Định nghĩa đặc quyền của quản trị viên

Vai trò quản trị viên · https://gcs.vn/kho-tai-nguyen/google-workspace-admin-center/dinh-nghia-dac-quyen-cua-quan-tri-vien/

Khi chỉ định vai trò quản trị viên cho người dùng trong Bảng điều khiển dành cho quản trị viên của Google, bạn cấp cho họ các đặc quyền của quản trị viên và quyền truy cập vào Bảng điều khiển dành cho quản trị viên.

Đặc quyền của vai trò xác định các quyền kiểm soát của quản trị viên trong Bảng điều khiển dành cho quản trị viên, thông tin họ có thể truy cập và nhiệm vụ họ có thể thực hiện. Quản trị viên cũng có thể thực hiện các hành động tương ứng trong API quản trị.

Phân công vai trò ngay bây giờ

Tạo vai trò tùy chỉnh

Quyền quản trị viên

* **Lưu ý** : Một số đặc quyền, chẳng hạn như Quản lý Jamboard, chỉ có sẵn với một số phiên bản Google Workspace, phần cứng hoặc giấy phép người dùng nhất định.

Đặc quyền cài đặt quản trị viên	Đặc quyền dịch vụ	

- Admin API
- Domain Settings
- Groups
- Organizational Units
- Reports
- Security
- Support
- Users

- Service Settings
- Alert Center
- App Maker
- Calendar
- Chrome Management*
- Classroom
- Cloud Search*
- Contacts
- Currents
- Data loss prevention (DLP)*
- Data regions
- Data Security
- Directory settings
- Directory Sync
- Drive and Docs
- Gmail
- Google Chat and classic Hangouts
- Google Cloud Print

- Google Hangouts
- Google Meet
- Google Meet hardware*
- Google Vault*
- Google Workspace Marketplace
- Groups for Business
- Jamboard
- Jamboard Management*
- Looker Studio
- Managed Google Play (also listed as "*Google Managed Play* ")
- Mobile Device Management
- Password Vault*
- Pinpoint
- Secure LDAP*
- Security Center*
- Shared device settings
- Sites
- Storage
- Trust rules
- Work Insights*
- YouTube

Đặc quyền cài đặt

Admin AP

Việc cấp đặc quyền cho quản trị viên trong Bảng điều khiển dành cho quản trị viên sẽ mang lại cho họ các quyền tương ứng trong API. Ví dụ: việc cấp đặc quyền tạo người dùng trong Bảng điều khiển dành cho quản trị viên cũng cho phép quản trị viên tạo người dùng bằng API. Tương tự như vậy, việc cập nhật quyền API quản trị sẽ cập nhật các đặc quyền tương ứng trong Bảng điều khiển dành cho quản trị viên.

Để cấp đặc quyền trong Bảng điều khiển dành cho quản trị viên mà không cho phép quản trị viên

thực hiện các hành động trong API, hãy tắt quyền truy cập API cho tài khoản của bạn. Để biết chi tiết, hãy truy cập Quản lý quyền truy cập vào các dịch vụ của Google: Bị hạn chế hoặc Không bị hạn chế.

Đặc quyền **API quản trị** cho phép API quản trị viên Google Workspace thực hiện các hành động trên:

- **Đơn vị tổ chức** —Quản trị viên có thể thực hiện tất cả các hoạt động được cấp bởi đặc quyền Bảng điều khiển dành cho quản trị viên của Đơn vị tổ chức.

Với đặc quyền API, bạn thực hiện các thao tác này bằng API thư mụ.

- **Người dùng**—Quản trị viên có thể thực hiện tất cả các thao tác được cấp bởi đặc quyền Bảng điều khiển dành cho quản trị viên của Người dùng.

Với đặc quyền API, bạn thực hiện các thao tác này bằng API thư mụ.

- **Nhóm**Quản trị viên có thể thực hiện tất cả các thao tác được cấp bởi đặc quyền đặc quyền Bảng điều khiển dành cho quản trị viên của Nhóm .

Với đặc quyền API, bạn thực hiện các thao tác này bằng cách sử dụng:

- API thư mục
- API cài đặt nhóm

- **Quản lý bảo mật người dùng**—Quản trị viên có thể thực hiện tất cả các hoạt động được cấp bởi đặc quyền Bảng điều khiển quản trị quản lý bảo mật người dùng .

Với đặc quyền API, bạn thực hiện các thao tác này bằng cách sử dụng:

- API thư mục
- API cài đặt quản trị viên

- **Truyền dữ liệu**—Quản trị viên cấp cao hoặc quản trị viên dịch vụ có thể chuyển quyền sở hữu tệp Drive của người dùng bằng Bảng điều khiển dành cho quản trị viên. Quản trị viên cũng cần có đặc quyền Dịch vụ Drive để truy cập cài đặt Chuyển quyền sở hữu trong bảng điều khiển. Không có hành động nào trong số này có thể bị giới hạn ở các đơn vị tổ chức cụ thể.
  Lưu ý : Chỉ quản trị viên cấp cao mới có thể chuyển quyền sở hữu tệp khi xóa người dùng.
- **Quản lý lược đồ**Quản trị viên cấp cao hoặc quản trị viên dịch vụ có thể tạo lược đồ để xác định các trường tùy chỉnh cho miền của họ, chẳng hạn như dự án người dùng, vị trí hoặc ngày thuê.

- **Quản lý giấy phép** —Quản trị viên cấp cao và quản trị viên có vai trò Quản lý giấy phép có thể chỉ định và quản lý giấy phép Google Workspace cho tổ chức, đơn vị tổ chức, một nhóm người dùng hoặc một người dùng cá nhân.
- **Quản lý thanh toán**—Quản trị viên có thể thực hiện các tác vụ thanh toán như thiết lập tài khoản thanh toán hoặc thay đổi phương thức thanh toán. Đặc quyền này chỉ hoạt động trong Bảng điều khiển dành cho quản trị viên.
- **Quản lý miền**Quản trị viên có thể thêm hoặc xóa miền và thiết lập bí danh miền.
- **Quản lý danh sách cho phép miền**Quản trị viên có thể tạo và quản lý danh sách cho phép của các miền đáng tin cậy có thể chia sẻ tệp với tổ chức của bạn.
- **Đọc danh sách cho phép của miền** Quản trị viên có thể xem danh sách cho phép của các miền đáng tin cậy có thể chia sẻ tệp với tổ chức của bạn.
- **Thêm nhãn bảo mật vào nhóm**Quản trị viên có thể xác định các nhóm kiểm soát quyền truy cập vào thông tin và tài nguyên nhạy cảm. Để biết chi tiết, hãy xem Cập nhật Nhóm Google thành nhóm bảo mật.

Nếu tạo vai trò tùy chỉnh, bạn có thể chọn hộp bên cạnh đặc quyền để cho phép sử dụng API để thực hiện tất cả các hành động trên đối tượng đó. Hoặc nhấp vào từng hành động riêng lẻ (chẳng hạn như **Tạo** hoặc **Đọc**) để chỉ cho phép các hành động được chọn.

Cài đặt tên miền

Quản trị viên có đặc quyền Cài đặt miền có thể:

- Thay đổi tên tổ chức, ngôn ngữ, logo và múi giờ.
- Xóa tài khoản Google Workspace hoặc Cloud Identity của bạn.
- Xem thông tin thanh toán cho Tài khoản Google Workspace hoặc Cloud Identity của bạn.
- Thêm và xóa tên miền cũng như bí danh tên miền.
- Ánh xạ URL tùy chỉnh tới một trang web trong Google Sites.
- Quản lý quá trình phát hành tính năng của bạn.
- Chọn loại email bạn nhận được từ Google. Để biết thông tin chi tiết, hãy xem Chọn tùy chọn thông báo Google Workspace của bạn .

Những hành động này không thể giới hạn ở các đơn vị tổ chức cụ thể.

Nhóm

Quản trị viên có đặc quyền **Nhóm** có toàn quyền kiểm soát các nhóm được tạo trong Bảng điều khiển dành cho quản trị viên của bạn. Đồng thời cấp các đặc quyền API quản trị tương ứng (ở trên).

Quản trị viên có đặc quyền này có thể:

- Xem hồ sơ người dùng và cơ cấu tổ chức của bạn.
- Tạo, quản lý và xóa nhóm trong Bảng điều khiển dành cho quản trị viên.
- Quản lý cài đặt truy cập nhóm.
- Bật dịch vụ cho các nhóm truy cập (cũng yêu cầu đặc quyền cho Đơn vị tổ chức và Dịch vụ). Để biết chi tiết, hãy xem Tùy chỉnh cài đặt dịch vụ với các nhóm cấu hình .

Những hành động này không thể giới hạn ở các đơn vị tổ chức cụ thể.

Mẹo : Để cho phép quản trị viên xem các nhóm mà người dùng thuộc về nhưng không chỉnh sửa họ, hãy cấp cho họ đặc quyền **Groups** > **Read** API

Đơn vị tổ chức

Quản trị viên có quyền truy cập vào báo cáo sử dụng và nhật ký kiểm tra. Để biết chi tiết, hãy chuyển đến Tổng quan về báo cáo.

Quản trị viên có đặc quyền **Báo cáo** có thể:

- Xem biểu đồ hiển thị việc sử dụng dịch vụ.
- Theo dõi các hoạt động của người dùng như chỉnh sửa tài liệu.
- Theo dõi các thay đổi do quản trị viên khác thực hiện trong Bảng điều khiển dành cho quản trị viên.

Những hành động này không thể giới hạn ở các đơn vị tổ chức cụ thể.

Báo cáo

Quản trị viên có quyền truy cập vào báo cáo sử dụng và nhật ký kiểm tra. Để biết chi tiết, hãy chuyển đến Tổng quan về báo cáo.

Quản trị viên có đặc quyền **Báo cáo** có thể:

- Xem biểu đồ hiển thị việc sử dụng dịch vụ.
- Theo dõi các hoạt động của người dùng như chỉnh sửa tài liệu.

- Theo dõi các thay đổi do quản trị viên khác thực hiện trong Bảng điều khiển dành cho quản trị viên.

Những hành động này không thể giới hạn ở các đơn vị tổ chức cụ thể.

Bảo mật

Quản lý bảo mật người dùng

Lưu ý: Chỉ quản trị viên cấp cao mới có thể xem cài đặt bảo mật của quản trị viên khác.
Quản trị viên có thể quản lý cài đặt bảo mật cho từng người dùng. Họ chỉ có thể quản lý những người dùng không có đặc quyền quản trị viên. Đồng thời cấp các đặc quyền API quản trị tương ứng (ở trên).
Trên trang quản lý **Người dùng ,** quản trị viên có đặc quyền **Quản lý bảo mật người dùng** có thể:

- Tắt Xác minh 2 bước. Chỉ quản trị viên cấp cao mới có thể thực thi Xác minh 2 bước cho toàn bộ tổ chức.
- Tắt thử thách đăng nhập trong 10 phút.
- Xem xét và thu hồi khóa bảo mật.
- Xem xét và thu hồi mật khẩu ứng dụng.
- Đặt lại cookie đăng nhập (không dành cho quản trị viên của người bán lại).
- Xem xét và thu hồi mọi mã thông báo OAuth 3 chân mà người dùng đã cấp cho ứng dụng của bên thứ ba.

Tất cả những hành động này có thể được giới hạn ở các đơn vị tổ chức cụ thể, ngoại trừ việc thực thi hoặc vô hiệu hóa Xác minh 2 bước.

Cài đặt hệ thống bảo vệ

- Cho phép các ứng dụng kém an toàn hơn truy cập vào tài khoản
- Giám sát mật khẩu người dùng
- Thiết lập đăng nhập một lần (SSO) và xác thực

Cho phép các ứng dụng kém an toàn hơn truy cập
Hỗ trợ

Quản trị viên có đặc quyền **Hỗ trợ** có thể sử dụng các tùy chọn gọi điện, trò chuyện và email để liên hệ với bộ phận hỗ trợ của Google Workspace. Họ cũng có thể gửi các trường hợp lên Cổng

chăm sóc khách hàng của Google.

Khả năng liên hệ với bộ phận hỗ trợ của Google Workspace không bị giới hạn ở các đơn vị tổ chức cụ thể.

Người dùng

Quản trị viên có đặc quyền **Người dùng** có thể thực hiện các hành động đối với người dùng. Chỉ quản trị viên cấp cao mới có thể thay đổi cài đặt của quản trị viên khác. Đồng thời cấp các đặc quyền API quản trị tương ứng (ở trên).

- Tạo nên
- Đọc
- Cập nhật – Cấp khả năng thay đổi tài khoản người dùng, bao gồm lưu trữ, hủy lưu trữ và cấp khả năng khôi phục dữ liệu. Nó cũng bao gồm các quyền sau đây có thể được ủy quyền riêng lẻ.
  - Di chuyển người dùng

Lưu ý: Chỉ quản trị viên cấp cao mới có thể sử dụng công cụ Chuyển để chuyển tài khoản người dùng không được quản lý sang tài khoản người dùng do Google Workspace quản lý.

- Đình chỉ người dùng
- Đổi tên người dùng
- Đặt lại mật khẩu
- Bắt buộc thay đổi mật khẩu
- Thêm/xóa bí danh
- Xóa bỏ

Đặc quyền **Tạo** tự động cấp đặc quyền **Đọc** và **Cập nhật**. **Đặc quyền Cập nhật** hoặc **Xóa** tự động cấp đặc quyền **Đọc**.

Bạn có thể cho phép quản trị viên thực hiện hành động đối với tất cả người dùng trong tài khoản của mình hoặc chỉ người dùng trong các đơn vị tổ chức cụ thể. Để biết chi tiết, hãy chuyển đến Đặt người dùng làm quản trị viên.

Mẹo : Để cho phép quản trị viên xem nhóm của người dùng nhưng không chỉnh sửa họ, hãy cấp cho họ đặc quyền API bằng cách nhấp vào đặc quyền **Groups** > **Read** API

Đặc quyền dịch vụ

Mở rộng phần | Thu gọn tất cả

Cài đặt dịch vụ

*Đặc quyền **Cài đặt dịch vụ** không tự động cấp đặc quyền cho một số dịch vụ và cài đặt, chẳng hạn như vùng dữ liệu, Bảo mật dữ liệu, Google Vault và Trung tâm bảo mật.*

Quản trị viên có đặc quyền **Cài đặt dịch vụ** có thể bật hoặc tắt dịch vụ và thay đổi cài đặt dịch vụ. Áp dụng cho một số sản phẩm nhất định mà bạn đã thêm vào tài khoản của mình (các dịch vụ Google Workspace, chẳng hạn như Calendar và Drive), ứng dụng Marketplace và các dịch vụ miễn phí của Google, chẳng hạn như YouTube và Blogger.

Trung tâm cảnh báo

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ.***

Để biết mô tả về các đặc quyền và đề xuất tạo vai trò, hãy truy cập Cấp quyền truy cập vào trung tâm cảnh báo .

App Maker

Đặc quyền của App Maker không còn được dùng nữa. Để biết chi tiết, hãy xem Tắt App Maker .

Calendar

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ**.*

Quản trị viên có đặc quyền Lịch có thể tạo, chỉnh sửa và xóa tài nguyên. Họ không thể sửa đổi cài đặt chia sẻ của tài nguyên Lịch Google.

Quyền quản lý lịch:

- **Tất cả cài đặt** —Quản trị viên có thể truy cập và quản lý cài đặt chia sẻ, tài nguyên, Bảng thông tin chi tiết về phòng và cài đặt chung.
- **Xem cài đặt** —Quản trị viên chỉ có thể xem cài đặt lịch nhưng không thể chỉnh sửa chúng.
- **Tòa nhà và Tài nguyên** —Quản trị viên có thể tạo, chỉnh sửa và xóa tài nguyên lịch cũng như truy cập Bảng thông tin chi tiết về phòng.
- **Thông tin chi tiết về phòng** —Quản trị viên có thể xem và đặt bộ lọc cũng như điều chỉnh phạm vi ngày trên Bảng điều khiển thông tin chi tiết về phòng.

Quản lý tài nguyên —Quản trị viên có thể tạo, chỉnh sửa và xóa tài nguyên Lịch, tòa nhà và tính năng tài nguyên.
Xem tài nguyên —Quản trị viên có thể xem tài nguyên nhưng không thể chỉnh sửa chúng.
Lưu ý : Quản trị viên không thể giới hạn những hành động này ở các đơn vị tổ chức cụ thể.

Chrome Management

Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ**.
Quản trị viên có thể quản lý các chính sách và thiết bị Chrome của tổ chức bạn, bao gồm:

- Thiết lập người dùng
- Cài đặt thiết bị
- Các ứng dụng và tiện ích mở rộng của Chrome cũng như Managed Google Play trên thiết bị Chrome

Để biết thêm thông tin, hãy chuyển đến phần Ủy quyền vai trò quản trị viên trong Chrome.

Classroom

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ .***

Quản trị viên có đặc quyền **Lớp học** có thể bật hoặc tắt dịch vụ này cho người dùng. Họ cũng có thể:

- Đặt quyền của giáo viên và quyền truy cập của người giám hộ.
- Chọn người có thể tham gia lớp học và lớp nào họ có thể tham gia.
- Kiểm soát cách người dùng truy cập dữ liệu Lớp học của họ.
- Xuất điểm và bài tập từ Lớp học sang hệ thống thông tin của trường.

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*

Quản lý lớp học—Quản trị viên cấp cao có thể chỉ định người dùng có quyền truy cập lớp học tạm thời. Họ có thể giới hạn quyền truy cập lớp học vào các đơn vị tổ chức cụ thể.

Cloud Search

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ**.*

Quản trị viên có đặc quyền **Cloud Search** có thể:

- Cấp cho người dùng quyền truy cập vào Google Cloud Search.
- Bật hoặc tắt dịch vụ.

- Xem báo cáo về cách tổ chức sử dụng Cloud Search, bao gồm số lượng truy vấn tìm kiếm từ các loại thiết bị khác nhau và số lượng người dùng đang hoạt động.
- Quản lý cài đặt cho kho lưu trữ của bên thứ ba, chẳng hạn như cài đặt cho nguồn dữ liệu, nguồn nhận dạng và ứng dụng tìm kiếm. Quản trị viên cũng có quyền truy cập đọc hoặc ghi để lập chỉ mục.

Tìm hiểu về cách tạo vai trò quản trị viên Cloud Search cho nhà phát triển .

Contacts

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ**.*

Người đại diện liên hệ là người dùng có quyền truy cập và quản lý danh bạ cho người dùng khác. Quản trị viên có đặc quyền **Danh bạ** có thể xem, tạo hoặc xóa người được ủy quyền cho một người dùng cụ thể bằng cách sử dụng API Ủy quyền Danh bạ:

- **Delegates Read** – Quản trị viên có thể sử dụng API để liệt kê đại biểu cho một người dùng cụ thể. Tương đương với phạm vi OAuth https://www.googleapis.com/auth/admin.contact.delegation.readonly.
- **Delegates Write** – Quản trị viên có thể sử dụng API để tạo hoặc xóa đại biểu cho một người dùng cụ thể. Tương đương với phạm vi OAuth https://www.googleapis.com/auth/admin.contact.delegation.

Currents

*Chỉ đặc quyền **Cài đặt mới** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ**.*

Đặc quyền của quản trị viên đối với Currents

- **Cài đặt**—Quản lý cài đặt cho Currents
- **Thêm hàng loạt nhóm người dùng vào cộng đồn**—Quản trị viên có thể thêm người dùng trực tiếp vào cộng đồng Currents.
- **Truy cập các công cụ để quản lý luồng, thẻ và người dẫn đầu**—Kiểm duyệt nội dung trên Currents. Tìm hiểu thêm

Ngăn chặn mất dữ liệu - Data loss prevention (DLP)

*Chỉ đặc quyền **quy tắc Xem DLP** mới được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ***

.

Đặc quyền DLP:

- **Xem quy tắc DLP**—Quản trị viên có thể xem nhưng không thể sửa đổi hoặc tạo quy tắc DLP..
- **Quản lý quy tắc DLP**—Quản trị viên có thể xem, sửa đổi và tạo quy tắc DLP.

Bạn phải kích hoạt *cả hai* đặc quyền này để có toàn quyền truy cập vào việc tạo và chỉnh sửa quy tắc. Chúng tôi khuyên bạn nên tạo một vai trò tùy chỉnh có cả hai đặc quyền.

Vùng dữ liệu - Data regions

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*

Đặc quyền vùng dữ liệu:

- **Cài đặt vùng dữ liệu** —Quản trị viên có thể chọn lưu trữ dữ liệu theo chính sách vùng dữ liệu ở một vị trí địa lý cụ thể bằng cách sử dụng chính sách vùng dữ liệu. Để biết chi tiết, hãy chuyển đến Vùng dữ liệu: Chọn vị trí địa lý cho dữ liệu của bạn .
- **Báo cáo vùng dữ liệu** —Quản trị viên có thể xem tiến trình khi dữ liệu di chuyển từ vùng này sang vùng khác. Để biết chi tiết, hãy truy cập Xem tiến trình di chuyển vùng dữ liệu .

Bảo mật dữ liệu

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có thể quản lý các chính sách truy cập theo ngữ cảnh của tổ chức. Quản trị viên có thể kiểm soát các ứng dụng mà người dùng có thể truy cập dựa trên ngữ cảnh của họ, chẳng hạn như vị trí của họ hoặc liệu thiết bị của họ có tuân thủ chính sách của tổ chức bạn hay không.

Quyền quản lý bảo mật dữ liệu:

- **Quản lý cấp truy cập** —Quản trị viên có thể tạo cấp truy cập.
- **Quản lý quy tắc** —Quản trị viên có thể bật hoặc tắt quyền truy cập theo ngữ cảnh và chỉ định cấp truy cập cho ứng dụng.

Cài đặt thư mục

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có thể quản lý cài đặt và kiểm soát các thay đổi trong hồ sơ Thư mục để cho phép người dùng thực hiện các thay đổi đối với hồ sơ của họ, bao gồm tên, ảnh, giới tính và ngày sinh của họ

Đồng bộ thư mục - Directory Sync

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*

Đặc quyền đồng bộ hóa thư mục:

- **Quản lý cài đặt Đồng bộ hóa Thư mục** —Thêm, cập nhật và quản lý cài đặt Đồng bộ hóa Thư mục.
- **Đọc cài đặt đồng bộ hóa thư mục** —Xem nhưng không thay đổi cài đặtĐể biết thêm thông tin, hãy truy cập Đồng bộ hóa thư mụcDrive & Docs
  *Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*
  Quyền quản lý Google Drive và Docs:
- **Cài đặt** —Quản trị viên có thể quản lý tất cả cài đặt cho dịch vụ Drive và Tài liệu của tổ chức bạn. Bạn cần có đặc quyền này và đặc quyền Truyền dữ liệu để chuyển quyền sở hữu tệp Drive. Để biết chi tiết, hãy chuyển tới phần Chuyển tệp trên Drive sang chủ sở hữu mới .
- **Mẫu Tài liệu** —Quản trị viên có thể xóa và phân loại các mẫu trong thư viện mẫu Docs, Sheets, Slides, vaf Forms cũng như trong phần **Drive và Docs** của Bảng điều khiển dành cho quản trị viên. Khi việc gửi mẫu được đặt thành **Kiểm duyệt** trong Bảng điều khiển dành cho quản trị viên, quản trị viên có thể chấp nhận hoặc từ chối việc gửi mẫu. Khi gửi được đặt thành **Bị hạn chế** , quản trị viên có thể thêm mẫu vào thư viện. Để biết chi tiết, hãy đi tới Tạo mẫu Drive tùy chỉnh .
- **Di chuyển bất kỳ tệp hoặc thư mục nào vào bộ nhớ dùng chung** —Quản trị viên có thể di chuyển tệp và thư mục vào bộ nhớ dùng chung trong tổ chức của bạn. Tuy nhiên, quản trị viên không thể di chuyển tệp và thư mục từ bộ nhớ dùng chung này sang bộ nhớ dùng chung khác. Tìm hiểu thêm về các cấp truy cập bộ nhớ dùng chung
- **Quản lý nhãn** —Quản trị viên có thể tạo loại nhãn tùy chỉnh cho các tệp và thư mục trên Drive. Họ cũng có thể biết liệu nhãn có được sử dụng theo quy tắc lưu giữ của Google Vault, quy tắc phân loại dữ liệu hay quy tắc ngăn chặn mất dữ liệu (DLP) hay không. Tuy nhiên, họ không thể nhìn thấy quy tắc lưu giữ hoặc DLP trừ khi họ cũng có những đặc quyền đó. Để biết chi tiết, hãy đi tới Quản lý nhãn Drive .
- **Xem chi tiết về Google Sites mới** —Quản trị viên có thể xác định chủ sở hữu của trang web, xem ngày xuất bản lần cuối của trang web và yêu cầu quyền truy cập chỉnh sửa vào trang web.
  Quản lý Google Sites cổ điển —Quản trị viên có thể sử dụng Trình quản lý Sites cổ điển để xem, quản lý và di chuyển tất cả Google Sites cổ điển của tổ chức bạn. Tìm hiểu thêm
- GmailChỉ đặc quyền *Cài đặt mới* được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .

Quyền quản lý Gmail:

- **Cài đặt** —Quản lý tất cả cài đặt Gmail cho tổ chức của bạn.
- **Tìm kiếm nhật ký email** —Tìm kiếm nhật ký, khắc phục sự cố gửi và điều tra các vấn đề bảo mật liên quan đến email.
- **Truy cập Vùng cách ly dành cho quản trị viên** —Truy cập và quản lý email trong tất cả các vùng cách ly, bao gồm cả vùng cách ly mặc định.
- **Truy cập các vùng cách ly bị hạn chế** —Chỉ truy cập và quản lý email trong các vùng cách ly được liên kết với các nhóm mà quản trị viên thuộc về.

Google Chat và Hangouts

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có thể đọc và sửa đổi các tùy chọn cài đặt cho Google Chat, chẳng hạn như lưu cuộc trò chuyện và cho phép trò chuyện với những người bên ngoài hoặc tổ chức của bạn.

Google Cloud Print

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*
Quản trị viên có đặc quyền này có thể thiết lập và quản lý các dịch vụ Google Cloud Print cho tổ chức của họ, bao gồm cả việc in từ:

- Thiết bị Chrome và Trình duyệt Chrome trên máy tính Windows, Mac và Linux
- Phiên bản di động của các dịch vụ Google Workspace, chẳng hạn như Gmail
- Ứng dụng di động gốc của bên thứ ba

Để biết chi tiết, hãy truy cập In từ Chrome .

Google Hangouts

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có thể:

- Quản lý cài đặt
- Truy cập bảng điều khiển chất lượng cho Hangouts. Để biết chi tiết, hãy đi tới Theo dõi số liệu thống kê và chất lượng cuộc họp.

Google Meet

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có thể:

- Quản lý cài đặt
- Truy cập bảng điều khiển chất lượng cho Google Meet. Để biết chi tiết, hãy xem Theo dõi số liệu thống kê và chất lượng cuộc họp.

Phần cứng Google Meet

Đặc quyền này không có sẵn trừ khi tài khoản của bạn có ít nhất một giấy phép phần cứng Google Meet hoặc thiết bị đã đăng ký.

Quản trị viên có thể tạo vai trò người dùng và chỉ định đặc quyền để cho phép xem và quản lý các thiết bị phần cứng Google Meet với nhiều cấp độ truy cập vào dữ liệu và chức năng. Việc cấp quyền truy cập vào đặc quyền gốc cũng sẽ cấp quyền truy cập vào bất kỳ đặc quyền con lồng nhau nào bên dưới đặc quyền đó trong cây.

Phân cấp đặc quyền

- Quản lý phần cứng và lịch của Google Meet
  - Quản lý phần cứng Google Meet
  - Quản lý thiết bị
  - Xem thiết bị
- Quản lý cài đặt đơn vị tổ chức
  - Xem cài đặt đơn vị tổ chức
- Thực hiện hành động
  - Thực hiện các lệnh của thiết bị
  - Quản lý cuộc họp trên thiết bị
- Hủy cấp phép phần cứng Google Meet
- Quản lý phân công lịch
- Đăng ký phần cứng Google Meet

Mô tả chi tiết

- **Quản lý phần cứng và lịch của Google Meet**– Quản trị viên có toàn quyền truy cập vào tất cả dữ liệu và chức năng có sẵn của thiết bị phần cứng Meet, ngoại trừ Đăng ký phần cứng Google Meet. Quản trị viên có thể truy cập và xem tất cả lịch của người dùng và tài nguyên.

- **Quản lý phần cứng Google Meet**– Quản trị viên có quyền truy cập vào tất cả dữ liệu và chức năng hiện có của thiết bị phần cứng Meet, ngoại trừ Đăng ký phần cứng Google Meet và Quản lý phân công lịch.
- **Quản lý thiết bị** – Quản trị viên có thể sửa đổi tất cả cài đặt thiết bị riêng lẻ ngoài việc gán lịch; cũng cấp đặc quyền Xem thiết bị.
- **Xem thiết bị** – Quản trị viên có quyền truy cập chỉ đọc vào dữ liệu thiết bị, bao gồm lịch sử sự cố và chức năng xuất dữ liệu nhóm; bắt buộc để có thể truy cập chức năng lưu trữ các trang bằng nhiều đặc quyền khác (bao gồm Quản lý phân công lịch, Thực hiện các hành động và các đặc quyền con của nó cũng như Hủy cấp phép phần cứng Google Meet).
- **Quản lý cài đặt đơn vị tổ chức**– Quản trị viên có thể chỉnh sửa cài đặt phần cứng Google Meet được kiểm soát ở cấp đơn vị tổ chức và di chuyển thiết bị giữa các đơn vị tổ chức.
- **Xem cài đặt đơn vị tổ chức** – Quản trị viên có thể xem cài đặt phần cứng Google Meet được kiểm soát ở cấp đơn vị tổ chức.
- **Thực hiện hành động** – Quản trị viên có thể thực hiện bất kỳ hành động nào trong hai đặc quyền con: Quản lý cuộc họp trên thiết bị và Thực hiện lệnh trên thiết bị.
- **Quản lý cuộc họp trên thiết bị** – Quản trị viên có thể kết nối với cuộc họp từ xa và tắt tiếng hoặc kết thúc cuộc gọi đang diễn ra.
- **Thực hiện lệnh thiết bị** – Quản trị viên có thể khởi động lại thiết bị hoặc kích hoạt kiểm tra chẩn đoán.
- **Hủy cấp phép phần cứng Google Meet**– Quản trị viên có thể hủy đăng ký một thiết bị, khiến dữ liệu của thiết bị đó bị xóa và giấy phép của thiết bị đó bị thu hồi.
- **Quản lý phân công lịch**– Quản trị viên có thể phân công lịch cá nhân hoặc lịch phòng cho thiết bị.
- **Đăng ký phần cứng Google Meet**– Hoạt động cùng với chính sách đặc quyền Yêu cầu đăng ký. Khi chính sách này được bật, chỉ những người dùng có đặc quyền này mới có thể đăng ký thiết bị phần cứng Meet mới trong tổ chức của bạn. Để biết chi tiết, hãy xem Đăng ký thiết bị của bạn .

Lưu ý : Quản trị viên không thể giới hạn các đặc quyền này đối với các thiết bị trong đơn vị tổ chức cụ thể tại thời điểm này.

Google Vault

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có thể xem tất cả các vấn đề và quản lý các vấn đề, lưu giữ, tìm kiếm, xuất, chính sách lưu giữ và kiểm tra. Để biết chi tiết, hãy đi tới Hiểu và cấp đặc quyền của Vault .

Google Workspace Marketplace

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có thể kiểm soát những ứng dụng nội bộ hoặc bên thứ ba mà người dùng có thể cài đặt từ Marketplace bằng các tùy chọn sau:

- **Cho phép người dùng cài đặt và chạy bất kỳ ứng dụng nào từ Marketplace**
- **Cho phép người dùng chỉ cài đặt và chạy các ứng dụng đã chọn từ Marketplace**
- **Không cho phép người dùng cài đặt và chạy ứng dụng từ Marketplace**

Để biết chi tiết về quyền truy cập của người dùng vào ứng dụng Marketplace, hãy xem Quản lý ứng dụng Marketplace trên danh sách cho phép của bạn .

Groups for Business

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*
Quản trị viên có đặc quyền này có thể đọc và sửa đổi cài đặt của Groups for Business, bao gồm:

- Ai có thể tạo nhóm.
- Liệu những người bên ngoài tổ chức của bạn có thể xem, tìm kiếm và đăng lên nhóm của bạn hay không.
- Giá trị mặc định cho những người có thể xem cuộc hội thoại trong nhóm.

Jamboard

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*
Quản trị viên có đặc quyền này có thể bật hoặc tắt dịch vụ Jamboard cho tổ chức của bạn. Nếu bạn có Jamboards được cấp phép thực tế, bạn sẽ có quyền truy cập vào các cài đặt bổ sung, bao gồm:

- Liệu chủ sở hữu mứt có thể được chỉ định mà không cần xác nhận qua email hay không.
- Thông báo bảo vệ màn hình và giá trị thời gian chờ cho tất cả Jamboard.

Lưu ý: Để xem và quản lý từng Jamboard, quản trị viên cần có đặc quyền Quản lý Jamboard .

Quản lý Jamboard

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có thể thực hiện các tác vụ như xem và chỉnh sửa cài đặt Jamboard cũng như thiết lập thiết bị.

Looker Studio

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có thể quản lý cài đặt Looker Studio, bao gồm xem, chia sẻ cũng như tùy chỉnh trang tổng quan và báo cáo. Tìm hiểu thêm về Looker Studio .

Quản lý Google Play

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*

Đặc quyền này cũng được liệt kê là “Google Managed Play”. Quản trị viên có đặc quyền này có thể:

- Phân phối nội bộ ứng dụng Android cho người dùng.
- Tải ứng dụng riêng tư lên cửa hàng Google Play.
- Sử dụng các gói ứng dụng Android (APK) được lưu trữ bên ngoài Google Play.

Quản lý thiết bị di động

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có toàn quyền kiểm soát các thiết bị được liệt kê trong Bảng điều khiển dành cho quản trị viên của bạn và có thể:

- Quản lý cài đặt và chính sách của thiết bị.
- Thực hiện tất cả các hoạt động quản lý, chẳng hạn như phê duyệt, chặn, xóa và xóa thiết bị.
- Xuất bản và quản lý ứng dụng di động.

Password Vault

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có thể thiết lập và quản lý các ứng dụng được lưu trữ bằng mật khẩu.

Chủ đề liên quan

- Bắt đầu với các ứng dụng được lưu trữ bằng mật khẩu

- Chỉ định đặc quyền quản trị viên cho dịch vụ ứng dụng được lưu trữ bằng mật khẩu

Pinpoint

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền **Pinpoint** có thể bật hoặc tắt dịch vụ này cho người dùng. Họ cũng có thể đặt xem người dùng có thể sao chép tệp từ Google Drive sang Pinpoint hay không.

Secure LDAP

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có thể quản lý dịch vụ LDAP an toàn và thêm hoặc xóa ứng dụng khách LDAP. Tìm hiểu thêm

Quan trọng: Dịch vụ LDAP bảo mật chỉ khả dụng cho quản trị viên có đặc quyền Quản trị viên cấp cao—do đó, Quản trị viên cấp cao không thể chỉ định đặc quyền LDAP bảo mật cho quản trị viên được ủy quyền. Khi thiết lập vai trò quản trị viên cho người dùng của bạn, vui lòng bỏ qua cài đặt này.

Security Center

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có quyền truy cập vào thông tin và phân tích bảo mật nâng cao, đồng thời bổ sung khả năng hiển thị và kiểm soát các vấn đề bảo mật ảnh hưởng đến tổ chức của họ.

Quản trị viên cấp cao có quyền truy cập tự động vào tất cả các tính năng của trung tâm bảo mật, bao gồm bảng thông tin bảo mật, trang tình trạng bảo mật và công cụ điều tra. Bạn có thể cấp cho quản trị viên quyền truy cập vào một tính năng của trung tâm bảo mật cụ thể (ví dụ: chỉ bảng điều khiển bảo mật) bằng cách cấp cho họ các đặc quyền quản trị cần thiết để truy cập vào tính năng này.

Chủ đề liên quan

- Đặc quyền quản trị viên cho trung tâm bảo mật
- Sử dụng bảng điều khiển bảo mật
- Bắt đầu với trang tình trạng bảo mật
- Giới thiệu về công cụ điều tra bảo mật

Cài đặt thiết bị dùng chung

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có thể quản lý tất cả các cấu hình thiết bị phổ biến. Họ có thể thiết lập mạng riêng ảo (VPN), Wi-Fi và mạng Ethernet cho thiết bị di động, Chrome và Chromebox dành cho hội họp.

Sites

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có thể đọc và sửa đổi cài đặt cho Trang web, chẳng hạn như liệu người dùng có thể tạo và chỉnh sửa trang web hay không và liệu các trang web có thể được chia sẻ ra bên ngoài tổ chức của bạn hay không.

Lưu ý : Kiểm tra các đặc quyền bổ sung cho Google Sites và Google Sites cổ điển trong đặc quyền Drive và Docs .

Storage

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có thể mở trang Bộ nhớ trong Bảng điều khiển dành cho quản trị viên và đặt giới hạn bộ nhớ. Tuy nhiên, để xem dữ liệu lưu trữ cần có thêm đặc quyền. Để biết danh sách đầy đủ, hãy xem mô tả về vai trò Quản trị viên bộ nhớ .

Trust Rules

Các quyền quy định tin cậy để quản lý việc chia sẻ Drive:

- **Xem Quy tắc tin cậy** —Quản trị viên có thể đọc danh sách quy tắc tin cậy trong danh sách Quy tắc. Để xem chi tiết cài đặt quy tắc, quản trị viên cũng cần có đặc quyền Đọc đơn vị tổ chức .
- **Quản lý quy tắc tin cậy** —Chỉ đặc quyền này không cung cấp quyền truy cập vào bất kỳ cài đặt nào trong Bảng điều khiển dành cho quản trị viên. Để quản lý các quy tắc tin cậy, quản trị viên cần có các đặc quyền sau:
  - Để bật hoặc tắt quy tắc tin cậy, quản trị viên cần có đặc quyền **Quản lý quy tắc tin cậy** và Drive & Docs Settings .

- Để tạo, chỉnh sửa hoặc xóa quy tắc tin cậy, quản trị viên cần có các **đặc quyền Xem quy tắc tin cậy** , **Quản lý quy tắc tin cậy** , Drive & Docs > Settings, Groups > Read, and Organizational Units > Read
- Để xóa các quy tắc tin cậy, quản trị viên cần có các đặc quyền **Xem quy tắc tin cậy** , **Quản lý quy tắc tin cậy** và Cài đặt Drive & Docs > Settings.

Work Insights

*Đặc quyền này **không** được chọn tự động cùng với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có thể truy cập dữ liệu trên bảng thông tin Work Insights. Dữ liệu chỉ có sẵn cho các nhóm đã bật Work Insights.

Bạn có thể cho phép người dùng xem dữ liệu của tất cả các nhóm có sẵn hoặc chỉ các nhóm cụ thể, bao gồm các đơn vị tổ chức, nhóm được ủy quyền hoặc các nhóm trong dòng báo cáo của người quản lý.

Chủ đề liên quan

- Kiểm soát dữ liệu nào có sẵn trong Work Insights
- Cấp quyền truy cập vào Thông tin chi tiết về công việc

YouTube

*Đặc quyền này được chọn tự động với đặc quyền **Cài đặt dịch vụ** .*

Quản trị viên có đặc quyền này có thể:

- Hạn chế các video YouTube có thể xem được trong tổ chức của bạn.
- Đặt các cấp độ truy cập YouTube khác nhau (nghiêm ngặt, vừa phải, không hạn chế) cho các đơn vị tổ chức khác nhau.

Để biết chi tiết, hãy xem Quản lý cài đặt YouTube của tổ chức bạn .