

HỆ THỐNG QUẢN LÝ VÀ GIÁM SÁT TÍN HIỆU GIAO THÔNG THÔNG MINH

INTELLIGENT TRAFFIC MANAGEMENT SYSTEM (ITMS)

TÀI LIỆU HƯỚNG DẪN NGƯỜI DÙNG

ĐĂNG NHẬP VÀ XÁC THỰC BẢO MẬT

Quy trình đăng nhập đa tầng, xác thực 2 bước (2FA SMS & Authenticator App)

Mã tài liệu:	ITMS-UG-AUTH-01	Phiên bản:	1.1
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 & Thông tin cần chuẩn bị

3. Giao diện & Vị trí truy cập

4. Hướng dẫn thao tác đăng nhập từng bước

- 4.1 Đăng nhập tiêu chuẩn
- 4.2 Xác thực 2 bước (2FA Challenge)
 - Kịch bản 1: Chỉ bật Ứng dụng xác thực (Authenticator App)
 - Kịch bản 2: Chỉ bật Xác thực qua tin nhắn (SMS OTP)
 - Kịch bản 3: Bật đồng thời cả Ứng dụng xác thực và SMS
- 4.3 Lưu trình duyệt tin cậy (Trust Browser)

5. Các cơ chế bảo mật tự động cần lưu ý

- 5.1 Xác minh chống Bot (Cloudflare Turnstile Captcha)
- 5.2 Khóa tạm thời tài khoản do nhập sai quá số lần quy định

6. Xử lý khi Quên mật khẩu

7. Bảng câu hỏi thường gặp (FAQ & Troubleshooting)

8. Kênh hỗ trợ kỹ thuật

PHỤ LỤC TÀI LIỆU

- Phụ lục A: Bảng mã trạng thái & Mã lỗi đăng nhập
- Phụ lục B: Danh mục phím tắt & Thao tác nhanh
- Phụ lục C: Yêu cầu môi trường & Trình duyệt khuyến nghị
- Phụ lục D: Lịch sử cập nhật tài liệu

1. Giới thiệu tổng quan

Màn hình **Đăng nhập (Login)** là cổng xác thực đầu vào bắt buộc của hệ thống **ITMS (Intelligent Traffic Management System)**. Do hệ thống vận hành theo mô hình đa khách hàng (SaaS Multi-tenant), quy trình đăng nhập được bảo mật nghiêm ngặt với 3 lớp định danh: Tổ chức (Tenant/Khách hàng), Danh tính người dùng (Username) và Mật khẩu (Password).

Hệ thống tích hợp các tiêu chuẩn bảo mật hiện đại:

- Xác thực 2 yếu tố (2FA):** Hỗ trợ qua ứng dụng TOTP (Google Authenticator/Microsoft Authenticator) và tin nhắn SMS OTP.
- Bảo vệ chống Brute-force & Bot:** Tự động kích hoạt Cloudflare Turnstile Captcha và khóa tạm thời có đồng hồ đếm ngược khi phát hiện đăng nhập sai nhiều lần liên tiếp.

2. Điều kiện tiên quyết & Thông tin cần chuẩn bị

Trước khi tiến hành đăng nhập, người dùng cần chuẩn bị sẵn các thông tin do Quản trị viên hệ thống hoặc Đơn vị chủ quản cung cấp:

Thông tin	Tên hiển thị trên giao diện	Ý nghĩa	Ví dụ
Mã tổ chức	Mã khách hàng	Mã định danh riêng biệt của công ty / đơn vị quản lý	DEMO_ORG , HANOI_LIGHTING
Tên tài khoản	Tên đăng nhập	Tên tài khoản định danh cá nhân của người dùng	operator_01 , admin
Mật khẩu	Mật khẩu	Mật khẩu truy cập tương ứng	

3. Giao diện & Vị trí truy cập

- Đường dẫn truy cập (URL):** `https://<domain-he-thong>/login`
(Nếu người dùng truy cập bất kỳ trang nghiệp vụ nào khi chưa đăng nhập, hệ thống sẽ tự động chuyển hướng về trang này).



4. Hướng dẫn thao tác đăng nhập từng bước

4.1 Đăng nhập tiêu chuẩn

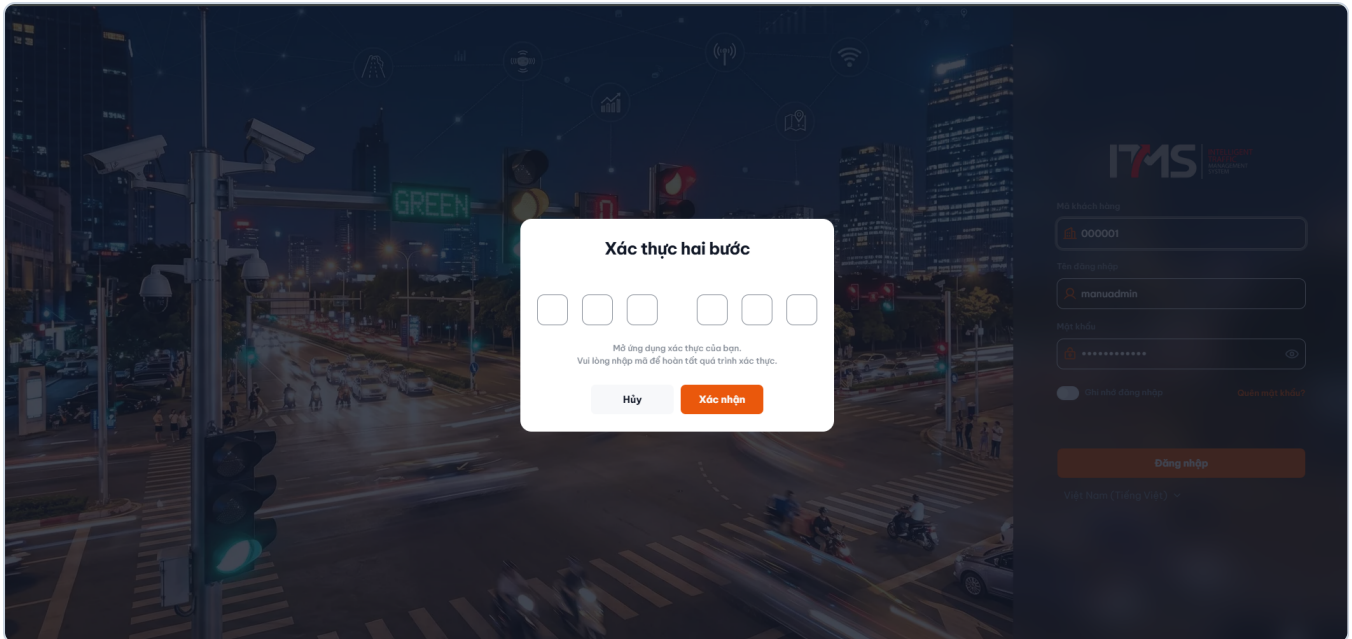
1. **Bước 1:** Truy cập vào trang Đăng nhập của hệ thống ITMS.
2. **Bước 2:** Nhập các thông tin xác thực:
 - Ô **Mã khách hàng**: Nhập mã định danh của tổ chức/doanh nghiệp bạn đang công tác.
 - Ô **Tên đăng nhập**: Nhập tên tài khoản hoặc mã nhân viên đã được cấp.
 - Ô **Mật khẩu**: Nhập mật khẩu của tài khoản. Bạn có thể nhấn vào biểu tượng con mắt ở cuối ô nhập để ẩn/hiện mật khẩu kiểm tra.
3. **Bước 3 (Tùy chọn):** Bật công tắc **Ghi nhớ đăng nhập** nếu đang thao tác trên thiết bị cá nhân an toàn (giúp duy trì phiên làm việc không bị đăng xuất nhanh khi tắt trình duyệt).
4. **Bước 4:** Nhấn nút **Đăng nhập**.
5. **Kết quả:** Khi thông tin chính xác, hệ thống sẽ thông báo **Đăng nhập thành công** và tự động chuyển hướng bạn vào màn hình Trang chủ (Dashboard).

4.2 Xác thực 2 bước (2FA Challenge - Khi tài khoản đã kích hoạt 2FA)

Nếu tài khoản của bạn được cấu hình bảo mật 2 lớp, sau khi bấm **Đăng nhập**, hộp thoại xác thực hai bước sẽ xuất hiện tùy theo phương thức bạn đã cài đặt trên tài khoản:

Kịch bản 1: Chỉ bật Ứng dụng xác thực (Authenticator App)

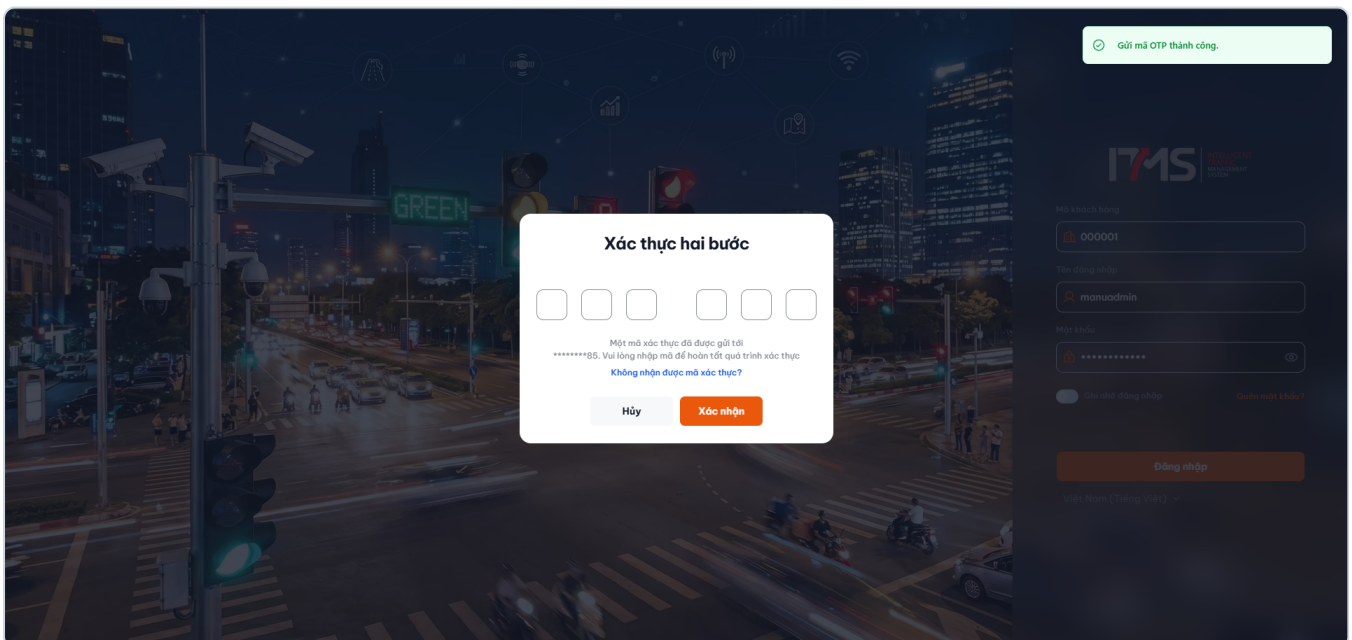
Khi tài khoản chỉ kích hoạt phương thức ứng dụng Authenticator:



1. Mở ứng dụng xác thực trên điện thoại của bạn (ví dụ: Google Authenticator, Microsoft Authenticator, Duo).
2. Xem mã 6 chữ số ngẫu nhiên tương ứng với tài khoản ITMS.
3. Nhập 6 chữ số này vào các ô mã OTP trên màn hình.
4. Nhấn nút **Xác nhận** màu cam.

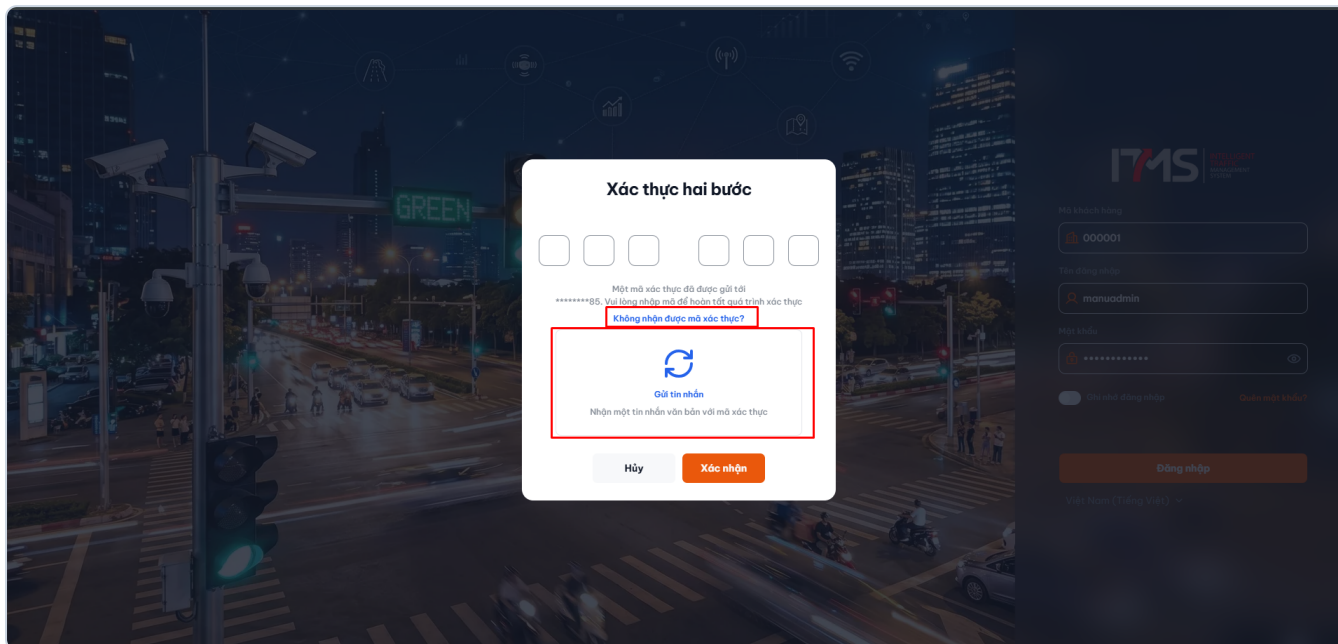
Kịch bản 2: Chỉ bật Xác thực qua tin nhắn (SMS OTP)

Khi tài khoản chỉ kích hoạt phương thức nhận mã qua SMS:



1. Hệ thống tự động gửi tin nhắn chứa mã OTP đến số điện thoại đã đăng ký (hiển thị thông báo "Gửi mã OTP thành công" và số điện thoại được che dạng *****85).
2. Mở tin nhắn SMS trên điện thoại để lấy mã xác thực.
3. Nhập 6 chữ số vào các ô trên màn hình và nhấn **Xác nhận**.

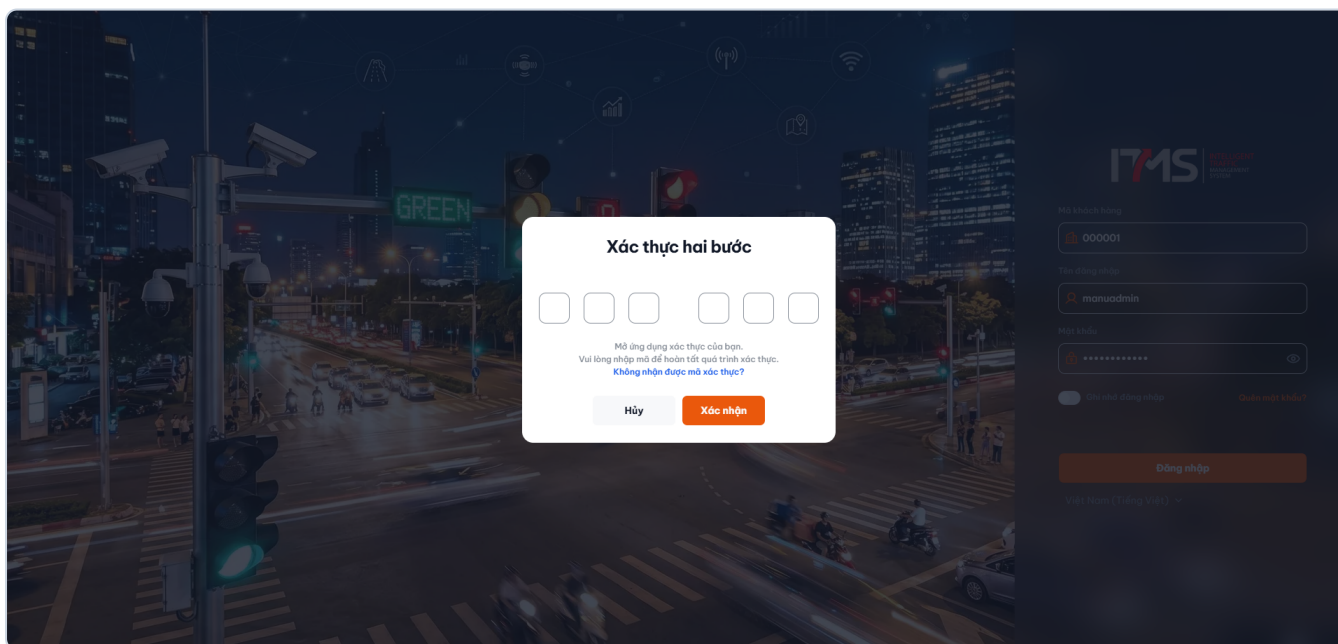
Nếu chưa nhận được tin nhắn SMS:



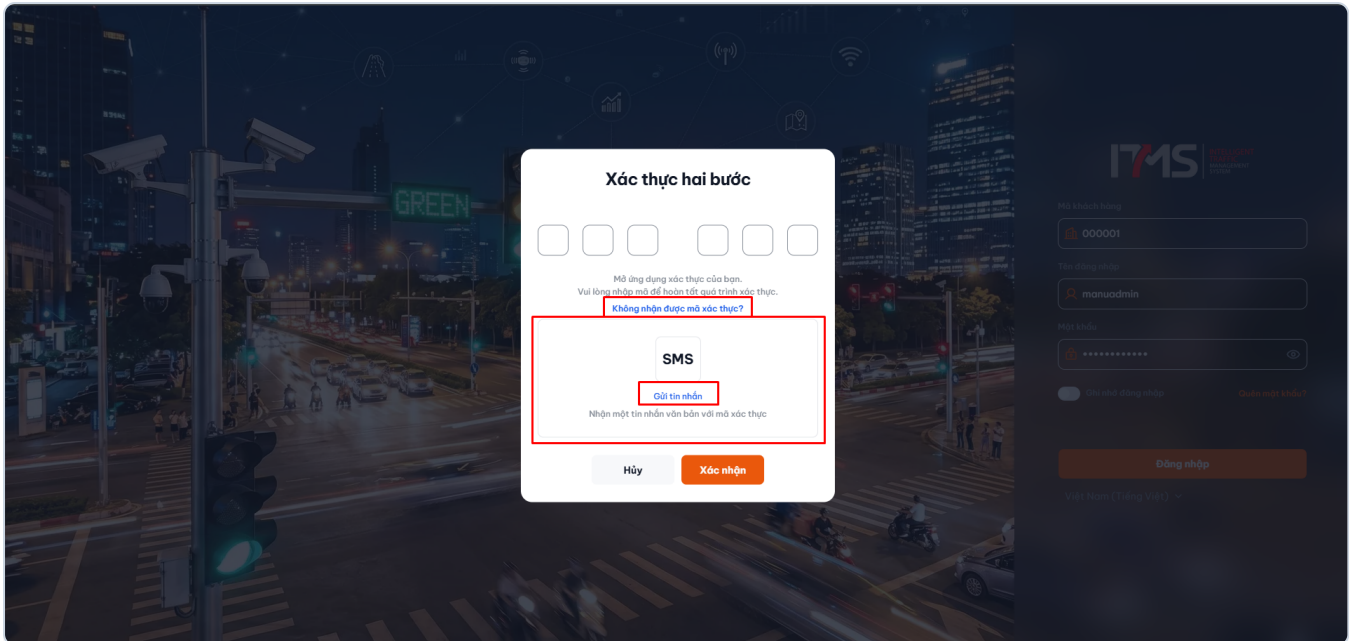
- Nhấp vào dòng liên kết màu xanh "**Không nhận được mã xác thực?**".
- Khung tùy chọn mở rộng xuất hiện với biểu tượng làm mới và nút **Gửi tin nhắn**.
- Nhấp nút **Gửi tin nhắn** để hệ thống tạo và gửi lại mã OTP mới đến điện thoại của bạn.

Kịch bản 3: Bật đồng thời cả Ứng dụng xác thực và SMS (Chuyển đổi phương thức linh hoạt)

Khi tài khoản cài đặt cả 2 phương thức bảo vệ, hệ thống sẽ ưu tiên mở xác thực qua ứng dụng Authenticator trước:



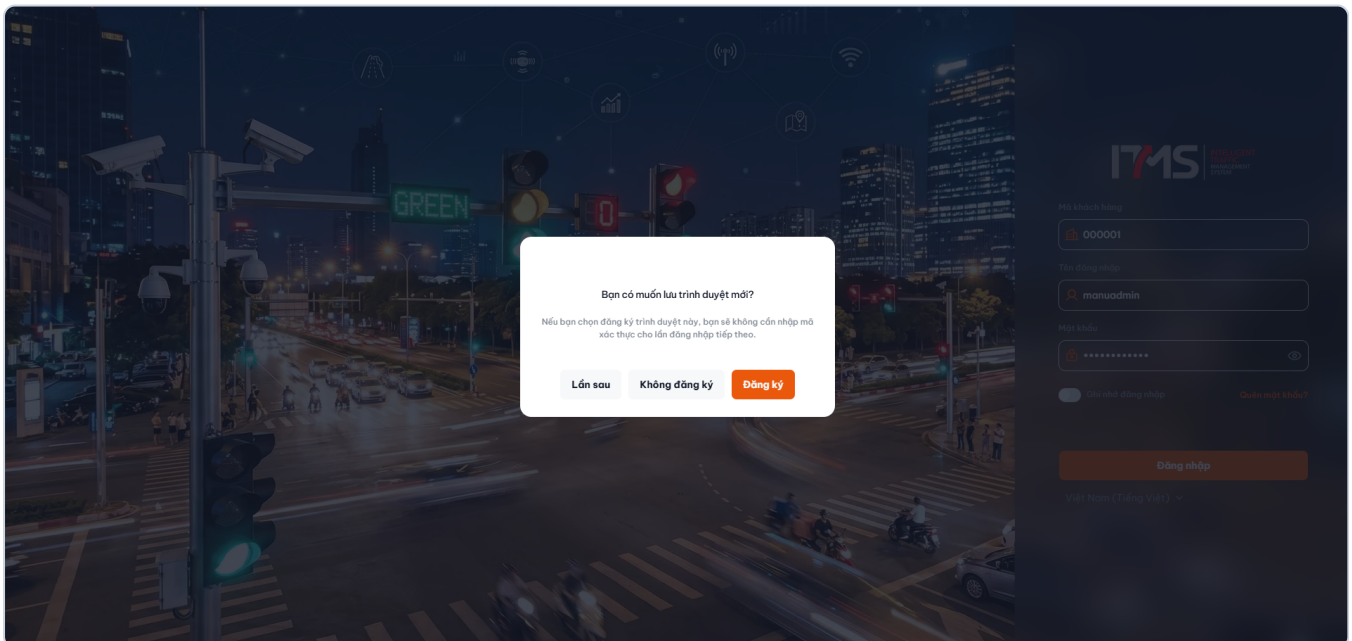
1. Nhập mã từ ứng dụng Authenticator như bình thường.
2. **Trường hợp không mở được App Authenticator:**
 - Nhấp vào dòng liên kết màu xanh "**Không nhận được mã xác thực?**":



- Khung tùy chọn chuyển đổi xuất hiện với logo **SMS** và nút **Gửi tin nhắn** ("Nhận một tin nhắn văn bản với mã xác thực").
- Nhấp vào nút **Gửi tin nhắn**, hệ thống sẽ lập tức chuyển hướng và gửi mã OTP về số điện thoại SMS của bạn để hoàn tất quá trình xác thực.

4.3 Lưu trình duyệt tin cậy (Trust Browser)

Sau khi hoàn tất xác thực 2FA thành công, nếu đây là lần đầu tiên bạn đăng nhập trên trình duyệt này, hệ thống sẽ hiển thị hộp thoại:



Hộp thoại thông báo: "Bạn có muốn lưu trình duyệt mới? Nếu bạn chọn đăng ký trình duyệt này, bạn sẽ không cần nhập mã xác thực cho lần đăng nhập tiếp theo."

Người dùng có 3 lựa chọn:

1. **Đăng ký (Khuyến dùng trên thiết bị làm việc cá nhân):** Bấm nút màu cam **Đăng ký**. Trình duyệt này sẽ được lưu vào danh sách thiết bị tin cậy, các lần đăng nhập tiếp theo bạn chỉ cần nhập mật khẩu mà không bị hỏi lại mã 2FA.
2. **Không đăng ký (Khuyến dùng trên máy tính công cộng / dùng chung):** Bấm nút **Không đăng ký**. Hệ thống sẽ luôn yêu cầu mã 2FA ở mỗi lần đăng nhập để đảm bảo an toàn tuyệt đối.
3. **Lần sau:** Tạm thời bỏ qua quyết định và sẽ hỏi lại ở phiên làm việc sau.

5. Các cơ chế bảo mật tự động cần lưu ý

5.1 Xác minh chống Bot (Cloudflare Turnstile Captcha)

- **Khi nào xuất hiện:** Khi hệ thống phát hiện có dấu hiệu truy cập bất thường hoặc sau một số lần đăng nhập không thành công.
- **Cách thao tác:** Hộp thoại Captcha sẽ tự động hiển thị bên trên nút Đăng nhập. Người dùng chỉ cần tích chọn ô vuông xác nhận "Tôi là con người" (hoặc chờ hệ thống tự xác thực). Khi xuất hiện dấu tích xanh xác nhận, bạn có thể tiếp tục nhấn nút **Đăng nhập**.

5.2 Khóa tạm thời tài khoản do nhập sai quá số lần quy định

- **Quy tắc an toàn:** Hệ thống giới hạn tối đa **5 lần** nhập sai liên tiếp (`LIMIT_RETRY_LOGIN = 5`).
- **Hành vi hệ thống:**
- Nếu vượt quá số lần cho phép, nút **Đăng nhập** sẽ tự động bị vô hiệu hóa và hiển thị đồng hồ đếm ngược: `Thử lại sau MM:SS` (Ví dụ: `Thử lại sau 04:59`).
- Người dùng bắt buộc phải đợi đồng hồ đếm ngược về `00:00` thì nút Đăng nhập mới mở lại để nhập tiếp.

[!WARNING]

Không cố tình tải lại trang (F5) liên tục vì thời gian khóa được quản lý chặt chẽ từ phía máy chủ; việc tải lại trang không làm mất thời gian đếm ngược.

6. Xử lý khi Quên mật khẩu

Nếu không nhớ mật khẩu đăng nhập, tuyệt đối không thử đoán mò quá 5 lần để tránh bị khóa tài khoản:

1. Tại góc phải của form đăng nhập, bấm vào liên kết **Quên mật khẩu?**.
 2. Hệ thống chuyển sang giao diện Khôi phục mật khẩu (`/forgot-password`).
 3. Nhập **Mã khách hàng** và **Email** hoặc **Số điện thoại** đã đăng ký trên hồ sơ tài khoản.
 4. Bấm **Đặt lại mật khẩu** và làm theo hướng dẫn gửi về qua OTP để thiết lập mật khẩu mới.
-

7. Bảng câu hỏi thường gặp (FAQ & Troubleshooting)

Hiện tượng / Vấn đề	Nguyên nhân có thể	Hướng xử lý
Báo lỗi "Mã khách hàng / Tên đăng nhập không đúng"	Nhập sai khoảng trắng hoặc viết hoa/thường không chuẩn	Kiểm tra lại phím Caps Lock , kiểm tra chính xác mã định danh tổ chức do quản trị viên cấp.
Báo lỗi "Mã khách hàng không được để trống"	Chưa điền ô đầu tiên trong form	Điền đầy đủ cả 3 ô: Mã khách hàng, Tên đăng nhập, Mật khẩu.
Nút Đăng nhập bị mờ và có đồng hồ đếm ngược	Đã nhập sai quá 5 lần quy định	Đợi hết thời gian đếm ngược hiển thị trên nút để thử lại, hoặc dùng tính năng <i>Quên mật khẩu?</i> .
Không nhận được SMS OTP 2FA	Điện thoại mất sóng hoặc nhà mạng chặn tin nhắn thương hiệu	Nhấn nút Gửi lại mã sau khi thời gian chờ kết thúc, hoặc chọn chuyển sang dùng <i>Ứng dụng xác thực (Authenticator App)</i> .
Sau khi đăng nhập bị vắng lại trang Login	Phiên đăng nhập hết hạn hoặc tài khoản bị đăng nhập từ nơi khác	Tiến hành đăng nhập lại. Đảm bảo trình duyệt không chặn lưu Cookie.

8. Kênh hỗ trợ kỹ thuật

Trong trường hợp tài khoản bị khóa hoàn toàn, quên Mã khách hàng hoặc mất thiết bị chứa mã 2FA, vui lòng liên hệ bộ phận hỗ trợ kỹ thuật:

- **Đầu mối nội bộ:** Liên hệ Quản trị viên Tenant của cơ quan/tổ chức bạn.
- **Tổng đài hỗ trợ kỹ thuật ITMS:** 1900 xxxx (Nhánh 1 - Vận hành hệ thống)
- **Email hỗ trợ:** support@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 đăng nhập thường gặp

Bảng tổng hợp các mã phản hồi từ hệ thống khi thao tác đăng nhập và 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	Dữ liệu không hợp lệ	Thiếu một trong các trường bắt buộc (Mã khách hàng, Tên đăng nhập, Mật khẩu) hoặc định dạng không đúng chuẩn.	Kiểm tra lại các ô nhập liệu, đảm bảo không bỏ trống bất kỳ trường nào.
401 Unauthorized	Tên đăng nhập hoặc mật khẩu không chính xác	Thông tin định danh không khớp với cơ sở dữ liệu xác thực của tổ chức.	Kiểm tra phím Caps Lock , kiểm tra lại mã khách hàng và mật khẩu chính xác.
403 Forbidden	Tài khoản đã bị tạm dừng / Tổ chức hết hạn	Tài khoản bị vô hiệu hóa bởi Quản trị viên hoặc gói dịch vụ thuê bao của khách hàng đã hết hạn.	Liên hệ Quản trị viên đơn vị hoặc đầu mối kỹ thuật ITMS để kích hoạt lại tài khoản.
422 Unprocessable	Mã xác thực không đúng hoặc đã hết hạn	Nhập sai 6 chữ số OTP hoặc mã đã quá thời gian hiệu lực (thông thường 60 giây).	Nhập lại mã mới hoặc bấm <i>Gửi lại mã</i> để nhận mã mới.
429 Too Many Requests	Đăng nhập sai quá nhiều lần. Vui lòng chờ...	Người dùng nhập sai quá 5 lần liên tiếp, kích hoạt cơ chế chống dò mật khẩu tự động.	Chờ đồng hồ đếm ngược trên nút Đăng nhập chạy về 00:00 hoặc sử dụng tính năng <i>Quên mật khẩu</i> .
500 Internal Server Error	Lỗi hệ thống máy chủ xác thực	Sự cố kết nối cơ sở dữ liệu xác thực hoặc dịch vụ gửi tin nhắn SMS của nhà mạng gặp gián đoạn.	Chờ vài phút và thử lại, hoặc thông báo tổng đài kỹ thuật ITMS.

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

Nhằm tối ưu hóa tốc độ thao tác cho người vận hành hệ thống, giao diện đăng nhập hỗ trợ các phím tắt sau:

Phím tắt / Thao tác	Vị trí áp dụng	Chức năng thực thi
Enter	Tại bất kỳ ô nhập liệu nào	Gửi yêu cầu đăng nhập ngay lập tức (tương đương bấm nút Đăng nhập).
Enter	Tại ô nhập mã OTP (2FA)	Gửi mã xác nhận ngay lập tức khi đã điền đủ 6 chữ số.
Tab	Toàn bộ form	Di chuyển con trỏ tuần tự: <i>Mã khách hàng</i> → <i>Tên đăng nhập</i> → <i>Mật khẩu</i> → <i>Ghi nhớ đăng nhập</i> → <i>Nút Đăng nhập</i> .
Shift + Tab	Toàn bộ form	Di chuyển con trỏ ngược lại ô nhập liệu liền trước.
Space	Khi con trỏ đang ở công tắc <i>Ghi nhớ đăng nhập</i>	Bật / Tắt trạng thái ghi nhớ phiên làm việc trên trình duyệt.
Click biểu tượng con mắt	Ô Mật khẩu	Chuyển đổi qua lại giữa chế độ ẩn ký tự và hiển thị văn bản rõ.

Phụ lục C: Yêu cầu môi trường & Trình duyệt khuyến nghị

Để đảm bảo hiệu năng tối đa và hoạt động ổn định của các tính năng bảo mật (Cloudflare Turnstile), người dùng nên vận hành trên môi trường khuyến nghị:

1. Trình duyệt web hỗ trợ

- **Google Chrome:** Phiên bản 90 trở lên (*Khuyến dùng tối ưu nhất*).
- **Microsoft Edge (Chromium):** Phiên bản 90 trở lên (*Khuyến dùng trên môi trường Windows*).
- **Mozilla Firefox:** Phiên bản 88 trở lên.
- **Apple Safari:** Phiên bản 14 trở lên (trên macOS / iPadOS / iOS).

2. Yêu cầu về mạng và cấu hình bảo mật trình duyệt

- Bật cho phép lưu trữ **Cookie** và **Local Storage** cho tên miền của hệ thống ITMS.
- Cho phép tải và chạy JavaScript (không sử dụng các tiện ích chặn script quá mức làm gián đoạn Cloudflare Turnstile Captcha).
- Đảm bảo thiết bị di động nhận SMS có sóng viễn thông ổn định khi sử dụng kênh 2FA SMS.

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 đăng nhập cơ bản và luồng xác thực ban đầu.