Triển khai xác minh 2 bước

Xác minh hai bước · https://gcs.vn/kho-tai-nguyen/google-workspace-admin-center/trien-khai-xac-minh-2-buoc/

Bạn và người dùng của bạn đóng vai trò quan trọng trong việc thiết lập **Xác minh 2 bước** (**2 Steps Verification - 2SV**). Người dùng của bạn có thể chọn phương thức 2SV của họ hoặc bạn có thể thực thi một phương thức cho một số người dùng hoặc nhóm nhất định trong tổ chức của mình. Ví dụ: bạn có thể yêu cầu một nhóm nhỏ trong bộ phận Bán hàng sử dụng khóa bảo mật.

Bước 1: Thông báo cho người dùng về việc triển khai Xác minh 2 bước

Trước khi triển khai 2SV, hãy truyền đạt kế hoạch của công ty bạn tới người dùng, bao gồm:

- 2SV là gì và tại sao công ty của bạn sử dụng nó.
- 2SV là tùy chọn hay bắt buộc.
- Nếu được yêu cầu, hãy cung cấp ngày mà người dùng phải bật 2SV.
- Phương pháp 2SV nào là bắt buộc hoặc được khuyến nghị.

Bước 2: Cho phép người dùng bật Xác minh 2 bước

Tài khoản người dùng được tạo trước tháng 12 năm 2016 có 2SV được bật theo mặc định.

Cho phép người dùng bật 2SV và sử dụng bất kỳ phương thức xác minh nào.

1. Đăng nhập vào Bảng điều khiển dành cho quản trị viên của Google của bạn .
2. Trong Bảng điều khiển dành cho quản trị viên, hãy chuyển tới Menu > **Bảo mật** > **Xác thực** > **Xác minh 2 bước.**
3. Để áp dụng cài đặt này cho mọi người, hãy chọn đơn vị tổ chức cấp cao nhất. Nếu không, hãy chọn đơn vị tổ chức con hoặc nhóm cấu hình .
4. Chọn hộp **Cho phép người dùng bật Xác minh 2 bước** .
5. Chọn **Enforcement** > **Off**.
6. Nhấp vào **Lưu** . Nếu đã định cấu hình một đơn vị tổ chức hoặc nhóm, thì bạn có thể **Kế thừa** hoặc **Ghi đè** đơn vị tổ chức mẹ hoặc **Hủy đặt** một nhóm.

Bước 3: Yêu cầu người dùng của bạn đăng ký Xác minh 2 bước

1. Yêu cầu người dùng của bạn đăng ký 2SV bằng cách làm theo hướng dẫn trong Bật xác minh 2 bước .
2. Hướng dẫn đăng ký phương thức 2SV:
   - Khóa bảo mật
   - Lời nhắc của Google, tin nhắn văn bản hoặc cuộc gọi điện thoại
   - Ứng dụng xác thực Google
   - Mã dự phòng

Bước 4: Theo dõi việc đăng ký của người dùng

Sử dụng báo cáo để đo lường và theo dõi việc đăng ký 2SV của người dùng. Kiểm tra trạng thái đăng ký, trạng thái thực thi và số lượng khóa bảo mật của người dùng.

1. Đăng nhập vào Bảng điều khiển dành cho quản trị viên của Google của bạn .
2. Trong Bảng điều khiển dành cho quản trị viên, đi tới Menu > **Báo cáo** > **Báo cáo người dùng** > **Bảo mật**.
3. (Tùy chọn) Để thêm cột thông tin mới, nhấp vào Cài đặt > **Thêm cột mới** . Chọn cột cần thêm vào bảng rồi nhấn **Lưu**.

Để biết thêm thông tin, hãy đi tới Quản lý cài đặt bảo mật của người dùng .

View enrollment trends

1. Đăng nhập vào Bảng điều khiển dành cho quản trị viên của Google của bạn .
2. Từ Trang chủ Bảng điều khiển dành cho quản trị viên, đi tới **Báo cáo** > **Báo cáo ứng dụng** > **Tài khoản** .

Xác định các đơn vị và nhóm tổ chức không sử dụng Xác minh 2 bước

1. Đăng nhập vào Bảng điều khiển dành cho quản trị viên của Google của bạn .
2. Trong Bảng điều khiển dành cho quản trị viên, đi tới Menu > **Bảo mật** > **Trung tâm bảo mật** > **Tình trạng bảo mật** .

3. Tìm kiếm **Tình trạng bảo mật** để **xác minh hai bước dành cho quản trị viên** hoặc **Xác minh hai bước dành cho người dùng** để xem lại thông tin 2SV.

Bước 5: Thực thi xác minh 2 bước (Tùy chọn)

Trước khi bạn bắt đầu: Đảm bảo người dùng đã đăng ký 2SV.

Quan trọng: Khi 2SV được thực thi, những người dùng chưa hoàn tất quy trình đăng ký 2SV nhưng đã thêm thông tin Xác thực 2 yếu tố (2FA) vào tài khoản của họ, chẳng hạn như khóa bảo mật hoặc số điện thoại, sẽ có thể đăng nhập bằng thông tin này . Nếu bạn thấy đăng nhập từ người dùng chưa đăng ký thuộc đơn vị tổ chức nơi 2SV đã được thực thi thì đó là đăng nhập 2SV.

1. Đăng nhập vào Bảng điều khiển dành cho quản trị viên của Google của bạn .
2. Trong Bảng điều khiển dành cho quản trị viên, hãy chuyển tới Menu > **Bảo mật** > **Xác thực** > **Xác minh 2 bước.**
3. Để áp dụng cài đặt này cho mọi người, hãy chọn đơn vị tổ chức cấp cao nhất. Nếu không, hãy chọn đơn vị tổ chức con hoặc nhóm cấu hình .
4. Nhấn vào **Cho phép người dùng bật Xác minh 2 bước** .
5. Đối với **Thực thi** , hãy chọn một tùy chọn:
   - **Bật** —Bắt đầu ngay lập tức.
   - **Bật thực thi từ ngày** —Chọn ngày bắt đầu. Người dùng sẽ thấy lời nhắc đăng ký 2SV khi họ đăng nhập.
     Lưu ý: Khi sử dụng tùy chọn **Bật từ ngày** , quá trình thực thi sẽ bắt đầu trong vòng 24-48 giờ kể từ ngày đã chọn. Nếu bạn muốn thời gian bắt đầu thực thi chính xác, hãy sử dụng tùy chọn **Bật** .
6. (Tùy chọn) Để cho nhân viên mới có thời gian đăng ký trước khi áp dụng biện pháp thực thi đối với tài khoản của họ, đối với **Thời gian đăng ký người dùng mới** , hãy chọn khung thời gian từ 1 ngày đến 6 tháng.
   Trong thời gian này, người dùng có thể đăng nhập chỉ bằng mật khẩu của mình.
7. (Tùy chọn) Để cho phép người dùng tránh việc kiểm tra 2SV lặp đi lặp lại trên các thiết bị đáng tin cậy, trong **Tần suất** , hãy chọn hộp **Cho phép người dùng tin cậy vào thiết bị** .
   Lần đầu tiên người dùng đăng nhập từ một thiết bị mới, họ có thể chọn hộp để tin cậy thiết bị của mình. Sau đó, người dùng sẽ không được nhắc thực hiện 2SV trên thiết bị trừ khi người dùng xóa cookie hoặc thu hồi thiết bị hoặc bạn đặt lại cookie đăng nhập của người dùng.
   Bạn không nên tránh 2SV trên các thiết bị đáng tin cậy trừ khi người dùng của bạn thường

xuyên di chuyển giữa các thiết bị.

8. Đối với **Methods** , chọn phương thức thực thi:
   - **Bất kỳ** —Người dùng có thể thiết lập bất kỳ phương thức 2SV nào.
   - **Mọi thứ ngoại trừ mã xác minh qua tin nhắn, cuộc gọi điện thoại** —Người dùng có thể thiết lập bất kỳ phương thức 2SV nào ngoại trừ việc sử dụng điện thoại của họ để nhận mã xác minh 2SV.

     Quan trọng : Người dùng sử dụng tin nhắn và cuộc gọi điện thoại để xác minh sẽ bị khóa tài khoản của họ. Để tránh khóa những người dùng này khỏi tài khoản của họ:
     - Trước khi thực thi, hãy yêu cầu người dùng bắt đầu sử dụng phương thức 2SV khác vì mã 2SV sẽ không có trên điện thoại của họ sau ngày thực thi.
     - Bạn có thể sử dụng sự kiện hoạt động login_verification Kiểm tra đăng nhập để theo dõi những người dùng sử dụng mã từ tin nhắn văn bản hoặc cuộc gọi thoại. Nếu tham số login_challenge_method có giá trị idv_preregistered_phone, người dùng sẽ xác thực bằng mã xác minh bằng văn bản hoặc giọng nói.

   - **Chỉ khóa bảo mật** —Người dùng phải thiết lập khóa bảo mật.
     Trước khi chọn phương pháp thực thi này, hãy tìm những người dùng đã thiết lập khóa bảo mật (dữ liệu báo cáo có thể bị trễ tới 48 giờ). Để xem trạng thái 2SV theo thời gian thực cho từng người dùng, hãy đi tới Quản lý cài đặt bảo mật của người dùng .

9. Nếu bạn chọn **Chỉ khóa bảo mật** , hãy đặt **thời gian gia hạn tạm dừng chính sách Xác minh 2 bước** .
   Khoảng thời gian này cho phép người dùng đăng nhập bằng mã xác minh dự phòng mà bạn tạo cho người dùng. Mã này rất hữu ích khi người dùng mất khóa bảo mật. Chọn độ dài của thời gian gia hạn này, bắt đầu khi bạn tạo mã xác minh. Để biết thông tin về mã dự phòng, hãy truy cập Nhận mã xác minh dự phòng cho người dùng .
10. Đối với **Mã bảo mật** , hãy chọn xem người dùng có thể đăng nhập bằng mã bảo mật hay không.
    - **Không cho phép người dùng tạo mã bảo mật** —Người dùng không thể tạo mã bảo mật.
    - **Cho phép mã bảo mật mà không cần truy cập từ xa** —Người dùng có thể tạo mã bảo mật và sử dụng chúng trên cùng một thiết bị hoặc mạng cục bộ (NAT hoặc LAN).
    - **Cho phép mã bảo mật có quyền truy cập từ xa** —Người dùng có thể tạo mã bảo mật và sử dụng chúng trên các thiết bị hoặc mạng khác, chẳng hạn như khi truy cập máy chủ từ xa hoặc máy ảo.

Mã bảo mật khác với mã dùng một lần mà các ứng dụng như Google Authenticator tạo ra. Để tạo mã bảo mật, người dùng chạm vào khóa bảo mật trên thiết bị của họ để tạo mã bảo mật. Mã bảo mật có hiệu lực trong 5 phút.

11. Nhấp vào **Lưu** . Nếu đã định cấu hình một đơn vị tổ chức hoặc nhóm, thì bạn có thể **Kế thừa** hoặc **Ghi đè** đơn vị tổ chức mẹ hoặc **Hủy đặt** một nhóm.

If users don't comply by the enforcement date

Bạn có thể cho người dùng thêm thời gian để đăng ký bằng cách thêm họ vào nhóm mà 2SV không được thực thi. Mặc dù cách giải quyết này cho phép người dùng đăng nhập nhưng nó không được khuyến khích như một thông lệ tiêu chuẩn. Tìm hiểu cách tránh bị khóa tài khoản khi thực thi Xác minh 2 bước .

Chủ đề có liên quan

- Xem báo cáo Ứng dụng về tổ chức của bạn

<

Tiếp theo: Cách xác minh 2 bước hoạt động khác với các ứng dụng cũ >

Bấm vào đây