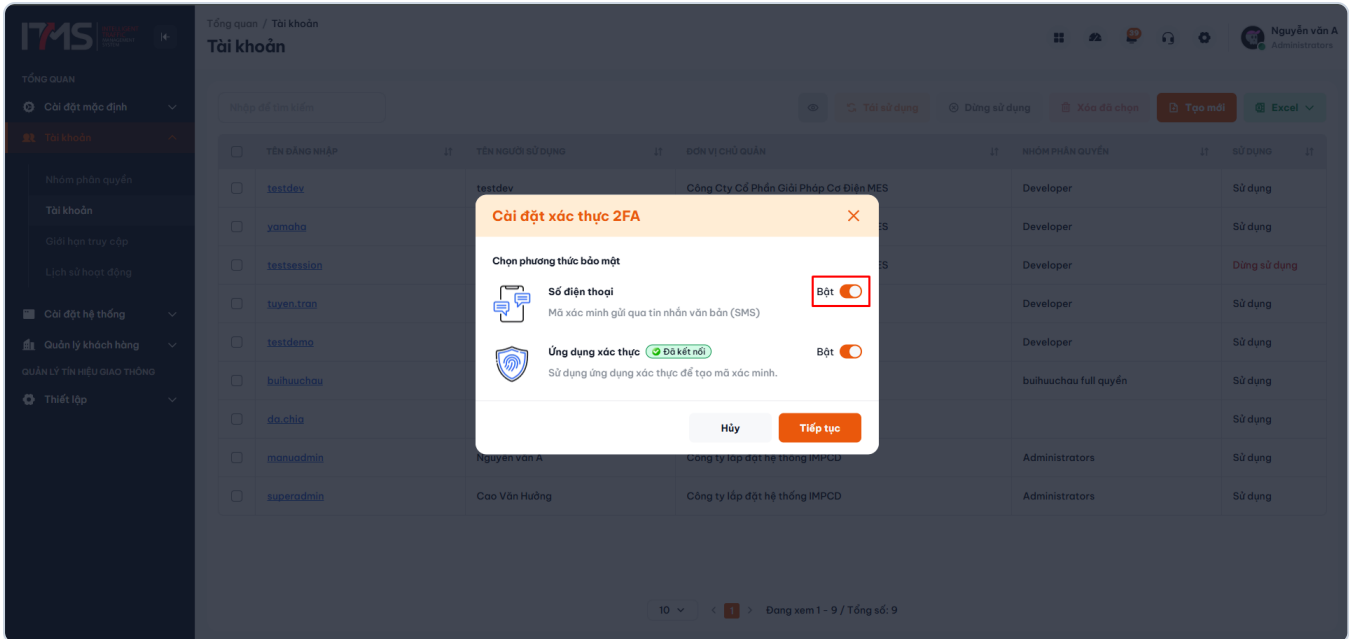
- **Số điện thoại (Mã xác minh gửi qua tin nhắn văn bản - SMS):** Đang ở trạng thái tắt.
- **Ứng dụng xác thực (Sử dụng ứng dụng xác thực để tạo mã xác minh):** Tùy chọn 2FA qua ứng dụng tạo OTP (Google Authenticator, Microsoft Authenticator,...).
- **Nút điều hướng:** Nút **Hủy** và nút **Tiếp tục**.

4. Hướng dẫn quy trình thiết lập từng bước

[1. Bật công tắc SMS] → [2. Nhập số điện thoại] → [3. Nhập mã OTP SMS] → [4. Hoàn tất kích hoạt]

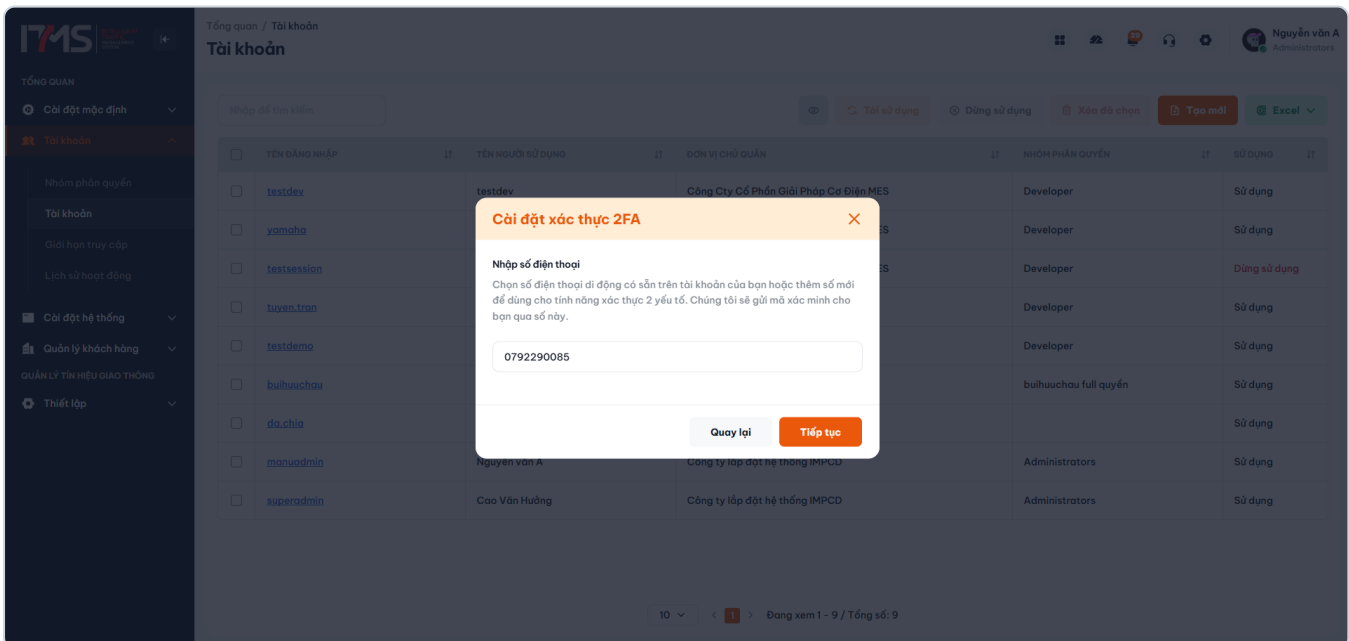
4.1 Bước 1: Kích hoạt phương thức Số điện thoại

1. Tại hộp thoại **Cài đặt xác thực 2FA**, tìm đến dòng **Số điện thoại**.
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 tiếp theo.
4. Nhấn nút **Tiếp tục**.



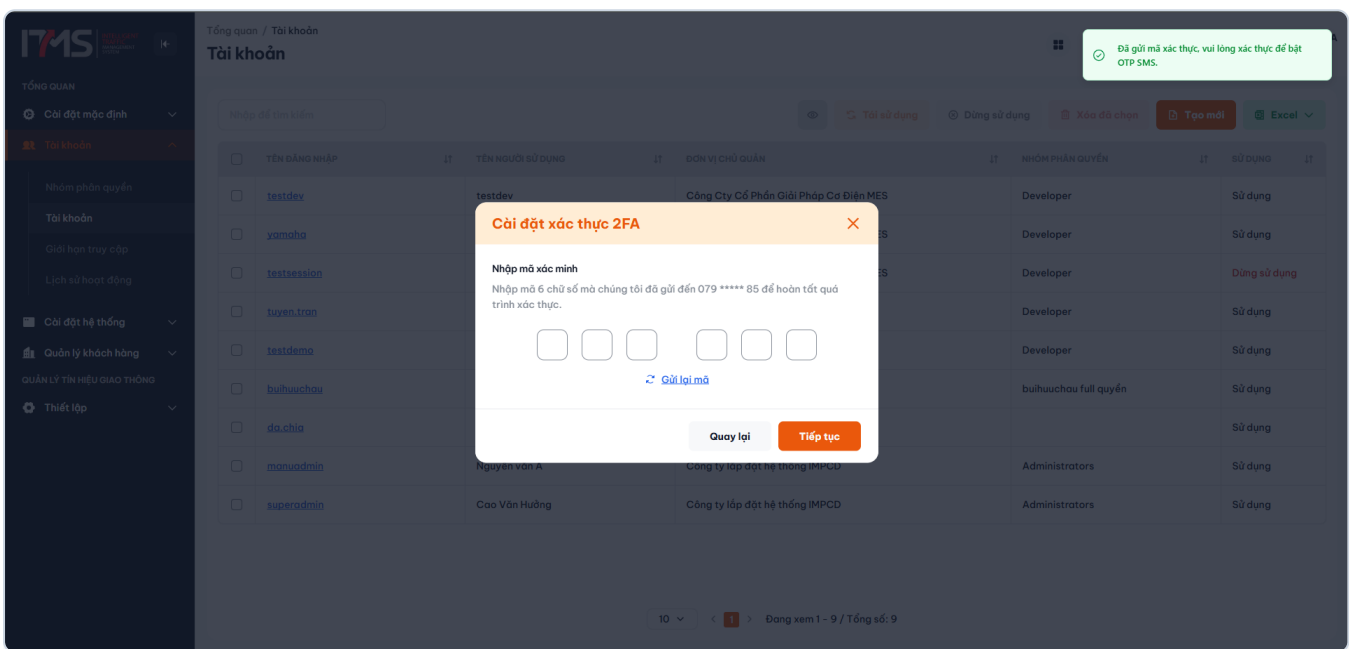
4.2 Bước 2: Nhập số điện thoại nhận mã xác minh

- Hệ thống chuyển sang màn hình **Nhập số điện thoại**.
- Người dùng có thể:
 - Sử dụng số điện thoại di động đã có sẵn trên hồ sơ tài khoản của mình.
 - Hoặc nhập một số điện thoại mới muốn dùng làm phương thức nhận mã 2FA (ví dụ: 0792290085).
- Kiểm tra tính chính xác của số điện thoại vừa nhập để đảm bảo nhận được tin nhắn SMS.
- Nhấn nút **Tiếp tục** (hoặc nhấn **Quay lại** nếu cần điều chỉnh lựa chọn trước đó).



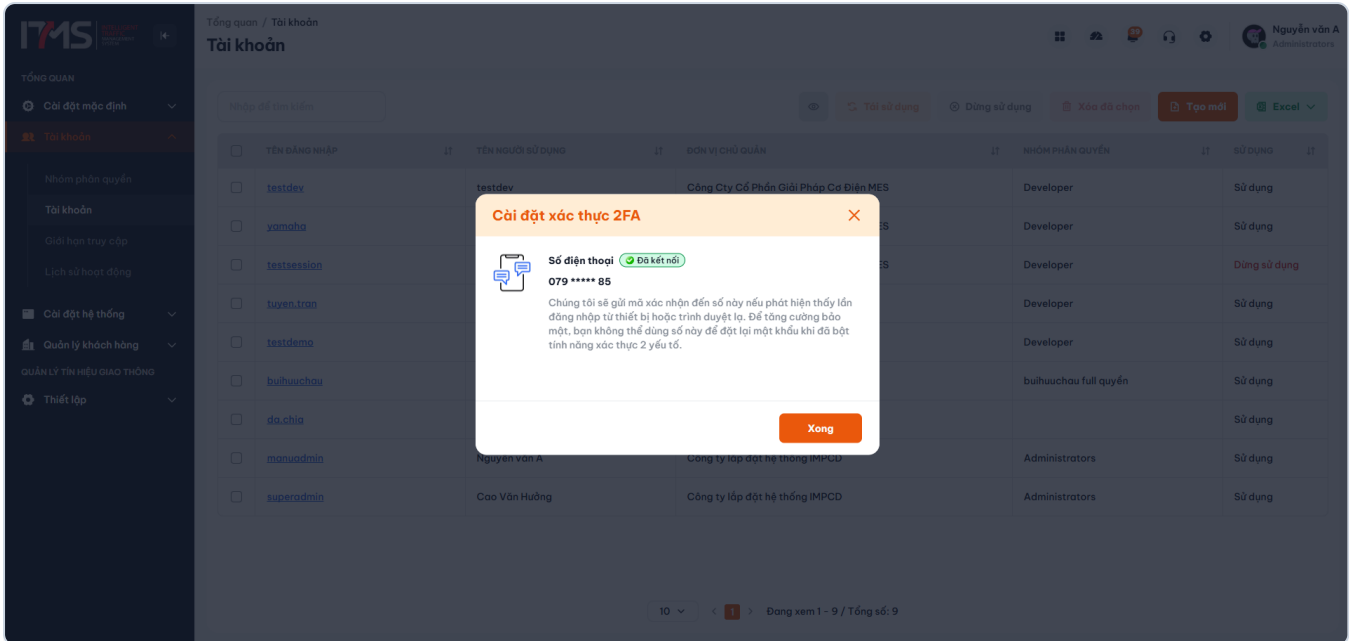
4.3 Bước 3: Nhập mã xác minh (OTP) gửi về tin nhắn

- Hệ thống sẽ ngay lập tức gửi một mã số OTP gồm **6 chữ số** đến số điện thoại vừa đăng ký và hiển thị thông báo toast:
"Đã gửi mã xác thực, vui lòng xác thực để bật OTP SMS."
- Trên màn hình hiển thị lời nhắc:
*"Nhập mã 6 chữ số mà chúng tôi đã gửi đến 079 ***** 85 để hoàn tất quá trình xác thực." (Số điện thoại được che một phần ký tự để đảm bảo an toàn).*
- Mở tin nhắn SMS trên điện thoại của bạn, lấy mã 6 chữ số và nhập lần lượt vào 6 ô trống trên màn hình.
- Trường hợp chưa nhận được tin nhắn sau một khoảng thời gian, bạn có thể nhấn vào nút **Gửi lại mã** (có biểu tượng làm mới) để hệ thống phát lại mã OTP mới.
- Sau khi nhập đầy đủ 6 chữ số hợp lệ, nhấn nút **Tiếp tục**.



4.4 Bước 4: Xác nhận kết nối thành công

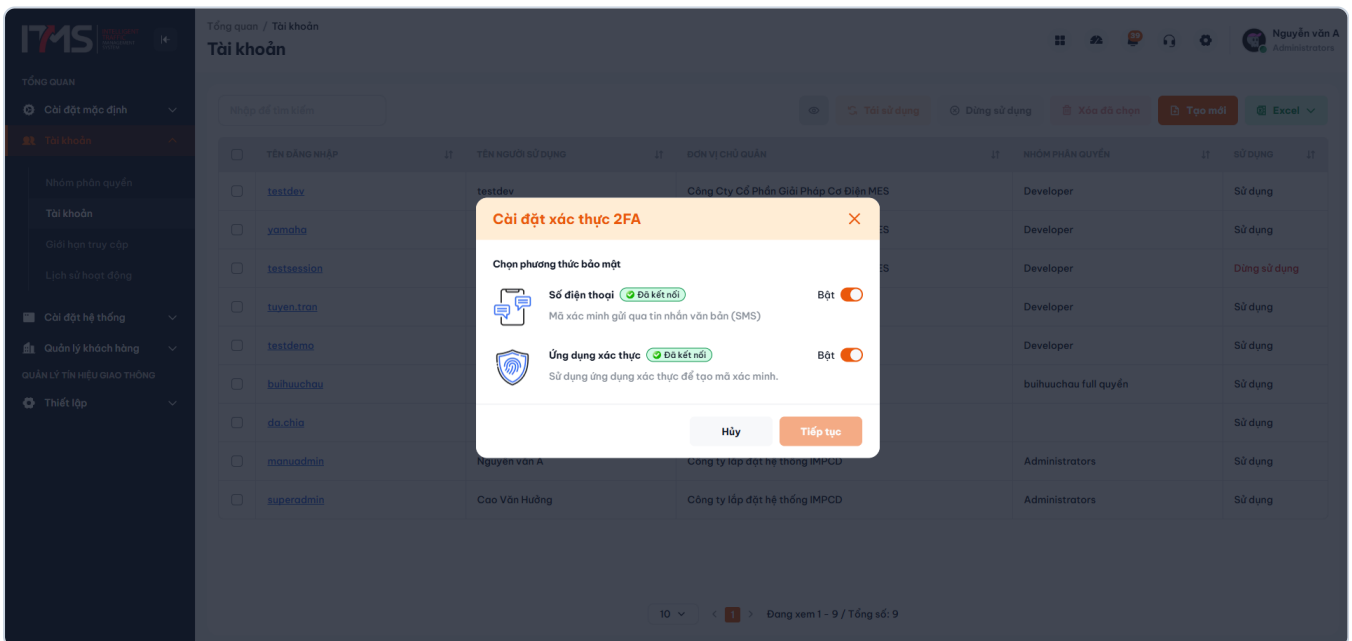
- Khi mã OTP được xác thực thành công, màn hình sẽ hiển thị trạng thái kết nối hoàn tất:
 - Biểu tượng điện thoại kèm huy hiệu màu xanh lá **[Đã kết nối]**.
 - Dòng hiển thị số điện thoại bảo mật đã được ẩn danh: **079 ***** 85**.
 - Lưu ý an toàn từ hệ thống:
> *"Chúng tôi sẽ gửi mã xác nhận đến số này nếu phát hiện thấy lần đăng nhập từ thiết bị hoặc trình duyệt lạ. Để tăng cường bảo mật, bạn không thể dùng số này để đặt lại mật khẩu khi đã bật tính năng xác thực 2 yếu tố."*
- Nhấn nút **Xong** màu cam để đóng màn hình chúc mừng 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 sẽ đưa bạn trở lại màn hình danh mục **Cài đặt xác thực 2FA**:

- Phương thức **Số điện thoại** lúc này hiển thị huy hiệu màu xanh lá **[Đã kết nối]**.
- Công tắc trạng thái hiển thị rõ ràng là **Bật** (màu cam).
- Tài khoản của bạn đã được bảo vệ thành công bằng 2FA qua tin nhắn SMS.



5. Hoạt động của 2FA SMS trong quá trình đăng nhập

Sau khi đã bật tính năng xác thực 2FA qua SMS:

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 phát hiện thiết bị chưa tin cậy và tự động gửi mã OTP 6 số qua tin nhắn SMS tới số điện thoại bạn đã đăng ký.
 - Màn hình đăng nhập chuyển sang bước yêu cầu nhập mã OTP SMS.
 - Chỉ khi nhập đúng mã xác minh từ điện thoại, bạn mới có thể truy cập vào hệ thống ITMS.

6. Lưu ý quan trọng & Khắc phục sự cố

Trường hợp	Nguyên nhân	Hướng dẫn khắc phục
Không nhận được mã SMS OTP	Sóng di động yếu, SIM bị khóa 1 chiều hoặc nghẽn mạng viễn thông	Kiểm tra cột sóng điện thoại, khởi động lại máy hoặc nhấn "Gửi lại mã" sau khi hết thời gian chờ.
Báo lỗi mã không chính xác	Nhập sai số hoặc mã OTP đã hết hiệu lực	Kiểm tra lại tin nhắn mới nhất (nếu bạn đã bấm gửi lại nhiều lần, hãy dùng mã trong tin nhắn gửi đến sau cùng).
Không thể dùng số này để đặt lại mật khẩu	Chính sách bảo mật bắt buộc của ITMS khi kích hoạt 2FA	Để khôi phục mật khẩu khi quên, người dùng cần dùng các phương thức khác (như xác thực qua Email công vụ) hoặc liên hệ Quản trị viên hệ thống để được hỗ trợ.
Muốn đổi sang số điện thoại khác	Người dùng thay đổi số thuê bao di động	Truy cập lại vào Cài đặt xác thực 2FA , gạt tắt phương thức Số điện thoại (yêu cầu xác thực mật khẩu/OTP hiện tại) rồi tiến hành thiết lập lại với số điện thoại mới.

7. Kênh hỗ trợ kỹ thuật

Trong trường hợp người dùng gặp sự cố liên quan đến thiết lập 2FA hoặc mất điện thoại nhận mã:

- **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 SMS

Bảng tổng hợp các mã phản hồi từ hệ thống khi kích hoạt và xác thực phương thức 2FA qua tin nhắn SMS:

Mã phản hồi (HTTP/Status)	Thông báo hiển thị trên giao diện	Nguyên nhân kỹ thuật & Nghiệp vụ	Hướng khắc phục
400 Bad Request	Số điện thoại không hợp lệ	Số điện thoại nhập vào không đúng cấu trúc 10 chữ số của các nhà mạng viễn thông Việt Nam.	Kiểm tra lại số điện thoại, đảm bảo bắt đầu bằng số 0 và gồm 10 chữ số.
401 Unauthorized	Phiên làm việc hết hạn	Phiên đăng nhập của tài khoản kết thúc trong quá trình thiết lập.	Đăng nhập lại vào hệ thống và mở lại hộp thoại Cài đặt xác thực 2FA.
403 Forbidden	Tài khoản không được phép đổi cấu hình 2FA	Chính sách tổ chức hoặc vai trò phân quyền hạn chế việc người dùng tự chỉnh sửa cơ chế xác thực.	Liên hệ Quản trị viên hệ thống của cơ quan/tổ chức để được cấp quyền hoặc hỗ trợ kích hoạt.
422 Unprocessable	Mã xác thực không chính xác hoặc đã hết hạn	Người dùng nhập sai 6 chữ số mã OTP nhận qua SMS hoặc mã đã quá thời hạn cho phép.	Kiểm tra tin nhắn SMS mới nhất gửi tới điện thoại và nhập lại đúng mã, hoặc bấm <i>Gửi lại mã</i> .
429 Too Many Requests	Vui lòng chờ trước khi yêu cầu gửi lại mã	Thao tác nhấn nút gửi lại mã nhiều lần vượt quá ngưỡng an toàn viễn thông.	Chờ đồng hồ đếm ngược kết thúc (khoảng 60 giây) trước khi nhấn gửi lại lần tiếp theo.
500 Internal Server Error	Không thể kết nối cổng SMS Gateway	Hệ thống máy chủ hoặc nhà cung cấp dịch vụ SMS viễn thông gặp gián đoạn tạm thời.	Thử lại sau ít phút hoặc phản hồi sự cố tới bộ phận kỹ thuật ITMS.

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

Nhằm tối ưu hóa tốc độ thao tác trên hộp thoại thiết lập 2FA:

Phím tắt / Thao tác	Vị trí áp dụng	Chức năng thực thi
Enter	Tại ô nhập số điện thoại hoặc ô nhập mã OTP 6 số	Xác nhận gửi yêu cầu hoặc hoàn tất xác thực mà không cần nhấp chuột vào nút Tiếp tục .
Tab	Toàn bộ hộp thoại	Di chuyển con trỏ lần lượt qua switch bật/tắt, ô nhập số điện thoại, nút Hủy, Quay lại và 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 và chuyển con trỏ ngay sang ô số kế tiếp.
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: Cơ chế an toàn & Khóa đặt lại mật khẩu khi bật 2FA

Để bảo vệ tối đa tính toàn vẹn và danh tính tài khoản người dùng, hệ thống ITMS áp dụng các quy định an toàn nghiêm ngặt sau:

1. Quy tắc vô hiệu hóa chức năng Đặt lại mật khẩu bằng Số điện thoại 2FA

- Khi một số điện thoại được đăng ký làm phương thức **Xác thực 2 yếu tố (2FA)**, số điện thoại này sẽ **tự động bị vô hiệu hóa tính năng làm phương tiện quên mật khẩu thông thường**.
- Mục đích an toàn:** Ngăn chặn tuyệt đối nguy cơ tấn công chiếm quyền kiểm soát SIM (SIM-swap) hoặc đánh cắp điện thoại để vừa đặt lại mật khẩu vừa vượt qua 2FA.

2. Kênh khôi phục tài khoản thay thế khi quên mật khẩu

- Khi người dùng đã kích hoạt 2FA qua SMS nhưng quên mật khẩu, quy trình khôi phục phải thực hiện qua:
- Kênh Email công vụ:** Đã được xác minh danh tính chính chủ.
- Ủy quyền Quản trị viên Tenant:** Liên hệ Quản trị viên quản lý đơn vị để cấp mã khôi phục an toàn nội bộ.

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 SMS, bổ sung Trang bìa chuẩn in ấn A4, Mục lục nằm riêng 1 trang và hệ thống Phụ lục A, B, C, D.