TÀI LIỆU HƯỚNG DẪN NGƯỜI DÙNG

QUẢN LÝ HẠN CHẾ TRUY CẬP (ACCESS RESTRICTIONS)

Quy trình thiết lập quy tắc tường lửa ứng dụng, kiểm soát địa chỉ IP, loại thiết bị, tài khoản áp dụng, chế độ chặn toàn hệ thống và xuất báo cáo an toàn mạng trên ITMS

Mã tài liệu:	`ITMS-UG-ACR-01`	**Phiên bản:**	`1.0`
Ngày ban hành:	25/09/2026	**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

Phân hệ **Quản lý Hạn chế truy cập (Access Restrictions)** là lá chắn bảo mật lớp ứng dụng thiết yếu của hệ thống điều hành và giám sát tín hiệu giao thông thông minh ITMS. Tính năng này cho phép Quản trị viên hệ thống chủ động kiểm soát các luồng truy cập kết nối vào phần mềm, ngăn ngừa việc đăng nhập trái phép từ các địa chỉ mạng lạ, thiết bị không tin cậy hoặc ngoài phạm vi địa bàn quản trị.

Các vai trò trọng tâm của phân hệ Quản lý Hạn chế truy cập bao gồm:

- **Kiểm soát truy cập theo địa chỉ mạng (IP Whitelist / Blacklist):** Giới hạn chỉ cho phép các dải địa chỉ IPv4 nội bộ, IP tĩnh của trung tâm điều hành hoặc ngăn chặn các địa chỉ IP bị nghi vấn.
- **Phân loại môi trường thiết bị:** Áp dụng chính sách truy cập tách biệt theo loại thiết bị như Máy tính để bàn/Laptop (PC), Thiết bị di động/Máy tính bảng (Mobile), hoặc áp dụng đồng thời cho tất cả các loại thiết bị.
- **Gắn kết quy tắc linh hoạt theo tài khoản người dùng:** Cho phép ban hành quy tắc áp dụng chung cho toàn bộ tổ chức hoặc chỉ đích danh các tài khoản nhân sự đặc thù cần siết chặt bảo mật.
- **Chế độ Chặn tất cả khẩn cấp (Emergency Reject All):** Cung cấp công tắc bảo vệ cấp tổ chức cho phép Quản trị viên phong tỏa tức thời toàn bộ các kết nối thông thường khi xảy ra sự cố an ninh mạng hoặc đợt bảo trì hệ thống.
- **Tương tác trực tiếp trên bảng (Inline Table Editing):** Hỗ trợ nhập liệu, điều chỉnh trực tiếp trên các dòng của bảng danh sách, tích hợp cơ chế tự động phát hiện thay đổi chưa lưu (Dirty State Tracking) và tự động lưu khi thêm dòng mới.

---

2. Điều kiện tiên quyết & Phân quyền truy cập

Để thực hiện các tác vụ trong phân hệ Quản lý Hạn chế truy cập, người dùng cần đáp ứng các điều kiện sau:

- **Tài khoản:** Đã đăng nhập vào hệ thống ITMS với phiên làm việc hợp lệ.
- **Phân quyền người dùng:** Tài khoản phải được phân quyền tương ứng trong phân hệ Quản lý Hạn chế truy cập:

Quyền hạn	Phạm vi tác vụ cho phép
Xem danh sách quy tắc truy cập	Cho phép truy cập màn hình Hạn chế truy cập, theo dõi các quy tắc kiểm soát IP, thiết bị và tài khoản áp dụng hiện hành trong tổ chức.
Tạo mới quy tắc truy cập	Cho phép thêm mới các dòng quy tắc giới hạn IP, thiết lập mô tả, lựa chọn hành động (Chặn / Cho phép), loại thiết bị và gán tài khoản.
Chỉnh sửa quy tắc truy cập	Cho phép sửa đổi trực tiếp các thông số quy tắc trên bảng, lưu cập nhật dữ liệu và kích hoạt/hủy kích hoạt chế độ "Chặn tất cả" cấp tổ chức (dành riêng cho Quản trị viên).
Xóa quy tắc truy cập	Cho phép gỡ bỏ một quy tắc khỏi hệ thống sau khi đã xác nhận an toàn qua hộp thoại cảnh báo.
Xuất dữ liệu Excel	Cho phép kết xuất toàn bộ danh sách quy tắc hạn chế truy cập ra tệp bảng tính Excel (.xlsx).

- **Môi trường vận hành:** Trình duyệt web hiện đại (Google Chrome, Microsoft Edge, Mozilla Firefox, Apple Safari) với màn hình tối ưu từ 1366x768 trở lên.

---

3. Bố cục giao diện & Vị trí truy cập

3.1 Vị trí truy cập trên menu hệ thống

Người dùng truy cập vào phân hệ Quản lý Hạn chế truy cập theo đường dẫn:

- Chọn menu **Hệ thống** $\rightarrow$ chọn mục **Quản lý Tài khoản** $\rightarrow$ nhấp vào tab hoặc mục con **Hạn chế truy cập** (đường dẫn trực tiếp: `/overview/accounts/access-restrictions`).

3.2 Bố cục màn hình làm việc

Giao diện Quản lý Hạn chế truy cập được thiết kế tinh giản, trực quan và tối ưu cho thao tác nhanh:

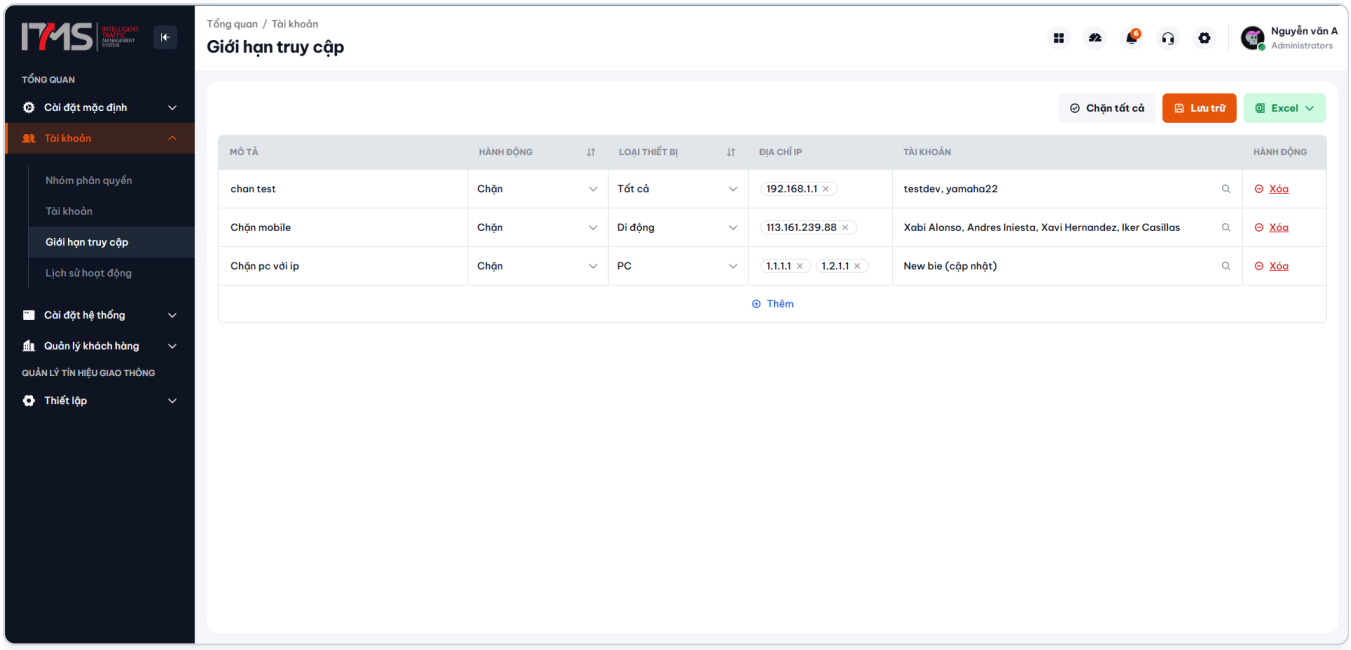
1. **Thanh công cụ tác vụ (Action Toolbar):**
   - *Nút "+ Thêm":* Thêm một dòng quy tắc mới vào cuối bảng dữ liệu (tự động kiểm tra và lưu các dòng cũ trước khi thêm).
   - *Nút "Lưu":* Kiểm tra tính hợp lệ toàn bảng và gửi yêu cầu lưu các thay đổi về máy chủ.
   - *Nút "Từ chối tất cả" / "Hủy từ chối tất cả":* Nút chức năng đặc biệt chỉ hiển thị cho Quản trị viên cấp cao (`Admin`), cho phép bật/tắt chế độ khóa truy cập toàn diện.
   - *Nút "Xuất Excel":* Trích xuất danh sách quy tắc ra tệp bảng tính.
2. **Bảng dữ liệu tương tác trực tiếp (Inline Editing Table):**
   - *STT:* Số thứ tự tự động của quy tắc.
   - *Mô tả:* Ô nhập văn bản thể hiện mục đích của quy tắc (tối đa 255 ký tự).
   - *Hành động:* Hộp chọn giữa **Chặn** (Reject - từ chối kết nối) hoặc **Cho phép** (Accept - cho phép kết nối).
   - *Loại thiết bị:* Hộp chọn môi trường truy cập (**PC**, **Mobile**, hoặc **Tất cả**).
   - *Danh sách địa chỉ IP:* Ô nhập liệu các địa chỉ IPv4 hợp lệ, hỗ trợ nhiều IP cách nhau bởi dấu phẩy.
   - *Danh sách tài khoản:* Nút mở hộp thoại chọn tài khoản người dùng chịu tác động hoặc để trống nếu áp

dụng cho tất cả tài khoản.
- *Thao tác:* Biểu tượng thùng rác để kích hoạt lệnh xóa quy tắc.

4. Hướng dẫn xem & Quản lý danh sách quy tắc truy cập

4.1 Xem danh sách tổng quan các quy tắc hiện hành

Khi truy cập vào màn hình Hạn chế truy cập, hệ thống tự động tải toàn bộ danh sách các quy tắc bảo mật đang có hiệu lực trong phạm vi tổ chức:



Hình 4.1: Bảng dữ liệu danh sách quy tắc hạn chế truy cập trên hệ thống ITMS.

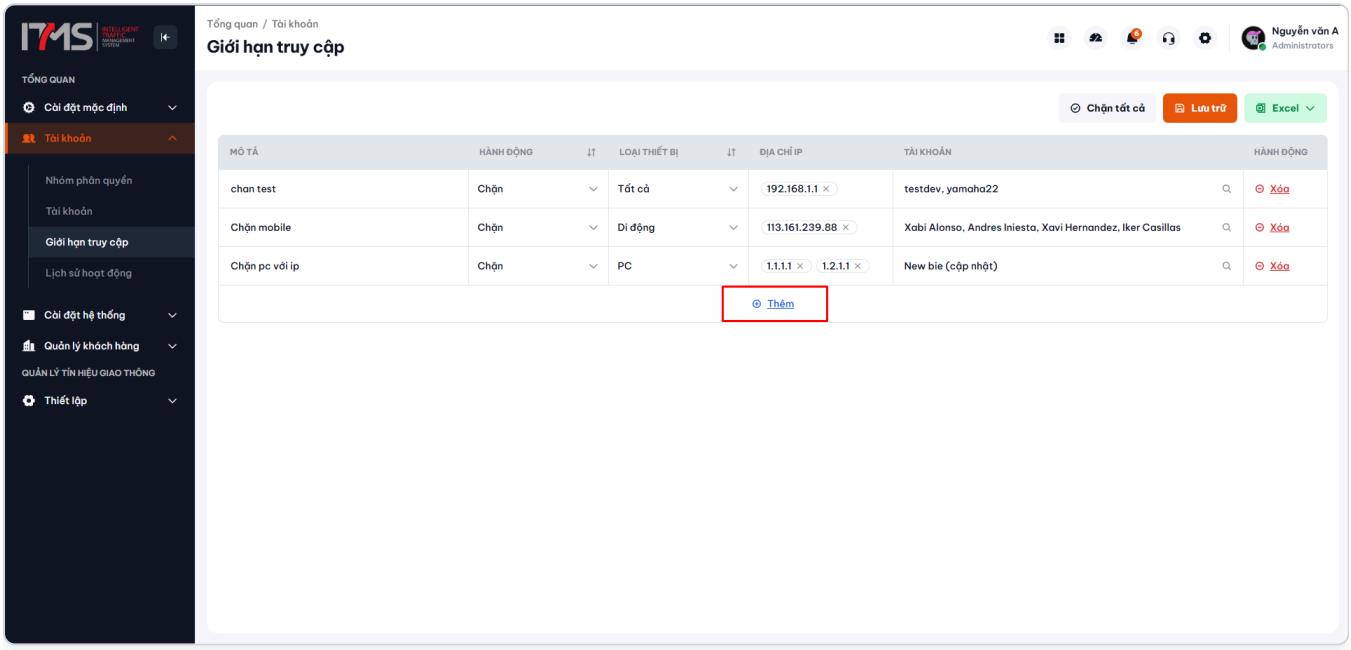
- Toàn bộ các dòng dữ liệu đều cho phép người dùng nhấp trực tiếp vào từng ô để xem hoặc chỉnh sửa thông tin.
- Nếu tổ chức chưa thiết lập quy tắc nào, bảng sẽ hiển thị ở trạng thái rỗng và người dùng có thể nhấp nút **+ Thêm** để bắt đầu khởi tạo quy tắc bảo vệ đầu tiên.

5. Hướng dẫn Thêm mới quy tắc hạn chế truy cập

5.1 Khởi tạo dòng nhập liệu mới

Để tạo mới một quy tắc bảo vệ truy cập:

1. Trên thanh công cụ, nhấp vào nút **+ Thêm** (nền xanh dương đậm):

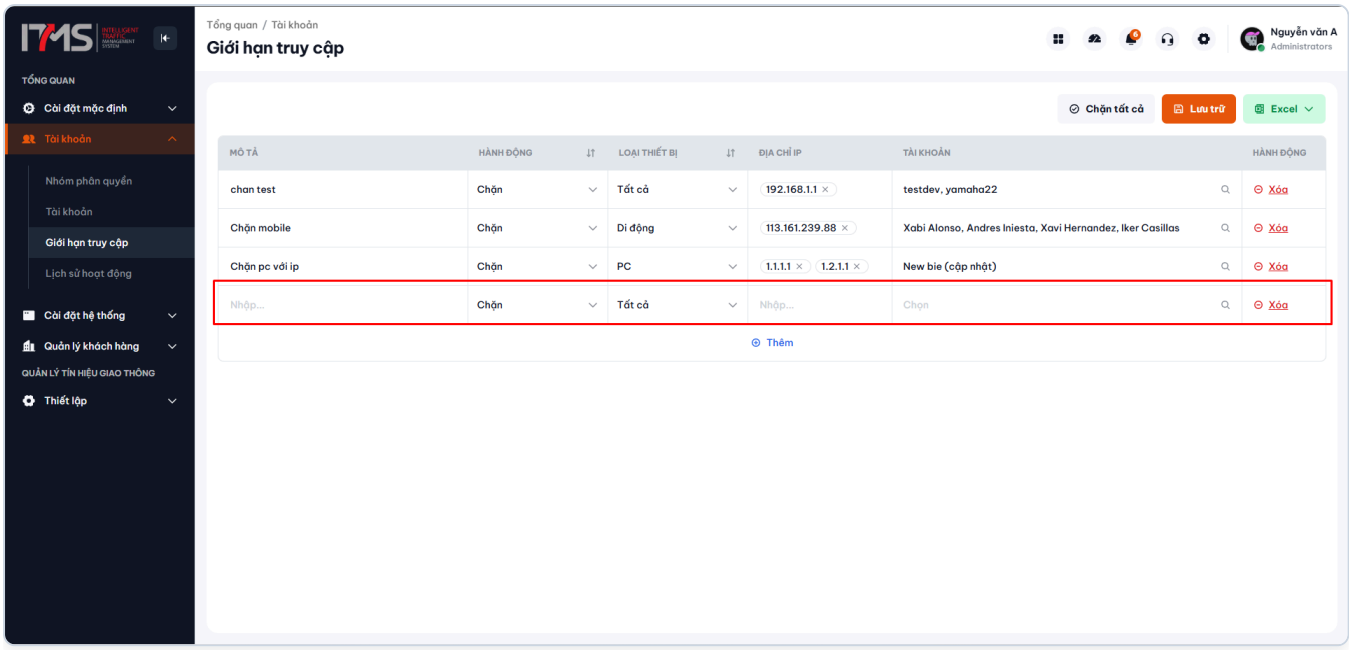


Hình 5.1: Vị trí nút "+ Thêm" trên thanh công cụ tác vụ.

Cơ chế tự động lưu thông minh (Auto-save on Add):
- Khi người dùng nhấn **+ Thêm**, hệ thống sẽ tự động kiểm tra xem các dòng hiện tại trên bảng có thay đổi chưa lưu hay không.
- Nếu có dòng đang chỉnh sửa, hệ thống sẽ tự động xác thực và thực hiện lưu ngầm thành công trước khi chèn thêm dòng mới vào bảng, ngăn chặn triệt để tình trạng mất dữ liệu thao tác.

5.2 Nhập Mô tả, Hành động, Loại thiết bị & Địa chỉ IP

Ngay sau khi kích hoạt, một dòng dữ liệu mới sẽ xuất hiện ở cuối bảng để người dùng tiến hành điền thông tin:



Hình 5.2: Nhập Mô tả, chọn Hành động, Loại thiết bị và điền địa chỉ IPv4.

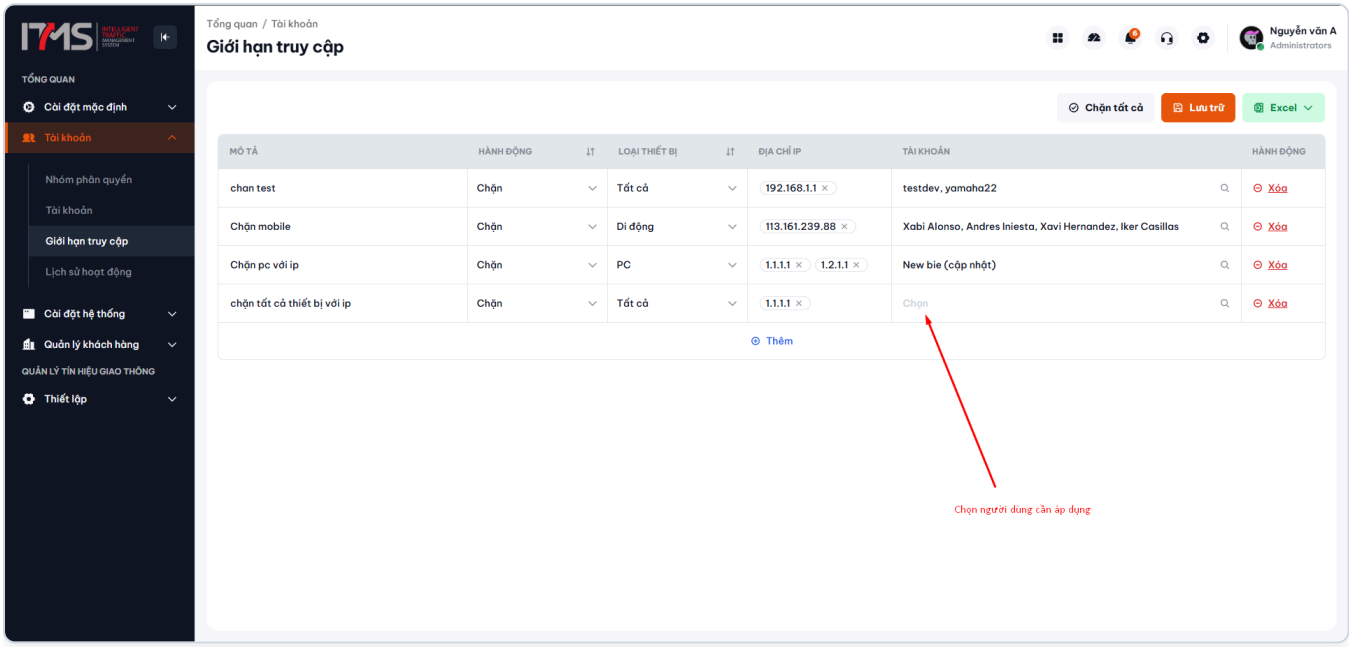
Bảng chi tiết các trường thông tin quy tắc:

Cột dữ liệu	Tính chất	Hướng dẫn nhập liệu & Quy chuẩn nghiệp vụ
Mô tả (*)	Bắt buộc	Nhập văn bản mô tả ngắn gọn mục đích kiểm soát (ví dụ: `Chặn IP mạng ngoài giờ hành chính`, `Chỉ cho phép dải mạng văn phòng`). Tối đa 255 ký tự.
Hành động (*)	Bắt buộc	Chọn một trong hai giá trị: **Chặn** (ngăn chặn không cho đăng nhập) hoặc **Cho phép** (chỉ cho phép đăng nhập từ các IP đã khai báo).
Loại thiết bị (*)	Bắt buộc	Chọn một trong ba giá trị: **PC** (Máy tính), **Mobile** (Điện thoại/Máy tính bảng) hoặc **Tất cả** (Toàn bộ thiết bị).
Danh sách địa chỉ IP (*)	Bắt buộc	Nhập ít nhất một địa chỉ IPv4 hợp lệ (từ `0.0.0.0` đến `255.255.255.255`). Nếu có nhiều địa chỉ IP, nhập cách nhau bằng dấu phẩy.

5.3 Mở giao diện lựa chọn tài khoản áp dụng

Mỗi quy tắc hạn chế truy cập có thể áp dụng cho toàn bộ nhân sự trong tổ chức hoặc chỉ giới hạn trên một số tài khoản cụ thể:

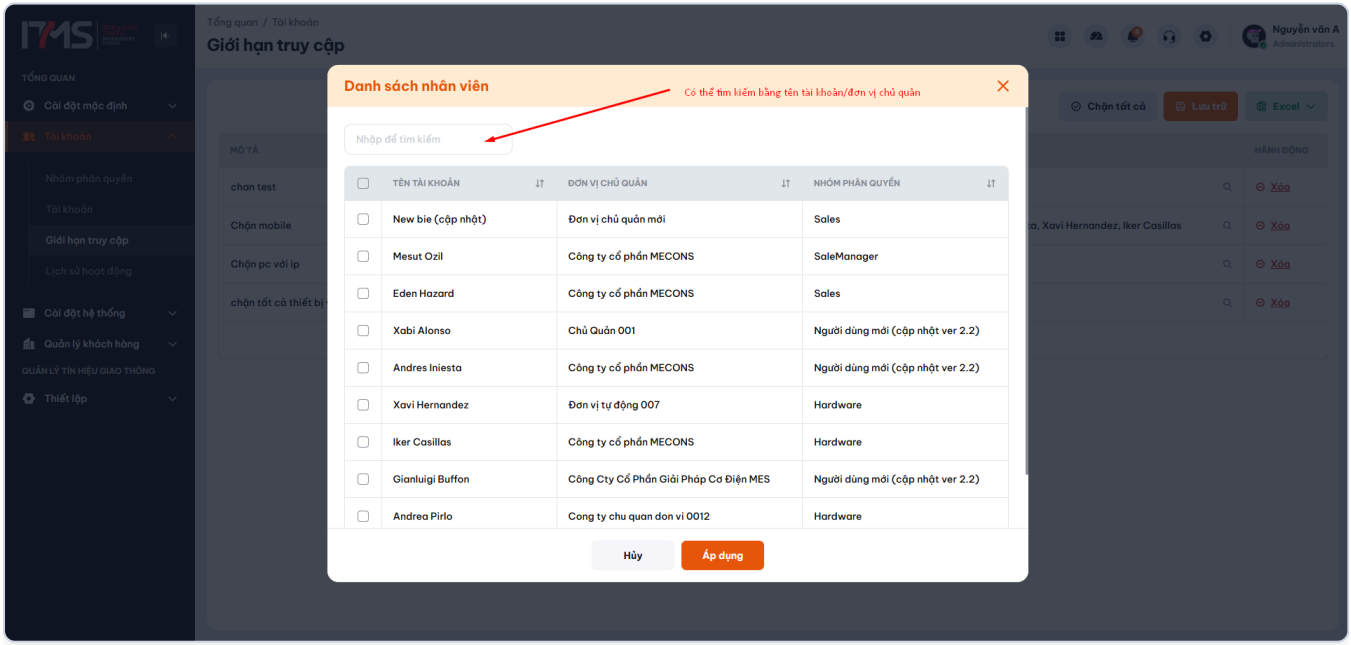
1. Tại cột **Danh sách tài khoản** của dòng quy tắc tương ứng, nhấp vào nút **Chọn tài khoản**:



Hình 5.3: Nút mở hộp thoại chọn tài khoản áp dụng trên dòng dữ liệu.

5.4 Tra cứu tài khoản người dùng trong danh sách

Hộp thoại **Chọn tài khoản** xuất hiện, liệt kê danh sách tài khoản người dùng thuộc tổ chức:

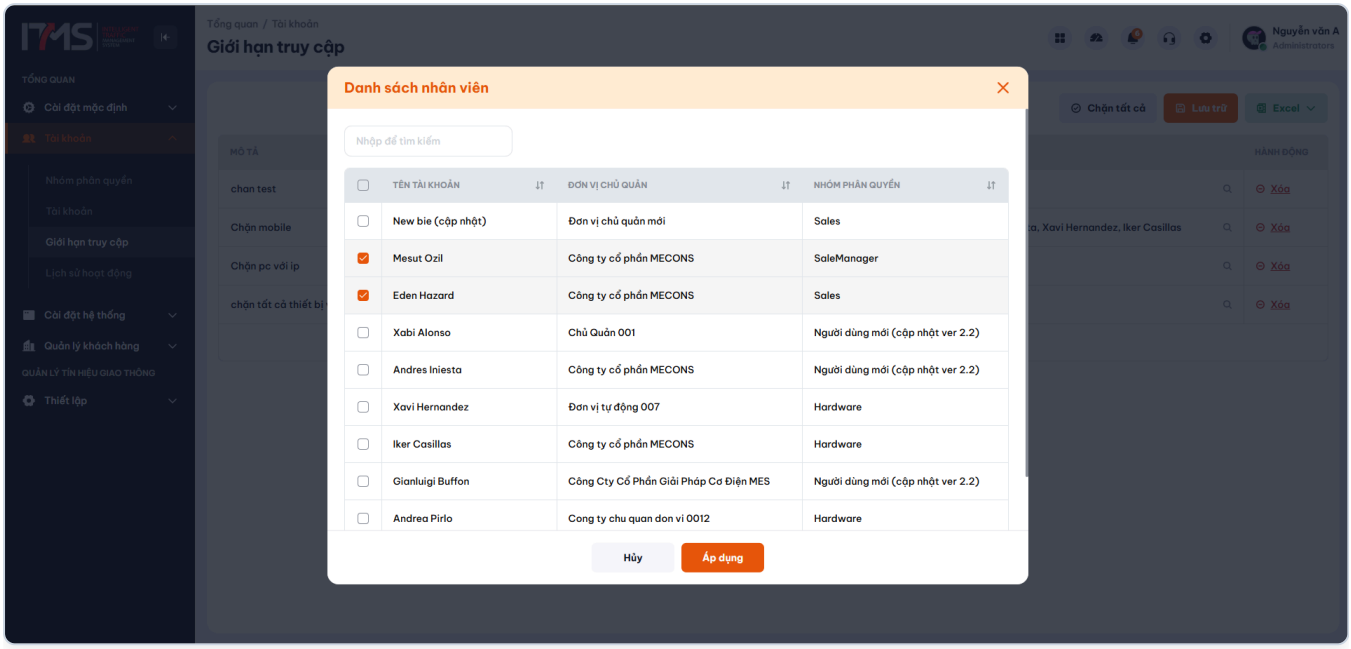


Hình 5.4: Giao diện hộp thoại lựa chọn tài khoản với công cụ tra cứu.

- Người dùng có thể nhập Tên đăng nhập hoặc Họ tên vào ô tìm kiếm ở đầu hộp thoại để lọc nhanh tài khoản cần tìm.
- Hộp thoại tích hợp tính năng cuộn vô tận (Infinite Scroll), tự động tải thêm các tài khoản tiếp theo khi cuộn chuột xuống dưới.

5.5 Tích chọn tài khoản cụ thể hoặc áp dụng toàn bộ

Người dùng lựa chọn phạm vi đối tượng chịu ảnh hưởng của quy tắc:

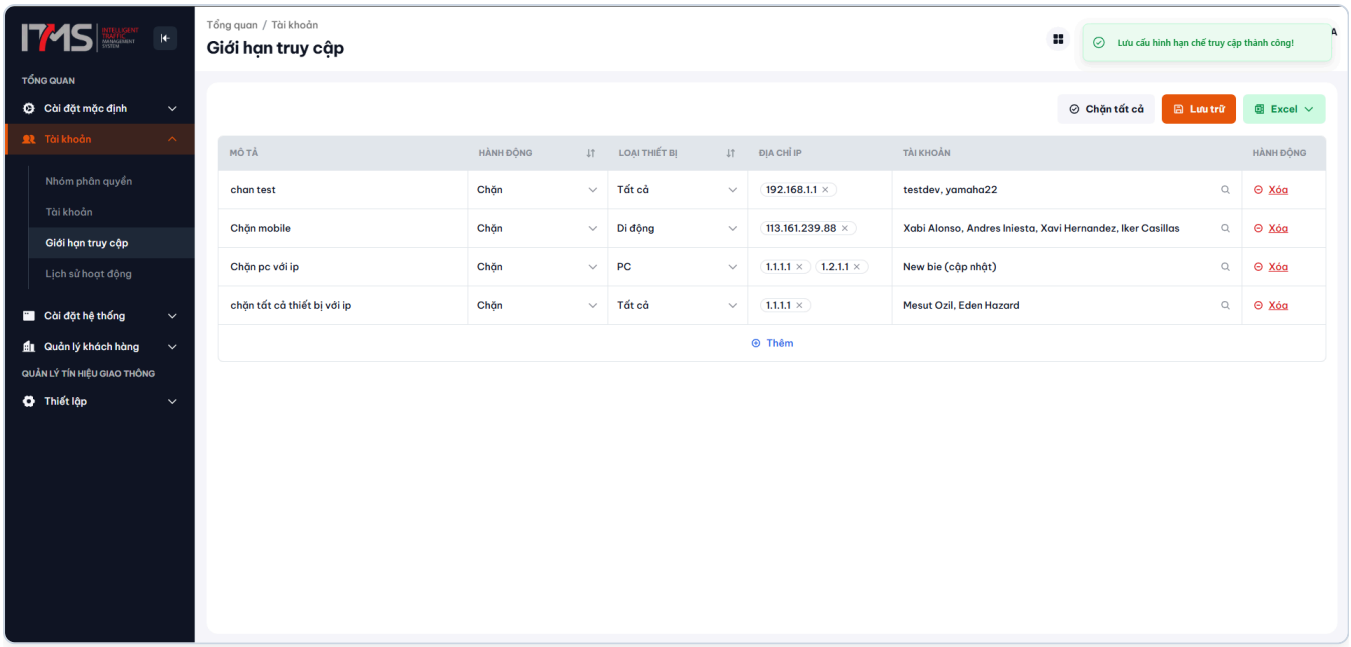


Hình 5.5: Đánh dấu tích chọn các tài khoản nhân sự cần gán quy tắc.

Quy tắc nghiệp vụ đối tượng áp dụng:
- **Áp dụng cho tài khoản cụ thể:** Tích chọn vào ô vuông trước tên các tài khoản cần áp dụng hạn chế truy cập $\rightarrow$ Nhấp nút **Áp dụng**.
- **Áp dụng cho tất cả tài khoản:** Bỏ chọn toàn bộ tài khoản (danh sách để trống) $\rightarrow$ Nhấp nút **Áp dụng**. Khi đó, quy tắc sẽ tự động có hiệu lực đối với mọi người dùng trong tổ chức.

5.6 Kiểm tra danh sách tài khoản đã gán

Sau khi nhấn Áp dụng, hộp thoại sẽ đóng lại và thông tin các tài khoản đã chọn lập tức hiển thị trên ô tương ứng:



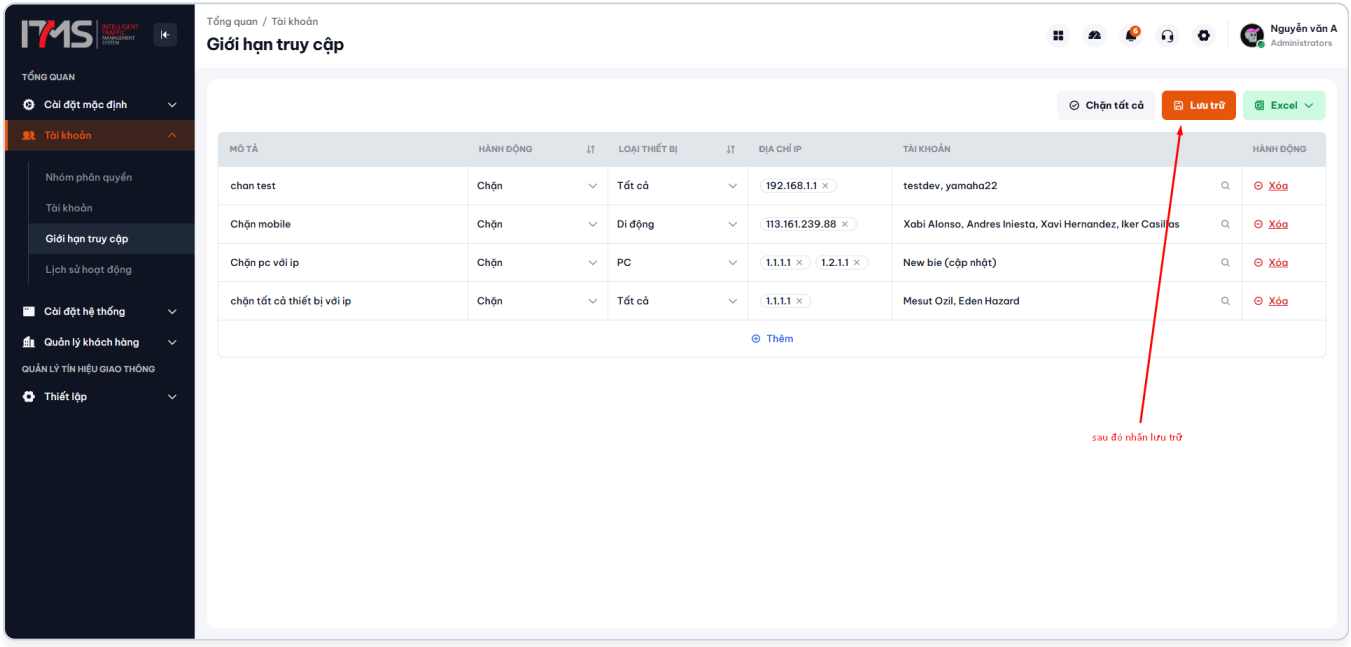
Hình 5.6: Cột danh sách tài khoản hiển thị đầy đủ tên các tài khoản đã gán.

- Người dùng có thể kiểm tra lại tên tài khoản đã được gán để đảm bảo không gán nhầm đối tượng.

5.7 Lưu trữ quy tắc mới vào hệ thống

Sau khi hoàn tất việc nhập các trường thông tin của quy tắc:

1. Di chuyển lên thanh công cụ tác vụ và nhấp vào nút **Lưu** (màu xanh dương):



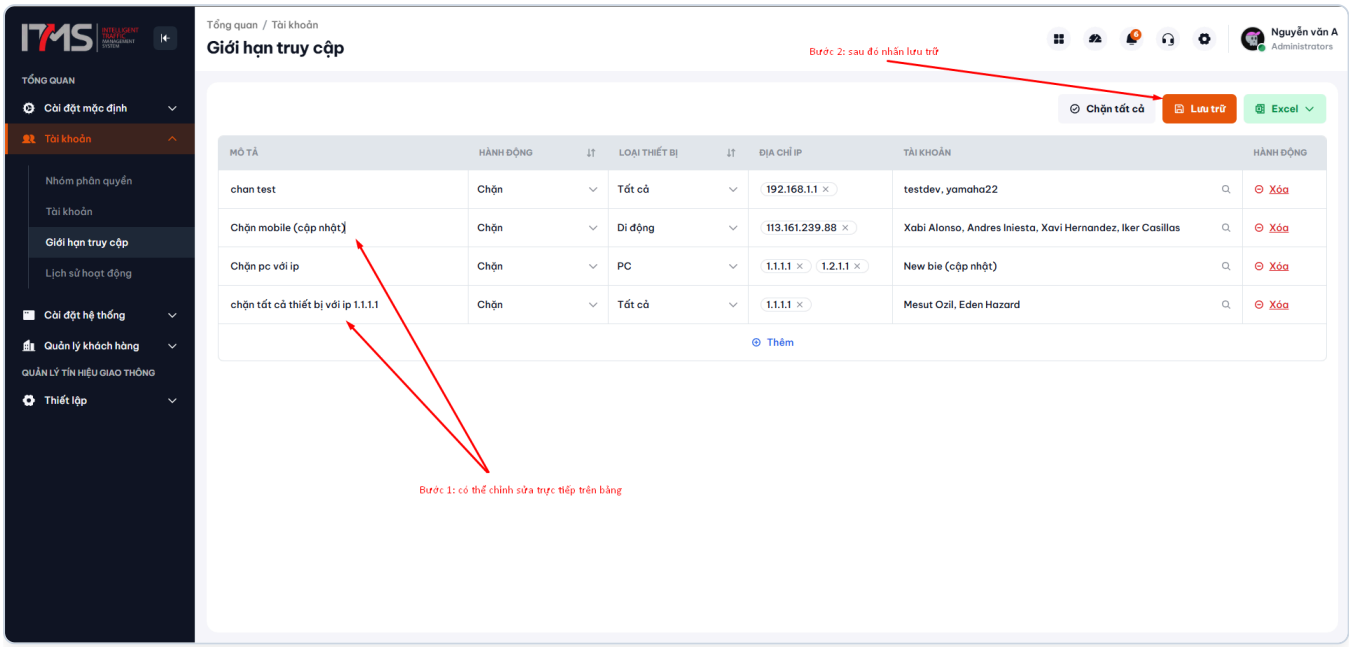
Hình 5.7: Thao tác nhấp nút "Lưu" để đồng bộ dữ liệu về máy chủ.

2. Hệ thống tự động kiểm tra cú pháp định dạng của tất cả các trường dữ liệu qua bộ xác thực (Zod Schema Validation).
3. Nếu hợp lệ, hệ thống sẽ gửi yêu cầu khởi tạo đến máy chủ và hiển thị thông báo thành công.

6. Hướng dẫn Chỉnh sửa quy tắc & Cơ chế theo dõi thay đổi

6.1 Chỉnh sửa dữ liệu trực tiếp trên bảng

Hệ thống ITMS cho phép chỉnh sửa tức thời bất kỳ trường dữ liệu nào mà không cần mở hộp thoại phức tạp:

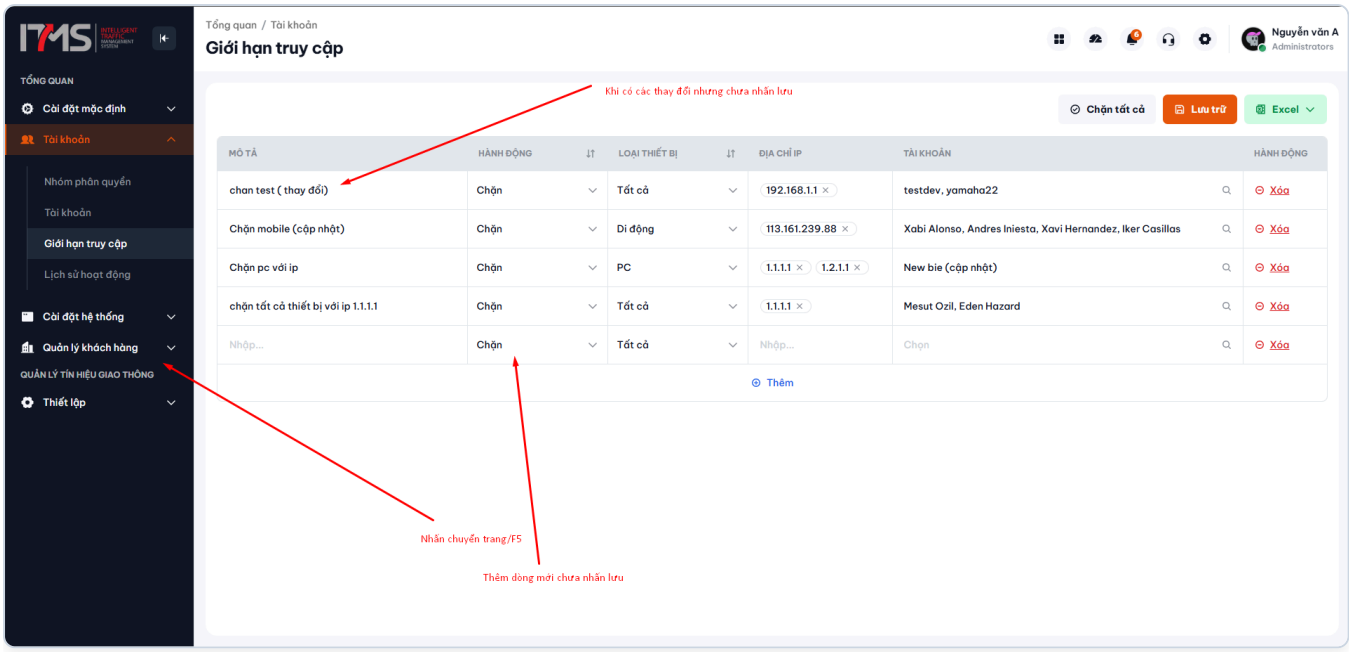


Hình 6.1: Nhấp chuột và sửa đổi trực tiếp Mô tả hoặc Địa chỉ IP trên từng dòng.

Các thao tác chỉnh sửa hỗ trợ:
- Sửa lại nội dung tại cột **Mô tả**.
- Chuyển đổi giữa hai hành động **Chặn** $\leftrightarrow$ **Cho phép**.
- Đổi loại thiết bị từ **PC** sang **Mobile** hoặc **Tất cả**.
- Nhập thêm hoặc bớt các địa chỉ IP trong cột **Danh sách địa chỉ IP**.
- Nhấp vào cột **Danh sách tài khoản** để chọn lại đối tượng người dùng áp dụng.

6.2 Nhận biết trạng thái dữ liệu chưa lưu (Dirty State Tracking)

Ngay khi người dùng thay đổi bất kỳ ký tự hoặc lựa chọn nào trên bảng, hệ thống sẽ tự động kích hoạt cơ chế theo dõi thay đổi:



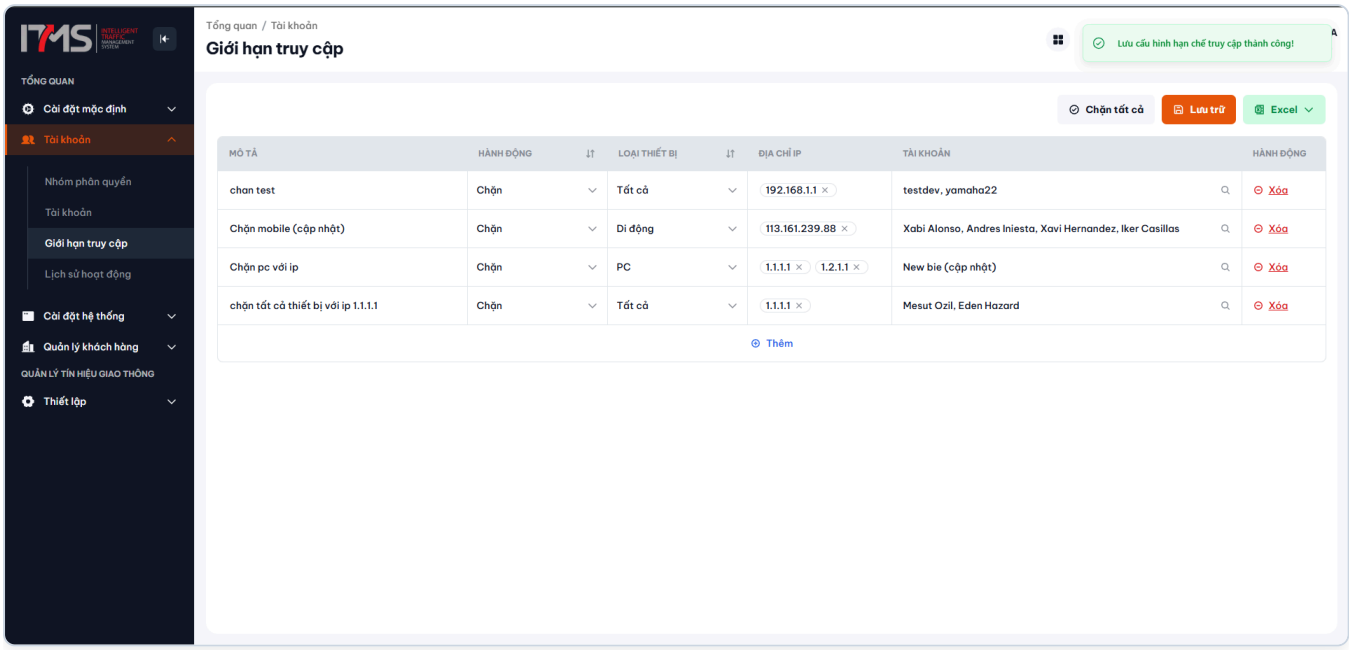
Hình 6.2: Dòng dữ liệu được hệ thống ghi nhận có thay đổi chưa lưu.

- Hệ thống tự động đánh dấu định danh của dòng bị thay đổi vào bộ nhớ đệm (Dirty Rule Tracking).
- Nút **Lưu** trên thanh công cụ sẽ sẵn sàng để người dùng thực thi đồng bộ dữ liệu.

6.3 Lưu cập nhật và đồng bộ dữ liệu máy chủ

Khi đã hoàn thành các chỉnh sửa trên một hoặc nhiều dòng:

1. Nhấp nút **Lưu** trên thanh công cụ.
2. Hệ thống chỉ tổng hợp và gửi đi các dòng thực sự có thay đổi lên máy chủ (Batch Update Optimization), giúp tiết kiệm lưu lượng mạng và tránh ghi đè dữ liệu không cần thiết:

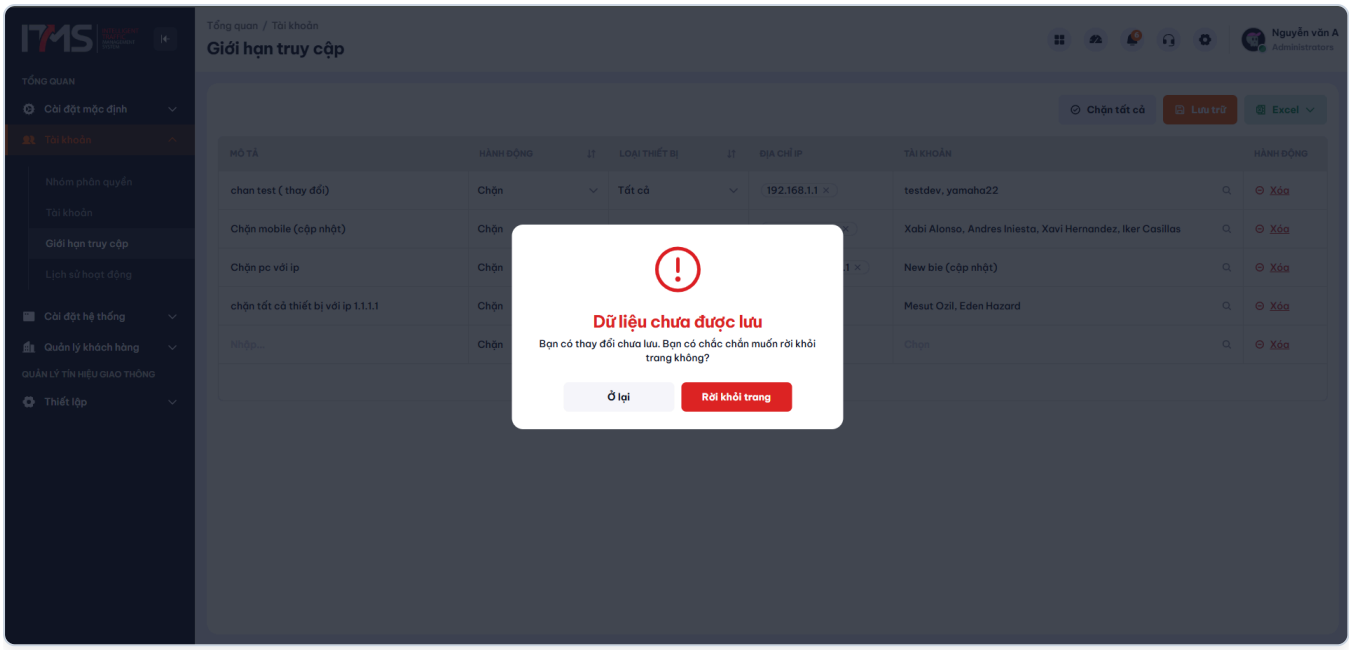


Hình 6.3: Thông báo lưu dữ liệu thành công xuất hiện ở góc màn hình.

- Hệ thống hiển thị thông báo: **"Cập nhật hạn chế truy cập thành công"**.
- Trạng thái chưa lưu được xóa sạch và bảng dữ liệu trở lại trạng thái đồng bộ hoàn toàn với máy chủ.

6.4 Cơ chế cảnh báo an toàn khi chuyển trang chưa lưu

Để bảo vệ người dùng không bị mất công sức nhập liệu khi vô tình chuyển sang trang khác, tải lại trang (F5) hoặc đóng thẻ trình duyệt:



Hình 6.4: Hộp thoại cảnh báo an toàn khi người dùng cố gắng rời khỏi trang có dữ liệu chưa lưu.

Hướng dẫn xử lý khi gặp cảnh báo:

- Nhấp **Hủy bỏ** (hoặc ở lại trang): Quay lại giao diện làm việc để bấm nút **Lưu** trước khi rời đi.
- Nhấp **Rời khỏi trang** (hoặc xác nhận chuyển trang): Chấp nhận hủy bỏ toàn bộ các chỉnh sửa vừa thực hiện mà không lưu lại.

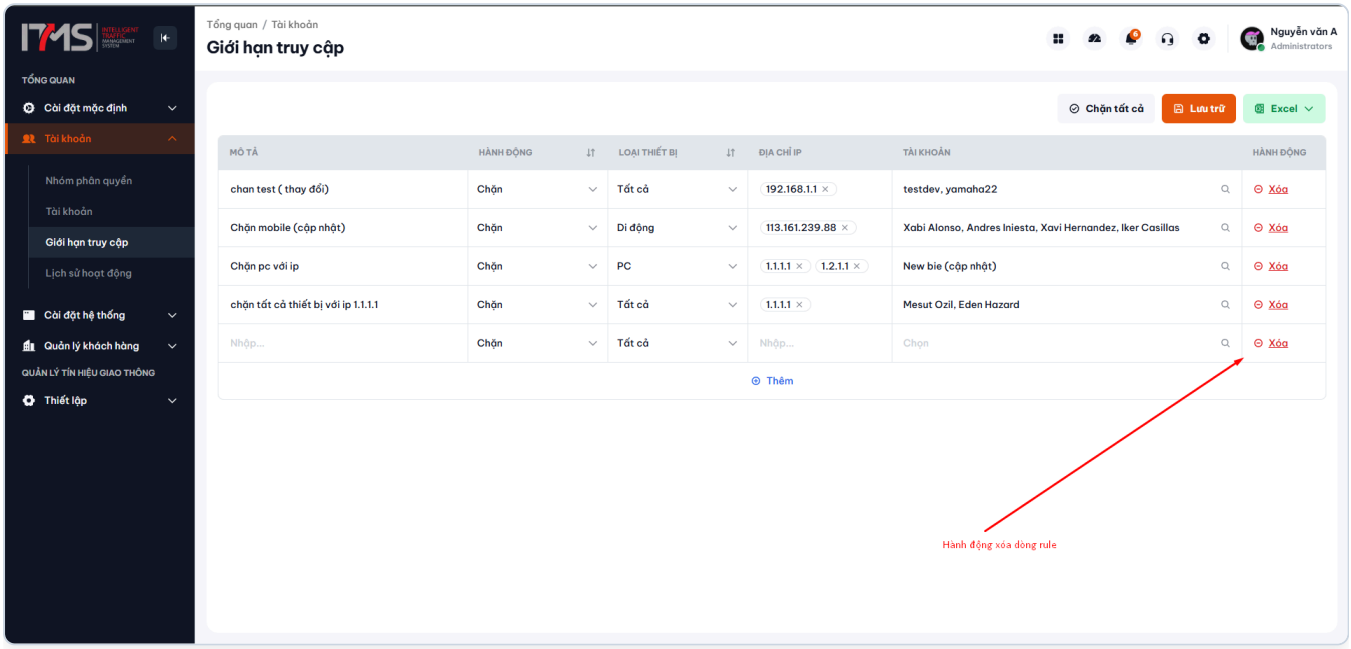
---

7. Hướng dẫn Xóa quy tắc truy cập

7.1 Kích hoạt thao tác xóa trên dòng quy tắc

Khi một quy tắc không còn phù hợp với chính sách an ninh hiện tại của đơn vị:

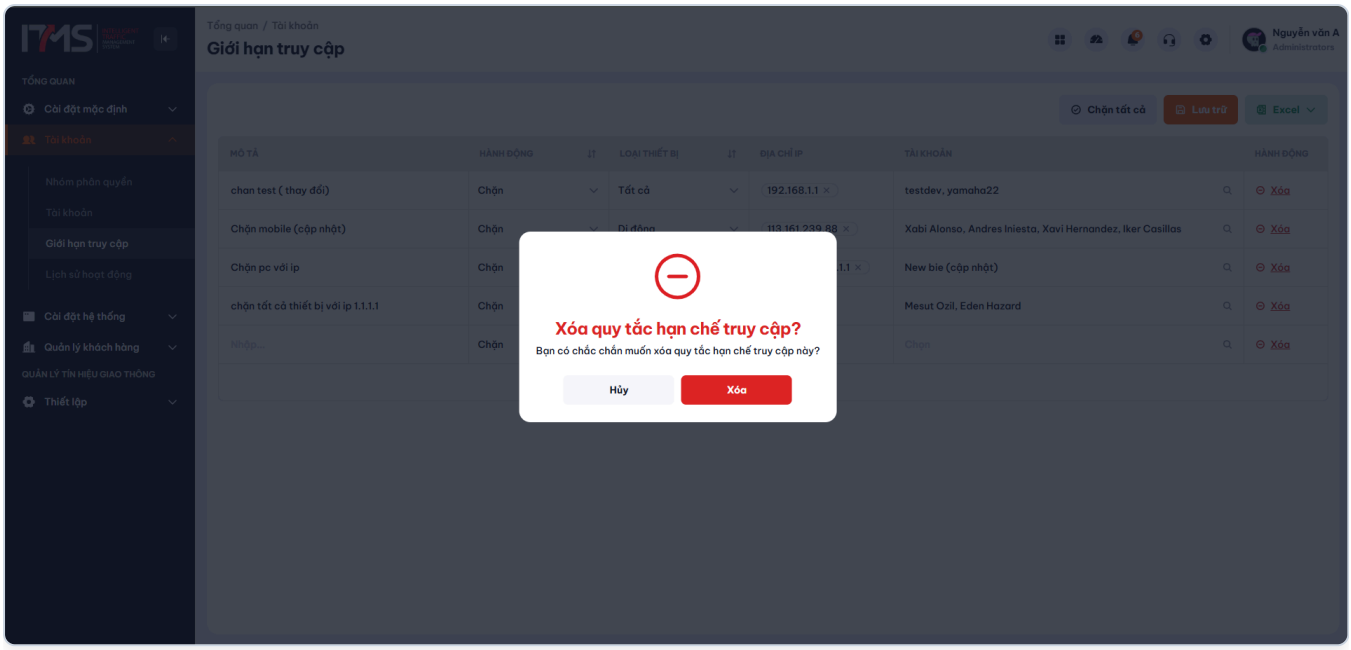
1. Rà soát và xác định đúng dòng quy tắc cần loại bỏ trên bảng.
2. Nhấp vào biểu tượng **Thùng rác màu đỏ** tại cột **Thao tác** ở cuối dòng tương ứng:



Hình 7.1: Biểu tượng xóa ở cột Thao tác trên dòng dữ liệu.

7.2 Xác nhận cảnh báo an toàn xóa vĩnh viễn

Hệ thống hiển thị hộp thoại xác nhận chuyên biệt để tránh tình trạng xóa nhầm:



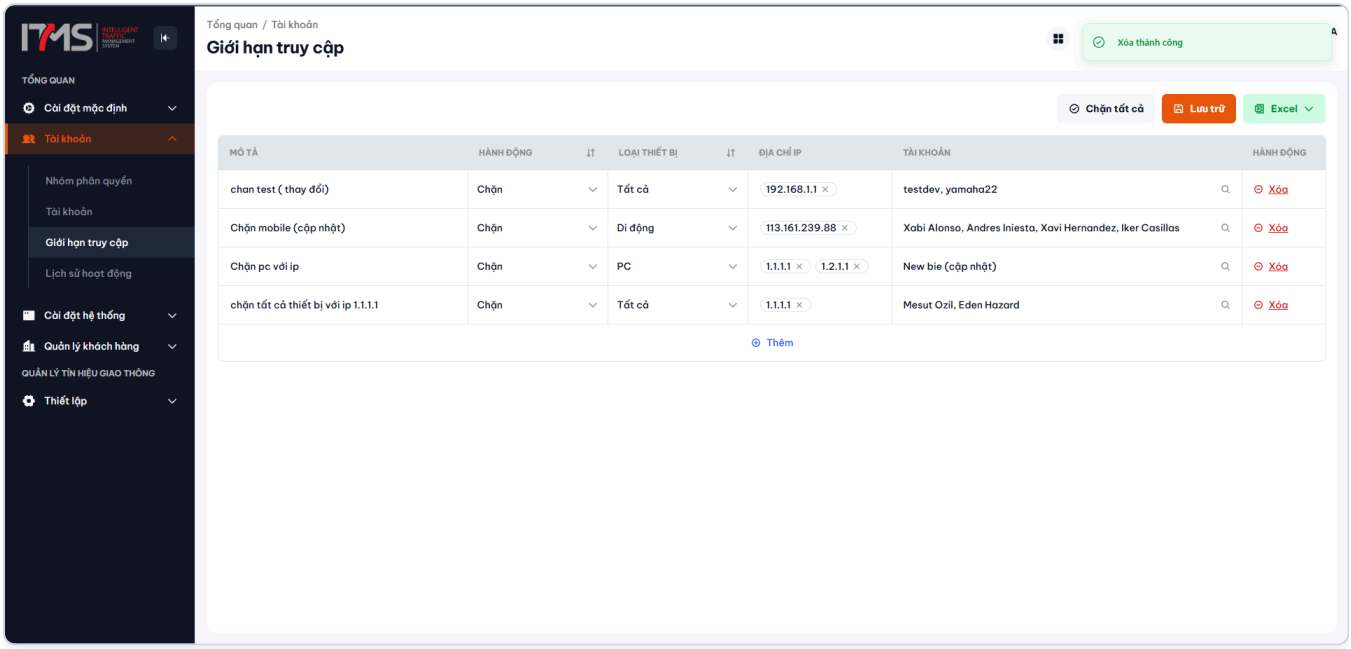
Hình 7.2: Hộp thoại cảnh báo an toàn xác nhận xóa quy tắc truy cập.

Thao tác xác nhận:

- Đọc kỹ thông báo xác nhận: "*Bạn có chắc chắn muốn xóa quy tắc hạn chế truy cập này không?*".
- Nhấp nút **Đồng ý** (nền đỏ) để thực hiện lệnh xóa.
- Nếu không muốn xóa, nhấp nút **Hủy bỏ** để đóng hộp thoại và bảo toàn quy tắc.

7.3 Ghi nhận kết quả xóa quy tắc khỏi hệ thống

Sau khi xác nhận:



Hình 7.3: Quy tắc bị loại bỏ khỏi bảng danh sách kèm thông báo thành công.

- Hệ thống gửi yêu cầu xóa đến máy chủ và hiển thị thông báo góc màn hình: **"Xóa quy tắc hạn chế truy cập thành công"**.
- Dòng quy tắc lập tức bị gỡ bỏ khỏi bảng dữ liệu và chính sách chặn/cho phép tương ứng sẽ hết hiệu lực ngay tức khắc.

---

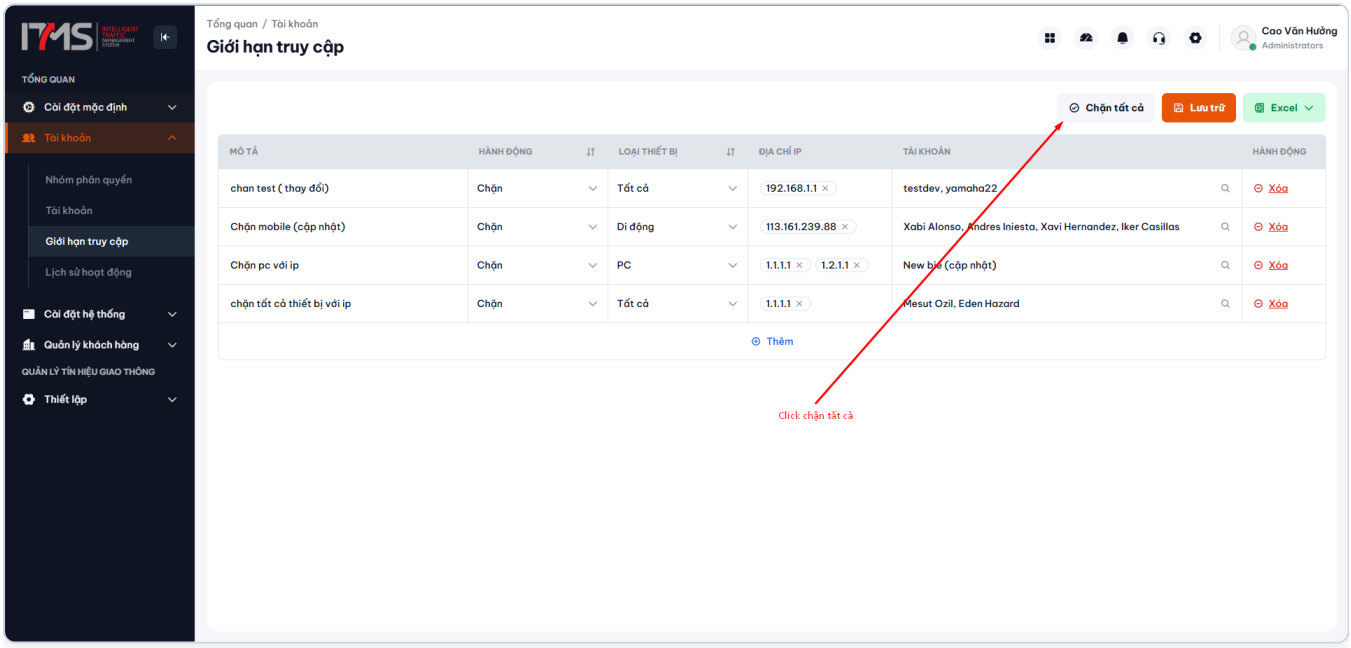
8. Hướng dẫn Quản lý chế độ "Chặn tất cả" (Reject All) cấp tổ chức

> **QUYỀN HẠN ĐẶC BIỆT:**
> Chức năng **Chặn tất cả / Hủy chặn tất cả** là công cụ an ninh cấp cao nhất của hệ thống, chỉ hiển thị và cho phép thao tác đối với người dùng giữ vai trò **Quản trị viên (Admin)** của tổ chức.

8.1 Kích hoạt chế độ Chặn tất cả

Khi phát hiện các dấu hiệu tấn công mạng bất thường hoặc cần tạm ngừng toàn bộ hoạt động truy cập của người dùng để nâng cấp hệ thống:

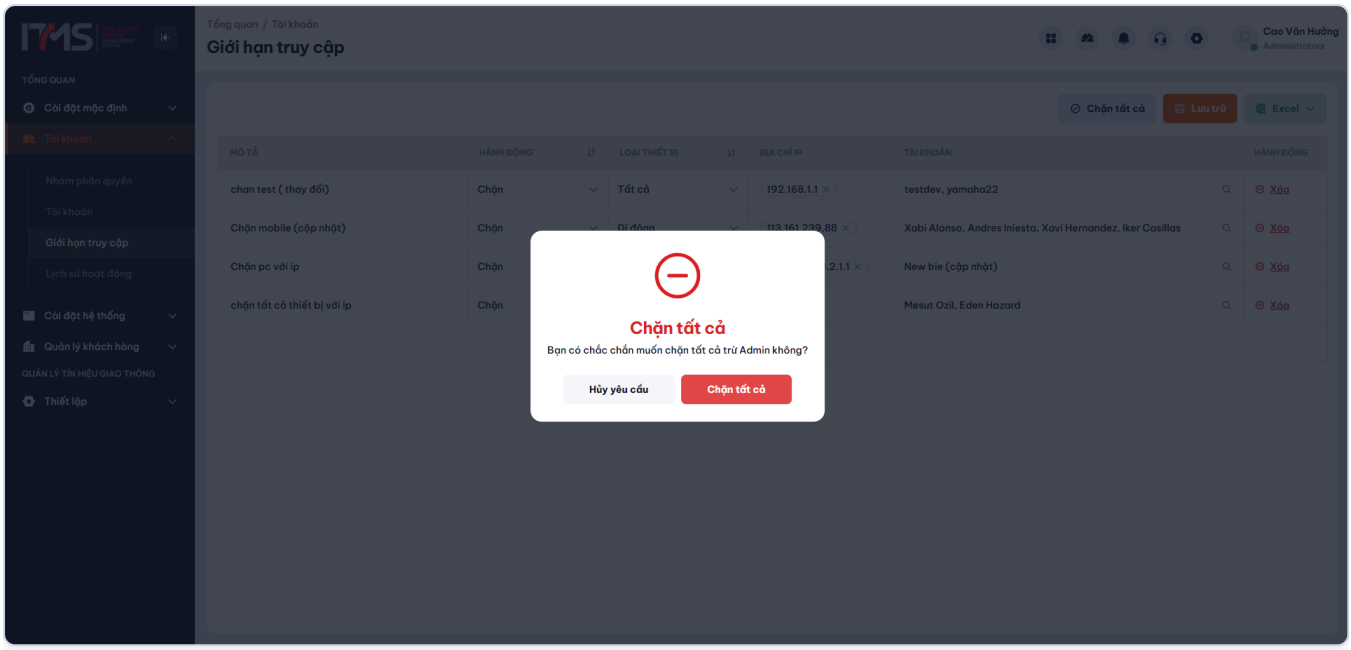
1. Quản trị viên nhấp vào nút **Từ chối tất cả** trên thanh công cụ tác vụ:



Hình 8.1: Vị trí nút "Từ chối tất cả" trên thanh công cụ của Quản trị viên.

8.2 Xác nhận cảnh báo bảo mật cấp tổ chức

Hệ thống kích hoạt hộp thoại cảnh báo cấp cao với giao diện màu đỏ cảnh báo nguy cơ:



Hình 8.2: Hộp thoại cảnh báo an toàn màu đỏ xác nhận kích hoạt Từ chối tất cả.

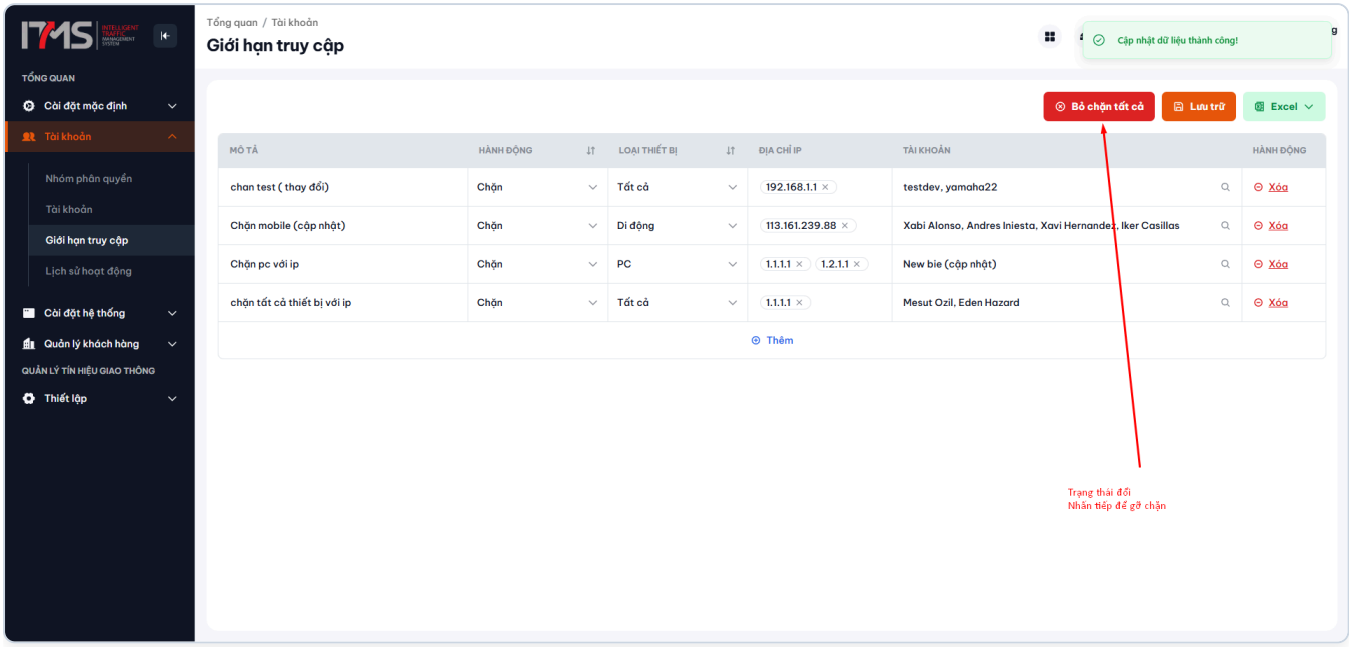
Nội dung cảnh báo quan trọng:

- Khi kích hoạt, toàn bộ người dùng thông thường trong tổ chức sẽ bị từ chối truy cập ngay lập tức khi đăng nhập vào hệ thống, bất kể quy tắc riêng lẻ của họ là gì.
- Chỉ tài khoản Quản trị viên cấp cao mới duy trì được phiên làm việc để xử lý sự cố.
- Nhấp nút **Đồng ý** (nền đỏ) để chính thức kích hoạt chế độ phong tỏa an ninh.

8.3 Hủy kích hoạt chế độ Chặn tất cả

Sau khi sự cố an ninh đã được khắc phục hoàn toàn hoặc hoàn tất đợt bảo trì, Quản trị viên cần khôi phục lại quyền truy cập bình thường cho toàn bộ nhân sự:

1. Trên thanh công cụ, nút chức năng lúc này sẽ hiển thị là **Hủy từ chối tất cả**:

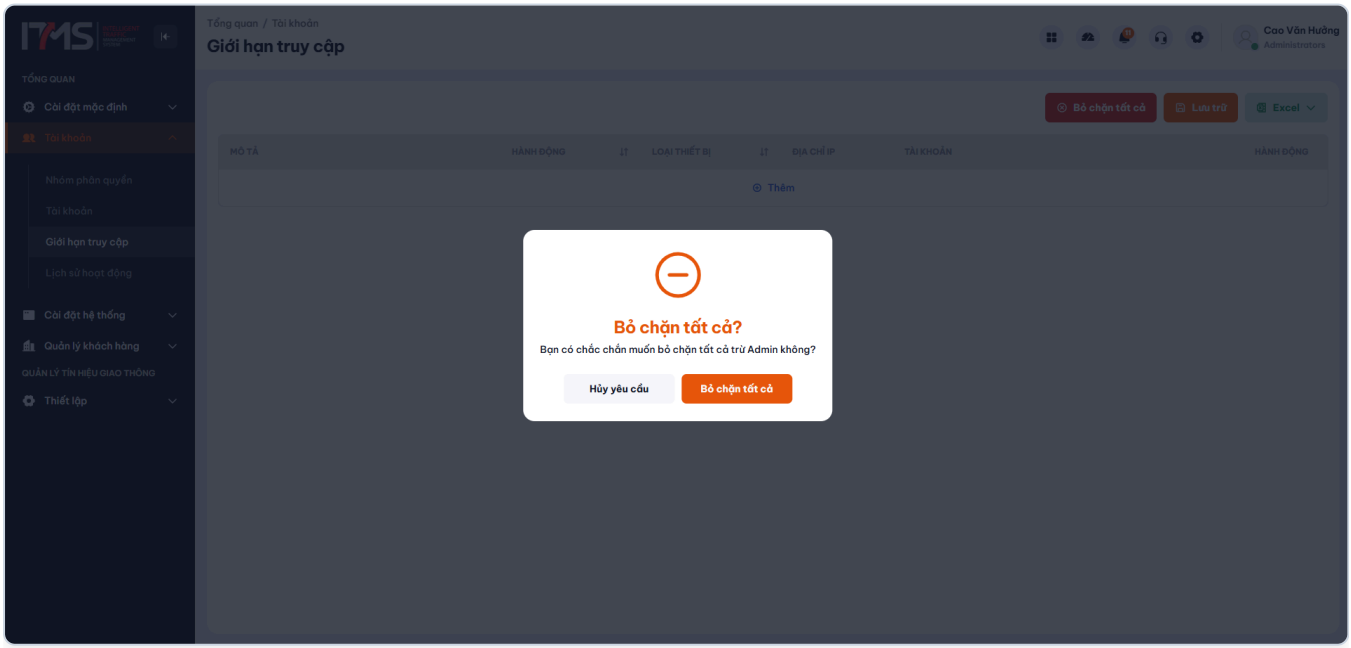


Hình 8.3: Vị trí nút "Hủy từ chối tất cả" khi hệ thống đang ở chế độ phong tỏa.

- Nhấp chọn nút **Hủy từ chối tất cả**.

8.4 Xác nhận khôi phục kết nối an toàn

Hệ thống hiển thị hộp thoại xác nhận khôi phục trạng thái với giao diện màu xanh an toàn:



Hình 8.4: Hộp thoại xác nhận màu xanh khôi phục lại trạng thái truy cập bình thường.

- Nhấp chọn nút **Đồng ý** để hoàn tất việc dỡ bỏ lệnh phong tỏa.
- Kể từ thời điểm này, mọi tài khoản nhân sự trong tổ chức sẽ được phép đăng nhập lại bình thường theo đúng các quy tắc kiểm soát IP thông thường đã thiết lập.

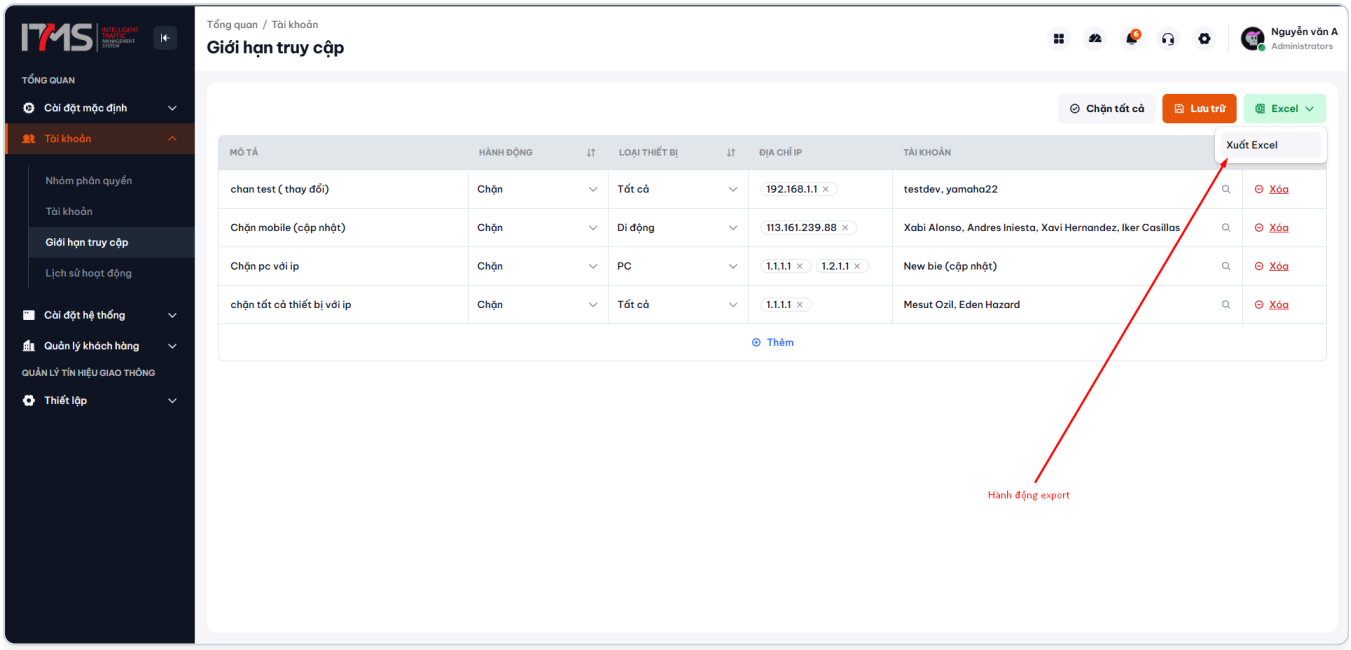
---

9. Hướng dẫn Xuất danh sách quy tắc ra tệp Excel

9.1 Khởi chạy tính năng Xuất Excel

Để phục vụ công tác rà soát chính sách bảo mật định kỳ hoặc lập báo cáo gửi Ban lãnh đạo:

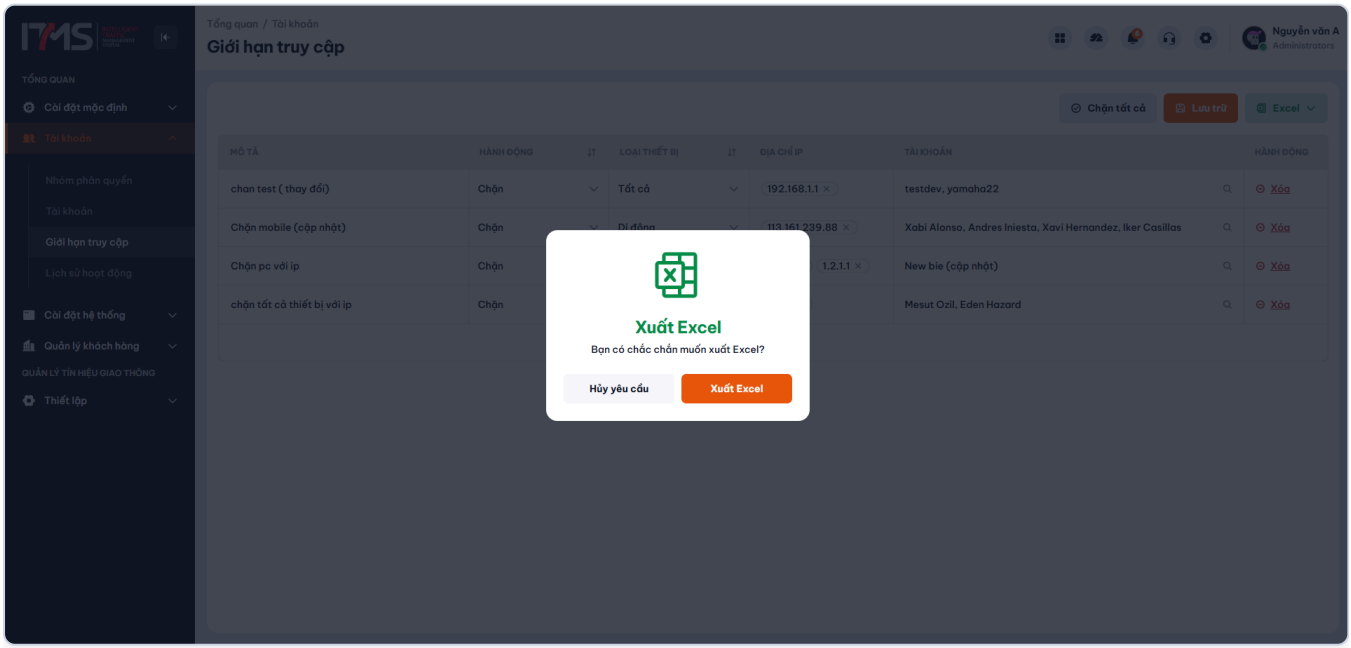
1. Trên thanh công cụ tác vụ, nhấp vào nút **Xuất Excel** (màu xanh lá):



Hình 9.1: Nút "Xuất Excel" trên thanh công cụ tác vụ.

9.2 Xác nhận trích xuất danh sách

Hộp thoại xác nhận xuất dữ liệu xuất hiện:

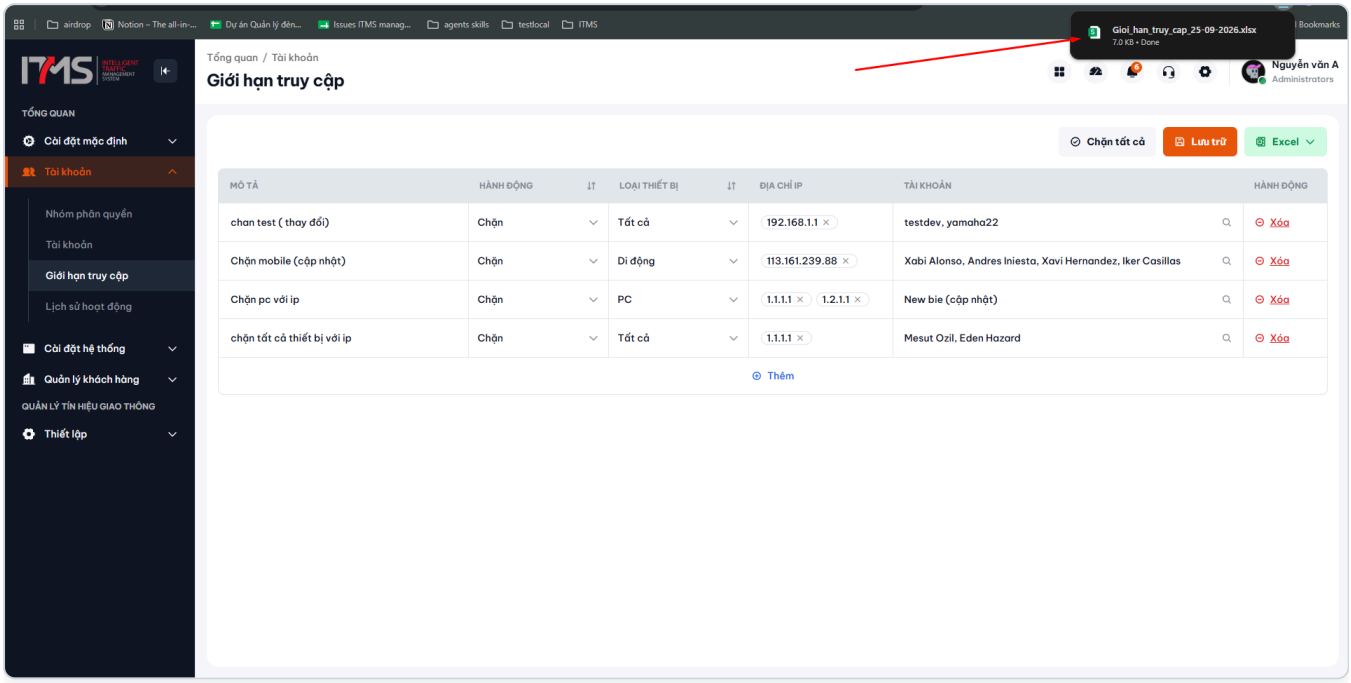


Hình 9.2: Hộp thoại xác nhận tải dữ liệu bảng tính.

- Người dùng kiểm tra thông tin và nhấp nút **Đồng ý** để yêu cầu hệ thống khởi tạo tệp bảng tính.

9.3 Tải xuống tệp dữ liệu tự động

Ngay sau khi máy chủ đóng gói dữ liệu xong, trình duyệt web sẽ tự động kích hoạt tiến trình tải xuống tệp tin:

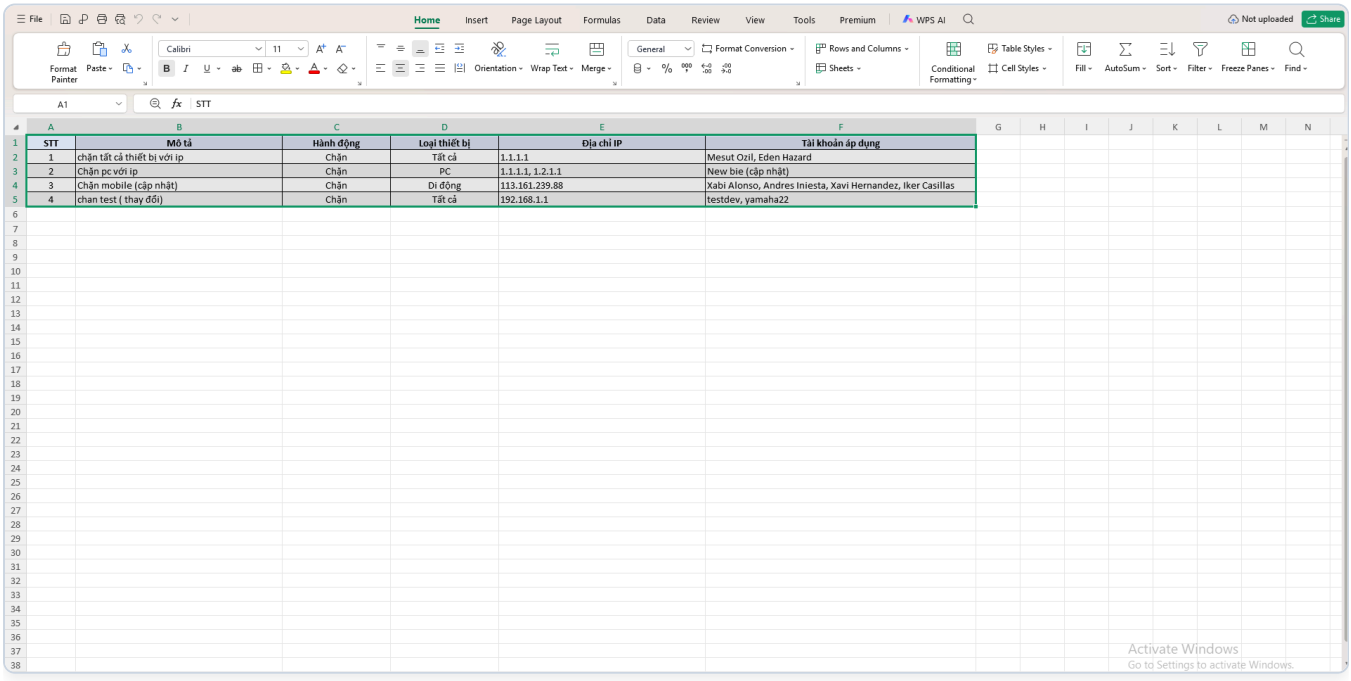


Hình 9.3: Trình duyệt tự động lưu tệp bảng tính vào thư mục tải về của máy tính.

- Người dùng có thể theo dõi tiến trình tải xuống tại thanh thông báo của trình duyệt web.

9.4 Cấu trúc bảng tính báo cáo kết quả

Tệp bảng tính kết xuất có định dạng chuẩn Microsoft Excel (`.xlsx`), sẵn sàng mở và in ấn:



STT	Mô tả	Hành động	Loại thiết bị	Địa chỉ IP	Tài khoản áp dụng
1	chặn tất cả thiết bị với ip	Chặn	Tất cả	1.1.1.1	Mesut Ozil, Eden Hazard
2	Chặn pc với ip	Chặn	PC	1.1.1.1, 1.2.1.1	New bie (cập nhật)
3	Chặn mobile (cập nhật)	Chặn	Di động	113.161.239.88	Xabi Alonso, Andres Iniesta, Xavi Hernandez, Iker Casillas
4	chan test (thay đổi)	Chặn	Tất cả	192.168.1.1	testdev, yamaha22

Hình 9.4: Cấu trúc chi tiết danh sách quy tắc trong tệp bảng tính Excel.

Đặc điểm bảng tính xuất khẩu:

- Bảng tính thể hiện đầy đủ các trường: Thứ tự (STT), Mô tả quy tắc, Hành động (Chặn / Cho phép), Loại thiết bị áp dụng, Danh sách địa chỉ IP được kiểm soát và Danh sách tài khoản người dùng áp dụng tương ứng.

---

10. Xử lý sự cố & Bảng câu hỏi thường gặp (FAQ)

1. Tại sao tôi không nhìn thấy nút "Từ chối tất cả" trên thanh công cụ?

Giải thích: Nút chức năng "Từ chối tất cả" là công cụ quản trị an ninh khẩn cấp cấp tổ chức. Hệ thống chỉ hiển thị nút này cho tài khoản có quyền Quản trị viên cấp cao (`Admin`). Người dùng thông thường hoặc các tài khoản nhân sự kỹ thuật thông thường sẽ không nhìn thấy nút này để tránh các nguy cơ thao tác làm gián đoạn hệ thống.

2. Định dạng địa chỉ IP nào được hệ thống chấp nhận?

Giải thích: Hệ thống chấp nhận các địa chỉ IPv4 tiêu chuẩn dạng 4 nhóm số nguyên từ `0` đến `255` ngăn cách bởi dấu chấm (ví dụ: `192.168.1.100` , `14.232.208.55`). Nếu một quy tắc áp dụng cho nhiều IP, các địa chỉ phải được ngăn cách rõ ràng bằng dấu phẩy. Hệ thống sẽ báo viền đỏ cảnh báo nếu địa chỉ IP không đúng định dạng.

3. Nếu cột "Danh sách tài khoản" bị để trống thì quy tắc có hiệu lực với ai?

Giải thích: Khi cột Danh sách tài khoản để trống (không chọn tài khoản cụ thể nào), hệ thống mặc định hiểu rằng quy tắc này được áp dụng cho **toàn bộ tài khoản người dùng** thuộc tổ chức.

4. Tại sao khi tôi nhấn "+ Thêm" thì hệ thống lại tự động lưu các dòng trước đó?

Giải thích: Đây là cơ chế bảo vệ dữ liệu tự động thông minh (Auto-save on Add). Nhằm ngăn ngừa việc người dùng quên nhấn nút Lưu khiến dữ liệu đang nhập bị thất lạc, hệ thống sẽ tự động xác thực và gửi lưu các dòng cũ trước khi chèn thêm một dòng mới vào bảng.

---

11. Kênh hỗ trợ kỹ thuật

Trong quá trình quản trị chính sách bảo mật và hạn chế truy cập trên hệ thống ITMS, nếu Quản trị viên gặp sự cố kỹ thuật hoặc nghi vấn an ninh mạng, xin vui lòng liên hệ ngay:

- **Bộ phận Hỗ trợ An ninh & Vận hành Hệ thống ITMS**
- **Đường dây nóng hỗ trợ khẩn cấp 24/7:** `1900 xxxx`
- **Hòm thư điện tử tiếp nhận sự cố an toàn thông tin:** `security-itms@domain.vn`
- **Cổng thông tin hỗ trợ kỹ thuật:** `https://support.itms-system.vn`

PHỤ LỤC TÀI LIỆU

Phụ lục A: Bảng mã trạng thái & Thông điệp phản hồi hệ thống

Bảng tổng hợp các mã phản hồi từ máy chủ khi thao tác trong phân hệ Quản lý Hạn chế truy cập:

Mã phản hồi (HTTP/Status)	Thông báo hiển thị trên giao diện	Nguyên nhân nghiệp vụ	Hướng xử lý đề xuất
200 OK / 201 Created	*Lưu hạn chế truy cập thành công! / Xóa quy tắc thành công!*	Thao tác ghi nhận chính sách truy cập thành công trên hệ thống.	Tiếp tục các tác vụ cấu hình an ninh bình thường.
400 Bad Request	*Dữ liệu quy tắc không hợp lệ*	Bỏ trống Mô tả hoặc địa chỉ IP không đúng định dạng IPv4 chuẩn.	Kiểm tra lại các ô có viền đỏ cảnh báo và sửa đúng định dạng.
401 Unauthorized	*Phiên làm việc đã hết hạn*	Phiên đăng nhập của Quản trị viên đã quá hạn trong quá trình thao tác.	Đăng nhập lại vào hệ thống và thực hiện lại thao tác lưu.
403 Forbidden	*Truy cập bị từ chối (Access Denied)*	Tài khoản không có đủ quyền hạn chỉnh sửa hoặc không phải Admin (với thao tác Từ chối tất cả).	Liên hệ Quản trị viên cấp cao để được cấp quyền tương ứng.
409 Conflict	*Quy tắc xung đột dữ liệu*	Địa chỉ IP hoặc cấu hình trùng lặp với một chính sách khác đang có hiệu lực.	Rà soát lại dải địa chỉ IP và các tài khoản đã chọn.
500 Server Error	*Lỗi hệ thống trong quá trình xử lý*	Sự cố máy chủ dịch vụ xác thực hoặc gián đoạn kết nối cơ sở dữ liệu.	Chờ giây lát và thử lại hoặc liên hệ ngay bộ phận kỹ thuật ITMS.

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

Nhằm nâng cao năng suất thao tác cấu hình an ninh cho Quản trị viên:

Phím tắt / Thao tác	Khu vực tác động	Chức năng chi tiết
`Enter`	Ô tìm kiếm tài khoản	Kích hoạt tìm kiếm tài khoản ngay lập tức với từ khóa vừa nhập.
`Esc` (Escape)	Hộp thoại Chọn tài khoản / Hộp thoại Cảnh báo	Đóng nhanh hộp thoại đang mở mà không lưu các thao tác vừa chọn.
`Tab`	Trên bảng dữ liệu trực tiếp	Di chuyển con trỏ tuần tự qua các ô nhập liệu (Mô tả $\rightarrow$ Hành động $\rightarrow$ Loại thiết bị $\rightarrow$ IP).
Nhấp đúp chuột	Ô nhập liệu trên bảng	Kích hoạt chế độ chỉnh sửa văn bản ngay lập tức.
Nhấp biểu tượng thùng rác	Cột Thao tác	Mở hộp thoại xác nhận xóa quy tắc truy cập tương ứng.

Phụ lục C: Quy chuẩn cấu trúc dữ liệu địa chỉ IP & Chính sách an ninh mạng

1. Quy chuẩn cấu trúc dữ liệu thực thể quy tắc truy cập

Thuộc tính dữ liệu	Định dạng kỹ thuật	Tính chất	Ý nghĩa nghiệp vụ
Mô tả (`description`)	Chuỗi ký tự, tối đa 255 ký tự	Bắt buộc	Thể hiện mục đích, lý do ban hành quy tắc an ninh.
Hành động (`action`)	Chuỗi ký tự: `accept` hoặc `reject`	Bắt buộc	Xác định cho phép hay ngăn chặn kết nối đối với dải IP tương ứng.
Loại thiết bị (`device_type`)	Chuỗi ký tự: `pc`, `mobile`, `all`	Bắt buộc	Phân loại môi trường máy trạm kết nối vào hệ thống ITMS.
Địa chỉ IP (`ip_address`)	Chuỗi địa chỉ IPv4 phân tách bằng dấu phẩy	Bắt buộc	Danh sách các địa chỉ IP bị tác động bởi chính sách kiểm soát.
Tài khoản áp dụng (`account_ids`)	Danh sách mã định danh tài khoản (`number[]`)	Tùy chọn	Nếu để trống, quy tắc có hiệu lực cho toàn bộ nhân sự của tổ chức.
Chặn tất cả (`reject_all`)	Giá trị nhị phân: `0` (Tắt), `1` (Bật)	Toàn cục	Chế độ phong tỏa toàn diện áp dụng cấp tổ chức của Quản trị viên.

---

2. Nguyên tắc hoạt động của chính sách kiểm soát truy cập

Hệ thống ITMS vận hành cơ chế kiểm soát truy cập theo các nguyên tắc an ninh tuần tự:

1. **Ưu tiên chế độ Chặn tất cả (Reject All Priority):** Nếu trạng thái `reject_all = 1` được kích hoạt ở cấp tổ chức, hệ thống lập tức từ chối mọi yêu cầu đăng nhập từ tài khoản người dùng thông thường, bỏ qua toàn bộ các quy tắc con bên dưới.
2. **Quy tắc chặn cụ thể (Denylist First):** Nếu địa chỉ IP hoặc tài khoản của người dùng khớp với một quy tắc có hành động là **Chặn (Reject)**, kết nối sẽ bị hủy bỏ ngay lập tức.
3. **Quy tắc cho phép (Allowlist):** Nếu tổ chức áp dụng chính sách chỉ cho phép truy cập từ các địa chỉ IP tin cậy (Hành động: **Cho phép - Accept**), mọi kết nối xuất phát từ các địa chỉ IP ngoài danh sách sẽ bị từ chối truy cập.

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	25/09/2026	ITMS Frontend Team	Khởi tạo tài liệu Hướng dẫn sử dụng tính năng Quản lý Hạn chế truy cập (Access Restrictions). Thiết lập Trang bìa chuẩn in ấn A4, Mục lục riêng biệt 1 trang, tích hợp trọn vẹn chuỗi 23 ảnh chụp màn hình thực tế bao phủ đầy đủ 6 nhóm nghiệp vụ (Xem danh sách trực tiếp - Thêm mới & Tự động lưu - Sửa trực tiếp & Theo dõi Dirty State - Xóa quy tắc an toàn - Chế độ Chặn tất cả khẩn cấp - Xuất Excel), chuẩn hóa ngôn ngữ người dùng thuần túy (loại bỏ hoàn toàn code permissions) và tích hợp hệ thống 4 Phụ lục A-D theo quy chuẩn xuất bản ITMS.