ĐẠI HỌC DUY TÂN
BAN ĐÀO TẠO

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập – Tự Do – Hạnh Phúc

Đà Nẵng, ngày 16 tháng 11 năm 2026

THÔNG BÁO

(Về việc xác thực danh tính trước khi sử dụng hệ thống AMS)

Kính gửi:

- Lãnh đạo các Trường;
- Trưởng các Khoa;
- Tổ trưởng các Bộ môn;
- Các cá nhân được phân quyền sử dụng hệ thống AMS.

Nhằm đảm bảo an toàn thông tin, tăng cường kiểm soát truy cập và đảm bảo hoạt động sử dụng hệ thống AMS được thông suốt. Ban Đào Tạo thông báo đến Quý Thầy/Cô được phân quyền sử dụng hệ thống AMS về việc **thực hiện xác thực danh tính trước khi truy cập hệ thống**, cụ thể như sau:

1. Trường hợp sử dụng máy tính trong mạng LAN của Trường

- Kết nối máy tính vào mạng LAN của Trường.
- Mở trình duyệt và truy cập địa chỉ: https://auth.duytan.edu.vn
- Đăng nhập bằng tài khoản email cá nhân (###@dtu.edu.vn, ###@duytan.edu.vn) do Trường cấp và hoàn tất các bước xác thực theo hướng dẫn.
- Sau khi xác thực thành công (hệ thống thông báo **User Authenticated**), tắt trình duyệt, mở phần mềm AMS và đăng nhập bằng tài khoản AMS đã được cấp.

2. Trường hợp sử dụng máy tính bên ngoài mạng LAN của Trường

Người dùng cần kết nối VPN thông qua **phần mềm GlobalProtect** trước khi truy cập AMS. Cụ thể:

- Đối với email có tên miền **@dtu.edu.vn**: sử dụng Portal **vpn-dtu.dtu.edu.vn**.
- Đối với email có tên miền **@duytan.edu.vn**: sử dụng Portal **vpn-duytan.duytan.edu.vn**.
- Đăng nhập bằng email tương ứng, hoàn tất xác thực bổ sung (MFA) nếu được yêu cầu.
- Chỉ mở AMS sau khi GlobalProtect hiển thị trạng thái **Connected**. Duy trì kết nối VPN trong suốt thời gian sử dụng AMS.

3. Một số lưu ý

- Người dùng phải sử dụng tài khoản email cá nhân do Trường cấp và đã được đăng ký phục vụ xác thực.
- Việc xác thực danh tính hoặc kết nối VPN thành công không đồng nghĩa với việc được cấp thêm quyền sử dụng AMS. Người dùng chỉ được truy cập các chức năng theo quyền đã được phê duyệt.
- Khi gặp sự cố trong quá trình xác thực hoặc truy cập AMS, vui lòng ghi nhận thông báo lỗi, thời điểm xảy ra và gửi thông tin đến Bộ phận Công nghệ thông tin để được hỗ trợ (**bandaotao@duytan.edu.vn** và **cit@duytan.edu.vn**).
- Không cung cấp mật khẩu, mã OTP hoặc mã khôi phục tài khoản cho bất kỳ cá nhân nào.

4. Tài liệu hướng dẫn

Ban Đào Tạo gửi kèm tài liệu ***Hướng dẫn xác thực danh tính trước khi sử dụng AMS*** (*cập nhật ngày 14/11/2026, do Trung tâm CIT phát hành*), trong đó có hướng dẫn chi tiết cách xác thực qua mạng LAN, cài đặt và kết nối VPN bằng GlobalProtect, kiểm tra kết nối và xử lý các sự cố thường gặp.

Kính đề nghị Quý Thầy/Cô phối hợp thực hiện để đảm bảo việc truy cập và sử dụng hệ thống AMS được thông suốt, an toàn.

Trân trọng thông báo./.

Ban Đào Tạo

(đã ký)

Nguyễn Đăng Quang Huy

HƯỚNG DẪN XÁC THỰC DANH TÍNH VÀ KẾT NỐI TRƯỚC KHI SỬ DỤNG AMS

I. MỤC ĐÍCH VÀ PHẠM VI ÁP DỤNG

Trước khi sử dụng phần mềm AMS, người dùng cần thực hiện xác thực danh tính để bảo đảm máy tính được phép truy cập vào hệ thống mạng nội bộ của Trường.

Tùy theo vị trí và phương thức kết nối Internet, người dùng ***thực hiện xác thực theo một trong hai phương thức sau***:

- **Phương thức 1 – Kết nối mạng LAN của Trường (người dùng đang sử dụng mạng có Dây và Không dậy tại các cơ sở của Đại Học Duy Tân):** Truy cập trang xác thực **https://auth.duytan.edu.vn** và đăng nhập bằng tài khoản cá nhân được Trường cấp.
- **Phương thức 2 – Kết nối bên ngoài mạng LAN (người dùng đang ở ngoài các cơ sở của Đại Học Duy Tân):** Sử dụng phần mềm **GlobalProtect để kết nối VPN vào hệ thống mạng của Trường**.

Sau khi hoàn tất xác thực hoặc kết nối VPN thành công, người dùng mở phần mềm AMS và đăng nhập bằng tài khoản AMS đã được cấp.

Lưu ý: Việc xác thực danh tính hoặc kết nối VPN thành công không đồng nghĩa với việc tài khoản đã được cấp quyền sử dụng AMS. **Người dùng phải có tài khoản AMS và quyền truy cập phù hợp với chức năng, nhiệm vụ được giao**.

II. CHUẨN BỊ TRƯỚC KHI THỰC HIỆN

Người sử dụng cần chuẩn bị:

- Tài khoản cá nhân theo email do Trường cấp.
- Đã đăng ký email và được cấp quyền sử dụng AMS theo quy định.
- Máy tính đã cài đặt phần mềm AMS.
- Có kết nối Internet hoặc mạng LAN ổn định.
- Trường hợp sử dụng VPN: máy tính đã cài đặt phần mềm GlobalProtect.
- Chuẩn bị thiết bị hoặc ứng dụng xác thực bổ sung (MFA) nếu tài khoản được yêu cầu.

Lưu ý: Các hình ảnh trong tài liệu chỉ nhằm minh họa trình tự thao tác, không phải ảnh chụp trực tiếp từ hệ thống. Giao diện, tên nút và bố cục thực tế có thể thay đổi tùy theo phiên bản phần mềm và cấu hình hệ thống.

III. PHƯƠNG THỨC 1: XÁC THỰC KHI SỬ DỤNG MẠNG LAN CỦA TRƯỜNG

Áp dụng đối với máy tính đang kết nối trực tiếp vào hệ thống mạng LAN của Đại học Duy Tân.

Bước 1. Kết nối mạng LAN

- Kiểm tra cáp mạng và bảo đảm máy tính đang kết nối vào hệ thống mạng LAN của Trường.

Bước 2. Truy cập trang xác thực

- Mở trình duyệt Chrome, Microsoft Edge hoặc Firefox.
- Nhập địa chỉ sau vào thanh địa chỉ:
  - **https://auth.duytan.edu.vn**
  - Nhấn **Enter** để truy cập trang xác thực.

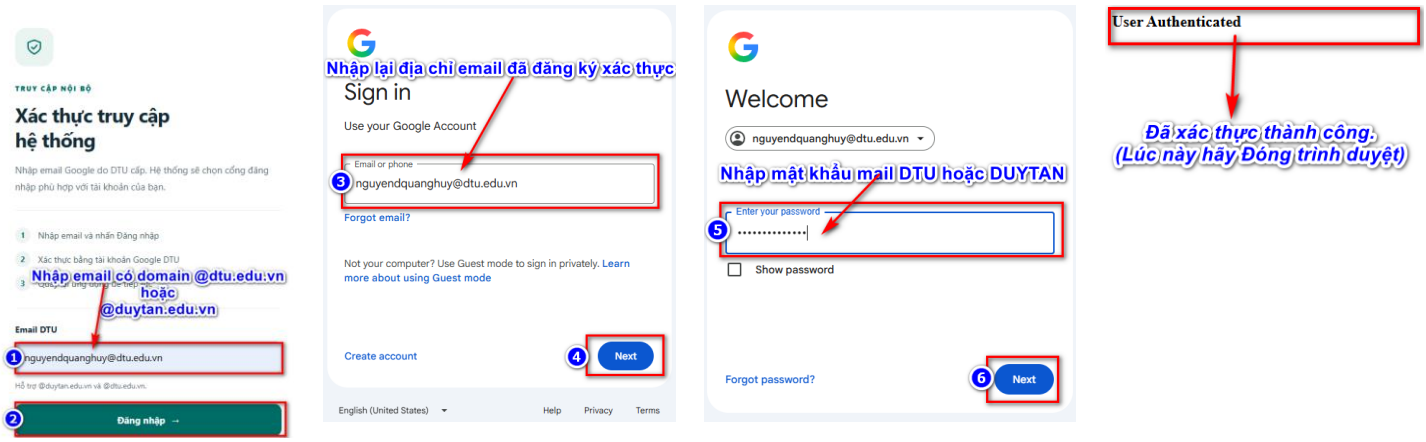
Bước 3. Đăng nhập tài khoản cá nhân

Thực hiện đăng nhập theo hướng dẫn hiển thị trên trang xác thực.

- Sử dụng đúng tài khoản email do Trường cấp.
- Nhập mật khẩu tương ứng với tài khoản.
- Nếu trình duyệt tự động chọn một tài khoản khác, cần chuyển sang đúng tài khoản được cấp.
- Thực hiện xác thực bổ sung nếu hệ thống yêu cầu.

Bước 4. Hoàn tất xác thực

- Chờ hệ thống xử lý và hiển thị thông báo xác thực thành công **(User Authenticated).**
- **Lưu ý:** *Việc truy cập được trang đăng nhập hoặc nhập tài khoản, mật khẩu chưa đồng nghĩa với việc xác thực đã hoàn tất.*



Hình 1. Minh họa quy trình xác thực danh tính khi sử dụng mạng LAN.

Lưu ý: Chỉ sử dụng duy nhất 1 tài khoản email đã được cấp để xác thực

Bước 5. Kiểm tra kết nối và sử dụng AMS

Sau khi xác thực thành công:

1. Thực hiện kiểm tra kết nối theo hướng dẫn tại Mục V.
2. Mở phần mềm AMS.

3. Đăng nhập bằng tài khoản AMS đã được cấp.
4. Kiểm tra các chức năng tương ứng với quyền sử dụng.

Nếu đổi máy tính, thay đổi phương thức kết nối hoặc hệ thống yêu cầu xác thực lại, người dùng thực hiện lại các bước nêu trên.

Trường hợp không truy cập được trang xác thực, cần kiểm tra kết nối mạng LAN hoặc liên hệ **Trung tâm CIT** để được hỗ trợ.

IV. PHƯƠNG THỨC 2: KẾT NỐI VPN KHI SỬ DỤNG BÊN NGOÀI MẠNG LAN CỦA TRƯỜNG

Áp dụng đối với cán bộ, giảng viên và nhân viên sử dụng AMS từ bên ngoài hệ thống mạng LAN của Trường.

Người dùng **cần cài đặt và kết nối VPN bằng phần mềm GlobalProtect**.

4.1. Cài đặt phần mềm GlobalProtect

Trường hợp máy tính đã cài đặt GlobalProtect, có thể chuyển trực tiếp sang Mục 4.2.

Bước 1. Tải bộ cài đặt

Truy cập một trong các địa chỉ VPN tương ứng với tài khoản email được đăng ký:

- Tài khoản @dtu.edu.vn: https://vpn-dtu.dtu.edu.vn
- Tài khoản @duytan.edu.vn: https://vpn-duytan.duytan.edu.vn

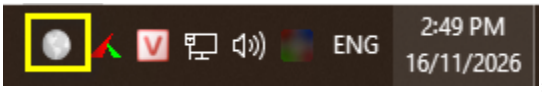
Thực hiện tải bộ cài GlobalProtect theo hướng dẫn trên trang tương ứng.

Bước 2. Cài đặt phần mềm

- Mở bộ cài GlobalProtect vừa tải về.
- Thực hiện các bước cài đặt theo hướng dẫn.
- Chấp nhận yêu cầu cấp quyền cài đặt nếu được phép.
- Chọn **Close** hoặc **Finish** khi hoàn tất.

4.2. Chọn địa chỉ Portal VPN

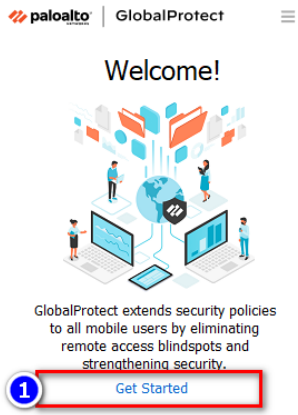
Bước 3. Mở phần mềm GlobalProtect

Mở **Start Menu** của Windows, tìm kiếm **GlobalProtect** hoặc chọn biểu tượng **GlobalProtect** tại khu vực thông báo (**System Tray**) 

, cạnh đồng hồ Windows.

Nếu chưa thấy biểu tượng, nhấn mũi tên mở rộng để hiển thị các biểu tượng đang ẩn.

Bước 4. Nhập địa chỉ Portal



Hình 2. Màn hình khởi động GloblProtect

Căn cứ vào tên miền email đã đăng ký, nhập địa chỉ Portal tương ứng:

Tài khoản email	Địa chỉ Portal cần nhập
@dtu.edu.vn	**vpn-dtu.dtu.edu.vn**
@duytan.edu.vn	**vpn-duytan.duytan.edu.vn**



Hình 3. Màn hình khai báo portal

Nhập chính xác địa chỉ Portal vào ô tương ứng, **không nhập tiền tố https://** hoặc đường dẫn bổ sung.

Sau đó chọn **Connect**.

Lưu ý quan trọng:

- *Chỉ chọn một Portal phù hợp với tên miền email đã đăng ký.*
- *Không chọn Portal theo tên đăng nhập Windows.*
- *Không sử dụng Portal của tên miền email còn lại.*
- *Nếu GlobalProtect đã lưu Portal cũ, cần kiểm tra và chuyển sang Portal phù hợp.*

4.3. Đăng nhập và xác thực VPN

Bước 5. Đăng nhập tài khoản

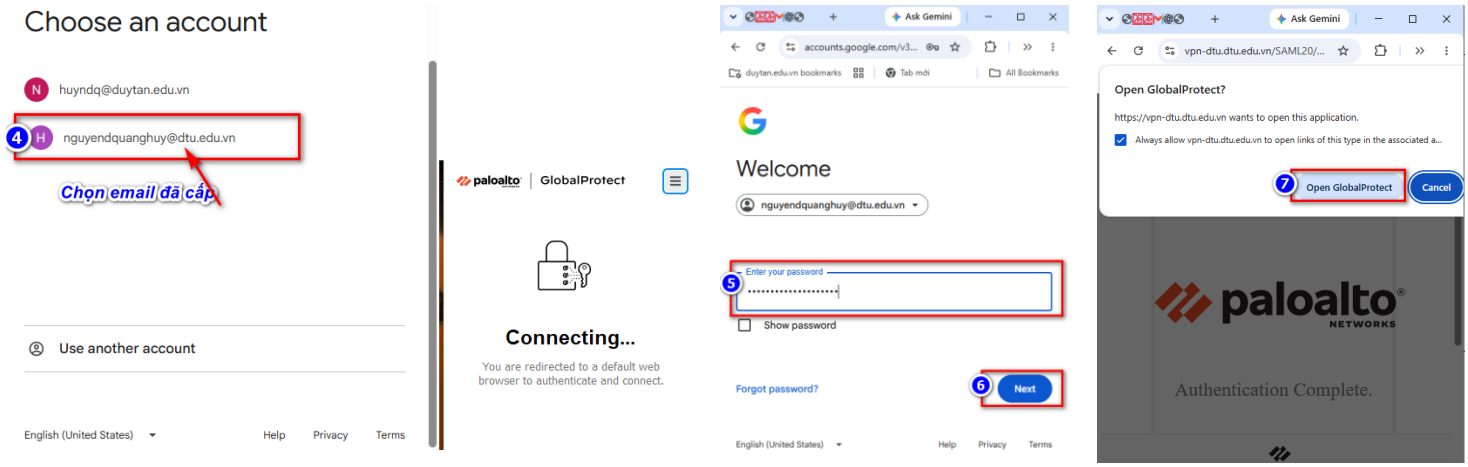
Sau khi chọn Connect, GlobalProtect sẽ mở cửa sổ đăng nhập hoặc trình duyệt để thực hiện xác thực.

Người dùng sử dụng tài khoản email tương ứng với Portal đã chọn.

Bước 6. Hoàn tất xác thực

- Nhập mật khẩu tài khoản.
- Thực hiện xác thực bổ sung MFA nếu được yêu cầu.
- Nếu trình duyệt hiển thị yêu cầu mở ứng dụng GlobalProtect, chọn cho phép mở ứng dụng để tiếp tục.

Không đóng ứng dụng GlobalProtect trong quá trình xác thực.



Hình 4. Minh họa quy trình đăng nhập và xác thực VPN.

Lưu ý: Chỉ sử dụng duy nhất 1 tài khoản email đã được cấp để xác thực

Bước 7. Kiểm tra trạng thái kết nối VPN

Sau khi xác thực trên trình duyệt thành công, người dùng quay lại ứng dụng GlobalProtect.

Cần phân biệt hai trạng thái:

- **Authentication Complete:** Quá trình xác thực danh tính trên trình duyệt đã hoàn tất.
- **Connected:** GlobalProtect đã thiết lập kết nối VPN thành công.

Chỉ khi GlobalProtect hiển thị trạng thái **Connected** mới được xem là đã kết nối VPN thành công.



Hình 5. Trạng thái Connected trên phần mềm GlobalProtect.

Bước 8. Kiểm tra kết nối và sử dụng AMS

Sau khi GlobalProtect hiển thị Connected:

1. Thực hiện kiểm tra kết nối theo hướng dẫn tại Mục V.
2. Mở phần mềm AMS.
3. Đăng nhập bằng tài khoản AMS đã được cấp.
4. Kiểm tra các chức năng tương ứng với quyền sử dụng.

Lưu ý: Giữ GlobalProtect ở trạng thái Connected trong suốt thời gian sử dụng AMS. Nếu VPN bị ngắt kết nối, cần kết nối lại trước khi tiếp tục sử dụng.

V. KIỂM TRA KẾT NỐI SAU KHI XÁC THỰC

Áp dụng cho cả hai phương thức:

- Máy tính kết nối mạng LAN và đã xác thực tại https://auth.duytan.edu.vn.
- Máy tính sử dụng VPN và GlobalProtect đã hiển thị Connected.

Người dùng có thể kiểm tra khả năng kết nối đến địa chỉ mạng nội bộ theo các bước sau.

Bước 1. Mở Command Prompt

- Nhấn tổ hợp phím Windows + R Nhập: **cmd**
- Nhấn Enter để mở cửa sổ Command Prompt.

Bước 2. Thực hiện lệnh kiểm tra

Ở cửa sổ **Command Prompt**, nhập lệnh sau và nhấn Enter: **ping 20.20.0.1**

Windows sẽ gửi các gói tin kiểm tra đến địa chỉ 20.20.0.1.

- **Trường hợp 1: Có phản hồi**

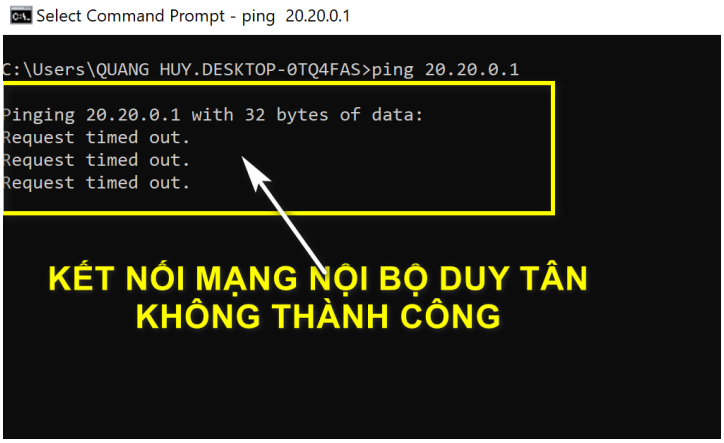


Hình 6. Minh họa kết quả kiểm tra kết nối thành công bằng lệnh ping.

- **Trường hợp 2: Không có phản hồi**

Nếu xuất hiện các thông báo:

- Request timed out.
- Destination host unreachable.
- Có gói tin bị mất (Packet loss).



Hình 7. Minh họa kết quả kiểm tra kết nối không thành công bằng lệnh ping.

Người dùng thực hiện:

1. Kiểm tra lại kết nối mạng.
2. Đối với mạng LAN: xác thực lại tại trang https://auth.duytan.edu.vn.
3. Đối với VPN: kiểm tra GlobalProtect còn ở trạng thái Connected hay không.
4. Thực hiện lại lệnh ping.

Nếu vẫn không có phản hồi, chụp ảnh toàn bộ kết quả và gửi đến Trung tâm CIT (**cit@duytan.edu.vn**) để được hỗ trợ.

VI. KẾT THÚC SỬ DỤNG VÀ XỬ LÝ SỰ CỐ

6.1. Kết thúc phiên làm việc

Sau khi hoàn thành công việc, người dùng thực hiện:

1. Lưu lại các nội dung đang xử lý.
2. Đăng xuất khỏi phần mềm AMS.
3. Đóng phần mềm AMS.
4. Nếu sử dụng VPN, mở GlobalProtect và chọn Disconnect khi không còn nhu cầu truy cập hệ thống mạng nội bộ.
5. Nếu sử dụng máy tính dùng chung, đăng xuất tài khoản trên trình duyệt và không lưu mật khẩu cá nhân.

6.2. Các tình huống thường gặp và cách xử lý

Hiện tượng	Hướng xử lý
Không truy cập được auth.duytan.edu.vn	*Kiểm tra máy tính có đang kết nối mạng LAN của Trường hay không. Nếu ở bên ngoài, sử dụng VPN.*
Không đăng nhập được VPN	*Kiểm tra email và Portal đã chọn. Đảm bảo sử dụng đúng tài khoản tương ứng với Portal. Kiểm tra kết nối Internet.*

Authentication Complete nhưng chưa Connected	*Quay lại GlobalProtect và chờ kết quả kết nối. Nếu trình duyệt yêu cầu mở ứng dụng, cho phép mở GlobalProtect.*
GlobalProtect báo Connection Failed	*Kiểm tra kết nối Internet, địa chỉ Portal và thử kết nối lại. Nếu vẫn lỗi, chụp ảnh thông báo gửi CNTT.*
Xuất hiện cảnh báo chứng chỉ hoặc trang web không an toàn	*Dừng thao tác đăng nhập, kiểm tra lại địa chỉ truy cập và liên hệ CNTT. Không tự ý bỏ qua cảnh báo hoặc cài đặt chứng chỉ từ nguồn không được xác nhận.*
Đã xác thực nhưng AMS không truy cập được	*Kiểm tra trạng thái VPN (nếu sử dụng VPN), đóng và mở lại AMS. Nếu vẫn lỗi, liên hệ CNTT để kiểm tra quyền và kết nối.*
AMS báo tài khoản không có quyền truy cập	*Liên hệ đơn vị quản trị AMS để kiểm tra tài khoản và quyền sử dụng.*

VII. TẢI PHẦN MỀM GLOBALPROTECT

Người dùng có thể tải phần mềm GlobalProtect từ các Portal VPN của Trường.

7.1. Trang tải phần mềm

- Portal dành cho tài khoản @dtu.edu.vn: https://vpn-dtu.dtu.edu.vn
- Portal dành cho tài khoản @duytan.edu.vn: https://vpn-duytan.duytan.edu.vn

7.2. Liên kết tải trực tiếp

Các liên kết tải bộ cài từ Portal vpn-duytan.duytan.edu.vn:

Windows 32-bit:

- https://vpn-duytan.duytan.edu.vn/global-protect/getmsi.esp?version=32&platform=windows

Windows 64-bit:

- https://vpn-duytan.duytan.edu.vn/global-protect/getmsi.esp?version=64&platform=windows

macOS:

- https://vpn-duytan.duytan.edu.vn/global-protect/getmsi.esp?version=none&platform=mac

Lưu ý: *Người dùng cần chọn đúng phiên bản tương thích với hệ điều hành đang sử dụng. Đối với macOS, sử dụng bộ cài dành riêng cho macOS, không sử dụng bộ cài MSI của Windows.*

VIII. TÀI LIỆU THAM KHẢO

1. Hướng dẫn truy cập và xác thực danh tính trên hệ thống mạng nội bộ Đại học Duy Tân.
2. Hướng dẫn sử dụng hệ thống VPN của Đại học Duy Tân.
3. Tài liệu chính thức của Palo Alto Networks:
    - Download and Install the GlobalProtect App for Windows.
    - Use the GlobalProtect App for Windows.

Đề nghị: Cán bộ, giảng viên và nhân viên thực hiện đúng hướng dẫn để bảo đảm an toàn tài khoản, xác thực danh tính và truy cập AMS ổn định, đúng quy định của Nhà trường.