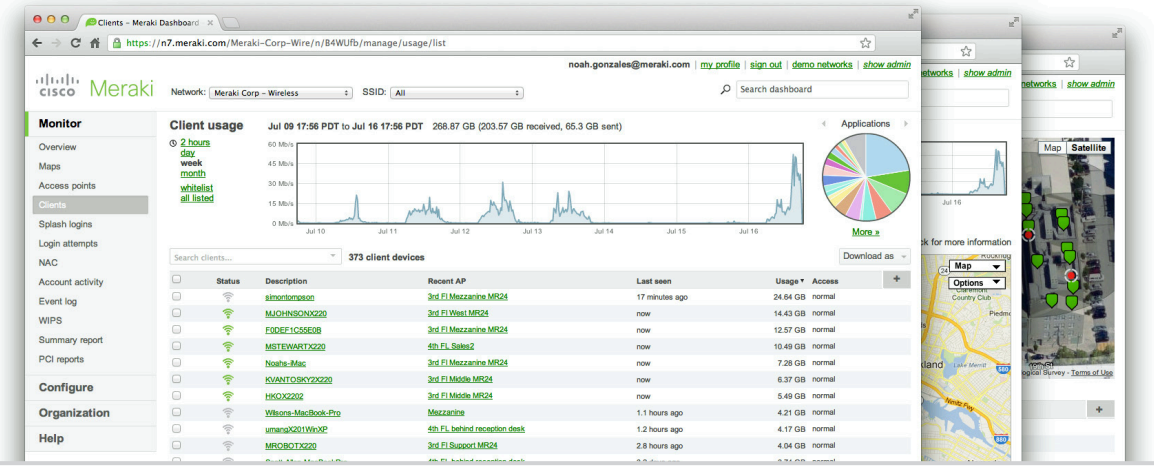
基于云端的 SaaS 网络管理平台管理



概述

基于基于云端的 SaaS 网络管理平台的管理功能可针对 Meraki 有线和无线网络硬件提供集中的可视性与可控性，帮助您告别无线控制器或重叠管理系统的成本和复杂性。通过将基于云端的 SaaS 网络管理平台管理功能集成到 Meraki 的整个产品组合，您将能够以直观的方式对任意规模的网络进行集中管理，并获得丰富的功能和可扩展性。

产品亮点

- 通过单个控制面板实现全网范围的统一可视性与可控性（包括无线设备、交换设备和安全设备）
- 轻松运维包含数万终端的大型网络
- 通过零接触调配实现快速部署
- 内置多站点网络管理工具
- 自动执行网络监控并发出警报
- 直观的界面无需进行成本高昂的培训或增加员工即可轻松操作
- 网络标记引擎 - 按标记搜索和同步设置
- 支持基于角色的管理和可审计的更改日志
- 由基于云端的 SaaS 网络管理平台持续推送功能更新
- 高度可用且安全（符合 PCI/HIPAA 标准）

由基于云端的 SaaS 网络管理平台管理的网络

Meraki 硬件产品从零构建，考虑了基于云端的 SaaS 网络管理平台管理需求。因此，它们在出厂时即预装集中可控性、第 7 层设备和应用可视性、基于 Web 的实时诊断、监控、报告等功能。

Meraki 网络部署简单快捷，无需任何培训或专门人员。此外，Meraki 还提供可完全控制设备、用户和应用的丰富功能集，可在不增加成本和复杂性的前提下，实现灵活的访问策略和充分的安全保护。

基于云端的 SaaS 网络管理平台管理可在功能、安全性和 可扩展性方面，满足各种规模的网络的实际需求。Meraki 可以从小型站点扩展到园区，乃至包含成千上万个站点的分布式网络。通过基于云端的 SaaS 网络管理平台进行自我调配的 Meraki 设备可在没有 IT 支持的情况下部署到分支机构。固件和安全签名更新通过 Web 无缝提供。借助基于云端的 SaaS 网络管理平台，只需点击一下，系统即会自动在分支机构之间建立安全的 VPN 隧道。

Meraki 采用可在 WAN 中断时保留本地网络功能的既安全又符合 PCI 和 HIPAA 标准的架构和容错设计，并且在高度安全的任务关键型网络应用中经过了实践检验。

基于云端的 SaaS 网络管理平台管理架构

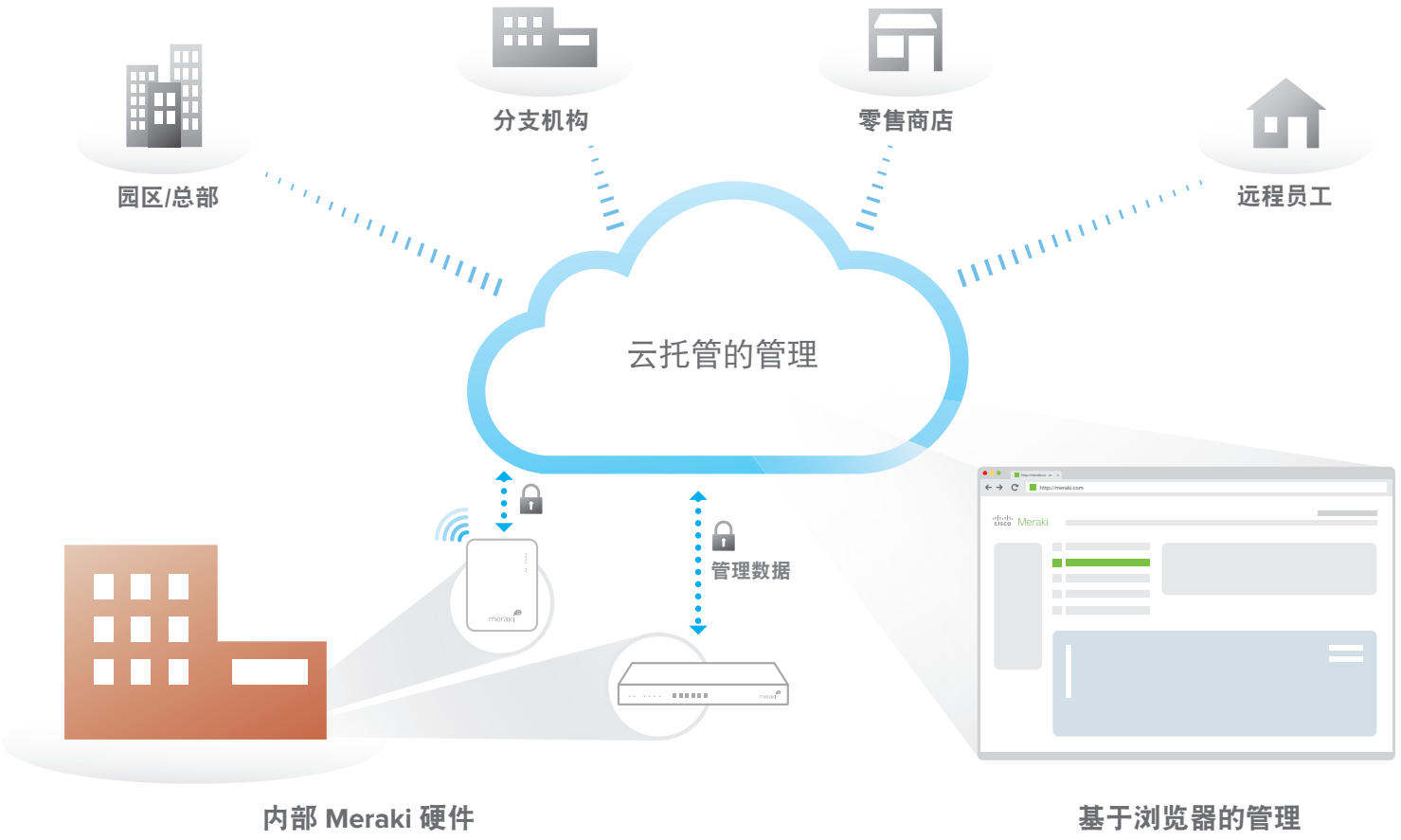
Meraki 的架构提供功能丰富的网络管理系统，免除了使用现场管理设备或 WiFi 控制器的需要。

包括无线接入点、以太网交换机和安全设备在内的所有 Meraki 设备都通过互联网连接到运行基于云端的 SaaS 网络管理平台的 Meraki 数据中心。这些连接通过 SSL 受到保护，利用提供实时可视性与可控性的专利协议，并将消耗的带宽控制在最低限度（通常为 1 kbps 或更少）。

Meraki 取代了传统的基于命令行的网络配置，它通过基于 Web 的内容丰富的控制面板，对世界各地数以万计的 Meraki 设备提供可视性与可控性。为扩展到大型分布式网络而设计的工具使策略更改、固件更新、部署新分支机构等操作变得简单便捷，而且无需考虑规模或位置。Meraki 的实时协议兼具内部管理应用的即时性与云应用的简便性和集中控制性。

每个 Meraki 设备都针对基于云端的 SaaS 网络管理平台管理进行了设计。具体来说，这意味着 Meraki 设备在设计上具备在网络边缘执行分组处理、QoS、第 3 至 7 层安全服务、加密等所需的内存和 CPU 资源。因此，不会有任何网络流量流经基于云端的 SaaS 网络管理平台，同时基于云端的 SaaS 网络管理平台在数据路径以外提供管理功能。这种架构确保只需添加更多终端即可增加网络容量，实现水平扩展，而且完全无需担心集中瓶颈或阻塞点。同样重要的一点是，所有分组处理均在本地执行，因此如果网络与基于云端的 SaaS 网络管理平台的连接中断，最终用户功能不会受到影响。

基于云端的 SaaS 网络管理平台旨在将计算和存储分布到位于不同地理位置的数据中心的独立服务器集群上。这样，任何服务器或数据中心的故障都不会影响客户或系统的其余部分。此外，Meraki 的数据中心设计已经过现场验证，可支持数以万计的终端。

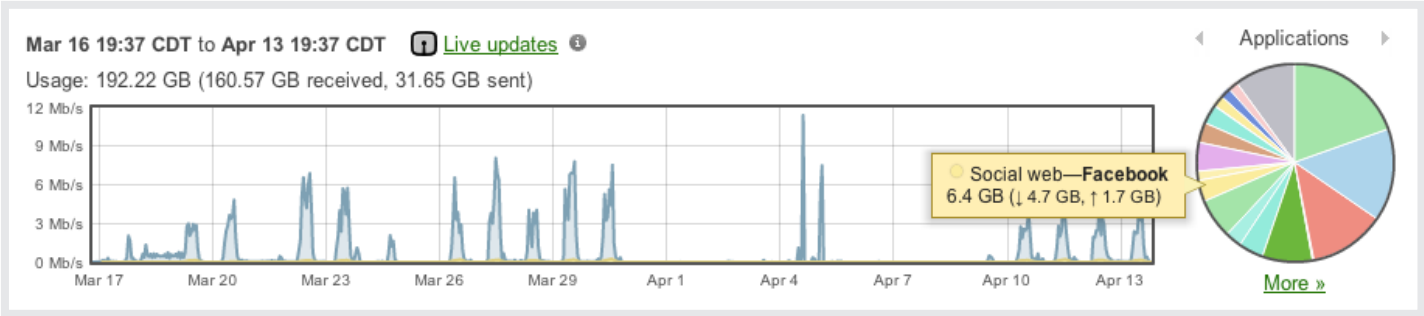


Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

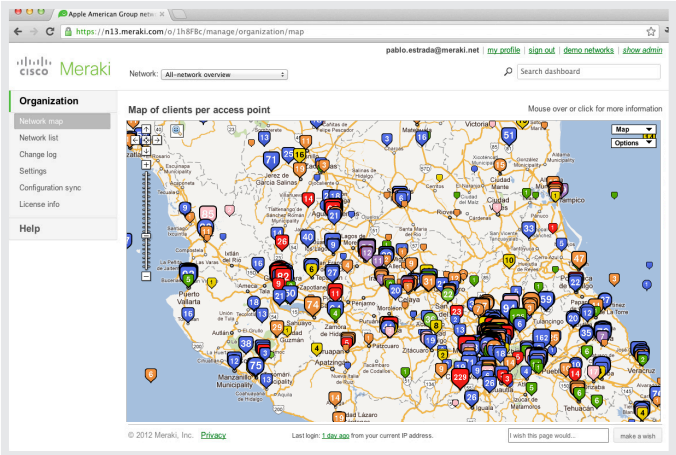
强大的洞察力和故障排除工具

基于云端的 SaaS 网络管理平台架构提供强大的洞察力，而且包括直接集成到控制面板中的现场工具，能够对性能、连接等进行即时分析。借助现场工具，网络管理员可无需再前往现场执行常规故障排除测试。对设备、用户和应用的可视性使管理员能够获得所需的信息，在当今要求严苛的网络环境中实施安全策略，实现所需性能。

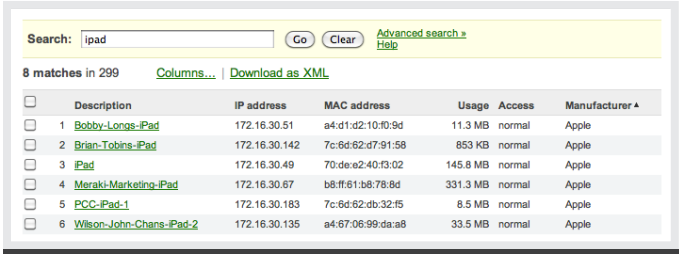
故障排除工具（例如 ping、traceroute、吞吐量，甚至实时数据包捕获）已直接集成到 Meraki 控制面板中，极大地缩短了问题解决时间，并支持远程故障排除，免除了派遣现场 IT 人员的需要。



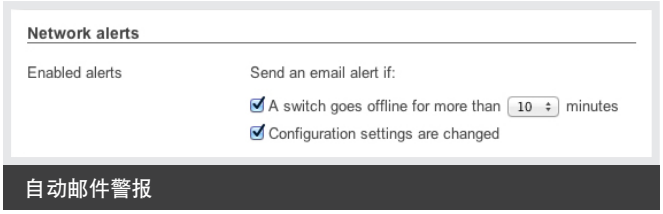
第 7 层应用可视性



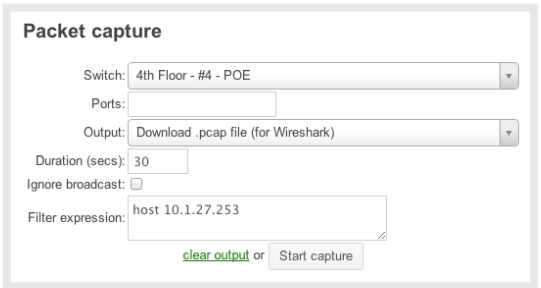
集成多站点管理



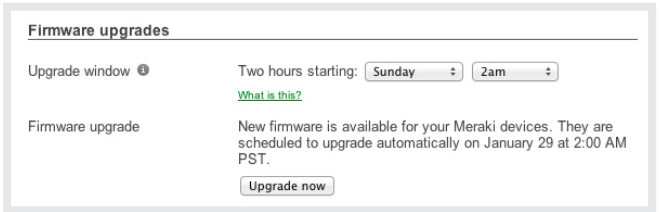
用户和设备指纹



自动邮件警报



实时故障排除工具

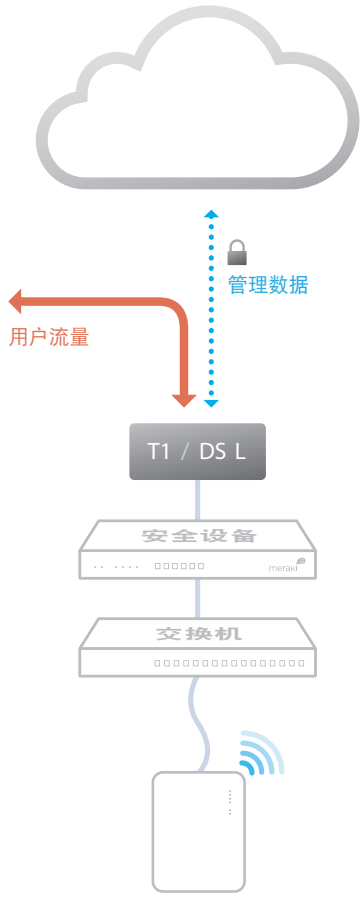


计划的固件更新

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

带外控制平面

Meraki 的带外控制平面实现了网络管理数据与用户数据的分离。管理数据（例如，配置、统计、监控等）通过安全的互联网连接从 Meraki 设备（无线接入点、交换机和安全设备）流到基于云端的 SaaS 网络管理平台。用户数据（Web 浏览、内部应用等）则不流经基于云端的 SaaS 网络管理平台，而是直接流到 LAN 上或 WAN 中的目的地。



带外控制平面的优势：

可扩展性
- 吞吐量不受限制：无集中控制器瓶颈
- 无需 MPLS 隧道即可添加设备或站点
- 增加交换容量无堆栈限制

可靠性
- 冗余的基于云端的 SaaS 网络管理平台服务提供高可用性
- 即使管理流量中断，网络仍能正常工作

安全性
- 不会有任何用户流量通过 Meraki 的数据中心
- 完全符合 HIPAA/PCI 标准

如果网络与基于云端的 SaaS 网络管理平台的连接中断，会发生什么情况？
由于 Meraki 采用带外架构，在 Meraki 无线接入点、交换机或安全设备无法与基于云端的 SaaS 网络管理平台服务进行通信的情况下（例如，由于暂时的 WAN 故障），大多数最终用户不会受到任何影响：

- 用户可以访问本地网络（打印机、文件共享等）
- 如果 WAN 连接可用，用户可以访问互联网
- 继续实施网络策略（防火墙规则、QoS 等）
- 用户可以通过 802.1X/RADIUS 进行身份验证，并可在无线接入点之间进行无线漫游
- 用户可以启动并更新 DHCP 租约
- 已建立的 VPN 隧道继续运行
- 本地配置工具可用（例如，设备 IP 配置）

无法连接基于云端的 SaaS 网络管理平台时，管理、监控和托管服务暂时都不可用：
- 配置和诊断工具不可用
- 使用统计信息存储在本地，直到重新建立与基于云端的 SaaS 网络管理平台的连接，彼时，使用统计信息会被推送到基于云端的 SaaS 网络管理平台
- 启动页面和相关功能不可用

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

Meraki 数据中心设计

基于云端的 SaaS 网络管理平台管理服务位于已通过 SAS70 类型 II 认证的一级数据中心中。这些数据中心具备先进的物理和网络安全性以及高可靠性设计。所有 Meraki 服务在多个独立数据中心之间进行复制，因此，面向客户的服务能够在数据中心发生灾难性故障的情况下快速故障切换。

冗余

- 五个在地理位置上分散的数据中心
- 每个客户的数据（网络配置和使用指标）在三个独立的数据中心之间进行复制
- 在数据中心之间进行实时数据复制（60 秒内）
- 夜间存档备份

可用性监控

- 全天候自动故障检测 — 每五分钟从不同位置测试所有服务器
- 多个运营团队之间的快速升级程序
- 具有 3 倍冗余的独立中断警报系统

灾难恢复

- 在发生硬件故障或自然灾害的情况下快速故障切换至热备用系统
- 即使与基于云端的 SaaS 网络管理平台服务的连接中断，带外架构仍能保留最终用户的网络功能
- 每周钻取的故障切换程序

基于云端的 SaaS 网络管理平台服务安全

- 全天候自动入侵检测
- 通过基于 IP 和端口的防火墙进行保护
- 按 IP 地址限制并通过公钥进行验证 (RSA) 的访问
- 无法通过密码访问系统
- 一旦发生配置更改，将自动向管理员发出警报

物理安全

- 高安全性磁卡钥匙和生物信息读取器控制设施出入
- 所有进出及机房均通过视频监控进行监控
- 安全卫士全天候监控流入或流出数据中心的所有流量，从而确保跟踪输入过程

带外架构

- 基于云端的 SaaS 网络管理平台中仅存储配置和使用统计信息
- 最终用户数据不流经数据中心
- 所有敏感数据（例如，密码）均以加密格式存储

灾难防备状态

- 数据中心采用先进的洒水灭火系统，并带有联锁装置以防止意外排水
- 柴油发电机在电力损耗的情况下可提供备用电源
- UPS 系统在完全断电的情况下可调节电量并确保有序关闭
- 每个数据中心拥有至少两家顶级运营商所提供的服务
- 对高架地板、机房和支撑系统提供抗震支撑
- 如果数据中心出现灾难性故障，服务将故障切换至其他在地理位置上独立的数据中心

环境控制

- 超额调配的 HVAC 系统提供冷却和湿度控制功能
- 地板系统专用于空气分配

认证

- Meraki 数据中心已通过 SAS70 类型 II 认证
- 已通过 PCI 等级 1 认证

服务级别协议

- Meraki 的基于云端的 SaaS 网络管理平台管理以 99.99% 运行时间 SLA 为后盾。有关详细信息，请参阅 www.meraki.com/trust。

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

面向管理员的安全工具

除了 Meraki 的安全带外架构和加强的数据中心之外，Meraki 还为管理员提供了大量用于实现其网络部署安全最大化的工具。这些工具可提供对 Meraki 网络的最佳保护、可视性和可控性。

双因素身份验证

双因素身份验证为组织的网络增加了一层额外的安全保护，其方法是要求想要登录基于云端的 SaaS 网络管理平台服务的管理员不仅提供用户名和密码，还提供手机号码。Meraki 的双因素身份验证实现使用安全、便捷和低成本的 SMS 技术：在管理员输入用户名和密码后，系统通过 SMS 向管理员发送一个一次性密码，管理员必须输入该密码才能完成身份验证。即便黑客已经猜到或得知管理员的密码也仍然无法访问组织的账户，因为管理员的手机不在黑客手上。Meraki 包括面向所有企业用户的双因素身份验证，并且不收取额外的费用。

密码策略

组织范围内用于 Meraki 账户的安全策略有助于保护对 Meraki 控制面板的访问。管理员可以通过这些工具：

- 强制定期更改密码（例如，每 90 天）
- 要求达到最低密码长度和复杂性
- 在登录尝试反复失败后将用户锁定
- 不允许密码重复使用
- 按 IP 地址限制登录

基于角色的管理

基于角色的管理允许主管针对组织的特定子集委派管理员，并指定他们是对报告和故障排除工具拥有只读权限，管理托管的访客接入，还是可以对网络进行配置更改。这可最大程度地减少意外或恶意错误配置的几率，并将错误限制到网络的孤立部分。

配置更改警报

在发生配置更改时，Meraki 系统可自动发送用户可读的邮件和短信警报，从而使整个 IT 组织能够及时更新策略。更改警报对于大型或分布式 IT 组织尤其重要。

配置和登录审计

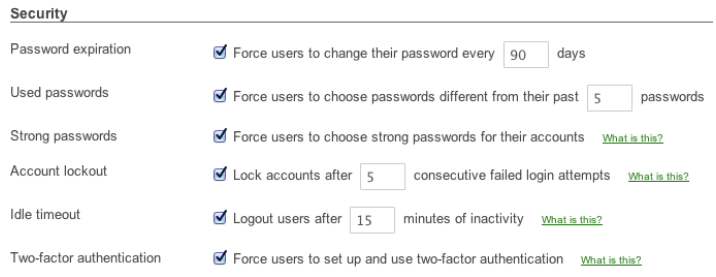
Meraki 会记录登录管理员的登录时间、IP 和大致位置（城市、省/市/自治区）。可搜索的配置更改日志指示所进行的具体配置更改、更改执行人员，以及发生更改的相关组织部分。

SSL 证书

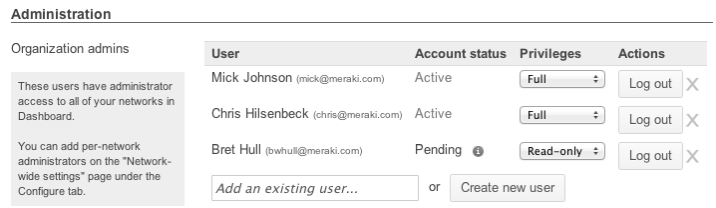
Meraki 账户只能通过 https 进行访问，确保管理员浏览器与基于云端的 SaaS 网络管理平台服务之间的所有通信都会加密。

空闲超时值

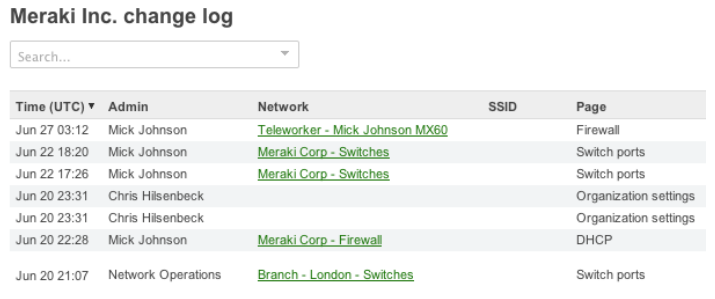
注销前 30 秒钟，系统会向用户显示一条允许他们延长会话时间的通知。时间到期后，系统将要求用户重新登录。



密码安全策略



基于角色的管理



配置更改审计

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com