Thực thi và giám sát các yêu cầu mật khẩu cho người dùng

Đặt lại và khôi phục mật khẩu · https://gcs.vn/kho-tai-nguyen/google-workspace-admin-center/thuc-thi-va-giam-sat-cac-yeu-cau-mat-khau-cho-nguoi-dung/

Với tư cách là quản trị viên, bạn có thể thực thi các yêu cầu về mật khẩu để bảo vệ Tài khoản Google được quản lý của người dùng và đáp ứng nhu cầu tuân thủ của tổ chức bạn. Bạn cũng có thể biết mật khẩu nào của người dùng yếu bằng cách theo dõi độ mạnh mật khẩu của họ.

Giúp bảo mật tài khoản người dùng

- **Yêu cầu mật khẩu mạnh** —Bạn có thể buộc người dùng có mật khẩu yếu thay đổi chúng. Bạn cũng có thể yêu cầu một số ký tự nhất định cho mật khẩu.
- **Ngăn chặn người dùng sử dụng lại mật khẩu cũ**.
- **Giải thích tầm quan trọng của mật khẩu mạnh** —Để giúp người dùng tạo mật khẩu mạnh, hãy chia sẻ các mẹo về mật khẩu này .

Trước khi bắt đầu

Mở rộng tất cả | Thu gọn tất cả

Khi chính sách mật khẩu không được áp dụng

- Google không thể thực thi các yêu cầu về độ mạnh và độ dài mật khẩu đối với mật khẩu được đặt bằng phương pháp băm—ví dụ: mật khẩu được tạo bằng công cụ tải lên hàng loạt người dùng , API thư mục hoặc các công cụ đồng bộ hóa như Đồng bộ hóa mật khẩu hoặc Google Cloud Directory Sync. Để biết thông tin chi tiết, hãy truy cập SDK quản trị Google Workspace hoặc xem Giới thiệu về đồng bộ hóa mật khẩu.
- Yêu cầu về độ dài và độ mạnh của mật khẩu không áp dụng cho bất kỳ mật khẩu người dùng nào mà bạn đặt lại theo cách thủ công. Nếu bạn đặt lại mật khẩu theo cách thủ công, hãy đảm bảo chọn hộp **Yêu cầu người dùng thay đổi mật khẩu của họ khi họ** đăng nhập cho người dùng đó.

- Chính sách mật khẩu bạn định cấu hình không áp dụng cho người dùng được xác thực trên nhà cung cấp danh tính bên thứ ba (IdP) bằng SAML.

Điều gì làm cho mật khẩu mạnh

Điều gì làm cho mật khẩu mạnh
Nếu bạn thực thi mật khẩu mạnh, Google sẽ sử dụng thuật toán xếp hạng độ mạnh mật khẩu để đảm bảo rằng mật khẩu:

- Có mức độ ngẫu nhiên cao, được gọi là *entropy* mật khẩu , bạn có thể đạt được điều này bằng cách sử dụng một chuỗi ký tự dài thuộc các loại khác nhau, chẳng hạn như chữ hoa, chữ thường, chữ số và ký tự đặc biệt
  Lưu ý: Mật khẩu mạnh không cần phải có số lượng ký tự cụ thể của một loại cụ thể.
- Không phải là mật khẩu yếu thường được sử dụng, như “123456” hoặc “password123”
- Không dễ đoán, chẳng hạn như các từ hoặc cụm từ đơn giản hoặc các mẫu có mật khẩu giống với tên người dùng
- Không được biết là bị xâm phạm—nghĩa là nó không có trong cơ sở dữ liệu về các tài khoản bị vi phạm

Cách hết hạn mật khẩu hoạt động

Theo mặc định, việc hết hạn mật khẩu bị tắt vì nghiên cứu cho thấy ít tác động tích cực đến bảo mật. Bạn có thể đặt mật khẩu của người dùng hết hạn sau một số ngày (chẳng hạn như 90 hoặc 180 ngày) nếu cần vì lý do tuân thủ.

Việc hết hạn mật khẩu chỉ được thực thi đối với những lần đăng nhập vào ứng dụng dựa trên trình duyệt. Nó không được thực thi đối với những người dùng chỉ sử dụng điện thoại hoặc những người đăng nhập bằng ứng dụng được xác thực OAuth.

Cảnh báo mật khẩu

Nếu bạn đặt thời hạn hết hạn mật khẩu, người dùng sẽ nhận được thông báo bật lên (chứ không phải lời nhắc qua email) trong các dịch vụ Google của họ, chẳng hạn như Gmail và Lịch, 30 ngày trước ngày hết hạn mật khẩu. Người dùng có thể thay đổi mật khẩu hoặc đóng cảnh báo. Nếu người dùng không thay đổi mật khẩu, cảnh báo sẽ xuất hiện vào lần tiếp theo họ đăng nhập vào tài khoản của mình. Cảnh báo sẽ ngừng xuất hiện sau khi người dùng đóng nó 3 lần. Tuy nhiên, sau khi mật khẩu hết hạn, người dùng phải thay đổi mật khẩu ở lần đăng nhập tiếp theo.

Khi người dùng cần thay đổi mật khẩu

Khi bạn thiết lập chính sách hết hạn mật khẩu lần đầu tiên, một số người dùng có thể được nhắc thay đổi mật khẩu ngay lập tức, trong khi những người khác không cần thay đổi mật khẩu ngay lập tức. Ví dụ:

- Nếu bạn thiết lập chính sách hết hạn 90 ngày và người dùng thay đổi mật khẩu lần cuối *cách đây 100 ngày* thì mật khẩu của người dùng đó sẽ hết hạn ngay khi bạn thiết lập chính sách. Họ sẽ được nhắc thay đổi mật khẩu vào lần tiếp theo khi họ cố gắng đăng nhập vào tài khoản của mình.
- Nếu bạn thiết lập chính sách hết hạn trong 90 ngày và người dùng thay đổi mật khẩu lần cuối *cách đây 30 ngày* thì mật khẩu của người dùng đó vẫn chưa hết hạn. Sau 60 ngày, họ sẽ được nhắc thay đổi mật khẩu vào lần đăng nhập tiếp theo.

Đặt yêu cầu mật khẩu

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** > **Xác thực quản lý** > **Mật khẩu** .
3. Ở bên trái, hãy chọn đơn vị tổ chức mà bạn muốn đặt chính sách mật khẩu.
   Đối với tất cả người dùng, hãy chọn đơn vị tổ chức cấp cao nhất. Nếu không, hãy chọn một tổ chức khác để thực hiện cài đặt cho người dùng của tổ chức đó. Ban đầu, tổ chức sẽ kế thừa các cài đặt của tổ chức mẹ.
4. Trong phần **Sức mạnh**, hãy chọn hộp **Thực thi mật khẩu mạnh**.
   Tìm hiểu thêm về mật khẩu mạnh.
5. Trong phần **Độ dài**, nhập độ dài tối thiểu và tối đa cho mật khẩu người dùng của bạn. Nó có thể có từ 8 đến 100 ký tự.
6. (Tùy chọn) Để buộc người dùng thay đổi mật khẩu, hãy chọn hộp **Thực thi chính sách mật khẩu ở lần đăng nhập tiếp theo** .
   Nếu bạn không chọn tùy chọn này, người dùng có mật khẩu yếu có thể truy cập vào các dịch vụ Google của tổ chức bạn cho đến khi họ quyết định thay đổi mật khẩu của mình.
7. (Tùy chọn) Để cho phép người dùng sử dụng lại mật khẩu cũ, hãy chọn hộp **Cho phép sử dụng lại mật khẩu** .
   Bạn không thể đặt lịch sử mật khẩu mà Google xem xét để ngăn chặn việc sử dụng lại.

8. Trong phần **Hết hạn**, chọn khoảng thời gian mà mật khẩu sẽ hết hạn.
   Lưu ý: Nếu tài khoản người dùng đã thêm người dùng được ủy quyền thì người dùng được ủy quyền vẫn có thể truy cập vào tài khoản, ngay cả khi mật khẩu tài khoản đã hết hạn. Để ngăn truy cập liên tục, hãy đặt lại mật khẩu tài khoản hoặc xóa người dùng được ủy quyền .
9. Bấm **Ghi đè** để giữ nguyên cài đặt, ngay cả khi cài đặt gốc thay đổi.
10. Nếu trạng thái của đơn vị tổ chức đã **bị ghi đè**, hãy chọn một tùy chọn:
    - **Kế thừa** —Hoàn nguyên về cùng cài đặt với cha mẹ của nó.
    - **Lưu** —Lưu cài đặt mới của bạn (ngay cả khi cài đặt gốc thay đổi).
11. Cung cấp cho người dùng các mẹo để tạo mật khẩu mạnh .

Theo dõi độ mạnh mật khẩu 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** > **Báo cáo người dùng** > **Tài khoản**.
3. (Tùy chọn) Để kiểm tra thông tin độ mạnh mật khẩu ở dạng biểu đồ, hãy truy cập **Báo cáo** > **Báo cáo ứng dụng** > **Tài khoản**. Tìm hiểu thêm về Báo cáo tài khoản .

Chủ đề liên quan

- Đặt yêu cầu mật khẩu cho thiết bị di động được quản lý
- Quản lý cài đặt bảo mật người dùng