GlobalProtect 管理员指南

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2020-2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 4, 2020

Table of Contents

GlobalProtect 概述 7
关于 GlobalProtect 组件 8
GlobalProtect 网络门户 8
GlobalProtect 网关 8
GlobalProtect App 8
GlobalProtect 支持哪些操作系统版本？ 10
关于 GlobalProtect 许可证 11

入门 13
为 GlobalProtect 创建接口和区域 14
在 GlobalProtect 组件间启用 SSL 16
关于 GlobalProtect 证书部署 16
GlobalProtect 证书最佳做法 16
将服务器证书部署至 GlobalProtect 组件 18

身份验证 23
关于 GlobalProtect 用户身份验证 24
支持的 GlobalProtect 身份验证方法 24
应用如何知道提供哪些凭据？ 26
应用如何知道提供哪些证书？ 26
设置外部身份验证 28
设置 LDAP 身份验证 28
设置 SAML 身份验证 30
设置 Kerberos 身份验证 35
设置 RADIUS 或 TACACS+ 身份验证 36
设置客户端证书身份验证 38
部署共享客户端证书进行身份验证 38
部署机器证书进行身份验证 38
部署特定用户的客户端证书进行身份验证 42
设置双重身份验证 45
使用证书和身份验证配置文件启用双重身份验证 45
使用一次性密码 (OTP) 启用双重身份验证 47
使用智能卡启用双重身份验证 51
使用软件令牌应用程序启用双因素身份验证 52
设置 strongSwan Ubuntu 和 CentOS 端点的身份验证 57
使用证书配置文件启用身份验证 57
使用身份验证配置文件启用身份验证 59
启用使用双因素身份验证进行身份验证 61
配置 GlobalProtect 以实现多因素身份验证通知 63
启用向 RADIUS 服务器交付 VSA 67
启用组映射 68

GlobalProtect 网关 71
GlobalProtect 网关概述 72
GlobalProtect 网关概念 73
网关的类型 73
多网关配置中的网关优先级 73

GlobalProtect MIB 支持 74
配置 GlobalProtect 网关的前提任务 75
配置 GlobalProtect 网关 76
在 GlobalProtect 网关上拆分隧道流量 85
根据访问路由配置拆分隧道 85
根据域和应用程序配置拆分隧道 88
从 GlobalProtect VPN 隧道排除视频流量 89

GlobalProtect 门户 91
GlobalProtect 门户概述 92
配置 GlobalProtect 门户的前提任务 93
设置 GlobalProtect 门户访问权限 94
定义 GlobalProtect 客户端身份验证配置 96
定义 GlobalProtect 代理配置 97
自定义 GlobalProtect 应用程序 102
自定义 GlobalProtect 门户登录、欢迎和帮助页面 115

GlobalProtect 应用程序 125
向最终用户部署 GlobalProtect 应用程序 126
下载 GlobalProtect 应用 127
在门户上载入应用更新 128
在 Web 服务器上载入应用更新 128
测试应用安装 129
下载和安装 GlobalProtect 移动应用 133
以透明方式部署应用设置 135
可自定义的应用设置 135
将应用设置部署到 Windows 端点 141
将应用设置部署到 macOS 端点 151

GlobalProtect 无客户端 VPN 155
无客户端 VPN 概述 156
支持的技术 158
配置无客户端 VPN 160
无客户端 VPN 故障排除 166

移动设备管理 171
移动设备管理概述 172
设置 MDM 与 GlobalProtect 的集成 175
使用受支持的第三方 MDM 管理 GlobalProtect 应用 175
使用其他第三方 MDM 管理 GlobalProtect 应用 326

用于 IoT 设备的 GlobalProtect 333
满足 IoT 要求的 GlobalProtect 334
为 IoT 设备配置 GlobalProtect 门户和网关 335
在 Android 上安装用于 IoT 的 GlobalProtect 338
在 Raspbian 上安装用于 IoT 的 GlobalProtect 341
在 Ubuntu 上安装用于 IoT 的 GlobalProtect 343
在 Windows 上安装用于 IoT 的 GlobalProtect 345
在 IoT 设备上下载并安装 MSIEXEC 文件 345

修改 IoT 设备上的注册表项（On-Demand（按需）或 Always On（始终打开））..... 345
修改 IoT 设备上的注册表项（Always On with Pre-logon（预登录时始终打开））..... 346

主机信息..... 349
关于主机信息..... 350
GlobalProtect 应用收集哪些数据？..... 350
GlobalProtect 应用程序在每种操作系统上会收集哪些数据？..... 352
网关如何使用主机信息实施策略？..... 359
用户如何知道其系统是否合规？..... 359
如何查看端点的状态？..... 360
配置基于 HIP 的策略实施..... 361
从端点收集应用程序和流程数据..... 369
重新分发 HIP 报告..... 375
阻止端点访问..... 377
配置 Windows User-ID 代理以收集主机信息..... 380
MDM 集成概述..... 380
收集的信息..... 380
系统要求..... 382
配置 GlobalProtect 以检索主机信息..... 382
解决 MDM 集成服务问题..... 385
使用主机信息隔离设备..... 387
识别并隔离受影响的设备 — 概述和许可证要求..... 387
查看隔离设备信息..... 387
从隔离列表中手动添加并删除设备..... 389
自动隔离设备..... 391
使用 GlobalProtect 和安全策略阻止访问隔离设备..... 394
从 Panorama 重新分发设备隔离信息..... 396

认证..... 399
启用并验证 FIPS-CC 模式..... 400
通过 Windows 注册表启用并验证 FIPS-CC 模式..... 400
通过 macOS 属性列表启用并验证 FIPS-CC 模式..... 402
FIPS-CC 安全功能..... 406
FIPS-CC 故障排除模式..... 407
查看并收集 GlobalProtect 日志..... 407
解决 FIPS-CC 模式问题..... 408

GlobalProtect 快速配置..... 411
远程访问 VPN（身份验证配置文件）..... 412
远程访问 VPN（证书配置文件）..... 415
带双重身份验证的远程访问 VPN..... 418
始终打开 VPN 配置..... 422
使用预登录远程访问 VPN..... 423
GlobalProtect 多网关配置..... 429
适用于内部 HIP 验证和基于用户的访问的 GlobalProtect..... 432
内部和外部网关混合配置..... 436
强制网络门户和对网络访问强制执行 GlobalProtect..... 441

GlobalProtect 架构 445
GlobalProtect 参考架构拓扑 446
GlobalProtect 网络门户 446
GlobalProtect 网关 446
GlobalProtect 参考架构功能 448
最终用户体验 448
管理和日志记录 448
监控和高可用性 448
GlobalProtect 参考架构配置 449
网关配置 449
门户配置 449
策略配置 449

GlobalProtect 加密 451
关于 GlobalProtect 密码选择 452
GlobalProtect 应用与网关之间的密码交换 453
GlobalProtect 加密参考 455
参考资料：GlobalProtect 应用加密函数 455
GlobalProtect 应用支持的 TLS 密码套件 455
用于建立 IPsec 隧道的密码 461
SSL API 462

GlobalProtect 概述

无论是在家中查阅电子邮件或在机场更新公司文档，当今多数员工的工作地点都在公司之外。随着员工机动性的增强，生产力和灵活性虽然得以提升，但同时也带来了巨大的安全挑战。每当用户携带其便携式计算机或智能手机离开公司，便意味着他们绕开了公司防火墙以及设计用于保护用户和网络的相关策略。通过将物理外围网络内强制执行的下一代基于防火墙的策略同样应用于所有用户（无论其身在何处），GlobalProtect™ 可有效解决因漫游用户引发的安全问题。

下列章节提供了有关 Palo Alto Networks 旗下 GlobalProtect 产品的概念信息，同时描述 GlobalProtect 的各大组件及各类部署场景：

> 关于 GlobalProtect 组件
> GlobalProtect 支持哪些操作系统版本？
> GlobalProtect 支持哪些功能？
> 关于 GlobalProtect 许可证

关于 GlobalProtect 组件

GlobalProtect 提供了用于管理移动员工，从而让所有用户进行安全访问而无论其使用何种端点或身在何处的完整基础架构。该基础架构包含下列组件：

- GlobalProtect 网络门户
- GlobalProtect 网关
- GlobalProtect App

GlobalProtect 网络门户

GlobalProtect 门户提供了针对 GlobalProtect 基础架构的管理功能。参与 GlobalProtect 网络的每个端点都会从门户收到配置信息，其中包括可用网关的相关信息以及连接到 GlobalProtect 网关时可能需要的任何客户端证书的相关信息。此外，门户还控制 GlobalProtect 应用程序软件的行为，以及向 macOS 和 Windows 端点的分发（在移动端点上，GlobalProtect 应用程序通过 Apple App Store 向 iOS 端点分发，通过 Google Play 向 Android 端点和 Chromebooks 分发，通过 Microsoft Store 向 Windows 10 UWP 端点分发）。如果您正在使用主机信息配置文件 (HIP) 功能，则门户还会定义将从主机采集哪些信息，其中包括所需的任何自定义信息。您可以在任何 Palo Alto Networks 下一代防火墙的接口上配置 GlobalProtect 门户的访问权限。

GlobalProtect 网关

GlobalProtect 网关为从 GlobalProtect 应用发出的通信提供安全实施。此外，如果启用了 HIP 功能，该网关还将根据应用程序提交的原始主机数据生成 HIP 报告，并将该信息用于策略实施。您可以配置不同的网关类型，从而为您的远程用户提供安全强制和/或虚拟专用网络 (VPN) 访问，或应用安全策略访问内部资源。

您可以在 Palo Alto Networks 下一代防火墙的任何接口上配置 GlobalProtect 网关。您可以在同一防火墙上同时运行网关和门户，或是在企业内部署多个分散的网关。

GlobalProtect App

GlobalProtect 应用程序软件运行于端点上。它允许用户通过已部署的 GlobalProtect 门户和网关访问网络资源。

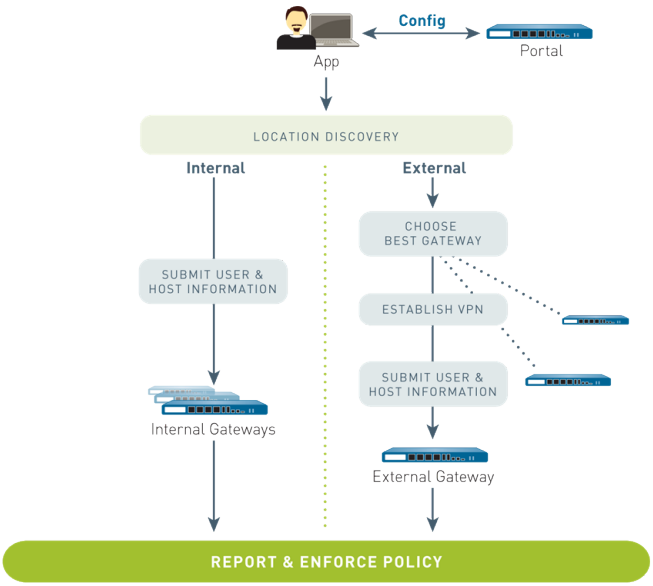
用于 Windows 和 mac OS 端点的 GlobalProtect 应用程序通过 GlobalProtect 门户进行部署。通过门户上所定义的客户端配置，您可以配置应用程序的行为；例如，允许用户查看哪些选项卡。有关详情，请参阅定义 GlobalProtect 代理配置、自定义 GlobalProtect 应用以及部署 GlobalProtect 应用程序软件。

用于移动端点（iOS、Android 和 Windows UWP）的 GlobalProtect 应用程序通过端点官方商店获取，即，从 Apple App Store 获取 iOS 版，从 Google Play 获取 Android 版，以及从 Microsoft Store 获取 Windows UWP 版。或者，您可以使用 AirWatch 部署 GlobalProtect 移动应用，这是一个第三方移动端点管理系统.

有关详情，请参阅 GlobalProtect 支持哪些操作系统版本？。

下图阐述了 GlobalProtect 门户、网关和应用如何协同工作，从而让所有用户进行安全访问，而无论其使用何种端点或身在何处。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

GlobalProtect 支持哪些操作系统版本？

常见的台式机、笔记本电脑、平板电脑和智能手机均支持 GlobalProtect 应用程序。我们建议您在运行 PAN-OS 6.1 或更高版本的防火墙上配置 GlobalProtect，建议最终用户在端点安装仅受支持的 GlobalProtect 应用版本。最低 GlobalProtect 应用版本因操作系统而异；要确定适用于特定操作系统的最低 GlobalProtect 应用版本，请参阅 Palo Alto Networks® 兼容性矩阵中的下列主题：

- 我可在何处安装 GlobalProtect 应用？
- 哪些 X-Auth IPSec 客户端受支持？

旧版本的 GlobalProtect 应用仍受随同其发布的操作系统和 PAN-OS 版本支持。对于最低 PAN-OS 版本支持，请参阅软件更新站点上与特定版本相对应的 GlobalProtect 应用程序发行说明。

© 2019 Palo Alto Networks, Inc.

关于 GlobalProtect 许可证

如果您想使用 GlobalProtect 以通过单个或多个内部/外部网关提供安全的远程访问或 VPN 解决方案，则无需使用任何 GlobalProtect 许可证。但是，若要使用一些更高级的功能，例如 HIP 检查和关联的内容更新，GlobalProtect 移动应用支持，或 IPv6 支持，则需要购买年度 GlobalProtect 订阅。运行执行以下任务的网关的每个防火墙都必须安装该许可证：

- 执行 HIP 检查
- 支持用于移动端点的 GlobalProtect 应用
- 支持用于 Linux 端点的 GlobalProtect 应用
- 支持用于 IoT 端点的 GlobalProtect 应用
- 提供 IPv6 连接
- 根据目的域、应用程序进程名、或 HTTP/HTTPS 视频流应用程序拆分隧道流量。
- 支持添加受影响的设备到隔离列表。
- 支持使用网关上的端点序列号识别受管设备

对于 GlobalProtect 无客户端 VPN，还需要在从 GlobalProtect 门户托管无客户端 VPN 的防火墙上安装 GlobalProtect 订阅。您还需要 **GlobalProtect Clientless VPN**（**GlobalProtect** 无客户端 **VPN**）动态更新才能使用此功能。

功能	需要订阅吗？
单个外部网关（Windows 和 MacOS）	—
单个或多个内部网关	—
多个外部网关	—
物联网 (IoT) 设备	✓
HIP 检查	✓
使用网关上的端点序列号识别受管设备	✓
基于端点状态的 HIP 策略实施	✓
适用于运行 Windows 和 macOS 的端点的应用程序	—
适用于运行 iOS、Android、Chrome OS 和 Windows 10 UWP 的端点的应用程序	✓
适用于运行 Linux 的端点的应用程序	✓
适用于运行 IoT 的端点的应用程序	✓
适用于外部网关的 IPv6	✓
适用于内部网关的 IPv6 （变更为默认行为 — 从 4.1.3 版本的 GlobalProtect 应用开始，此用例将不再需要订阅 GlobalProtect ）	—

© 2019 Palo Alto Networks, Inc.

功能	需要订阅吗？
无客户端 VPN	✓
根据目的域、客户端进程和视频流应用程序拆分隧道	✓
拆分 DNS	✓
添加受影响的设备到隔离列表	✓

有关在防火墙上安装许可证的信息，请参阅激活许可证。

入门

要使用 GlobalProtect™，您必须对允许所有组件进行通信的基础结构进行设置。就基础层面而言，即设置 GlobalProtect 最终用户为访问门户和网关而须连接至的接口和区域。由于 GlobalProtect 组件通过安全通道进行通信，因此须在各类组件上获取并部署所需的 SSL 证书。以下各节将指导您完成 GlobalProtect 基础架构设置：

> 为 GlobalProtect 创建接口和区域
> 在 GlobalProtect 组件间启用 SSL

为 GlobalProtect 创建接口和区域

须为 GlobalProtect 基础结构配置下列接口和区域：

- **GlobalProtect** 门户 — 需为 GlobalProtect 应用程序连接提供第三层接口或回环接口。如果门户和网关位于同一防火墙，则可使用同一接口。门户须位于可从网络外部访问的区域内；例如 DMZ。
- **GlobalProtect** 网关 — 网关的接口和区域要求取决于是否正按下列方法配置外部网关或内部网关：
  - 外部网关 — 需为应用程序提供第三层接口或回环接口以及逻辑隧道接口，以便建立连接。第三层/回环接口须位于外部区域内，例如 DMZ。隧道接口可与连接至内部资源的接口位于同一区域（例如`trust`）内。为了增强安全性和可视性，您可创建一个单独区域，例如 `corp-vpn`。如果为隧道接口创建单独区域，则需创建安全策略以便在 VPN 区域和信任区域间启用通信流。
  - 内部网关 — 需在信任区域内提供第三层接口或回环接口。此外，还可选择性创建用于访问内部网关的隧道接口。

有关如何使用回环接口以通过不同端口和地址访问 *GlobalProtect* 的提示，请参阅能否将 GlobalProtect 门户页面配置为可通过任意端口进行访问？

有关门户和网关的详细信息，请参阅关于 GlobalProtect 组件。

STEP 1 | 为计划部署的所有门户和/或网关配置第三层接口。

如果网关和门户位于同一防火墙，则可为二者使用单个接口。

最佳做法是为门户和网关使用静态 *IP* 地址。

请勿在已配置 *GlobalProtect* 门户或网关的接口上附加允许 *HTTP*、*HTTPS*、*Telnet* 或 *SSH* 的接口管理配置文件，因为这样可以从 *Internet* 访问管理界面。按照安全管理访问的最佳实践确保您以防止成功攻击的方式保护对防火墙的管理访问权限。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）或 **Network**（网络）> **Interfaces**（接口）> **Loopback**（回环），然后选择要为其配置 GlobalProtect 的接口。在本示例中，我们将 `ethernet1/1` 配置为门户接口。
2. （仅限以太网）将 **Interface Type**（接口类型）设置为 **Layer3**（第 3 层）。
3. 在 **Config**（配置）选项卡上，按下列方法选择门户或网关接口所属的 **Security Zone**（安全区域）：
   - 将门户和外部网关置于不可信区域内（例如，`l3-untrust`），以便网络外的主机进行访问。
   - 将内部网关置于内部区域内；例如，`l3-trust`。
   - 如果尚未创建区域，添加 **New Zone**（新区域）。在“区域”对话框中，为新区域定义 **Name**（名称），然后单击 **OK**（确定）。
4. 选择默认 **Virtual Router**（虚拟路由器）。
5. 为接口分配一个 IP 地址：
   - 对于 IPv4 地址，选择 **IPv4**，**Add**（添加）IP 地址和子网掩码并分配给接口，例如 203.0.11.100/24。
   - 对于 IPv6 地址，选择 **IPv6**，**Enable IPv6 on the interface**（在接口上启用 **IPv6**），**Add**（添加）IP 地址和子网掩码并分配给接口，例如 2001:1890:12f2:11::10.1.8.160/80。
6. 单击 **OK**（确定）以保存接口配置。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 在承载 GlobalProtect 网关的防火墙上，配置用于终止 GlobalProtect 应用程序所建立 VPN 隧道的逻辑隧道接口。

除非需要动态路由，否则无需为隧道接口配置 *IP* 地址。此外，为隧道接口分配 *IP* 地址有助于对连通性问题进行故障排除。

确保在 *VPN* 隧道终止的区域内启用用户 *ID*。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道）并 **Add**（添加）隧道接口。
2. 在 **Interface Name**（接口名称）字段中，输入数字后缀，例如 **.2**。
3. 在 **Config**（配置）选项卡上，按下列方法为 VPN 隧道终止选择 **Security Zone**（安全区域）：
   - 要将信任区域用作隧道的终止点，请从下拉列表中选择该区域。
   - （推荐）要为 VPN 隧道终止创建单独区域，请单击 **New Zone**（新区域）。在区域对话框中，定义新区域的 **Name**（名称）（如`corp-vpn`），**Enable User Identification**（启用用户标识），然后单击 **OK**（确定）。
4. 将 **Virtual Router**（虚拟路由器）设置为 **None**（无）。
5. 为接口分配一个 IP 地址：
   - 对于 IPv4 地址，选择 **IPv4**，**Add**（添加）IP 地址和子网掩码并分配给接口，例如 203.0.11.100/24。
   - 对于 IPv6 地址，选择 **IPv6**，**Enable IPv6 on the interface**（在接口上启用 **IPv6**），**Add**（添加）IP 地址和子网掩码并分配给接口，例如 2001:1890:12f2:11::10.1.8.160/80。
6. 单击 **OK**（确定）以保存接口配置。

STEP 3 | 如果已为 VPN 连接的隧道终止单独创建区域，则需创建安全策略以便在 VPN 区域和信任区域间启用通信流。

例如，下列策略规则可在 `corp-vpn` 域和 `l3-trust` 域间启用通信。

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 4 | **Commit**（提交）配置。

© 2019 Palo Alto Networks, Inc.

在 GlobalProtect 组件间启用 SSL

GlobalProtect 组件间的所有交互均通过 SSL/TLS 连接实现。因此，在配置每个组件前须生成并/或安装必要的证书，以便在配置中引用相应的证书。下列章节描述了针对各类 GlobalProtect 证书所支持的证书部署方法、描述和最佳实践准则，同时提供了生成和部署必要证书的相关指导：

- 关于 GlobalProtect 证书部署
- GlobalProtect 证书最佳做法
- 将服务器证书部署至 GlobalProtect 组件

关于 GlobalProtect 证书部署

要为 GlobalProtect 组件部署服务器证书，有三种基本方法：

- （推荐）第三方证书和自签名证书组合 — 由于 GlobalProtect 应用程序将在 GlobalProtect 配置前访问门户，因此应用程序须信任证书以便建立 HTTPS 连接。
- 企业证书颁发机构 — 如果已取得个人的企业 CA，则可使用该 CA 为所有 GlobalProtect 组件颁发证书，然后将其导入至承载门户和网关的防火墙上。在此情况下，还须确保端点信任用于为其必须连接至的 GlobalProtect 服务颁发证书的根 CA 证书。
- 自签名证书 — 可在门户上创建自签名证书，并将其用于为所有 GlobalProtect 组件颁发证书。但由于该解决方案的安全性不及其他选项，因此不推荐使用。如果确实需要选择该选项，则最终用户在首次连接至门户时将出现证书错误。要避免此问题，可向所有端点手动部署自签名根 CA 证书，或选用某种集中式部署；例如，Active Directory 组策略对象 (GPO)。

GlobalProtect 证书最佳做法

根据计划使用的功能，下表对所需 SSL/TLS 证书进行了总结：

证书	使用情况	颁发流程/最佳做法
CA 证书	用于签署向 GlobalProtect 组件颁发的证书。	如果计划使用自签名证书，请使用专用 CA 服务器或 Palo Alto Networks 防火墙生成 CA 证书，然后颁发由 CA 或中间 CA 签名的 GlobalProtect 门户和网关证书。
门户服务器证书	允许 GlobalProtect 应用建立与门户的 HTTPS 连接。	• 该证书在 SSL/TLS 服务配置文件中予以标识。通过在门户配置中选择与其相关联的服务配置文件来分配门户服务器证书。 • 使用来自众所周知的第三方 CA 的证书。该选项不但安全性最高，还可确保用户端点能与门户建立信任关系而无需部署根 CA 证书。 • 如果不使用众所周知的公共 CA，应导出用于生成门户服务器证书的根 CA 证书至运行 GlobalProtect 应用的所有端点。导出该证书可防止最终用户在初次登录门户期间看到证书警告。 • 证书的 Common Name (CN)（公用名 (CN)）和 Subject Alternative Name (SAN)（主题备用名称 (SAN)）字段必须与托管门户的接口的 IP 地址或完全限定域名 (FQDN) 相匹配。 • 一般来说，每个门户均须拥有各自的服务器证书。如果将单个网关和门户部署至同一接口，则须为这两者使用同一证书。

© 2019 Palo Alto Networks, Inc.

证书	使用情况	颁发流程/最佳做法
		• 如果在同一接口上配置网关和门户，我们也建议您为网关和门户使用相同的证书配置文件和 SSL/TLS 服务配置文件。如果他们不使用相同的证书配置文件和 SSL/TLS 服务配置文件，则在 SSL 握手期间，网关配置优先于门户配置。
网关服务器证书	允许 GlobalProtect 应用建立与网关的 HTTPS 连接。	• 该证书在 SSL/TLS 服务配置文件中予以标识。通过在网关配置中选择与其相关联的服务配置文件来分配网关服务器证书。 • 在防火墙或 CA 服务器上生成 CA 证书，并使用该 CA 证书生成所有网关证书。 • 证书的 CN 和 SAN 字段必须与计划在其上配置网关的接口的 FQDN 或 IP 地址相匹配。 • 门户可以根据配置（Portal configuration Agent（门户配置代理）选项卡中的受信任根 CA 列表）将网关根 CA 证书分发给 GlobalProtect 应用程序。但是，网关根 CA 证书不必预先安装在用户的受信任证书存储区中，也不一定由公共 CA 颁发网关证书。 • 一般来说，每个网关均须拥有各自的服务器证书。但是，如果为基本 VPN 访问部署采用同一接口的单个网关和门户，则须为两个组件使用单个服务器证书。作为最佳实践，请使用公共 CA 签名的证书。 • 如果在同一接口上配置网关和门户，我们也建议您为网关和门户使用相同的证书配置文件和 SSL/TLS 服务配置文件。如果他们不使用相同的证书配置文件和 SSL/TLS 服务配置文件，则在 SSL 握手期间，网关配置优先于门户配置。

（可选）客户端证书	用于在 GlobalProtect 应用与网关/门户之间建立 HTTPS 会话时启用相互身份验证。这确保仅具备有效客户端证书的端点才可认证并连接至网络。	• 要实现客户端证书的简化部署，请配置门户以便在成功登录后立即使用下列方法之一将客户端证书部署至应用：
		  • 对接收同一配置的所有 GlobalProtect 应用使用单一客户端证书。通过将证书上传至门户并在门户代理配置中选中来分配 **Local**（本地）客户端证书。
		  • 使用简单证书注册协议 (**SCEP**) 来允许 GlobalProtect 门户部署唯一客户端证书至 GlobalProtect 应用。通过配置 SCEP 配置文件并在门户代理配置中选中该配置文件实现。
		• 为 GlobalProtect 端点生成客户端证书时，使用以下摘要算法之一：sha1、sha256 、sha384 或 sha512。
		• 此外，还可在对最终用户进行身份验证时使用其他机制以将唯一客户端证书部署至所有端点。
		• 试想在没有客户端证书时首先测试配置，然后在确保所有其他配置设置均正确无误后添加客户端证书。

（可选）机器证书	计算机证书是颁发给驻留在本地计算机存储区或系统密钥链中的端点的客户端证书。每份机器证书在“主题”字段（例	• 为 GlobalProtect 端点生成客户端证书时，使用以下摘要算法之一：sha1、sha256 、sha384 或 sha512。 • 如果计划使用预登录功能，则须在启用 GlobalProtect 访问前使用个人 PKI 基础结构将机器证书部署至所有端点。该方法对于确保安全而言极为重要。

© 2019 Palo Alto Networks, Inc.

证书	使用情况	颁发流程/最佳做法
	如，CN=laptop1.example.com）标识端点而非用户。该证书确保仅可信端点可以连接至网关或门户。 配置有登录前连接方法的用户所需的机器证书	有关详细信息，请参阅使用预登录远程访问 VPN。

表：GlobalProtect 证书要求

有关用来在 GlobalProtect 端点与门户和网关之间建立安全通信的密钥的类型的详细信息，请参阅参考资料：GlobalProtect 应用加密函数。

将服务器证书部署至 GlobalProtect 组件

下表描述了将 SSL/TLS 证书部署至 GlobalProtect 组件的最佳操作步骤：

- 导入来自众所周知的第三方 CA 的服务器证书。

  为 *GlobalProtect* 门户使用来自众所周知的第三方 *CA* 的服务器证书。此举确保最终用户可建立 *HTTPS* 连接，而不会看到有关不可信证书的警告。

  证书的“公用名 *(CN)*”和“主题备用名称 *(SAN)*”字段（如适用）必须与计划在其上配置门户的接口或第三方移动端点管理系统上的设备检入接口的完全限定域名 *(FQDN)* 或 *IP* 地址相匹配。支持使用通配符匹配项。

  在导入证书之前，请确保可从管理系统访问该证书和密钥文件且拥有用于私钥解密的通行码。

  1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后 **Import**（导入）一个新证书。
  2. 使用 **Local**（本地）证书类型（默认）。
  3. 输入 **Certificate Name**（证书名称）。
  4. 输入从 CA 处所接收的 **Certificate File**（证书文件）的路径和名称，或 **Browse**（浏览）以查找该文件。
  5. 选择**File Format**（文件格式）为**Encrypted Private Key and Certificate (PKCS12)**（加密私钥和证书 **(PKCS12)**）。
  6. 输入 **Key File**（密钥文件）字段中 PKCS#12 文件的路径和名称，或 **Browse**（浏览）以查找该文件。
  7. 输入并重新输入用于加密私钥的 **Passphrase**（密码）。
  8. 单击 **OK**（确定）以导入证书和密钥。

- 创建用于向 GlobalProtect 组件颁发自签名证书的根 CA 证书。

  在门户上创建根 *CA* 证书并将其用于为网关和客户端（可选）颁发服务器证书。

  在部署自签名证书之前，首先须创建为 GlobalProtect 组件签署证书的根 CA 证书：

  1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后 **Generate**（生产）一个新证书。
  2. 使用 **Local**（本地）证书类型（默认）。
  3. 输入 **Certificate Name**（证书名称），例如 GlobalProtect_CA。证书名称不得包含空格。

© 2019 Palo Alto Networks, Inc.

4. 不要选择 **Signed By**（签名者）字段中的值。在不选择 **Signed By**（签名者）的情况下，证书为自签名证书。
5. 启用 **Certificate Authority**（证书颁发机构）选项。
6. 单击 **OK**（确定）以生成证书。

- 使用门户中的根 CA 生成自签名服务器证书。

为计划部署的所有网关和可选第三方移动端点管理系统管理接口（如果该接口被网关用于检索 *HIP* 报告）生成服务器证书。

在网关服务器证书中，“公用名 *(CN)*”和“主题备用名称 *(SAN)*”字段中的值必须一致。如果值不同，则 *GlobalProtect* 代理检测不匹配项，且不信任该证书。仅当添加了 *Host Name*（主机名）属性时，自签名证书才包含“主题备用名称 *(SAN)*”字段。

也可使用简单证书注册协议 (SCEP) 从企业 CA 请求服务器证书。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后 **Generate**（生产）一个新证书。
2. 使用 **Local**（本地）证书类型（默认）。
3. 输入 **Certificate Name**（证书名称）。该名称不得包含空格。
4. 在 **Common Name**（公用名）字段中输入计划在其上配置网关的接口的 FQDN（推荐）或 IP 地址。
5. 在 **Signed By**（签名者）字段中，选择先前创建的 GlobalProtect_CA。
6. 在“证书属性”区域，**Add**（添加）并定义用于唯一标识网关的属性。请牢记，如果添加 **Host Name**（主机名称）属性（将填充证书 SAN 字段），则该属性须与已定义 **Common Name**（公用名）的值相同。
7. 为服务器证书配置加密设置，包括加密 **Algorithm**（算法）、密钥长度（**Number of Bits**（位数））、**Digest**（摘要）算法以及证书 **Expiration**（过期期限）（天数）。
8. 单击 **OK**（确定）以生成证书。

- 使用简单证书注册协议 (SCEP) 从企业 CA 请求服务器证书。

为计划部署的所有门户和网关配置单独 *SCEP* 配置文件。然后使用特定的 *SCEP* 配置文件为各 *GlobalProtect* 组件生成服务器证书。

在门户和网关服务器证书中，“公用名 *(Cn)*”字段的值必须包含计划在其上配置门户或网关的接口的 *FQDN*（推荐）或 *IP* 地址，且必须与“主题备用名称 *(SAN)*”字段的值一致。

为了符合《美国联邦信息处理标准》*(FIPS)*，还必须在 *SCEP* 服务器与 *GlobalProtect* 门户之间启用相互 *SSL* 身份验证。（*FIPS-CC* 操作已在防火墙登录页面及防火墙状态栏中予以指明。）

在您提交配置后，门户尝试使用 SCEP 配置文件中的设置请求 CA 证书。如果成功，承载门户的防火墙将保存 CA 证书，并将其显示在 **Device Certificates**（设备证书）列表中。

1. 为各 GlobalProtect 门户或网关配置 SCEP 配置文件。
   1. 输入用于标识此 SCEP 配置文件和在其上部署服务器证书的组件的 **Name**（名称）。如果此配置文件用于具有多重虚拟系统功能的防火墙，选择一个虚拟系统，或者 **Shared**（共享）为有此配置文件的 **Location**（位置）。
   2. （可选）为各证书请求配置 PKI 与门户之间的 **SCEP Challenge**（**SCEP** 质询）响应机制。使用从 SCEP 服务器获得的 **Fixed**（固定）质询密码或门户-客户端向 SCEP 服务器提交所选用户名的 OTP 时所用的 **Dynamic**（动态）密码。对于动态 SCEP 质询，可以是 PKI 管理员的凭据。

© 2019 Palo Alto Networks, Inc.

3. 配置门户用于访问 PKI 中 SCEP 服务器的 **Server URL**（服务器 **URL**）（例如，`http://10.200.101.1/certsrv/mscep/`）。
4. 在 **CA-IDENT Name**（**CA-IDENT** 名称）字段中输入字符串（最长不超过 255 个字符）以标识 SCEP 服务器。
5. 输入在 SCEP 服务器生成的证书中使用的 **Subject**（主题）名称。该主题必须包含格式为 `CN=<value>` 的公用名 (CN) 秘钥，其中 `<value>` 为门户或网关的 FQDN 或 IP 地址。
6. 选择 **Subject Alternative Name Type**（主题备用名称类型）。要输入证书主题或"主题备用名称"扩展中的电子邮件名称，请选择 **RFC 822 Name**（RFC 822 名称）。也可输入用于评估证书的 **DNS Name**（DNS 名称），或用于标识客户端从其获取证书的资源的 **Uniform Resource Identifier**（统一资源标识符）。
7. 配置附加加密设置，包括密钥长度（**Number of Bits**（位数））和证书签名请求的 **Digest**（摘要）算法。
8. 配置证书的允许用途：签名（**Use as digital signature**（用作数字签名））或加密（**Use for key encipherment**（用于密钥加密））。
9. 为确保门户连接到正确的 SCEP 服务器，请输入 **CA Certificate Fingerprint**（CA 证书指纹）。该指纹可从 SCEP 服务器界面的"指纹"字段中获取。
10. 启用 SCEP 服务器与 GlobalProtect 门户之间的相互 SSL 身份验证。
11. 单击 **OK**（确定），然后 **Commit**（提交）配置。

2. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Generate**（生成）。
3. 输入 **Certificate Name**（证书名称）。该名称不得包含空格。
4. 选择用于自动执行向门户或网关颁发经企业 CA 签名的服务器证书的 **SCEP Profile**（**SCEP** 配置文件），然后单击 **OK**（确定）以生成证书。GlobalProtect 门户使用 SCEP 配置文件中的设置向企业 PKI 提交 CSR。

- 将您导入或生成的服务器证书分配给 SSL/TLS 服务配置文件。

1. 选择 **Device**（服务）> **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件），然后 **Add**（添加）一个新的 SSL/TLS 服务配置文件。
2. 输入 **Name**（名称）以标识此配置文件，选择您导入或生成的服务器 **Certificate**（证书）。
3. 定义允许与 GlobalProtect 组件通信的 SSL/TLS 版本范围（**Min Version**（最低版本）到 **Max Version**（最高版本））。

   支持的 *Max Version*（最高版本）为 *TLSv1.2*。

   要提供最强的安全性，设置 *Min Version*（最小版本）为 *TLSv1.2*。

4. 单击 **OK**（确定）以保存 SSL/TLS 服务配置文件。
5. **Commit**（提交）更改。

- 部署自签名服务器证书。

  - 导出由门户上根 *CA* 所颁发的自签名服务器证书，然后将其导入至网关。
  - 请确保为每个网关发布唯一的服务器证书。
  - 指定自签名证书时，必须将根 *CA* 证书分发至门户客户端配置中的最终客户端。

从门户导出证书：

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。
2. 选择要部署的网关证书，然后单击 **Export Certificate**（导出证书）。

© 2019 Palo Alto Networks, Inc.

3. 选择**File Format**（文件格式）为**Encrypted Private Key and Certificate (PKCS12)**（加密私钥和证书 **(PKCS12)**）。
4. 输入并确认加密私钥的 **Passphrase**（密码）。
5. 单击 **OK**（确定）以下载 PKCS12 文件至所选位置。

导入网关上的证书：

1. 选择 **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书） > **Device Certificates**（设备证书），然后 **Import**（导入）证书。
2. 输入 **Certificate Name**（证书名称）。
3. **Browse**（浏览）以查找和选择在前述步骤中下载的 **Certificate File**（证书文件）。
4. 选择**File Format**（文件格式）为**Encrypted Private Key and Certificate (PKCS12)**（加密私钥和证书 **(PKCS12)**）。
5. 输入并确认在从门户导出时用于加密私钥的 **Passphrase**（密码）。
6. 单击 **OK**（确定）以导入证书和密钥。
7. **Commit**（提交）更改至网关。

© 2019 Palo Alto Networks, Inc.

身份验证

GlobalProtect™ 门户和网关必须在允许最终用户访问 GlobalProtect 资源前对其进行身份验证。您必须在门户和网关设置之前配置身份验证机制。下列章节将详细描述支持的身份验证机制及其配置方法：

> 关于 GlobalProtect 用户身份验证
> 设置外部身份验证
> 设置客户端证书身份验证
> 设置双重身份验证
> 设置 strongSwan Ubuntu 和 CentOS 端点的身份验证
> 配置 GlobalProtect 以实现多因素身份验证通知
> 启用向 RADIUS 服务器交付 VSA
> 启用组映射

关于 GlobalProtect 用户身份验证

GlobalProtect 应用程序首次连接至门户时，会提示用户验证至门户。如果成功通过验证，则 GlobalProtect 门户会发送 GlobalProtect 配置，其中包括应用程序可连接的网关列表以及用于连接至网关的客户端证书。成功下载并缓存该配置后，应用程序将尝试连接至配置中所指定的某一网关。由于这些组件提供了网络资源和设置的访问权限，因此它们也要求最终用户进行身份验证。

门户和网关所要求的相应安全级别随网关保护的资源的敏感性而变化。GlobalProtect 提供灵活的身份验证框架，以便您选择适用于各组件的身份验证配置文件和证书配置文件。

- 支持的 GlobalProtect 身份验证方法
- 应用如何知道提供哪些凭据？

支持的 GlobalProtect 身份验证方法

以下主题介绍了 GlobalProtect 支持的身份验证方法，并提供了各种方法的使用指南。

- 本地身份验证
- 外部身份验证
- 客户端证书身份验证
- 双因素身份验证
- 非基于浏览器的应用程序的多重身份验证
- 使用单点登录

本地身份验证

用户帐户凭据和身份验证机制对防火墙而言均属于本地。由于该身份验证机制要求每位 GlobalProtect 用户对应一个帐户，因此它无法扩展且仅适用于少数部署场景。

外部身份验证

用户身份验证功能由外部 LDAP、Kerberos、TACACS+、SAML 或 RADIUS 服务（其中包括支持基于令牌的双重身份验证机制，例如一次性密码 (OTP) 身份验证）执行。要启用外部身份验证：

- 创建设置为可访问外部身份验证服务的服务器配置文件。
- 创建引用服务器配置文件的身份验证配置文件。
- 在门户和网关配置中指定客户端身份验证，并选择性地指定将使用这些设置的端点的操作系统。

可为每个 GlobalProtect 组件使用不同的身份验证配置文件。有关说明，请参阅设置外部身份验证。有关配置示例，请参阅远程访问 VPN（身份验证配置文件）。

如果您配置门户或网关以通过 *SAML* 身份验证来验证用户，当您禁用单点注销 *(SLO)* 时，运行 *GlobalProtect* 应用 *4.1.8* 或之前版本的用户将无法选择 *Sign Out*（注销）应用。运行 *GlobalProtect* 应用 *4.1.9* 或更新版本的用户，可选择 *Sign Out*（注销）应用，无论 *SLO* 是启用还是禁用。

如果您配置门户或网关以通过 *Kerberos* 身份验证来验证用户，那么当用户通过此验证方法成功验证时，其无法选择 *Sign Out*（注销）*GlobalProtect* 应用。

如果您不允许 *GlobalProtect* 应用程序 *Save User Credentials*（保存用户凭据）（*Network*（网络）> *GlobalProtect* > *Portals*（门户）> *<portal-config>* > *Agent*（代理）> *<agent-config>* > *Authentication*（验证）），用户如果通过 *LDAP*、*TACACS+* 或 *RADIUS* 身份验证成功完成身份验证，则他们无法选择 *Sign Out*（注销）应用程序。

© 2019 Palo Alto Networks, Inc.

客户端证书身份验证

为增强安全性，您可将门户或网关配置为在授权用户访问系统之前使用客户端证书获取用户名并验证该用户。

- 要验证该用户，某一证书字段（例如“主题名称”字段）必须识别该用户名。
- 要验证端点，证书的“主题”字段必须识别设备类型而非用户名。（通过预登录连接方法，门户或网关可在用户登录之前验证端点。）

如果您配置门户或网关以通过客户证书身份验证的方式验证用户，那么当用户仅通过客户端证书成功验证身份时，其无法选择 *Sign Out*（注销）*GlobalProtect* 应用。

对于指定客户端证书的代理配置文件，每位用户将收到一份客户端证书。提供证书的机制决定各证书对每位用户是唯一的、还是对该代理配置下的所有用户均一样。

- 要为每位用户和端点部署唯一的客户端证书，使用 **SCEP**。当用户首次登录时，门户要求来自企业 PKI 的证书。门户获得唯一证书，并将其部署至端点。
- 要为接收代理配置的所有用户配置相同的客户端证书，则部署属于防火墙 **Local**（本地）的证书。

使用可选证书配置文件来验证端点提出连接请求的客户端证书。证书配置文件指定用户名和用户域字段内容；列明 CA 证书和阻止会话的标准；并提供确定 CA 证书吊销状态的方法。由于证书是端点或用户对新会话的身份验证的一部分，因此，您必须在用户初次登录门户之前，将证书配置文件中使用的证书预先部署到端点。

证书配置文件将指定哪个证书字段包含用户名。如果证书配置文件指定了“用户名字段”中的“主题”，则端点提供的证书必须包含公用名方可进行连接。如果证书配置文件将“带电子邮件或主体名称的主题备用名称”指定为“用户名字段”，则端点提供的证书必须包含相应字段，以便在 GlobalProtect 应用程序验证至门户或网关时用作用户名。

GlobalProtect 还支持基于通用访问卡 (CAC) 和智能卡的身份验证，该验证方法依赖于证书配置文件。在此情况下，证书配置文件须包含已在智能卡或 CAC 中发布证书的根 CA 证书。

如果指定客户端证书身份验证，则不应在门户配置中设定客户端证书，因为端点在用户连接时会提供该证书。有关如何配置客户端证书身份验证的示例，请参阅远程访问 VPN（证书配置文件）。

双因素身份验证

对于双重身份验证，门户或网关使用两种机制来对用户进行身份验证，例如一次性密码和 Active Directory (AD) 登录凭据。要启用双重身份验证，必须配置证书配置文件和身份验证配置文件并将两者添加至门户和/或网关配置。

您可将门户和网关配置为使用相同或不同的身份验证方法。无论如何，用户必须先成功通过组件所需的两种机制进行身份验证，然后才能访问网络资源。

如果证书配置文件指定了 GlobalProtect 可从其获得用户名的 **Username Field**（用户名字段），外部身份验证服务将自动使用该用户名将用户验证至身份验证配置文件中指定的外部身份验证服务。例如，如果将证书配置文件中的 **Username Field**（用户名字段）设为**Subject**（主题），当身份验证服务器尝试验证用户时，该证书公用名字段中的值将被用作用户名。如果不想强制用户通过证书中的用户名进行身份验证，则必须将证书配置文件中 **Username Field**（用户名字段）设置为 **None**（无）。有关配置示例，请参阅使用双重身份验证远程访问 VPN。

非基于浏览器的应用程序的多重身份验证

（仅 Windows 和 macOS）对于敏感且非基于浏览器的网络资源（例如财务应用程序或软件开发应用程序），可能需要额外身份验证，GlobalProtect 应用程序可以通知并提示用户及时执行访问这些资源所需的多因素身份验证。

© 2019 Palo Alto Networks, Inc.

使用单点登录

（仅限 Windows）启用单点登录 (SSO) 后，GlobalProtect 应用程序使用用户的 Windows 登录凭据自动进行身份验证，并连接到 GlobalProtect 门户和网关。您还可以配置应用程序以包装第三方凭据，确保 Windows 用户能够进行身份验证，甚至是与第三方凭据提供程序连接。

如果您启用单点登录，当用户通过 *SSO* 成功验证时，运行 *GlobalProtect* 应用 *4.1.9* 或更新版本的用户将无法选择 *Sign Out*（注销）应用。

应用如何知道提供哪些凭据？

默认情况下，GlobalProtect 应用程序会尝试将用于门户登录的登录凭证也用于网关登录。就最简单的例子而言，当网关和门户使用同一身份验证配置文件和/或证书配置文件时，应用程序将透明连接至网关。

根据每应用配置，您还可自定义哪些 GlobalProtect 门户和网关（内部、外部或仅手动）需要不同凭证（例如唯一 OTP）。以便 GlobalProtect 门户或网关提示唯一 OTP，而非首先提示在身份验证配置中指定的凭证。

有两个选项可对默认应用程序验证行为进行修改，以使身份验证更强、更快：

- 门户或网站上的 Cookie 身份验证
- 转发到部分或所有网关的凭据

门户或网站上的 *Cookie* 身份验证

Cookie 身份验证可简化最终用户的身份验证流程，因为用户无须再接连登录至门户和网关或输入多个 OTP 以便验证至二者。这最大程度减少了用户须输入凭证的次数，从而改善用户体验。此外，Cookie 允许用户在密码到期后使用临时密码重新启用 VPN 访问。

您可单独为门户和独立网关配置 Cookie 身份验证设置（例如，可对保护敏感性资源的网关设置更短的 Cookie 生命周期）。在门户或网关将身份验证 Cookie 部署至端点后，门户和网关二者都依赖于同一 Cookie 对用户进行身份验证。当应用程序出示 Cookie 时，门户或网关基于所配置的 Cookie 生命周期评估该 Cookie 是否有效。如果该 Cookie 已过期，GlobalProtect 自动提示用户验证至门户或网关。当验证成功时，门户或网关向端点颁发替代性身份验证 Cookie，Cookie 有效期重新开始计算。

下例中，将非用于保护敏感性信息的网关的 Cookie 生命周期配置为 15 天，但将同样非用于保护敏感性信息的网关的 Cookie 生命周期配置为 24 小时。当用户首次验证至门户时，门户颁发身份验证 Cookie。如果用户在五天后尝试连接至门户，该身份验证 Cookie 将仍然有效。但是，如果用户在五天后尝试连接至网关，则网关将评估 Cookie 生命周期并判定 Cookie 已过期（5 天 > 24 小时）。然后，代理将自动提示用户验证至网关，而且在成功验证后将收到替代性身份验证 Cookie。该新身份验证 Cookie 的有效期重新开始计算，对门户而言为 15 天，对网关而言为 24 小时。

有关如何使用这些选项的示例，请参阅设置双重身份验证。

转发到部分或所有网关的凭据

对于双重身份验证，您可指定提示使用其自身凭证集的门户和/或网关类型（内部、外部或仅手动）。该选项可在门户和网关需要不同凭证时（完全不同的 OTP 或登录凭证）加速身份验证流程。对于所选择的各门户或网关，应用程序不会转发凭证，从而允许您为不同 GlobalProtect 组件自定义安全。例如，您可在门户和内部网关上实现同一安全级别，同时要求使用第二重 OTP 或不同密码以便访问为最敏感资源提供访问权限的那些网关。

有关如何使用这些选项的示例，请参阅设置双重身份验证。

应用如何知道提供哪些证书？

将 GlobalProtect 配置为在 macOS 或 Windows 端点上使用客户端证书进行身份验证时，GlobalProtect 必须提供有效的客户端证书才能通过门户和/或网关的身份验证。

© 2019 Palo Alto Networks, Inc.

要使客户证书有效，必须满足以下要求：

- 证书由在门户和网关配置的证书配置文件中定义的证书颁发机构 (CA) 颁发。
- 在证书管理员创建证书时，证书用于指定客户端身份验证目的。
- 证书位于在 GlobalProtect 门户代理配置中配置的证书存储区中。默认情况下，GlobalProtect 应用首先会在用户存储中查找有效证书。如果未找到有效证书，则应用将在机器存储中查找。因为用户存储优先，所以如果 GlobalProtect 应用在用户存储中找到证书，则不会在机器存储中查找。要强制 GlobalProtect 应用只在一个证书库中查找证书，请在适当的 GlobalProtect 门户代理配置中配置 **Client Certificate Store Lookup**（客户端证书存储查找）选项。
- 证书与 GlobalProtect 门户代理配置中指定的任何其他目的相匹配。要指定其他目的，您必须标识证书的对象标识符 (OID)，并在适当的 GlobalProtect 门户代理配置中配置 **Extended Key Usage OID**（扩展密钥用法 **OID**）值。OID 是一个数字值，用于标识要使用证书的应用程序或服务，并在证书颁发机构 (CA) 创建证书时自动附加到证书。有关指定通用或自定义 OID 的详细信息，请参阅 OID 证书选择。

当只有一个客户端证书满足上述要求时，应用自动使用该客户端证书进行身份验证。但是，当多个客户端证书满足这些要求时，GlobalProtect 会提示用户从端点上的有效客户端证书列表中选择客户端证书。虽然 GlobalProtect 要求用户仅在首次连接时选择客户端证书，但用户可能不知道要选择哪个证书。在这种情况下，我们建议您通过证书目的（如 OID 所示）和证书存储缩小可用客户端证书的列表。有关可以配置以自定义应用的这些和其他设置的详细信息，请参阅自定义 GlobalProtect 代理。

© 2019 Palo Alto Networks, Inc.

设置外部身份验证

以下工作流描述了如何设置 GlobalProtect 门户和网关以使用外部身份验证服务。支持的身份验证服务包括 LDAP、Kerberos、RADIUS、SAML 或 TACACS+。

GlobalProtect 还支持本地身份验证。要使用本地身份验证，请创建一个包含允许访问 *GlobalProtect* 的用户和组的本地用户数据库（*Device*（设备）> *Local User Database*（本地用户数据库）），然后在身份验证配置文件中引用该数据库。

有关详细信息，请参阅支持的 GlobalProtect 身份验证方法。

设置外部身份验证的选项包括：

- 设置 LDAP 身份验证
- 设置 SAML 身份验证
- 设置 Kerberos 身份验证
- 设置 RADIUS 或 TACACS+ 身份验证

设置 LDAP 身份验证

组织经常将 LDAP 用作身份验证服务和用户信息中央存储库。它也可以用来存储应用程序用户的角色信息。

STEP 1 | 创建服务器配置文件。

服务器配置文件将辨识外部身份验证服务，并指导防火墙如何连接至外部身份验证服务和访问用户的身份验证凭据。

如果使用 *LDAP* 连接至 *Active Directory (AD)*，则须为每个 *AD* 域分别创建 *LDAP* 服务器配置文件。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **LDAP**，并 **Add**（添加）LDAP 服务器配置文件。
2. 输入 **Profile Name**（配置文件名称），例如 `GP-User-Auth`。
3. 如果此配置文件用于具有多重虚拟系统功能的防火墙，选择一个虚拟系统，或者 **Shared**（共享）为有此配置文件的 **Location**（位置）。
4. 在 **Server List**（服务器列表）部分单击 **Add**（添加），然后输入连接至身份验证服务器所需的信息，其中包括服务器 **Name**（名称）、**LDAP Server**（**LDAP** 服务器）的 IP 地址或 FQDN 及 **Port**（端口）。
5. 选择 LDAP 服务器 **Type**（类型）。
6. 输入 **Bind DN**（绑定 **DN**）和 **Password**（密码）以启用身份验证服务对防火墙进行身份验证。
7. （可选）如果您希望端点使用 SSL 或 TLS 与目录服务器建立更安全的连接，启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项（默认启用）。端点使用的协议取决于服务器端口：
   - 389（默认）— TLS（具体来说，设备使用 StartTLS 操作，这可以将初始明文连接升级至 TLS。）
   - 636 — SSL
   - 任何其他端口 — 设备首先尝试使用 TLS。如果目录服务器不支持 TLS，则设备回滚至 SSL。
8. （可选）如需额外的安全性，启用 **Verify Server Certificate for SSL sessions**（验证 **SSL** 会话的服务器证书）选项，使端点验证目录服务器为 SSL/TLS 连接出示的证书。要启用验证，还必须启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项。为了验证成功，证书必须符合以下条件之一：

© 2019 Palo Alto Networks, Inc.

- 它位于设备证书列表中：**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。必要时，将证书导入设备。
- 证书签发机构位于可信证书授权机构列表中：**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Default Trusted Certificate Authorities**（默认可信证书授权机构）。

9. 单击 **OK**（确定）保存服务器配置文件。

STEP 2 | （可选）创建身份验证配置文件。

身份验证配置文件指定了门户或网关验证用户身份时使用的服务器配置文件。在门户或网关上，可将一个或多个身份验证配置文件分配至一个或多个客户端身份验证配置文件中。有关客户端身份验证配置文件中的身份验证配置文件如何支持细粒度的用户身份验证，请参阅配置 GlobalProtect 网关和设置 GlobalProtect 门户访问权限。

要让用户在没有管理干预的情况下连接并更改自己的过期密码，可考虑使用使用预登录远程访问 VPN。

如果用户密码过期，可以分配临时 *LDAP* 密码以使用户能够登录到 *GlobalProtect*。在这种情况下，可以使用临时密码对门户进行身份验证，但网关登录可能会失败，因为不能重复使用同一临时密码。为了防止上述情况发生，请在门户配置（*Network*（网络）> *GlobalProtect* > *Portal*（门户））中配置身份验证覆盖，使 *GlobalProtect* 应用能够使用 *Cookie* 对门户进行身份验证并使用临时密码对网关进行身份验证。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），然后**Add**（添加）新配置文件。
2. 输入配置文件的 **Name**（名称）。
3. 将 **Authentication**（身份验证）**Type**（类型）设置为 **LDAP**。
4. 选择您在步骤 1 中创建的 LDAP 身份验证**Server Profile**（服务器配置文件）。
5. 输入 **sAMAccountName** 作为 **Login Attribute**（登录属性）。
6. 设置 **Password Expiry Warning**（密码到期警告），这指定可以将密码过期之前的天数告知用户。默认情况下，将会在密码过期（范围为 1-255 天）前七天告知用户。由于用户必须在过期期限结束前更改密码，您必须为用户群提供足以确保继续访问 GlobalProtect 的通知期限。要使用该功能，您必须在 LDAP 服务器配置文件中指定以下 LDAP 服务器类型之一：**active-directory**、**e-directory**或**sun**。

   除非您启用预登陆，否则用户无法在密码过期时访问 GlobalProtect。
7. 指定 **User Domain**（用户域）和 **Username Modifier**（用户名修饰符）。端点组合 **User Domain**（用户域）和 **Username Modifier**（用户名修饰符）值来修改用户在登录时输入的域/用户名字符串。端点使用修改后的字符串进行身份验证，并使用 **User Domain**（用户域）值进行 User-ID 组映射。当身份验证服务需要特定格式的域/用户名字符串而您不想依赖用户正确输入域名时，修改用户输入十分有用。您可以选择下列选项：

   - 要只发送未修改的用户输入，将 **User Domain**（用户域）留空（默认）并将 **Username Modifier**（用户名修饰符）设置为变量 **%USERINPUT%**（默认）。
   - 要将域预置到用户输入，输入 **User Domain**（用户域）并将 **Username Modifier**（用户名修饰符）设置为 **%USERDOMAIN%\%USERINPUT%**。
   - 要将域附加到用户输入，输入用户域并将用户名修饰符设置为 **%USERINPUT%@%USERDOMAIN%**。

   如果 *Username Modifier*（用户名修饰符）包括变量 *%USERDOMAIN%*，则 *User Domain*（用户域）值会替换用户输入的所有域字符串。如果 *User Domain*（用户域）为空，则设备移除用户输入的任何域字符串。
8. 在 **Advanced**（高级）选项卡中，**Add**（添加）**Allow List**（允许列表）以选择允许使用此配置文件验证身份的用户和组。**all**（所有）选项允许每个用户使用此配置文件进行身份验证。默认下，此列表没有条目，这表示没有用户可验证身份。

© 2019 Palo Alto Networks, Inc.

9. 单击 **OK**（确定）。

STEP 3 | 提交配置。

单击 **Commit**（提交）。

设置 SAML 身份验证

安全声明标记语言 (SAML) 是一种基于 XML 的开放标准数据格式，用于在各方（特别是身份提供商 (IdP) 和服务提供商）之间交换身份验证和授权数据。SAML 是 OASIS 安全服务技术委员会的产品。

STEP 1 | 创建服务器配置文件。

服务器配置文件将辨识外部身份验证服务，并指导防火墙如何连接至身份验证服务和访问用户的身份验证凭据。

以下步骤介绍了如何从 IdP 导入 SAML 元数据文件，以便防火墙能够自动创建服务器配置文件并填充连接、注册和 IdP 证书信息。如果 IdP 未提供元数据文件，请选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **SAML Identity Provider**（**SAML** 标识提供商），然后手动 **Add**（添加）服务器配置文件。

1. 将 SAML 元数据文件从 IdP 导出到防火墙可以访问的端点。

   有关导出文件的说明，请参阅您的 IdP 文档。
2. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **SAML Identity Provider**（**SAML** 标识提供商）。
3. 将元数据文件 **Import**（导入）防火墙。
4. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件，例如 `GP-User-Auth`。
5. **Browse**（浏览）元数据文件。
6. （推荐）选择 **Validate Identity Provider Certificate**（验证标识提供商证书）（默认），让防火墙验证 IdP 证书。

   只有在将服务器配置文件分配给身份验证配置文件并 **Commit**（提交）更改后，才会进行验证。防火墙使用身份验证配置文件中的证书配置文件来验证证书。
7. 输入 **Maximum Clock Skew**（最大时钟偏差），这是当防火墙验证 IdP 消息时，IdP 和防火墙之间允许的系统时间差（以秒为单位）。默认值为 60 秒，范围为 1 到 900 秒。如果差值超过此值，则验证失败。
8. 单击 **OK**（确定）保存服务器配置文件。

STEP 2 | （可选）创建身份验证配置文件。

身份验证配置文件指定了门户或网关验证用户身份时使用的服务器配置文件。在门户或网关上，可将一个或多个身份验证配置文件分配至一个或多个客户端身份验证配置文件中。有关客户端身份验证配置文件中的身份验证配置文件如何支持细粒度的用户身份验证的更多信息，请参阅配置 GlobalProtect 网关和设置 GlobalProtect 门户访问权限。

SAML 验证支持通过 GlobalProtect 应用 5.0 和更新版本使用预登录远程访问 VPN。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），然后 **Add**（添加）新身份验证配置文件。
2. 输入身份验证配置文件的 **Name**（名称）。
3. 设置 **SAML** 的 **Authentication**（身份验证）**Type**（类型）。
4. 选择您在步骤 1 中创建的 SAML **IdP Server Profile**（**IdP** 服务器配置文件）。
5. 配置以下选项来启用防火墙和 SAML 身份提供者之间的证书身份验证。更多详细信息，请参阅 SAML 2.0 身份验证。

© 2019 Palo Alto Networks, Inc.

- 防火墙用于签署发送给 IdP 的消息的 **Certificate for Signing Requests**（签名请求证书）。
- 防火墙用于验证 IdP 证书的 **Certificate Profile**（证书配置文件）。

6. 指定用户名和管理员角色格式。
   - 指定 **Username Attribute**（用户名属性）和 **User Group Attribute**（用户组属性）。

     与其他外部身份验证类型不同，*SAML* 身份验证配置文件没有 *User Domain*（用户域）属性。

   - （可选）如果您计划使用此配置文件对在 IdP 身份存储中管理的管理帐户进行身份验证，请指定 **Admin Role Attribute**（管理员角色属性）和 **Access Domain Attribute**（访问域属性）。
7. 在 **Advanced**（高级）选项卡中， **Add**（添加） **Allow List**（允许列表） 以选择允许使用此配置文件验证身份的用户和组。**all**（所有） 选项允许每个用户使用此配置文件进行身份验证。默认下，此列表没有条目，这表示没有用户可验证身份。

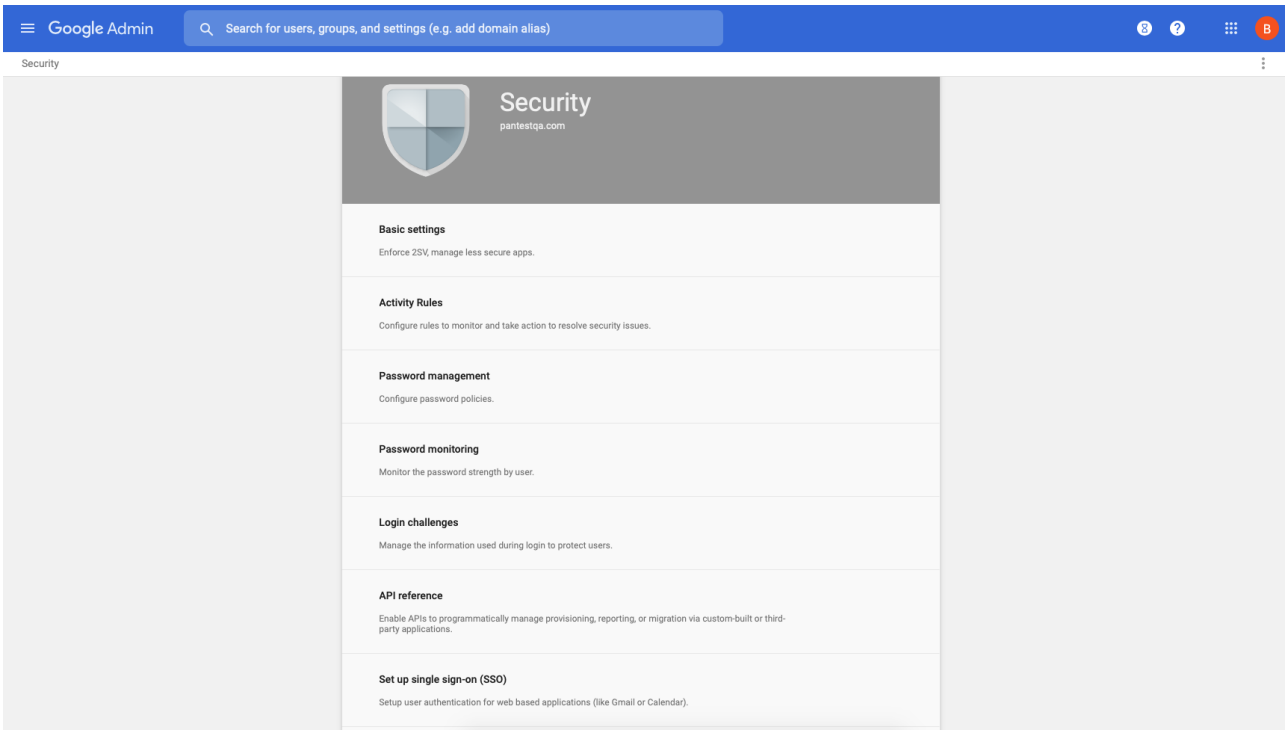
   确保**Allow List**（允许列表）中的用户名与 SAML IdP 服务器返回的用户名匹配。
8. 单击 **OK**（确定）。

STEP 3 | **Commit**（提交）配置。

STEP 4 | （仅限 Chromebook）为 Chromebook 启用 SAML SSO。

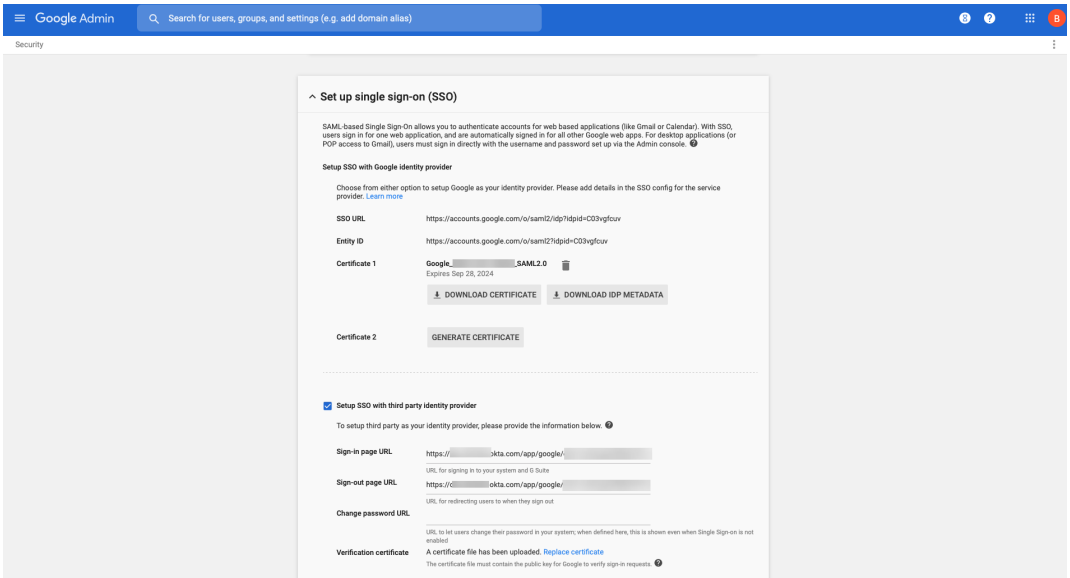
这些步骤可让您在 Chromebook 上为 Android 版 GlobalProtect 应用程序设置 SAML SSO。

1. 登录到 Google 管理控制台，然后选择 **Security**（安全）。

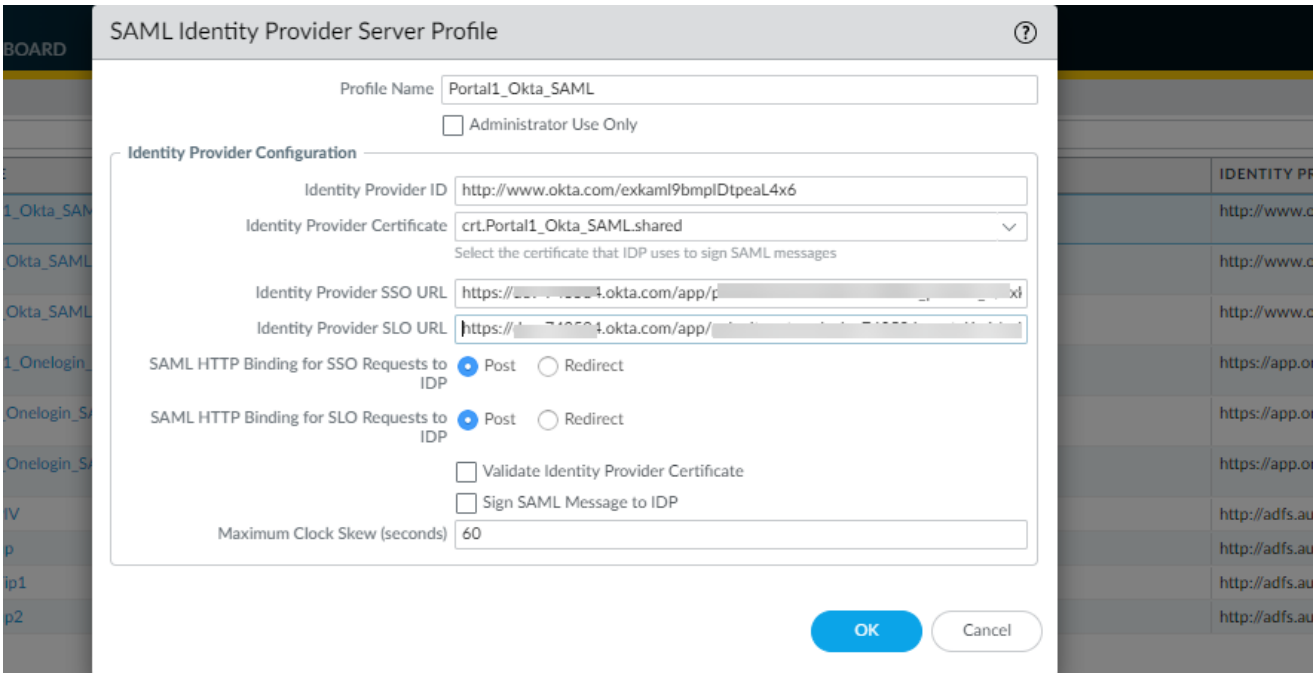


2. 选择 **Set up single sign-on (SSO)**（设置单点登录 **(SSO)**）。
3. （可选）如果您想与除 Google 之外的任何其他提供商一起设置 SSO，请选择 **Setup SSO with third party identity provider**（使用第三方标识提供商设置 **SSO**），并指定登录页 **URL** 和注销页 **URL**，并上载有效的验证证书。

© 2019 Palo Alto Networks, Inc.



4. 在 GlobalProtect 中配置 SAML 标识提供商。
   1. 在 GlobalProtect 控制台中，选择**Device**（设备）> **Server Profiles**（服务器配置文件）> **SAML Identity Provider**（**SAML** 标识提供商）。
   2. 与您在 Google 管理控制台中为 IdP 输入的值匹配。



使用默认系统浏览器进行 *SAMI* 身份验证

如果您已将 GlobalProtect 门户配置为通过 SAML 身份验证对用户身份进行验证，则最终用户无需重新输入其凭据即可连接到应用程序或其他启用了 SAML 的应用程序，以实现无缝单点登录 (SSO) 的体验。最终用户可享受使用默认系统浏览器进行 SAML 身份验证带来的好处，因为可利用 Chrome、Firefox 或 Safari 等默认系统浏览器上保存的用户凭据，使用相同的登录信息登录到 GlobalProtect。

此外，在支持 Web 身份验证 (WebAuthn) API 的任何浏览器上，您可以使用 YubiKeys 等通用第二因素 (U2F) 安全令牌执行多重因素身份验证 (MFA)，以识别 Onelogin 或 Okta 等身份提供商 (IdP)。

© 2019 Palo Alto Networks, Inc.

从 *GlobalProtect™* 应用程序版本 *5.2* 开始，*Windows*、 *macOS*、*Linux*、*Android* 和 *iOS* 设备支持此功能。

STEP 1 | 更改 Windows、macOS、Linux、Android 和 iOS 端点上的预部署设置，以使用默认系统浏览器进行 SAML 身份验证。

您必须先设置客户端端点上的预部署设置，然后才能启用默认系统浏览器进行 SAML 身份验证。GlobalProtect 仅在 GlobalProtect 应用程序初始化时检索一次这些条目。

如果在使用默认系统浏览器进行 SAML 身份验证时最终用户 Windows 或 macOS 端点上没有指定任何预部署值，门户配置中的 **Use Default Browser for SAML Authentication**（使用默认浏览器进行 **SAML** 身份验证）选项设为 **Yes**（是），且用户是首次将应用程序版本从 5.0.x 或 5.1.x 升级到 5.2.0，则应用程序将打开内嵌的浏览器，而不是默认的系统浏览器。用户连接到 GlobalProtect 应用程序，且在门户配置中将 **Use Default Browser for SAML Authentication**（使用默认浏览器进行 **SAML** 身份验证）设为 **Yes**（是）后，应用程序将在下次登录时打开 Windows 和 macOS 端点上的默认系统浏览器。

如果在客户端计算机预部署设置中将 **default browser**（默认浏览器）值设为**Yes**（是），并在门户配置中将 **Use Default Browser for SAML Authentication**（使用默认浏览器进行 **SAML** 身份验证）选项设为 **No**（否），则最终用户将不会获得最佳用户体验。应用程序将打开默认系统浏览器进行首次 SAML 身份验证。因为客户端计算机和门户之间的默认浏览器值不一样，因此，应用程序会在下次登录时检测不匹配情况，并打开内嵌的浏览器。

要为用户提供最佳体验，*Globalprotect* 门户中 *Use Default Browser for SAML Authentication*（使用默认浏览器进行 *SAML* 身份验证）选项的值与客户端计算机预部署设置中该选项的值必须一致。

- 在 Windows 端点上，您可以使用系统中心配置管理器 (SCCM) 预先部署 5.2 版本的 GlobalProtect 应用程序，并通过使用以下语法从 Windows Installer (Msiexec) 将 **DEFAULTBROWSER** 值设为 **yes**（是）：

```
msiexec.exe /i GlobalProtect.msi DEFAULTBROWSER=YES
```

- 在 macOS 端点上，您可以通过使用以下语法在 macOS plist (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`) 中，将 GlobalProtect 应用程序的 **default-browser**（默认浏览器）值设为 **yes**（是）：

```
sudo defaults write /Library/Preferences/
com.paloaltonetworks.GlobalProtect.settings.plist '{"Palo Alto Networks"
 ={GlobalProtect={Settings={default-browser=yes;};};};}'
```

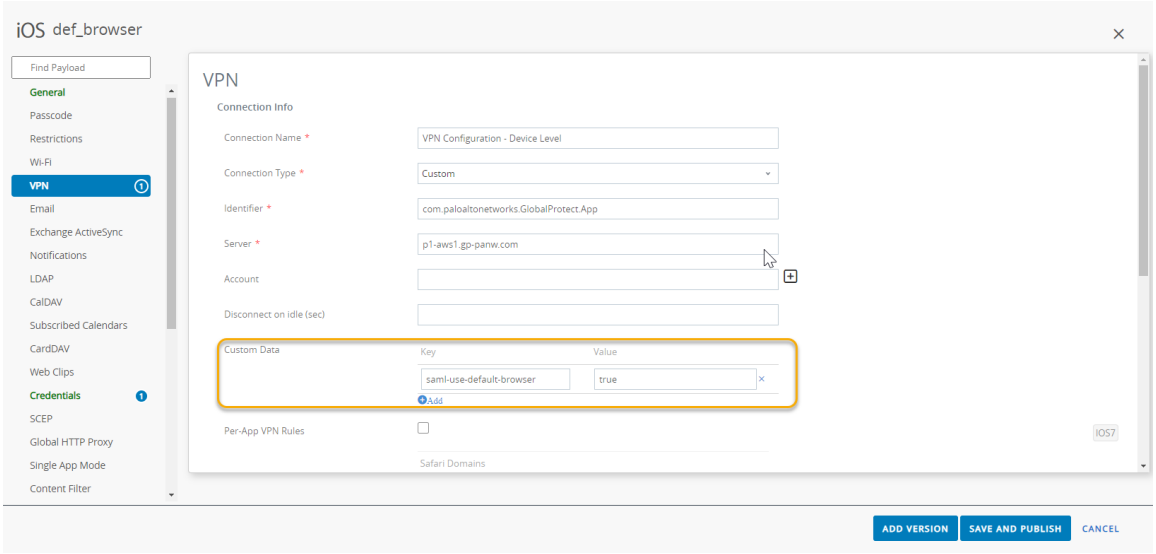
  您必须在安装 5.2 版本 GlobalProtect 应用程序后，指定 plist 键值以启动默认系统浏览器进行 SAML 身份验证。

  添加 plist 键值后，要使该 plist 键值生效，您必须重新启动 macOS 端点。系统重新启动后，用于进行 SAML 身份验证的默认系统浏览器也将启动。
- 在 Linux 端点上，在 `<Settings>` 下的 `/opt/paloaltonetworks/globalprotect/pangps.xml` 预部署配置中，将 **default-browser**（默认浏览器）值设为 **yes**（是）。添加 **default-browser**（默认浏览器）值后，要使这一更改生效，您还必须重新启动 Linux 端点。
- 在 Android 和 iOS 端点上，使用受支持的移动设备管理系统 (MDM)（例如，Airwatch）创建 VPN 配置文件。
  - 以管理员身份登录 Airwatch。
  - 在列表中选择现有 VPN 配置文件（**Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件））。
  - 选择 **VPN** 以添加 VPN 配置文件。

© 2019 Palo Alto Networks, Inc.

在 Android 端点上，输入 **Custom Data Key**（自定义数据项）(**use_default_browser_for_saml**)。输入 **Custom Data Value**（自定义数据值）(**true**)。

在 iOS 端点上，输入 **Custom Data Key**（自定义数据项）(**saml-use-default-browser**)。输入 **Custom Data Value**（自定义数据值）(**true**)。



- 单击 **Save and Publish**（保存并发布）保存更改。

STEP 2 | 设置 SAML 身份验证以验证用户身份。

为确保用于 *SAML* 身份验证的默认系统浏览器不会为每个连接打开多个选项卡，我们建议您配置身份验证覆盖。有关详细信息，请参阅门户或网站上的 Cookie 身份验证。

STEP 3 | 启用 GlobalProtect 应用程序，以便最终用户可以为 GlobalProtect 使用相同的登录，并使用默认系统浏览器进行 SAML 身份验证。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）*<agent-config>* > **App**（应用程序）> **Use Default Browser for SAML Authentication**（使用默认浏览器进行 **SAML** 身份验证）。
2. 选择 **Yes**（是）以使 GlobalProtect 应用程序打开用于 SAML 身份验证的默认系统浏览器。

如果已启用单点登录 *(SSO)*，我们建议您禁用它。在使用默认系统浏览器进行 *SAML* 身份验证时，请将 *Use Single Sign-On (Windows)*（使用单点登录 *(Windows)*）或 *Use Single Sign-On (macOS)*（使用单点登录 *(macOS)*）设为 *No*（否）以禁用单点登录。

STEP 4 | 双击 **OK**（确定）。

STEP 5 | **Commit**（提交）配置。

STEP 6 | 验证最终用户是否能通过其保存的凭据对 IdP 成功执行身份验证。

1. 选择 GlobalProtect 应用程序上的 **Refresh Connection**（刷新连接）、**Connect**（连接）或 **Enable**（启用）以启动连接。

   系统默认浏览器上的新选项卡将打开，以进行 SAML 身份验证。
2. 使用用户名和密码登录以在 IdP 上执行身份验证。
3. 最终用户在 IdP 上成功执行身份验证后，单击 **Open GlobalProtect**（打开 **GlobalProtect**）。
4. 连接到 GlobalProtect 应用程序或其他启用 SAML 的应用程序，无需重新输入用户凭据。

© 2019 Palo Alto Networks, Inc.

设置 Kerberos 身份验证

Kerberos 是一种基于 *tickets*（票据）的计算机网络身份验证协议，用于允许通过非安全网络进行通信的节点以安全的方式彼此证明他们的身份。

Windows（*7*、*8* 和 *10*）以及 *macOS*（*10.10* 和更高版本）端点支持 *Kerberos* 身份验证。适用于 *macOS* 端点的 *Kerberos* 身份验证至少需要 *GlobalProtect* 应用版本 *4.1.0*。

STEP 1 | 创建服务器配置文件。

服务器配置文件将辨识外部身份验证服务，并指导防火墙如何连接至身份验证服务和访问用户的身份验证凭据。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **Kerberos**，并 **Add**（添加）Kerberos 服务器配置文件。
2. 输入 **Profile Name**（配置文件名称），例如 `GP-User-Auth`。
3. 如果此配置文件用于具有多重虚拟系统功能的防火墙，选择一个虚拟系统，或者 **Shared**（共享）为有此配置文件的 **Location**（位置）。
4. 单击**Servers**（服务器）区域中的**Add**（添加），然后输入以下信息以连接到身份验证服务器：
   - 服务器 **Name**（名称）
   - **Kerberos Server**（**Kerberos** 服务器）IP 地址或 FQDN
   - 端口
5. 单击 **OK**（确定）保存服务器配置文件。

STEP 2 | （可选）创建身份验证配置文件。

身份验证配置文件指定了门户或网关验证用户身份时使用的服务器配置文件。在门户或网关上，可将一个或多个身份验证配置文件分配至一个或多个客户端身份验证配置文件中。有关客户端身份验证配置文件中的身份验证配置文件如何支持细粒度的用户身份验证，请参阅配置 GlobalProtect 网关和设置 GlobalProtect 门户访问权限。

要让用户在没有管理干预的情况下连接并更改自己的过期密码，可考虑使用使用预登录远程访问 VPN。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），然后**Add**（添加）新配置文件。
2. 输入配置文件的 **Name**（名称），然后选择 **Kerberos** 作为身份验证 **Type**（类型）。
3. 选择您在步骤 1 中创建的 Kerberos 身份验证 **Server Profile**（服务器配置文件）。
4. 指定 **User Domain**（用户域）和 **Username Modifier**（用户名修饰符）。端点与这些值组合以修改用户在登录时输入的域/用户名字符串。端点使用修改后的字符串进行身份验证，并使用 **User Domain**（用户域）值进行 User-ID 组映射。当身份验证服务需要特定格式的域/用户名字符串而您不想依赖用户正确输入域名时，修改用户输入十分有用。您可以选择下列选项：
   - 要发送未修改的用户输入，将 **User Domain**（用户域）留空（默认），并将 **Username Modifier**（用户名修饰符）设置为变量 **%USERINPUT%**（默认）。
   - 要将域预置到用户输入，输入 **User Domain**（用户域）并将 **Username Modifier**（用户名修饰符）设置为 **%USERDOMAIN%\%USERINPUT%**。
   - 要将域附加到用户输入，输入用户域并将用户名修饰符设置为 **%USERINPUT%@%USERDOMAIN%**。

   如果 *Username Modifier*（用户名修饰符）包括变量 *%USERDOMAIN%*，则 *User Domain*（用户域）值会替换用户输入的所有域字符串。如果 *User Domain*（用户域）为空，则设备移除用户输入的任何域字符串。
5. 配置 Kerberos 单点登录 (SSO)（如网络支持此功能）。

© 2019 Palo Alto Networks, Inc.

- 输入 **Kerberos Realm**（**Kerberos** 域）（最多 127 个字符）以指定用户登录名的主机名部分。例如，用户帐户名 user@EXAMPLE.LOCAL 的领域为 EXAMPLE.LOCAL。
- **Import**（导入） **Kerberos Keytab**（**Kerberos** 密钥表） 文件。出现提示时，**Browse**（浏览）密钥表文件，然后单击 **OK**（确定）。进行身份验证时，端点首先尝试使用密钥表建立 SSO。如果成功且用户尝试访问位于 **Allow List**（允许列表）中，则身份验证立即成功。否则，身份验证过程回滚到指定身份验证 **Type**（类型）的手动（用户名/密码）身份验证。**Type**（类型）无需为 Kerberos。要更改此行为以使用户可仅通过 Kerberos 进行身份验证，在 GlobalProtect 门户代理配置中将 **Use Default Authentication on Kerberos Authentication Failure**（**Kerberos** 身份验证失败时使用默认身份验证）设置为 **No**（否）。

6. 在 **Advanced**（高级）选项卡中， **Add**（添加） **Allow List**（允许列表） 以选择允许使用此配置文件验证身份的用户和组。**all**（所有） 选项允许每个用户使用此配置文件进行身份验证。默认下，此列表没有条目，这表示没有用户可验证身份。
7. 单击 **OK**（确定）。

STEP 3 | 提交配置。

单击 **Commit**（提交）。

设置 RADIUS 或 TACACS+ 身份验证

RADIUS 是一种客户端/服务器协议和软件，它使远程访问服务器能够与中央服务器进行通信，以对拨入用户进行身份验证，并授权他们访问所请求的系统或服务。TACACS 是 UNIX 网络常用的认证协议，允许远程访问服务器将用户的登录密码转发给身份验证服务器，以确定是否允许访问给定的系统。

STEP 1 | 创建服务器配置文件。

服务器配置文件将辨识外部身份验证服务，并指导防火墙如何连接至外部身份验证服务和访问用户的身份验证凭据。

如果要启用向 RADIUS 服务器交付 VSA，必须创建 *RADIUS* 服务器配置文件。

1. 选择 **Device**（设备） > **Server Profiles**（服务器配置文件），然后选择配置文件类型（**RADIUS** 或 **TACACS+**）。
2. **Add**（添加）新的 RADIUS 或 TACACS+ 服务器配置文件。
3. 输入 **Profile Name**（配置文件名称），例如 `GP-User-Auth`。
4. 如果此配置文件用于具有多重虚拟系统功能的防火墙，选择一个虚拟系统，或者 **Shared**（共享）为有此配置文件的 **Location**（位置）。
5. 配置以下 **Server Settings**（服务器设置）：
   - **Timeout (sec)**（超时(秒)）— 由于缺少来自身份验证服务器的响应，服务器连接请求超时之前的秒数。
   - **Authentication Protocol**（身份验证协议）— 用于连接到身份验证服务器的协议。选项包括 **CHAP**、**PAP**、**PEAP-MSCHAPv2**、**PEAP with GTC**或 **EAP-TTLS with PAP**。

     如果将 *PEAP-MSCHAPv2*（受保护的可扩展身份验证协议 *Microsoft* 质询握手身份验证协议版本 *2*）配置为身份验证协议，则远程用户可以在密码过期或 *RADIUS/AD* 在下次登录需要更改密码时，通过 *GlobalProtect* 应用更改其 *RADIUS* 或 *Active Directory(AD)* 密码。
   - （仅限 RADIUS）**Retries**（重试）— 丢弃请求前防火墙尝试连接到验证服务器的次数。
   - （仅 TACACS+）**Use single connection for all authentication**（使用单一连接进行所有认证）允许所有 TACACS 认证请求在单个 TCP 会话上发生，而不是为每个请求单独分配会话的选项。
6. 单击**Servers**（服务器） 区域中的**Add**（添加），然后输入以下信息以连接到身份验证服务器：

© 2019 Palo Alto Networks, Inc.

- 姓名
- **RADIUS** 或 **TACACS+ Server**（服务器）（服务器 IP 地址或 FQDN）
- **Secret**（秘密）（共享秘密以启用身份验证服务来验证防火墙）。
- 端口

7. 单击 **OK**（确定）保存服务器配置文件。

STEP 2 | （可选）创建身份验证配置文件。

身份验证配置文件指定了门户或网关验证用户身份时使用的服务器配置文件。在门户或网关上，可将一个或多个身份验证配置文件分配至一个或多个客户端身份验证配置文件中。有关客户端身份验证配置文件中的身份验证配置文件如何支持细粒度的用户身份验证，请参阅配置 GlobalProtect 网关和设置 GlobalProtect 门户访问权限。

要让用户在没有管理干预的情况下连接并更改自己的过期密码，可考虑使用使用预登录远程访问 VPN。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），然后**Add**（添加）新配置文件。
2. 输入配置文件的 **Name**（名称）。
3. 选择 **Authentication**（身份验证）**Type**（类型）（**RADIUS** 或 **TACACS+**）。
4. 从下拉列表中选择在步骤 1 中创建的 RADIUS 或 TACACS+ 身份验证 **Server Profile**（服务器配置文件）。
5. （仅限 RADIUS）如果您想在身份验证配置文件中包含这些信息，请启用 **Retrieve user group from RADIUS**（从 **RADIUS** 检索用户组）。
6. 指定 **User Domain**（用户域）和 **Username Modifier**（用户名修饰符）。端点与这些值组合以修改用户在登录时输入的域/用户名字符串。端点使用修改后的字符串进行身份验证，并使用 **User Domain**（用户域）值进行 User-ID 组映射。当身份验证服务需要特定格式的域/用户名字符串而您不想依赖用户正确输入域名时，修改用户输入十分有用。您可以选择下列选项：
   - 要发送未修改的用户输入，将 **User Domain**（用户域）留空（默认）并将 **Username Modifier**（用户名修饰符）设置为变量 **%USERINPUT%**（默认）。
   - 要将域预置到用户输入，输入 **User Domain**（用户域）并将 **Username Modifier**（用户名修饰符）设置为 **%USERDOMAIN%\%USERINPUT%**。
   - 要将域附加到用户输入，输入用户域并将用户名修饰符设置为 **%USERINPUT%@%USERDOMAIN%**。

   如果 *Username Modifier*（用户名修饰符）包括变量 *%USERDOMAIN%*，则 *User Domain*（用户域）值会替换用户输入的所有域字符串。如果 *User Domain*（用户域）为空，则设备移除用户输入的任何域字符串。
7. 在 **Advanced**（高级）选项卡中，**Add**（添加）**Allow List**（允许列表）以选择允许使用此配置文件验证身份的用户和组。**all**（所有）选项允许每个用户使用此配置文件进行身份验证。默认下，此列表没有条目，这表示没有用户可验证身份。
8. 单击 **OK**（确定）。

STEP 3 | **Commit**（提交）配置。

© 2019 Palo Alto Networks, Inc.

设置客户端证书身份验证

采用可选客户端证书身份验证时，用户将向 GlobalProtect 门户和/或网关提供客户端证书和连接请求。门户或网关可使用共享的或唯一的客户端证书来验证用户或端点是否属于您的组织。

部署客户端证书的方法取决于您组织的安全要求。

- 部署共享客户端证书进行身份验证
- 部署机器证书进行身份验证
- 部署特定用户的客户端证书进行身份验证

部署共享客户端证书进行身份验证

要验证端点用户是否属于组织，可为所有端点使用相同客户端证书，或单独生成证书以便与特定代理配置进行部署。按照此工作流颁发自签名客户端证书并从门户部署。

STEP 1 | 生成待部署至多个 GlobalProtect 端点的证书。

1. 创建用于向 GlobalProtect 组件颁发自签名证书的根 CA 证书。
2. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后 **Generate**（生产）一个新证书。
3. 将 **Certificate Type**（证书类型）设置为 **Local**（本地）（默认）。
4. 输入 **Certificate Name**（证书名称）。该名称不得包含空格。
5. 输入 **Common Name**（公用名）以将该证书标识为应用证书（例如 `GP_Windows_App`）。由于该证书还将部署至采用同一代理配置的所有应用，因此该证书无需唯一标识特定用户或端点。
6. 在 **Signed By**（签名者）字段中，选择根 CA。
7. 选择 **OSCP Responder**（OCSP 响应者）来验证证书的吊销状态。
8. 单击 **OK**（确定）以生成证书。

STEP 2 | 设置双重身份验证。

在 GlobalProtect 门户代理配置中配置身份验证设置，以允许门户以透明方式将对防火墙而言属于 **Local**（本地）的客户端证书部署至接收配置的应用。

部署机器证书进行身份验证

要确认端点是否属于组织，使用个人公钥基础结构 (PKI) 向每个端点颁发和分发机器证书（推荐），或生成自签名机器证书以便导出。若使用预登录连接方法，则需要机器证书且必须在 GlobalProtect 组件授权访问之前将其安装在端点上。

要确认端点是否属于组织，还必须配置身份验证配置文件以对用户进行身份验证（请参阅双重身份验证）。

按照下列工作流创建客户端证书并手动将其部署至端点。有关详细信息，请参阅关于 GlobalProtect 用户身份验证。有关配置示例，请参阅远程访问 VPN（证书配置文件）。

STEP 1 | 向 GlobalProtect 应用和端点颁发客户端证书。

这使 GlobalProtect 门户和网关能够验证端点是否属于您的组织。

1. 创建用于向 GlobalProtect 组件颁发自签名证书的根 CA 证书。
2. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Generate**（生成）。
3. 输入 **Certificate Name**（证书名称）。证书名称不得包含空格。
4. 输入 **Common Name**（共用名）字段中将显示在证书上的 IP 地址或 FQDN。
5. 从 **Signed By**（签名者）下拉列表中选择根 CA。

© 2019 Palo Alto Networks, Inc.

6. 选择 **OSCP Responder**（**OCSP** 响应者）来验证证书的吊销状态。
7. 为证书配置 **Cryptographic Settings**（加密设置），包括加密 **Algorithm**（算法）、密钥长度（**Number of Bits**（位数））、**Digest**（摘要）算法（使用 sha1、sha256 、sha384 或 sha512 ）以及证书 **Expiration**（过期期限）（天数）。

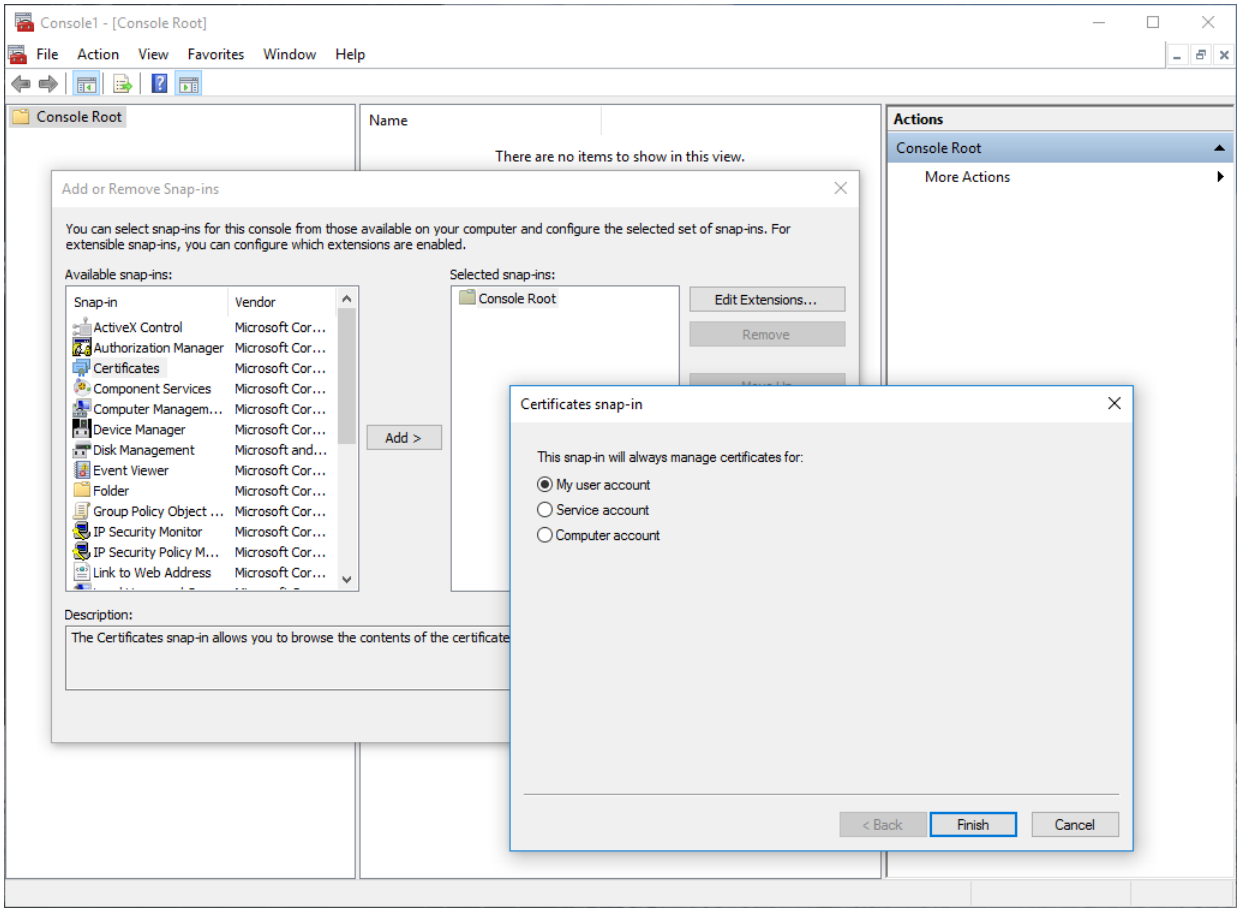
   如果防火墙处于 FIPS-CC 模式且密钥生成算法为 RSA，则 RSA 密钥必须为 2,048 或 3072 位。
8. 在 **Certificate Attributes**（证书属性）区域，**Add**（添加）并定义属性以便将端点唯一标识为属于组织。请牢记，如果添加 **Host Name**（主机名称）属性（将填充证书 SAN 字段），则该属性须与已定义 **Common Name**（公用名）的值相同。
9. 单击 **OK**（确定）以生成证书。

STEP 2 | 在端点的个人证书存储库中安装证书。

如果使用唯一用户证书或机器证书，则必须在首次连接门户或网关前将所有证书安装于端点的个人证书存储库中。将机器证书安装于 Windows 的“本地计算机”证书存储库和 macOS 的“系统密钥链”。将用户证书安装于 Windows 的“当前用户”证书存储库和 macOS 的“密钥链”。

例如，要在使用 Microsoft 管理控制台的 Windows 系统上安装证书：

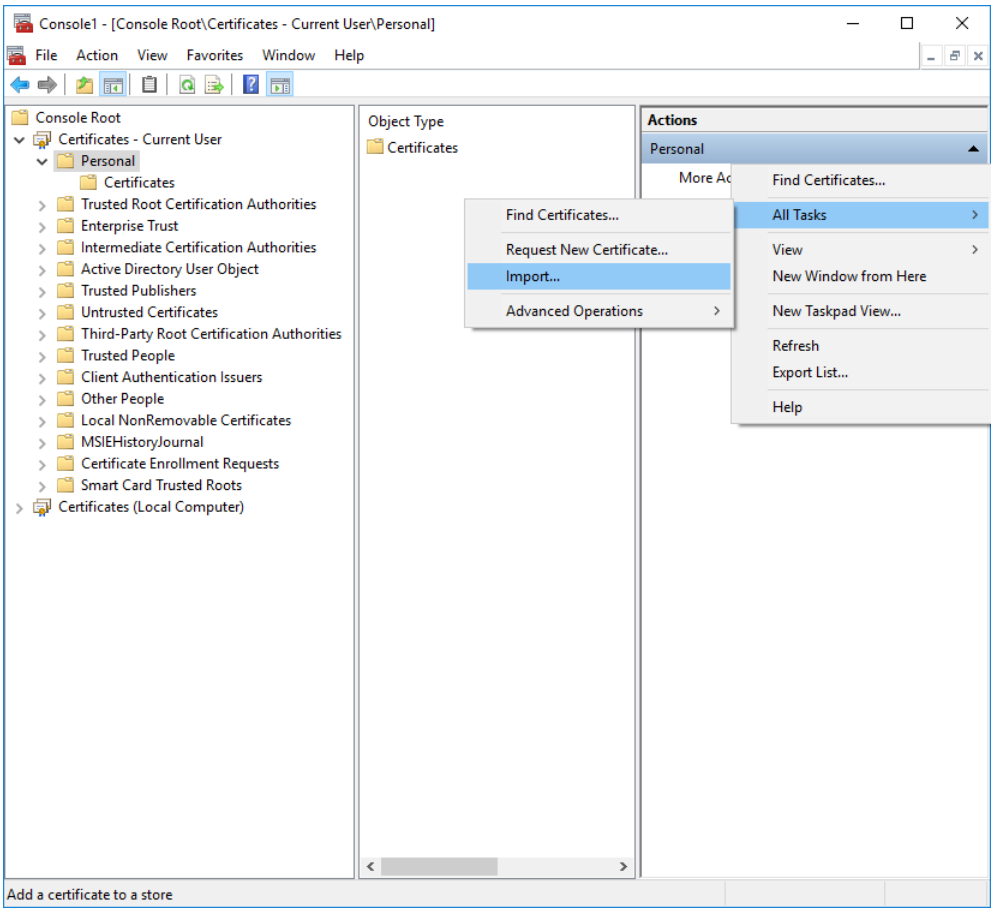
1. 在命令提示符处，输入 `mmc` 以启动“Microsoft 管理控制台”。
2. 选择 **File**（文件）> **Add/Remove Snap-in**（添加/移除管理单元）。
3. 从 **Available snap-ins**（可用单元）列表选择 **Certificates**（证书），然后 **Add**（添加）并根据要导入的证书类型选择以下证书单元之一：
   - **Computer account**（计算机帐户）— 如果正在导入机器证书则选择该选项。
   - **My user account**（我的用户帐户）— 如果正在导入用户证书则选择该选项。



4. 从 **Console Root**（控制台根部）中展开 **Certificates**（证书），然后选择 **Personal**（个人）。

© 2019 Palo Alto Networks, Inc.

5. 在 **Actions**（操作）列中选择 **Personal**（个人） > **More Actions**（更多操作） > **All Tasks**（所有任务） > **Import**（导入）。接着，遵循“证书导入向导”中的步骤导入已从 CA 处获取的 PKCS 文件。

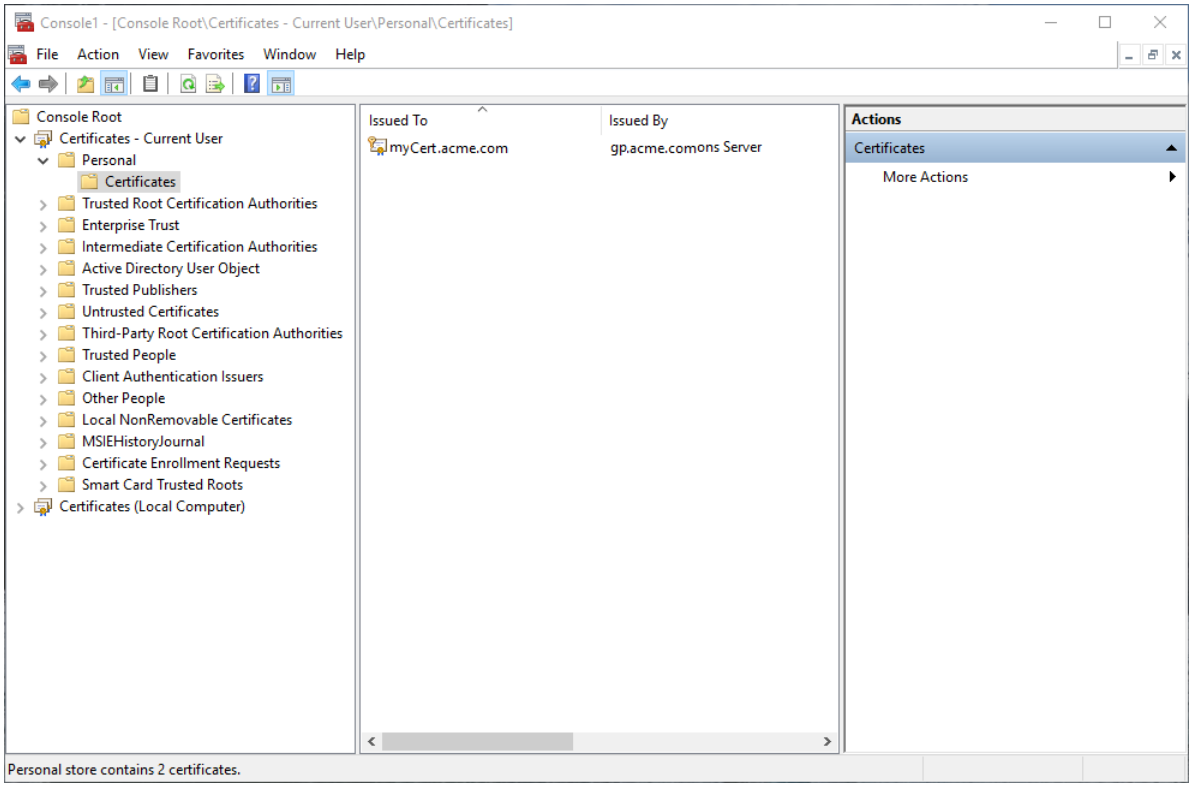


6. **Browse**（浏览）至 .p12 证书文件以便导入（选择**Personal Information Exchange**（个人信息交换）作为文件类型进行浏览），然后输入用于加密私钥的**Password**（密码）。将 **Certificate store**（证书存储库）设置为 **Personal**（个人）。

STEP 3 | 验证证书已添加至个人证书存储。

从 **Console Root**（控制台根部）导航至个人证书存储库（**Certificates**（证书） > **Personal**（个人） > **Certificates**（证书）：

© 2019 Palo Alto Networks, Inc.



STEP 4 | 将用于颁发客户端证书的根 CA 证书导入至防火墙。

仅当客户端证书已由外部 CA（例如，公共 CA 或企业 PKI CA）颁发时才需执行本步骤。如果正在使用自签名证书，则门户和网关已信任根 CA。

1. 下载用于颁发客户端证书的根 CA 证书（Base64 格式）。
2. 从生成客户端证书的 CA 中将根 CA 证书导入到防火墙：
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Import**（导入）。
   2. 将 **Certificate Type**（证书类型）设置为 **Local**（本地）（默认）。
   3. 输入 **Certificate Name**（证书名称），该名称可将证书标识为您的客户端 CA 证书。
   4. **Browse**（浏览）到并选择从 CA 下载的 **Certificate File**（证书文件）。
   5. 将 **File Format**（文件格式）设置为 **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**），然后单击 **OK**（确定）。
   6. 在 **Device Certificates**（设备证书）选项卡上，选择刚刚导入以用于打开“证书信息”的证书。
   7. 选择 **Trusted Root CA**（可信根 **CA**），然后单击 **OK**（确定）。

STEP 5 | 创建客户端证书配置文件。

1. 选择 **Device**（设备）> **Certificates**（证书）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），**Add**（添加）新的证书配置文件。
2. 输入配置文件 **Name**（名称）。
3. 选择 **Username Field**（用户名字段）值以指定用证书中的哪个字段包含用户的标识信息。

   如果计划将门户或网关配置为仅使用证书对用户进行身份验证，则必须指定 **Username Field**（用户名字段）。这使得 GlobalProtect 能够将用户名与证书相关联。

   如果计划将门户或网关设置为双重身份验证，则可将默认值设为 **None**（无），或者，若要添加附加安全层，则指定用户名。如果指定用户名，则外部身份验证服务将验证客户端证书中的用户名是否与请求身份验证的用户名相匹配。此举可确保用户确为证书的既定颁发对象。

© 2019 Palo Alto Networks, Inc.

用户无法更改包含在证书中的用户名。

4. 在 **CA Certificates**（**CA** 证书）区域中，单击 **Add**（添加）。从 **CA Certificate**（**CA** 证书）下拉列表中选择在步骤 4 导入的“可信根 CA” 证书，然后单击 **OK**（确定）。

STEP 6 | 保存配置。

Commit（提交）更改。

部署特定用户的客户端证书进行身份验证

要验证单个用户，必须为每个 GlobalProtect 用户颁发唯一客户端证书，并在启用 GlobalProtect 前将其部署至端点。要自动生成和部署特定用户的客户端证书，可配置 GlobalProtect 门户作为企业 PKI 内的简单证书注册协议 (SCEP) 服务器客户端。

SCEP 操作是动态的，因为当门户提出请求时，企业 PKI 生成特定用户的证书并将其发送至门户。然后，门户以透明方式将该证书部署至应用。当用户请求访问时，应用可出示该客户端证书以验证至门户或网关。

GlobalProtect 门户或网关使用端点和用户的相关标识信息来评估是否允许用户访问。如果主机 ID 在设备阻止列表中或会话与证书配置文件中指定的任何阻止选项相匹配，则 GlobalProtect 阻止访问。如果身份验证因基于 SCEP 的客户端证书无效而失败，则 GlobalProtect 应用尝试根据身份验证配置文件中的设置验证至门户并检索证书。如果应用无法从门户检索证书，则端点无法连接。

STEP 1 | 创建 SCEP 配置文件。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **SCEP**，然后 **Add**（添加）新的 SCEP 配置文件。
2. 输入 **Name**（名称）以标识 SCEP 配置文件。
3. 如果此配置文件用于具有多重虚拟系统功能的防火墙，选择一个虚拟系统，或者 **Shared**（共享）为有此配置文件的 **Location**（位置）。

STEP 2 | （可选）要让基于 SCEP 的证书生成更安全，可在公钥基础结构 (PKI) 与门户之间为各证书请求配置 SCEP 质询-响应机制。

配置此机制后，其操作不可见，无需再进行任何输入操作。

为了符合《美国联邦信息处理标准》(FIPS)，请使用 **Dynamic**（动态）**SCEP Challenge**（**SCEP** 质询）并指定使用 HTTPS 的 **Server URL**（服务器 **URL**）（请参阅步骤 7）。

选择以下 **SCEP** 质询选项之一：

- **None**（无）—（默认）SCEP 服务器不会在门户发布证书前对其进行质询。
- **Fixed**（固定）— 输入从 PKI 基础结构中的 SCEP 服务器获取的注册质询 **Password**（密码）。
- **Dynamic**（动态）— 输入选中项的 **Username**（用户名）和 **Password**（密码）（可能是 PKI 管理员的凭据）以及门户-客户端提交这些凭据的 SCEP **Server URL**（服务器 **URL**）。凭据用于对 SCEP 服务器进行身份验证，SCEP 服务器在接收到每个证书请求时，会以透明的方式为门户生成 OTP 密码（每次提出证书请求后，您可在 `The enrollment challengepassword is`（注册质询密码是）字段所在屏幕刷新后发现此 OTP 更改）。PKI 会以透明方式将各新密码传到门户，然后门户可将此密码用于其证书请求。

STEP 3 | 指定 SCEP 服务器与门户之间的连接设置，以便门户请求和接收客户端证书。

您可通过指定证书 **Subject**（主题）名称中的令牌纳入有关端点或用户的其他信息。

在 SCEP 服务器的 CSR 的 **Subject**（主题）字段中，门户网站包含令牌值 **CN**和 Host-ID 作为 **SerialNumber**。主机 ID 因端点类型而异：GUID (Windows)、接口 (macOS) 的 MAC 地址、Android ID（Android 端点）、UDID（iOS 端点）、或 GlobalProtect 分配的唯一名称 (Chrome)。

© 2019 Palo Alto Networks, Inc.

1. 在 **Configuration**（配置）区域中，输入门户用于访问 PKI 中 SCEP 服务器的 **Server URL**（服务器 **URL**）（例如，`http://10.200.101.1/certsrv/mscep/`）。
2. 输入 **CA-IDENT Name**（**CA-IDENT** 名称）（最长不超过 255 个字符）以标识 SCEP 服务器。
3. 输入在 SCEP 服务器生成的证书中使用的 **Subject**（主题）名称。该主题必须是格式为 <**attribute**>=<**value**> 的可分辨名称，且必须包含公用名属性 (CN=<**variable**>)。CN 支持以下动态令牌：
   - `$USERNAME` — 使用此令牌让门户为特定用户请求证书。要使用这个变量，必须启用组映射。用户输入的用户名必须与用户组映射表中的名称匹配。
   - `$EMAILADDRESS` — 使用此令牌请求与特定电子邮件地址相关联的证书。要使用此变量，必须启用组映射，并在服务器配置文件的 **Mail Domains**（邮件域）部分配置 **Mail Attributes**（邮件属性）。如果 GlobalProtect 无法识别用户的电子邮件地址，则会生成唯一 ID 并使用该值填充 CN。
   - `$HOSTID` — 要仅为端点请求证书，请指定主机 ID 令牌。当用户尝试登录至门户时，端点将发送包含其主机 ID 值的标识信息。

   当 GlobalProtect 门户将 SCEP 设置推送到应用时，将会使用证书所有者（例如 **O=acme,CN=johndoe**）的实际值（用户名、主机 ID 或电子邮箱地址）替换主题名称的公用名 (CN) 部分。
4. 选择 **Subject Alternative Name Type**（主题备用名称类型）。
   - **RFC 822 Name**（**RFC 822** 名称）— 输入证书主题或“主题备选名称”扩展中的电子邮件名称。
   - **DNS Name**（**DNS** 名称）— 输入用于评估证书的 DNS 名称。
   - **Uniform Resource Identifier**（统一资源标识符）— 输入应用将从其获取证书的资源名称。
   - **None**（无）— 不指定证书属性。

STEP 4 | （可选）为证书配置 **Cryptographic Settings**（加密设置）。

- 选择证书的 **Number of Bits**（位数）（密钥长度）。

  如果防火墙为 FIPS-CC 模式且密钥生成算法为 RSA，则 RSA 密钥必须为 2,048 位或更大。
- 选择 **Digest for CSR**（**CSR** 摘要）以标识证书签名请求 (CSR) 的摘要算法：sha1、sha256 、sha384 或 sha512。

STEP 5 | （可选）配置证书的允许用途：签名或加密。

- 要将证书用于签名，选中 **Use as digital signature**（用作数字签名）复选框。该选项可使端点能够使用证书中的密钥来验证数字签名。
- 要将证书用于加密，选中 **Use for key encipherment**（用于加密）复选框。该选项可使应用能够使用证书中的密钥来加密通过 SCEP 服务器颁发的证书建立的 HTTPS 连接所交换的数据。

STEP 6 | （可选）为确保门户连接到正确的 SCEP 服务器，请输入 **CA Certificate Fingerprint**（**CA** 证书指纹）。从 SCEP 服务器界面的 **Thumbprint**（指纹）字段中获取指纹。

1. 输入 SCEP 服务器管理 UI 的 URL（例如，**http://<hostname or IP>/CertSrv/mscep_admin/**）。
2. 复制指纹并将其输入 **CA Certificate Fingerprint**（**CA** 证书指纹）字段中。

STEP 7 | 启用 SCEP 服务器与 GlobalProtect 门户之间的相互 SSL 身份验证。这必须符合《美国联邦信息处理标准》(FIPS)。

FIPS-CC 操作已在防火墙登录页面及防火墙状态栏中予以指明。

选择 SCEP 服务器的根 **CA Certificate**（**CA** 证书）。或者，您也可以通过选择 **Client Certificate**（客户端证书）在 SCEP 服务器和 GlobalProtect 门户之间启用相互 SSL 身份验证。

© 2019 Palo Alto Networks, Inc.

STEP 8 | 保存并提交配置。

1. 单击 **OK**（确定）以保存设置。
2. **Commit**（提交）配置。

门户尝试使用 SCEP 配置文件中的设置请求 CA 证书，并将其保存至承载门户的防火墙。如果成功，则 CA 证书显示在 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）中。

STEP 9 | （可选）如果门户在保存 SCEP 配置文件后未能获取证书，您可手动从门户生成证书签名请求 (CSR)。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后 **Generate**（生产）一个新证书。
2. 选择 **SCEP** 作为 **Certificate Type**（证书类型）。
3. 输入 **Certificate Name**（证书名称）。该名称不得包含空格。
4. 选择用于提交 CSR 至企业 PKI 的 **SCEP Profile**（**SCEP** 配置文件）。
5. 单击 **OK**（确定）以提交请求和生成证书。

STEP 10 | 设置双重身份验证。

为 SCEP 配置文件分配 GlobalProtect 门户代理配置，以允许门户以透明方式请求客户端证书并将其部署至接收此配置的应用。

© 2019 Palo Alto Networks, Inc.

设置双重身份验证

如果需要强身份验证以保护敏感资产或遵从法规要求（例如 PCI、SOX 或 HIPAA），请将 GlobalProtect 配置为使用双重身份验证服务。双重身份验证方案需具备两大要素：最终用户知晓的（例如 PIN 或密码）和最终用户持有的（硬件或软件令牌/OTP、智能卡或证书）。还可启用采取外部身份验证服务、客户端和证书配置文件组合的双重身份验证。

以下主题提供了如何在 GlobalProtect 上设置双重身份验证的示例：

- 使用证书和身份验证配置文件启用双重身份验证
- 使用一次性密码 (OTP) 启用双重身份验证
- 使用智能卡启用双重身份验证
- 使用软件令牌应用程序启用双因素身份验证

使用证书和身份验证配置文件启用双重身份验证

下列工作流描述了如何配置要求用户同时验证至证书配置文件和身份验证配置文件的 GlobalProtect。用户必须使用上述两种方法成功进行验证方可连接至门户/网关。有关此配置的详细信息，请参阅“使用双重身份验证远程访问 VPN。

STEP 1 | 创建身份验证服务器配置文件。

身份验证服务器配置文件确定防火墙连接至外部身份验证服务的方式并检索用户的身份验证凭据。

如果使用 *LDAP* 连接至 *Active Directory (AD)*，则须为每个 *AD* 域分别创建 *LDAP* 服务器配置文件。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）和配置文件类型（**LDAP**、**Kerberos**、**RADIUS** 或 **TACACS+**）。
2. **Add**（添加）新服务器配置文件。
3. 输入 **Profile Name**（配置文件名称），例如 `gp-user-auth`。
4. （仅限 LDAP）选择 LDAP 服务器的 **Type**（类型）（**active-directory**、**e-directory**、**sun** 或 **other**（其他））。
5. 单击 **Servers**（服务器）或 **Servers List**（服务器列表）区域中的**Add**（添加）（取决于服务器配置文件的类型），然后输入以下信息以连接至身份验证服务：
   - 服务器 **Name**（名称）
   - **Server**（服务器）IP 地址或 FQDN
   - 端口
6. （仅限 RADIUS、TACACS+ 和 LDAP）指定以下设置以便防火墙验证至身份验证服务：
   - RADIUS 和 TACACS+ — 添加服务器条目时输入共享 **Secret**（机密）。
   - LDAP — 输入 **Bind DN**（绑定 DN）和 **Password**（密码）。
7. （仅限 LDAP）如果您希望端点使用 SSL 或 TLS 与目录服务器建立更安全的连接，启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项（默认启用）。端点使用的协议取决于 **Server list**（服务器列表）中的服务器 **Port**（端口）：
   - 389（默认）— TLS（具体来说，端点使用 StartTLS 操作，这可以将初始明文连接升级至 TLS。）
   - 636—SSL。
   - 任何其他端口 — 端点首先尝试使用 TLS。如果目录服务器不支持 TLS，则端点使用 SSL。
8. （仅限 LDAP）如需额外的安全性，启用 **Verify Server Certificate for SSL sessions**（验证 **SSL** 会话的服务器证书）选项，使端点验证目录服务器为 SSL/TLS 连接出示的证书。要启用验证，还必须启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项。为了成功验证，下列条件之一必须为真：

© 2019 Palo Alto Networks, Inc.

- 证书位于设备证书列表中：**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。如有需要，将证书导入端点。
- 证书签发机构位于可信证书授权机构列表中：**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Default Trusted Certificate Authorities**（默认可信证书颁发机构）。

9. 单击 **OK**（确定）保存服务器配置文件。

STEP 2 | 创建身份验证配置文件以标识对用户进行身份验证的服务。稍后，您可选择将该配置文件分配到门户和网关上。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），然后**Add**（添加）新配置文件。
2. 输入配置文件的 **Name**（名称）。
3. 选择 **Authentication**（身份验证）**Type**（类型）。
4. 选择您在步骤 1 中创建的 **Server Profile**（服务器配置文件）。
5. （仅限 LDAP）输入 **sAMAccountName** 作为 **Login Attribute**（登录属性）。
6. 单击 **OK**（确定）保存身份验证配置文件。

STEP 3 | 配置门户用于对来自用户端点的客户端证书进行身份验证的客户端证书配置文件。

当您配置双重身份验证使用客户端证书时，外部身份验证服务使用客户端证书（如指定）中的用户名值验证用户。此举可确保当前登录的用户确为证书的既定颁发对象。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），然后 **Add**（添加）新的证书配置文件。
2. 输入配置文件的 **Name**（名称）。
3. 选择以下 **Username Field**（用户名字段）值之一：
   - 如果拟采用客户端证书对个人用户进行身份验证，请选择用于标识用户的证书字段。
   - 如果从门户部署客户端证书，请选择 **None**（无）。
   - 如果为使用预登录连接方法而设置证书配置文件，请选择 **None**（无）。
4. **Add**（添加）要分配给配置文件的**CA Certificates**（**CA** 证书），然后配置以下设置：
   1. 选择 **CA certificate**（CA 证书）：可信根 CA 证书或来自 SCEP 服务器的 CA 证书。必要时，导入证书。
   2. （可选）输入 **Default OCSP URL**（默认 **OCSP URL**）。
   3. （可选）选择 **OCSP Verify Certificate**（**OCSP** 验证证书）证书。
   4. （可选）输入用于签名证书的模板的 **Template Name**（模板名称）。
5. （可选）选择下列选项以指定何时阻止用户请求的会话：
   1. 证书状态未知。
   2. 在 **Certificate Status Timeout**（证书状态超时）秒数内，GlobalProtect 组件并不检索证书状态。
   3. 客户端证书主题中的序列号属性不匹配 GlobalProtect 应用报告端点的主机 ID。
   4. 证书已过期。
6. 单击 **OK**（确定）。

STEP 4 | （可选）向 GlobalProtect 客户端和端点颁发客户端证书。

要以透明方式部署客户端证书，请将门户配置为向端点分发共享客户端证书，或将门户配置为使用 SCEP 为所有用户请求并部署唯一客户端证书。

1. 使用企业 PKI 或公共 CA 向所有 GlobalProtect 用户颁发客户端证书。
2. 对于预登录连接方法，请将证书安装在端点的个人证书存储库中。

© 2019 Palo Alto Networks, Inc.

STEP 5 | 保存 GlobalProtect 配置。

单击 **Commit**（提交）。

使用一次性密码 (OTP) 启用双重身份验证

按照此工作流使用一次性密码 (OTP) 在门户和网关上配置双重身份验证。当用户请求访问时，门户或网关提示用户输入 OTP。身份验证服务将该 OTP 作为令牌发送至用户 RSA 设备。

双重身份验证方案的设置与其他类型的身份验证设置类似。双重身份验证方案要求您配置：

- 分配给身份验证配置文件的服务器配置文件（通常为进行双重身份验证的 RADIUS 服务）。
- 客户端身份验证配置文件，其包含用于组件所使用服务的身份验证配置文件。

默认情况下，应用将提供用于登录至门户和网关的相同凭证。针对 OTP 身份验证，该操作将导致身份验证最初在网关上失败，同时由于延迟而又导致系统提示用户进行登录，因而用户的 OTP 可能会过期。为防止此问题，您必须配置门户和网关提示 OTP 而非基于应用配置使用相同凭证。

您还可通过配置身份验证覆盖减少向用户提示 OTP 的频率。这使得门户和网关能够生成和接受安全加密的 Cookie，以在指定时间对用户进行身份验证。在 Cookie 到期之前，门户和/或网关不会要求新 OTP，从而减少了用户须提供 OTP 的次数。

STEP 1 | 在配置后端 RADIUS 服务为 OTP 生成令牌并确保用户拥有所有必要设备（例如硬件令牌）之后，设置与防火墙交互的 RADIUS 服务器。

有关具体操作指导，请参阅 RADIUS 服务器文档。在大多数情况下，需在 RADIUS 服务器上设置身份验证代理和客户端配置，以便在防火墙与 RADIUS 服务器间启用通信。此外，还需定义用于在防火墙与 RADIUS 服务器间加密会话的共享秘密。

STEP 2 | 在承载网关和/或门户的防火墙上，创建 RADIUS 服务器配置文件。（对于小型部署，一个防火墙就可承载门户和网关。）

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **RADIUS**。
2. **Add**（添加）新配置文件。
3. 输入 RADIUS 配置文件的 **Name**（名称）。
4. 在 **Servers**（服务器）区域中，**Add**（添加）RADIUS 实例并输入以下内容：
   - 用于标识该 RADIUS 服务器的描述性 **Name**（名称）。
   - **RADIUS Server**（**RADIUS** 服务器）的 IP 地址。
   - 用于在防火墙与 RADIUS 服务器间加密会话的共享 **Secret**（秘密）。
   - RADIUS 服务器上用于侦听身份验证请求的 **Port**（端口）号（默认为 1812）。
5. 单击 **OK**（确定）保存配置文件。

STEP 3 | 创建身份验证配置文件。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），**Add**（添加）新配置文件。
2. 输入配置文件的 **Name**（名称）。该名称不得包含空格。
3. 选择 **RADIUS** 作为身份验证服务 **Type**（类型）。
4. 选择创建用于访问 RADIUS 服务器的 **Server Profile**（服务器配置文件）。
5. 输入 **User Domain**（用户域）名称。防火墙使用该值根据允许列表条目匹配身份验证用户，并用于 User-ID 组映射。
6. 选择一个 **Username Modifier**（用户名称修饰符）以修改 RADIUS 服务器期望的“用户名/域”格式。
7. 单击 **OK**（确定）保存身份验证配置文件。

STEP 4 | 将身份验证配置文件分配给 GlobalProtect 门户和/或网关。

您可为门户和网关配置多客户端身份验证配置。对于各客户端身份验证配置，您可指定用于特定操作系统端点的身份验证配置文件。

© 2019 Palo Alto Networks, Inc.

此步骤仅描述如何将身份验证配置文件添加至门户或网关配置。有关设置这些组件的其他详细信息，请参阅 GlobalProtect 门户和 GlobalProtect 网关。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）或 **Gateways**（网关）。
2. 选择现有门户或网关配置，或**Add**（添加）新配置。如果添加新网关或门户，请指定其名称、位置以及网络参数。
3. 在 **Authentication**（身份验证）选项卡上，选择 **SSL/TLS service Profile**（**SSL/TLS** 服务配置文件）或 **Add**（添加）新配置文件。
4. **Add**（添加）新的 **Client Authentication**（客户端身份验证）配置，并配置以下设置：
   - 客户端身份验证配置的 **Name**（名称）。
   - 要应用此配置的端点 **OS**（操作系统）。
   - 您在创建身份验证配置文件中创建的 **Authentication Profile**（身份验证配置文件）。
   - （可选）自定义 **Username Label**（用户名标签）。
   - （可选）自定义 **Password Label**（密码标签）。
   - （可选）自定义 **Authentication Message**（身份验证消息）。
5. 单击 **OK**（确定）保存配置。

STEP 5 | （可选）配置门户或网关在用户每次登录时提示用户名和密码或仅密码。使用 OTP 的双重身份验证不支持保存密码，因为用户每次登录时都必须输入动态密码。

此步骤描述如何在门户代理配置中配置密码设置。有关详细信息，请参阅自定义 GlobalProtect 应用。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portal**（门户），然后选择现有门户配置。
2. 在 GlobalProtect 门户配置对话框中选择**Agent**（代理）。
3. 选择现有代理配置或 **Add**（添加）新配置。
4. 在 **Authentication**（身份验证）选项卡上，设置 **Save User Credentials**（保存用户凭据）为 **Save Username Only**（仅保存用户名）或 **No**（否）。此设置使 GlobalProtect 能够提示用户在下步中选择的每个组件上的动态密码。
5. 双击 **OK**（确定）以保存配置。

STEP 6 | 选择提示动态密码（例如 OTP）的 GlobalProtect 组件 — 门户和网关类型。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portal**（门户），然后选择现有门户配置。
2. 在 GlobalProtect 门户配置对话框中选择**Agent**（代理）。
3. 选择现有代理配置或 **Add**（添加）新配置。
4. 在 **Authentication**（身份验证）选项卡上，选择 **Components that Require Dynamic Passwords (Two-Factor Authentication)**（要求动态密码（双重身份验证）的组件）。一旦选择，门户和/或网关类型提示 OTP。

   不要为任何使用 *SAML* 身份验证的组件选择 *Components that Require Dynamic Passwords (Two-Factor Authentication)*（要求动态密码（双因素身份验证）的组件）选项。
5. 双击 **OK**（确定）以保存配置。

STEP 7 | 如果启用了单点登录 (SSO)，请禁用。因为代理配置指定 RADIUS 作为身份验证服务，因此不支持 Kerberos SSO。

此步骤描述如何禁用 SSO。有关详细信息，请参阅定义 GlobalProtect 代理配置。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portal**（门户），然后选择现有门户配置。
2. 在 GlobalProtect 门户配置对话框中选择**Agent**（代理）。
3. 选择现有代理配置或 **Add**（添加）新配置。
4. 在 **App**（应用程序）选项卡上，设置 **Use Single Sign-on (Windows Only)**（使用单点登录（仅 **Windows**））为 **No**（否）。

© 2019 Palo Alto Networks, Inc.

5. 双击 **OK**（确定）以保存配置。

STEP 8 | （可选）要使用户须提供凭据的次数最少，请配置身份验证覆盖。

默认情况下，门户或网关使用身份验证配置文件和可选证书配置文件对用户进行身份验证。通过身份验证覆盖，门户或网关使用其已部署至端点的加密 Cookie 对用户进行身份验证。只要 Cookie 有效，用户就可登录，而无需定期输入凭据或 OTP。有关更多信息，请参阅 门户或网关上的 Cookie 身份验证。

如果必须立即阻止对 *Cookie* 尚未过期的端点的访问（例如，当端点遗失或被盗时），可通过将设备添加至阻止列表阻止端点访问。

有关详细信息，请参阅 GlobalProtect 门户和 GlobalProtect 网关。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）或 **Gateways**（网关）。
2. 选择现有门户或网关配置，或**Add**（添加）新配置。
3. 根据您是否配置门户或网关，请选择以下选项之一：
   - **GlobalProtect Portal Configuration**（**GlobalProtect** 门户配置）— 在 GlobalProtect Portal Configuration（GlobalProtect 门户配置）对话框中，选择 **Agent**（代理）> *<agent-config>* > **Authentication**（身份验证）。
   - **GlobalProtect Gateway Configuration**（**GlobalProtect** 网关配置）— 在 GlobalProtect Gateway Configuration（GlobalProtect 网关配置）对话框中，选择 **Agent**（代理）> **Client Settings**（客户端设置）> *<client-setting>* > **Authentication Override**（身份验证覆盖）。
4. 配置以下 **Authentication Override**（身份验证覆盖）设置。
   - 身份验证覆盖的 **Name**（名称）。
   - **Generate cookie for authentication override**（生成身份验证覆盖 **Cookie**）— 允许门户或网关生成加密的特定端点 Cookie。用户成功验证后，门户或网关向端点颁发身份验证 Cookie。

     身份验证 cookie 中包含以下字段：

     - `user`— 用于验证用户身份的用户名。
     - `Domain`（域）— 用户的域名。
     - `os`— 设备上使用的应用程序名称。
     - `hostID`— GlobalProtect 分配用于识别主机的唯一 ID。
     - `gen time`— 身份验证 cookie 生成的日期和时间。
     - `ip`— 用于对 GlobalProtect 成功执行身份验证，并获取 cookie 的设备 IP 地址。
   - **Accept cookie for authentication override**（接受身份验证覆盖 **Cookie**）— 命令门户或网关通过有效加密 Cookie 对用户进行身份验证。端点出示有效 Cookie 后，门户或网关将验证此 Cookie 是否已经过门户或网关加密，再对其进行解密，然后对用户进行身份验证。

     GlobalProtect 应用必须知道正在连接的用户的用户名，才能从用户端点匹配和检索相关身份验证 *Cookie*。在应用检索 *Cookie* 后，会将 *Cookie* 发送至门户或网关进行用户身份验证。

     （*仅限 Windows*）如果您在门户代理配置中将 Use Single Sign-On（使用单点登录）选项设置为 *Yes*（是）（启用 *SSO*）（*Network*（网络）> *GlobalProtect* > *Portals*（门户）> *<portal-config>* > *Agent*（代理）> *<agent-config>*. > *App*（应用程序）），*GlobalProtect* 应用程序使用 *Windows* 用户名为用户检索本地身份验证 *cookie*。如果您将 *Use Single Sign-On*（使用单点登录）选项设为 *No*（否）（*SSO* 被禁用），则必须允许 *GlobalProtect* 应用保存用户凭据，从而让应用可以为用户检索身份验证 *Cookie*。将 *Save User Credentials*（保存用户凭据）选项设为 *Yes*（是），以保存用户名和密码，或 *Save Username Only*（仅保存用户名）以仅保存用户名。

© 2019 Palo Alto Networks, Inc.

（仅限 *macOS*）由于 *macOS* 端点不支持单点登录，您必须启用 *GlobalProtect* 应用程序以 *Save User Credentials*（保存用户凭据），从而让应用程序可以为用户检索身份验证 *Cookie*。将 *Save User Credentials*（保存用户凭据）选项设为 *Yes*（是），以保存用户名和密码，或 *Save Username Only*（仅保存用户名）以仅保存用户名。

- **Cookie Lifetime**（**Cookie** 生命周期）— 指定 Cookie 有效的小时数、天数或周数。一般而言，保护敏感信息的网关的 Cookie 生命周期为 24 小时，门户的 Cookie 生命周期为 15 天。小时数范围为 1–72；周数范围为 1–52；天数范围为 1–365。门户或网关 Cookie 过期后（以先到者为准），门户或网关将提示用户进行身份验证，随后加密新 Cookie并发送至端点。
- **Certificate to Encrypt/Decrypt Cookie**（加密/解密 **Cookie** 的证书）— 选择对 Cookie 进行加密和解密时所使用的 RSA 证书。必须在门户和网关上使用相同证书。

  最佳做法是配置 *RSA* 证书，以使用网络支持的最强摘要算法。

  门户和网关使用 RSA 加密填充方案 PKCS#1 V1.5 来生成 Cookie（使用证书公钥）和解密 Cookie（使用证书私钥）。

5. 双击 **OK**（确定）以保存配置。

STEP 9 | **Commit**（提交）配置。

STEP 10 | 验证配置。

在运行 GlobalProtect 应用的端点上，尝试连接至已在其上启用 OTP 身份验证的网关或门户。此时应可看到如下提示：

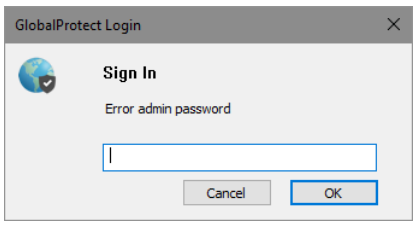


图 **1: OTP** 弹出提示

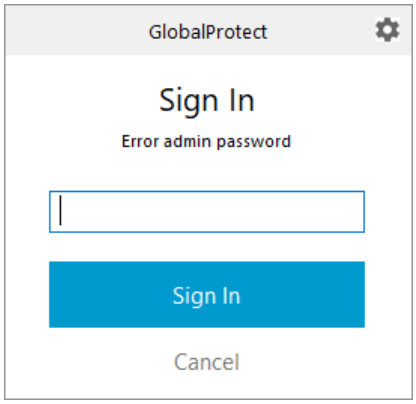


图 **2: GlobalProtect** 状态面板上的 **OTP** 提示

© 2019 Palo Alto Networks, Inc.

使用智能卡启用双重身份验证

如果要允许最终用户使用智能卡或通用访问卡 (CAC) 进行身份验证，则须将已颁发 CAC 或智能卡上所含证书的根 CA 证书导入至门户和网关。然后，即可创建包括该根 CA 的证书配置文件并将其应用至门户和/或网关配置，以便在身份验证期间允许使用智能卡。

STEP 1 | 设置智能卡基础结构。

该过程假设已将智能卡和智能卡读卡器部署至最终用户。

有关具体操作指导，请参阅身份验证提供商软件的文档。

在大多数情况下，智能卡基础结构设置涉及到为最终用户以及加入系统的服务器（在本用例中，即为 GlobalProtect 门户和网关）生成证书。

STEP 2 | 导入已颁发最终用户智能卡上所含客户端证书的根 CA 证书。

确保可以从管理系统访问证书，并完成下列步骤：

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后 **Import**（导入）证书。
2. 输入 **Certificate Name**（证书名称）。
3. 输入从 CA 收到的 **Certificate File**（证书文件）的路径和名称，或 **Browse**（浏览）以查找该文件。
4. 从 **File Format**（文件格式）下拉列表中选择 **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**），然后单击 **OK**（确定）以导入证书。

STEP 3 | 在所有计划使用 CAC 或智能卡身份验证的门户/网关上创建证书配置文件。

有关其他证书配置文件字段（例如，是使用 *CRL* 还是 *OCSP*）的详细信息，请参阅联机帮助。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 选择现有证书文件或 **Add**（添加）新文件。
3. 输入证书文件的 **Name**（名称）。
4. 选择 PAN-OS 用于匹配用户 ID 的 IP 地址的证书**Username Field**（用户名字段）——**Subject**（主题）以使用共用名，或 **Subject Alt:Email**（主题 Alt：电子邮件）来使用电子邮件地址，或 **Subject Alt:Principal Name**（主题 Alt：主体名称）来使用主体名称。
5. 在 **CA Certificates**（**CA** 证书）区域中， **Add**（添加）在步骤 2 中导入到证书配置稳健的可信根 CA 证书。系统提示时，选择 **CA Certificate**（**CA** 证书），然后单击 **OK**（确定）。
6. 单击确定以保存证书配置文件。

STEP 4 | 将证书配置文件分配给门户或网关。此步骤描述如何将证书配置文件添加至门户或网关配置。有关设置这些组件的详细信息，请参阅 GlobalProtect 门户和 GlobalProtect 网关。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）或 **Gateways**（网关）。
2. 选择现有门户或网关配置，或 **Add**（添加）新配置。
3. 在 GlobalProtect 网关配置对话框中选择 **Authentication**（身份验证认）。
4. 选择刚创建的 **Certificate Profile**（证书配置文件）。
5. 单击 **OK**（确定）保存配置。

STEP 5 | **Commit**（提交）配置。

STEP 6 | 验证配置。

© 2019 Palo Alto Networks, Inc.

在运行 GlobalProtect 应用的端点上，尝试连接至已在其上设置启用智能卡的身份验证的网关或门户。出现提示时，插入智能卡并验证可成功验证至 GlobalProtect。

使用软件令牌应用程序启用双因素身份验证

如果您的组织使用软件令牌（软令牌）应用程序（如 RSA SecurID）来实施双因素身份验证，则用户需要首先打开其软件令牌应用程序并输入其 PIN 以获取通行码，然后在其 GlobalProtect 应用程序的 **Password**（密码）字段中输入此通行码。此两步过程使登录过程复杂化。

为了简化登录过程并改善用户体验，GlobalProtect 提供无缝软令牌身份验证。用户在 GlobalProtect **Password**（密码）字段中输入 RSA PIN，GlobalProtect 从 RSA 检索通行码并继续连接，而不需要用户执行打开 RSA 应用程序的额外步骤。

全部三种 RSA 模式都支持此功能：PinPad 样式（PIN 与令牌代码集成）、Fob 样式（PIN 后跟令牌代码）和 Pinless 模式。对于 PinPad 和 Fob 样式，用户在 **Password**（密码）字段中输入 PIN，随后 GlobalProtect 检索通行码。在 Pinless 模式下，Password（密码）字段变灰，用户输入其用户名。

从 *GlobalProtect™ 应用程序 5.1 开始的 Windows 设备支持此功能。*

STEP 1 | 更改客户端 Windows 设备上的注册表项以启用无缝软令牌身份验证。

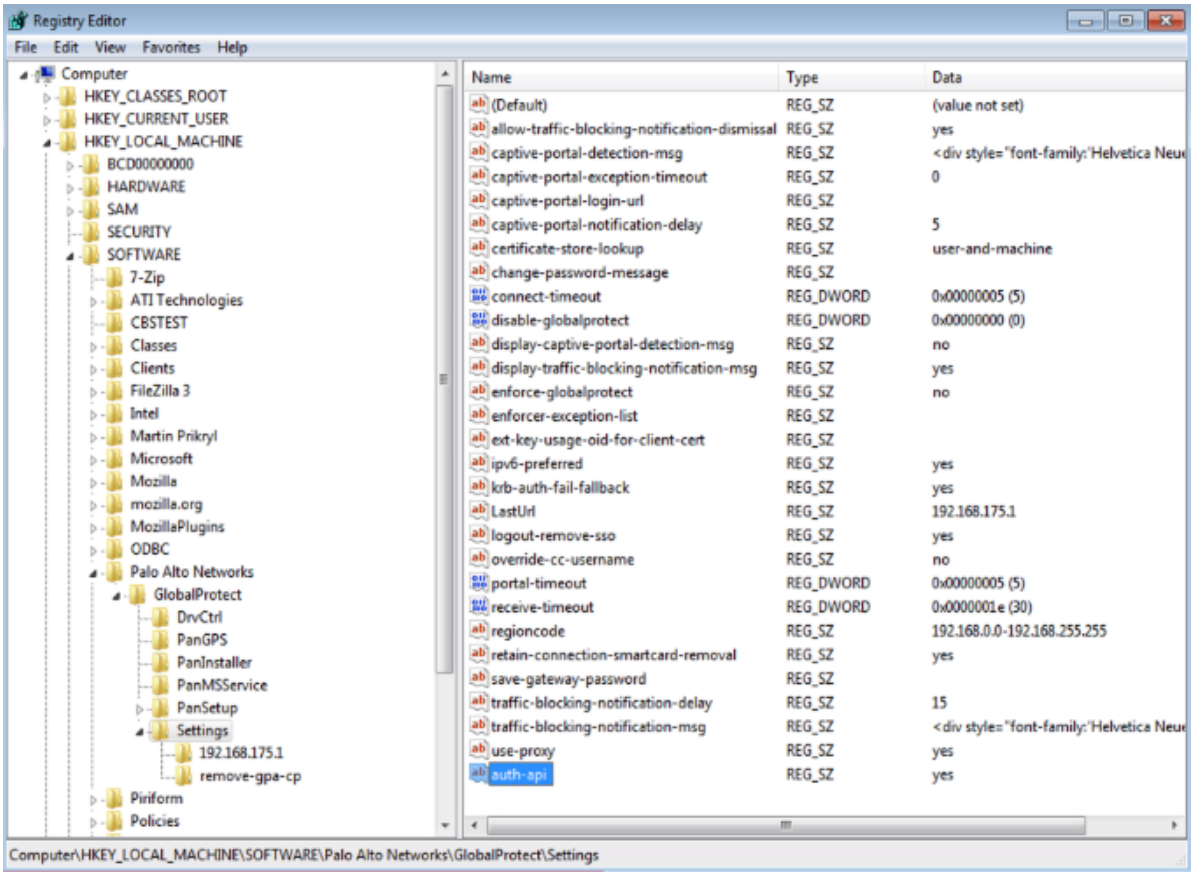
必须先更改客户端 Windows 设备上的 Windows 注册表，然后才能启用无缝软令牌身份验证。GlobalProtect 仅在 GlobalProtect 应用程序初始化时检索此注册表项一次。

1. 打开 Windows 注册表编辑器并选择 **HKEY\'U LOCAL_MACHINE** > **SOFTWARE** > **Palo Alto Networks** > **GlobalProtect** > **Settings**（设置）。
2. 将 **auth-api** 值更改为 **yes**（是）。

因为 *auth api* 在客户端计算机上被设置为 *yes*（是），所以应使用基于 *RSA* 的身份验证来配置门户和网关。不支持其他身份验证配置文件，因为 *GlobalProtect* 将尝试检索通行码。

由于门户和网关使用 *RSA* 身份验证，因此建议您在网关上启用基于 *Cookie* 的身份验证。当 *GlobalProtect* 尝试获取网关通行码时，为门户检索的令牌可能仍处于活动状态，并且身份验证可能会失败，因为通行码已被使用。因此，我们建议您在门户上生成一个身份验证覆盖 *Cookie*，并在网关上接受此 *Cookie*。

© 2019 Palo Alto Networks, Inc.



STEP 2 | 使用基于 RSA 的身份验证配置门户和网关。

STEP 3 | 在 GlobalProtect 门户上启用基于 Cookie 的身份验证。

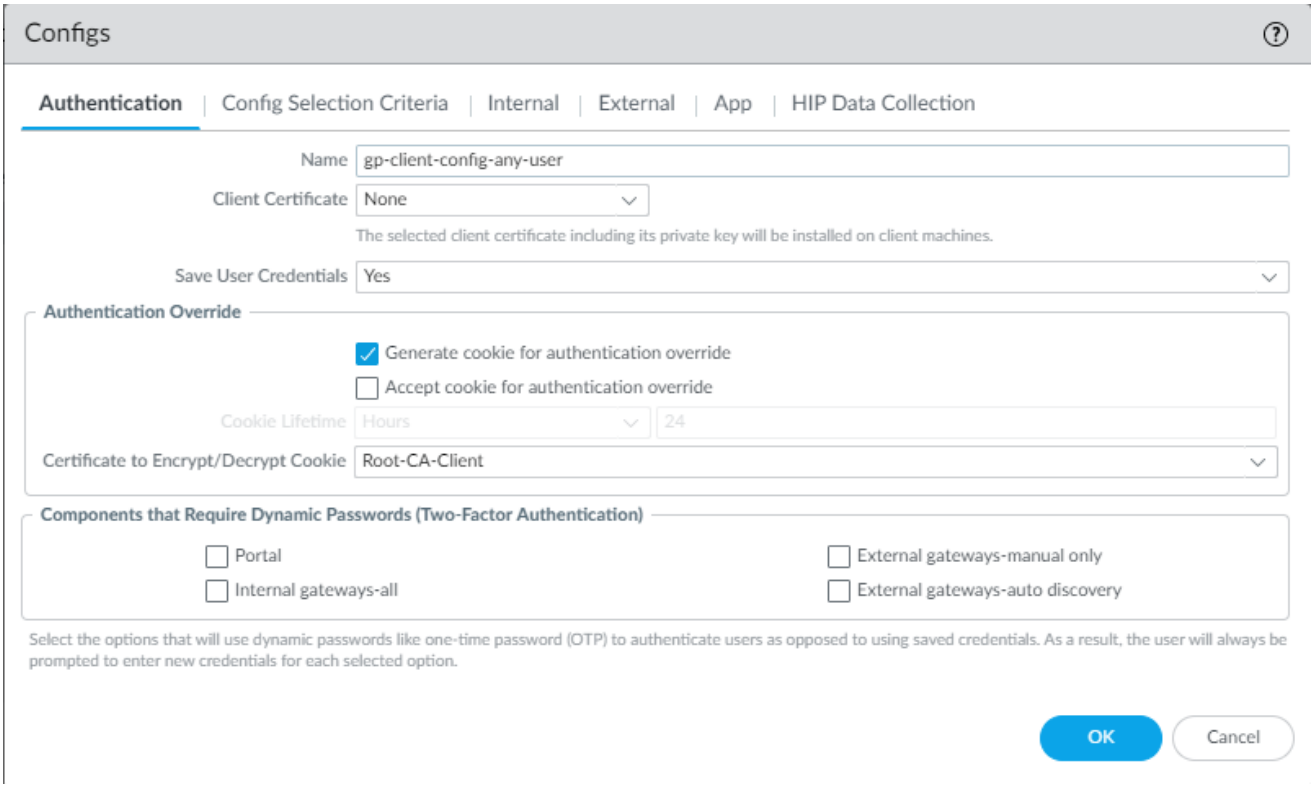
指定 GlobalProtect 覆盖现有身份验证将允许 GlobalProtect 用新创建的通行码覆盖现有通行码。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>*，然后选择 **Agent**（代理）选项卡。
2. **Add**（添加）代理配置或选择一个现有配置。
3. 选择 **Generate cookie for authentication override**（生成用于身份验证覆盖的 **Cookie**）。

   身份验证 cookie 中包含以下字段：

   - `user`— 用于验证用户身份的用户名。
   - `Domain`（域）— 用户的域名。
   - `os`— 设备上使用的应用程序名称。
   - `hostID`— GlobalProtect 分配用于识别主机的唯一 ID。
   - `gen time`— 身份验证 cookie 生成的日期和时间。
   - `ip`— 用于对 GlobalProtect 成功执行身份验证，并获取 cookie 的设备 IP 地址。

© 2019 Palo Alto Networks, Inc.



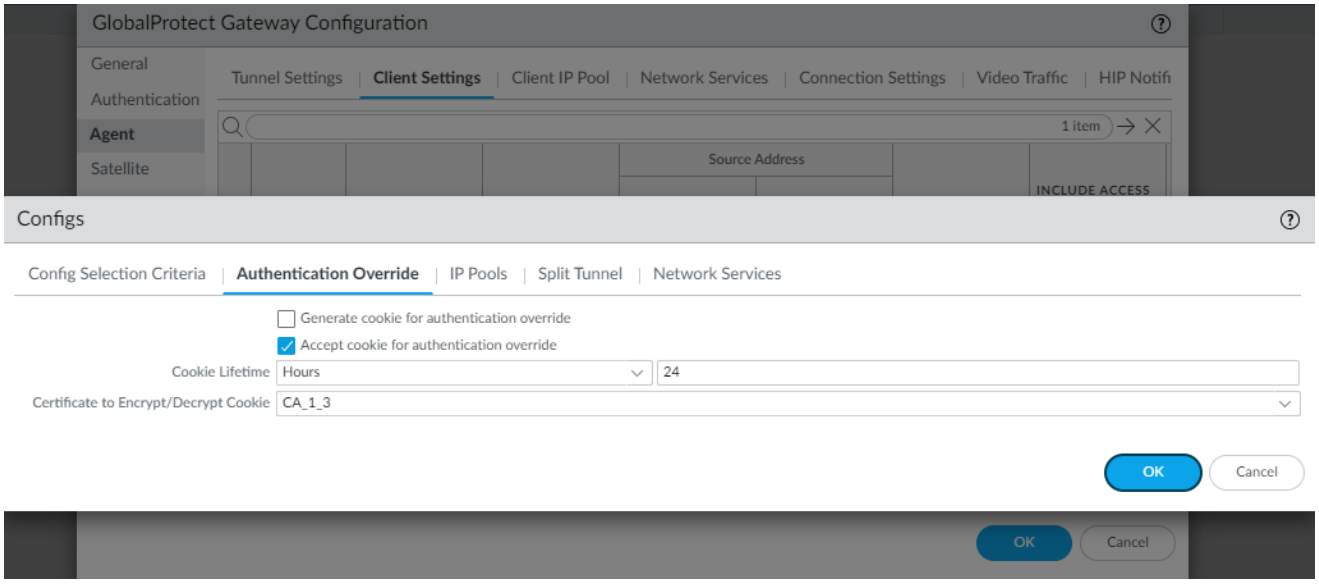
STEP 4 | 启用 GlobalProtect 网关以接受 Cookie 进行身份验证覆盖。

1. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway>*，然后选择 **Agent**（代理）选项卡。
2. 选择 **Client Settings**（客户端设置），然后选择 GlobalProtect 客户端配置或添加一个新配置。
3. 选择 **Authentication Override**（身份验证覆盖），然后选择 **Accept cookie for authentication override**（接受 **Cookie** 进行身份验证覆盖）。

   身份验证 cookie 中包含以下字段：

   - `user`— 用于验证用户身份的用户名。
   - `Domain`（域）— 用户的域名。
   - `os`— 设备上使用的应用程序名称。
   - `hostID`— GlobalProtect 分配用于识别主机的唯一 ID。
   - `gen time`— 身份验证 cookie 生成的日期和时间。
   - `ip`— 用于对 GlobalProtect 成功执行身份验证，并获取 cookie 的设备 IP 地址。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>*，然后，选择 **Authentication**（身份验证）选项卡。

STEP 6 | **Add**（添加）新客户端身份验证配置文件或选择一个现有配置文件，然后，选择 **Automatically retrieve passcode from SoftToken application**（自动从软令牌应用程序检索通行码）。

© 2019 Palo Alto Networks, Inc.

Client Authentication

Name: Local

OS: Any

Authentication Profile: Local

☑ Automatically retrieve passcode from SoftToken application

GlobalProtect App Login Screen

Username Label: Username

Password Label: Password

Authentication Message: Enter login credentials

Authentication message can be up to 256 characters.

Allow Authentication with User Credentials OR Client Certificate: No (User Credentials AND Client Certificate Required)

To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.

OK Cancel

© 2019 Palo Alto Networks, Inc.

设置 strongSwan Ubuntu 和 CentOS 端点的身份验证

要将 GlobalProtect 访问扩展至 strongSwan Ubuntu 和 CentOS 端点，必须为这些端点设置身份验证。

要查看在 *Ubuntu Linux* 和 *CentOS* 上支持 *strongSwan* 的最低 *GlobalProtect* 发布版本，请参阅 GlobalProtect 支持哪些操作系统版本？。

要连接到 GlobalProtect 网关，用户必须成功验证身份。以下工作流显示了如何为 strongSwan 端点启用身份验证。有关 strongSwan 的完整信息，请参阅 strongSwan wiki。

- 使用证书配置文件启用身份验证
- 使用身份验证配置文件启用身份验证
- 启用使用双因素身份验证进行身份验证

使用证书配置文件启用身份验证

以下工作流显示了如何为 strongSwan 客户端启用使用证书配置文件进行身份验证。

STEP 1 | 为 GlobalProtect 网关配置与 strongSwan 客户端通信的 IPsec 隧道。

1. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）。
2. 选择现有网关或 **Add**（添加）新网关。
3. 在“GlobalProtect 网关配置”对话框的 **Authentication**（身份验证）选项卡上，选择想要用于身份验证的 **Certificate Profile**（证书配置文件）。
4. 选择 **Agent**（代理）> **Tunnel Settings**（隧道设置）以启用**Tunnel Mode**（隧道模式），并指定以下设置来建立隧道：
   - 选中此复选框可 **Enable X-Auth Support**（启用扩展身份验证支持）。
   - 如果 **Group Name**（组名）和 **Group Password**（组密码）已配置，请删除它们。
   - 单击 **OK**（确定）以保存设置。

STEP 2 | 验证 IPsec 隧道配置文件 (`ipsec.conf`) 的`conn %default` 部分中的默认连接设置是否为 strongSwan 客户端正确定义。

`ipsec.conf` 文件通常位于 `/etc` 文件夹中。

此程序中的配置已为以下版本进行测试和验证：

- 搭载 *strongSwan 5.1.2* 的 *Ubuntu 14.0.4* 和搭载适用于 *PAN-OS 6.1* 的 *strongSwan 5.1.3* 的 *CentOS 6.5*。
- 搭载适用于 *PAN-OS 7.0* 的 *strongSwan 5.2.1* 的 *Ubuntu 14.0.4*。

如果您使用其他版本的 *strongSwan*，此程序中的配置可用作参考。有关详细信息，请参见 strongSwan wiki。

将 `ipsec.conf` 文件的 `conn %default` 部分中的以下设置修改为这些推荐设置。

```
ikelifetime=20m
reauth=yes
rekey=yes
keylife=10m
rekeymargin=3m
```


© 2019 Palo Alto Networks, Inc.

```
rekeyfuzz=0%
keyingtries=1
type=tunnel
```

STEP 3 | 修改 strongSwan 客户端的 IPsec 配置文件 (**`ipsec.conf`**) 和 IPsec 密码文件 (**`ipsec.secrets`**) 以使用推荐设置。

`ipsec.secrets` 文件通常位于 `/etc` 文件夹中。

将 strongSwan 客户端用户名用作证书的公用名。

将 `ipsec.conf` 文件中的以下项目修改为这些推荐设置。

```
conn <connection name>
keyexchange=ikev1
authby=rsasig
ike=aes-sha1-modp1024,aes256
left=<strongSwan/Linux-client-IP-address>
leftcert=<client certificate with the strongSwan client username used as the
 certificate's common name>
leftsourceip=%config
leftauth2=xauth
right=<GlobalProtect-Gateway-IP-address>
rightid="CN=<Subject-name-of-gateway-certificate>"
rightsubnet=0.0.0.0/0
auto=add
```

将 `ipsec.conf` 文件中的以下项目修改为这些推荐设置。

```
:RSA
<private key file> "<passphrase if used>"
```

STEP 4 | 启动 strongSwan IPsec 服务，连接到您希望 strongSwan 客户端用来对 GlobalProtect 网关进行身份验证的 IPsec 隧道。

使用 `config <name>` 变量为隧道配置命名。

- Ubuntu：

```
ipsec start
ipsec up <name>
```

- CentOS:

```
strongSwan start
strongswan up <name>
```

STEP 5 | 验证隧道是否正确设置，是否建立了与 strongSwan 客户端和 GlobalProtect 网关的 VPN 连接。

1. 验证特定连接（通过指定连接）的详细状态信息或验证 strongSwan 客户端所有连接的状态信息：
   - Ubuntu：

```
ipsec statusall [<connection name>]
```

   - CentOS:

© 2019 Palo Alto Networks, Inc.

```
strongswan statusall [<connection name>]
```

2. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）。在**Info**（信息）列中，为配置与 strongSwan 客户端连接的网关选择 **Remote Users**（远程用户）。strongSwan 客户端应列在 **Current Users**（当前用户）下方。

使用身份验证配置文件启用身份验证

以下工作流显示了如何为 strongSwan 客户端启用使用身份验证配置文件进行身份验证。身份验证配置文件指定了验证 strongSwan 客户端身份时使用哪个服务器配置文件。

STEP 1 | 为 GlobalProtect 网关设置将与 strongSwan 客户端通信的 IPsec 隧道。

1. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）。
2. 选择现有网关或 **Add**（添加）新网关。
3. 在“GlobalProtect 网关配置”对话框的 **Authentication**（身份验证）选项卡上，选择想要使用的 **Authentication Profile**（身份验证配置文件）。
4. 选择 **Agent**（代理）> **Tunnel Settings**（隧道设置）以启用**Tunnel Mode**（隧道模式），并指定以下设置来建立隧道：
   - 选中此复选框可 **Enable X-Auth Support**（启用扩展身份验证支持）。
   - 如果尚未配置 **Group Name**（组名）和 **Group Password**（组密码），请输入。
   - 单击 **OK**（确定）以保存这些隧道设置。

STEP 2 | 验证 IPsec 隧道配置文件 (**`ipsec.conf`**) 的**`conn %default`** 部分中的默认连接设置是否为 strongSwan 客户端正确定义。

`ipsec.conf` 文件通常位于 `/etc` 文件夹中。

此程序中的配置已为以下版本进行测试和验证：

- 搭载 *strongSwan 5.1.2* 的 *Ubuntu 14.0.4* 和搭载适用于 *PAN-OS 6.1* 的 *strongSwan 5.1.3* 的 *CentOS 6.5*。
- 搭载适用于 *PAN-OS 7.0* 的 *strongSwan 5.2.1* 的 *Ubuntu 14.0.4*。

如果您使用其他版本的 *strongSwan*，此程序中的配置可用作参考。有关详细信息，请参见 strongSwan wiki。

在 `ipsec.conf` 文件的 `conn %default` 部分中，配置以下推荐设置：

```
ikelifetime=20m
reauth=yes
rekey=yes
keylife=10m
rekeymargin=3m
rekeyfuzz=0%
keyingtries=1
type=tunnel
```

STEP 3 | 修改 strongSwan 客户端的 IPsec 配置文件 (**`ipsec.conf`**) 和 IPsec 密码文件 (**`ipsec.secrets`**) 以使用推荐设置。

`ipsec.secrets` 文件通常位于 `/etc` 文件夹中。

将 strongSwan 客户端用户名用作证书的公用名。

在 `ipsec.conf` 文件中配置以下推荐设置：

© 2019 Palo Alto Networks, Inc.

```
conn <connection name>
keyexchange=ikev1
ikelifetime=1440m
keylife=60m
aggressive=yes
ike=aes-sha1-modp1024,aes256
esp=aes-sha1
xauth=client
left=<strongSwan/Linux-client-IP-address>
leftid=@#<hex of Group Name configured in the GlobalProtect gateway>
leftsourceip=%modeconfig
leftauth=psk
rightauth=psk
leftauth2=xauth
right=<gateway-IP-address>
rightsubnet=0.0.0.0/0
xauth_identity=<LDAP username>
auto=add
```

在 `ipsec.secrets` 文件中配置以下推荐设置：

```
: PSK <Group Password configured in the gateway>
 <username> : XAUTH "<user password>"
```

STEP 4 | 启动 strongSwan IPsec 服务，连接到您希望 strongSwan 客户端用来对 GlobalProtect 网关进行身份验证的 IPsec 隧道。

- Ubuntu：

```
ipsec start
ipsec up <name>
```

- CentOS:

```
strongSwan start
strongswan up <name>
```

STEP 5 | 验证隧道是否正确设置，是否建立了与 strongSwan 客户端和 GlobalProtect 网关的 VPN 连接。

1. 验证特定连接（通过指定连接）的详细状态信息或验证 strongSwan 客户端所有连接的状态信息：
   - Ubuntu：

     ```
     ipsec statusall [<connection name>]
     ```

   - CentOS:

     ```
     strongswan statusall [<connection name>]
     ```

2. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）。在**Info**（信息）列中，为配置与 strongSwan 客户端连接的网关选择 **Remote Users**（远程用户）。strongSwan 客户端应列在 **Current Users**（当前用户）下方。

© 2019 Palo Alto Networks, Inc.

启用使用双因素身份验证进行身份验证

使用双重身份验证，需要同时使用证书配置文件和身份验证配置文件对 strongSwan 客户端成功进行身份验证，这样才能连接到 GlobalProtect 网关。以下工作流显示了如何为 strongSwan 客户端启用使用双因素身份验证进行身份验证。

STEP 1 | 为 GlobalProtect 网关设置将与 strongSwan 客户端通信的 IPsec 隧道。

1. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）。
2. 选择现有网关或 **Add**（添加）新网关。
3. 在“GlobalProtect 网关配置”对话框的 **Authentication**（身份验证）选项卡上，选择想要使用的 **Certificate Profile**（证书配置文件）和 **Authentication Profile**（身份验证配置文件）。
4. 选择 **Agent**（代理）> **Tunnel Settings**（隧道设置）以启用**Tunnel Mode**（隧道模式），并指定以下设置来建立隧道：
   - 选中此复选框可 **Enable X-Auth Support**（启用扩展身份验证支持）。
   - 如果 **Group Name**（组名）和 **Group Password**（组密码）已配置，请删除它们。
   - 单击 **OK**（确定）以保存这些隧道设置。

STEP 2 | 验证 IPsec 隧道配置文件 (**`ipsec.conf`**) 的**`conn %default`** 部分中的默认连接设置是否为 strongSwan 客户端正确定义。

`ipsec.conf` 文件通常驻留在 `/etc` 文件夹中。

此程序中的配置已为以下版本进行测试和验证：

- 搭载 *strongSwan 5.1.2* 的 *Ubuntu 14.0.4* 和搭载适用于 *PAN-OS 6.1* 的 *strongSwan 5.1.3* 的 *CentOS 6.5*。
- 搭载适用于 *PAN-OS 7.0* 的 *strongSwan 5.2.1* 的 *Ubuntu 14.0.4*。

如果您使用其他版本的 *strongSwan*，此程序中的配置可用作参考。有关详细信息，请参见 strongSwan wiki。

在 `ipsec.conf` 文件中配置以下推荐设置：

```
ikelifetime=20m
reauth=yes
rekey=yes
keylife=10m
rekeymargin=3m
rekeyfuzz=0%
keyingtries=1
type=tunnel
```

STEP 3 | 修改 strongSwan 客户端的 IPsec 配置文件 (**`ipsec.conf`**) 和 IPsec 密码文件 (**`ipsec.secrets`**) 以使用推荐设置。

`ipsec.secrets` 文件通常位于 `/etc` 文件夹中。

将 strongSwan 客户端用户名用作证书的公用名。

在 `ipsec.conf` 文件中配置以下推荐设置：

```
conn <connection name>
keyexchange=ikev1
authby=xauthrsasig
ike=aes-sha1-modp1024
```


© 2019 Palo Alto Networks, Inc.

```
esp=aes-sha1
xauth=client
left=<strongSwan/Linux-client-IP-address>
leftcert=<client-certificate-without-password>
leftsourceip=%config
right=<GlobalProtect-gateway-IP-address>
rightid=%anyCN=<Subject-name-of-gateway-cert>"
rightsubnet=0.0.0.0/0
leftauth2=xauth
xauth_identity=<LDAP username>
auto=add
```

在 `ipsec.secrets` 文件中配置以下推荐设置：

```
<username> :XAUTH "<user password>"
::RSA <private key file> "<passphrase if used>"
```

STEP 4 | 启动 strongSwan IPsec 服务，连接到您希望 strongSwan 客户端用来对 GlobalProtect 网关进行身份验证的 IPsec 隧道。

- Ubuntu：

```
ipsec start
ipsec up <name>
```

- CentOS:

```
strongSwan start
strongswan up <name>
```

STEP 5 | 验证隧道是否正确设置，是否建立了与 strongSwan 客户端和 GlobalProtect 网关的 VPN 连接。

1. 验证特定连接（通过指定连接）的详细状态信息或验证 strongSwan 客户端所有连接的状态信息：
   - Ubuntu：

   ```
   ipsec statusall [<connection name>]
   ```

   - CentOS:

   ```
   strongswan statusall [<connection name>]
   ```

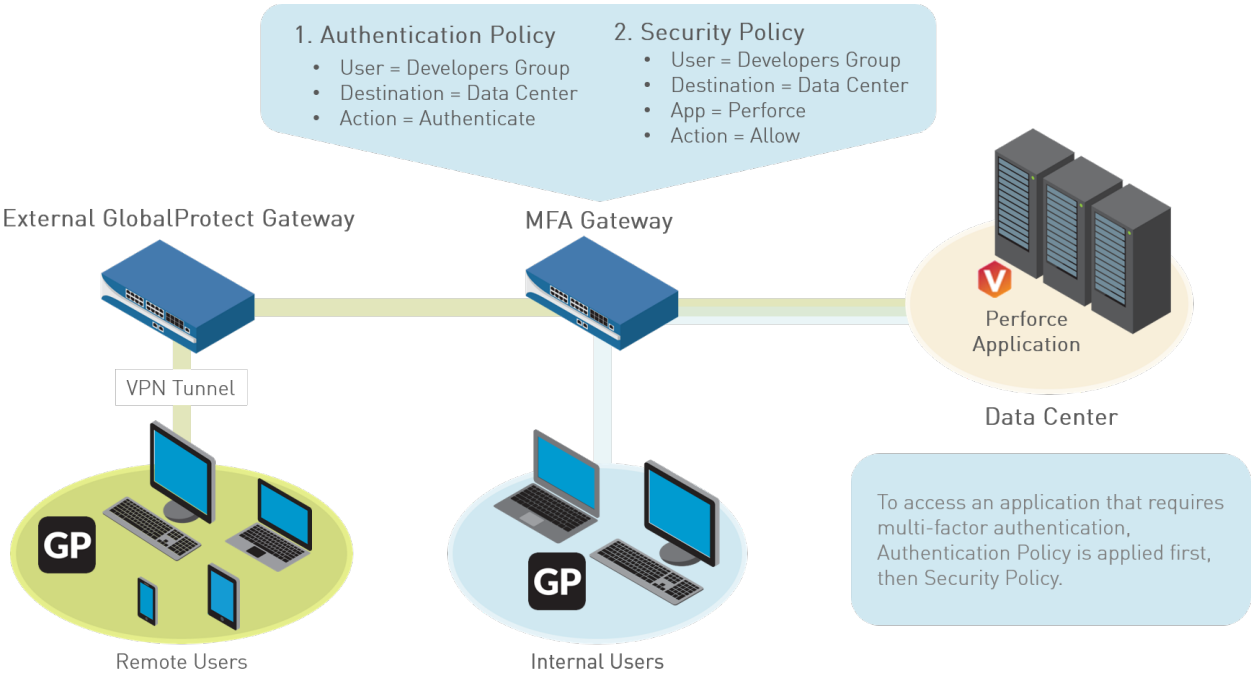
2. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）。在**Info**（信息）列中，为配置与 strongSwan 客户端连接的网关选择 **Remote Users**（远程用户）。strongSwan 客户端应列在 **Current Users**（当前用户）下方。

© 2019 Palo Alto Networks, Inc.

配置 GlobalProtect 以实现多因素身份验证通知

为了保护关键应用程序并阻止攻击者使用被盗取的证书在整个网络中横向移动，您可以配置基于策略的多重因素身份验证 (MFA)。这可以确保每个用户在访问高度敏感的服务和应用程序之前，对不同类型（因素）的多个身份验证质询做出响应。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

如果用户会话与身份验证策略匹配，则应用程序或服务的类型将确定有关身份验证质询的通知的用户体验：

- （仅 Windows 或 macOS 端点）非基于浏览器的应用程序— 为了在 Windows 或 macOS 端点上为非 HTTP 应用程序（例如 Perforce）提供 MFA 通知，需要 GlobalProtect 应用程序。当会话与认证策略规则相匹配时，防火墙会向 GlobalProtect 应用程序发送一个 UDP 通知，并通过嵌入的 URL 指向身份验证门户页面。GlobalProtect 应用程序然后会以弹出通知形式向用户显示此消息。
- 基于浏览器的应用程序— 基于浏览器的应用程序不要求 GlobalProtect 向用户显示通知消息。当防火墙将会话识别为 Web 浏览流量（基于 App-ID）时，防火墙会自动向用户呈现身份验证策略规则中指定的身份验证门户页面（以前称为 Captive 门户页面）。有关更多信息，请参阅配置多重因素身份验证。

要将 GlobalProtect 配置为显示非基于浏览器的应用程序的 MFA 通知，请使用以下工作流程：

STEP 1 | 在配置 GlobalProtect 之前，请在防火墙上配置多重因素身份验证。

如果使用 *GlobalProtect* 的双重身份验证来对网关或门户进行身份验证，则需要使用 *RADIUS* 服务器配置文件。如果使用 *GlobalProtect* 通知用户身份验证策略匹配（*UDP* 消息），则多重因素验证服务器配置文件即已足够。

要使用多重因素身份验证来保护敏感资源，最简单的解决方案是将防火墙与已在网络中建立的 MFA 供应商集成。当 MFA 结构准备就绪时，您可以开始配置身份验证策略的组件。有关更多信息，请参阅配置多重因素身份验证。

- 启用强制网络门户来记录身份验证时间戳和更新用户映射。
- 创建定义防火墙如何连接到身份验证用户的服务的服务器配置文件。
- 将服务器配置文件分配给指定验证参数的验证配置文件。
- 配置安全策略规则，允许用户访问需要身份验证的资源。

STEP 2 | （仅外部网关）要使 GlobalProtect 支持外部网关的多重因素身份验证，您必须为防火墙的入口隧道接口配置响应页面：

1. 选择 **Device**（设备）> **Response Pages**（响应页面）> **MFA Login Page**（**MFA** 登录页面）。
2. 选择并 **Export**（导出）**Predefined**（预定义）模板到所选位置。
3. 在您的端点上，使用 HTML 编辑器自定义下载的响应页面，并使用唯一文件名保存。
4. 返回到防火墙上的 **MFA Login Page**（ **MFA** 登录页面）对话框，**Import**（导入）您的自定义页面，**Browse**（浏览）以选择 **Import File**（导入文件），选择 **Destination**（目标）（虚拟系统或共享位置）。单击 **OK**（确定），然后单击 **Close**（关闭）。

STEP 3 | （仅外部网关）启用 **Response Pages**（响应页面）作为 许可的服务（接口管理）配置文件中许可的服务：

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Interface Mgmt**（接口管理），然后选择配置文件。
2. 在 **Permitted Services**（允许的服务）区域，选择 **Response Pages**（响应页面）并单击 **OK**（确定）。

STEP 4 | （仅外部网关）将 **Interface Mgmt**（接口管理）配置文件附加到隧道接口：

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Interfaces**（隧道）以及您要使用响应页面的通道接口。
2. 选择 **Advanced**（高级），然后选择您在上一步中配置的 **Interface Mgmt**（接口管理）配置文件作为 **Management Profile**（管理配置文件）。

STEP 5 | （仅外部网关）在与隧道接口相关联的区域上 **Enable User Identification**（启用用户标识）（**Network**（网络）> **Zones**（区域）> **<tunnel-zone**）。

STEP 6 | 配置 GlobalProtect 客户端以支持非基于浏览器的应用程序的多重因素身份验证通知。

© 2019 Palo Alto Networks, Inc.

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户），并选择门户配置（或**Add**（添加）新配置）。
2. 选择 **Agent**（代理），然后选择现有代理配置或 **Add**（添加）新配置。
3. 在 **App**（应用）选项卡中，指定以下项目：
   - 将 **Enable Inbound Authentication Prompts from MFA Gateways**（从 **MFA** 网关启用入站身份验证提示）设置为 **Yes**（是）。要支持多因素身份验证 (MFA)，GlobalProtect 应用程序必须接收并确认从网关入站的 UDP 提示。选择 **Yes**（是）可使 GlobalProtect 应用程序接收并确认提示。默认情况下，该值设置为 **No**（否），这意味着 GlobalProtect 将阻止来自网关的 UDP 提示。
   - 在字段 **Network Port for Inbound Authentication Prompts (UDP)**（入站身份验证提示的网络端口 **(UDP)**）中，指定 GlobalProtect 应用程序用于接收来自 MFA 网关的传入 UDP 身份验证提示的端口号。默认端口为 4501。要更改端口，请指定从 1 至 65535 之间的数字。
   - 在 **Trusted MFA Gateways**（信任的 **MFA** 网关）字段中，指定重新导向 URL 的网关地址和端口号（仅非默认端口需要，如 6082），其被 GlobalProtect 应用信任并用于多重身份验证。当 GlobalProtect 应用收到带有重新导向 URL（以指定网络端口为目标）的 UDP 身份验证提示时，GlobalProtect 仅在重新导向 URL 被信任时显示身份验证消息。
   - 配置 **Default Message for Inbound Authentication Prompts**（传入身份验证提示的默认消息）。当用户尝试访问需要额外身份验证的资源时，GlobalProtect 会收到一个包含入站身份验证提示的 UDP 数据包，并显示此消息。UDP 数据包还包含您在配置多重因素身份验证中指定的身份验证门户页面的 URL。GlobalProtect 自动将 URL 附加到消息中。例如，要显示本主题开头所示的通知，请输入以下消息：

     您试图访问需要附加身份验证的受保护资源。通过以下网址继续进行身份验证：
4. 保存代理配置（单击 **OK**（确定）两次），然后 **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

启用向 RADIUS 服务器交付 VSA

与门户或网关通信时，GlobalProtect 端点会发送一些信息，包括端点 IP 地址、操作系统 (OS)、主机名、用户域和 GlobalProtect 应用版本。您可让防火墙在身份验证过程中将此信息作为供应商特定属性 (VSA) 发送给 RADIUS 服务器（默认情况下，防火墙不发送 VSA）。然后，RADIUS 管理员根据这些 VSA 执行管理任务。例如，RADIUS 管理员可使用 OS 属性定义强制对 Microsoft Windows 用户使用密码身份验证和对 Google Android 用户使用一次性密码 (OTP) 身份验证的策略。

以下是此程序的先决条件：

- 将 Palo Alto Networks RADIUS 词典导入您的 RADIUS 服务器。
- 配置 RADIUS 服务器配置文件，将它分配给一个身份验证配置文件。有关更多信息，请参阅设置外部身份验证。
- 将身份验证配置文件分配给 GlobalProtect 门户或网关。有关更多信息，请参阅设置 GlobalProtect 门户访问权限或配置 GlobalProtect 网关。

STEP 1 | 登录至防火墙 CLI。

STEP 2 | 为您想发送的每个 VSA 输入命令：

```
username@hostname> set authentication radius-vsa-on client-source-ip
username@hostname> set authentication radius-vsa-on client-os
username@hostname> set authentication radius-vsa-on client-hostname
username@hostname> set authentication radius-vsa-on user-domain
username@hostname> set authentication radius-vsa-on client-gp-version
```

如果稍后想停止防火墙发送特定 *VSA*，请运行相同命令，但使用 ***radius-vsa-off*** 选项，而不是 ***radius-vsa-on***。

© 2019 Palo Alto Networks, Inc.

启用组映射

由于运行于最终用户系统上的代理或应用要求用户成功进行身份验证方可授权访问 GlobalProtect，因此每个 GlobalProtect 用户的标识为已知状态。但是，如果想要能定义 GlobalProtect 配置和/或基于组成员资格的安全策略，则防火墙须从目录服务器检索组列表以及相应的成员列表。此过程称为组映射。

如果要启用此功能，则须创建 LDAP 服务器配置文件以指示防火墙如何连接和验证至目录服务器，以及如何在目录中搜索用户和组信息。当防火墙成功连接至 LDAP 服务器并检索组映射后，则可在定义代理配置和安全策略时选择组。防火墙支持各种 LDAP 目录服务器，包括 Microsoft Active Directory (AD)、Novell eDirectory 和 Sun ONE Directory Server。

使用以下步骤连接到 LDAP 目录，以使防火墙检索用户到组的映射信息：

STEP 1 | 创建 LDAP 服务器配置文件，该文件将指定如何连接至防火墙通过与其连接以获取组映射信息的目录服务器。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **LDAP**，单击 **Add**（添加）。
2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. 如果此配置文件用于具有多重虚拟系统功能的防火墙，选择一个虚拟系统，或者 **Shared**（共享）为有此配置文件的 **Location**（位置）。
4. 对于每个 LDAP 服务器（最多四个），**Add**（添加）并输入 **Name**（名称）（以标识服务器）、服务器 IP 地址（**LDAP Server**（**LDAP** 服务器）字段）和服务器 **Port**（端口）（默认值为 389）。
5. 从下拉列表中选择服务器 **Type**（类型）：**active-directory**、**e-directory**、**sun** 或 **other**（其他）。
6. 如果您希望此设备使用 SSL 或 TLS 与目录服务器建立更安全的连接，选择 **Require SSL/TLS secured connection**（需要 SSL/TLS 安全连接）复选框（默认选中）。设备使用的协议取决于服务器 **Port**（端口）：
   - 389（默认）— TLS（具体来说，设备使用 StartTLS 操作，这可以将初始明文连接升级至 TLS。）
   - 636 — SSL
   - 任何其他端口 — 设备首先尝试使用 TLS。如果目录服务器不支持 TLS，则设备回滚至 SSL。
7. 如需额外的安全性，选择 **Verify Server Certificate for SSL sessions**（验证 SSL 会话的服务器证书）复选框（默认为清除状态），使设备验证为 SSL/TLS 连接出示的目录服务器的证书。要启用验证，还必须选中 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）复选框。为了验证成功，证书必须符合以下条件之一：
   - 它位于设备证书列表中：**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。如有需要，将证书导入设备。
   - 证书签发机构位于可信证书授权机构列表中：**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Default Trusted Certificate Authorities**（默认可信证书授权机构）。
8. 单击 **OK**（确定）。

STEP 2 | 将 LDAP 服务器配置文件添加到 User-ID 组映射配置中。

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置），然后单击 **Add**（添加）以添加新的组映射配置。
2. 选择 **Server Profile**（服务器配置文件）。
3. 为该组映射配置输入 **Name**（名称）。
4. 选择刚创建的 **Server Profile**（服务器配置文件）。
5. 指定在防火墙启动与 LDAP 目录服务器的连接，以获取任何针对防火墙策略所使用的组的更新之后的 **Update Interval**（更新间隔）秒数（范围为 60 至 86,400 秒）。
6. 确保服务器配置文件 **Enabled**（已启用）组映射。

STEP 3 | （可选）启用 GlobalProtect 以从目录服务器检索序列号。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 能够标识连接端点的状态，并根据出现的端点序列号执行基于 HIP 的安全策略。如果端点受管，您可以将端点序列号绑定至目录服务器中的端点计算机帐户。之后，防火墙可以在从目录服务器检索组映射信息时，为这些受管端点提前提取序列号。

1. 从组映射配置中选择 **Server Profile**（服务器配置文件）。
2. 启用 **Fetch list of managed devices**（提取受管设备列表）选项。

STEP 4 | （可选）指定属性以识别用户和用户组。

1. 从组映射配置中选择 **User and Group Attributes**（用户和组属性）。
2. 在用户属性区域中，指定用于识别单独用户的 **Primary Username**（主用户名）、**E-Mail**（电子邮件）和 **Alternate Username 1-3**（备用用户名 **1-3**）。
3. 在组属性区域中，指定用于识别用户组的 **Group Name**（组名称）、**Group Member**（组成员）和 **E-Mail**（电子邮件）。

STEP 5 | （可选）限制可在策略规则中选择哪些组。

默认情况下，如果不指定组，那么所有组将在策略规则中可用。

1. 从目录服务添加现有组：
   1. 从组映射配置中选择 **Group Include List**（组包含列表）。
   2. 在 Available Groups（可用组列表）中，选择要在策略规则中显示的组，单击添加图标 (⊕) 以将组移动至 Included Groups（包含的组）列表。
2. 如果要将策略规则基于不匹配现有用户组的用户属性，请创建基于 LDAP 筛选器的自定义组：
   1. 从组映射配置中选择 **Custom Group**（自定义组）。
   2. **Add**（添加）新的自定义组。
   3. 输入组 **Name**（名称）（该名称在当前防火墙或虚拟系统的组映射配置中是唯一的）。如果 **Name**（名称）的值与现有 AD 组域的可辨别名称 (DN) 相同，则防火墙会在所有引用中使用自定义组的该名称（例如，在策略和日志中）。
   4. 指定最多 2,048 个 UTF-8 字符的 **LDAP Filter**（**LDAP** 筛选程序），然后单击 **OK**（确定）。该防火墙不会验证 LDAP 筛选程序。

   要优化 *LDAP* 搜索并最大限度地降低对 *LDAP* 目录服务器的性能影响，请使用索引属性并减小搜索范围，以包括策略或可见性所需的用户和组对象。或者，您可以基于 *LDAP* 筛选器创建自定义组。

STEP 6 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关

> GlobalProtect 网关概念
> 配置 GlobalProtect 网关的前提任务
> 配置 GlobalProtect 网关
> 在 GlobalProtect 网关上拆分隧道流量

GlobalProtect 网关概述

因为传递至应用的 GlobalProtect 门户配置包括端点可连接的网关列表，因此建议在配置门户前配置网关。

可配置 GlobalProtect 网关提供两大功能：

- 为连接至网关的 GlobalProtect 应用强制执行安全策略。还可在网关上启用 HIP 采集以实现增强的安全策略粒度。有关启用 HIP 检查的详细信息，请参阅主机信息。
- 提供针对内部企业网络的虚拟专用网 (VPN) 访问权限。VPN 访问将通过介于端点与网关防火墙上隧道接口间的 IPsec 或 SSL 隧道实现。

您也可以配置部署在 *AWS* 云中的 *VM* 系列防火墙上的 *GlobalProtect* 网关。通过在 *AWS* 云中部署 *VM* 系列防火墙，您可以在任何区域中快速和轻松地部署 *GlobalProtect* 网关，而不需要使用设置此基础架构通常所需的费用或 *IT* 物流。有关详情，请参阅用例：VM 系列防火墙作为 AWS 中的 GlobalProtect 网关。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关概念

这些部分提供有关多个网关配置中的网关连接优先级和 GlobalProtect 网关的 MIB 支持的信息。

- 网关的类型
- 多网关配置中的网关优先级
- GlobalProtect MIB 支持

网关的类型

GlobalProtect 网关为从 GlobalProtect 应用发出的通信提供安全实施。此外，如果启用了主机信息配置文件 (HIP) 功能，该网关还将根据端点提交的原始主机数据生成 HIP 报告，并将该信息用于策略实施。

在 Palo Alto Networks 任何下一代防火墙上配置 GlobalProtect 网关。您可以在同一防火墙上同时运行网关和门户，或是在企业内部署多个分散的网关。

GlobalProtect 支持下列网关类型：

- 内部 — 内部网关是配置为 GlobalProtect 网关的内部网络上的一个接口，用于应用访问内部资源的安全策略。与用户 ID 和/或 HIP 验证协同使用时，通过使用内部网关还可提供一种按用户和/或设备状态来辨识和控制通信的安全而精确的方法。在需要进行身份验证以访问关键资源的敏感环境下，内部网关十分有用。您可以在隧道模式或非隧道模式下配置内部网关。执行内部主机检测以确定端点的位置后，GlobalProtect 应用将连接到内部网关。
- 外部网关（自动发现）— 外部网关位于公司网络之外，为您的远程用户提供安全执行和/或虚拟专用网络 (VPN) 访问。默认情况下，GlobalProtect 应用自动连接到 **Best Available**（最佳可用）外部网关，具体取决于您分配给网关、源区域和响应时间的优先级（请参阅多网关配置中的网关优先级）。
- 外部网关（手动）— 手动外部网关也位于公司网络之外，为您的远程用户提供安全执行和/或 VPN 访问。自动发现外部网关与手动外部网关之间的区别在于，GlobalProtect 应用只在用户发起连接时连接到手动外部网关。您还可以为手动外部网关配置不同的身份验证要求。要配置手动网关，您必须在定义 GlobalProtect 代理配置时将网关标识为 **Manual**（手动）。

多网关配置中的网关优先级

要使移动办公人员无论身处何处都能进行安全访问，您可战略性部署额外 Palo Alto Networks 下一代防火墙，并将其配置为 GlobalProtect 网关。要确定应用连接的优选网关，请将网关添加至门户代理配置，然后为每个网关分配连接优先级。请参阅定义 GlobalProtect 代理配置。

如果 GlobalProtect 门户代理配置包含多个网关，则应用将尝试与其代理配置中所列的全部网关通信。应用将使用优先级和响应时间来决定要连接的网关。对于 GlobalProtect 应用 4.0.2 及更低版本，仅当较高优先级网关的响应时间长于所有网关的平均响应时间时，应用才连接至较低优先级网关。

例如，考虑下列 gw1 和 gw2 的响应时间：

姓名	优先级	响应时间
gw1	最高	80 ms
gw2	高	25 ms

应用确定具有最高优先级（数字更大）的网关的响应时间长于两个网关的平均响应时间 (52.5 ms)，因此连接至 gw2。在本例中，应用并没有连接到优先级更高的 gw1，因为 80 ms 的响应时间长于两个网关的平均响应时间。

© 2019 Palo Alto Networks, Inc.

现在考虑下列 gw1、gw2 以及第三个网关 gw3 的响应时间：

姓名	优先级	响应时间
gw1	最高	30 ms
gw2	高	25 ms
gw3	中	50 ms

在本例中，所有网关的平均响应时间为 35 ms。然后，应用评估哪些网关的响应时间快于平均响应时间，并发现 gw1 和 gw2 的响应时间都快于平均响应时间。随后，应用将连接至具有最高优先级的网关。在本例中，应用连接至 gw1，因为 gw1 在响应时间慢于平均响应时间的所有网关中具有最高优先级。

除网关优先级外，还可以将一个或多个源区域添加到外部网关配置中。GlobalProtect 会识别源区域，且只允许用户连接到为该区域配置的网关。对于选择网关，请首先考虑源区域，然后考虑网关优先级。

在 GlobalProtect 应用 4.0.3 和更高版本中，GlobalProtect 应用会优先分配分配最高、最高和中等优先级的网关，而不管网关的响应时间是低优先级还是低优先级。GlobalProtect 应用随后会将分配了低优先级或最低优先级的所有网关添加到网关列表中。这可以确保应用首先尝试连接到您配置的网关，具有更高的优先级。

GlobalProtect MIB 支持

Palo Alto Networks 端点支持标准和企业管理信息库 (MIB)，让您可以监控端点物理状态、利用率统计、陷阱以及其他有用信息。大多数 MIB 使用对象组来描述采用简单网络管理协议 (SNMP) 框架的端点的特征。您必须将这些 MIB 加载进您的 SNMP 管理器中，以监控在这些 MIB 中定义的对象（端点统计和陷阱）（有关详细信息，请参阅 PAN-OS 8.1 管理员指南中的使用 SNMP 管理器浏览 MIB 和对象。

PAN-COMMON-MIB — 包含在企业 MIB 中，使用 panGlobalProtect 对象组。下表描述了构成 panGlobalProtect 对象组的对象。

object	说明
panGPGWUtilizationPct	GlobalProtect 网关利用率（以百分比计）
panGPGWUtilizationMaxTunnels	允许最大隧道数量
panGPGWUtilizationActiveTunnels	活动隧道数量

使用这些 SNMP 对象来监控 GlobalProtect 网关的利用率，并在必要时进行更改。例如，如果活动隧道数量达到 80% 或高于允许最大隧道数量，您应考虑添加额外网关。

© 2019 Palo Alto Networks, Inc.

配置 GlobalProtect 网关的前提任务

完成下列步骤后方可配置 GlobalProtect 网关：

- 为计划在其上配置所有网关的防火墙创建接口（和区域）。对于需隧道连接的网关，则须配置物理接口和虚拟隧道接口。请参阅为 GlobalProtect 创建接口和区域。
- 设置 GlobalProtect 应用为建立与网关的 SSL 连接所需的网关服务器证书和 SSL/TLS 服务配置文件。请参阅在 GlobalProtect 组件间启用 SSL。
- 定义用于验证 GlobalProtect 用户的身份验证配置文件和/或证书配置文件。请参阅身份验证。

© 2019 Palo Alto Networks, Inc.

配置 GlobalProtect 网关

完成前提任务后，配置GlobalProtect 网关：

STEP 1 | 添加网关。

1. **Add**（添加）一个新网关（**Network**（网络）> **GlobalProtect** > **Gateways**（网关））。
2. **Name**（命名）网关。

   网关名称不能包含空格，且对于每个虚拟系统必须是唯一的。最佳实践是在名称中包括有助用户和其他管理员标识网关的位置或其他描述性信息。
3. （可选）选择网关所属的虚拟系统 **Location**（位置）。

STEP 2 | 指定网络信息以允许端点连接至网关。

如果其不存在，则为该网关创建网络接口。

请勿在您配置的接口上附加允许 *HTTP*、*HTTPS*、*Telnet* 或 *SSH* 的接口管理配置文件，因为这样可以从 *Internet* 访问管理界面。按照安全管理访问的最佳实践确保您以防止成功攻击的方式保护对防火墙的管理访问权限。

1. 选择端点用于与网关通信的 **Interface**（接口）。
2. 指定网关 Web 访问的 **IP Address Type**（**IP** 地址类型）和 **IP address**（**IP** 地址）。
   - 将 **IP Address Type**（**IP** 地址类型）设置为：**IPv4 Only**（仅 **IPv4**）、**IPv6 Only**（仅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。如果您的网络支持双栈配置（IPv4 和 IPv6 同时运行），请使用 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。
   - IP 地址必须与 IP 地址类型兼容。例如，`172.16.1.0`（对于 IPv4 地址）或 `21DA:D3:0::2F3b`（对于 IPv6 地址）。对于双栈配置，请输入 IPv4 和 IPv6 地址。

STEP 3 | 配置解密日志设置。

您可以记录成功的和失败的 TLS/SSL 握手，还可以转发解密日志到日志收集器、其他存储设备和特定管理员。

- 防火墙默认只记录失败的 TLS 握手。最佳做法是将成功握手和失败握手都记录下来，以查看设备可用资源允许的解密流量（但不要解密私有或敏感流量；遵循解密最佳实践并尽可能多地解密流量）。
- 如果尚未这样操作，请创建日志转发配置文件以转发解密日志，并在网关配置中进行指定。
- 如果您不仅记录了成功的 TLS 握手，还记录了失败的 TLS 握手，请为解密日志配置一个更大的日志存储空间配额（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **Logging and Reporting Settings**（记录和报告设置）> **Log Storage**（日志存储））。解密日志和常规解密摘要的默认配额（分配）均为设备日志存储容量的 1%。每小时、每天或每周的解密摘要没有默认配额。配置解密日志记录部分中提供更多有关如何将防火墙日志空间分配给解密日志的信息。

STEP 4 | 指定网关如何验证用户。

如果网关的 SSL/TLS 服务配置文件不存在，则部署服务器证书至 GlobalProtect 组件。

如果身份验证配置文件或证书配置文件不存在，则完成身份验证设置任务，为网关配置这些配置文件。

配置以下任何网关 **Authentication**（身份验证）设置（**Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* > **Authentication**（身份验证））：

- 要在网关和 GlobalProtect 应用程序之间建立安全通信，为网关选择 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。

© 2019 Palo Alto Networks, Inc.

SSL/TLS Service Profile（*SSL/TLS* 服务配置文件）中 *TLS* 的 *Max Version*（最高版本）为 *TLSv1.2*。*GlobalProtect* 应用程序和无客户端 *VPN* 连接当前不支持 *TLSv1.3*。

要提供最强的安全性，将 *SSL/TLS* 服务配置文件 *Min Version*（最小版本）设置为*TLSv1.2*。

- 要使用本地用户数据库或外部身份验证服务（例如 LDAP、Kerberos、TACACS+、SAML 或 RADIUS（包括 OTP））验证用户，使用下列设置 **Add**（添加）**Client Authentication**（客户端身份验证）配置：
  - 指定 **Name**（名称）以标识客户端身份验证配置。
  - 标识此配置适用的**OS**（操作系统）类型。默认情况下，配置应用到**Any**（任意）操作系统。
  - 选择或添加 **Authentication Profile**（身份验证配置文件）以对寻求访问网关的端点进行身份验证。
  - 输入用于网关登录的自定义 **Username Label**（用户名标签）（例如，电子邮箱地址 **(`username@domain`)**）。
  - 输入用于网关登录的 **Password Label**（密码标签）（例如，用于基于令牌的双重身份验证的 带通行码允许 ）。
  - 输入 **Authentication Message**（身份验证消息），帮助最终用户了解登录时使用了哪些凭证。此消息的最大长度为 256 个字符（默认为`Enter login credentials`）。
  - 选择以下选项之一，定义用户是否可以通过凭据和/或客户端证书向网关验证身份：
    - 如需要求用户通过用户凭据和客户端证书向网关验证身份，则将 **Allow Authentication with User Credentials OR Client Certificate**（允许通过用户凭据或客户端证书验证身份）选项设置为 **No (User Credentials AND Client Certificate Required)**（否（需要用户凭据和客户端证书））（默认）。
    - 如需允许用户通过用户凭据或客户端证书向网关验证身份，将 **Allow Authentication with User Credentials OR Client Certificate**（允许通过用户凭据或客户端证书验证身份）选项设置为 **Yes (User Credentials OR Client Certificate Required)**（是（需要用户凭据或客户端证书））。

      当您将此选项设置为 **Yes**（是）时，网关先检查端点是否有客户端证书。如果端点没有客户端证书，或您没有为客户端身份验证配置证书配置文件，端点用户可通过其用户凭据向网关验证身份。
- 要基于客户端证书或智能卡/CAC 以验证用户，请选择相应的 **Certificate Profile**（证书配置文件）。您可以使用简单证书注册协议 (SCEP)预先部署客户端证书，或部署特定用户的客户端证书进行身份验证。
  - 如果您需要用户通过其用户凭据和客户端证书向网关验证身份，则必须指定 **Certificate Profile(证书配置文件)**和身份验证配置文件
  - 如果您想要允许用户通过其用户凭据或客户端证书向网关验证身份，且您为用户身份验证指定了 **Authentication Profile**（身份验证配置文件），则 **Certificate Profile**（证书配置文件）为可选项。
  - 如果您想要允许用户通过其用户凭据或客户端证书向网关验证身份，且您没有为用户身份验证指定 **Authentication Profile**（身份验证配置文件），则 **Certificate Profile**（证书配置文件）为必选项。
  - 如果您没有配置任何与指定 OS 匹配的 **Authentication Profile**（身份验证配置文件），则 **Certificate Profile**（证书配置文件）为必选项。

  如果您允许用户通过用户凭据或客户端证书向网关验证身份，请勿选择 *Username Field*（用户名字段）配置为 *None*（无）的 *Certificate Profile*（证书配置文件）。
- 要使用双重身份验证，请选择 **Authentication Profile**（身份验证配置文件）和 **Certificate Profile**（证书配置文件）。这将要求用户通过两种方法成功验证身份才能获得访问权限。

  （仅限 *Chrome*）如果您配置网关以使用客户端证书和 *LDAP* 进行双重身份验证，运行 *Chrome OS 47* 或更新版本的 *Chromebook* 会频繁提示选择客户端证书。为防止出现频

© 2019 Palo Alto Networks, Inc.

繁提示，可配置策略以指定 *Google* 管理控制台内的客户端证书，然后部署策略至您的受管 *Chromebook*：

1. 登录 Google 管理控制台上，选择 *Device management*（设备管理）> *Chrome management*（*Chrome* 管理）> *User settings*（用户设置）。
2. 在客户端证书部分内，输入以下 *URL* 模式以 *Automatically Select Client Certificate for These Sites*（自动选择这些网站的客户端证书）：

   ```
   {"pattern": "https://[*.]","filter":{}}
   ```

3. 单击 *Save*（保存）。*Google* 管理控制台会在几分钟内将策略部署至所有设备。
4. 若要阻止 *GlobalProtect* 用户从隔离设备登录到 *GlobalProtect* 网关，请选择 *Block login for quarantined devices*（阻止隔离设备登录）。

STEP 5 | 启用隧道，然后配置隧道参数。

外部网关需要隧道参数；对于内部网关，隧道参数属于可选项。

要强制使用 SSL-VPN 隧道模式，请禁用（取消选中）**Enable IPSec**（启用 **IPSec**）选项。默认情况下，仅当端点无法建立 IPSec 隧道时才会使用 SSL-VPN。

扩展身份验证 *(X-Auth)* 仅受 *IPSec* 隧道支持。如果您 *Enable X-Auth Support*（启用 *X-Auth* 支持），则不会使用 *GlobalProtect IPSec Crypto* 配置文件。

有关受支持加密算法的详细信息，请参阅 GlobalProtect 应用加密功能。

1. 在“GlobalProtect 网关配置”对话框中，选择 **Agent**（代理）> **Tunnel Settings**（隧道设置）。
2. 启用 **Tunnel Mode**（隧道模式），然后启用拆分隧道。
3. 选择您在为网关创建网络接口时定义的 **Tunnel Interface**（隧道接口）。
4. （可选）输入**Max User**（最大用户数），指定可以同时访问网关以进行身份验证、HIP 更新和 GlobalProtect 应用程序更新的最大用户数。字段为空时显示值范围，该范围根据平台而变化。
5. **Enable IPSec**（启用 **IPSec**），然后选择 **GlobalProtect IPSec Crypto**（**GlobalProtect IPSec** 加密）配置文件来加密 GlobalProtect 应用和网关之间的 VPN 隧道。**default**（默认）配置文件使用 AES-128-CBC 加密算法和 SHA1 身份验证。

   Windows 10 UWP 端点不支持 *IPSec*。

   您还可以创建 **New GlobalProtect IPSec Crypto**（新的 **GlobalProtect IPSec** 加密）配置文件（**GlobalProtect IPSec Crypto**（**GlobalProtect IPSec** 加密）下拉列表），然后配置以下设置：

   1. 指定 **Name**（名称）以标识配置文件。
   2. **Add**（添加）VPN 对等设备可使用的 **Authentication**（身份验证）和 **Encryption**（加密）算法，以协商用于在隧道内安全传输数据的密钥：
      - **Encryption**（加密）— 如果不确定 VPN 对端支持什么，您可按照以下方法添加多个加密算法，最安全的算法优先显示：**aes-256-gcm**、**aes-128-gcm**、**aes-128-cbc**。对等设备将协调最强算法来建立隧道。
      - **Authentication**（身份验证）— 选择身份验证算法 (**sha1**) 以确保数据完整性和真实性。尽管配置文件需要身份验证算法，但此设置仅适用于 AES-CBC 密码 (**aes-128-cbc**)。如果您使用 AES-GCM 加密算法（**aes-256-gcm** 或 **aes-128-gcm**），则此设置被忽略，因为这些密码本身就提供 ESP 完整性保护。
   3. 单击 **OK**（确定）保存配置文件。
6. （可选）如果有任何端点需使用第三方 VPN（例如，运行于 Linux 的 VPNC 客户端）连接至网关，则请选择 **Enable X-Auth Support**（启用 **X-Auth** 支持）。如果启用 X-Auth，则当端点需要时还须提供 **Group**（组）名称和 **Group Password**（组密码）。默认情况下，当用于建立 IPSec 隧道的密钥

© 2019 Palo Alto Networks, Inc.

过期后，用户不需要重新进行身份验证。若要求用户重新进行身份验证，请禁用 **Skip Auth on IKE Rekey**（在 **IKE Rekey** 上跳过身份验证）选项。

> 要为 *strongSwan* 端点 *Enable X-Auth Support*（启用 *X-Auth* 支持），您还必须禁用选项以 *Skip Auth on IKE Rekey*（在 *IKE Rekey* 上跳过身份验证），因为在 *IKE SA* 协商期间，这些端点需要重新验证身份。此外，您必须添加 ***closeaction=restart*** 设置至 *strongSwan IPSec* 配置文件的 `conn %default` 部分。（有关 *StrongSwan IPSec* 配置的详细信息，请参阅设置 strongSwan Ubuntu 和 CentOS 端点的身份验证。）

> 虽然 *iOS* 和 *Android* 端点支持 *X-Auth* 访问，但它在这些端点上只提供有限的 *GlobalProtect* 功能。为此，请使用 *GlobalProtect* 应用以对 *iOS* 和 *Android* 端点上提供的所有 *GlobalProtect* 安全功能进行简化访问。*GlobalProtect iOS* 应用可从 *Apple App Store* 获取。*GlobalProtect Android* 应用可从 *Google Play* 获取。

STEP 6 | （仅限隧道模式）指定客户端设置配置的选择条件。

网关将使用选择条件以确定将哪个配置传递给进行连接的 GlobalProtect 应用。如果有多个配置，则须确保对其进行正确排序。一旦网关找到匹配项（根据 **Source User**（源用户）、**OS**（操作系统）和 **Source Address**（源地址）），会将相关配置传输给用户。因此，较为具体的配置必须先于较为常规的配置。请参阅步骤 13 了解有关对客户端设置配置列表进行排序的说明。

1. 在“GlobalProtect 网关配置”对话框中，选择 **Agent**（代理）> **Client Settings**（客户端设置）。
2. 选择现有客户端配置文件或**Add**（添加）新的配置文件。
3. 配置以下 **Config Selection Criteria**（配置文件选择条件）：
   - 要将此配置部署至指定用户或用户组，**Add**（添加）**Source User**（源用户）（或用户组）。要将此配置部署到预登录模式中拥有 GlobalProtect 应用程序的用户，请从 **Source User**（源用户）下拉列表中选择 **pre-logon**（预登录）；要部署此配置至所有用户，请选择 **any**（任何）。

     > 要将配置部署到特定组，首先必须在启用组映射时，按所述方法将用户映射至组。

   - 要基于此端点操作系统部署此配置，请 **Add**（添加）一种 **OS**（操作系统）（如 Android 或 Chrome）。要将此配置部署至所有操作系统，请选择 **Any**（任何）。
   - 要根据用户位置部署此配置，**Add**（添加）源 **Region**（区域）或 **IP Address**（**IP** 地址）（IPv4 和 IPv6）。要将此配置部署到所有用户地址，请不要指定 **Region**（区域）和 **IP Address**（**IP** 地址）。
4. 单击 **OK**（确定）以保存配置选择条件。

STEP 7 | （仅隧道模式）配置身份验证覆盖设置，以允许网关生成和接受安全加密的 Cookie 对用户进行身份验证。

此功能允许用户在指定时间段（例如，每 24 小时）内仅需出示一次登录凭据。

默认情况下，网关使用身份验证配置文件和可选证书配置文件对用户进行身份验证。当启用身份验证覆盖时，GlobalProtect 缓存成功登录结果，并使用 Cookie 验证用户，而非提示用户出示凭据。有关更多信息，请参阅 门户或网关上的 Cookie 身份验证。如果需要客户端证书，则端点还必须出示有效证书以获取访问权限。

> 如果需要立即阻止对 *Cookie* 尚未过期的设备的访问（例如，当设备遗失或被盗时），可通过将设备添加至阻止列表立即阻止端点访问。

1. 在“GlobalProtect 网关配置”对话框中，选择 **Agent**（代理）> **Client Settings**（客户端设置）。
2. 选择现有客户端配置文件或**Add**（添加）新的配置文件。
3. 配置以下 **Authentication Override**（身份验证覆盖）设置。
   - **Name**（名称）—配置标识。

© 2019 Palo Alto Networks, Inc.

- **Generate cookie for authentication override**（生成用于身份验证覆盖的 **Cookie**）— 允许网关生成加密的特定端点 Cookie 并将身份验证 Cookie 颁发至端点。

  身份验证 cookie 中包含以下字段：

  - `user`— 用于验证用户身份的用户名。
  - `Domain`（域）— 用户的域名。
  - `os`— 设备上使用的应用程序名称。
  - `hostID`— GlobalProtect 分配用于识别主机的唯一 ID。
  - `gen time`— 身份验证 cookie 生成的日期和时间。
  - `ip`— 用于对 GlobalProtect 成功执行身份验证，并获取 cookie 的设备 IP 地址。
- **Accept cookie for authentication override**（接受用于身份验证覆盖的 **Cookie**）— 允许网关使用有效的加密 Cookie 对用户进行身份验证。应用程序出示有效 Cookie 后，网关将验证此 Cookie 是否已经过门户或网关加密，再对其进行解密，然后对用户进行身份验证。

  GlobalProtect 应用必须知道正在连接的用户的用户名，才能从用户端点匹配和检索相关身份验证 *Cookie*。在应用检索 *Cookie* 后，会将 *Cookie* 发送至门户或网关进行用户身份验证。

  （仅限 *Windows*）如果您在门户代理配置中将 Use Single Sign-On（使用单点登录）选项设置为 *Yes*（是）（启用 *SSO*）（*Network*（网络）> *GlobalProtect* > *Portals*（门户）> *<portal-config>* > *Agent*（代理）> *<agent-config>.* > *App*（应用程序）），*GlobalProtect* 应用程序使用 *Windows* 用户名为用户检索本地身份验证 *cookie*。如果您将 *Use Single Sign-On*（使用单点登录）选项设为 *No*（否）（*SSO* 被禁用），则必须允许 *GlobalProtect* 应用保存用户凭据，从而让应用可以为用户检索身份验证 *Cookie*。将 *Save User Credentials*（保存用户凭据）选项设为 *Yes*（是），以保存用户名和密码，或 *Save Username Only*（仅保存用户名）以仅保存用户名。
- **Cookie Lifetime**（**Cookie** 生命周期）— 指定 Cookie 有效的小时数、天数或周数（默认为 24 小时）。小时数范围为 1 至 72；周数范围为 1 至 52；天数范围为 1 至 365。Cookie 过期后，用户必须再次输入登录凭据，网关随后会加密新 Cookie 以发送到应用程序。该值可与为门户配置的 **Cookie Lifetime**（**Cookie** 生命周期）相同或不同。
- **Certificate to Encrypt/Decrypt Cookie**（加密/解密 **Cookie** 的证书）— 选择对 Cookie 进行加密和解密时所使用的 RSA 证书。必须在门户和网关上使用相同证书。

  最佳做法是配置 *RSA* 证书，以使用网络支持的最强摘要算法。

  门户和网关使用 RSA 加密填充方案 PKCS#1 V1.5 来生成 Cookie（使用证书公钥）和解密 Cookie（使用证书私钥）。

STEP 8 | （仅隧道模式 — 可选）配置将 IPv4 或 IPv6 地址分配给连接至网关的端点上虚拟网络适配器的客户端级别 IP 池。

您只能在客户端级别（*Network*（网络）> *GlobalProtect* > *Gateways*（网关）> *<gateway-config>* > *GlobalProtect Gateway Configuration*（*GlobalProtect* 网关配置）> *Agent*（代理）> *Client Settings*（客户端设置）> *<client-setting>* > *Configs*（配置）> *IP Pools*（*IP* 池））或网关级别（*Network*（网络）> *GlobalProtect* > *Gateways*（网关）> *<gateway-config>* > *GlobalProtect Gateway Configuration*（*GlobalProtect* 网关配置）> *Agent*（代理）> *Client IP Pool*（客户端 *IP* 池））配置 *IP* 池。

在非隧道模式下，无需为内部网关配置设置 *IP* 池和隧道分离，因为应用程序将使用已分配给物理网络适配器的网络设置。

© 2019 Palo Alto Networks, Inc.

不支持在配置网关 *IP* 地址池时使用地址对象。

1. 在“GlobalProtect 网关配置”对话框中，选择 **Agent**（代理）> **Client Settings**（客户端设置）。
2. 选择现有客户端配置文件或**Add**（添加）新的配置文件。
3. 配置以下任意 **IP Pools**（**IP** 池）设置：
   - 要指定为需要静态 IP 地址的端点指定身份验证服务器 IP 地址池，启用选项至 **Retrieve Framed-IP-Address attribute from authentication server**（从身份验证服务器检索帧 **IP** 地址属性），然后 **Add**（添加）**Authentication Server IP Pool**（身份验证服务器 **IP** 池）中的子网或 IP 地址范围。建立隧道时，使用与身份验证服务器的帧 IP 属性 匹配的子网或 IP 范围中的一个地址，在远程用户的计算机上创建一个接口。

     身份验证服务器 *IP* 地址池必须足够大以支持所有的并发连接。*IP* 地址分配是静态的，甚至在用户断开连接后予以保留。
   - 要指定将 IPv4 或 IPv6 地址分配给连接至网关的端点的 **IP Pool**（**IP** 池），**Add**（添加）IP 地址子网/范围。您可以添加 IPv4 或 IPv6 子网或范围，或两者组合。

     要确保正确路由回网关，必须使用不同的 IP 地址范围，包括已分配给网关现有 IP 池（如适用）以及已分配给与物理连接到 LAN 的端点的这些地址。我们建议您使用专用 IP 寻址方案。
4. 单击 **Ok**（确定）保存 IP 池配置。

STEP 9 | （仅限隧道模式 — 可选）禁用拆分隧道以确保所有流量（包括本地子网流量）经过 VPN 隧道，以进行检查和实施策略。

STEP 10 | （仅隧道模式 — 可选）根据访问路由配置拆分隧道设置。

STEP 11 | （仅隧道模式 — 可选）根据目标域配置拆分隧道设置。

STEP 12 | （仅隧道模式 — 可选）根据应用程序配置拆分隧道设置。

STEP 13 | （仅限隧道模式 — 可选）为客户端设置配置 DNS 设置。

如果在客户端设置配置中配置至少一个 *DNS* 服务器或 *DNS* 后缀（*Network*（网络）> *GlobalProtect* > *Gateways*（网关）> *<gateway-config>* > *Agent*（代理）> *Client Settings*（客户端设置）> *<client-settings-config>* > *Network Services*（网络服务）），网关会将 *DNS* 服务器和 *DNS* 后缀的配置发送至端点。即使在您配置全局（网关级）*DNS* 服务器和 *DNS* 后缀时，也会发送。

如果您没有在客户端设置配置中配置任何 *DNS* 服务器或 *DNS* 后缀，网关会将全局 *DNS* 服务器和 *DNS* 后缀发送至端点（如有配置）（*Network*（网络）> *GlobalProtect* > *Gateways*（网关）> *<gateway-config>* > *Agent*（代理）> *Network Services*（网络服务））。

1. 在“GlobalProtect 网关配置”对话框中，选择 **Agent**（代理）> **Client Settings**（客户端设置）。
2. 选择现有客户端配置文件或**Add**（添加）新的配置文件。
3. 配置以下任意 **Network Services**（网络服务）设置：
   - 指定 **DNS Server**（**DNS** 服务器）的 IP 地址，以便拥有此客户端设置配置的 GlobalProtect 应用程序向其发送 DNS 查询。您可以采用逗号分隔每个 IP 地址的方式添加最多 10 个 DNS 服务器。
   - 当遇到非限定主机名无法被端点解析时，指定客户端应在本地使用的 **DNS Suffix**（**DNS** 后缀）。

STEP 14 | （仅隧道模式）分配网关代理配置，以便将正确的配置部署至每个 GlobalProtect 应用程序。

© 2019 Palo Alto Networks, Inc.

应用程序进行连接时，网关会将数据包中的源信息与已定义的代理配置进行比较（**Agent**（代理）> **Client Settings**（客户端设置））。与安全规则评估相同，网关会从列表的顶部开始查找匹配项。在其找到匹配项后，会将对应的配置提交给应用程序。

- 要在配置列表中上移网关配置，请选择该配置并单击 **Move Up**（上移）。
- 要在配置列表中下移网关配置，请选择该配置并单击 **Move Down**（下移）。

STEP 15 | （仅隧道模式 — 可选）配置将 IPv4 或 IPv6 地址分配给连接至网关的所有端点上虚拟网络适配器的全局 IP 地址池。

使用此选项，您可以通过在网关级别定义 IP 池，而不是在网关配置中定义每个客户端设置的 IP 池来进行配置。

您只能在网关级别（*Network*（网络）> *GlobalProtect* > *Gateways*（网关）> *<gateway-config>* > *Agent*（代理）> *Client IP Pool*（客户 *IP* 池））或客户端级别（*Network*（网络）> *GlobalProtect* > *Gateways*（网关）> *<gateway-config>* > *Agent*（代理）> *Client Settings*（客户端设置）> *<client-setting>* > *IP Pools*（*IP* 池））来配置 *IP* 池。

不支持在配置网关 *IP* 地址池时使用地址对象。

1. 在“GlobalProtect 网关配置”对话框中，选择 **Agent**（代理）> **Client IP Pool**（客户端 **IP** 池）。
2. **Add**（添加）用于将 IPv4 或 IPv6 地址分配给连接至网关的所有端点的 IP 地址子网或范围。您可以添加 IPv4 或 IPv6 子网或范围，或两者组合。

   要确保正确路由回网关，必须使用不同的 IP 地址范围，包括已分配给网关现有 IP 池（如适用）以及已分配给与物理连接到 LAN 的端点的这些地址。我们建议您使用专用 IP 寻址方案。

STEP 16 | （仅隧道模式）为端点指定网络配置设置。

在非隧道模式下，无需为内部网关配置设定网络设置，因为 *GlobalProtect* 应用程序将使用已分配给物理网络适配器的网络设置。

在“GlobalProtect 网关配置”对话框中，选择 **Agent**（代理）> **Network Services**（网络服务），然后配置以下任何网络配置设置：

- 如果防火墙的某一接口被配置为 DHCP 客户端，则可将 **Inheritance Source**（继承源）设置给该接口，同时将 DHCP 客户端接收的相同设置分配给 GlobalProtect 应用程序。还可从继承源启用选项，以便 **Inherit DNS Suffixes**（继承 **DNS** 后缀）。
- 手动分配 **Primary DNS**（主 **DNS**）服务器，**Secondary DNS**（辅助 **DNS**）服务器，**Primary WINS**（主 **WINS**）服务器，**Secondary WINS**（辅助 **WINS**）服务器，以及**DNS Suffix**（**DNS** 后缀）。可以输入多个 DNS 后缀（以逗号分隔，最多 100 个）。

  DNS Suffix（*DNS* 后缀）不能包含任何非 *ASCII* 字符。

STEP 17 | （可选）修改端点的默认超时设置。

在“GlobalProtect 网关配置”对话框中，选择 **Agent**（代理）> **Connection Settings**（连接设置），然后在超时配置区域配置以下设置：

- 修改单个网关登录会话的最长 **Login Lifetime**（登录生命周期）（默认为 30 天）。在此期间，只要网关在 **Inactivity Logout**（非活动注销）期间从端点收到 HIP 检查，则用户保持登录状态。在此期限后，登录会话自动结束。

© 2019 Palo Alto Networks, Inc.

- 修改 **Inactivity Logout**（非活动注销）期间，以指定非活动会话经过多长时间后自动注销（默认为 3 小时）。如果网关在配置的时间内未从端点收到 HIP 检查，则用户将从 GlobalProtect 注销。
- 修改 **Disconnect on Idle**（闲置时断开连接）设置，以指定经过多长时间后将闲置用户从 GlobalProtect 注销（默认为 180 分钟）。如果 GlobalProtect 应用在配置的时间内未通过 VPN 隧道路由流量，则用户将从 GlobalProtect 注销。此设置仅适用于使用按需连接方法的 GlobalProtect 应用。

STEP 18 | （可选）配置 SSL VPN 隧道的自动恢复。

如果由于网络不稳定或端点状态变化导致 GlobalProtect 连接丢失，则可以通过配置 SSL VPN 隧道的自动恢复，允许或阻止 GlobalProtect 应用自动重新建立 VPN 隧道用于特定网关。

1. 在“GlobalProtect 网关配置”对话框中，选择 **Agent**（代理）> **Client Settings**（客户端设置）。
2. 配置身份验证 Cookie 使用限制的以下选项之一：
   - 要防止 GlobalProtect 应用自动为此网关重新建立 VPN 隧道，请**Disable Automatic Restoration of SSL VPN**（禁用 **SSL VPN** 自动恢复）。
   - 要允许 GlobalProtect 应用自动为此网关重新建立 VPN 隧道，请禁用（取消选中）该选项以 **Disable Automatic Restoration of SSL VPN**（禁用 **SSL VPN** 自动恢复）（默认）。

STEP 19 | （选项）为身份验证 Cookie 配置源 IP 地址实施。

您可以配置 GlobalProtect 门户或网关，以仅在端点 IP 地址与发布 Cookie 的源 IP 地址匹配时，或当端点 IP 地址与指定的网络 IP 地址范围匹配时，接受来自端点的 Cookie。您可以通过 CIDR 子网掩码，如 /24 或 /32 定义网络 IP 地址范围。例如，如果身份验证 Cookie 通过公共源 IP 地址 201.109.11.10 被最初颁发至端点，且网络 IP 地址范围的子网掩码被设为 /24，则身份验证 Cookie 在公共源 IP 地址在 201.109.11.0/24 网络 IP 地址范围内的端点上仍然有效。

1. 在“GlobalProtect 网关配置”对话框中，选择 **Agent**（代理）> **Client Settings**（客户端设置）。
2. 在“身份验证 Cookie 使用限制”部分中，**Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override)**（限制身份验证 **Cookie** 的使用（以便自动恢复 **VPN** 隧道或覆盖身份验证）），然后配置以下条件之一：
   - 如果您选择 **The original Source IP for which the authentication cookie was issued**（颁布验证 **Cookie** 的原源 **IP**），则仅在尝试使用 Cookie 的端点公共源 IP 地址为接受所发布 Cookie 的端点的相同公共源 IP 地址时，验证 Cookie 才有效。
   - 如果您选择 **The original Source IP network range**（原源 **IP** 网络范围），仅当尝试使用 Cookie 的端点公共源 IP 地址位于指定网络 IP 地址范围内时，身份验证 Cookie 才有效。输入 **Source IPv4 Netmask**（源 **IPv4** 网络掩码）或 **Source IPv6 Netmask**（源 **IPv6** 网络掩码）以定义对身份验证 Cookie 有效的网络 IP 地址范围的子网掩码（例如，`32` 或 `128`）。

STEP 20 | （仅隧道模式）从 VPN 隧道排除 HTTP/HTTPS 视频流流量。

STEP 21 | （可选）定义在强制执行带主机信息配置文件 (HIP) 的安全规则时，最终用户将看到的通知消息。

仅当已创建了主机信息配置文件并且将其添加到了安全策略时，此步骤才适用。有关配置 HIP 功能和创建 HIP 通知消息的详细信息，请参阅主机信息。

1. 在“GlobalProtect 网关配置”对话框中，选择 **Agent**（代理）> **HIP Notification**（**HIP** 通知）。
2. 选择现有 HIP 通知配置文件或**Add**（添加）新的配置文件。
3. 配置以下设置：
   - 选择此消息适用的 **Host Information**（主机信息）对象或配置文件。
   - 根据您是否希望在策略中匹配相应的 HIP 配置文件时，或是在配置文件不匹配时显示消息，选择**Match Message**（匹配消息）或 **Not Match Message**（不匹配消息），然后 **Enable**（启用）通知。您可能要为匹配和不匹配创建实例消息，这取决于匹配的对象和策略的目标。对于**Match**

© 2019 Palo Alto Networks, Inc.

Message（匹配消息），您还可启用 **Include Mobile App List**（包含移动应用程序列表）选项，以指示可触发 HIP 匹配的应用程序。
- 选择将消息显示为 **System Tray Balloon**（系统托盘气球）或 **Pop Up Message**（弹出消息）。
- 在您的消息（**Template**（模板））中输入消息文本并格式化，然后单击 **OK**（确定）。
- 为您要定义的每条消息重复执行上述步骤。

STEP 22 | 保存网关配置。

1. 单击 **OK**（确定）以保存设置。
2. **Commit**（提交）更改。

STEP 23 | （可选）要配置 GlobalProtect 应用以显示标签（该标签可在最终用户连接时识别此网关的位置），请指定配置此网关的防火墙的物理位置。

当最终用户体验到异常行为时，如网络性能差，他们可以向支持部门或服务台专业人员提供此位置信息，以协助进行故障排除。他们还可以使用此位置信息确定他们与网关的接近性。根据其接近性，他们可以评估是否需要切换至更近的网关。

如果您没有指定网关位置，*GlobalProtect* 应用会显示空的位置字段。

- 在 **CLI** 中 — 使用以下 CLI 命令指定配置了网关的防火墙的物理位置：

```
<username@hostname> set deviceconfig setting global-protect
 location <location>
```

- 在 **XML API** 中 — 使用以下 XML API 指定配置了网关的防火墙的物理位置：
  - 设备 — 配置了网关的防火墙的名称
  - 位置 — 配置了网关的防火墙的位置

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```


© 2019 Palo Alto Networks, Inc.

在 GlobalProtect 网关上拆分隧道流量

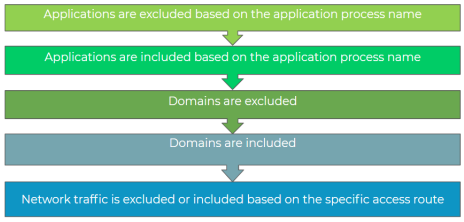
您可以根据访问路由、目标域、应用程序和 HTTP/HTTPS 视频流应用程序配置拆分隧道流量。

通过 *GlobalProtect* 订阅，您可以对 *Windows* 和 *macOS* 端点实施或应用拆分隧道规则。

拆分隧道功能可让您节省带宽并将流量路由到：

- 隧道企业 SaaS 和公共云应用程序以实现全面的 SaaS 应用程序可见性和控制，从而避免在无法隧道化所有流量的环境中与 Shadow IT（影子 IT）相关的风险。
- 将对延迟敏感的流量（如 VoIP）发送到 VPN 隧道之外，而所有其他流量都通过 VPN，以便 GlobalProtect 网关进行检查和实施策略。
- 从 VPN 隧道排除 HTTP/HTTPS 视频流流量。视频流应用程序，如 YouTube 和 Netflix，消耗大量带宽。从 VPN 隧道排除低风险视频流流量可以减少网关的带宽消耗。

拆分隧道规则按以下顺序应用于 Windows和 macOS 端点：



有关如何在网关上配置拆分隧道流量，请参阅以下部分：

- 根据访问路由配置拆分隧道
- 根据域和应用程序配置拆分隧道
- 从 GlobalProtect VPN 隧道排除视频流量

根据访问路由配置拆分隧道

如果不包括或排除路由，则每个请求都会通过 VPN 隧道进行路由（无拆分隧道）。您可以包括或排除通过 VPN 隧道发送的特定目标 IP 子网流量。通过 VPN 隧道发送的路由可以定义为隧道中包含的路由或从隧道中排除的路由，或两者组合。例如，可以将一个拆分隧道设置为允许远程用户不经由 VPN 隧道便可访问互联网。路由越具体，优先级越高。

当您将拆分隧道流量定义为包括访问路由时，这些路由是网关推送到远程用户端点的路由，以指定用户端点可以通过 VPN 隧道发送的流量。当您将拆分隧道流量定义为排除访问路由时，这些路由将通过端点上的物理适配器发送，而非经由虚拟适配器（隧道）通过 GlobalProtect VPN 隧道发送。通过按访问路由排除拆分隧道流量，您可以将对延迟敏感或高带宽消耗流量发送到 VPN 隧道之外，而所有其他流量都通过 VPN 路由以供 GlobalProtect 网关检查和实施策略。

本地路由优先于网关发布的路由。当您启用拆分隧道时，用户可以直接访问代理和本地资源（如本地打印机），而不通过 VPN 隧道发送任何本地子网流量。通过禁用隧道分离，当用户连接至 GlobalProtect 时，您可以强制所有流量经过 VPN 隧道以进行检查和实施策略。根据您是启用还是禁用对本地网络的直接访问，您可以考虑以下 IPv4 和 IPv6 流量行为。

© 2019 Palo Alto Networks, Inc.

表 **1: IPv4** 流量行为

IPv4 流量至本地子网	“不能直接访问本地网络”选项已启用		“不能直接访问本地网络”选项已禁用	
	建立隧道前	建立隧道后	建立隧道前	建立隧道后
新传入流量	通过物理适配器允许本地子网流量。	（仅限 Windows 10） 当您根据目标域和应用程序禁用拆分隧道时，流量将通过 VPN 隧道发送。 当您根据目标域和应用程序启用拆分隧道时，通过物理适配器允许本地子网流量。 （仅限 macOS）通过物理适配器允许本地子网流量。	通过物理适配器允许本地子网流量。	通过物理适配器允许本地子网流量。
新传出流量	通过物理适配器允许本地子网流量。	流量通过 VPN 隧道发送。	通过物理适配器允许本地子网流量。	通过物理适配器允许本地子网流量。
现有流量	通过物理适配器允许本地子网流量。	流量终止。	通过物理适配器允许本地子网流量。	通过物理适配器允许本地子网流量。

表 **2: IPv6** 流量行为

IPv6 流量至本地子网	“不能直接访问本地网络”选项已启用		“不能直接访问本地网络”选项已禁用	
	建立隧道前	建立隧道后	建立隧道前	建立隧道后
新传入流量	通过物理适配器允许本地子网流量。	通过物理适配器允许本地子网流量。	通过物理适配器允许本地子网流量。	通过物理适配器允许本地子网流量。
新传出流量	通过物理适配器允许本地子网流量。	流量通过 VPN 隧道发送。	通过物理适配器允许本地子网流量。	通过物理适配器允许本地子网流量。
现有流量	通过物理适配器允许本地子网流量。	通过物理适配器允许本地子网流量。	通过物理适配器允许本地子网流量。	通过物理适配器允许本地子网流量。

使用以下步骤基于访问路由配置拆分隧道。

STEP 1 | 准备工作：

1. 配置 GlobalProtect 网关。
2. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* 修改现有网关或添加新网关。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 启用拆分隧道。

1. 在 **GlobalProtect Gateway Configuration**（**GlobalProtect** 网关配置）对话框中，选择 **Agent**（代理）> **Tunnel Settings**（隧道设置）以启用 **Tunnel Mode**（隧道模式）。
2. 为 GlobalProtect 应用程序配置隧道参数。

STEP 3 | （仅限隧道模式）禁用拆分隧道以确保所有流量（包括本地子网流量）经过 VPN 隧道，以进行检查和实施策略。

1. 在 **GlobalProtect Gateway Configuration**（**GlobalProtect** 网关配置）对话框中，选择 **Agent**（代理）> **Client Settings**（客户端设置）> *<client-setting-config>* 来选择现有客户端设置配置或添加新配置。
2. 选择 **Split Tunnel**（隧道分离）> **Access Route**（访问路由），然后启用 **No direct access to local network**（不能直接访问本地网络）选项。

   如果启用此选项，拆分隧道流量将被禁用，当连接到 *GlobalProtect* 时，用户不能向代理或本地资源直接发送流量。

STEP 4 | （仅隧道模式）基于访问路由配置拆分隧道设置。

当 GlobalProtect 应用程序与网关建立隧道时，此拆分隧道配置将分配至端点上的虚拟网络适配器。

避免指定相同的访问路由作为包含和排除访问路由；这会导致配置错误。

您可以通过指定目标子网或地址对象（**IP Netmask**（**IP** 网络掩码）类型）来路由要包含在隧道中或从中排除的特定流量。

1. 在 **GlobalProtect Gateway Configuration**（**GlobalProtect** 网关配置）对话框中，选择 **Agent**（代理）> **Client Settings**（客户端设置）> *<client-setting-config>* 来选择现有客户端设置配置或添加新配置。
2. 配置以下任何一个基于访问路由的 **Split Tunnel**（拆分隧道）设置（**Split Tunnel**（拆分隧道）> **Access Route**（访问路由））：
   - （可选）在 **Include**（包含）区域中，**Add**（添加）目标子网或地址对象（**IP Netmask**（**IP** 网络掩码）类型），以便仅将指定给 LAN 的特定流量路由到 GlobalProtect。您可以包含 IPv6 或 IPv4 子网。

     在 PAN-OS 8.0.2 及更高版本上，最多可以使用 100 条访问路由来将流量包括在拆分隧道网关配置中。除非与 GlobalProtect 应用程序 4.1.x 或更高版本结合使用，否则最多可使用 1000 条访问路由。
   - （可选）在 **Exclude**（排除）区域中，**Add**（添加）您希望应用程序排除的目标子网或地址对象（**IP Netmask**（**IP** 网络掩码）类型）。排除的路由应比包括的路由更具体，以免排除不想排除的流量。您可以排除 IPv6 或 IPv4 子网。在拆分隧道网关配置中，防火墙最多支持 100 条排除访问路由。除非与 GlobalProtect 应用程序 4.1 或更高版本结合使用，否则最多可使用 200 条排除访问路由。

     不能排除在 *Chromebook* 上运行 *Android* 的端点的访问路由。*Chromebook* 只支持 *IPv4* 路由。
3. 单击 **OK**（确定）以保存拆分隧道配置。

STEP 5 | 保存网关配置。

1. 单击 **OK**（确定）以保存设置。
2. **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

根据域和应用程序配置拆分隧道

将拆分隧道配置为包括基于目标域和端口（可选）或应用程序的所有流量（IPv4 和 IPv6）时，流向该特定域或应用程序的所有流量都通过 VPN 隧道发送以进行检查和实施策略。例如，您可以使用 ***Salesforce.com** 目标域允许所有 Salesforce 流量通过 VPN 隧道。通过在 VPN 隧道中包含所有 Salesforce 流量，您可以提供对整个 Salesforce 域和子域的安全访问。您可以在未指定目标 IP 地址子网的情况下配置拆分隧道，从而将拆分隧道功能扩展至具有动态公共 IP 地址的域和应用程序，例如 SaaS 和公共云应用程序。

将拆分隧道配置为基于目标域和端口（可选）或应用程序排除流量（IPv4 和 IPv6)时，该特定应用程序或域的所有流量都直接发送到端点上的物理适配器，而不进行检查。例如，您可以使用 **C:\Program Files (x86)\Skype\Phone\Skype** 应用程序进程名称从 VPN 隧道中排除所有 Skype 流量。

仅在 *Windows 7 Service Pack 2* 和更高版本以及 *macOS 10.10* 和更高版本的端点上受支持。

使用以下步骤将拆分隧道配置为根据目标域或应用程序进程名称包含或排除流量。

STEP 1 | 准备工作：

1. 配置 GlobalProtect 网关。
2. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* 修改现有网关或添加新网关。

STEP 2 | 启用拆分隧道。

1. 在 **GlobalProtect Gateway Configuration**（**GlobalProtect** 网关配置）对话框中，选择 **Agent**（代理）> **Tunnel Settings**（隧道设置）以启用 **Tunnel Mode**（隧道模式）。
2. 为 GlobalProtect 应用程序配置隧道参数。

STEP 3 | （仅隧道模式）根据目标域配置拆分隧道设置。当 GlobalProtect 应用程序与网关建立隧道时，这些设置将分配至端点的虚拟网络适配器。

（需要 5.2 版本的 GlobalProtect™ 应用程序。）

如果您已在 GlobalProtect 门户的 **App Configurations**（应用程序配置）区域将 **Both Network Traffic and DNS**（网络流量和 **DNS** 两者）指定为 **Split-Tunnel Option**（拆分隧道选项），则您不仅可以应用网络流量，还可以应用 DNS 流量。

1. 在 GlobalProtect Gateway Configuration（GlobalProtect 网关配置）对话框中，选择 **Agent**（代理）> **Client Settings**（客户端设置）> *<client-setting-config>* 来选择现有客户端设置配置或添加新配置。
2. （可选）**Add**（添加）您想要通过 VPN 连接使用目标域和端口路由至 GlobalProtect 的 SaaS 或公共云应用程序（**Split Tunnel**（拆分隧道）> **Domain and Application**（域和应用程序）> **Include Domain**（包含域））。您最多可在列表上添加 200 个条目。例如，添加 `*.gmail.com` 允许所有 Gmail 流量通过 VPN 隧道。
3. （可选）**Add**（添加）您想要使用目标域和端口从 VPN 隧道排除的 SaaS 或公共云应用程序（**Split Tunnel**（拆分隧道）> **Domain and Application**（域和应用程序）> **Exclude Domain**（排除域））。您最多可在列表上添加 200 个条目。例如，添加 `*.target.com` 可排除来自 VPN 隧道的所有 Target 流量。
4. 单击 **OK**（确定）以保存拆分隧道设置。

STEP 4 | （仅隧道模式）根据应用程序配置拆分隧道设置。

无法将 *Safari* 流量添加到 *macOS* 端点上基于应用程序的拆分隧道规则。

您可以使用环境变量根据 *Windows* 和 *macOS* 端点上的应用程序配置拆分隧道。

© 2019 Palo Alto Networks, Inc.

1. 在 GlobalProtect Gateway Configuration（GlobalProtect 网关配置）对话框中，选择 **Agent**（代理）> **Client Settings**（客户端设置）> *<client-setting-config>* 来选择现有客户端设置配置或添加新配置。
2. （可选）**Add**（添加）您想要通过 VPN 连接使用应用程序进程名路由至 GlobalProtect 的 SaaS 或公共云应用程序（**Split Tunnel**（拆分隧道）> **Domain and Application**（域和应用程序）> **Include Client Application Process Name**（包含客户端应用程序进程名））。您最多可在列表上添加 200 个条目。例如，添加 **`/Applications/RingCentral for Mac.app/Contents/MacOS/Softphone`** 可允许所有基于 RingCentral 的流量通过 macOS 端点上的 VPN 隧道。
3. （可选）**Add**（添加）您想要使用应用程序进程名从 VPN 隧道 排除的 SaaS 或公共云应用程序（**Split Tunnel**（拆分隧道）> **Domain and Application**（域和应用程序）> **Exclude Client Application Process Name**（排除客户端应用程序进程名））。您最多可在列表上添加 200 个条目。例如，添加 **`/Applications/Microsoft Lync.app/Contents/MacOS/Microsoft Lync`** 可排除 VPN 隧道中所有 Microsoft Lync 应用程序流量。
4. 单击 **OK**（确定）以保存拆分隧道设置。

STEP 5 | 保存网关配置。

1. 单击 **OK**（确定）保存网关配置。
2. **Commit**（提交）更改。

从 GlobalProtect VPN 隧道排除视频流量

您可以配置拆分隧道，以排除通过 VPN 隧道发送到特定域的 HTTP/HTTPS 视频流流量。这允许直接从端点上的物理接口发送视频流量。防火墙上的 App-ID 功能可在流量执行拆分隧道前识别视频流。从 VPN 隧道排除低风险的视频流流量（YouTube 和 Netflix 等）时，您可以减少网关的带宽消耗。

所有视频流量类型都将重定向至以下视频流应用程序：

- YouTube
- Dailymotion
- Netflix

如果从 VPN 排除任何其他视频流应用程序，以下是仅适用于这些应用程序重定向的视频流类型：

- MP4
- WebM
- MPEG

使用以下步骤配置拆分隧道以从 VPN 隧道排除视频流流量。

STEP 1 | 准备工作：

1. 遵循以下前提条件：
   - 仅在 Windows 7 Service Pack 2 和更高版本以及 macOS 10.10 和更高版本的端点上受支持。
   - 确保用于将 IP 地址分配给这些端点上虚拟网络适配器的 IP 池不包含任何 IPv6 地址。如果 Windows 或 macOS 端点上的物理适配器仅支持 IPv4 地址，当您配置将 IPv6 地址分配给连接至网关的端点上虚拟网络适配器的 GlobalProtect 网关时，端点用户无法访问您从 VPN 隧道排除的视频流应用陈谷.
   - 如果从 VPN 隧道排除视频流流量，请不要在 VPN 隧道中包含 Web 浏览器应用程序，如 Firefox 或 Chrome。这能确保拆分隧道配置中不会存在逻辑冲突，您的用户也不会从 web 浏览器传输视频流。
   - 要从 VPN 隧道中排除 Sling TV 应用程序流量，请根据应用程序配置拆分隧道。
2. 配置 GlobalProtect 网关。
3. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* 修改现有网关或添加新网关。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 启用拆分隧道。

1. 在 **GlobalProtect Gateway Configuration**（**GlobalProtect** 网关配置）对话框中，选择 **Agent**（代理）> **Tunnel Settings**（隧道设置）以启用 **Tunnel Mode**（隧道模式）。
2. 为 GlobalProtect 应用程序配置隧道参数。

STEP 3 | （仅隧道模式）从 VPN 隧道排除 HTTP/HTTPS 视频流流量。

1. 在 **GlobalProtect Gateway Configuration**（**GlobalProtect** 网关配置）对话框中，选择 **Agent**（代理）> **Video Traffic**（视频流量）。
2. 启用此选项，**Exclude video applications from the tunnel**（从隧道排除视频应用程序）。

   如果启用此选项，但未从 *VPN* 隧道排除特定视频流应用程序，则所有视频流流量都将被排除。

3. （可选）**Browse**（浏览）**Applications**（应用程序）列表，参看您可以从 VPN 隧道排除的所有视频流应用程序。单击要排除的应用程序的添加 ( ) 图标。例如，单击**directv**的添加图标可从 VPN 隧道排除 DIRECTV 视频流流量。
4. 使用 **Applications**（应用程序）下拉列表（**Applications**（应用程序）列表的缩减版本），**Add**（添加）想要从 VPN 隧道排除的视频流应用程序。最多可以向列表中添加 200 个视频应用程序条目。例如，选择 **youtube-streaming**，可从 VPN 隧道排除所有基于 YouTube 的视频流流量。

STEP 4 | 保存网关配置。

1. 单击 **OK**（确定）保存网关配置。
2. **Commit**（提交）更改。

GlobalProtect 门户

> GlobalProtect 门户概述
> 配置 GlobalProtect 门户的前提任务
> 设置 GlobalProtect 门户访问权限
> 定义 GlobalProtect 代理配置
> 自定义 GlobalProtect 应用程序
> 自定义 GlobalProtect 门户登录、欢迎和帮助页面
> GlobalProtect 无客户端 VPN

GlobalProtect 门户概述

GlobalProtect 门户提供了针对 GlobalProtect 基础架构的管理功能。参与 GlobalProtect 网络的每个端点都会从门户收到配置信息，其中包括可用网关的相关信息以及连接到这些网关时可能需要的任何客户端证书的相关信息。此外，门户还控制 GlobalProtect 应用程序软件的行为，以及向 macOS 和 Windows 端点的分发。

该门户不会分发在移动端点上使用的 *GlobalProtect* 应用。要获取适用于移动端点的 *GlobalProtect* 应用，最终用户须从设备商店下载该应用。*iOS* 设备的 *App Store*、*Android* 设备的 *Google Play*、*Chromebook* 设备的 *Chrome Web Store* 或 *Windows 10 UWP* 设备的 *Microsoft Store*。但是，部署至移动应用用户的代理配置并不控制移动端点可访问的网关。有关受支持版本的详细信息，请参阅 GlobalProtect 支持哪些操作系统版本？。

除了分发 GlobalProtect 应用软件外，您还可以配置 GlobalProtect 门户，以提供对使用 HTML、HTML5 和 Javascript 技术的常见企业 Web 应用程序的远程安全访问。用户无需安装 GlobalProtect 应用软件，即可从启用 SSL 的 Web 浏览器进行安全访问。如果您需要合作伙伴或承包商能够访问应用程序，且安全启用非托管资产（包括个人端点），则这非常有用。请参考 GlobalProtect 无客户端 VPN。

© 2019 Palo Alto Networks, Inc.

配置 GlobalProtect 门户的前提任务

完成下列任务后方可配置 GlobalProtect 门户：

- 已为计划在其上配置门户的防火墙创建接口（和区域）。请参阅为 GlobalProtect 创建接口和区域。
- 设置待部署至最终用户的门户服务器证书、网关服务器证书、SSL/TLS 服务配置文件和任意客户端证书（可选），以便为 GlobalProtect™ 服务启用 SSL/TLS 连接。请参阅在 GlobalProtect 组件间启用 SSL。
- 定义门户可用于验证 GlobalProtect 用户的可选身份验证配置文件和证书配置文件。请参阅身份验证。
- 配置 GlobalProtect 网关并理解多网关配置中的网关优先级。

© 2019 Palo Alto Networks, Inc.

设置 GlobalProtect 门户访问权限

完成配置 GlobalProtect 门户的前提任务后，请按如下步骤配置 GlobalProtect 门户：

STEP 1 | 添加门户。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portal**（门户），然后 **Add**（添加）门户。
2. 输入门户的 **Name**（名称）。

   网关名称不能包含空格，且对于每个虚拟系统必须是唯一的。
3. （可选）从 **Location**（位置）字段中选择该门户所属的虚拟系统。

STEP 2 | 指定网络设置以允许 GlobalProtect 应用与门户进行通信。

如果尚未为门户创建网络接口，请参阅为 GlobalProtect 创建接口和区域。如果尚未为门户创建 SSL/TLS 服务配置文件，请参阅将服务器证书部署至 GlobalProtect 组件。

请勿在已配置 *GlobalProtect* 门户或网关的接口上附加允许 *HTTP*、*HTTPS*、*Telnet* 或 *SSH* 的接口管理配置文件，因为这样可以从 *Internet* 访问管理界面。按照安全管理访问的最佳实践确保您以防止成功攻击的方式保护对防火墙的管理访问权限。

1. 选择 **General**（常规）。
2. 在“网络设置”区域，选择 **Interface**（接口）。
3. 指定门户 Web 服务的 **IP Address Type**（**IP** 地址类型）和 **IP address**（**IP** 地址）。
   - IP 地址类型可以是 **IPv4 Only**（仅 **IPv4**）、**Ipv6**、**IPv6 Only**（仅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。如果您的网络支持双栈配置（IPv4 和 IPv6 同时运行），请使用 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。
   - IP 地址必须与 IP 地址类型兼容。例如，`172.16.1.0`（对于 IPv4 地址）或 `21DA:D3:0::2F3b`（对于 IPv6 地址）。对于双栈配置，请输入 IPv4 和 IPv6 地址。
4. 选择 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。

STEP 3 | 选择**General**（常规），并配置解密日志设置。

您可以记录成功的和失败的 TLS/SSL 握手，还可以转发解密日志到日志收集器、其他存储设备和特定管理员。

- 防火墙默认只记录失败的 TLS 握手。最佳做法是将成功握手和失败握手都记录下来，以查看设备可用资源允许的解密流量（但不要解密私有或敏感流量；遵循解密最佳实践并尽可能多地解密流量）。
- 如果尚未这样操作，请创建日志转发配置文件以转发解密日志，并在网关配置中进行指定。
- 如果您不仅记录了成功的 TLS 握手，还记录了失败的 TLS 握手，请为解密日志配置一个更大的日志存储空间配额（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **Logging and Reporting Settings**（记录和报告设置）> **Log Storage**（日志存储））。解密日志和常规解密摘要的默认配额（分配）均为设备日志存储容量的 1%。每小时、每天或每周的解密摘要没有默认配额。配置解密日志记录部分中提供更多有关如何将防火墙日志空间分配给解密日志的信息。

STEP 4 | 选择自定义登录和帮助页面或完全禁用登录和帮助页面。有关创建自定义登录页面和帮助页面的更多详细信息，请参阅自定义 GlobalProtect 门户登录、欢迎和帮助页面。

1. 选择 **General**（常规）。
2. 在“外观”区域，配置下列设置中的任一项：
   - 要设置用户访问门户的 **Portal Login Page**（门户登录页面），请选择**factory-default**（出厂默认值）登录页面，**Import**（导入）自定义登录页面或 **Disable**（禁用）对登录页面的访问权限。

© 2019 Palo Alto Networks, Inc.

- 要设置 **App Help Page**（应用帮助页面）以通过 GlobalProtect 应用向用户提供帮助，请选择 **factory-default**（出厂默认值）帮助页面，**Import**（导入）自定义帮助页面，或选择 **None**（无）以从 GlobalProtect 状态面板的 **Settings**（设置）菜单中删除 **Help**（帮助）选项。

STEP 5 | 指定门户如何验证用户。

1. 选择 **Authentication**（验证）。
2. 配置以下任意门户身份验证设置：

> 如果尚未为门户创建服务器证书并发出网关证书，请参阅将服务器证书部署至 GlobalProtect 组件。

- 要在门户和 GlobalProtect 应用之间建立安全通信，选择已为门户配置的 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。
- 要使用本地用户数据库或外部身份验证服务（如 LDAP、Kerberos、TACACS+、SAML 或 RADIUS（包括 OTP））来验证用户，请定义 GlobalProtect 客户端身份验证配置。
- 要基于客户端证书或智能卡/CAC 以验证用户，请选择相应的 **Certificate Profile**（证书配置文件）。您可以使用简单证书注册协议 (SCEP)预先部署客户端证书，或部署特定用户的客户端证书进行身份验证。
  - 如果您想要求用户通过用户凭据和客户端证书向门户验证身份，则 **Certificate Profile**（证书配置文件）和验证配置文件都需要。
  - 如果您想要允许用户通过其用户凭据或客户端证书向门户或网关验证身份，且您为用户身份验证选择了 Authentication Profile（身份验证配置文件），则 **Certificate Profile**（证书配置文件）为可选项。
  - 如果您想要允许用户通过其用户凭据或客户端证书向门户或网关验证身份，且您没有为用户身份验证选择 Authentication Profile（身份验证配置文件），则 **Certificate Profile**（证书配置文件）为必选项。
  - 如果您没有配置任何与指定 OS 匹配的 Authentication Profile（身份验证配置文件），则 **Certificate Profile**（证书配置文件）为必选项。

> 如果您允许用户通过用户凭据或客户端证书身份向门户验证身份，请选择 *Username Field*（用户名字段）配置为 *Subject*（主题）或 *Subject Alt*（主题备选）的 *Certificate Profile*（证书配置文件）。

STEP 6 | 定义用户成功向门户验证身份后，GlobalProtect 应用从连接端点收集的数据。

GlobalProtect 应用发送此数据至门户，以匹配您为各门户代理配置定义的 选择条件。基于这些条件，门户将传递指定代理配置至连接的 GlobalProtect 应用。

1. 选择 **Portal Data Collection**（门户数据收集）。
2. 配置以下任意数据收集设置：
   - 如果您想要 GlobalProtect 应用收集来自连接端点的计算机证书，请选择指定了您想要收集的计算机证书的 **Certificate Profile**（证书配置文件）。
   - 如果您想要 GlobalProtect 应用从连接端点收集自定义主机信息，请在自定义检查区域内定义以下注册表或 plist 数据：
     - 要从 Windows 端点收集注册表数据，请选择 **Windows**，然后 **Add**（添加）**Registry Key**（注册表项）和对应的 **Registry Value**（注册表值）。
     - 要从 macOS 端点收集 plist 数据，请选择 **Mac**，然后 **Add**（添加）**Plist** 项和对应 **Key**（项）值。

STEP 7 | 保存门户配置。

1. 单击 **OK**（确定）以保存设置。
2. **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

定义 GlobalProtect 客户端身份验证配置

每个 GlobalProtect 客户端身份验证配置均指定了允许用户验证至 GlobalProtect 门户的设置。您可为各操作系统自定义这些设置，或者配置适用于所有端点的设置。例如，您可配置安卓用户使用 RADIUS 身份验证，Windows 用户使用 LDAP 身份验证。您还可为从 Web 浏览器访问门户（以下载 GlobalProtect 应用程序）的用户或第三方 IPsec VPN (X-Auth) 访问 GlobalProtect 网关自定义客户端身份验证。

STEP 1 | 设置 GlobalProtect 门户访问权限。

STEP 2 | 指定门户如何验证用户。

可使用本地用户数据库或外部身份验证服务（例如 LDAP、Kerberos、TACACS+、SAML 或 RADIUS（包括 OTP））配置 GlobalProtect 门户对用户进行身份验证。如果尚未设置身份验证配置文件和/或证书配置文件，请参阅 Authentication（身份验证）以了解相关操作说明。

在 GlobalProtect Portal Configuration（GlobalProtect 门户配置）对话框中（**Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>*），选择 **Authentication**（身份验证）以 **Add**（添加）带有如下设置的新 **Client Authentication**（客户端身份验证）：

- 输入 **Name**（名称）以标识客户端身份验证配置。
- 指定想要部署此配置的端点。要将此配置应用至所有端点，请接受默认 **OS**（操作系统）为 **Any**（任意）。要将此配置应用至运行指定操作系统的端点，选择 **OS**（操作系统），如 **Android**。或者，您可以将此配置应用至通过 Web **Browser**（浏览器）连接至无客户端 VPN 门户的端点。
- 要允许用户使用用户凭据向门户或网关验证身份，请选择或添加 **Authentication Profile**（身份验证配置文件）。
  - 如果您想要求用户通过用户凭据和客户端证书向门户或网关验证身份，则 **Authentication Profile**（身份验证配置文件）和证书配置文件都需要。
  - 如果您想要允许用户通过其用户凭据或客户端证书向门户或网关验证身份，且您为用户身份验证选择了证书配置文件，则 **Authentication Profile**（身份验证配置文件）为可选项。
  - 如果您想要允许用户通过其用户凭据或客户端证书向门户或网关验证身份，但您没有为用户身份验证选择证书配置文件（或您将 **Certificate Profile**（证书配置文件）设为 **None**（无）），则 **Authentication Profile**（身份验证配置文件）为必选项。
- （可选）输入用于 GlobalProtect 门户登录的自定义 **Username Label**（用户名标签）（例如，**Email Address**（电子邮件地址）**(username@domain)**）。
- （可选）输入用于 GlobalProtect 门户登录的自定义 **Password Label**（密码标签）（例如，用于基于令牌的双重身份验证的 **Passcode**（通行码））。
- （可选）输入 **Authentication Message**（身份验证消息），帮助最终用户了解登录时使用了哪些凭证。此消息的最大长度为 256 个字符（默认为`Enter login credentials`）。
- 选择以下选项之一，定义用户是否可以通过凭据和/或客户端证书向门户验证身份：
  - 如需要求用户通过用户凭据和客户端证书向门户验证身份，将 **Allow Authentication with User Credentials OR Client Certificate**（允许通过用户凭据或客户端证书身份验证）选项设置为 **No (User Credentials AND Client Certificate Required)**（否（需要用户凭据和客户端证书））（默认）。
  - 如需允许用户通过用户凭据或客户端证书向门户验证身份，将 **Allow Authentication with User Credentials OR Client Certificate**（允许通过用户凭据或客户端证书验证）选项设置为 **Yes (User Credentials OR Client Certificate Required)**（是（需要用户凭据或客户端证书））。

    当您将此选项设置为 **Yes**（是）时，GlobalProtect 门户会先搜索端点是否有客户端证书。如果端点没有客户端证书，或您没有为客户端身份验证配置证书配置文件，则最终用户必须通过其用户凭据向门户验证身份。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 利用列表顶部的特定操作系统配置和适用于列表底部的 **Any**（任何）操作系统的配置分配客户端身份验证配置（**Network**（网络）> **GlobalProtect** > **Portals**（门户）> **<portal-config>** > **Authentication**（身份验证））。与安全规则评估相同，门户从列表的顶部开始查找匹配项。在其找到匹配项后，会将对应的配置提交给应用程序。

- 要在配置列表中上移客户端身份验证配置，请选择该配置并单击 **Move Up**（上移）。
- 要在配置列表中下移客户端身份验证配置，请选择该配置并单击 **Move Down**（下移）。

STEP 4 | （可选）要使用身份验证配置文件和证书配置文件启用双重身份验证，请在门户配置中配置这两者。

门户必须在用户获得访问权限之前使用这两种方法对端点进行身份验证。

（仅限 *Chrome*）如果您配置门户以使用客户端证书和 *LDAP* 进行双重身份验证，运行 *Chrome OS 47* 或更新版本的 *Chromebook* 会频繁提示选择客户端证书。为防止出现频繁提示，可配置策略以指定 *Google* 管理控制台内的客户端证书，然后部署策略至您的受管 *Chromebook*：

1. 登录 Google 管理控制台上，选择 *Device management*（设备管理）> *Chrome management*（*Chrome* 管理）> *User settings*（用户设置）。
2. 在客户端证书部分内，输入以下 *URL* 模式以 *Automatically Select Client Certificate for These Sites*（自动选择这些网站的客户端证书）：

   ```
   {"pattern": "https://[*.]","filter":{}}
   ```
3. 单击 *Save*（保存）。*Google* 管理控制台会在几分钟内将策略部署至所有设备。

在 GlobalProtect Portal Configuration（GlobalProtect 门户配置）对话框中（**Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>*），选择 **Authentication**（身份验证）以选取 **Certificate Profile**（证书配置文件），从而根据客户端证书或智能卡对用户进行身份验证。

证书的“公用名 *(CN)*”和“主题备用名称 *(SAN)*”字段（如适用）必须与在其上配置门户的接口的 *IP* 地址或完全限定域名 *(FQDN)* 完全匹配；否则，与门户的 *HTTPS* 连接将失败。

STEP 5 | 保存门户配置。

1. 单击 **OK**（确定）以保存您的配置。
2. **Commit**（提交）更改。

定义 GlobalProtect 代理配置

当 GlobalProtect 用户连接并成功验证至 GlobalProtect 门户时，门户会基于已定义的设置将代理配置发送至应用。如果您具有需要特定配置的不同用户或组角色，您可为每个用户类型或用户组创建单独代理配置。门户根据端点操作系统和用户名或组名来确定要部署的代理配置。与其他安全规则评估相同，门户会从列表的顶部开始搜索匹配项。在其找到匹配项后，门户会将对应的配置发送至应用。

该配置可能包括下列内容：

- 端点可连接的网关列表。
- 用户可从外部网关中为会话手动选择的任何网关。
- 允许应用与 GlobalProtect 网关建立 SSL 连接所需的根 CA 证书。
- SSL 转发代理解密的根 CA 证书。
- 端点连接时需提供给网关的客户端证书。仅当应用与门户或网关之间需相互认证时才需要此配置。
- 端点连接时需提供给门户或网关的安全加密 Cookie。仅当允许门户生成时才包含此 Cookie。
- 端点用于确定其连接对象是本地网络还是外部网络的相关设置。
- 应用行为设置，例如最终用户可查看的视图、最终用户是否可保存其 GlobalProtect 密码以及是否提示用户升级软件。

© 2019 Palo Alto Networks, Inc.

如果门户关闭或无法访问，则应用将使用其上次成功获得设置的门户连接的代理配置缓存版本，包括应用可连接的网关、用来与网关建立安全通信的根 *CA* 证书以及使用的连接方法。

按照下列步骤创建代理配置。

STEP 1 | 将一个或多个受信任的根 CA 证书添加到门户网站代理配置，以使 GlobalProtect 应用程序能够验证门户和网关的身份。

门户网站将证书部署到仅由 GlobalProtect 读取的证书文件中。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）。
2. 选择正向其添加代理配置的门户配置，然后选择 **Agent**（代理）选项卡。
3. 在 **Trusted Root CA**（可信根 **CA**）字段中，单击 **Add**（添加），然后选择已用于颁发网关和/或网关服务器证书的 CA 证书。

   Web 界面显示在用作 GlobalProtect 门户的防火墙上导入的 CA 证书列表。Web 界面还从您可以选择的证书列表中排除最终实体证书（有时称为叶证书）。您也可以 **Import**（导入）一个新的 CA 证书。

   在创建和添加证书时使用以下最佳实践：

   - 使用相同的证书颁发者为您的所有网关颁发证书。
   - 将整个证书链（可信根 *CA* 和中间 *CA* 证书）添加到门户网站代理配置。

4. （可选）部署其他 CA 证书，用于 GlobalProtect 以外的其他用途（例如，SSL 转发代理解密）。

   通过此选项，您可以使用门户将证书部署到端点，代理将其安装在本地根证书存储区中。如果您没有其他分发这些服务器证书的方法，或者希望使用门户网站进行证书分发，这可能很有用。

   对于 SSL 转发代理解密，您可以转发防火墙使用的信任证书（仅在 Windows 和 macOS 端点上），以终止 HTTPS 连接，检查流量的策略合规性，以及重新建立 HTTPS 连接以转发加密流量。

   1. 按照上一步骤所述添加证书。
   2. 启用选项以 **Install in Local Root Certificate Store**（安装于本地根证书存储区）。

      当用户登录门户时，门户自动发送此证书并将其安装在端点本地商店中，从而无需您手动安装证书。

STEP 2 | 添加代理配置。

代理配置指定了用于部署至连接应用的 GlobalProtect 配置设置。至少必须定义一个代理配置。

1. 从您的门户配置（**Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>*）**Add**（添加）新的代理配置。
2. 输入 **Name**（名称）以标识配置。如果计划创建多个配置，则应确保为每个配置定义的名称包含足够的描述性信息，以便对其进行区分。

STEP 3 | （可选）配置设置以指定有此配置的用户如何验证至门户。

如果网关使用客户端证书对端点进行身份验证，则必须选择证书分发源。

配置以下任意 **Authentication**（身份验证）设置：

- 要允许用户使用客户端证书验证至门户，请选择分发证书及其私钥到端点的 **Client Certificate**（客户端证书）源（**SCEP**、**Local**（本地）或 **None**（无））。如果使用内部 CA 将证书分发到端点，请选择 **None**（无）（默认）。要允许门户生成并发送机器证书到应用以存储在本地证书库中，同时允许使用此证书进行门户和网关身份验证，请选择 **SCEP** 及相关联的 SCEP 配置文件。这些证书视设备而定，仅可用在签发至的端点上。要对所有端点使用相同证书，请选择对门户而言属于 **Local**（本地）的证书。如果选择 **None**（无），则门户不会将证书推送至端点，但您可通过其他方式从端点获取证书。
- 指定是否 **Save User Credentials**（保存用户凭据）。选择 **Yes**（是）保存用户名和密码（默认），选择 **Save Username Only**（仅保存用户名）保存用户名，选择 **Only with User Fingerprint**（仅保存用

© 2019 Palo Alto Networks, Inc.

户指纹）保存用户生物特征（指纹），或仅在 iOS X 端点上选择人脸 ID 凭据，或选择 **No**（否）从不保存凭据。

> 将 *Save User Credentials*（保存用户凭据）设为 *No*（否）时，如果门户和网关配置为使用相同的身份验证方法，*GlobalProtect* 应用程序可通过用户提供的用于向门户验证身份的凭据，透明地向网关验证身份。在向网关验证身份时，用户无需重新输入凭据。

如果配置门户或网关提示动态密码，例如一次性密码 (OTP)，则用户必须在每次登录时输入新密码。在此情况下，GlobalProtect 应用忽视保存用户名和密码二者的选项，如果指定，则仅保存用户名。有关详细信息，请参阅使用一次性密码 (OTP) 启用双重身份验证。

如果选择 GlobalProtect 在 **Only with User Fingerprint**（仅保存用户指纹）的情况下 **Save User Credentials**（保存用户凭据），则 GlobalProtect 可以利用应用程序的操作系统功能在允许 GlobalProtect 身份验证之前验证用户。最终用户必须提供与端点上可信指纹模板匹配的指纹，这样才能使用保存的密码进行 GlobalProtect 门户和网关身份验证。在 iOS X 上，GlobalProtect 还支持使用人脸 ID 进行面部识别。GlobalProtect 不存储用于身份验证的指纹或面部模板，而是依赖操作系统扫描功能来确定扫描匹配的有效性。

STEP 4 | 如果 GlobalProtect 端点在内部网络上时无需隧道连接，则配置内部主机检测。

1. 选择 **Internal**（内部）。
2. 启用 **Internal Host Detection**（内部主机检测）（**IPv4** 或 **IPv6**）。
3. 输入只可从内部网络进行访问的主机的 **IP Address**（**IP** 地址）。指定的 IP 地址必须与该 IP 地址类型匹配（**IPv4** 或 **IPv6**）。例如，172.16.1.0（对于 IPv4）或 21DA:D3:0:2F3b（对于 IPv6）。
4. 输入与该 IP 地址对应的 DNS **Hostname**（主机名）。试图连接至 GlobalProtect 的端点尝试在指定地址执行逆向 DNS 查询。如果查询失败，端点确定其在外部网络上，然后向位于外部网关列表上的网关发起隧道连接。

STEP 5 | 设置第三方移动端点管理系统的访问权限。

如果采用该配置的移动端点受第三方移动端点管理系统管理，则必须执行此步骤。所有端点最初连接至门户，如果已在相应门户代理配置中设定第三方移动端点管理系统，则会将该设备重定向至第三方移动端点管理系统以便进行注册。

1. 输入与移动端点管理系统相关联的端点检入接口的 IP 地址或 FQDN。此处输入的值必须与和该端点检入接口相关联的服务器证书中的此值完全匹配。您可以制定 IPv6 或 IPv4 地址。
2. 指定移动端点管理系统在其上侦听注册请求的 **Enrollment Port**（注册端口）。该值必须与在移动端点管理系统上设置的值匹配（默认值 = 443）。

STEP 6 | 为您的门户代理配置指定选择条件。

门户将使用指定的用户/用户组设置来确定将哪个配置传递给进行连接的 GlobalProtect 应用。因此，如果有多个配置，则须确保对其进行正确排序。一旦找到匹配项，门户便会提供配置。因此，较为具体的配置必须先于较为常规的配置。有关对代理配置列表进行排序的说明，请参阅步骤 12。

选择 **Config Selection Criteria**（配置选择条件），然后配置以下任意选项：

- 要指定此配置应用的用户、用户组和/或操作系统，选择 **User/User Group**（用户/用户组），然后配置以下任意选项：
  - 要将此配置传递给正在特定操作系统中运行的应用，请 **Add**（添加）并选择应用此配置 **OS**（操作系统）（**Android**、**Chrome**、 **iOS**、**Linux**、 **Mac**、 **Windows**或 **WindowsUWP**）。将 **OS**（操作系统）设为 **Any**（任何）以将配置部署至所有操作系统。
  - 要将配置限定于特定的用户和/或组， **Add**（添加）并选择想要接收此配置的 **User/User Group**（用户/用户组）。为您要添加的所有用户/组重复执行此步骤。要将配置限定于尚未登录至其端点的用户，请从 **User/User Group**（用户/用户组）下拉列表中选择 **pre-logon**（预登录）。要将此配置应用于无论登录状态如何的任何用户（包括预登录和已登录用户），从 **User/User Group**（用户/用户组）下拉列表中选择 **any**（任何）。

© 2019 Palo Alto Networks, Inc.

要将配置限定于特定组，首先必须按启用组映射中所述方法将用户映射至组。

- 要将此配置传递给基于指定设备属性的应用，请选择 **Device Checks**（设备检查）然后配置以下任何选项：
  - 要根据 Active Directory 或 Azure AD 内是否存在端点序列号来传递此配置，请从 **Machine account exists with device serial number**（机器帐户设有设备序列号）下拉列表选择一个选项。如果您将此选项设为 **Yes**（是），代理配置仅应用于带有已存在序列号的端点（受管端点）。如果您将此选项设为 **No**（否），代理配置仅应用于不存在序列号的端点（非受管端点）。如果您将此选项设为 **None**（无），则配置不会传递至应用（根据端点序列号存在与否）。
  - 要根据端点的计算机证书传递此配置，请选择 **Certificate Profile**（证书配置文件）以匹配端点上安装的计算机证书。
- 要根据自定义的主机信息传递此配置至应用，请选择 **Custom Checks**（自定义检查）。启用 **Custom Checks**（自定义检查）然后定义以下任何注册表和 plist 数据：
  - 要验证 Windows 端点是否有指定的注册表项，使用以下步骤：
    1. **Add**（添加）一个新的注册表项（**Custom Checks**（自定义检查）> **Registry Key**（注册表项））。
    2. 根据提示输入 **Registry Key**（注册表项）以匹配。
    3. （可选）要仅在端点没有指定注册表项或键值时传递此配置，请选择 **Key does not exist or match the specified value data**（键值不存在或不匹配指定的值数据）。
    4. （可选）要根据指定注册表项传递此配置，**Add**（添加）**Registry Value**（注册表项）和对应的 **Value Data**（值数据）。要仅在端点没有指定的 **Registry Value**（注册表项）或 **Value Data**（值数据）时传递此配置，请选择 **Negate**（求反）。
  - 要验证 macOS 端点是否在 plist 中有指定的项目，请使用以下步骤：
    1. **Add**（添加）新 plist（**Custom Checks**（自定义检查）> **Plist**）。
    2. 按照提示输入 **Plist** 的名称。
    3. （可选）要仅在端点没有指定的 plist 时传递此配置，请选择 **Plist does not exist**（**Plist** 不存在）。
    4. （可选）要根据 plist 中的特定键值对传递此配置，请单击 **Add**（添加），然后输入要匹配的 **Key**（键）和对应的 **Value**（值）。要仅匹配没有指定键或值的端点，请选择 **Negate**（求反）。

STEP 7 | 指定采用此配置的用户可连接至的外部网关。

配置网关时，可考虑以下最佳做法：

- 如果将内、外部网关添加至同一配置，则请确保启用 *Internal Host Detection*（内部主机检测）（步骤 *4*）。
- 有关 *GlobalProtect* 应用程序如何确定其应连接的网关的详细信息，请参阅多网关配置中的网关优先级。

1. 选择 **External**（外部）。
2. **Add**（添加）用户可以连接的 **External Gateways**（外部网关）。
3. 为网关输入描述性 **Name**（名称）。此处所输入的名称应与配置网关时所定义的名称匹配，同时还应包含足够的描述性信息，以便用户了解其所连接至的网关的位置。
4. 在 **Address**（地址）字段中，输入在其上配置网关的接口的 FQDN 或 IP 地址。您可以配置 IPv4 或 IPv6 地址。指定的地址必须与网关服务器证书中的公用名 (CN) 完全匹配。
5. 为网关 **Add**（添加）一个或多个 **Source Regions**（源区域），或选择 **Any**（任何）以使网关可供所有区域使用。当用户进行连接时，GlobalProtect 会识别区域，且只允许用户连接到为该区域配置的网关。对于选择网关，请首先考虑源区域，然后考虑网关优先级。
6. 通过在字段中单击并选择以下其中一个值以设置网关的 **Priority**（优先级）：

© 2019 Palo Alto Networks, Inc.

- 如果只有一个外部网关，则可依旧将该值设为最高（默认值）。
- 如果有多个外部网关，则可修改优先级值（从最高到最低），以便为该配置所应用于的特定用户组指明首选项。例如，如果希望用户组连接至外部网关，则可将优先级设为高于地理距离较远的网关的优先级。然后，该优先级值将用于测定代理的网关选择算法的权重。
- 如果不想应用程序与网关自动建立隧道连接，则请选择**Manual only**（仅手动）。该设置在测试环境下十分有用。

7. 如果允许用户能手动切换至网关，则请选中 **Manual**（手动）复选框。

STEP 8 | 指定采用此配置的用户可连接至的内部网关。

如果配置包括内部网关，则请勿将“按需”用作连接方法。

1. 选择 **Internal**（内部）。
2. **Add**（添加）用户可以连接的 **Internal Gateways**（内部网关）。
3. 为网关输入描述性 **Name**（名称）。此处所输入的名称应与配置网关时所定义的名称匹配，同时还应包含足够的描述性信息，以便用户了解其所连接至的网关的位置。
4. 在 **Address**（地址）字段中，输入在其上配置网关的接口的 FQDN 或 IP 地址。您可以配置 IPv4 或 IPv6 地址。指定的地址必须与网关服务器证书中的公用名 (CN) 完全匹配。
5. （可选）**Add**（添加）一个或多个 **Source Addresses**（源地址）到网关配置。源地址可以是 IP 子网、范围或预定义地址。GlobalProtect 支持 IPv6 和 IPv4 地址。当用户进行连接时，GlobalProtect 会识别端点的源地址，且只允许用户连接到为该地址配置的网关。
6. 单击 **OK**（确定）保存更改。
7. （可选）**Add**（添加）一个 **DHCP Option 43 Code**（**DHCP** 选项 **43** 代码）到网关配置。您可以包含一个或多个与供应商特定信息（选项 43）关联的子选项代码，其中 DHCP 服务器已配置为向客户端提供。例如，您可能有一个与 IP 地址 192.168.3.1 关联的子选项代码 100。

   当用户连接时，GlobalProtect 门户将门户配置中的选项代码列表发送到 GlobalProtect 应用，应用选择由选项指示的网关。

   同时配置源地址和 DHCP 选项时，呈现给端点的可用网关列表基于两种配置的组合（联合）。

   DHCP 选项仅受 Windows 和 macOS 端点支持。不能使用 DHCP 选项来选择使用 IPv6 寻址的网关。

8. （可选）选择 **Internal Host Detection**（内部主机检测）可让 GlobalProtect 应用程序确定其是否在企业网络内。用户尝试登录时，应用程序将从内部 **Hostname**（主机名）到指定的 **IP Address**（**IP** 地址）执行逆向 DNS 查询。

   如果端点在企业网络内，则主机将作为可访问的参考点。如果应用程序找到主机，表示端点在网络内部，且应用程序会连接到内部网关；如果应用程序无法找到内部主机，表示端点在网络外部，且应用程序会与其中一个外部网关相连接。

   您可以为 **Internal Host Detection**（内部主机检测）配置 **IPv4** 或 **IPv6** 寻址。指定的 IP 地址必须与该 IP 地址类型匹配。例如，172.16.1.0（对于 IPv4）或 21DA:D3:0:2F3b（对于 IPv6）。

STEP 9 | 为具有此配置的用户自定义 GlobalProtect 应用行为。

根据需要修改 **App**（应用）设置。有关每个选项的详细信息，请参阅自定义 GlobalProtect 应用。

STEP 10 | （可选）定义任何需要应用程序收集和/或在收集时排除的自定义主机信息配置文件 (HIP) 数据。

© 2019 Palo Alto Networks, Inc.

仅当计划使用 *HIP* 功能、存在想收集的信息但又无法使用标准 *HIP* 对象进行采集，或是存在不想收集的 *HIP* 信息时才需执行本步骤。有关设置和使用 *HIP* 功能的详细信息，请参阅主机信息。

有关收集自定义 *HIP* 数据的其他信息，请参阅 从端点收集应用程序和流程数据。

1. 选择 **HIP Data Collection**（**HIP** 数据收集）。
2. 启用 GlobalProtect 应用以 **Collect HIP Data**（收集 **HIP** 数据）。
3. 指定 **Max Wait Time (sec)**（最长等待时间（秒）），应用程序应在提交可用数据前搜索 HIP 数据的秒数（范围为 10-60 秒，默认为 20 秒）。
4. 选择 GlobalProtect 门户用于匹配 GlobalProtect 应用程序所发送计算机证书的 **Certificate Profile**（证书配置文件）。
5. 选择 **Exclude Categories**（排除类别）以排除特定类别和/或某一类别中的供应商、应用程序或版本。有关详细信息，请参阅配置基于 HIP 的策略实施。
6. 选择 **Custom Checks**（自定义检查）以定义您要从正运行此代理配置的主机收集的自定义数据。

STEP 11 | 保存代理配置。

单击 **OK**（确定）以保存代理配置。

STEP 12 | 分配代理配置，以便将正确的配置部署至每个应用。

应用进行连接时，门户会将数据包中的源信息与已定义的代理配置进行比较。与安全规则评估相同，门户从列表的顶部开始查找匹配项。在其找到匹配项后，会将对应的配置提交给应用程序。

- 要在配置列表中上移代理配置，请选择该配置并单击 **Move Up**（上移）。
- 要在配置列表中下移代理配置，请选择该配置并单击 **Move Down**（下移）。

STEP 13 | 保存门户配置。

1. 单击确定以保存门户配置。
2. **Commit**（提交）更改。

自定义 GlobalProtect 应用程序

门户代理配置允许自定义最终用户如何与安装于其端点上的 GlobalProtect 应用程序进行交互。您可以自定义应用程序的显示和行为，并为您创建的不同 GlobalProtect 代理配置定义不同的应用设置。例如，您可指定以下项：

- 用户可访问的菜单和视图。
- 用户是否可卸载或禁用应用程序（仅限用户登录连接方法）。
- 是否在成功登录时显示欢迎页面。此外，还可配置用户是否可取消欢迎页面，自定义 GlobalProtect 门户登录、欢迎和帮助页面，以指导用户如何在登录环境中使用 GlobalProtect。
- 自动升级 GlobalProtect 应用程序或是提示用户手动升级 GlobalProtect。
- 是否提示用户是否需要多重因素身份验证才能访问敏感的网络资源。

此外，您还可以在 Windows 注册表、Windows Installer (Msiexec) 和全局 macOS plist 中定义应用程序设置。在 Web 界面定义的设置（门户代理配置）优先于在 Windows 注册表、Msiexec、和 macOS plist 中定义的设置。更多信息，请参阅以透明方式部署应用设置。

仅通过 Windows 注册表或 Windows Installer (Msiexec) 提供的其它设置可使您：

- 指定应用程序在 Windows SSO 失败时是否提示最终用户出示凭据。
- 指定默认门户 IP 地址（或主机名）。
- 让 GlobalProtect 在用户登录端点前发起一个连接。

© 2019 Palo Alto Networks, Inc.

- 部署在 GlobalProtect 建立连接之前或之后或在 GlobalProtect 断开连接之后运行的脚本。
- 在 Windows 端点上配置 GlobalProtect 应用程序包装第三方凭据，允许在使用第三方凭据提供程序时启用 SSO。

更多信息，请参阅自定义应用设置。

STEP 1 | 选择要自定义的代理配置。

此外，您还可以在 *Windows* 注册表、*Windows Installer (Msiexec)* 和 *macOS plist* 中配置大多数应用程序设置。但是，在 *Web* 界面定义的设置优先于在 *Windows* 注册表、*Msiexec*、和 *macOS plist* 中定义的设置。更多信息，请参阅以透明方式部署应用设置。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）。
2. 选择要在其上添加代理配置的门户，或**Add**（添加）一个新门户。
3. 在 **Agent**（代理）选项卡上，选择要修改的代理配置或 **Add**（添加）新配置。
4. 选择 **App**（应用）选项卡。

   "应用配置"区域显示可为每个代理配置自定义默认值的应用程序设置。当您更改默认行为时，文本颜色将从灰色变为默认颜色。

STEP 2 | 指定用用于 GlobalProtect 连接的 **Connect Method**（连接方法）。

使用 *Pre-logon (Always On)*（预登录（始终打开））、*Pre-logon then On-demand*（预登录，然后按需）或 *User-log on (Always On)*（用户登录（始终打开））连接方法使用内部网关访问网络。

在"应用配置"区域，配置下列**Connect Method**（连接方法）选项中的任一项：

- **User-logon (Always On)**（用户登录（始终启用））— 用户一旦登录至端点（或域），GlobalProtect 应用程序便会自动连接至门户。与 SSO（仅限 Windows 端点）一同使用时，GlobalProtect 登录对最终用户透明。

  在 *iOS* 端点上，此设置可防止一次性密码 *(OTP)* 应用程序运行，因为 *GlobalProtect* 会强制所有流量通过隧道。
- **Pre-logon (Always On)**（预登录（始终启用））— GlobalProtect 应用程序在用户登录端点之前对用户进行身份验证，并建立至 GlobalProtect 网关的 VPN 隧道。该选项要求使用外部 PKI 解决方案为接收此配置的所有端点预部署机器证书。有关预登录的详情，请参阅使用预登录远程访问 VPN。
- **On-demand (Manual user initiated connection)**（按需（用户手动发起连接））— 用户须手动启动应用程序以便连接至 GlobalProtect。仅为外部网关使用该连接方法。
- **Pre-logon then On-demand**（预登录后按需）— 与 **Pre-logon (Always On)**（预登录（始终启用））连接方法类似，该连接方法（要求"内容发布"版本为 590-3397 或更高）使 GlobalProtect 应用程序能够在用户登录端点之前对用户进行身份验证并建立至 GlobalProtect 网关的 VPN 隧道。与预登录连接方法不同的是，在用户登录端点之后，如果连接因故终止，用户必须手动启动应用程序以便连接至 GlobalProtect。此选项的好处在于，您可允许用户在密码过期或用户忘记其密码时指定新密码，但仍要求用户在登录后手动发起连接。

STEP 3 | 指定是否实施 GlobalProtect 连接以访问网络。

（仅限 Windows 10）如果启用 **Enforce GlobalProtect Connection for Network Access**（实施 **GlobalProtect** 连接以访问网络），将绕过以下应用程序类型，且会阻止所有其他出站连接（而不是入站连接）：

- GlobalProtect 代理 (**PanGPA.exe**)、GlobalProtect 服务 (**PanGPS.exe**)、以及本地安全机构子系统服务 (**lsass.exe**) 进程
- DHCP、DNS、NetBIOS（网络基本输入/输出系统）以及链路本地多播名称解析 (LLMNR) 协议

© 2019 Palo Alto Networks, Inc.

- 回环接口流量

（仅限 macOS）如果启用 **Enforce GlobalProtect Connection for Network Access**（实施 **GlobalProtect** 连接以访问网络），将绕过以下应用程序类型，且会阻止所有其他出站和入站连接：

- GlobalProtect 应用程序和 GlobalProtect 服务 (PanGPS)
- DHCP 和 DNS 协议
- 回环接口流量
- `ocspd`、`syspolicyd`、`ntpd`、`apsd` 和 `trustd` 进程

要强制执行 *GlobalProtect* 以访问网络，我们建议您仅对以 *User-logon*（用户登录）或 *Pre-logon*（预登录）模式连接的用户启用此功能。以 *On-demand*（按需）模式连接的用户可能无法在允许宽限期内建立连接。

在“应用配置”区域，配置下列选项中的任一项：

- 要强制所有网络流量通过 GlobalProtect 隧道，将 **Enforce GlobalProtect Connection for Network Access**（实施 GlobalProtect 连接以访问网络）设置为 **Yes**（是）。默认情况下，无需 GlobalProtect 进行网络访问，这意味着，如果 GlobalProtect 被禁用或断开连接，用户仍然可以访问 Internet。要在流量被阻止之前向用户说明，配置 GlobalProtect **Display Traffic Blocking Notification Message**（显示流量阻止通知消息）并可选择指定何时显示该消息（**Traffic Blocking Notification Delay**（流量阻止通知延迟））。

  启用 *Enforce GlobalProtect Connection for Network Access*（实施 *GlobalProtect* 连接以访问网络）时，则可能需要考虑允许用户使用密码禁用 *GlobalProtect* 应用程序。*Enforce GlobalProtect Connection for Network Access*（实施 *GlobalProtect* 连接以访问网络）功能通过要求 *GlobalProtect* 连接进行网络访问来增强网络安全性。在极少数情况下，端点可能无法连接到 *VPN*，需要远程管理登录才能进行故障排除。通过禁用 *GlobalProtect* 应用程序（对于 Windows 或 macOS）使用管理员在故障排除会话期间提供的密码，您可以允许管理员远程连接到您的端点。
- 为网络访问配置特定本地 IP 地址或网段的排除，方法是输入这些 IP 地址，以便在启用实施 **GlobalProtect** 连接以访问网络而无法建立 **GlobalProtect** 连接时，允许到指定主机/网络的流量。当您实施 GlobalProtect 连接以访问网络而无法建立 GlobalProtect 连接时，请指定最多十个您要允许访问的 IP 地址或网段。

  这些选项要求“内容发布”版本为 *8196-5685* 或更高。

  通过配置排除，您可以在 GlobalProtect 断开连接时允许用户访问本地资源，从而改善用户体验。例如，当未连接 GlobalProtect 时，GlobalProtect 可以允许访问链接本地地址。这允许用户访问本地网段或广播域。
- （仅限 Windows 10 和运行 macOS Catalina 10.15.4 或更高版本的 macOS；需要 5.2 版本的 GlobalProtect™ 应用程序。）为您想在实施 GlobalProtect 连接以访问网络时允许访问的特定完全限定域名配置排除项：输入这些完全限定域名以在启用“实施 **GlobalProtect** 连接以访问网络”后但未建立 **GlobalProtect** 连接时允许特定 **FQDN** 的流量。

  当您实施 GlobalProtect 连接以访问网络而无法建立 GlobalProtect 连接时，请指定最多 20 个您要允许访问的完全限定域名。

  仅当 **Enforce GlobalProtect Connection for Network Access**（实施 **GlobalProtect** 连接以访问网络）设为 **Yes**（是）时，才能使用您提供的完全限定域名。多个完全限定域名通过逗号分隔（例如，google.com，gmail.com）。域名使用通配符 (*)（例如，*.gmail.com）。最大长度为 1,024 个字符。

  此选项要求内容发布版本为 *8284-6139* 或更高。

© 2019 Palo Alto Networks, Inc.

通过配置 FQDN 排除项，您可以在 GlobalProtect 断开连接时允许用户访问特定资源，从而改善用户体验。例如，一旦启用实施 GlobalProtect 连接以访问网络这一功能，端点就可以与云托管的身份提供商 (IdP) 通信以进行身份验证，或是与远程设备管理服务器进行通信。

- 如果您的用户必须登录强制网络门户以访问 Internet，指定 **Captive Portal Exception Timeout (sec)**（强制网络门户例外超时）（秒）以显示用户可登录强制网络门户的时间（以秒为单位）（范围为 0 至 3600 秒；默认为 0 秒）。如果用户未在此时限内登录，强制网络门户登录页面超时，用户将被禁止访问网络。

  要启用 GlobalProtect 应用以在检测到强制网络门户时显示通知消息，将 **Display Captive Portal Detection Message**（显示强制网络门户检测消息）设置为 **Yes**（是）。在 **Captive Portal Notification Delay (sec)**（强制网络门户通知延迟）（秒）字段中，输入 GlobalProtect 应用显示此消息的延迟时间（以秒为单位）（范围为 1 至 120 秒；默认为 5 秒）。在检测到强制网络门户后，GlobalProtect 将在可访问 Internet 之前启动此计时器。您也可以通过配置 **Captive Portal Detection Message**（强制网络门户检测消息）提供附加说明。

  要在强制网络门户检测时自动启动默认 Web 浏览器，以便用户可以无缝登录到强制网络门户，请在 **Automatically Launch Webpage in Default Browser Upon Captive Portal Detection**（强制网络门户检测时自动在默认浏览器中启动网页）字段中输入要用于初始连接尝试的网站的完全限定域名 (FQDN) 或 IP 地址，该尝试在默认 Web 浏览器启动时启动 Web 流量（最大长度为 256 个字符）。然后，强制网络门户拦截该网站连接尝试，并将默认 Web 浏览器重定向到强制网络门户登录页面。如果此字段为空（默认），则 GlobalProtect 不会在强制网络门户检测时自动启动默认 Web 浏览器。

这些选项要求“内容发布”版本为 *607-3486* 或更高。*Captive Portal Notification Delay*（强制网络门户通知延迟）要求“内容发布”版本为 *8118-5277* 或更高。*Automatically Launch Webpage in Default Browser Upon Captive Portal Detection*（强制网络门户检测时自动在默认浏览器中启动网页）选项要求“内容发布”版本在 *2019* 年 *7* 月 *8* 日或之后发布。

STEP 4 | 指定附加 GlobalProtect 连接设置。

启用单点登录 *(SSO)* 后（默认），*GlobalProtect* 应用程序使用用户的 *Windows* 登录凭据自动进行身份验证，并连接到 *GlobalProtect* 门户和网关。此外，还允许 *GlobalProtect* 应用程序包装第三方凭据，允许 *Windows* 用户能够进行身份验证，甚至是与第三方凭据提供程序连接。

在“应用配置”区域，配置下列选项中的任一项：

- （仅限 Windows 和 macOS；macOS 支持要求“内容发布”版本为 8196-5685 或更高）将 **Use Single Sign-On (Windows)**（使用单点登录 **(Windows)**）或 **Use Single Sign-On (macOS)**（使用单点登录 **(macOS)**）设置为 **No**（否）以禁用单点登录。

  如果您配置 *GlobalProtect* 网关以通过 SAML 身份验证验证用户，并为身份验证覆盖生成和接受 Cookie，当用户 *Windows* 用户名与其 *SAML* 用户名不同（例如，*Windows* 用户名为“*user*”而 *SAML* 用户名为“*user123*”），或当用户名包含完全限定域名（例如，*Windows* 用户名为“*user*”，而 *SAML* 用户名为“*user@example.com*”）时，您必须将 *Use Single Sign-On*（使用单点登录）选项设为 *No*（否）。

- （内容发布版本 8284-6139 或以上；需要 5.2 版本的 GlobalProtect 应用程序）将 **Use Default Browser for SAML Authentication**（使用默认浏览器进行 **SAML** 身份验证）设为 **Yes**（是），以允许 GlobalProtect 应用程序打开默认系统浏览器进行 SAML 身份验证。默认值为 **No**（否）。此应用程序将打开内嵌的浏览器。

  如果您已将 GlobalProtect 门户配置为通过安全断言标记语言 (SAML) 身份验证对用户身份进行验证，则最终用户无需重新输入其凭据即可连接到应用程序或其他启用了 SAML 的应用程序，以实现无缝单点登录 (SSO) 的体验。您可以启用 GlobalProtect 应用程序，以便最终用户可以为 GlobalProtect 使用相同的登录信息，并使用 Chrome、Firefox 或 Safari 等默认系统浏览器进行 SAML 身份验证。

© 2019 Palo Alto Networks, Inc.

- 指定您希望 GlobalProtect 应用程序 **Automatically Use SSL When IPSec Is Unreliable**（在 **IPSec** 不可靠时自动使用 **SSL**）的时长（以小时为单位）（范围为 0-168 小时）。如果您配置此选项，GlobalProtect 应用不会在指定时间内尝试建立 IPSec 隧道。每当 IPSec 隧道由于隧道"保持连接"超时而关闭时，此计时器启动。

  如果您接受默认值 0，若此应用可以成功建立 IPSec 隧道，则不会回退以建立 SSL 隧道。仅当无法建立 IPSec 隧道时，其会回退以建立 SSL 隧道。

  此选项要求"内容发布"版本在 *2019* 年 *7* 月 *8* 日或之后发布。

- 为 GlobalProtect 应用程序选择 SSL 连接选项。您可以根据地理位置和网络性能选择仅实施 SSL 连接、禁止 SSL 连接或允许用户选择 SSL 或 IPSec（默认），以提供最佳用户体验。

  在 App Configuration（应用程序配置）区域中，选择您想要允许的 **Connect with SSL Only**（仅使用 **SSL** 连接）选项。

  这些选项要求"内容发布"版本为 *8207-5750* 或更高。

  - **Yes**（是）— 要求所有 GlobalProtect 客户端仅使用 SSL 连接。
  - **No**（否）— 使用网关上为 VPN 连接配置的协议进行连接。如果网关配置已启用 IPSec，则它将使用 IPSec 进行 VPN 连接。如果网关配置了 SSL，则它将使用 SSL 进行 VPN 连接。
  - **User can Change**（用户可更改）— 允许用户更改在 GlobalProtect 应用程序中使用 SSL 还是 IPSec。

    在应用程序中，用户可以选择 **Settings**（设置）> **General**（常规）来启用 **Connect with SSL Only**（仅使用 **SSL** 连接），以及 **Settings**（设置）> **Connection**（连接）来验证 **Protocol**（协议）是否为 **SSL**。

- （内容版本 8346-6423 或更高；需要 5.2.4 版本的 GlobalProtect 应用程序）输入应用程序为连接网关而使用的 **GlobalProtect Connection MTU (bytes)**（**GlobalProtect** 连接 **MTU**（字节））值。您可以指定 MTU 范围为 1000-1420 字节，而不是使用预设的默认 MTU 值（1400 字节）。默认值为 1400 字节。

  （仅限 Windows UWP）使用 `netsh` 命令手动配置 **GlobalProtect Connection MTU (bytes)**（**GlobalProtect** 连接 **MTU**（字节））值后，GlobalProtect 客户端无法在门户配置中设置一个大于手动配置值的 **GlobalProtect Connection MTU (bytes)**（**GlobalProtect** 连接 **MTU**（字节））值。

  如果 *MTU* 值小于 *1280* 字节，且已启用 *IPv6*，则 *GlobalProtect* 适配器会根据 *IPv6* 支持的最低 *MTU* 要求将此值更改为 *1280* 字节。

  通过配置 GlobalProtect 应用程序连接网关时使用的 MTU 值，您可以为通过网络连接且所需最大传输单位 (MTU) 值小于标准值（1500 字节）的最终用户优化连接体验。通过减小 MTU，一旦 VPN 隧道连接经过多个 MTU 值小于 1500 字节的互联网服务提供商 (ISP) 和网络路径，您就可以消除因分段导致的性能和连接问题。例如，您可以通过使用要求 MTU 值较低的不同门户配置，将区域内特定用户组的 MTU 值调整为较低的值。为特定门户配置的 MTU 值适用于该门户中使用 IPSec 和 SSL 隧道协议的所有网关隧道连接。

- 输入 **Maximum Internal Gateway Connection Attempts**（最大内部网关连接尝试次数）以指定 GlobalProtect 应用程序在第一次尝试连接到内部网关失败后进行重试的最大允许次数（范围为 0-100；建议 4 或 5；默认为 0，"0"表示 GlobalProtect 应用程序不会重试连接）。通过增加该值，您能使应用程序连接到临时关闭的内部网关，或连接到不可访问但在指定重试次数用尽前恢复正常的内部网关。增加该值还能确保内部网关接收到最新的用户和主机信息。
- 输入 **GlobalProtect App Config Refresh Interval**（**GlobalProtect** 应用程序配置刷新时间间隔）以指定 GlobalProtect 门户在发起下一次客户端配置刷新前要等待的小时数（范围为 1-168，默认为 24）。
- （仅适用于 Windows）根据您的安全要求，指定是否 **Retain Connection on Smart Card Removal**（在拆除智能卡时保留连接）。默认情况下，该选项被设置为 **Yes**（是），这意味着，当用

© 2019 Palo Alto Networks, Inc.

户拆除包含客户端证书的智能卡时，GlobalProtect 仍保持隧道连接。要终止隧道，将该选项设置为 **No**（否）。

此功能要求“内容发布”版本为 *590-3397* 或更高。

- 配置一个 **Automatic Restoration of VPN Connection Timeout**（自动恢复 **VPN** 连接超时）来指定在隧道断开连接时 GlobalProtect 采取的操作。将此选项设置为**Yes**（是），以允许 GlobalProtect 尝试在隧道断开连接后重新建立连接。将此选项设置为**No**（否），以阻止 GlobalProtect 在隧道断开连接后重新建立连接。配置 **Wait Time Between VPN Connection Restore Attempts**（**VPN** 连接恢复尝试之间的等待时间），以调整 GlobalProtect 在尝试恢复连接之间等待的时间量（以秒为单位），范围为 1-60 秒，默认为 5 秒。

  使用始终启用连接方法，如果用户在超时值过期之前从外部网络切换到内部网络，则 *GlobalProtect* 不会执行网络发现。因此，*GlobalProtect* 会将连接恢复到最后一个已知的外部网关。要触发内部主机检测，用户必须从 *GlobalProtect* 状态面板的设置菜单上选择*Refresh Connection*（刷新连接）。

STEP 5 | 配置拥有此代理配置的用户可用的菜单和 UI 视图。

在“应用配置”区域，配置下列选项中的任一项：

- 如果要用户仅能查看应用程序中的基本状态信息，将 **Enable Advanced View**（启用高级视图）设置为 **No**（否）。禁用此选项后，用户可以从以下选项卡查看信息：
  - **General**（常规）— 显示与 GlobalProtect 帐户相关联的用户名和门户。
  - **Notification**（通知）— 显示所有 GlobalProtect 通知。

  默认选项为 **Yes**（是）。启用此选项后，用户可以查看以下附加选项卡：
  - **Connection**（连接）— 列出为 GlobalProtect 应用程序配置的网关以及每个网关的信息。
  - **Host Profile**（主机配置文件）— 显示 GlobalProtect 使用 HIP 监视和实施安全策略的端点数据。
  - **Troubleshooting**（故障排除）— 显示有关网络配置、路由设置、活动连接和日志的信息。您还可以收集 GlobalProtect 生成的日志并设置日志记录级别。
- 若要在端点上隐藏 GlobalProtect 系统托盘图标，将 **GlobalProtect Icon**（ **GlobalProtect** 图标）设置为 **No**（否）。当图标隐藏时，用户无法执行其他任务，例如更改已保存密码、重新发现网络、重新提交主机信息、查看故障诊断信息或执行按需连接。但 HIP 通知消息、登录提示和证书对话框会在必要时显示。
- 要阻止用户执行网络发现，将 **Enable Rediscover Network Option**（启用重新发现网络选项）设置为 **No**（否）。禁用此选项时， GlobalProtect 状态面板的设置菜单上的**Refresh Connection**（刷新连接）变为灰色.
- 要阻止用户将 HIP 数据手动重新提交至网关，请将 **Enable Resubmit Host Profile Option**（启用重新提交主机配置文件选项）设置为 **No**（否）。默认情况下将启用该选项，此外在基于 HIP 的安全策略阻止用户访问资源时也十分有用；因为它允许用户在计算机上修复合规性问题，然后重新提交 HIP 数据。
- （仅适用于 Window）要允许 GlobalProtect 在系统托盘显示通知，请将 **Show System Tray Notifications**（显示系统托盘通知）设置为 **Yes**（是）。
- 要创建当用户密码快要到期时向用户显示的自定义消息，请输入 **Custom Password Expiration Message (LDAP Authentication Only)**（自定义密码到期消息（仅限 **LDAP** 身份验证））。消息长度不得超过 200 个字符。
- 要在用户更改其活动目录 (AD) 密码时创建自定义消息以指定密码策略或要求，请输入**Change Password Message**（更改密码消息）。消息长度不得超过 255 个字符。

STEP 6 | 定义采用该配置的最终用户可在其应用程序内执行的操作。

- 将**Allow User to Change Portal Access**（允许用户更改门户地址）设置为 **No**（否），以禁用 GlobalProtect 应用程序中状态面板上的 **Portal**（门户）字段。由于用户将无法指定要连接

© 2019 Palo Alto Networks, Inc.

的门户，所以必须提供 Windows 注册表（注册表项为 `Portal` 的 `(HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup`）或 macOS plist（在词典 `PanSetup` 下的注册表项为 `Portal` 的 `/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`）中的默认门户地址。更多信息，请参阅以透明方式部署应用设置。

- 要防止用户取消欢迎页面，请将 **Allow User to Dismiss Welcome Page**（允许用户取消欢迎页面）设置为 **No**（否）。否则，若该选项设置为 **Yes**（是），则用户可取消欢迎页面并在后续登录后阻止 GlobalProtect 显示此页面。

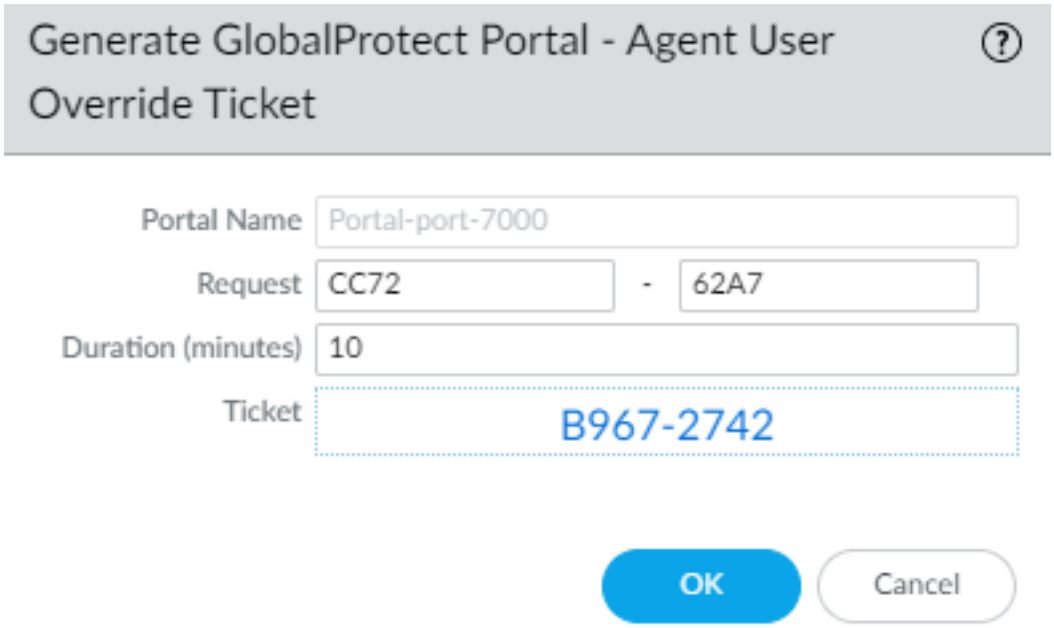
STEP 7 | 指定用户是否可禁用 GlobalProtect 应用程序。

Allow User to Disable GlobalProtect（允许用户禁用 **GlobalProtect**）适用于将 **Connect Method**（连接方法）设置为 **User-Logon (Always On)**（用户登录（始终启用））的代理配置。在用户登录模式下，一旦用户登录至端点，应用便会自动连接。该模式有时被称为“始终启用”，因此用户想禁用 GlobalProtect 应用程序时必须覆盖该行为。

默认情况下，该选项被设置为 **Allow**（允许），从而允许用户禁用 GlobalProtect 而无需提供评论、通行码或票据号。

若 *GlobalProtect* 系统托盘不可见，则用户不能禁用 *GlobalProtect* 应用程序。有关详细信息，请参阅步骤 5。

- 要防止使用用户登录连接方法的用户禁用 GlobalProtect，请将 **Allow User to Disable GlobalProtect App**（允许用户禁用 **GlobalProtect** 应用程序）设置为 **Disallow**（不允许）。
- 要允许用户仅在提供通行码的情况下禁用 GlobalProtect，请将 **Allow User to Disable GlobalProtect App**（允许用户禁用 **GlobalProtect** 应用程序）设置为 **Allow with Passcode**（带通行码允许）。然后，在“禁用 GlobalProtect 应用”区域，输入（并确认）最终用户必须提供的 **Passcode**（通行码）。
- 要允许用户仅在提供票据的情况下禁用 GlobalProtect，请将 **Allow User to Disable GlobalProtect**（允许用户禁用 **GlobalProtect**）设置为 **Allow with Passcode**（带票据允许）。使用此选项，禁用操作会触发应用程序生成“请求编号”，为此，最终用户必须与管理员进行沟通。随后，管理员可在 **Network**（网络）> **GlobalProtect** > **Portals**（门户）页面上单击 **Generate Ticket**（生成票据）并输入从用户处获取的请求编号以生成票据。管理员会将该票据提供给最终用户，后者可在“禁用 GlobalProtect”对话框中输入该票据以禁用该应用程序。



© 2019 Palo Alto Networks, Inc.

- 要限制用户可禁用 GlobalProtect 应用程序的次数，请在“禁用 GlobalProtect 应用”区域内指定 **Max Times User Can Disable**（用户可禁用的最大次数）值。“0”值（默认值）表示对用户可禁用应用程序次数无限制。

  此设置仅适用于禁用操作 *Allow*（允许）、*Allow with Comment*（带评论允许）和 *Allow with Passcode*（带通行码允许）。

  如果用户禁用了 GlobalProtect 应用程序的最大允许次数，且后续仍能够继续禁用该应用程序，则：

  - 您可以在 GlobalProtect 门户代理配置中增加 **Max Times User Can Disable**（用户可禁用的最大次数）值（**Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）> *<agent-config>* > **App**（应用程序））。随后，用户必须从 GlobalProtect 状态面板的设置菜单上选择**Refresh Connection**（刷新连接），或是新建一个 GlobalProtect 连接，以启用新值。
  - 用户可以通过重装应用程序来重置计数器。
- 要限制应用程序可以禁用的时间量，请在“禁用 GlobalProtect 应用程序”区域输入**Disable Timeout (min)**（禁用超时（分钟））。“0”值（默认值）表示对用户可保持应用程序禁用的时长无限制。

  此设置仅适用于禁用操作 *Allow*（允许）、*Allow with Comment*（带评论允许）和 *Allow with Passcode*（带通行码允许）。

STEP 8 | 指定用户是否可卸载 GlobalProtect 应用程序。

使用 **Allow User to Uninstall GlobalProtect App**（允许用户卸载 **GlobalProtect** 应用程序）选项来允许用户卸载 GlobalProtect 应用程序，阻止他们卸载 GlobalProtect 应用程序，或允许他们在指定您创建的密码时卸载。

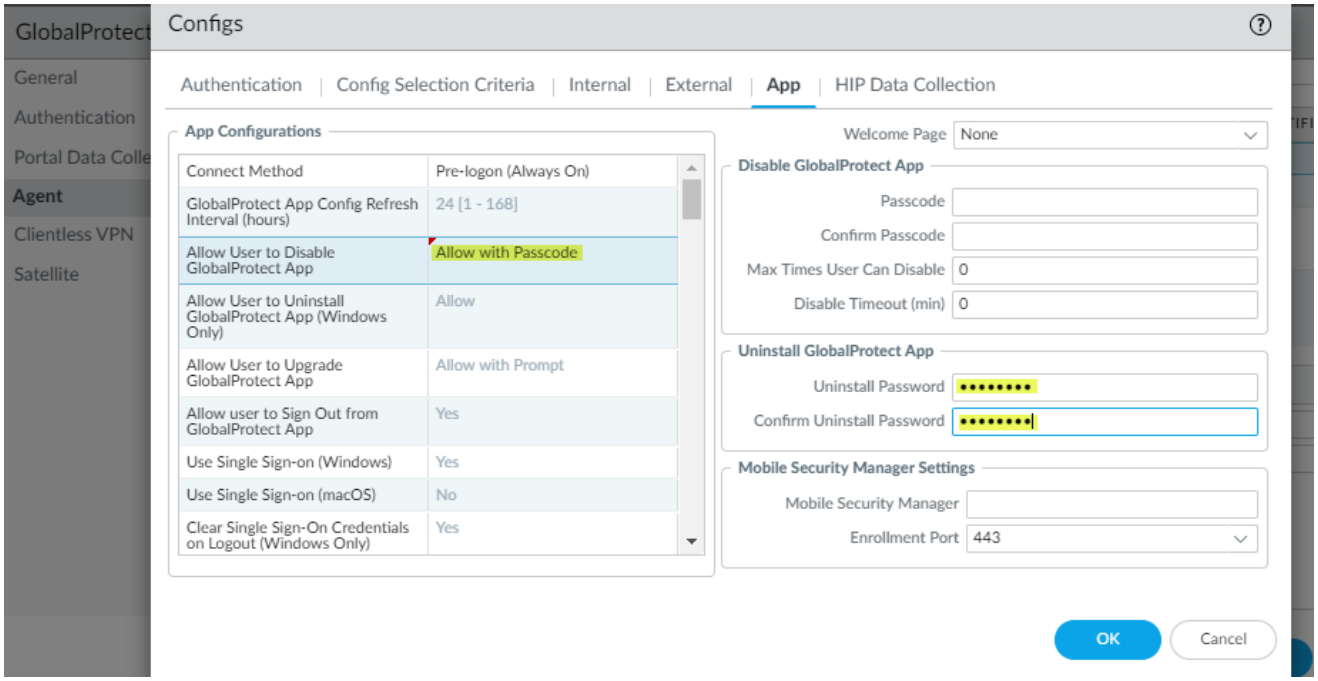
首次连接到门户时，此设置将被推送到端点设备注册表，并保存到它连接的每个门户。

这些选项要求“内容发布”版本为 *8207-5750* 或更高。

- 要允许用户无限制地卸载 GlobalProtect 应用程序，请选择 **Allow**（允许）。
- 要防止用户卸载 GlobalProtect 应用程序，请选择 **Disallow**（不允许）。

  当您在 Windows 注册表中将其设置为 **Disallow**（不允许）时，该门户的值将在 `Computer\\HKEY_LOCAL_MACHINE\\SOFTWARE\\Palo Alto Networks\\GlobalProtect\\Settings\\ 'Uninstall = 1'` 下设置为 1。
- 要允许用户使用密码卸载 GlobalProtect 应用程序，请选择 **Allow with Passcode**（允许使用密码）；然后，在卸载 GlobalProtect 应用程序部分，输入 **Uninstall Password**（卸载密码）和 **Confirm Uninstall Password**（确认卸载密码）。

© 2019 Palo Alto Networks, Inc.



STEP 9 | 指定用户是否可退出 GlobalProtect 应用程序。

在 App Configurations（应用程序配置）区域，将 **Allow user to Sign Out from GlobalProtect App**（允许用户退出 **GlobalProtect** 应用程序）设置为 **No**（否）可防止用户注销 GlobalProtect 应用程序；将 **Allow user to Sign Out from GlobalProtect App**（允许用户退出 **GlobalProtect** 应用程序）设置为 **Yes**（是）可允许用户注销。

这些选项要求“内容发布”版本为 *8196-5685* 或更高。

STEP 10 | 为接收此配置的用户配置证书设置和行为。

在“应用配置”区域，配置下列选项中的任一项：

- **Client Certificate Store Lookup**（客户端证书存储库查找）— 选择应用程序应用于查找客户端证书的存储库。**User**（用户）证书存储于 Windows “当前用户”证书存储库和 macOS 操作系统“个人密钥链”中。**Machine**（机器）证书存储于 Windows “本地计算机”证书存储库和 macOS 操作系统“系统密钥链”中。默认情况下，应用程序在这两处查找 **User and machine**（用户和机器）证书。
- **SCEP Certificate Renewal Period (days)**（SCEP 证书续订期限（天数））— 通过 SCEP，门户可在证书到期之前请求新客户端证书。证书到期之前的剩余时间为可选 *SCEP* 证书续订期限。在客户端证书到期之前的可配置天数内，门户可从企业 PKI 系统的 SCEP 服务器请求新证书（范围为 0-30，默认为 7）。“0”值表示门户不会在其刷新代理配置时自动续订客户端证书。

  对于在续订期限内要获取新证书的 GlobalProtect 应用，用户必须登录至应用程序。例如，如果客户端证书的生命周期为 90 天，则此证书的续订期为 7 天；若用户在此证书生命周期的最后 7 天登录，门户会获取新证书，并将其与已刷新的代理配置一同部署。有关详细信息，请参阅部署特定用户的客户端证书进行身份验证。
- **Extended Key Usage OID for Client Certificate(客户证书的扩展密钥用法 OID)**（仅 Windows 和 macOS 端点）— 仅当您启用客户端身份验证时才使用此选项，期望终端上存在多个客户端证书，并已确定可以过滤客户端证书的次要目的。使用此选项可以使用关联的对象标识符 (OID) 为客户端证书指定次要目的。例如，要仅显示也具有服务器身份验证目的的客户端证书，请输入 OID 1.3.6.1.5.5.7.3.1。当 GlobalProtect 应用程序只找到一个与次要用途相匹配的客户端证书时，GlobalProtect 会自动选择并使用该证书进行身份验证。否则，GlobalProtect 会提示用户从筛选

© 2019 Palo Alto Networks, Inc.

的符合条件的客户端证书列表中选择客户端证书。有关常见证书目的和 OID 列表的更多信息，请参阅 PAN-OS 7.1 新功能指南。

- 如果不想要应用程序在门户证书无效时与门户建立连接，请将 **Allow User to Continue with Invalid Portal Server Certificate**（允许用户继续使用无效门户服务器证书）设置为 **No**（否）。请牢记，门户仅提供代理配置而不提供网络访问权限。因此，门户安全的关键性不及网关安全。但是，如果已为门户部署可信服务器证书，禁用该选项有助于阻止中间人 (MITM) 攻击。

STEP 11 | 指定当需要使用多重因素身份验证来访问敏感网络资源时，用户是否收到登录提示。

对于内部网关连接，敏感网络资源（例如财务应用程序或软件开发应用程序）可能需要额外的身份验证。您可以配置 GlobalProtect 以实现多因素身份验证通知，允许访问这些资源。

在“应用配置”区域，配置下列选项中的任一项：

- 将 **Enable Inbound Authentication Prompts from MFA Gateways**（从 **MFA** 网关启用入站身份验证提示）设置为 **Yes**（是）。要支持多因素身份验证 (MFA)，GlobalProtect 应用程序必须接收并确认从网关入站的 UDP 提示。选择 **Yes**（是）可使 GlobalProtect 应用程序接收并确认提示。默认情况下，该值设置为 **No**（否），这意味着 GlobalProtect 将阻止来自网关的 UDP 提示。
- 指定 GlobalProtect 应用程序用于接收来自 MFA 网关的传入身份验证提示的 **Network Port for Inbound Authentication Prompts (UDP)**（入站身份验证提示的网络端口 **(UDP)**）。默认端口为 4501。要更改端口，请指定从 1 至 65535 之间的数字。
- 指定 GlobalProtect 应用程序将信任的 **Trusted MFA Gateways**（受信任 **MFA** 网关）用于多重因素身份验证。当 GlobalProtect 应用程序在指定的网络端口上接收 UDP 消息时，GlobalProtect 仅在 UDP 提示来自受信任的网关时才会显示身份验证消息。
- 配置 **Inbound Authentication Message**（入站身份验证消息）；例如，`You have attempted to access a protectedresource that requires additional authentication`（您试图访问需要附加身份验证的受保护资源）。通过以下网址继续进行身份验证：。当用户尝试访问需要额外身份验证的资源时，GlobalProtect 会收到并显示入站身份验证消息。GlobalProtect 会自动将您配置多重身份验证时指定的验证门户页面的 URL 附加到入站验证消息。

STEP 12 | （仅限 Windows）为接收此配置的 Windows 端点配置设置。

- **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Windows Only)**（使用隧道分配的 **DNS** 服务器解析所有 **FQDN**（仅限 **Windows**））— 为 GlobalProtect 隧道配置 DNS 解析首选项。选择 **No**（否），如果对网关上配置的 DNS 服务器的初始查询未解析，则允许 Windows 端点将 DNS 查询发送到设置在物理适配器上的 DNS 服务器。此选项保留本机 Windows 行为以递归方式查询所有适配器上的所有 DNS 服务器，但可能导致解决某些 DNS 查询很长的等待时间。选择 **Yes**（是）（默认），允许 Windows 端点使用在网关上配置的 DNS 服务器解析所有 DNS 查询，而不是允许端点将某些 DNS 查询发送到在物理适配器上设置的 DNS 服务器。

  此功能不能通过 *TCP* 支持 *DNS*。

  此功能需要内容发布版本 *731* 或更高版本，并可用于 *GlobalProtect* 应用程序 *4.0.3* 和更高版本。

- **Send HIP Report Immediately if Windows Security Center (WSC) State Changes**（**Windows** 安全中心 **(WSC)** 状态变更后立即发送 **HIP** 报告）— 选择 **No**（否）可防止 GlobalProtect 应用程序在 Windows 安全中心 (WSC) 状态变更后发送 HIP 数据。选择 **Yes**（是）（默认）可在 Windows 安全中心 (WSC) 状态变更后立即发送 HIP 数据。
- **Clear Single Sign-On Credentials on Logout**（退出登录时清空单点登录凭据）— 选择 **No**（否）可在用户退出登录时保留单点登录 (SSO) 凭据。选择 **Yes**（是）（默认）可将此凭据清除，并强制用户在下一次登录时输入凭据。
- **Use Default Authentication on Kerberos Authentication Failure**（**Kerberos** 身份验证失败时使用默认身份验证）— 选择 **No**（否）可仅使用 Kerberos 身份验证。选择 **Yes**（是）（默认）可在对 Kerberos 进行身份验证失败后使用默认的身份验证方法进行重试。

© 2019 Palo Alto Networks, Inc.

STEP 13 | （仅限 Windows）配置用于 Windows 端点的 GlobalProtect 应用程序，**Detect Proxy for Each Connection**（检测每个连接的代理）。

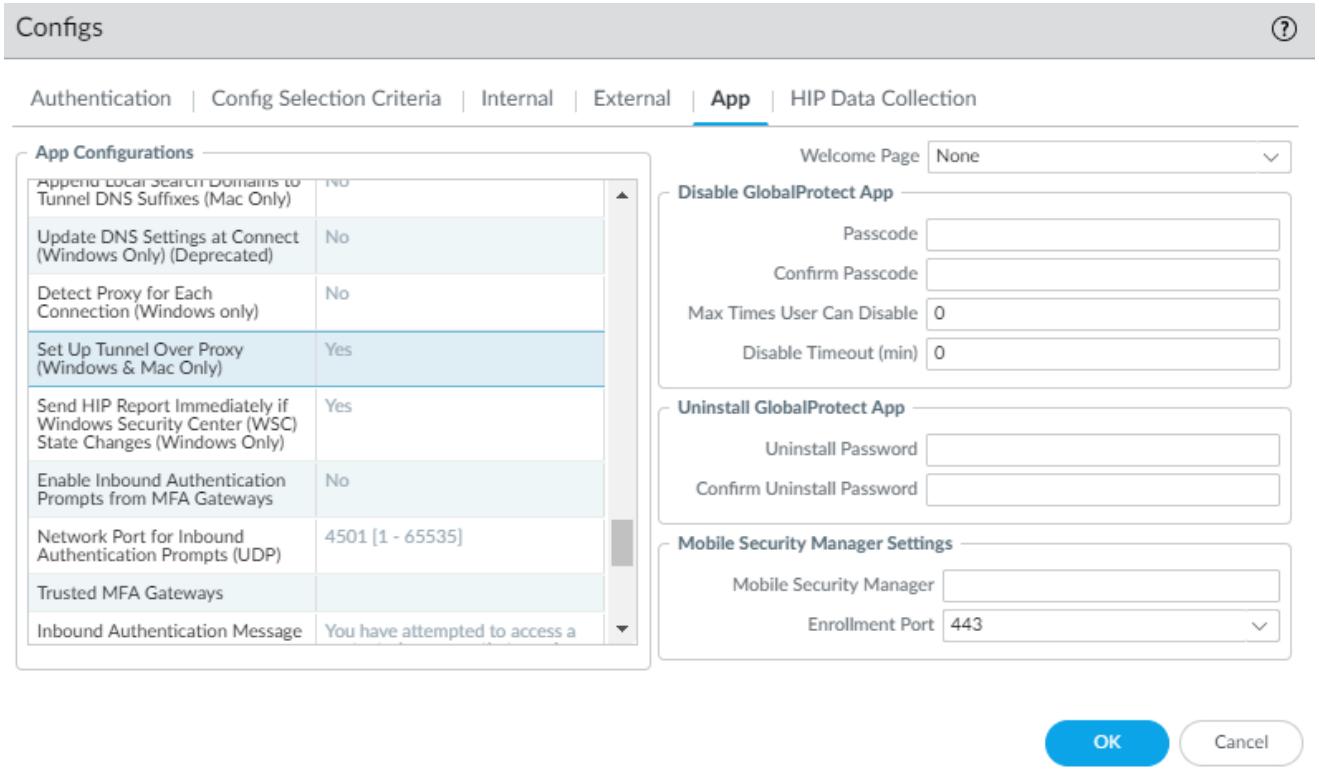
有关基于代理使用的网络流量行为的更多详细信息，请参阅代理上的隧道连接。

- 选择 **No**（否）可自动检测门户连接的代理并使用此代理进行后续连接。
- 选择 **Yes**（是）（默认）可自动检测每个连接的代理。

STEP 14 | （仅限 Windows 和 macOS）指定 GlobalProtect 是否必须使用代理或绕过代理。

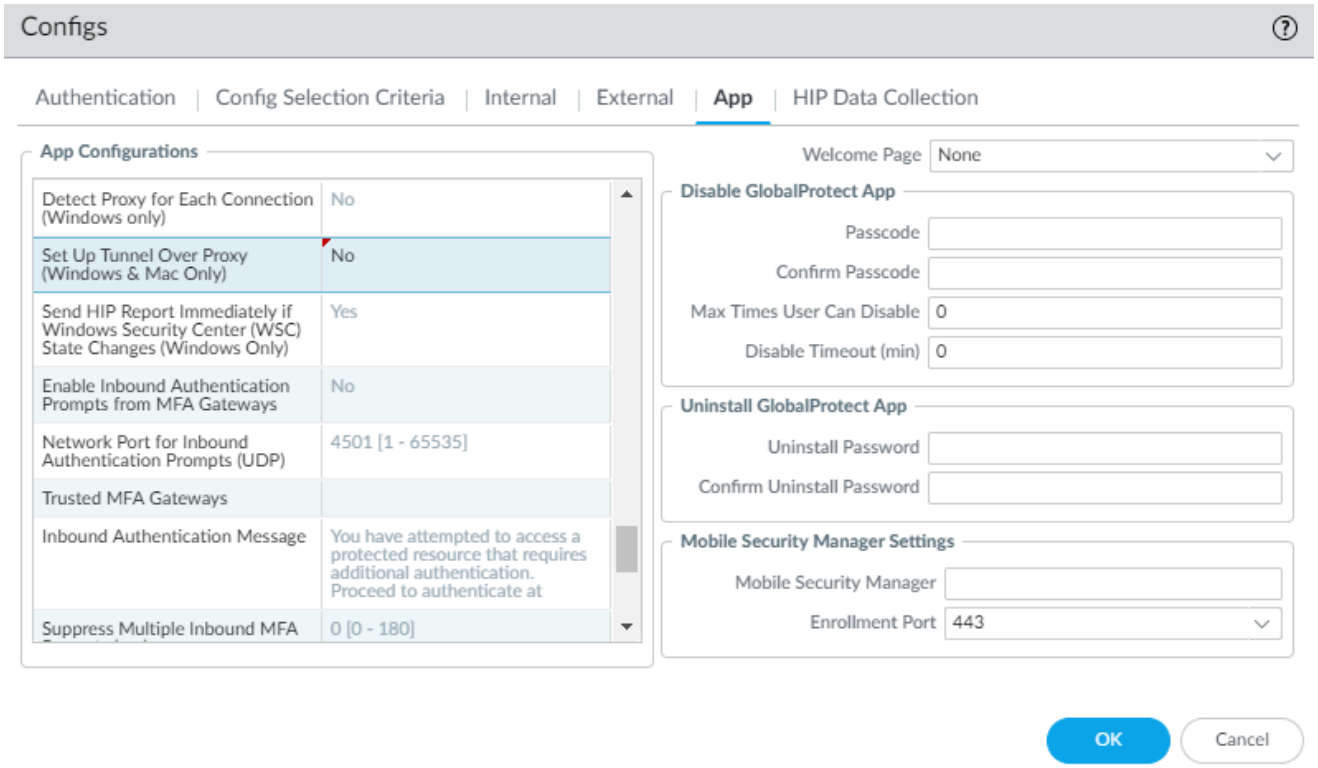
通过此设置，您可以根据 GlobalProtect 代理的使用情况配置网络流量行为。有关更多详细信息，请参阅代理上的隧道连接。

- 如需要 GlobalProtect 使用代理，请将 **Set Up Tunnel Over Proxy (Windows & Mac only)**（在代理上设置隧道（仅限 **Windows** 和 **Mac**））选项设为 **Yes**（是）。



- 如需要 GlobalProtect 绕过代理，请将 **Set Up Tunnel Over Proxy (Windows & Mac only)**（在代理上设置隧道（仅限 **Windows** 和 **Mac**））选项设为 **No**（否）。

© 2019 Palo Alto Networks, Inc.



STEP 15 | 如果端点频繁出现延迟或缓慢问题，当连接至 GlobalProtect 门户或网关时，可考虑调整门户和 TCP 超时值。

要允许端点有更多时间连接至门户或网关或从门户或网关接收数据，请按需增大超时值。请牢记，如果 GlobalProtect 应用程序无法建立连接，增大该值可能导致更长的等待时间。相反，当门户或网关在超时到期之前没有响应时，减小该值可能阻止 GlobalProtect 应用程序建立连接。

在“应用配置”区域，配置下列超时选项中的任一项：

- **Portal Connection Timeout (sec)**（门户连接超时（秒））—门户连接请求因门户无响应而超时之前的秒数（范围为 1 至 600）。如果防火墙运行的应用程序和威胁内容版本低于 777-4484，则默认值为 30。从内容版本 777-4484 开始，默认值为 5。
- **TCP Connection Timeout (sec)**（**TCP** 连接超时（秒））— TCP 连接请求因连接终端无响应而超时之前的秒数（范围为 1-600）。如果防火墙运行的应用程序和威胁内容版本低于 777-4484，则默认值为 60。从内容版本 777-4484 开始，默认值为 5。
- **TCP Receive Timeout (sec)**（TCP 接收超时（秒））— TCP 连接请求因 TCP 请求部分响应丢失而超时之前的秒数（范围为 1-600，默认为 30）。

STEP 16 | （Windows 10 和运行 macOS Catalina 10.15.4 或更高版本的 macOS；需要 5.2 版本的 GlobalProtect™ 应用程序）指定是否启用拆分 DNS 以允许用户在 VPN 隧道上或 VPN 隧道外引导用于应用程序和资源的 DNS 查询，此外，还可通过指定 **Split-Tunnel Option**（拆分隧道选项）允许网络流量。

选择 **Network Traffic Only**（仅限网络流量）以包含和排除仅适用于网络应用程序流量但不适用于 DNS 流量的规则。无论您是否为包含项和排除项指定了基于目标域的拆分隧道，所有 DNS 流量都会通过 VPN 隧道。一旦选择 **Both Network Traffic and DNS**（网络流量和 **DNS** 两者），您为包含项和排除项指定的基于目标域的拆分隧道将适用于该域的 DNS 流量和关联的网络应用程序流量。

通过拆分 DNS，您可以配置由 VPN 分配的 DNS 服务器解析的域以及由本地 DNS 服务器解析的域。

© 2019 Palo Alto Networks, Inc.

此选项要求内容发布版本为 *8284-6139* 或更高。

STEP 17 | 通过指定 **User Switch Tunnel Rename Timeout**（用户切换隧道重命名超时）指定是否允许通过现有 VPN 隧道建立远程桌面连接。当新用户使用远程桌面协议 (RDP) 连接至 Windows 机器时，网关重新为该新用户分配 VPN 隧道。然后，网关可对该新用户强制执行安全策略。

允许通过 VPN 隧道建立远程桌面连接在 IT 管理员需要使用远程桌面协议 (RDP) 访问远程最终用户系统时十分有用。

默认情况下，**User Switch Tunnel Rename Timeout**（用户切换隧道重命名超时）值设为 0，这表示，如果新用户通过 VPN 隧道验证身份，GlobalProtect 网关将终止连接。要修改此行为，配置介于 1 到 600 秒之间的超时值。如果新用户没有在超时值过期前登录网关，GlobalProtect 网关会终止分配给第一位用户的 VPN 隧道。

更改 *User Switch Tunnel Rename Timeout*（用户切换隧道重命名超时）值只影响 *RDP* 隧道，在配置时不会重命名预登录隧道。

STEP 18 | 要使 GlobalProtect 在用户注销其端点后保留现有 VPN 隧道，请指定 **Preserve Tunnel on User Logoff Timeout**（用户注销超时时保留隧道）的值（范围为 0-600 秒；默认为 0 秒）。如果接受默认值 0，则 GlobalProtect 不会在用户注销后保留隧道。

此选项要求“内容发布”版本在 *2019* 年 *7* 月 *8* 日或之后发布。

配置 GlobalProtect 以保留 VPN 隧道时，请考虑以下 GlobalProtect 连接行为：

- 如果同一用户在指定超时时段内以“始终打开”或“按需”模式注销并重新登录到某个端点，则 GlobalProtect 将保持连接，而不需要任何用户交互（包括门户和网关身份验证）。如果用户没有在指定超时时段内重新登录，隧道将断开连接，用户必须重新建立 GlobalProtect 连接。
- 如果一个用户从某个端点注销，然后另一个用户以“始终打开”或“按需”模式登录到同一端点，则只有在新用户在指定超时时段内成功通过 GlobalProtect 身份验证时，才会为新用户重命名现有隧道。如果新用户在指定超时时段内未成功登录和通过身份验证，则现有隧道将断开连接，并且必须建立新的 GlobalProtect 连接。如果新用户处于“始终打开”模式，GlobalProtect 会尝试自动建立新连接。如果新用户处于“按需”模式，则必须手动建立新的 GlobalProtect 连接。

STEP 19 | 指定 GlobalProtect 应用程序升级的执行方式。

如果要控制用户何时可以升级，则可以根据每个配置自定义应用升级。例如，如果您想对一小组用户测试发行版，然后将其部署到整个用户群中，则可以创建一个适用于您的 IT 小组中的用户的配置，从而允许他们升级和测试，并禁止所有其他用户/组配置升级。当新版本彻底测试完毕后，则可为其余用户修改代理配置以便进行升级。

默认情况下，**Allow User to Upgrade GlobalProtect App**（允许用户升级 **GlobalProtect** 应用程序）选项设置为**Allow with Prompt**（带提示允许），这意味着在防火墙上激活新版应用程序时会提示最终用户进行升级。要修改此操作，请选择下列任一选项：

- **Allow Transparently**（以透明方式允许）—自动升级，无需与用户交互。当用户远程工作或从公司网络内连接时，可能会发生升级。
- **Internal**（内部）— 自动升级，无需与用户交互，只要用户从公司网络内连接即可。建议使用此设置以防止在低带宽情况下升级缓慢。如果用户在公司网络外部连接，升级会延期；如果用户从公司网络内连接，则重新激活。您必须配置内部网关和内部主机检测才能使用此选项。
- **Disallow**（不允许）—此选项可防止应用程序升级。
- **Allow Manually**（手动允许）—最终用户发起应用程序升级。在此情况下，用户必须在 GlobalProtect 状态面板的设置菜单中选择**Check Version**（检查版本），以便确定是否存在新应用版本，然后按需进

© 2019 Palo Alto Networks, Inc.

行升级。请注意，如果向用户隐藏 GlobalProtect 应用，则该选项无效。有关 **Display GlobalProtect Icon**（显示 **GlobalProtect** 图标）设置的详细信息，请参阅步骤 5。

Allow Transparently（透明允许）和 *Internal*（内部）的升级仅在门户网站上的 *GlobalProtect* 软件版本比端点上的 *GlobalProtect* 软件版本更新时才会发生。例如，连接到 *GlobalProtect 3.1.1* 门户的 *GlobalProtect 3.1.3* 代理未升级。

STEP 20 | 添加 **Change Password Message**（更改密码消息）以指定用户更改密码时必须遵守的密码策略或要求（例如，密码必须包含至少一个数字和一个大写字母）。

STEP 21 | 通过指定 **Log Gateway Selection Criteria**（日志网关选择标准）选项，指定是否需要 GlobalProtect 应用程序发送网关选择标准日志到防火墙。

选择 **Yes**（是）以允许 GlobalProtect 应用程序发送网关选择标准增强日志到防火墙。默认值为 **No**（否）。此应用程序不会发送增强日志到防火墙。

为帮助您找出 GlobalProtect 应用程序选择连接到指定网关的详细原因，GlobalProtect 应用程序将收集并报告信息，以识别网关和端点之间的网关选择标准和延迟。通过网关选择标准相关的信息，您可以识别所选网关的优先级和响应时间、网关连接尝试列表，以及有关隧道前和隧道后网络延迟的统计信息。网关选择标准的增强日志字段已被添加到**Monitor**（监控）> **Logs**（日志）> **GlobalProtect** 中的 GlobalProtect 日志。

STEP 22 | 指定是否在成功登录时显示欢迎页面。

欢迎页面可有效引导用户访问其仅当连接至 GlobalProtect 后方可访问的内部资源，例如内部网或其他内部服务器。

默认情况下，应用程序已成功连接至系统托盘/菜单栏中显示的气球消息。

要在成功登录后显示欢迎页面，请在 **Welcome Page**（欢迎页面）下拉列表中选择 **factory-default**（出厂默认值）。GlobalProtect 在 GlobalProtect 应用程序中显示欢迎页面。也可选择提供特定于用户或某一组用户（基于已部署的门户配置）的信息的自定义欢迎页面。有关创建自定义页面的详细信息，请参阅自定义 GlobalProtect 门户登录、欢迎和帮助页面。

STEP 23 | （仅限 Windows）指定您是否想要 GlobalProtect 应用 **Display Status Panel at Startup**（在启动时显示状态面板）。

- 要在用户首次建立 GlobalProtect 连接时禁止显示状态面板，请选择 **No**（否）。
- 要在用户首次建立 GlobalProtect 连接时自动显示状态面板，请选择 **No**（否）。使用此选项后，用户必须点击状态面板外侧以将其手动关闭。

STEP 24 | 保存代理配置。

1. 如果已完成自定义代理配置，则请单击 **OK**（确定）以保存代理配置。否则，请返回定义 GlobalProtect 代理配置 以完成代理配置。
2. 单击**OK**（确定）以保存门户配置。
3. **Commit**（提交）更改。

自定义 GlobalProtect 门户登录、欢迎和帮助页面

GlobalProtect 提供默认的登录、欢迎和/或帮助页面。但是，您可以使用公司品牌、可接受的使用策略和指向内部资源的链接来创建自己的自定义页面。

您可以选择禁用浏览器访问门户登录页面，以防止未经授权地尝试 *GlobalProtect* 门户身份验证（从 *Network*（网络）> *GlobalProtect* > *Portals*（门户）> *<portal_config* > *General*（常规）配置 *Portal Login Page*（门户登录页面）> *Disable*（禁用）选项）。禁用门户登录

© 2019 Palo Alto Networks, Inc.

页面后，您可以使用软件分发工具（如 *Microsoft System Center Configuration Manager (SCCM)*）允许您的用户下载并安装 *GlobalProtect* 应用程序。

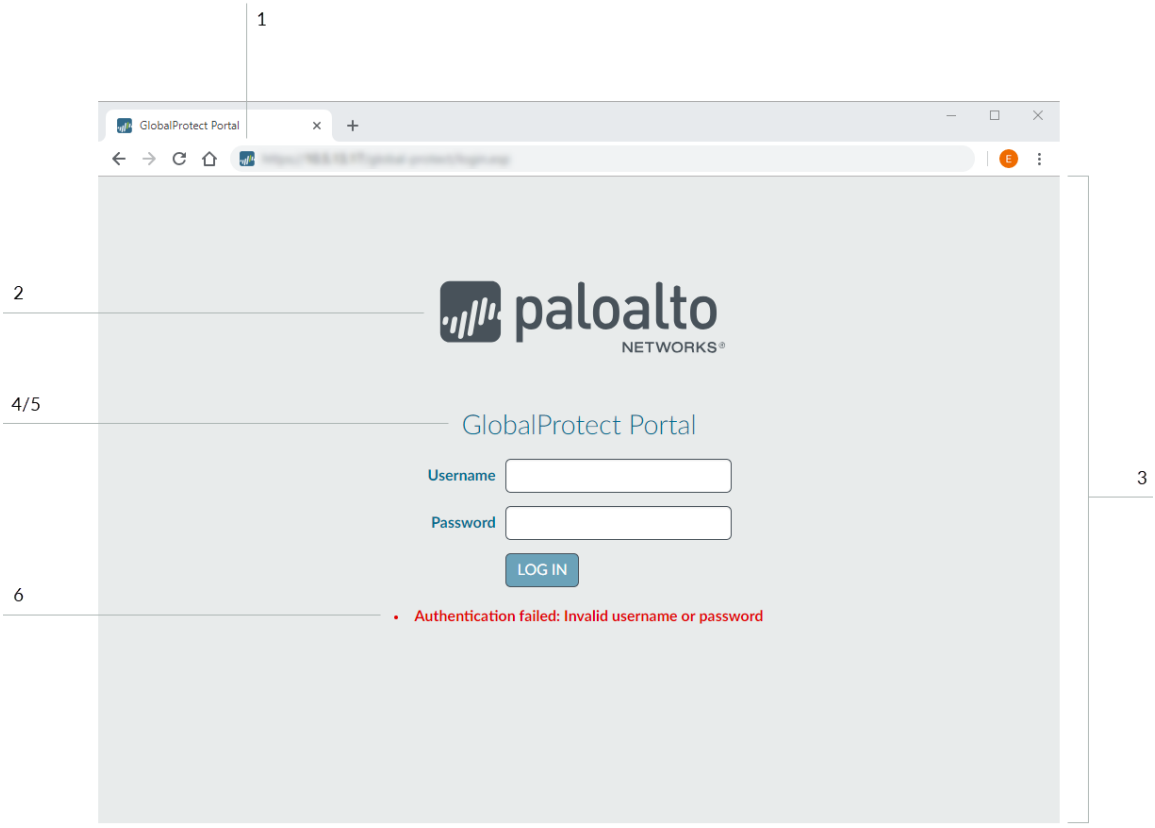
STEP 1 | 导出默认的门户登录、主页、欢迎或帮助页面。

1. 选择 **Device**（设备） > **Response Pages**（响应页面）。
2. 选择相应的 GlobalProtect 门户页面链接，例如 **GlobalProtect Portal Login Page**（**GlobalProtect** 门户登录页面）。
3. 选择预定义的 **Default**（默认）页面并单击 **Export**（导出）。

STEP 2 | 编辑导出的页面。

1. 使用所选 HTML 文本编辑器打开并编辑该页面。
2. 要编辑登录页面或主页，请配置以下任意变量：
   - **GlobalProtect** 门户登录页面：

© 2019 Palo Alto Networks, Inc.

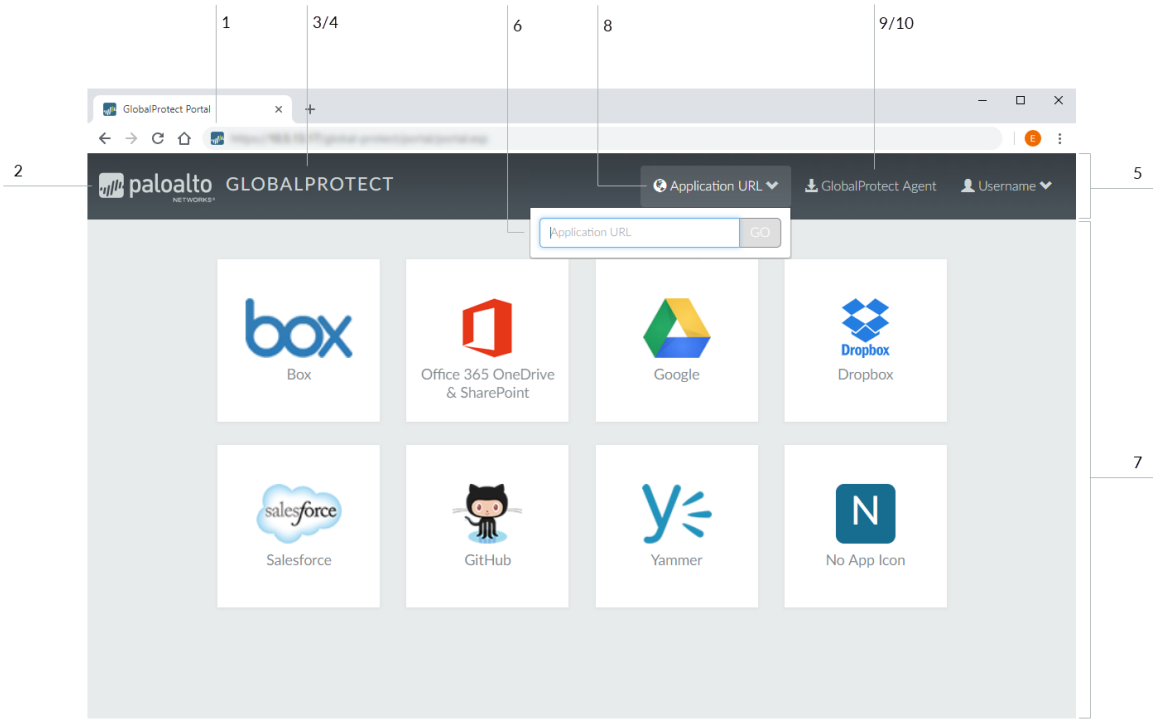


© 2019 Palo Alto Networks, Inc.

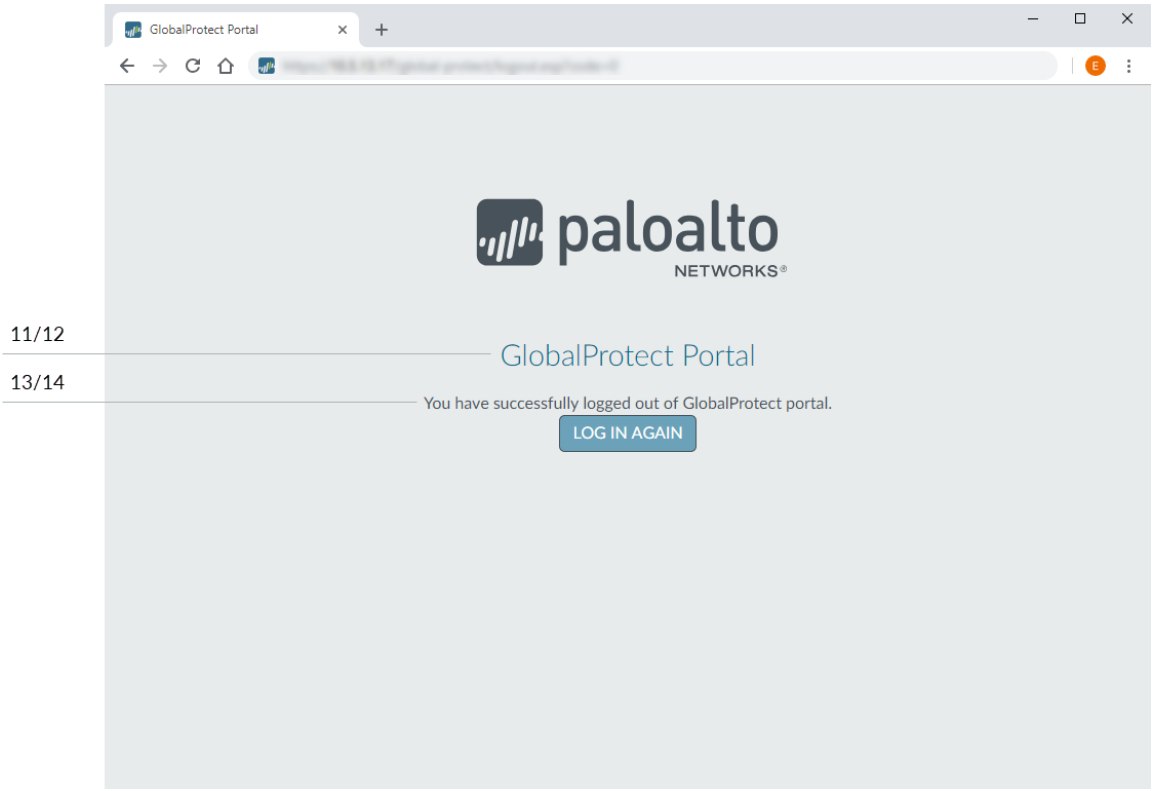
标签号	变量	说明	示例
1	`favicon`	Web 浏览器地址栏中显示的图标 URL。	`var favicon = 'http://cdn.slidesharecdn.com/logo-24x24.jpg?3975762018';`
2	`logo`	公司徽标的 URL。	`var logo = 'http://cdn.slidesharecdn.com/logo-96x96.jpg?1382722588';`
3	`bg_color`	登录页面的背景色。	`var bg_color = '#D3D3D3';`
4	`gp_portal_name`	公司徽标下显示的文字。	`var gp_portal_name = 'GlobalProtect Portal';`
5	`gp_portal_name_color`	公司徽标下显示的文字颜色。	`var gp_portal_name_color = '#000000';`
6	`error_text_color`	登录错误消息的文字颜色。	`var error_text_color = '#196390';`

- **GlobalProtect** 网络门户主页：

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.



标签号	变量	说明	示例
1	`favicon`	Web 浏览器地址栏中显示的图标 URL。	`var favicon = 'http://cdn.slidesharecdn.`

© 2019 Palo Alto Networks, Inc.

标签号	变量	说明	示例
			com/logo-24x24.jpg?3975762018';
2	logo	公司徽标的 URL。	var logo = 'http://cdn.slidesharecdn.com/logo-96x96.jpg?1382722588';
3	navbar_text	导航栏文字。	var navbar_text = 'GlobalProtect';
4	navbar_text_color	导航栏文字颜色。	var navbar_text_color = '#D3D3D3';
5	navbar_bg_color	导航栏背景颜色。	var navbar_bg_color = '#A9A9A9';
6	dropdown_bg_color	下拉菜单背景颜色。	var dropdown_bg_color = '#FFFFFF';
7	bg_color	主页背景色。	var bg_color = '#D3D3D3';
8	label_custom_app_url	自定义/内部应用 URL 标签。	var label_custom_app_url = 'Application URL';
9	display_globalprotect_agent	显示或隐藏 GlobalProtect 应用下载按钮的选项。输入 **1** 以显示下载按钮。输入 **0** 以隐藏下载按钮。	var display_globalprotect_agent = 1;
10	label_globalprotect_agent	GlobalProtect 应用下载按钮标签。	var label_globalprotect_agent = 'GlobalProtect Agent';
11	gp_portal_name	门户注销页面上公司徽标下显示的文字。	var gp_portal_name = 'GlobalProtect

© 2019 Palo Alto Networks, Inc.

标签号	变量	说明	示例
			`Portal';`
12	`gp_portal_name_color`	门户注销页面上公司徽标下显示的文字颜色。	`var gp_portal_name_color = '#000000';`
13	`logout_text_array`	用户从门户注销后，门户注销页面上显示的消息。 您仅可以修改已有消息；不能添加新消息或删除任何已有消息。	`var logout_text_array = ["You have successfully logged out of GlobalProtect portal.", "GlobalProtect Gateway is not licensed. Contact system administrator.", "User not authenticated to GlobalProtect portal.", "System error, contact system administrator.", "System error, failed to delete user session. Contact system administrator.", "Can not create user session. Max-capacity reached. Contact system administrator."];`
14	`logout_text_color`	用户从门户注销后，门户注销页面上显示的消息文字颜色。	`var logout_text_color = '#000000';`

3. 用新文件名保存编辑后的页面。确保该页面保持其 UTF-8 编码。

STEP 3 | 导入新页面。

1. 选择 **Device**（设备）> **Response Pages**（响应页面）。
2. 选择相应的 GlobalProtect 门户页面链接。
3. **Import**（导入）新的门户页面。在 **Import File**（导入文件）字段中输入路径和文件名，或 **Browse**（浏览）以定位文件，然后选中文件。
4. （可选）从 **Destination**（目标）下拉列表中选择将在其上使用该登录页面的虚拟系统，或选择 **shared**（共享）（默认）以使其可供所有虚拟系统使用。
5. 单击 **OK**（确定）以导入文件。

STEP 4 | 将门户配置为使用新登录页面。

© 2019 Palo Alto Networks, Inc.

- **Portal Login Page**（门户登录页面）、**Portal Landing Page**（门户登陆页面）和 **App Help Page**（应用帮助页面）：
  1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）.
  2. 选择想要添加登录、登陆（主页）或应用程序帮助页面的门户。
  3. 在 **General**（常规）选项卡的“外观”区域，从相关下拉列表中选择新页面。
- 自定义欢迎页面：
  1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）。
  2. 选择想要添加欢迎页面的门户。
  3. 在 **Agent**（代理）选项卡上，选择要添加欢迎页面的代理配置。
  4. 选择 **App**（应用）选项卡，从 **Welcome Page**（欢迎页面）下拉列表中选择新页面。
  5. 单击 **OK**（确定）以保存代理配置。

STEP 5 | 保存门户配置。

单击**OK**（确定）以保存门户配置，然后**Commit**（提交）更改。

STEP 6 | 验证新页面是否有显示。

- 测试登录页面 — 打开浏览器，转到门户的 URL（不得将“:4443”端口号添加至 URL 的末尾，否则将重定向至防火墙的 Web 接口）。例如，输入 **`https://myportal`**，而非 **`https://myportal:4443`**。随即显示新门户登录页面。
- 测试主页 — 打开浏览器，转到门户的 URL（不得将“:4443”端口号添加至 URL 的末尾，否则将重定向至防火墙的 Web 接口）。例如，输入 **`https://myportal`**，而非 **`https://myportal:4443`**。输入您的 **Username**（用户名）和 **Password**（密码），然后 **LOG IN**（登录）至门户。随即显示新门户的主页。
- 测试帮助页面 — 单击 GlobalProtect 系统托盘图标以启动 GlobalProtect 应用程序。当状态面板打开时，单击设置（⚙）图标，打开设置菜单。选中 **Help**（帮助）以查看新的帮助页面。
- 测试欢迎页面 — 单击 GlobalProtect 系统托盘图标以启动 GlobalProtect 应用程序。当状态面板打开时，单击设置（⚙）图标，打开设置菜单。选中 **Welcome Page**（欢迎页面）以查看新的欢迎页面。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用程序

> 下载 GlobalProtect 应用
> 部署 GlobalProtect 应用程序软件
> 定义 GlobalProtect 代理配置
> 自定义 GlobalProtect 应用程序
> 以透明方式部署代理设置

向最终用户部署 GlobalProtect 应用程序

要连接至 GlobalProtect™，端点须运行 GlobalProtect 应用程序。软件部署方法取决于下述端点类型：

平台	部署选项
macOS 和 **Windows** 端点	您可以使用几种选项来分发软件，并将其安装在 macOS 和 Windows 端点上： • 直接从门户 — 将应用软件下载至承载门户的防火墙并将其激活，以便最终用户连接至门户时安装更新。该选项十分灵活，因为它可根据为每个用户、组和/或操作系统所定义的代理配置设置来控制最终用户接收更新的方式和时间。但是，如果有大量应用需进行更新，则会对门户产生额外负载。有关说明请参阅在门户上载入应用更新。 • 从 **Web** 服务器 — 如果有大量端点需同时升级应用，请考虑将应用更新载入到 Web 服务器以减轻防火墙的负载。有关说明请参阅在 Web 服务器上载入应用更新。 • 从命令行透明执行 — 对于 Windows 端点，可通过 Windows Installer (Msiexec) 自动部署应用设置。但是，如果要用 Msiexec 升级至较高的应用版本，则必须先卸载现有应用。此外，Msiexec 还允许通过在 Windows 注册表中设置值来直接在端点上部署应用设置。同样，还可以通过在 macOS plist 中配置设置来将应用程序设置部署到 macOS 端点。请参阅以透明方式部署应用设置。 • 使用组策略规则 — 在 Active Directory 环境下，还可使用 Active Directory 组策略将 GlobalProtect 应用分发至最终用户。AD 组策略允许自动修改 Windows 端点设置和软件。有关如何使用“组策略”以自动将程序分发至端点或用户的详细信息，请参阅位于 http://support.microsoft.com/kb/816102 的文章。 • 从移动端点管理系统 — 如果使用 MDM 或 EMM 等移动管理系统管理移动端点，则可使用该类系统配置 GlobalProtect 应用。请参阅移动端点管理。
Windows 10 手机和 **Windows 10 UWP** 端点	• 从移动端点管理系统 — 如果使用 MDM 或 EMM 等移动管理系统支持 Windows 10 端点，则可使用该类系统配置 GlobalProtect 应用。请参阅移动端点管理。 • 从 **Microft Store** — 最终用户还可直接从 Microsoft Store 直接下载和安装 GlobalProtect 应用。有关如何下载和测试 GlobalProtect 应用安装的说明，请参阅下载和安装 GlobalProtect 移动应用。
iOS 和 **Android** 端点	• 从移动端点管理系统 — 如果使用 MDM 或 EMM 等移动管理系统，则可使用该类系统配置 GlobalProtect 应用。请参阅移动端点管理。 • 从 **app store** — 最终用户还可直接从 Apple App Store（iOS 端点）或 Google Play（Android 端点）下载和安装 GlobalProtect 应用。有关如何下载和测试 GlobalProtect 应用安装的说明，请参阅下载和安装 GlobalProtect 移动应用。
Chromebooks	• **From the Google Admin console**（从 **Google** 管理控制台）— Google 管理控制台使您能够从基于 Web 的中央位置管理 Chromebook 设置和应用程序。要使用 Google 管理控制台在受管 Chromebook 上部署 Android 版 GlobalProtect 应用程序，请参阅使用 Google 管理控制台在受管 Chromebook 上为 Android 部署 GlobalProtect 应用。 *Android 版 GlobalProtect 应用仅支持在某些 Chromebook 上使用。不支持 Android 应用程序的 Chromebook 必须*

© 2019 Palo Alto Networks, Inc.

平台	部署选项
	继续运行用于 *Chrome* 的 *GlobalProtect* 应用程序，从 *GlobalProtect app 5.0* 及更高版本开始不受支持。 • **From AirWatch**（从 **AirWatch**）— 可将 Android 版 GlobalProtect 应用程序部署在已注册 AirWatch 的受管 Chromebook 上。在部署应用后，配置并部署 VPN 配置文件，以便自动为最终用户设置 GlobalProtect 应用。要使用 AirWatch 在受管 Chromebook 上部署 Android 版 GlobalProtect 应用程序，请参阅使用 AirWatch 在受管 Chromebook 上为 Android 部署 GlobalProtect 应用。
Linux	从支持站点下载适用于 Linux 的 GlobalProtect 应用程序后，您可以分发并安装应用： • 使用 **Linux** 应用分发工具 — Linux 应用分发通过使用第三方工具（Chef 和 Puppet 等），或使用 Linux 操作系统的本地存储库（例如，Ubuntu 存储库和 RHEL 存储库）进行管理。有关更多信息，请参与 Linux 操作系统。 • 手动安装 — 要使软件可供最终用户使用，他们可以使用 **apt** 或 **dpkg** 等 Linux 工具手动安装软件。有关如何为 Linux 安装 GlobalProtect 应用的说明，请参阅 GlobalProtect 应用用户指南。

作为部署 *GlobalProtect* 应用软件的备选方法，您还可以配置 *GlobalProtect* 门户，以提供对使用 *HTML*、*HTML5* 和 *Javascript* 技术的常见企业 *Web* 应用程序的远程安全访问。用户无需安装 *GlobalProtect* 应用软件，即可从启用 *SSL* 的 *Web* 浏览器进行安全访问。请参考 GlobalProtect 无客户端 VPN。

下载 GlobalProtect 应用

如果您是最终用户，请联系您的 *IT* 管理员获得最新支持的 *GlobalProtect* 软件。

在您为最终用户部署 GlobalProtect 应用之前，必须上传新的应用程序包至承载门户的防火墙，然后激活该软件以便下载至连接到门户的应用上。此部署方法适用于所有非移动应用程序版本。要下载 GlobalProtect 应用的移动版本，请查看移动设备的应用商店（更多信息，请参阅 下载和安装 GlobalProtect 移动应用）。

要将最新的应用直接下载至防火墙，防火墙须具备可让其访问“Palo Alto Networks 更新服务器”的服务路由（请参阅向最终用户部署 GlobalProtect 应用程序）。如果防火墙没有访问 Internet 的权限，则可使用已连接至 Internet 的计算机从 Palo Alto Networks 软件更新支持站点下载应用软件包，然后将其手动上传至防火墙。

要手动下载应用软件包：

STEP 1 | 登录到 Palo Alto Networks 客户支持门户 (https://support.paloaltonetworks.com/)。

必须拥有有效 *Palo Alto Networks* 账户方可登录软件更新页面并下载软件。如果无法登录而需要帮助，请转到 https://www.paloaltonetworks.com/support/tabs/overview.html。

STEP 2 | 选择**Updates**（更新）> **Software Updates**（软件更新）。

STEP 3 | 按操作系统选择 GlobalProtect 应用版本。

STEP 4 | 查看应用版本的版本说明，然后选择下载链接以继续下载。

STEP 5 | 向最终用户部署 GlobalProtect 应用程序。

© 2019 Palo Alto Networks, Inc.

请参阅 Palo Alto Networks 兼容性矩阵，了解可以在其中安装 GlobalProtect 应用程序各版本的操作系统。

在门户上载入应用更新

部署 GlobalProtect 应用软件的最简方式是将新的应用程序包下载至承载门户的防火墙，然后激活该软件以便下载至连接到门户的应用上。要自动执行此操作，防火墙须具备可让其访问“Palo Alto Networks 更新服务器”的服务路由。如果防火墙没有访问 Internet 的权限，则可使用已连接至 Internet 的计算机从 Palo Alto Networks 软件更新支持站点 下载 GlobalProtect 应用 应用软件包，然后将其手动上传至防火墙。

自行定义如何在门户代理配置中部署应用软件更新：是在应用连接至门户时自动执行，还是提示用户升级应用，亦或允许最终用户手动查找和下载新应用版本。有关创建代理配置的详细信息，请参阅定义 GlobalProtect 代理配置。

STEP 1 | 在承载 GlobalProtect 门户的防火墙上，检查新的应用软件映像。

选择 **Device**（设备）> **GlobalProtect Client**（**GlobalProtect** 客户端）查看可用的应用软件映像列表。

- 如果防火墙拥有“更新服务器”的访问权限，则请单击 **Check Now**（立即检查）以查找最新更新。如果 **Action**（操作）列中的值为 **Download**（下载），则表示有可用的新版应用。
- 如果防火墙无权访问“更新服务器”，则必须从 Palo Alto Networks 软件更新支持站点手动下载软件映像，如步骤 2 所述。

STEP 2 | 下载应用软件映像。

- 如果防火墙可以访问“更新服务器”，请找到所需的应用版本，然后单击 **Download**（下载）。下载完成时，**Action**（操作）列中的值将变为 **Activate**（激活）。
- 如果防火墙无法访问更新服务器，下载 GlobalProtect 应用。下载软件映像后，返回防火墙的 **Device**（设备）> **GlobalProtect Client**（**GlobalProtect** 客户端）页面以进行 **Upload**（上传）。

STEP 3 | 激活应用软件映像以便最终用户可从门户进行下载。

一次只能激活一个版本的应用软件映像。如果激活新版本的同时有部分应用仍需先前激活的版本，则必须再次激活所需版本以便其可供下载。

- 如果已从“更新服务器”自动下载映像，则请单击 **Activate**（激活）。
- 如果已将软件映像手动上传至防火墙，则请单击 **Activate From File**（从文件激活），然后从下拉列表中选择已上传的 **GlobalProtect Client File**（**GlobalProtect** 客户端文件）。单击 **OK**（确定）以激活所选映像。可能需刷新页面方可使版本显示为 **Currently Activated**（当前已激活）。

在 Web 服务器上载入应用更新

如果有大量端点需安装和/或更新 GlobalProtect 应用软件，请考虑在外部 Web 服务器上载入 GlobalProtect 应用软件映像。当用户连接至防火墙以下载应用时，此举有助减轻防火墙的负载。

STEP 1 | 下载并激活您计划在 Web 服务器上托管到防火墙的 GlobalProtect 应用版本。

遵循在门户上载入应用更新中所述的在防火墙上下载和激活应用软件的步骤。

STEP 2 | 下载要在 Web 服务器上载入的 GlobalProtect 应用软件映像。

下载与在门户上所激活映像相同的映像。

从 Web 浏览器 下载 GlobalProtect 应用。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 将软件映像发布至 Web 服务器。

STEP 4 | 将最终用户重定向至 Web 服务器。

在承载门户的防火墙上，在操作模式下输入以下 CLI 命令：

```
> set global-protect redirect on
> set global-protect redirect location <path>
```

其中，*<path>* 为承载映像的文件夹 URL 路径，例如 **https://acme/GP**。

STEP 5 | 测试重定向。

1. 通过 Web 浏览器转到下列 URL：

   ```
   https://<portal address or name>
   ```

   例如，**https://gp.acme.com**。
2. 在门户登录页面上，输入用户 **Name**（名称）和 **Password**（密码），然后单击 **LOGIN**（登录）。成功登录后，门户会将您重定向至下载页面。

测试应用安装

使用下列过程测试 GlobalProtect 应用安装。

STEP 1 | 为测试应用安装创建代理配置。

在端点上初始安装 *GlobalProtect* 应用软件时，最终用户必须使用具有管理权限的帐户登录至系统。后续的应用软件更新无需具备管理权限。

最佳做法是创建仅限于少部分用户的代理配置，例如针对负责管理防火墙的 *IT* 部门中的管理员：

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）。
2. 选择想要修改的现有门户配置，或 **Add**（添加）新配置。
3. 在 **Agent**（代理）选项卡上，选择现有配置或 **Add**（添加）新配置，从而部署至测试用户/组。
4. 在 **User/User Group**（用户/用户组）选项卡上，**Add**（添加）将执行应用测试的**User/User Group**（用户/用户组）。
5. 在 **App**（应用程序）选项卡上，将 **Allow User to Upgrade GlobalProtect App**（允许用户升级 **GlobalProtect** 应用程序）设置为 **Allow with Prompt**（带提示允许）。单击 **OK**（确定）保存配置。
6. （可选）在 **Agent**（代理）选项卡上，选择刚刚创建/修改的代理配置，然后单击 **Move Up**（上移）以便将其置于列表中已创建的较通用配置之前。

   GlobalProtect 应用进行连接时，门户会将数据包中的源信息与已定义的代理配置进行比较。与安全规则评估相同，门户会从列表的顶部开始查找匹配项。在其找到匹配项后，会将对应的配置提交给应用程序。
7. **Commit**（提交）更改。

STEP 2 | 登录至 GlobalProtect 门户。

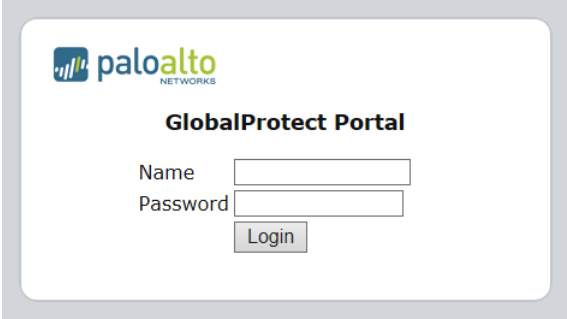
1. 启动 Web 浏览器并转到下列 URL：

   ```
   https://<portal address or name>
   ```


© 2019 Palo Alto Networks, Inc.

例如，`https://gp.acme.com`。

2. 在门户登录页面上，输入用户 **Name**（名称）和 **Password**（密码），然后单击 **LOG IN**（登录）。

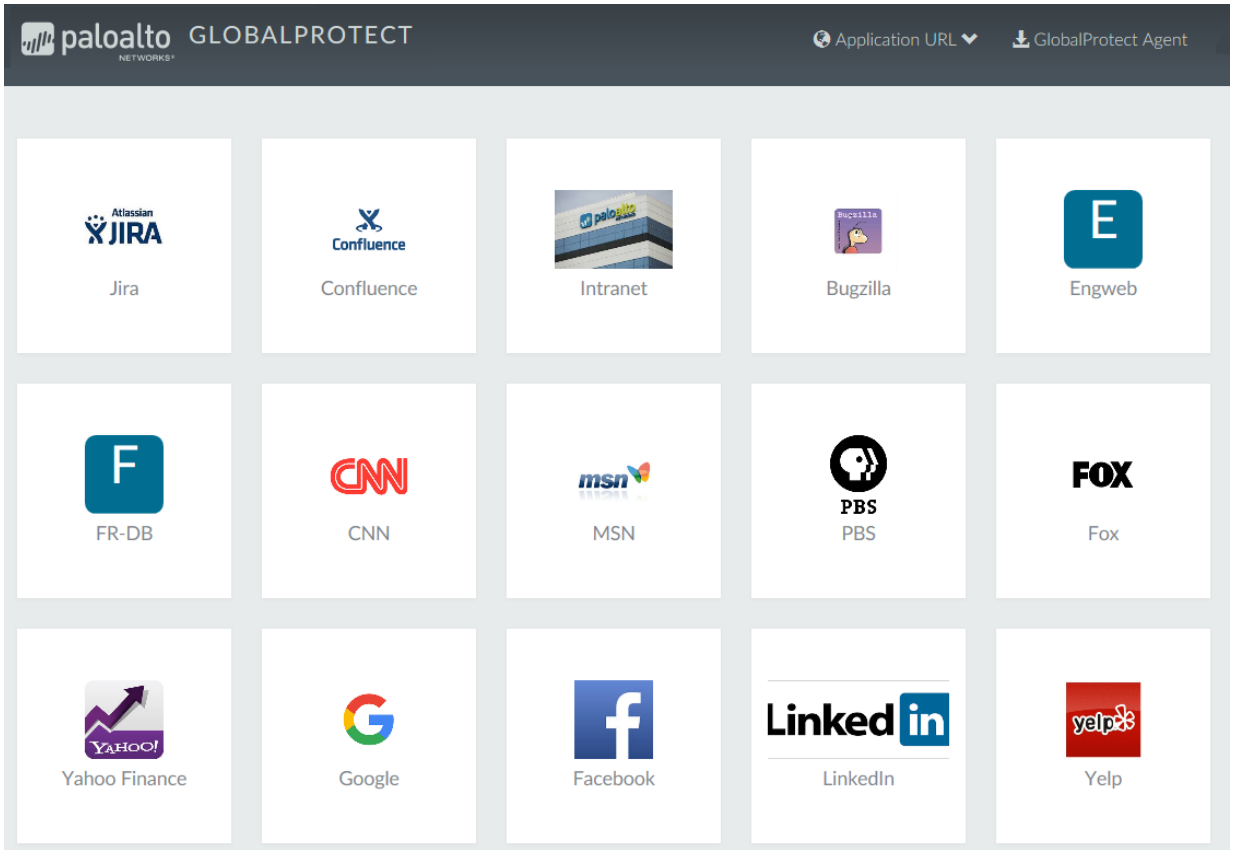


STEP 3 | 导航到应用下载页面。

在大多数情况下，登录门户后会立即显示应用下载页面。使用此页面下载最新的应用软件包。

如果您启用了 GlobalProtect 无客户端 VPN 访问，则应用程序将在您登录到门户后打开（而不是代理下载页面）。选择 **GlobalProtect Agent**（**GlobalProtect** 代理）打开下载页面。

© 2019 Palo Alto Networks, Inc.



STEP 4 | 下载应用程序。

1. 要开始下载，请单击与计算机上运行的操作系统相对应的链接。

© 2019 Palo Alto Networks, Inc.

2. 打开软件安装文件。
3. 当系统提示运行或保存软件时，单击 **Run**（运行）。
4. 出现提示时，单击 **Run**（运行）以启动“GlobalProtect 设置向导”。

在端点上初始安装 *GlobalProtect* 应用软件时，最终用户必须使用具有管理权限的帐户登录至系统。后续的应用软件更新无需具备管理权限。

STEP 5 | 完成 GlobalProtect 应用设置。

1. 在“GlobalProtect 设置向导”中，单击 **Next**（下一步）。
2. 单击 **Next**（下一步）接受默认安装文件夹 (`C:\Program Files\Palo Alto Networks\GlobalProtect`) 或 **Browse**（浏览）以选择新位置，然后双击 **Next**（下一步）。
3. 安装完成后，**Close**（关闭）向导。

STEP 6 | 登录至 GlobalProtect。

1. 单击系统托盘图片，启动 GlobalProtect 应用程序。状态面板打开。
2. 输入门户的 FQDN 或 IP 地址，然后单击 **Connect**（连接）。
3. （可选）默认情况下，您将根据管理员定义的配置和可用网关的响应时间自动连接到 **Best Available**（最佳可用）网关。要连接到其他网关，请从 **Gateway**（网关）下拉列表中选择网关（仅适用于外部网关）。

   仅当启用手动网关选择时，此选项才可用。

4. （可选）根据连接模式，单击 **Connect**（连接）以启动连接。
5. （可选）如果提示，请输入您的 **Username**（用户名）和 **Password**（密码），然后单击 **Sign In**（登录）。

如果身份验证成功，您将连接到企业网络，状态面板将显示 **Connected**（已连接）或 **Connected - Internal**（已连接 - 内部）状态。如果设置了 GlobalProtect 欢迎页面，则会在成功登录后显示。

© 2019 Palo Alto Networks, Inc.

下载和安装 GlobalProtect 移动应用

GlobalProtect 应用提供了将企业安全策略扩展至移动端点的简易方法。针对运行 GlobalProtect 应用的其他远程端点，该移动应用可实现通过 IPsec 或 SSL VPN 隧道安全访问公司网络。该应用将自动连接至距离最终用户当前所在位置最近的网关。此外，进出端点的流量也将自动受到应用于公司网络上其他主机的相同安全策略执行的控制。该移动应用将采集主机配置的相关信息，并将此信息用于实现基于 HIP 的增强安全策略执行。

安装 GlobalProtect 应用的方法主要有两种：可从第三方 MDM 部署应用，并以透明方式将应用推送至受管端点；或者，可直接从端点官方商店安装应用：

- iOS 端点 — 应用商店
- Android 端点和 Chromebook — Google Play

  从 GlobalProtect 应用程序 5.0 开始，用于Chrome OS 的 GlobalProtect 应用程序不再受支持；请改用 Android 版 GlobalProtect 应用程序。
- Windows 10 手机和 Windows 10 UWP 端点 — Microsoft Store

此工作流描述了如何直接在移动端点上安装 GlobalProtect 应用。有关如何从 AirWatch 部署 GlobalProtect 应用的说明，请参阅使用 AirWatch 部署 GlobalProtect 移动应用。

STEP 1 | 为测试应用安装创建代理配置。

最佳做法是创建仅限于少部分用户的代理配置，例如针对负责管理防火墙的 IT 部门中的管理员：

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）。
2. 选择现有门户配置进行修改，或 **Add**（添加）新配置。
3. 在 **Agent**（代理）选项卡上，选择现有配置或 **Add**（添加）新配置，从而部署至测试用户/组。
4. 在 **User/User Group**（用户/用户组）选项卡上，**Add**（添加）将执行应用测试的**User/User Group**（用户/用户组）。
5. 选择当前所测试的应用的 **OS**（操作系统）（**iOS**、**Android** 或 **WindowsUWP**）。
6. （可选）选择刚刚创建/修改的代理配置，然后单击 **Move Up**（上移）以便将其置于列表中已创建的较通用配置之前。
7. **Commit**（提交）更改。

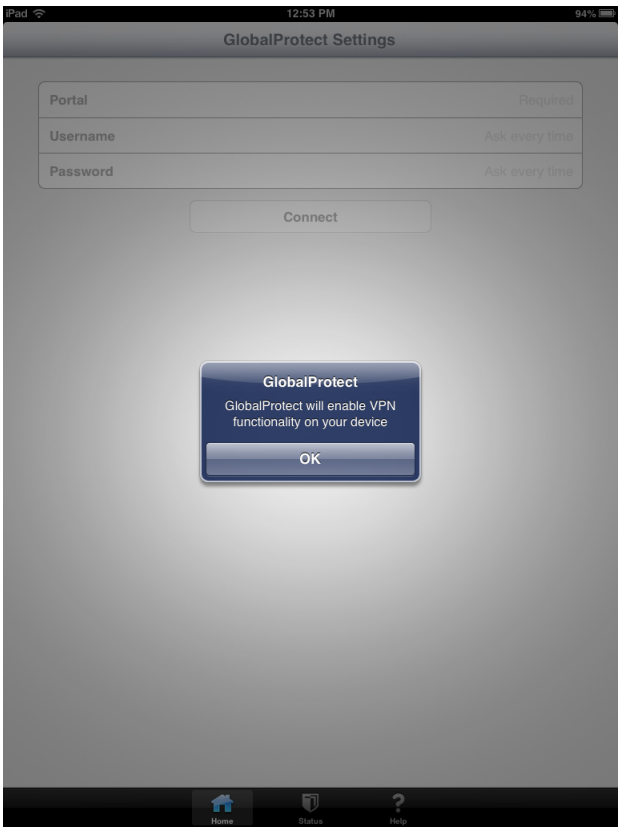
STEP 2 | 在端点上，按提示信息下载并安装应用。

- 在 Android 端点上，通过 Google Play 搜索该应用。
- 在 iOS 端点上，通过应用商店搜索该应用。
- 在 Windows 10 UWP 端点上，通过 Microsoft Store 搜索该应用。

STEP 3 | 启动应用。

安装成功后，GlobalProtect 应用图标将显示在端点的“主页”屏幕上。要启动应用，请点击图标。出现启用 GlobalProtect VPN 功能的提示时，点击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.



STEP 4 | 连接至门户。

1. 出现提示时，输入 **Portal**（门户）名称或地址、用户 **Name**（名称）和 **Password**（密码）。门户名称须为完全限定域名 (FQDN) 且开头不得包括“https://”。

2. 点击 **Connect**（连接）并验证该应用已与 GlobalProtect 成功建立连接。

   如果配置了第三方移动端点管理系统，该应用将提示您进行注册。

© 2019 Palo Alto Networks, Inc.

以透明方式部署应用设置

作为从门户配置部署应用设置的备用方法，可从 Windows 注册表、全局 macOS plist 或 Windows Installer (Msiexec)（仅适用于 Windows 端点）对其进行定义。其好处在于，可在端点首次连接至 GlobalProtect 门户前将 GlobalProtect 应用设置部署至端点。

在门户配置中定义的设置将始终替代在 Windows 注册表或 macOS plist 中定义的设置。如果在注册表或 plist 中定义了设置，但门户配置指定了不同设置，则应用程序从门户接收的设置将替代端点中所定义的设置。此覆盖还适用于与登录相关的设置，例如是否按需进行连接、是否使用单点登录 (SSO) 以及是否在门户证书无效时允许应用程序进行连接。所以，应避免设置冲突。此外，门户配置将缓存于端点上。缓存的配置将在 GlobalProtect 应用重启或端点机器重新引导时随时使用。

以下各节介绍了可用的可自定义应用设置以及如何将这些设置透明地部署到 Windows 和 macOS 客户端：

- 可自定义的应用设置
- 将应用设置部署到 Windows 端点
- 将应用设置部署到 macOS 端点

除了使用 *Windows* 注册表和 *macOS plist* 部署 *GlobalProtect* 应用程序设置以外，您还可以启用 *GlobalProtect* 应用程序从端点收集特定的 *Windows* 注册表或 *macOS plist* 信息，包括有关端点上安装的应用程序的数据、端点上运行的进程以及这些应用程序和进程的特性和属性。然后，您可以监控数据并将其添加到安全规则作为匹配条件。您可以根据安全规则强制执行与所定义的注册表设置相匹配的端点流量。此外，您还可设置自定义检查来从端点收集应用程序和流程数据。

可自定义的应用设置

除预部署门户地址外，还可定义应用程序设置。要将应用程序设置部署到 Windows 端点，可以在 Windows 注册表中定义密钥（`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`）。要 将应用程序设置部署到 macOS 端点，可在 macOS plist `PanSetup`词典中定义条目（`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`）。仅对于 Windows 端点，还可使用 Windows Installer 从 Msiexec 部署应用程序设置。

以下主题介绍各自定义应用程序设置。在 GlobalProtect 门户代理配置中定义的设置优先于在 Windows 注册表或 macOS plist 中定义的设置。

一些设置在 *Web* 界面上没有相应的门户配置设置，必须使用 *Windows* 注册表或 *Msiexec* 进行配置。这些附加设置包括：*`can-prompt-user-credential`*、*`wrap-cp-guid`* 以及 *`filter-non-gpcp`*。

- 应用显示选项
- 用户行为选项
- 应用行为选项
- 脚本部署选项

应用显示选项

下表列出了您可在 Windows 注册表和 macOS plist 中配置以自定义 GlobalProtect 应用程序的选项。

© 2019 Palo Alto Networks, Inc.

表 3: 表：可自定义的应用设置

门户代理配置	Windows 注册表/macOS Plist	Msiexec 参数	Default（默认）
启用高级视图	`enable-advanced-view yes | no`	`ENABLEADVANCEDVIEW="yes | no"`	是
显示 GlobalProtect 图标	`show-agent-icon yes | no`	`SHOWAGENTICON="yes | no"`	是
启用 Rediscover Network（重新发现网络）选项	`rediscover-network yes | no`	`REDISCOVERNETWORK="yes | no"`	是
启用 Resubmit Host Profile（重新提交主机配置文件）选项	`resubmit-host-info yes | no`	`RESUBMITHOSTINFO="yes | no"`	是
显示系统托盘通知	`show-system-tray-notifications yes | no`	`SHOWSYSTEMTRAYNOTIFICATIONS="yes | no"`	是

用户行为选项

下表列出了您可在 Windows 注册表和 macOS plist 中配置以自定义用户与 GlobalProtect 应用交互方式的选项。

表 4: 表：自定义用户行为选项

门户代理配置	Windows 注册表/macOS Plist	Msiexec 参数	Default（默认）
允许用户更改门户地址	`can-change-portal yes | no`	`CANCHANGEPORTAL="yes | no"`	是
允许用户解除欢迎页面	`enable-hide-welcome-page yes | no`	`ENABLEHIDEWELCOMEPAGE= "yes | no"`	是
允许用户继续使用无效门户服务器证书	`can-continue-if-portal-cert-invalid yes | no`	`CANCONTINUEIFPORTALCERTINVALID= "yes | no"`	是
允许用户禁用 GlobalProtect 应用程序	`disable-allowed yes | no`	`DISABLEALLOWED="yes | no"`	否
保存用户凭据 指定 0 防止 GlobalProtect 保存凭据，指定 1 保存用户名和密码，或	`save-user-credentials 0 | 1 | 2`	`SAVEUSERCREDENTIALS 0 | 1 | 2`	不适用

© 2019 Palo Alto Networks, Inc.

门户代理配置	Windows 注册表/macOS Plist	Msiexec 参数	Default（默认）
指定 2 仅保存用户名。			
不在门户中 不推荐在 PAN-OS 7.1 和更高版本的 Web 界面中设置 **Allow user to save password**（允许用户保存密码），但可从 Windows 注册表和 macOS plist 配置。**Save User Credentials**（保存用户凭据）字段中指定的任何值覆盖此处指定的值。	`can-save-password yes | no`	`CANSAVEPASSWORD="yes | no"`	是
仅限 **Windows**/不在门户中 此设置让 GlobalProtect 凭据提供程序可以显示 **Start GlobalProtect Connection**（开始 **GlobalProtect** 连接）按钮，允许用户手动启动 GlobalProtect 预登录连接。	`ShowPrelogonButton yes | no`	不适用	否

应用行为选项

下表列出了您可在 Windows 注册表和 macOS plist 中配置以自定义 GlobalProtect 应用行为的选项。

表 **5:** 表：自定义应用行为选项

门户代理配置	Windows 注册表/macOS Plist	Msiexec 参数	Default（默认）
连接方法	`connect-method on-demand | pre-logon | user-logon`	`CONNECTMETHOD="on-demand | pre-logon | user-logon"`	`user-logon`
GlobalProtect 应用程序配置刷新时间间隔（小时）	`refresh-config-interval <hours>`	`REFRESHCONFIGINTERVAL= "<hours>"`	`24`

© 2019 Palo Alto Networks, Inc.

门户代理配置	Windows 注册表/macOS Plist	Msiexec 参数	Default（默认）
连接时更新 DNS 设置（仅 Windows）	flushdns yes | no	FLUSHDNS="yes | no"	否
Windows 安全中心 (WSC) 状态变更后立即发送 HIP 报告（仅 Windows）	wscautodetect yes | no	WSCAUTODETECT="yes | no"	否
检测每个连接的代理（仅限 Windows）	ProxyMultipleAuto Detection yes | no	ProxyMultipleAuto Detection="yes | no"	否
退出登录时清空单点登录凭据（仅限 Windows）	LogoutRemoveSSO yes | no	LogoutRemoveSSO="yes | no"	是
Kerberos 身份验证失败时使用默认身份验证（仅限 Windows）	krb-auth-fail-fallback yes | no	KRBAUTHFAILFALLBACK= "yes | no"	否
使用默认浏览器进行 SAML 身份验证	(macOS plist) default-browser yes | no	DEFAULTBROWSER= "yes | no"	否
自定义密码到期信息（仅限 LDAP 身份验证）	PasswordExpiryMessage <message>	PasswordExpiryMessage "<message>"	
门户连接超时（秒）	PortalTimeout <portaltimeout>	PORTALTIMEOUT= "<portaltimeout>"	5
TCP 连接超时（秒）	ConnectTimeout <connecttimeout>	CONNECTTIMEOUT= "<connecttimeout>"	5
TCP 接收超时（秒）	ReceiveTimeout <receivetimeout>	RECEIVETIMEOUT= "<receivetimeout>"	30
客户端证书商店查找	certificate-store-lookup user | machine | user and machine | invalid	CERTIFICATESTORELOOKUP= "user | machine | user and machine | invalid"	user and machine
SCEP 证书续订期限（天数）	scep-certificate-renewal-period <renewalPeriod>	不适用	7
最大内部网关连接尝试次数	max-internal-gateway-connection-attempts <maxValue>	MIGCA="<maxValue>"	0

© 2019 Palo Alto Networks, Inc.

门户代理配置	Windows 注册表/macOS Plist	Msiexec 参数	Default（默认）
客户端证书扩展秘钥使用对象标识符 (OID)	`ext-key-usage-oid-for-client-cert <oidValue>`	`EXTCERTOID="<oidValue>"`	不适用
用户交换机隧道重命名超时（秒）	`user-switch-tunnel-rename-timeout <renameTimeout>`	不适用	0
使用单点登录 （仅限 Windows）	`use-sso yes | no`	`USESSO="yes | no"`	是
不在门户中 此设置指定默认门户 IP 地址（或主机名）。	`portal <IPaddress>`	`PORTAL="<IPaddress>"`	不适用
不在门户中 此设置可让 GlobalProtect 在用户登录设备并连接 GlobalProtect 门户前发起 VPN 隧道。	`prelogon 1`	`PRELOGON="1"`	1
仅限 Windows/不在门户中 该设置将与单点登录 (SSO) 一同使用，指示当 SSO 失败时是否提示用户提供凭证。	`can-prompt-user-credential yes | no`	`CANPROMPTUSERCREDENTIAL="yes | no"`	是
仅限 Windows/不在门户中 此设置从 Windows 登录页面筛选第三方凭据提供程序磁贴，从而只显示本机 Windows 磁贴。*	`wrap-cp-guid {third party credential provider guid}`	`WRAPCPGUID="{guid_value]"` `FILTERNONGPCP="yes | no"`	否
仅限 Windows/不在门户中 此设置是设置 wrap-cp-guid 的附加选项，除本机 Windows 登录磁贴以外，还允许在 Windows 登录页面	`filter-non-gpcp no`	不适用	不适用

© 2019 Palo Alto Networks, Inc.

门户代理配置	Windows 注册表/macOS Plist	Msiexec 参数	Default（默认）
上显示第三方凭据提供程序磁贴。*			
仅限 **Windows**/不在门户中 此设置允许您将静态 IP 地址分配给 Windows 端点。	**reserved-ipv4 <reserved-ipv4>** **reserved-ipv6 <reserved-ipv6>**	**RESERVEDIPV4="<reserved-ipv4>"** **RESERVEDIPV6="<reserved-ipv6>"**	不适用

*有关使用 *Windows* 注册表或 *Windows Installer (Msiexec)* 启用这些设置的详细步骤，请参阅 Windows 端点上第三方凭据提供程序的 SSO 包装。

脚本部署选项

下表显示了让 GlobalProtect 在建立连接前后和断开连接之前启动脚本的选项。因为这些选项在门户中不可用，必须从 Windows 注册表或 macOS plist 定义相关密钥的值 — pre-vpn-connect、post-vpn-connect 或 pre-vpn-disconnect。有关部署脚本的详细步骤，请参阅使用 Windows 注册表部署脚本、使用 Msiexec 部署脚本或使用 macOS Plist 部署脚本。

表：自定义脚本部署选项

门户代理配置	Windows 注册表/macOS Plist	Msiexec 参数	Default（默认）
执行在命令设置中指定的脚本（包括传递给此脚本的任何参数）。 支持环境变量。 指定在命令中的完整路径。	**command <parameter1> <parameter2> [...]** Windows 示例： **command %userprofile%\vpn_script.bat c:test_user** macOS 示例： **command $HOME/vpn_script.sh /Users/test_user test_user**	**PREVPNCONNECTCOMMAND="<parameter1> <parameter2> [...]"** **POSTVPNCONNECTCOMMAND="<parameter1> <parameter2> [...]"** **PREVPNDISCONNECTCOMMAND="<parameter1> <parameter2> [...]"**	不适用
（可选）指定命令可根据什么权限运行（默认值为 user（用户）；如果您不指定上下文，此命令作为当前活跃用户运行）。	**context admin | user**	**PREVPNCONNECTCONTEXT="admin | user"** **POSTVPNCONNECTCONTEXT="admin | user"** **PREVPNDISCONNECTCONTEXT="admin | user"**	**user**
（可选）指定 GlobalProtect 应用等待命令执行的秒数（范围是 0 -120）。如果命令没有在超时前完成，应用会继续建立或断开连接。0	**timeout <value>** 示例： **timeout 60**	**PREVPNCONNECTTIMEOUT="<value>"** **POSTVPNCONNECTTIMEOUT="<value>"**	0

© 2019 Palo Alto Networks, Inc.

门户代理配置	Windows 注册表/macOS Plist	Msiexec 参数	Default（默认）
值（默认）表示应用不会等待命令执行。 不支持 *post-vpn-connect*。		**PREVPNDISCONNECTTIMEOUT= ”<value>”**	
（可选）指定在命令中使用的文件的完整路径。GlobalProtect 应用将根据校验和密钥指定的值检查文件的完整性。 支持环境变量。	**file <path_file>**	**PREVPNCONNECTFILE= ”<path_file>”** **POSTVPNCONNECTFILE= ”<path_file>”** **PREVPNDISCONNECTFILE= ”<path_file>”**	不适用
（可选）指定文件密钥中引用的文件的 sha256 校验和。如果指定了校验和，GlobalProtect 应用只在 GlobalProtect 应用生成的校验和与在此指定的校验和值匹配时执行命令。	**checksum <value>**	**PREVPNCONNECTCHECKSUM= ”<value>”** **POSTVPNCONNECTCHECKSUM= ”<value>”** **PREVPNDISCONNECTCHECKSUM =”<value>”**	不适用
（可选）指定在命令不可执行或命令以非零返回码退出时向用户显示的错误消息。 消息长度不得超过 *1,024* 个 *ANSI* 字符。	**error-msg <message>** 示例： **error-msg pre-vpn-connect** 操作执行失败#	**PREVPNCONNECTERRORMSG= ”<message>”** **POSTVPNCONNECTERRORMSG= ”<message>”** **PREVPNDISCONNECTERRORMSG =”<message>”**	不适用

将应用设置部署到 Windows 端点

使用 Windows 注册表或 Windows Installer (Msiexec) 将 GlobalProtect 应用程序和设置透明地部署到 Windows 端点。

- 在 Windows 注册表中部署代理设置
- 从 Msiexec 部署代理设置
- 使用 Windows 注册表部署脚本
- 使用 Msiexec 部署脚本
- 在 Windows 注册表中部署“登录前连接”设置
- Windows 端点上第三方凭据提供程序的 SSO 包装
- 使用 Windows 注册表启用第三方凭据的 SSO 包装
- 使用 Windows Installer 启用第三方凭据的 SSO 包装

© 2019 Palo Alto Networks, Inc.

在 *Windows* 注册表中部署应用设置

在使用 Windows 注册表首次连接至 GlobalProtect 门户之前，可以将 GlobalProtect 应用程序设置部署到 Windows 端点。从使用下表中所述的选项开始，使用 Windows 注册表自定义 Windows 端点的应用设置。

除了使用 *Windows* 注册表部署 *GlobalProtect* 应用程序设置以外，您可以启用 *GlobalProtect* 应用程序从 *Windows* 端点收集特定的 *Windows* 注册表信息。然后，您可以监控数据并将其添加到安全规则作为匹配条件。您可以根据安全规则强制执行与所定义的注册表设置相匹配的端点流量。此外，您还可设置自定义检查来从端点收集应用程序和流程数据。

STEP 1 | 在 Windows 注册表中找到 GlobalProtect 应用程序自定义设置。

打开 Windows 注册表（在命令提示符中输入 **regedit**），并转到：

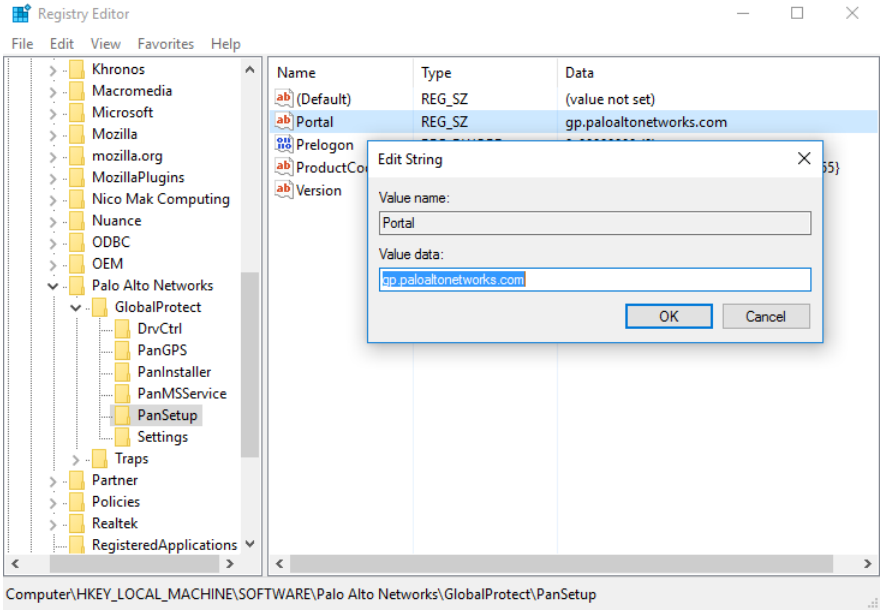
```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\
```

STEP 2 | 设置门户名称。

如果希望最终用户即便在首次连接时也无需手动输入门户地址，则可通过 Windows 注册表预部署门户地址：

1. 在 Windows 注册表中，请转到：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup
   ```
2. 右击 **Portal**（门户），然后选择 **Modify**（修改）。
3. 在 **Value data**（值数据）字段内输入门户名称，然后单击 **OK**（确定）。



STEP 3 | 将各种设置部署到 Windows 端点，包括配置 GlobalProtect 应用程序的连接方法和单点登录 (SSO)。

查看自定义应用设置，获取可以使用 Windows 注册表设置的命令和值的完整列表。

登录到端点之前，您可以在启用最终用户登录到 VPN 之前，选择此选项以部署登录前连接设置到 Windows 端点。

STEP 4 | 在 Windows 端点上启用 GlobalProtect 应用程序包装第三方凭据，允许在使用第三方凭据提供程序时启用 SSO。

© 2019 Palo Alto Networks, Inc.

使用 Windows 注册表启用第三方凭据的 SSO 包装。

从 *Msiexec* 部署应用设置

在 Windows 端点上，可使用下列语法从 Windows Installer (Msiexec) 自动部署 GlobalProtect 应用程序和应用程序设置：

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec 是从命令行安装或配置产品的可执行程序。在运行 *Microsoft Windows XP* 或更高操作系统的端点上，可在命令提示符中使用的最大字符串长度是 *8,191* 个字符。

Msiexec 示例	说明
msiexec.exe /i GlobalProtect.msi /quiet PORTAL="portal.acme.com"	以安静模式（无用户交互）安装 GlobalProtect，并配置门户地址。
msiexec.exe /i GlobalProtect.msi CANCONTINUEIFPORTALCERTINVALID="no"	安装 GlobalProtect，选择在证书无效时阻止用户连接至门户。

有关设置及相应默认值的完整列表，请参阅自定义应用设置。

此外，还可以使用 Windows Installer 启用第三方凭据的 SSO 包装。

使用 *Windows* 注册表部署脚本

可使用 Windows 注册表将自定义脚本部署到 Windows 端点。

可配置 GlobalProtect 应用程序为任何或所有以下事件启动并运行脚本：建立隧道前后，和断开隧道连接前。要在特殊事件发生时运行脚本，从 command 注册表项为此事件引用批处理脚本。

根据配置设置，GlobalProtect 应用可在应用建立与网关的连接前后，以及应用断开连接之前运行脚本。从使用下表中所述的选项开始，使用 Windows 注册表自定义 Windows 端点的应用设置。

运行 *GlobalProtect* 应用 *2.3* 及更高版本的端点支持可用于部署脚本的注册表设置。

STEP 1 | 打开 Windows 注册表，找到 GlobalProtect 应用自定义设置。

打开 Windows 注册表（在命令提示符中输入 **regedit**），根据要执行脚本的时间（连接前/后或断开连接前）转到其中一个注册表项位置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\pre-vpn-connect
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\post-vpn-connect
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\pre-vpn-disconnect
```


© 2019 Palo Alto Networks, Inc.

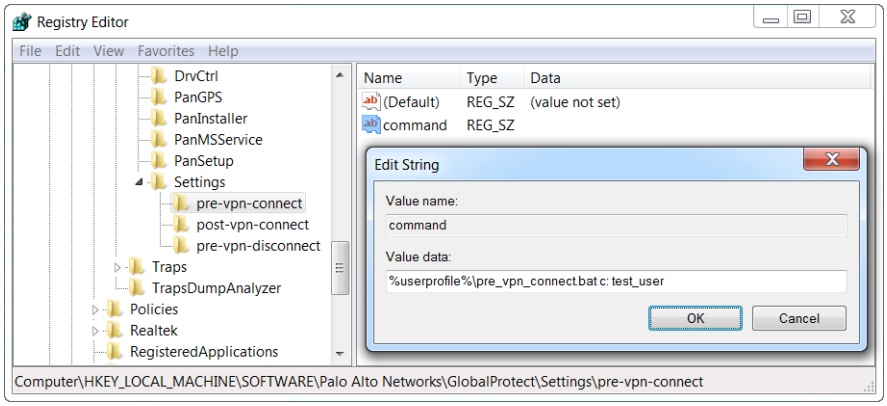
如果此注册表项不在 *Settings*（设置）注册表项中，创建一个（右击 *Settings*（设置），选择 *New*（新建）> *Key*（表项））。

STEP 2 | 创建名为 **command** 的新字符串值，让 GlobalProtect 应用运行脚本。

在此指定的批处理文件应包括您想在设备上运行的特定脚本（包含传递给此脚本的任何参数）。

1. 如果 `command` 字符串不存在，则创建一个，方法是右键单击 `pre-vpn-connect`、`post-vpn-connect` 或 `pre-vpn-disconnect`，选择 **New**（新建）> **String Value**（字符串值），并将其命名为 **command**。
2. 右击 `command`，然后选择 **Modify**（修改）。
3. 输入 GlobalProtect 应用应运行的命令或脚本。例如：

```
%userprofile%\pre_vpn_connect.bat c:test_user
```



STEP 3 | （可选）根据需要，为每个命令添加其他注册表项。

创建或修改注册表项和相应值，包括 `context`、`timeout`、`file`、`checksum` 或 `error-msg`。更多信息，请参阅自定义应用设置。

使用 *Msiexec* 部署脚本

在 Windows 端点上，可使用 Windows Installer (Msiexec) 部署 GlobalProtect 应用、应用设置和应用将自动运行的脚本（参阅自定义应用设置）。为此，请使用以下语法：

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec 是从命令行安装或配置产品的可执行程序。在运行 *Microsoft Windows XP* 或更高版本的系统上，可在命令提示符中使用的最大字符串长度是 *8,191* 个字符。

此限制适用于命令行、其他进程继承的个别环境变量（例如 *USERPROFILE* 变量）和所有环境变量扩展。如果从命令行运行批处理文件，此限制还适用于批处理文件处理。

例如，要部署在特定连接或断开连接事件发生时运行的脚本，可使用与以下示例类似的语法：

示例：使用 **Msiexec** 部署在连接事件前运行的脚本

有关您可复制粘贴的脚本，请转到此处。

© 2019 Palo Alto Networks, Inc.

```
msiexec.exe /i GlobalProtect.msi
PREVPNCONNECTCOMMAND="%userprofile%\pre_vpn_connect.bat c: test_user"
PREVPNCONNECTCONTEXT="user"
PREVPNCONNECTTIMEOUT="60"
PREVPNCONNECTFILE="C:\Users\test_user\pre_vpn_connect.bat"
PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
8647ccf599"
PREVPNCONNECTERRORMSG="Failed executing pre-vpn-connect action."
```

有关设置及相应默认值的完整列表，请参阅自定义应用设置。

示例：使用 **Msiexec** 部署在连接前、连接后或断开连接事件前运行的脚本

有关您可复制粘贴的脚本，请转到此处。

```
msiexec.exe /i GlobalProtect.msi
PREVPNCONNECTCOMMAND="%userprofile%\pre_vpn_connect.bat c: test_user"
PREVPNCONNECTCONTEXT="user"
PREVPNCONNECTTIMEOUT="60"
PREVPNCONNECTFILE="C:\Users\test_user\pre_vpn_connect.bat"
PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
8647ccf599"
PREVPNCONNECTERRORMSG="Failed executing pre-vpn-connect action."
POSTVPNCONNECTCOMMAND="c:\users\test_user\post_vpn_connect.bat c: test_user"
POSTVPNCONNECTCONTEXT="admin"
POSTVPNCONNECTFILE="%userprofile%\post_vpn_connect.bat"
POSTVPNCONNECTCHECKSUM="b48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
8647ccf598"
POSTVPNCONNECTERRORMSG="Failed executing post-vpn-connect action."
PREVPNDISCONNECTCOMMAND="%userprofile%\pre_vpn_disconnect.bat c: test_user"
PREVPNDISCONNECTCONTEXT="admin"
PREVPNDISCONNECTTIMEOUT="0"
PREVPNDISCONNECTFILE="C:\Users\test_user\pre_vpn_disconnect.bat"
PREVPNDISCONNECTCHECKSUM="c48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0
118647ccf597"
PREVPNDISCONNECTERRORMSG="Failed executing pre-vpn-disconnect action."
```

有关设置及相应默认值的完整列表，请参阅自定义应用设置。

在 *Windows* 注册表中部署“登录前连接”设置

登录到端点之前，您可以在启用最终用户登录到 VPN 之前，使用 Windows 注册表部署“登录前连接”设置到 Windows 10 端点。GlobalProtect 仅在 GlobalProtect 应用程序初始化时检索一次注册表项。

登录前连接无法同时支持“预登录”和“先预登录再按需”的连接方法。

STEP 1 | 在最终用户 Windows 端点上配置注册表项。

启用“登录前连接”之前，您必须更改最终用户 Windows 端点上的 Windows 注册表。您可以自动添加注册表项或手动添加此项。

© 2019 Palo Alto Networks, Inc.

- 若要在 **PanGPS.exe** 中自动添加 `PanPlapProvider` 和 `PanPlapProvider.dll` 的注册表项（`C:\Program Files\Palo Alto Networks\GlobalProtect`），请使用 `-registerplap` 命令，通过下列语法以管理员身份运行：

```
PanGPS.exe -registerplap
```

- 若要在 **PanGPS.exe** 中自动取消注册 `PanPlapProvider` 和 `PanPlapProvider.dll` 的注册表项（`C:\Program Files\Palo Alto Networks\GlobalProtect`），请使用 `-unregisterplap` 命令，通过下列语法以管理员身份运行：

```
PanGPS.exe -unregisterplap
```

若要手动添加注册表项，请打开 Windows 注册表编辑器，然后在命令提示符中输入 **regedit**。

您必须创建 *CLSID* 文件夹。

1. 在 Windows 注册表中，前往 `HKEY_CLASSES_ROOT\CLSID\{20A29589-E76A-488B-A520-63582302A285}`。

   添加 `PanPlapProvider` 值，格式为 **`@=PanPlapProvider`**。
2. 在 Windows 注册表中，前往 `HKEY_CLASSES_ROOT\CLSID\{20A29589-E76A-488B-A520-63582302A285}\InprocServer32@="PanPlapProvider.dll"`。

   验证 **ThreadingModel** 的值是否设为 **Apartment**。这是默认值。
3. 在 Windows 注册表中，前往 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers\{20A29589-E76A-488B-A520-63582302A285}@="PanPlapProvider"`。

   添加 `PanPlapProvider` 值，格式为 **`@=PanPlapProvider`**。

STEP 2 | （可选）配置其他要显示的门户地址或名称。

配置后，登录前连接将使用 *Windows* 注册表中默认的门户地址或名称（*`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup`*，注册表项为 *`Portal`*）。

您可以通过更改最终用户 Windows 端点上的注册表项，配置您要在门户下拉列表中显示的其他门户地址或名称。您最多可以添加 5 个门户地址或名称。您必须先更改最终用户 Windows 端点上的 Windows 注册表，然后才能定义门户地址或名称。

打开 Windows 注册表编辑器，然后在命令提示符中输入 **regedit**。

1. 在 Windows 注册表中的 `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect` 下创建 `CBL` 文件夹。
2. 在 Windows 注册表中，前往 `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`。
3. 选择 **Edit**（编辑）> **New**（新建）> **String Value**（字符串值），为您要添加的所有门户创建注册表项。

   您必须将各个条目指定为 *Portal1*、*Portal2*、*Portal3*、*Portal4* 和 *Portal5*。所有条目均不得包含空格。
4. 右键单击 *portal* 注册表值，然后选择 **Modify**（修改）。
5. 在 **Value Data** 字段中输入 GlobalProtect 门户的 IP 地址或名称，然后单击 **OK**（确定）。
6. 针对您要添加的各个门户，请重复步骤 3 和 4。

STEP 3 | （可选）显示预定义门户地址或名称。

© 2019 Palo Alto Networks, Inc.

您必须先更改最终用户 Windows 端点上的 Windows 注册表，然后才能显示门户地址或名称。

打开 Windows 注册表编辑器，然后在命令提示符中输入 **regedit**。

1. 在 Windows 注册表中的 `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect` 下创建 `CBL` 文件夹。
2. 在 Windows 注册表中，前往 `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`。
3. 选择 **Edit**（编辑）> **New**（新建）> **String Value**（字符串值），为 *AlwaysShowPortal* 创建注册表项。
4. 在 **Value data**（值数据）字段内输入值 *Yes*（是），然后单击 **OK**（确定）。

如果只定义一个门户，“登录前连接”默认不会显示门户地址或名称。

STEP 4 | （可选）启用最终用户使用智能卡执行身份验证。

您必须先更改最终用户 Windows 端点上的 Windows 注册表，然后才能启用智能卡身份验证。

打开 Windows 注册表编辑器，然后在命令提示符中输入 **regedit**。

1. 在 Windows 注册表中的 `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect` 下创建 `CBL` 文件夹。
2. 在 Windows 注册表中，前往 `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`。
3. 选择 **Edit**（编辑）> **New**（新建）> **String Value**（字符串值）为 *UseSmartCard* 创建注册表项。
4. 在 **Value data**（值数据）字段内输入值 *Yes*（是），然后单击 **OK**（确定）。

STEP 5 | 重新启动端点。

要使 PLAP 和登录前连接注册表项生效，必须重新启动端点。

STEP 6 | 验证配置。

在 Windows 注册表中配置完设置，并使用运行 GlobalProtect™ 应用程序 5.2 或更高版本的登录前连接后，请选择身份验证方法：

- 使用智能卡身份验证执行登录前连接
- 使用 SAML 身份验证执行登录前连接
- 使用基于用户名/密码的身份验证执行登录前连接

Windows 端点上第三方凭据提供程序的 *SSO* 包装

在 Windows 7 端点上，GlobalProtect 应用利用 Microsoft 凭据提供程序框架来支持单点登录 (SSO)。通过 SSO，GlobalProtect 凭据提供程序包装 Windows 本机凭据提供程序，这使得 GlobalProtect 能够使用 Windows 登录凭据自动进行身份验证并连接至 GlobalProtect 门户和网关。此外，SSO 包装使 Windows 10 用户可以在密码过期或管理员要求在下次登录时更改密码时，使用 GlobalProtect 凭据提供程序更新其 Active Directory (AD) 密码。

当端点上也存在其他第三方凭据提供程序时，GlobalProtect 凭据提供程序无法收集用户的 Windows 登录凭据。由此，GlobalProtect 将无法自动连接到 GlobalProtect 门户和网关。如果 SSO 失败，您可辨识第三方凭据提供程序，然后将 GlobalProtect 应用配置为包装这些第三方凭据，这使得用户能够仅通过 Windows 登录凭证成功验证至 Windows、GlobalProtect 以及第三方凭据提供程序。

您还可选择将 Windows 配置为显示单独的登录磁贴：一个用于各第三方凭据提供程序，另一个用于本机 Windows 登录。当第三方凭据提供程序添加不适用于 GlobalProtect 的其他功能时，这十分有用。

© 2019 Palo Alto Networks, Inc.

如果您想要从您的 *Windows* 端点移除 *GlobalProtect* 凭据供应商，请在命令提示符中执行 ***GlobalProtectPanGPS.exe -u*** 命令。

使用 Windows 注册表或 Windows Installer (`msiexec`)允许 GlobalProtect 包装第三方凭据：

- 使用 Windows 注册表启用第三方凭据的 SSO 包装
- 使用 Windows Installer 启用第三方凭据的 SSO 包装

针对第三方凭据提供程序 *(CP)* 的 *GlobalProtect SSO* 包装取决于第三方 *CP* 设置。在某些情况下，如果第三方 *CP* 实施不允许 *GlobalProtect* 成功包装其 *CP*，则 *GlobalProtect SSO* 包装可能无法正常工作。

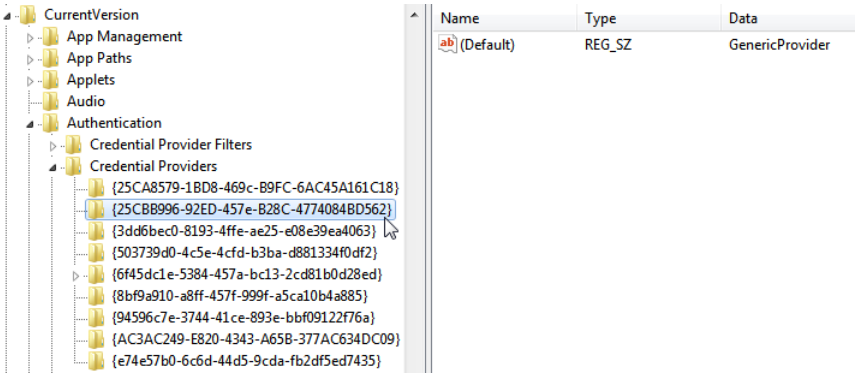
使用 *Windows* 注册表启用第三方凭据的 *SSO* 包装

在 Windows 注册表中按照以下步骤在 Windows 7 端点上启用 SSO 包装第三方凭据。

STEP 1 | 打开 Windows 注册表，并找到要包装的第三方凭据提供程序的全局唯一标识符 (GUID)。

1. 在命令提示符中，输入命令**`regedit`** 以打开 Windows 注册表编辑器。
2. 转到以下 Windows 注册表位置以查看当前安装的凭据提供程序列表：

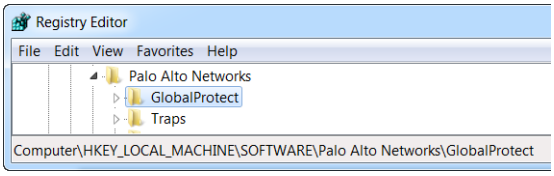
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers`。
3. 复制要包装的凭据提供程序的 GUID 项（包括 GUID 两端的大括号 — { 和 }）：



STEP 2 | 通过将设置 **`wrap-cp-guid`** 添加到 GlobalProtect 注册表来为第三方凭据提供商启用 SSO 包装。

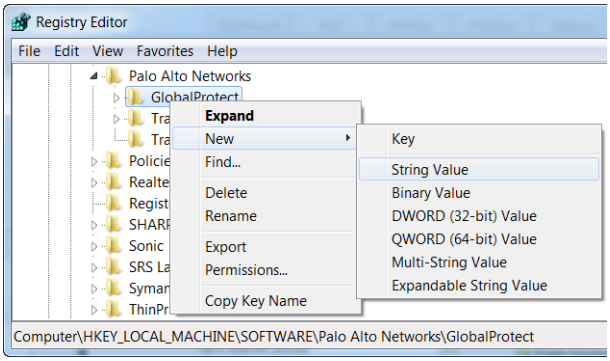
1. 转到以下 Windows 注册表位置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\ GlobalProtect:
```



2. 右击 **GlobalProtect** 文件夹，然后选择 **New**（新）> **String Value**（字符串值）以添加新的字符串值：

© 2019 Palo Alto Networks, Inc.



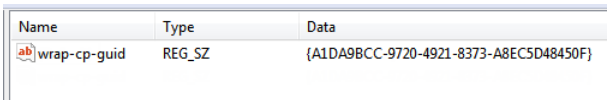
3. 配置以下 **String Value**（字符串值）字段：
   - **Name**（名称）：**`wrap-cp-guid`**
   - **Value data**（值数据）：{<**`third-party credential provider GUID`**>}

     在 *Value data*（值数据）字段中，输入的 *GUID* 值必须使用大括号括起来：*{ and }*。

     以下是 **Value data**（值数据）字段中的第三方凭据提供程序 GUID 的示例：

     ```
     {A1DA9BCC-9720-4921-8373-A8EC5D48450F}
     ```

     对于新的 **String Value**（字符串值），`wrap-cp-guid` 显示为该字符串值的 **Name**（名称），GUID 显示为 **Value Data**（值数据）。

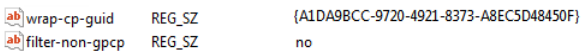


STEP 3 | 后续步骤：

- 使用此设置，可以在登录屏幕上向用户显示本机 Windows 登录磁贴。当用户单击磁贴并使用他们的 Windows 凭据登陆系统时，单点登录将对 Windows、GlobalProtect 和第三方凭据提供程序的用户进行身份验证。
- （可选）如果要在登录屏幕上向用户显示多个磁贴，即本机 Windows 磁贴和第三方凭据提供程序磁贴，可以继续执行步骤 4。
- （可选）如果要为用户分配默认凭据提供程序，可以继续执行步骤 5。
- （可选）如果要在登录屏幕上隐藏第三方凭据提供程序，可以继续执行步骤 6。

STEP 4 | （可选）允许在登录时向用户显示第三方凭据提供程序磁贴。

使用 **Name**（名称）**`filter-non-gpcp`** 添加第二个 **String Value**（字符串）值，并输入 **`no`** 作为字符串的 **Value data**（值数据）：



将此字符串值添加到 GlobalProtect 设置后，Windows 登录屏幕上的用户将看到两个登录选项：本机 Windows 磁贴和第三方凭据提供程序磁贴。

STEP 5 | 为用户登录分配默认凭据提供程序。

1. 打开 Windows 注册表，并找到要分配为为默认凭据提供程序的第三方凭据提供程序的全局唯一标识符 (GUID)。
   1. 在命令提示符中，输入命令`regedit` 以打开 Windows 注册表编辑器。

© 2019 Palo Alto Networks, Inc.

2. 转到以下 Windows 注册表位置以查看当前安装的凭据提供程序列表：

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers`。
3. 复制凭据提供程序的完整 GUID 项（包括 GUID 两端的大括号 — { 和 }）。

2. 打开“本地组策略编辑器”以启用并分配默认凭证提供程序。
   1. 在命令提示符中，输入命令 `gpedit.msc` 以打开“本地组策略编辑器”。
   2. 选择 **Computer Configuration**（计算机配置）> **Administrative Templates**（管理模板）> **System**（系统）> **Logon**（登录）。
   3. 在 **Setting**（设置）下，双击 **Assign a default credential provider**（分配默认凭据提供程序）以打开分配默认凭据提供程序窗口。
   4. 将策略设置为 **Enabled**（已启用）。
   5. 在 **Assign the following credential provider as the default credential provider**（将以下凭据提供程序分配为默认凭据提供程序）下，输入凭据提供程序的 GUID（从 Windows 注册表复制）。
   6. 单击 **Apply**（应用），然后单击 **OK**（确定）保存更改。

STEP 6 | （可选）从 Windows 登录屏幕隐藏第三方凭据提供程序磁贴。

1. 打开 Windows 注册表，并找到要隐藏的第三方凭据提供程序的全局唯一标识符 (GUID)。
   1. 在命令提示符中，输入命令`regedit` 以打开 Windows 注册表编辑器。
   2. 转到以下 Windows 注册表位置以查看当前安装的凭据提供程序列表：

      `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers`。
   3. 复制要隐藏的凭据提供程序的完整 GUID 项（包括 GUID 两端的大括号 — { 和 }）。
2. 打开“本地组策略编辑器”以隐藏默认凭证提供程序。
   1. 在命令提示符中，输入命令 `gpedit.msc` 以打开“本地组策略编辑器”。
   2. 选择 **Computer Configuration**（计算机配置）> **Administrative Templates**（管理模板）> **System**（系统）> **Logon**（登录）。
   3. 在 **Setting**（设置）下，双击 **Exclude credential providers**（排除凭据提供程序）以打开 **Exclude credential providers**（排除凭据提供程序）窗口。
   4. 将策略设置为 **Enabled**（已启用）。
   5. 在 **Exclude the following credential providers**（排除以下凭据提供程序）下，输入要隐藏的凭据提供程序的 GUID（从 Windows 注册表复制）。

      要隐藏多个凭据提供程序，请使用逗号将每个 *GUID* 分隔开。
   6. 单击 **Apply**（应用），然后单击 **OK**（确定）保存更改。

STEP 7 | 完成您的更改。

完成更改后，重新启动系统以使更改生效。

使用 *Windows Installer* 启用第三方凭据的 *SSO* 包装

在 Windows Installer (Msiexec) 中使用以下选项在 Windows 7 端点上启用 SSO 包装第三方凭据提供程序。

- 包装第三方凭据，并在登录时向用户显示本机磁贴。用户可以单击磁贴，并使用自己的本机 Windows 凭据登录到端点。单点登录要求用户对 Windows、GlobalProtect 及其第三方凭据提供程序进行身份验证。

  在 Windows Installer (MSIEXEC) 中使用以下语法：

© 2019 Palo Alto Networks, Inc.

```
msiexec.exe /i GlobalProtect.msi WRAPCPGUID="{guid_value}" FILTERNONGPCP="yes"
```

在上面的语法中，**FILTERNONGPCP** 参数通过使用第三方凭据来筛选用于登录到系统的选项以简化对用户进行身份验证。

- 如果您希望用户选择使用第三方凭据进行登录，可以在 Windows Installer (Msiexec) 中使用以下语法：

```
msiexec.exe /i GlobalProtect.msi WRAPCPGUID="{guid_value}"
FILTERNONGPCP="no"
```

在上述语法中，**FILTERNONGPCP** 参数设为 "**no**"，筛选了第三方凭据提供程序的登录磁贴，以便只显示本机磁贴。在这种情况下，当用户登录到 Windows 端点时将同时显示本机 Windows 磁贴和第三方凭据提供程序磁贴。

将应用设置部署到 macOS 端点

使用 macOS 全局 plist（属性列表）文件设置 GlobalProtect 应用程序自定义设置或将脚本部署到 macOS 端点。

- 在 macOS Plist 中部署应用设置
- 使用 macOS Plist 部署脚本

在 *macOS Plist* 中部署应用设置

您可以在 macOS 全局 plist（属性列表）文件中设置 GlobalProtect 应用程序自定义设置。此举可在 macOS 端点首次连接至 GlobalProtect 门户前将 GlobalProtect 应用程序设置部署至 macOS 端点。

在 macOS 端点上，plist 文件位于 `/Library/Preferences` 或 `~/Library/Preferences` 中。波浪（~）符号表示位置位于当前用户的主文件夹中。macOS 端点上的 GlobalProtect 应用程序首先会检查 GlobalProtect plist 设置。如果该位置不存在 plist，则 GlobalProtect 应用程序会在 `~/Library/Preferences` 中搜索 plist 设置。

除了使用 *macOS plist* 部署 *GlobalProtect* 应用程序设置以外，您可以启用 *GlobalProtect* 应用程序从 *Windows* 端点收集特定的 *macOS plist* 信息。然后，您可以监控数据并将其添加到安全规则作为匹配条件。您可以根据安全规则强制执行与所定义的注册表设置相匹配的端点流量。此外，您还可设置自定义检查来从端点收集应用程序和流程数据。

STEP 1 | 打开 GlobalProtect plist 文件，找到 GlobalProtect 应用程序自定义设置。

使用 Xcode 或备选 plist 编辑器以打开 plist 文件：

`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`

然后转到：

`/Palo Alto Networks/GlobalProtect/Settings`

如果 `Settings` 词典不存在，创建一个。将每个注册表项作为字符串添加到 `Settings` 词典。

STEP 2 | 设置门户名称。

如果希望最终用户即便在首次连接时也无需手动输入门户地址，则可通过 plist 预部署门户地址。在 `PanSetup` 词典中，为 `Portal`配置一个项。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 将各种设置部署到 macOS 端点，包括 GlobalProtect 应用程序的连接方法。

查看自定义应用设置，获取您可以使用 macOS plist 进行配置的注册表项和值的完整列表。

使用 *macOS Plist* 部署脚本

当用户首次连接到 GlobalProtect 网关时，GlobalProtect 应用会下载配置文件，将应用设置保存在 GlobalProtect macOS 属性文件 (Plist) 中。除了更改应用设置以外，还可以使用 plist 为任何或所有以下事件部署脚本：建立隧道前后，和断开隧道连接前。从使用以下工作流开始，使用 plist 将脚本部署到 macOS 端点。

运行 *GlobalProtect* 应用 *2.3* 及更高版本的端点支持可用于部署脚本的 *macOS plist* 设置。

STEP 1 | （运行 Mac OS X 10.9 或更高版本的端点）清除设置缓存。这可以防止操作系统在 plist 发生变更后使用缓存的首选项。

要清除默认首选项缓存，从 macOS 终端运行 **`killall cfprefsd`** 命令。

STEP 2 | 打开 GlobalProtect plist 文件，找到或创建与连接或断开连接事件关联的 GlobalProtect 词典。您向哪个词典添加设置决定了 GlobalProtect 应用运行此脚本的时间。

使用 Xcode 或备选 plist 编辑器打开 plist 文件（ `/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist` ），转到以下其中一个词典的所在位置：

- `/PaloAlto Networks/GlobalProtect/Settings/pre-vpn-connect`
- `/Palo Alto Networks/GlobalProtect/Settings/post-vpn-connect`
- `/Palo Alto Networks/GlobalProtect/Settings/pre-vpn-disconnect`

如果 *`Settings`* 词典不存在，创建一个。然后，在 *`Settings`* 中，为您希望运行脚本的事件创建新词典。

STEP 3 | 创建名为 **`command`** 的新 **`String`**，让 GlobalProtect 应用运行脚本。

在此指定的值应引用您希望在自己的端点上运行的外壳脚本（和要传递给此脚本的参数）。

如果 `command` 字符串不存在，在词典中添加一个，在 **Value**（值）字段中指定脚本和参数。例如：

```
$HOME\pre_vpn_connect.sh
/Users/username username
```

支持环境变量。

最好在命令中指定完整路径。

STEP 4 | （可选）添加与此命令有关的其他设置，包括管理员权限、脚本超时值、批处理文件的校验和值和在命令执行失败时显示的错误消息。

在 plist 中创建或修改其他字符串（`context`（上下文）、`timeout`（超时）、`file`（文件）、`checksum`（校验和）和/或 `error-msg`（错误消息）），输入相应的值。更多信息，请参阅自定义应用设置。

STEP 5 | 将所做更改保存到 plist 文件。

© 2019 Palo Alto Networks, Inc.

保存 plist。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 无客户端 VPN

GlobalProtect 无客户端 VPN 提供对一般企业 Web 应用程序的远程访问。用户无需安装 GlobalProtect 软件，即可从启用 SSL 的 Web 浏览器进行安全访问。如果您需要合作伙伴或承包商能够访问应用程序，且安全启用非托管资产（包括个人端点），则这非常有用。您可以配置 GlobalProtect 门户登录页面，以便基于用户和用户组访问 Web 应用程序，并允许单点登录到启用 SAML 的应用程序。以下主题提供有关如何配置和解决无客户端 VPN 问题的信息。

> 无客户端 VPN 概述
> 支持的技术
> 配置无客户端 VPN
> 无客户端 VPN 故障排除

无客户端 VPN 概述

配置无客户端 VPN 时，远程用户可以使用 Web 浏览器登录 GlobalProtect 门户，并启动为用户发布的 Web 应用程序。根据用户或用户组，您可以允许用户访问您提供给他们的一组应用程序，或允许他们通过输入自定义应用程序 URL 来访问其他企业应用程序。

登录门户后，用户将看到一个已发布的应用程序页面，其中包含可以启动的 Web 应用程序列表。您可以使用 GlobalProtect 门户上的默认应用程序登录页面，或为您的企业创建自定义登录页面。

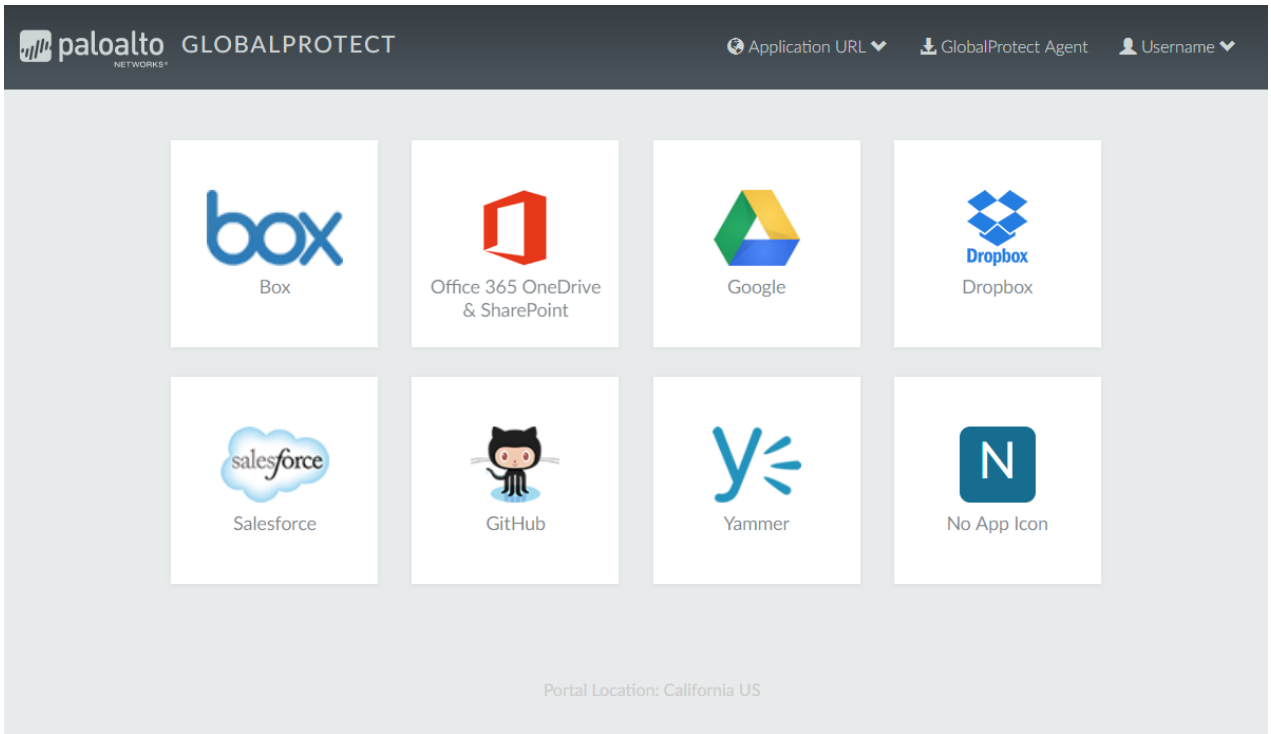


图 **3:** 无客户端 **VPN** 的应用程序登录页面

© 2019 Palo Alto Networks, Inc.

由于此页面替换了默认的门户网站登录页面，因此它包含指向 GlobalProtect 应用程序下载页面的链接。如果配置，用户也可以选择 **Application URL**（应用程序 **URL**）并输入 URL 以启动其他未发布的公司 Web 应用程序。

如果仅配置一个 Web 应用程序（并禁止访问未发布的应用程序），则不会将用户带到已发布的应用程序页面，只要用户登录，应用程序就会自动启动。如果不配置 GlobalProtect 无客户端 VPN，用户将在登录到门户时看到应用程序软件下载页面。

在配置 GlobalProtect 无客户端 VPN 时，需要安全策略来允许来自 GlobalProtect 端点的流量传递到与托管已发布应用程序登录页面和安全策略的 GlobalProtect 门户相关联的安全区域，以允许从 GlobalProtect 门户区域到基于用户的流量传递到已发布应用程序服务器所在的区域。您定义的安全策略控制哪些用户有权使用每个已发布的应用程序。

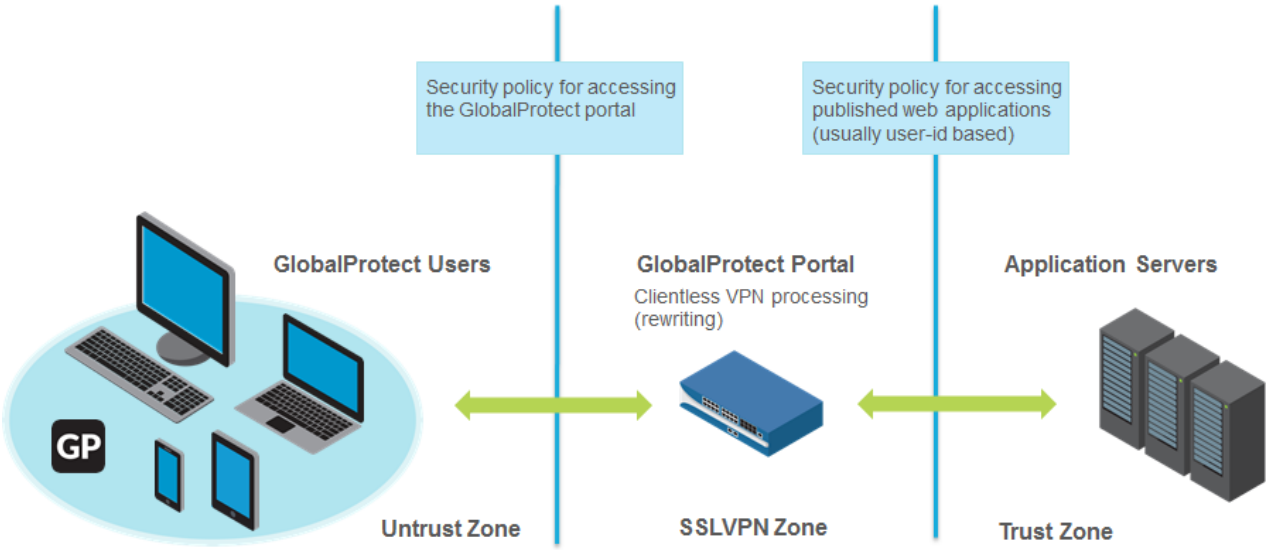


图 **4:** 无客户端 **VPN** 的区域和安全策略

© 2019 Palo Alto Networks, Inc.

支持的技术

现在，您可以配置 GlobalProtect 门户以提供对常见企业 Web 应用程序的远程安全访问权限。为了获得最佳效果，请确保在部署它们或将其提供给大量用户之前，在受控环境中全面测试您的无客户端 VPN 应用程序。

不支持下列 *Web* 应用程序技术：

- *SSH*、*FTP*、*SMTP*、 远程桌面协议 *(RDP)* 等非 *Web* 应用程序
- *HTTP 2.0*
- 非 *UTF-8* 编码
- *IPv6* 部署
- *HTTP* 中的多个事务，例如 *NT LAN* 管理器 *(NTLM)*身份验证
- *Javascript ES6*
- 无法重写的文件（*HTML*、*Javascript* 和 *CSS* 除外），包括 *Flash*、*Java Applet*、*Microsoft Silverlight*、*PDF*、*XML* 等
- 其他技术（例如 *Microsoft Sliverlight* 或 *XML/XSLT*）
- 任何内容编码（例如，`Accept-Encoding: gzip, defalte, br`）

技术	支持的版本

Web 应用程序技术	• HTML
	• HTML5
	• HTML5-Web-Sockets
	• Javascript ES5 或更低版本
	• RDP、VNC 或 SSH
	  • 虚拟桌面基础架构 (VDI) 和虚拟机 (VM) 环境，例如 Citrix XenApp 和 XenDesktop 或 VMWare Horizon 和 Vcenter，支持通过 HTML5 本地访问。可以通过无客户端 VPN 将 RDP、VNC 或 SSH 发送至这些机器，无需其他第三方中间件。
	  • 在不包含对 HTML5 本地支持或其他受无客户端 VPN 支持的网络应用该技术环境中，可以通过无客户端 VPN 将 HOBLink 或 Thinfinity 等第三方供应商用于 RDP。
	• Adobe Flash — 通过无客户端 VPN，浏览器可提供使用 Adobe Flash、Microsoft Word 文件或 Adobe PDF 的内容。但是，无客户端 VPN 将无法在 Adobe Flash、Microsoft Word 文件或 Adobe PDF 内重写 HTML URL 或链接，从而使内容正确渲染。

操作系统	• Windows • macOS • iOS • Android • Chrome • Linux
支持的浏览器	• Chrome • Edge • Internet Explorer • Safari

© 2019 Palo Alto Networks, Inc.

技术	支持的版本
	• Firefox

© 2019 Palo Alto Networks, Inc.

配置无客户端 VPN

要配置 GlobalProtect 无客户端 VPN：

STEP 1 | 准备工作：

- 在从 GlobalProtect 门户托管无客户端 VPN 的防火墙上安装 GlobalProtect 订阅。参考活动许可证和订阅。
- 安装最新 GlobalProtect 无客户端 VPN 动态更新（请参阅安装内容和软件更新），并为安装新动态内容更新设置时间表。作为最佳实践，建议 GlobalProtect 无客户端 VPN 始终安装最新内容更新。

GlobalProtect Clientless VPN **Last checked:** 2016/11/09 17:03:03 PST **Schedule:** Every hour (Download and Install)

58-11	panup-all-gp-58-11.candidate	GlobalProtectCli...	Full	75 KB	2016/11/07 18:57:21 PST	✔
58-10	panup-all-gp-58-10.candidate	GlobalProtectCli...	Full	74 KB	2016/10/25 17:51:17 PDT	✔ previously

- 最佳做法是为托管无客户端 VPN 的 GlobalProtect 门户配置单独的 FQDN。不要使用与 PAN-OS Web 界面相同的 FQDN。
- 在标准 SSL 端口（TCP 端口 443）上托管 GlobalProtect 门户。非标准端口不受支持。

STEP 2 | 使用 GlobalProtect 无客户端 VPN 配置可用的应用程序。GlobalProtect 门户在用户登录时看到的登录页面上显示这些应用程序（应用程序登录页面）。

1. 选择 **Network**（网络）> **GlobalProtect** > **Clientless Apps**（无客户端应用程序）并 **Add**（添加）一个或多个应用程序。对于每个应用程序，指定：
   - **Name**（名称）— 输入描述应用程序的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
   - **Location**（位置）（对于处于多虚拟系统模式下的防火墙）— 无客户端 VPN 应用程序可用的虚拟系统 (vsys)。对于不是处于多虚拟系统模式下的防火墙，**Location**（位置）字段不会出现。
   - **Application Home URL**（应用程序主页 **URL**）— 应用程序所在的 URL（最多 4095 个字符）。
   - **Application Description**（应用程序说明）（可选）— 应用程序的说明（最多 255 个字符）。
   - **Application Icon**（应用程序图标）（可选）— 标识已发布应用程序页面上的应用程序的图标。您可以浏览以上传图标。
2. 单击 **OK**（确定）。

STEP 3 | （可选）创建组来管理 Web 应用程序集。

如果您想要管理多个应用程序集合并提供基于用户组的访问，无客户端应用程序组十分有用。例如，G&A 团队的财务应用程序或工程团队的开发人员应用程序。

1. 选择 **Network**（网络）> **GlobalProtect** > **Clientless App Groups**（无客户端应用程序组）。**Add**（添加）一个新的无客户端 VPN 应用程序组并指定：
   - **Name**（名称）— 输入描述应用程序组的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
   - **Location**（位置）（对于处于多虚拟系统模式下的防火墙）— 无客户端 VPN 应用程序组可用的虚拟系统 (vsys)。对于不是处于多虚拟系统模式下的防火墙，**Location**（位置）字段不会出现。
2. 在 **Applications**（应用程序）区域，**Add**（添加）应用程序到组。您可以从现有无客户端 VPN 应用程序列表中选择或定义一个 **New Clientless App**（新无客户端应用程序）。
3. 单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

STEP 4 | 配置 GlobalProtect 门户以提供无客户端 VPN 服务。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户），然后选择现有门户配置或 **Add**（添加）新配置。参阅设置 GlobalProtect 门户访问权限。
2. 在 **Authentication**（身份验证）选项卡中，您可以：
   - （可选）专门为无客户端 VPN 创建新客户端身份验证。在这种情况下，选择 **Browser**（浏览器）作为 **Client Authentication**（客户端身份验证）的 **OS**。
   - 使用现有客户端身份验证。
3. 在 **Clientless**（无客户端）> **General**（常规）中，选择 **Clientless VPN**（无客户端 **VPN**）以启用门户服务并配置以下内容：
   - 为托管应用程序登录页面的 GlobalProtect 门户指定一个 **Hostname**（主机名）（IP 地址或 FQDN）。该主机名用于重写应用程序 URL。（有关 URL 重写的详细信息，请参阅步骤 8）。

     如果您使用网络地址转换 *(NAT)* 提供 *GlobalProtect* 门户的访问权限，则输入的 *IP* 地址或 *FQDN* 必须与 *GlobalProtect* 门户（公共 *IP* 地址）的 *NAT IP* 地址相匹配（或解析为 *NAT IP* 地址）。由于用户无法访问自定义端口上的 *GlobalProtect* 门户，因此 *NAT* 前端口也必须是 *TCP* 端口 *443*。

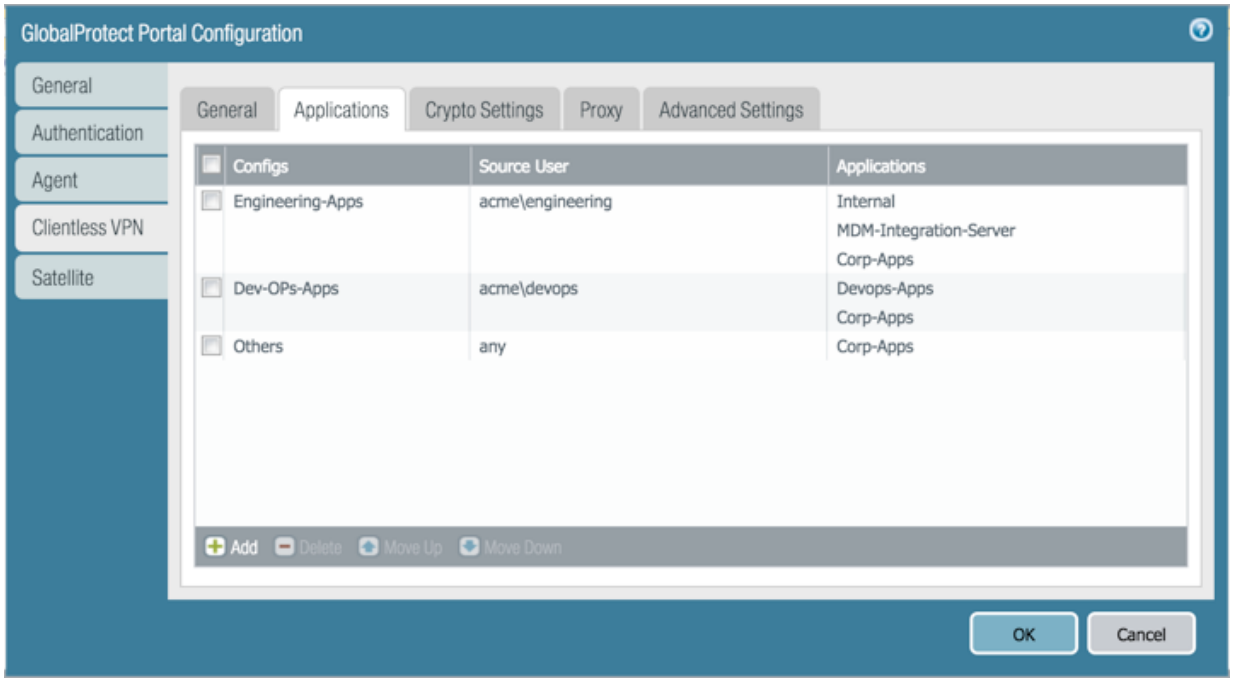
   - 指定一个 **Security Zone**（安全区）。此区域用作防火墙和应用程序之间通信的源区域。从此区域定义到应用程序区域的安全规则确定可以访问哪些应用程序。
   - 选择一个 **DNS Proxy**（**DNS** 代理）服务器或配置一个 **New DNS Proxy**（新 **DNS** 代理）。GlobalProtect 将使用此代理来解析应用程序名称。参考 DNS 代理对象。
   - **Login Lifetime**（登录生命周期）— 指定无客户端 VPN 会话最长有效期时长（小时数或分钟数）。通常的会话时间为 3 小时。小时范围是 1 至 24；分钟范围是 60 至 1440。在会话过期后，用户必须重新进行身份验证，并启动新的无客户端 VPN 会话。
   - **Inactivity Timeout**（不活动超时）— 指定无客户端 VPN 会话保持空闲的时长（小时数或分钟数）。通常不活动超时时间为 30 分钟。小时范围是 1-24；分钟范围是 5-1440。如果在指定的时间内用户没有执行任何操作，用户必须重新进行身份验证，并启动新的无客户端 VPN 会话。
   - **Max Users**（最大用户数）— 指定可以同时访问网关的最大用户数。如果没有指定值，则假定端点容量。如果端点容量未知，则假定容量为 50 个用户。如果达到最大用户数，其他无客户端 VPN 用户无法登录到门户。

STEP 5 | 将用户和用户组映射到应用程序。

此映射控制哪些应用程序用户或用户组可以从 GlobalProtect 无客户端 VPN 会话启动。

GlobalProtect 门户将使用指定的用户/用户组设置来确定将哪个配置传递给进行连接的 GlobalProtect 无客户端 VPN。如果您有多个配置，请确保它们已正确排序并映射到所有必需的应用程序，因为门户网站将从列表顶部开始查找配置匹配。只要门户网站找到匹配项，它就会将相关配置传送给 GlobalProtect 无客户端 VPN 用户。

© 2019 Palo Alto Networks, Inc.



将应用程序发布到用户/用户组或允许其启动未发布的应用程序并不意味着他们可以访问这些应用程序。您可以使用安全策略控制对应用程序（已发布或未发布）的访问。

必须配置组映射（*Device*（设备）> *User Identification*（用户标识）> *Group Mapping Settings*（组映射设置））之后才能选择组。

1. 在 **Applications**（应用程序）选项卡中，**Add**（添加）一个 **Applications to User Mapping**（应用程序到用户映射），以将用户与发布的应用程序进行匹配。
   - **Name**（名称）— 输入映射的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
   - **Display application URL address bar**（显示应用程序 **URL** 地址栏）— 选择此选项以显示应用程序 URL 地址栏，用户可以从中启动未在应用程序登录页面上发布的应用程序。启用后，用户可以选择 **Application URL**（应用程序 **URL**）
2. 指定 **Source Users**（源用户）。您可 **Add**（添加）要应用当前应用程序配置的独立用户或用户组。这些用户拥有使用 GlobalProtect 无客户端 VPN 启动配置的应用程序的权限。除用户和组之外，您还可指定何时将这些设置应用到用户或组：
   - **any**（任何）— 将应用程序配置应用到所有用户（无需 **Add**（添加）用户或用户组）。
   - **select**（选择）— 仅将应用程序配置应用到 **Add**（添加）到该列表的用户和用户组。
3. 将各个应用程序或应用程序组 **Add**（添加）到映射。配置中包含的 **Source Users**（源用户）可以使用 GlobalProtect 无客户端 VPN 以链接到添加的应用程序。

STEP 6 | 指定无客户端 VPN 会话的安全设置。

1. 在 **Crypto Settings**（加密设置）选项卡中，指定用于防火墙和发布的应用程序之间 SSL 会话的身份验证和加密算法。
   - **Protocol Versions**（协议版本）— 选择所需的最低和最高 TLS/SSL 版本。TLS 版本越高，连接越安全。选择包括 **SSLv3**、**TLSv1.0**、**TLSv1.1** 或 **TLSv1.2**。

© 2019 Palo Alto Networks, Inc.

无客户端 *VPN* 支持的 *TLS Max Version*（最高版本）为 *TLSv1.2*。无客户端 *VPN* 连接当前不支持 *TLSv1.3*。

- **Key Exchange Algorithms**（密钥交换算法）— 选择支持的密钥交换算法类型。选择包括：**RSA**，Diffie-Hellman (**DHE**) 或临时椭圆曲线 Diffie-Hellman (**ECDHE**)。
- **Encryption Algorithms**（加密算法）— 选择支持的加密算法。我们建议选择 **AES128** 或更高。
- **Authentication Algorithms**（身份验证算法）— 选择支持的身份验证算法。选择包括：**MD5**、**SHA1**、**SHA256**或**SHA384**。建议使用 **SHA256** 或更高版本。

2. 选择应用程序提供的服务器证书发生以下问题时要执行的操作：
   - **Block sessions with expired certificate**（阻止证书已过期的会话）— 如果服务器证书已过期，则阻止访问应用程序。
   - **Block sessions with untrusted issuers**（阻止颁发者不可信的会话）— 如果服务器证书是由不受信任的证书颁发机构颁发，则阻止访问应用程序。
   - **Block sessions with unknown certificate status**（阻止证书状态未知的会话）— 如果 OCSP 或 CRL 服务返回未知的证书吊销状态，则阻止访问应用程序。
   - **Block sessions on certificate status check timeout**（阻止证书状态检查超时的会话）— 如果证书状态检查在收到任何证书状态服务的响应之前超时，则阻止访问应用程序。

STEP 7 | （可选）指定一个或多个代理服务器配置来访问应用程序。

只支持对代理的基本身份验证（用户名和密码）。

如果用户需要通过代理服务器访问应用程序，请指定一个 **Proxy Server**（代理服务器）。您可以添加多个代理服务器配置，每组域配置一个。

- **Name**（名称）— 用来标识代理服务器的标签（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
- **Domains**（域）— 添加代理服务器提供的域。您可以在域名开头使用通配符 (*) 来表示多个域。
- **Use Proxy**（使用代理）— 选择以分配代理服务器来提供对域的访问。
- **Server**（服务器）— 指定代理服务器的 IP 地址或主机名。
- **Port**（端口）— 指定与代理服务器通信的端口。
- **User**（用户）和 **Password**（密码）— 指定登录到代理服务器所需要的 **User**（用户）和 **Password**（密码）凭据。再次指定密码以进行验证。

STEP 8 | （可选）为应用程序域指定任何特殊处理。

无客户端 VPN 充当反向代理，并修改发布的应用程序返回的 Web 页面。它会重写所有 URL，并向远程用户显示重写的页面，这样当访问这些 URL 时，请求将通过 GlobalProtect 门户。

在某些情况下，应用程序可能有不需要通过门户访问的页面（例如，应用程序可能包含 yahoo.finance.com 上的股票代码）。您可以排除这些页面。

在 **Advanced Settings**（高级设置）选项卡中，**Add**（添加）域名、主机名或 IP 地址到 **Rewrite Exclude Domain List**（重写排除域列表）。这些域将从重写规则中排除且无法重写。

主机和域名不支持路径。主机名和域名的通配符 (*) 只能出现在名称的开头（如 *.etrade.com）。

STEP 9 | 保存门户配置。

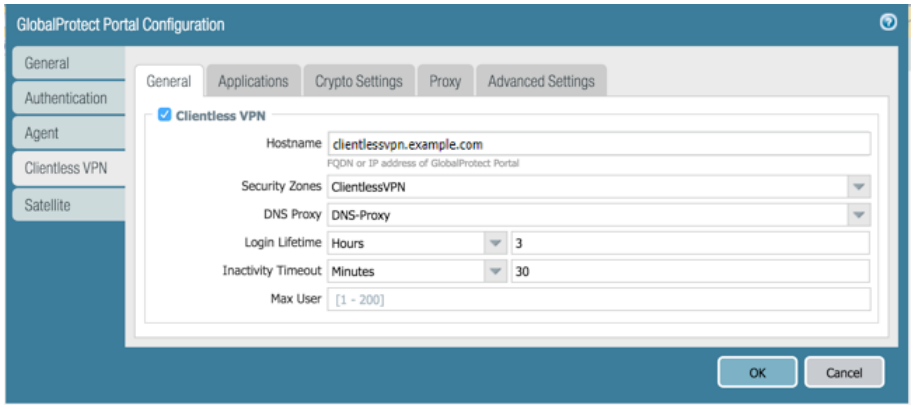
1. 双击 **OK**（确定）。
2. **Commit**（提交）更改。

STEP 10 | 配置一个安全策略规则，使用户能够访问已发布的应用程序。

您需要以下安全策略：

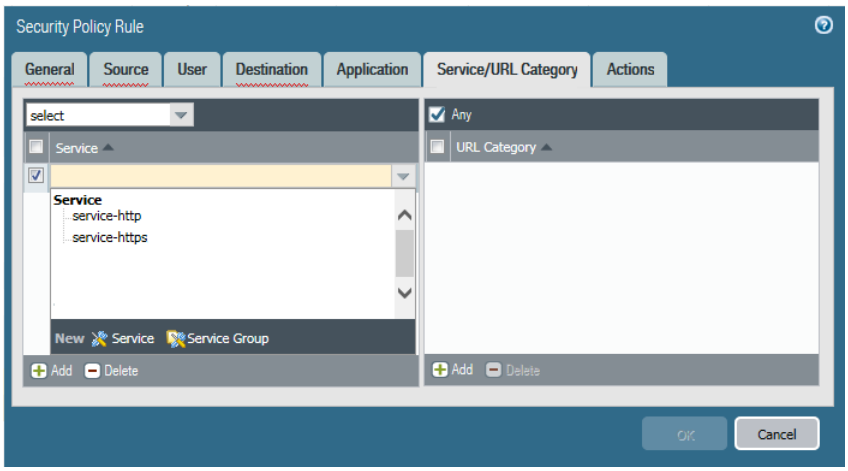
© 2019 Palo Alto Networks, Inc.

- 使托管无客户端 VPN 的 GlobalProtect 门户网站可从 Internet 访问。这是从 Untrust 或 Internet 区域到您托管无客户端 VPN 门户的区域的流量。
- 允许无客户端 VPN 用户访问 Internet。这是从无客户端 VPN 区域到 Untrust 或 Internet 区域的流量。



- 允许无客户端 VPN 用户访问企业资源。这是从无客户端 VPN 区域到信任或公司区域的流量。您定义的安全策略控制哪些用户有权使用每个已发布的应用程序。对于托管所发布应用程序服务器的安全区域，务必 **Enable User Identification**（启用用户识别）。

  默认情况下，**Security Policy Rule**（安全策略规则）中的 **Service/URL**（服务/**URL**）设置为 **application-default**（应用程序默认）。使用此默认设置，无客户端 VPN 将不适用于 HTTPS 站点。更改 **Service/URL**（服务/**URL**）以包括 **service-http** 和 **service-https** 两者。



- 配置代理服务器以访问无客户端 VPN 应用程序时，请确保在安全策略定义中包含代理 IP 地址和端口。当通过代理服务器访问应用程序时，仅应用为代理 IP 地址和端口定义的安全策略。

STEP 11 | （可选）要配置无客户端 VPN 门户登录页面以显示无客户端 VPN 用户连接的门户位置，请指定您配置了该门户的防火墙的物理位置。

当无客户端 VPN 用户体验到异常行为时，如网络性能差，他们可以向支持部门或服务台专业人员提供此位置信息，以协助进行故障排除。他们还可以使用此位置信息确定他们与门户的接近性。根据其接近性，他们可以评估是否需要切换至更近的门户。

如果您没有指定门户位置，无客户端 *VPN* 门户登录页面会显示空的位置字段。

- 在 **CLI** 中 — 使用以下 CLI 命令指定配置了门户的防火墙的物理位置：

© 2019 Palo Alto Networks, Inc.

```
<username@hostname> set deviceconfig setting global-protect
 location <location>
```

- 在 **XML API** 中 — 使用以下 XML API 指定配置了门户的防火墙的物理位置：
  - 设备 — 配置了门户的防火墙的名称
  - 位置 — 配置了门户的防火墙的位置

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```

无客户端 *VPN* 流量的源 *IP* 地址（通过应用程序查看）将可能是门户通过其访问应用的入口接口 *IP* 地址，也可能是源 *NAT* 正在使用时的转换 *IP* 地址。

© 2019 Palo Alto Networks, Inc.

无客户端 VPN 故障排除

由于此功能涉及 HTML 应用程序的动态重写，因此某些应用程序的 HTML 内容可能无法正确重写并中断应用程序。如果发生问题，请使用下表中的命令帮助您确定可能的原因：

表 **6:** 表：重写引擎统计信息

操作	命令
CLI 命令	
列出正在使用的无客户端 VPN 动态内容的版本 您也可以从 **Device**（设备）> **Dynamic Updates**（动态更新）> **GlobalProtect Clientless VPN**（**GlobalProtect** 无客户端 **VPN**）中查看动态更新版本。	**show system setting ssl-decrypt memory** proxy uses shared allocator SSL certificate cache: Current Entries: 1 Allocated 1, Freed 0 Current CRE (61-62) : 3456 KB (Actual 3343 KB) Last CRE (60-47) : 3328 KB (Actual 3283 KB) 在本例中，当前的动态更新是版本 61-62，最后一次安装的动态更新是版本 60-47。
列出无客户端 VPN 的活动（当前）用户	**show global-protect-portal current-user portal GPClientlessPortal filter-user all-users** GlobalProtect Portal : GPClientlessPortal Vsys-Id : 1 User : paloaltonetworks.com \johndoe Session-id : 1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0 Client-IP : 5.5.5.5 Inactivity Timeout : 1800 Seconds before inactivity timeout : 1750 Login Lifetime : 10800 Seconds before login lifetime : 10748 Total number of user sessions: 1
显示 DNS 解析结果 这对确定是否存在 DNS 问题很有用。如果出现 DNS 问题，您会注意到在 CLI 输出中无法解析的 FQDN。	**show system setting ssl-decrypt dns-cache** Total DNS cache entries: 89 Site IP Expire(secs) Interface bugzilla.panw.local 10.0.2.15 querying 0 www.google.com 216.58.216.4 Expired 0 stats.g.doubleclick.net 74.125.199.154 Expired 0
显示存储的所有无客户端 VPN 用户会话和 Cookie	**show**

© 2019 Palo Alto Networks, Inc.

操作	命令
	system setting ssl-decrypt gp-cookie-cache User: johndoe, Session-id: 1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0, Client-ip: 199.167.55.50
显示重写统计信息 这对识别无客户端 VPN 重写引擎的运行状况非常有用。 有关重写统计信息及其含义或目的的信息，请参阅无客户端 VPN 故障排除。	**show system setting ssl-decrypt rewrite-stats** Rewrite Statistics initiate_connection : 11938 setup_connection : 11909 session_notify_mismatch : 1 reuse_connection : 37 file_end : 4719 packet : 174257 packet_mismatch_session : 1 peer_queue_update_rcvd : 167305 peer_queue_update_sent : 167305 peer_queue_update_rcvd_failure: 66 setup_connection_r : 11910 packet_mismatch_session_r : 22 pkt_no_dest : 23 cookie_suspend : 2826 cookie_resume : 2826 decompress : 26 decompress_freed : 26 dns_resolve_timeout : 27 stop_openend_response : 43 received_fin_for_pending_req : 26 Destination Statistics To mp : 4015 To site : 12018 To dp : 17276 Return Codes Statistics ABORT : 18 RESET : 30 PROTOCOL_UNSUPPORTED : 7 DEST_UNKNOWN : 10 CODE_DONE : 52656 DATA_GONE : 120359 SWITCH_PARSER : 48 INSERT_PARSER : 591 SUSPEND : 2826 Total Rewrite Bytes : 611111955 Total Rewrite Useconds : 6902825 Total Rewrite Calls : 176545
调试命令	
在运行无客户端 VPN 门户的防火墙上启用调试日志	**debug dataplane packet-diag set log feature ssl all** **debug dataplane packet-diag set log feature misc all** **debug dataplane packet-diag set log feature proxy all** **debug dataplane packet-diag set log feature flow basic** **debug dataplane packet-diag set log on**

© 2019 Palo Alto Networks, Inc.

操作	命令
在运行无客户端 VPN 门户的防火墙上启用数据包捕获	**debug dataplane packet-diag set capture username *<portal-username>*** **debug dataplane packet-diag set capture stage clientless-vpn-client file *<clientless-vpn-client-file>*** **debug dataplane packet-diag set capture stage clientless-vpn-server file *<clientless-vpn-server-file>*** **debug dataplane packet-diag set capture stage firewall file *<firewall-file>*** **debug dataplane packet-diag set capture stage receive file *<receive-file>*** **debug dataplane packet-diag set capture stage transmit file *<transmit-file>*** **debug dataplane packet-diag set capture on** 当您执行数据包捕获命令时，在最终用户登录无客户端 *VPN* 门户后将显示一个同意页面，告知用户在其用户会话过程中捕获的数据包将包含未加密（明文）数据。如果用户同意数据包捕获会话，其后将前往应用程序登陆页面，并从该页面开始数据包捕获。如果用户不同意数据包捕获会话，其将从无客户端 *VPN* 门户注销，必须联系管理员才能继续常规用户会话（无数据包捕获）。 如果您为进行中的用户会话执行数据包捕获命令，则此类用户将自动从无客户端 *VPN* 门户注销，且必须再次登录以接收或拒绝数据包捕获会话。

显示数据包捕获文件	**debug dataplane packet-diag show setting**
	`----------`
	`Packet diagnosis setting:`
	`----------`
	`Packet filter`
	`Enabled: no`
	`Match pre-parsed packet: no`
	`----------`
	`Logging`
	`Enabled: no`
	`Log-throttle: no`
	`Sync-log-by-ticks: yes`
	`Features:`
	`Counters:`
	`----------`
	`Packet capture`
	`Enabled: yes`
	`Snaplen: 0`
	`Username: test1`
	`Stage clientless-vpn-client: file client.pcap`
	`  Captured: packets - 3558  bytes - 11366322`
	`  Maximum: packets - 0  bytes - 0`
	`Stage clientless-vpn-server: file server.pcap`
	`  Captured: packets - 1779  bytes - 5651923`
	`  Maximum: packets - 0  bytes - 0`
	`----------`

© 2019 Palo Alto Networks, Inc.

操作	命令
导出数据包捕获文件至安全复制 (SCP) 服务器	**scp export filter-pcap** + remote-port SSH port number on remote host + source-ip Set source address to specified interface address * from from * to Destination (username@host:path) **scp export filter-pcap from *<source-file>*** 至 <scp-server> 目标 (username@host:path)

表 **7:** 表：重写引擎统计信息

统计信息	说明
initiate_connection_failure	后端主机连接启动失败
setup_connection_failure	连接设置失败
setup_connection_duplicate	存在重复的对端会话
session_notify_mismatch	通常无效的会话
packet_mismatch_session	无法找到传入数据包的正确会话
peer_queue_update_rcvd_failure	对端收到分组更新时，会话无效
peer_queue_update_sent_failure	无法将数据包更新发送到对端或未能将数据包队列长度更新发送到对端
exceed_pkt_queue_limit	排队数据包太多
proxy_connection_failure	代理连接失败
setup_connection_r	将对端会话安装到应用程序服务器。该值应与 **initiate_connection** 和 **setup_connection** 的值匹配。
setup_connection_duplicate_r	代理中已有重复的会话
setup_connection_failure_r	无法建立对端会话
session_notify_mismatch_r	未找到对话会话
packet_mismatch_session_r	尝试获取数据包时未找到对端会话
exceed_pkt_queue_limit_r	滞留数据包太多
unknown_dest	无法找到目标主机
pkt_no_dest	没有此数据包的目的地

© 2019 Palo Alto Networks, Inc.

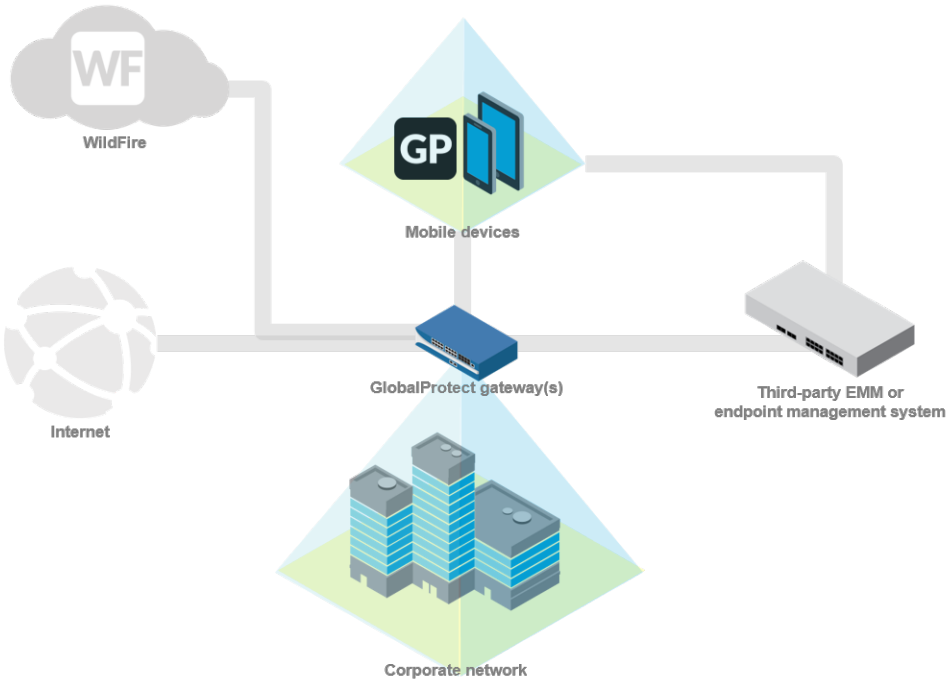
统计信息	说明
cookie_suspend	暂停会话以获取 Cookie
cookie_resume	从 MP 收到关于更新的 Cookie 的响应。该值通常与 cookie_suspend 的值匹配。
decompress_failure	无法解压缩
memory_alloc_failure	无法分配内存
wait_for_dns_resolve	暂停会话以解析 DNS 请求
dns_resolve_reschedule	由于无响应，已重新安排 DNS 查询（在超时之前重试）
dns_resolve_timeout	DNS 查询超时
setup_site_conn_failure	无法建立网站连接（代理、DNS）
site_dns_invalid	DNS 解析失败
multiple_multipart	已处理多部分内容类型
site_from_referer	已从引用站点收到后端主机。这可能表明从闪存重写链接失败或无客户端 VPN 未重写其他内容。
received_fin_for_pending_req	从服务器收到客户端的未决请求的 FIN
unmatched_http_state	意外的 HTTP 内容。这可能表明解析 http 标头或正文存在问题。

移动设备管理

> 移动设备管理概述
> 设置 MDM 与 GlobalProtect 的集成

移动设备管理概述

随着移动端点变得更加强大，最终用户越来越依赖于它们执行商业任务。但是，在没有防范威胁和安全漏洞的情况下，访问企业网络的端点同样可连接至互联网。



移动设备管理 (MDM) 系统或企业移动管理 (EMM) 系统使您可以自动将公司帐户配置和 VPN 设置部署至合规端点，从而简化了移动端点的管理。您还可使用移动设备管理系统与受影响端点交互来补救安全违规事件。这样可同时保护企业数据和个人最终用户数据。例如，如果最终用户丢失了端点，您可从移动设备管理系统远程锁定端点甚至擦除端点（完全或选择性擦除）。

移动设备管理系统除了可提供帐户 配置和远程设备管理功能之外，当与您的现有 GlobalProtect™ VPN 基础结构集成时，还可使您能够利用端点报告的主机信息通过 GlobalProtect 网关强制执行针对应用访问的安全策略。您还可使用内置于 Palo Alto 下一代防火墙中的监控工具来监控移动端点流量。

GlobalProtect 与 MDM 或 EMM 系统的集成

您可以通过下列方法之一，将您的 GlobalProtect 部署与 MDM 或 EMM 系统集成：

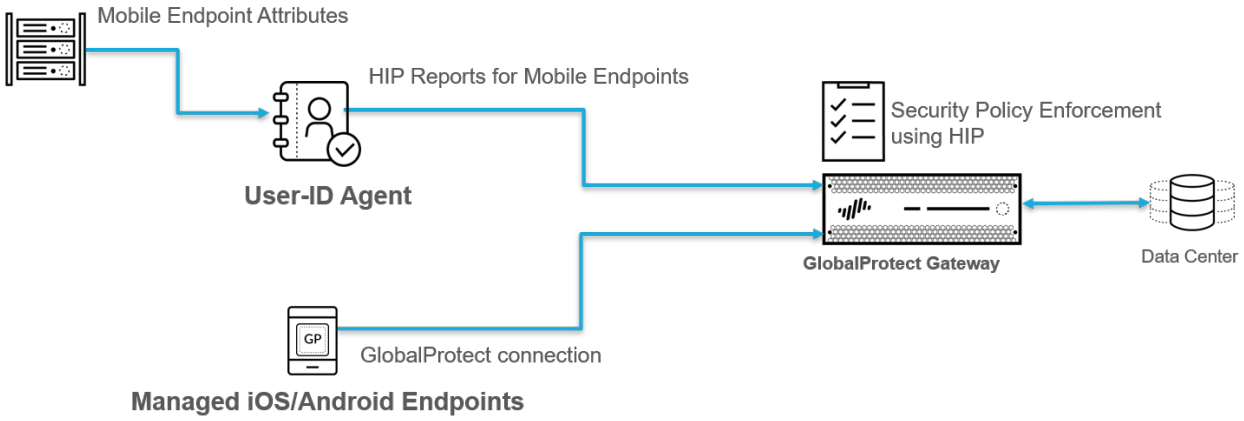
防火墙与 MDM 或 EMM 系统（仅限 AirWatch）的集成

您可以 配置 Windows User-ID 代理以便与 AirWatch MDM 服务器通讯，收集来自连接端点的主机信息。User-ID 代理将此主机信息发送至 GlobalProtect 网关，作为 HIP 报告的一部分用于基于 HIP 的策略实施。

PAN-OS 8.0 和更新版本支持防火墙集成。

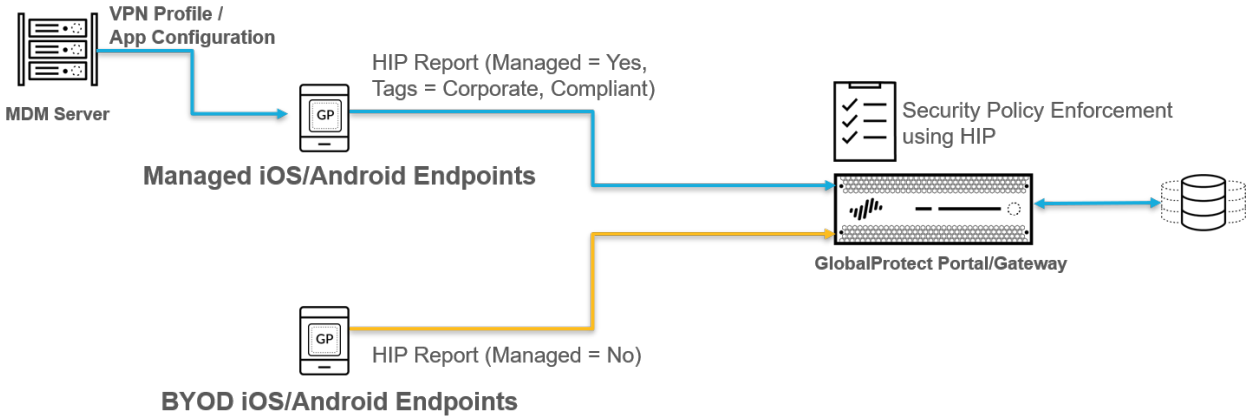
仅 *VMware AirWatch* 支持防火墙集成。

© 2019 Palo Alto Networks, Inc.



GlobalProtect 应用与 MDM 或 EMM 系统的集成

从 5.0 版本开始，iOS 和 Android 端点的 GlobalProtect 应用可从 MDM 系统获得供应商数据属性和标记。对于 iOS 端点，MDM 系统将这些属性作为 VPN 配置文件的一部分发送至 GlobalProtect 应用。对于 Android 端点，MDM 系统会将这些属性作为应用限制配置的一部分发送。GlobalProtect 应用之后可以将这些属性和标记发送至 GlobalProtect 网关，作为 HIP 报告的一部分用于基于 HIP 的策略实施。



GlobalProtect 应用集成符合 VMware AirWatch、MobileIron 和 Microsoft Intune 的要求。但是，任何支持 VPN 配置文件内供应商数据属性的 MDM 或 EMM 系统也支持此集成方法。

下表说明了支持的供应商数据属性：

© 2019 Palo Alto Networks, Inc.

MDM 属性	HIP 报告属性	HIP 报告类别	说明
mobile_id	主机 **ID**	通用	端点的唯一设备标识符 (UDID)。
受管	受管	通用	表示端点是否受管的值。如果此值为 **Yes**（是），则表示端点受管。如果此值为 **No**（否），则表示端点非受管。
合规性	标记	移动设备	合规状态表示端点是否符合您定义的 MDM 合规策略（例如，**Compliant**（符合））。此值附加于 HIP 报告中的 **Tag**（标记）属性。
所有权	标记	移动设备	端点的归属类别（例如，**Employee Owned**（归员工所有））。此值附加于 HIP 报告中的 **Tag**（标记）属性。
标签	标记	移动设备	依据其他基于 MDM 的属性进行匹配的标记。

© 2019 Palo Alto Networks, Inc.

设置 MDM 与 GlobalProtect 的集成

要设置 MDM 与 GlobalProtect 的集成，请使用以下工作流：

STEP 1 | 设置 GlobalProtect 基础结构

1. 为 GlobalProtect 创建接口和区域。
2. 在 GlobalProtect 组件间启用 SSL。
3. 设置 GlobalProtect 用户身份验证。请参阅关于 GlobalProtect 用户身份验证。
4. 启用组映射。
5. 配置 GlobalProtect 网关。
6. 为每个运行有支持在移动端点上使用 GlobalProtect 应用的网关的防火墙激活许可证。
7. 设置 GlobalProtect 门户访问权限。

STEP 2 | 设置移动设备管理系统，并决定是仅支持企业发放端点还是支持企业发放端点和个人端点。

请参阅有关移动设备管理 (MDM) 系统或企业移动性管理 (EMM) 系统的说明。

STEP 3 | 获取用于移动端点的 GlobalProtect 应用。

- 应用商店 — 下载和安装 GlobalProtect 移动应用
- 受支持的移动设备管理系统 — 部署 GlobalProtect 移动应用
- 其他第三方移动设备管理系统 — 请参阅供应商有关如何部署应用至受管端点的说明。

STEP 4 | 配置 MDM 集成。

使用以下方法之一配置 MDM 集成：

- 防火墙与 MDM 或 EMM 系统的集成：
  - 配置 Windows User-ID 代理以收集主机信息
- GlobalProtect 应用与 MDM 或 EMM 系统的集成：
  - 使用受支持的第三方 MDM 管理 GlobalProtect 应用
  - 使用其他第三方 MDM 管理 GlobalProtect 应用

STEP 5 | 使用主机信息配置指向移动端点的策略。

配置基于 HIP 的策略实施对于托管端点。

使用受支持的第三方 MDM 管理 GlobalProtect 应用

有关如何通过受支持的第三方 MDM 系统部署、配置和管理移动端点的 GlobalProtect 应用的信息， 请参阅以下部分：

- 合格的 MDM 供应商
- 部署 GlobalProtect 移动应用
- 始终打开 VPN 配置
- 用户发起远程访问 VPN 配置
- 每应用 VPN 配置
- 启用 App Scan 与 WildFire 集成
- 在用于 macOS 端点的 GlobalProtect 应用程序中抑制通知

如果未使用受支持的第三方 MDM 系统，则可以使用其他第三方 MDM 管理 GlobalProtect 应用。

© 2019 Palo Alto Networks, Inc.

合格的 *MDM* 供应商

下表列出了您可用于通过 OS 对 GlobalProtect 进行配置、部署和管理的受支持的 MDM 供应商。A — 表示不支持 OS。

如果您想要使用不合格的 MDM 供应商，使用其他第三方 MDM 管理 GlobalProtect 应用

受支持的 MDM 供应商	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
AirWatch	✓（仅限每应用 VPN）	✓	—	—	✓	—	—
Microsoft Intune	✓（仅限始终打开、远程访问和每应用 VPN）	✓	—	—	✓（仅限始终打开 VPN 和每应用 VPN）	—	—
MobileIron	✓（仅限始终打开 VPN）	✓	—	—	—	—	—
Google 管理控制台	✓（对于 Chromebook 上的 Android 应用支持；仅限应用部署）	—	✓（仅限应用部署）	—	—	—	—

您仅可使用 *Google* 管理控制台部署 *GlobalProtect* 应用；而不能使用 *Google* 管理控制台配置 *VPN* 配置。使用 *Google* 管理控制台部署应用前，必须通过 GlobalProtect 门户配置 *VPN* 配置。

部署 *GlobalProtect* 移动应用

GlobalProtect 应用提供了将企业安全策略扩展至移动端点的简易方法。针对运行 GlobalProtect 应用的其他远程端点，该移动应用可实现通过 IPsec 或 SSL VPN 隧道安全访问公司网络。该应用将连接至距离最终用户当前所在位置最近的网关。此外，进出移动端点的流量也将自动受到应用于公司网络上其他端点的相同安全策略执行的控制。该应用将采集主机配置的相关信息，并将此信息用于实现基于 HIP 的增强安全策略执行。

© 2019 Palo Alto Networks, Inc.

安装 GlobalProtect 应用的方法主要有两种：可直接从端点应用商店购买安装应用（请参阅下载和安装 GlobalProtect 移动应用）；或者，从移动设备管理系统（例如 AirWatch）部署应用，并以透明方式将应用推送至受管端点。

- 使用 AirWatch 部署 GlobalProtect 移动应用
- 使用 AirWatch 在受管 Chromebook 上为 Android 部署 GlobalProtect 应用
- 使用 Microsoft Intune 部署 GlobalProtect 移动应用
- 使用 MobileIron 部署 GlobalProtect 移动应用
- 使用 Google 管理控制台在受管 Chromebook 上为 Android 部署 GlobalProtect 应用

使用 **AirWatch** 部署 **GlobalProtect** 移动应用

可将 GlobalProtect 应用部署至已在 AirWatch 注册的受管端点。运行 iOS 或 Android 的端点必须下载 AirWatch 代理以注册 AirWatch MDM。Windows 10 端点无需 AirWatch 代理，但要求配置端点注册。在部署应用后，配置并部署 VPN 配置文件，以便自动为最终用户设置 GlobalProtect 应用。

如果您想在受管 *Chromebook* 上运行 *Android* 版 *GlobalProtect*，可以 使用 AirWatch 在受管 Chromebook 上为 Android 部署 GlobalProtect 应用。

STEP 1 | 在开始之前，请确保要在其上部署 GlobalProtect 应用的端点已注册 AirWatch：

- **Android** 和 **iOS** — 下载 AirWatch 代理并根据提示注册。
- **Windows Phone** 和 **Windows 10 UWP** — 配置 Windows 10 UWP 端点以注册 AirWatch（从端点上选择 **Settings**（设置）> **Accounts**（帐户）> **Work access**（工作访问）> **Connect**（连接））。

STEP 2 | 从 AirWatch 中选择 **APPS & BOOKS**（应用和书籍）> **Public**（公共）> **Add Application**（添加应用程序）。

STEP 3 | 选择哪个组织组来管理此应用。

STEP 4 | 选择 **Platform**（平台）（**Apple iOS**、 **Android** 或 **Windows Phone**）。

STEP 5 | 在端点应用商店中搜索 GlobalProtect 应用或输入 GlobalProtect 应用页面其中一个 URL：

- **Apple iOS**—https://itunes.apple.com/us/app/globalprotect/id592489989?mt=8&uo=4
- **Android**—https://play.google.com/store/apps/details?id=com.paloaltonetworks.globalprotect
- **Windows Phone**—https://www.microsoft.com/en-us/p/globalprotect/9nblggh6bzl3

STEP 6 | 单击 **Next**（下一步）。如果从端点应用商店中搜索应用，还必须从搜索结果列表中 **Select**（选择）应用。

如果已搜索 *GlobalProtect* 安卓应用但在列表中未找到该应用，请联系您的 *Android for Work* 管理员以将 *GlobalProtect* 添加至获批公司应用列表中，或使用 *Google Play Store* 中的应用 *URL*。

STEP 7 | 在 **Assignment**（分配）选项卡上，选择将具有此应用访问权限的 **Assigned Smart Groups**（分配智能组）。

STEP 8 | 选择 **App Delivery Method**（应用交付方法）为 **Auto**（自动）（自动将应用推送至设备）或 **On Demand**（按需）。

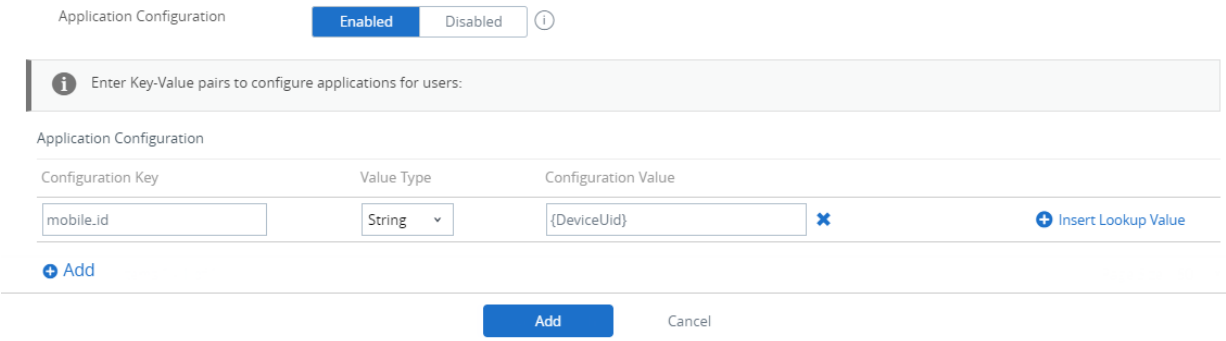
STEP 9 | （仅限 GlobalProtect 安卓应用）**Enable**（启用）应用程序配置），以使用 UDID 标识端点。

添加以下注册表项值对：

- 配置表项 — `mobile_id`

© 2019 Palo Alto Networks, Inc.

- 值类型 — **String**
- 配置值 — **{DeviceUid}**



STEP 10 | 选择 **Save & Publish**（保存并发布），将“应用目录”推送至在 **Assignment**（分配）部分分配的智能组中的端点。

使用 **AirWatch** 在受管 **Chromebook** 上为 **Android** 部署 **GlobalProtect** 应用

从 5.0 版本的 GlobalProtect 应用开始，可将 Android 版 GlobalProtect 应用部署至已在 AirWatch 注册的受管 Chromebook。在部署应用后，配置并部署 VPN 配置文件，以便自动为最终用户设置 GlobalProtect 应用。

Android 版 GlobalProtect 应用仅支持在某些 Chromebook 上使用。不支持 Android 应用程序的 Chromebook 必须继续运行用于 Chrome 的 GlobalProtect 应用程序，从 GlobalProtect app 5.0 及更高版本开始不受支持。

不得在相同的 Chromebook 上部署 Android 版 GlobalProtect 应用和 Chrome 版 GlobalProtect 应用。

使用以下步骤，通过 AirWatch 在受管 Chromebook 上部署 Android 版 GlobalProtect 应用：

STEP 1 | 设置 Google 管理控制台。

Google 管理控制台让您可以为公司内的用户管理 Google 服务。AirWatch 使用 Google 管理控制台与 Chromebook 集成。

1. 以管理员身份登录到 Google 管理控制台。
2. 从控制台，选择 **Security**（安全）> **Advanced Settings**（高级设置）> **Manage API client access**（管理 **API** 客户端访问）。
3. 在 **Client Name**（客户端名称）字段中，输入 AirWatch 提供的客户端 ID。
4. 在 **One or More API Scopes**（一个或多个 **API** 范围）字段中，输入以下您想要控制应用程序访问的 Google API 范围：

© 2019 Palo Alto Networks, Inc.

每个 *API* 范围必须用逗号隔开。

- https://www.googleapis.com/auth/chromedevicemanagementapi
- https://www.googleapis.com/auth/admin.directory.user
- https://www.googleapis.com/auth/admin.directory.device.chromeos

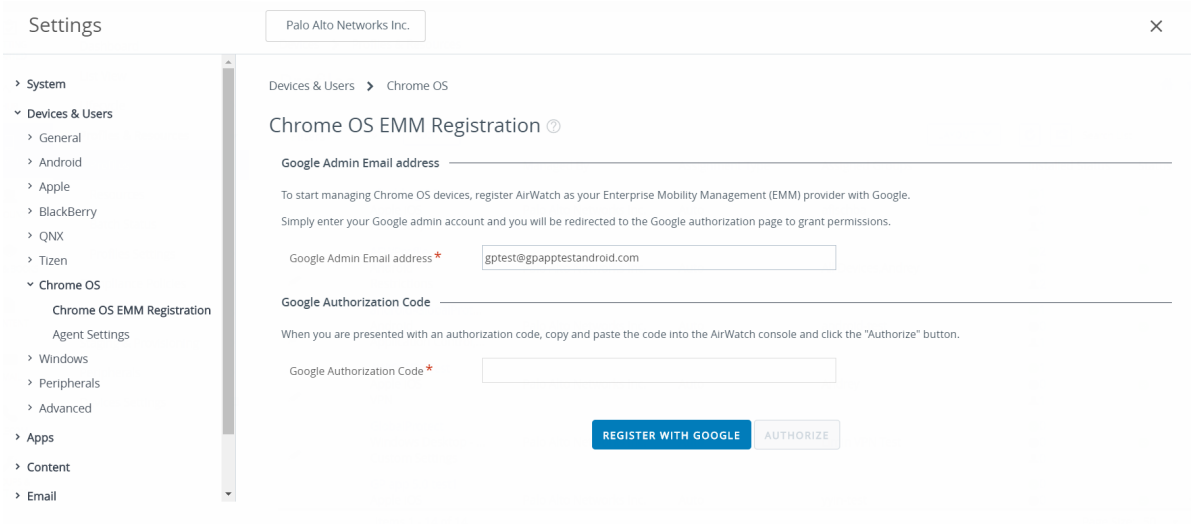
5. 点击 **Authorize**（授权）。
6. 为设备策略（**Device Management**（设备管理）> **Device Settings**（设备设置）> **Chrome Management**（**Chrome** 管理）> **Device Settings**（设备设置））和用户策略（**Device Management**（设备管理）> **Device Settings**（设备设置）> **Chrome Management**（**Chrome** 管理）> **User Settings**（用户设置））启用 **Chrome Management - Partner Access**（**Chrome** 管理 - 合作伙伴访问）。

STEP 2 | 注册 AirWatch 作为您的 Google 企业移动管理 (EMM) 供应商。

要通过 AirWatch 管理 Chromebook，您必须通过 Google 管理控制台注册 AirWatch。

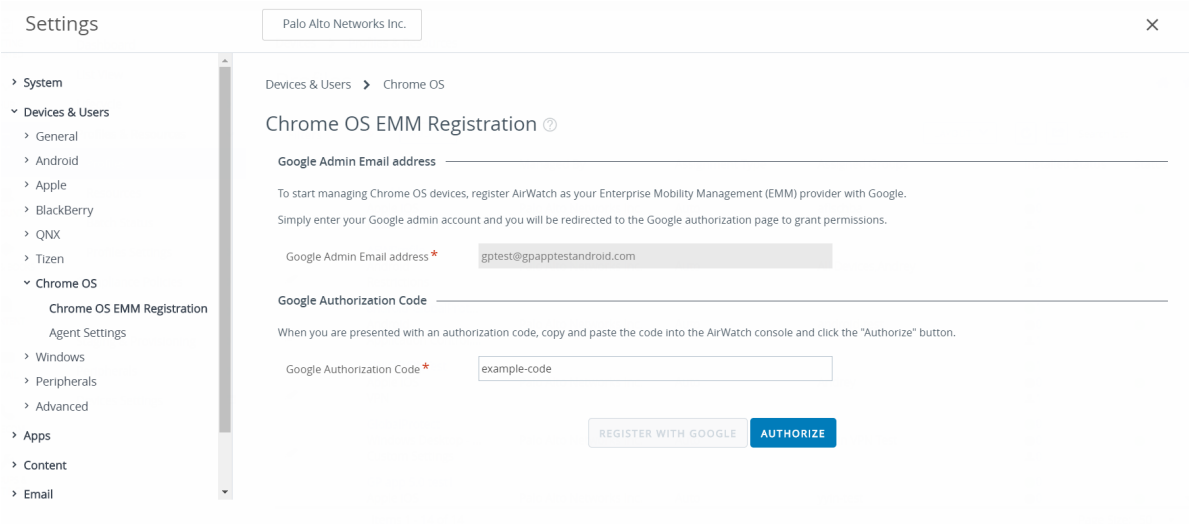
1. 登录到您的 AirWatch 控制台。
2. 选择 **Devices**（设备）> **Devices Settings**（设备设置）> **Devices & Users**（设备和用户）> **Chrome OS** > **Chrome OS EMM Registration**（**Chrome OS EMM** 注册）。
3. 输入您用于访问 Google 管理控制台的 **Google Admin Email address**（**Google** 管理电子邮件地址）。
4. 点击 **REGISTER WITH GOOGLE**（通过 **GOOGLE** 注册）。您将被重定向至 Google 授权页可以获得 Google 授权码。

© 2019 Palo Alto Networks, Inc.



5. 输入您从 Google 授权页面获得的 **Google Authorization Code**（**Google** 授权码）。
6. 单击 **AUTHORIZE**（授权）以完成注册。

© 2019 Palo Alto Networks, Inc.



STEP 3 | 通过 AirWatch 注册 Chromebook。

使用 AirWatch 开始管理 Chromebook 之前，您必须注册并同步 Chromebook 至 AirWatch。

1. 在 Chromebook 上，按 **CTRL+ALT+E** 打开企业注册屏幕。

© 2019 Palo Alto Networks, Inc.

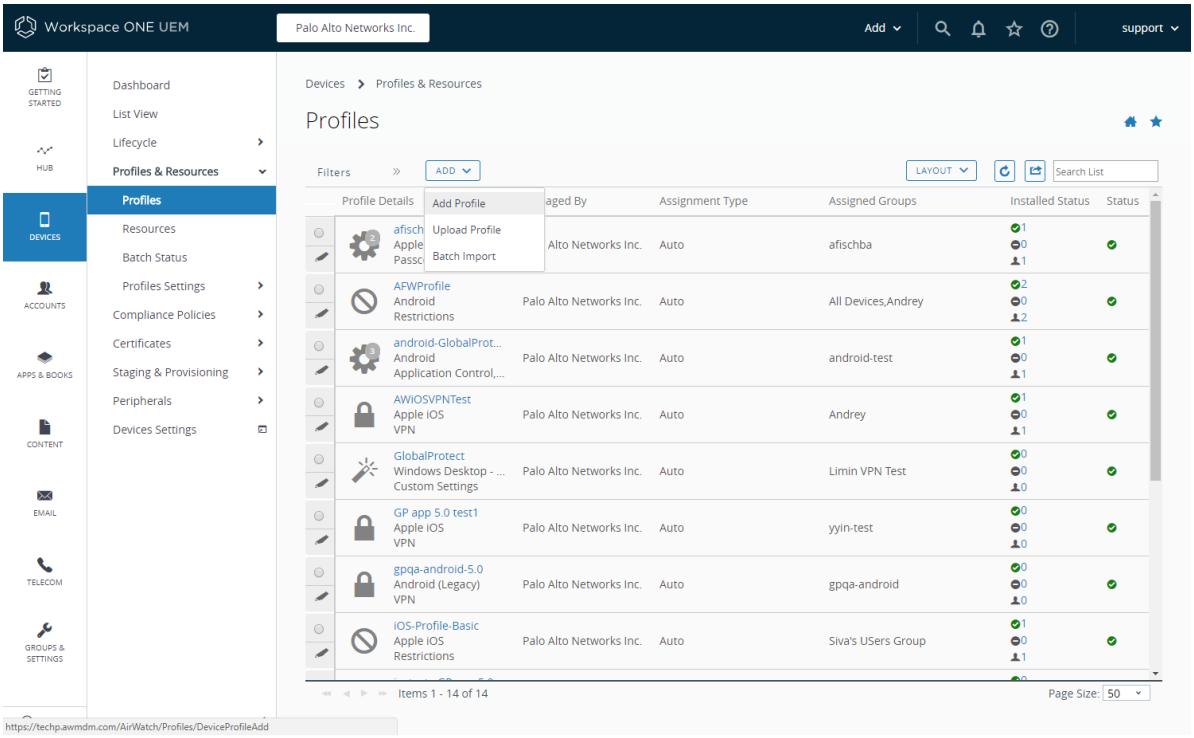
2. 输入您的 Google 管理欢迎信中用户名和密码，或输入您已有的 G Suite 用户凭据。
3. 单击 **Enroll Device**（注册设备）。Chromebook 注册成功后，您将收到确认消息。
4. 登录到您的 AirWatch 控制台。
5. 选择 **Devices**（设备）> **Devices Settings & Users**（设备设置和用户）> **Chrome OS** > 。
6. 单击 **Device Sync**（设备同步）以同步所有已注册的 Chromebook 至 AirWatch。

STEP 4 | 添加 Android 版 GlobalProtect 应用至 AirWatch 上的 Chrome OS 配置文件。

Application Control（应用程序控制）配置文件让您可以从 Google Play 和 Chrome Web Store 添加应用。

1. 登录到您的 AirWatch 控制台。
2. 选择 **Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件）以 **ADD**（添加）新 Chrome OS 配置文件。

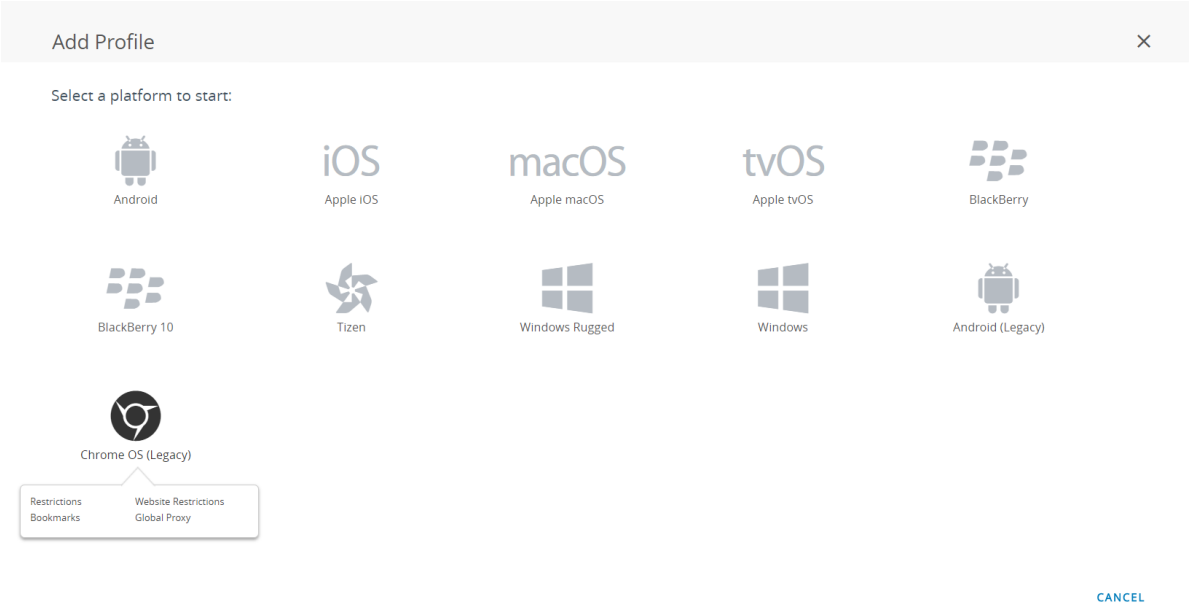
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

3. 从平台列表中选择 **Chrome OS (Legacy)**（**Chrome OS**（旧版））。

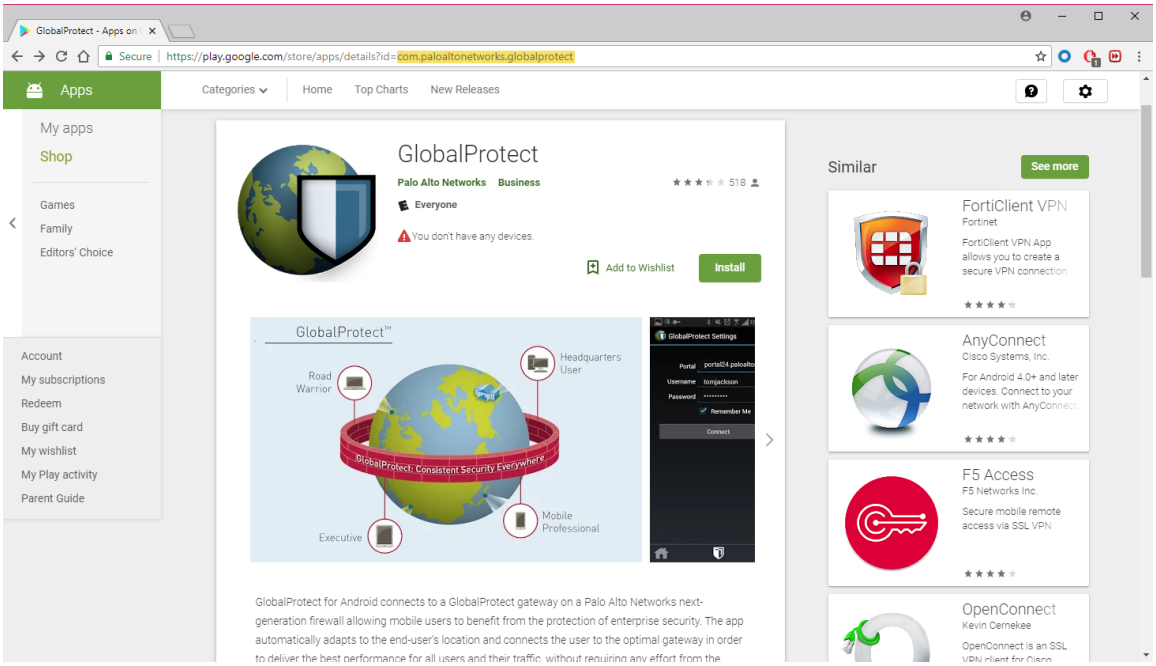
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

4. 配置**General**（常规）设置：
5. 配置 **Application Control**（应用程序控制）设置。
   1. 输入 Google Play URL 内显示的 GlobalProtect **App ID**（应用 **ID**）(com.paloaltonetworks.globalprotect)。

© 2019 Palo Alto Networks, Inc.



2. 输入应用 **Name**（名称）。

© 2019 Palo Alto Networks, Inc.

3. 指定您是否要 **Pin App to Shelf**（将应用锁定至存储架）。输入 **Y** 以将应用锁定至 Chromebook 应用存储架。
4. **SAVE & PUBLISH**（保存并发布）更改。

使用 **Microsoft Intune** 部署 **GlobalProtect** 移动应用

可以将 GlobalProtect 应用部署至已在 Microsoft Intune 注册的受管端点，或是其端点未在 Microsoft Intune（仅限 iOS）注册的用户。在部署应用后，配置并部署 VPN 配置文件至受管端点，以便自动为最终用户设置 GlobalProtect 应用。

STEP 1 | 通过 Microsoft Intune 注册端点。

要将 GlobalProtect 应用部署至您的端点，这些端点必须在 Microsoft Intune 中注册。

STEP 2 | 添加 GlobalProtect 应用到 Microsoft Intune。

在将 GlobalProtect 应用分配给任何用户或端点前，必须将此应用添加至 Microsoft Intune。

STEP 3 | 设置 GlobalProtect 应用的应用分配类型。

将 GlobalProtect 应用分配给用户或端点后，就可以确定谁拥有此应用的访问权限。分配应用之前，必须为此应用设置分配类型。分配类型可使此应用在必要时可用，也可以用于卸载应用。

STEP 4 | 分配 GlobalProtect 应用到特定用户或端点。

GlobalProtect 应用分配类型设置成功后，可以将此应用分配给特定用户或端点。

（仅限 *iOS*）可将 *GlobalProtect* 应用分配给其端点未在 *Microsoft Intune* 注册的用户。

使用 **MobileIron** 部署 **GlobalProtect** 移动应用

可将 GlobalProtect 应用部署至已在 MobileIron 注册的受管端点。在部署应用后，配置并部署 VPN 配置文件，以便自动为最终用户设置 GlobalProtect 应用。

STEP 1 | 添加用户至 MobileIron。

用户在 MobileIron 注册其端点之前，必须为每位用户创建一个用户表项。

STEP 2 | （可选）分配用户至用户组。

要基于组成员（而非独立用户）部署 GlobalProtect 应用，可以将用户分配给不同的用户组。

STEP 3 | 邀请用户在 MobileIron 注册其端点。

将用户添加至 MobileIron 后，可以邀请他们注册其端点。

STEP 4 | 添加 GlobalProtect 应用至 MobileIron 应用目录。

应用目录列出了可供用户使用的移动应用。既可以从 Apple App Store 等公共商店搜索并添加 GlobalProtect 应用，也可以将此应用作为内部应用直接上传至 MobileIron。然后，必须配置应用分发设置，指明 GlobalProtect 应用如何在注册端点上进行安装和配置。

使用 **Google** 管理控制台在受管 **Chromebook** 上为 **Android** 部署 **GlobalProtect** 应用

Google 管理控制台使您能够从基于 Web 的中央位置管理 Chromebook 设置和应用。可将 Android 版 GlobalProtect 应用程序部署至受管 Chromebook，并从控制台配置相关 VPN 设置。

要为用户自动设置应用程序，您可以选择使用 Google Chromebook 管理控制台来配置和部署受管 Chrome OS 设备的设置。您可以使用 Google 管理控制台来管理 Chromebook 的设置和应用程序。

© 2019 Palo Alto Networks, Inc.

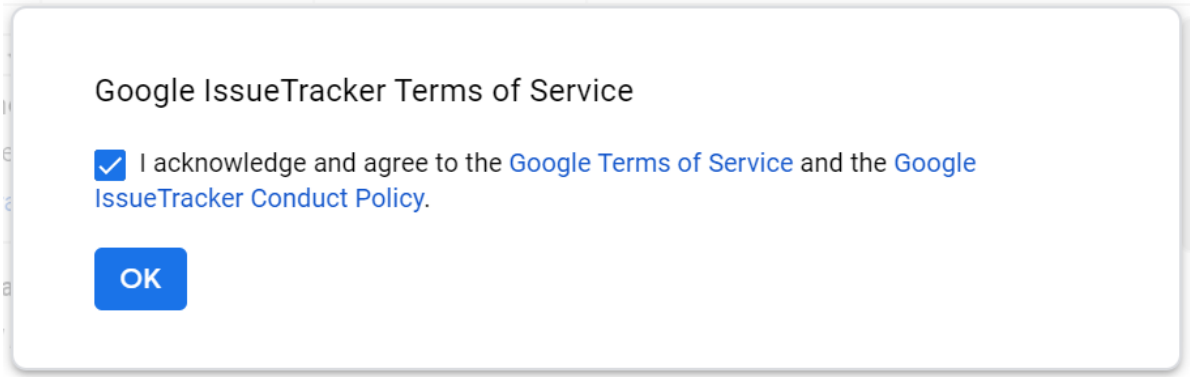
按照以下建议在受管 *Chromebook* 上部署 *Android* 版 *GlobalProtect* 应用程序：

- 不能使用 *Google* 管理控制台将用于身份验证的唯一证书推送到设备。
- 在 *Chromebook* 中，按 *CTRL+ALT+T* 打开终端命令行。使用 `route`（路由）命令显示设备上安装的路由。您可以决定是否包括用于拆分隧道的访问路由。
- 因为应用程序通常使用不同的文件格式，所以可以使用 *OpenSSL* 将证书从 *PKCS #12* 格式转换为 *Base64* 格式。使用 `openssl base64 -A -in` *<certificate-in-p12-format>* `-out` *<cert.txt>* 命令。

使用以下步骤，通过 Google 管理控制台在受管 Chromebooks 上部署 Android 版 GlobalProtect 应用：

STEP 1 | 准备工作：

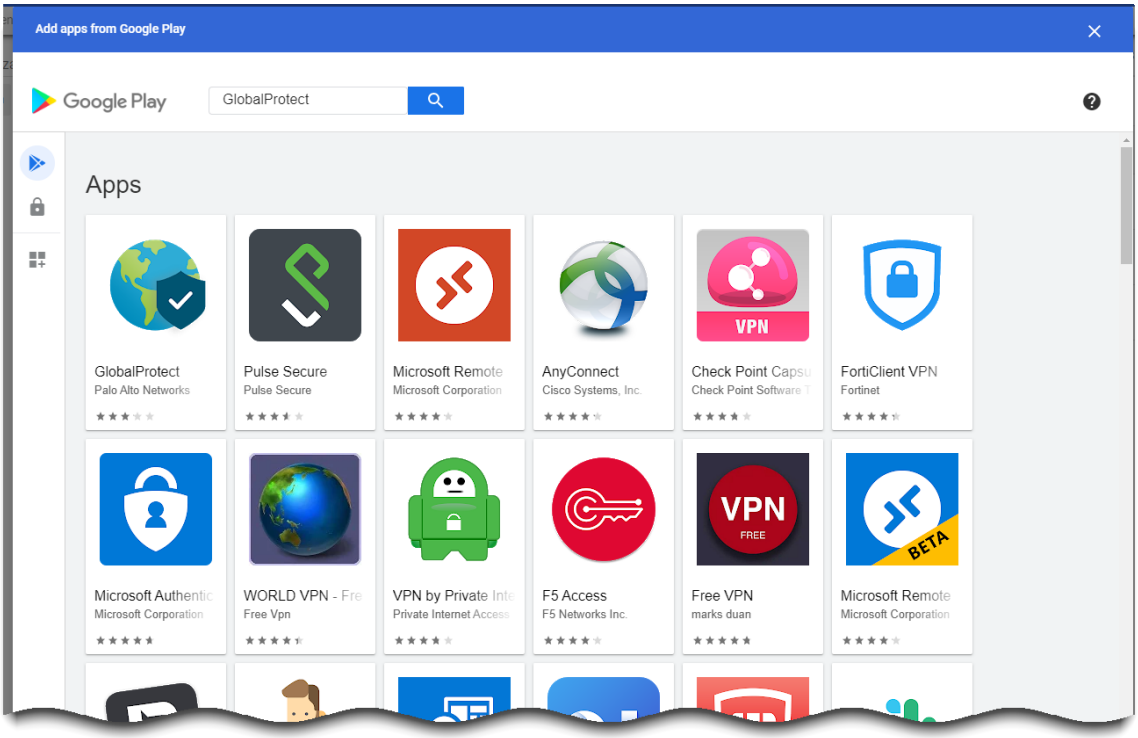
- 配置 GlobalProtect 网关以支持受管 Chromebook 上的 Android 版 GlobalProtect 应用程序。请参阅配置 GlobalProtect 网关。
- 在受管 Chromebook 上配置门户并自定义 Android 版 GlobalProtect 应用程序。您必须配置 GlobalProtect 应用程序可连接的一个或多个网关。请参阅设置 GlobalProtect 门户访问权限。请参阅 Palo Alto Networks 兼容性矩阵，了解 Chrome OS 上 Android 支持的功能列表。
- （推荐）在 Chromebook 上为 Android 版 GlobalProtect 应用程序启用 SAML SSO，以实现无缝身份验证。我们建议您设置 SAML SSO，以允许用户在登录 Chromebook 后自动连接，而无需在 GlobalProtect 应用程序中重新输入凭据。这确保用户可以访问持续安全性。请参阅设置 SAML 身份验证。
- 当用户在受管 Chromebook上首次连接到 Android 版 GlobalProtect 时，必须在设置隧道之前确认以下抑制 VPN 通知消息：



STEP 2 | 为 Chromebook 用户核准 GlobalProtect 应用。

1. 以管理员身份登录到 Google 管理控制台。
2. 从管理控制台选择 **Device**（设备）> **Chrome management**（**Chrome** 管理）以查看和修改 Chrome 管理设置。
3. 选择 **Apps & extensions**（应用程序和扩展）。
4. 在 Apps and extensions（应用程序和扩展）区域，点击 **application settings page**（应用程序设置页面）链接。
5. 单击添加（+）按钮以将 GlobalProtect 从 Google Play 商店添加至经批准的 Android 应用程序列表。
6. 当 Google Play 商店启动时，搜索 **`GlobalProtect`**，然后单击 GlobalProtect 应用程序图标。

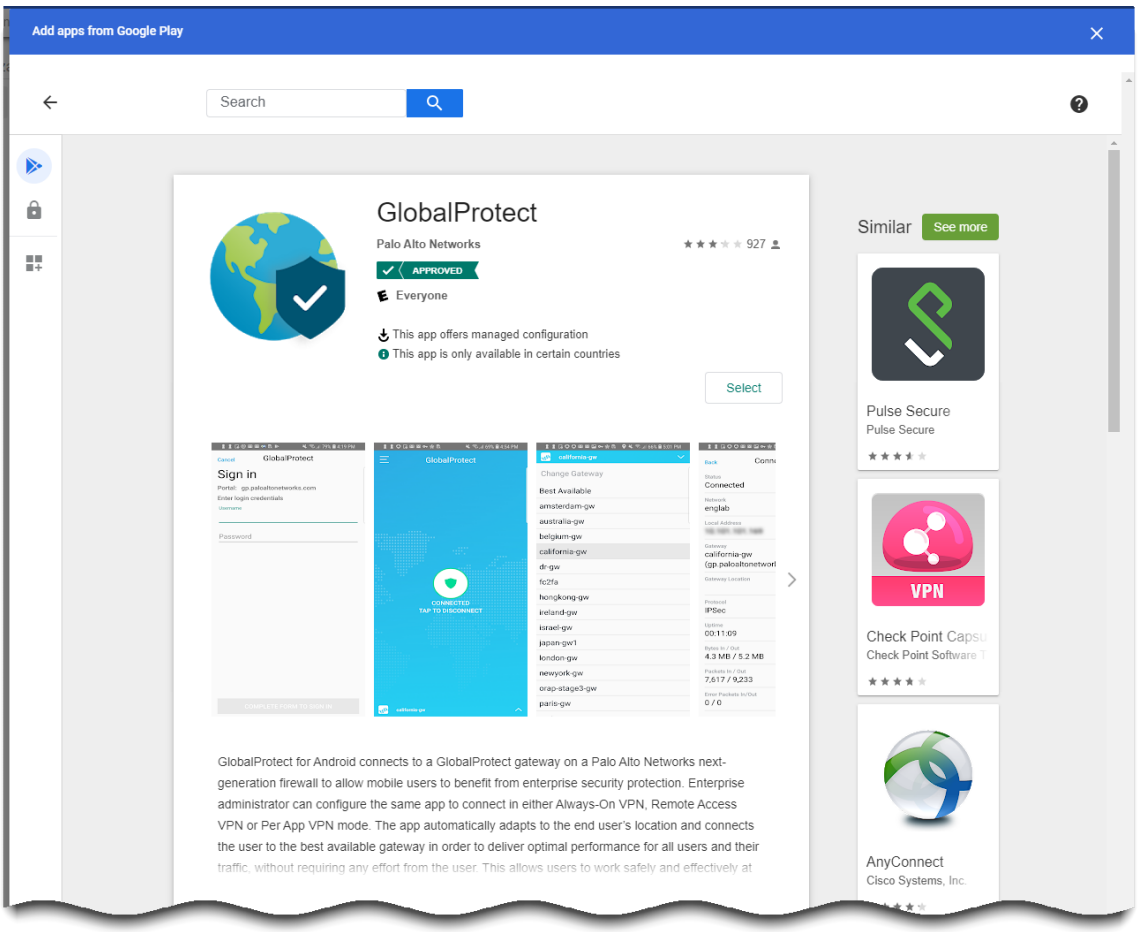
© 2019 Palo Alto Networks, Inc.



7. 单击 **Select**（选择）以添加 GlobalProtect 应用程序。

   如果成功添加 GlobalProtect 应用程序，则会显示一条消息。

© 2019 Palo Alto Networks, Inc.

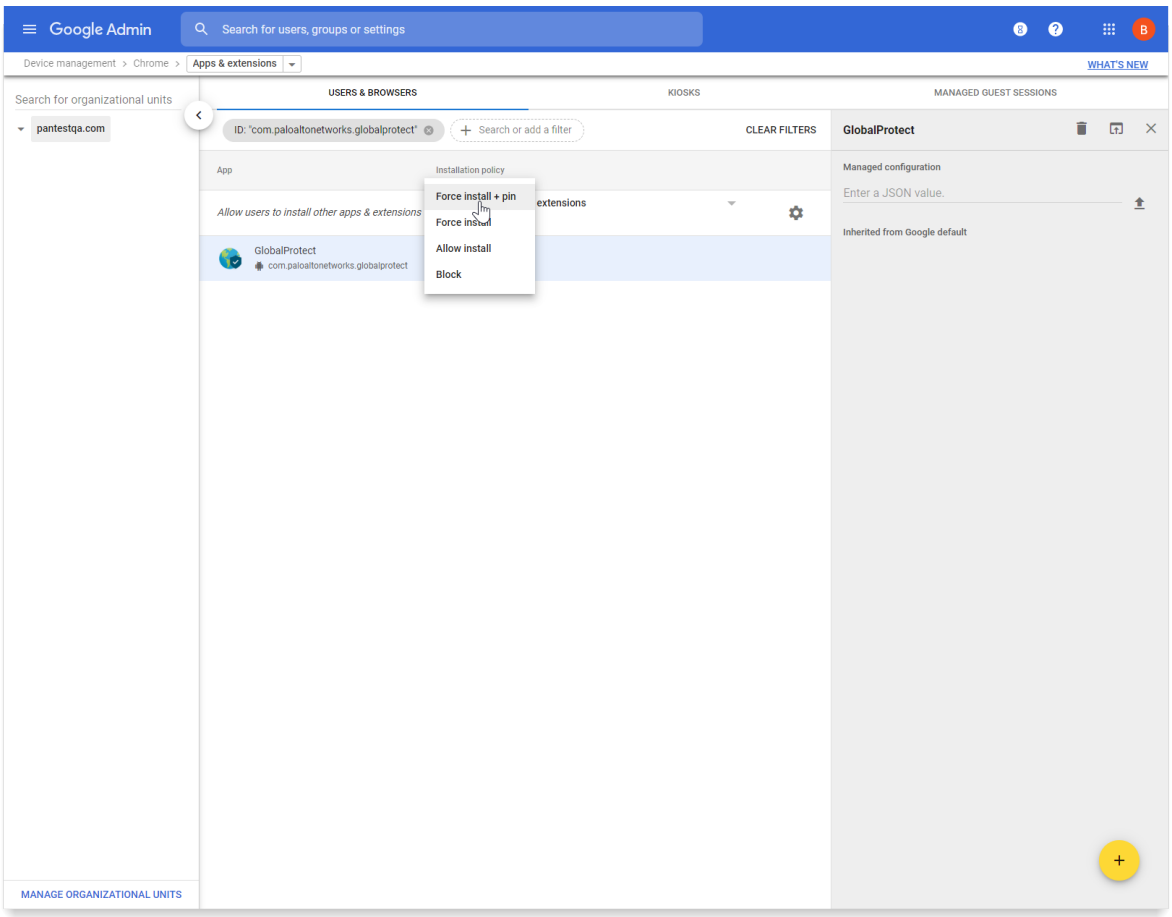


STEP 3 | 确定 GlobalProtect 应用如何安装至 Chromebook 上。

在您批准 GlobalProtect 应用程序后，您必须指定如何将应用程序安装到 Chromebook 上。为防止用户通过卸载应用绕过 GlobalProtect，当用户登录至他们的 Chromebook 时，强制所有 Chromebook 自动安装 GlobalProtect 应用。

1. 在应用程序扩展管理设置（**Device Management**（设备管理）> **Chrome** > **App & extensions**（应用程序和扩展））下，从应用程序列表中选择 **GlobalProtect**。
2. 从页面左边缘的列表中选择组织单位。
3. 选择以下任意选项：
   - （推荐）**Force install + pin**（强制安装+ 锁定）— 启用强制安装的 GlobalProtect 应用程序并将其锁定到任务栏。如果选择了此选项，则用户将无法选择退出应用程序。
   - **Force install**（强制安装）— 如果您想确保当用户登录到 Chromebook 时，在每个 Chromebook 上自动安装 GlobalProtect 应用程序，请使用此选项。为了防止用户卸载 GlobalProtect 应用程序并绕过安全性和合规要求，您需要实施 **Force install**（强制安装）选项。如果选择了此选项，则用户将无法选择退出应用程序。
   - **Allow install**（允许安装）— 从 Google Play 商店手动安装此应用程序。此选项还允许用户从 Chromebook 中卸载 GlobalProtect 应用程序。
   - **Block**（阻止）— 阻止用户安装此应用程序。

© 2019 Palo Alto Networks, Inc.



4. **Save**（保存）更改。

STEP 4 | 应用受管配置至 GlobalProtect 应用。

如果您已启用 GlobalProtect 应用以强制安装，您可以将受管配置文件应用至该应用。受管配置文件包含可配置应用设置的值。

1. 在应用程序管理设置（**Device Management**（设备管理）> **Chrome management**（**Chrome** 管理）> **App & Extensions**（应用程序和扩展））下，从应用程序列表中选择 **GlobalProtect**。
2. 从页面左边缘的列表中选择组织单位。
3. 单击页面右边缘的 **Upload from file**（从文件上传）图标，选择并上传受管配置文件。或者以 JSON 格式输入密钥值的名称，如下面的示例配置所示。

```
{
 "portal": "acme.portal.com",
 "username": "user123"
}
```

下表显示了受管配置文件中的设置示例。有关与贵公司相关的设置，请与您的 IT 管理员联系。

设置	说明	值类型	示例
门户	门户的 IP 地址或完全限定域名 (FQDN)。	字符串	`acme.portal.com`

© 2019 Palo Alto Networks, Inc.

设置	说明	值类型	示例
用户名	门户身份验证用户名。	字符串	`user123`
密码	门户身份验证密码。	字符串	`password123`
client_certificate	门户身份验证客户端证书。	字符串 (Base64)	`DAFDSaweEWQ23wDSAFD...`
client_certificate _passphrase	门户身份验证客户端证书密码。	字符串	`PA$$W0RD$123`
app_list	阻止列表或允许列表允许您在每应用 VPN 配置中控制哪些应用程序流量可经过 VPN 隧道。	字符串	`allow list| block list: com.google.calendar; com.android.email; com.android.chrome`
connect_method	VPN 连接方法。	字符串	`user-logon | on-demand`
mobile_id	用于识别移动端点的唯一标识符，如第三方 MDM 系统中所配置。	字符串	`5188a8193be43f42d332dde5cb2c941e`
remove_vpn_config _via_restriction	标记以移除 VPN 配置。	Boolean	`true | false`
allow_vpn_bypass	允许应用程序流量绕过 VPN 隧道的标志。	Boolean	`true | false`
cert_alias	在门户或网关身份验证期间用于标识客户端证书的唯一名称。	字符串	公司用户客户端
受管	指示设备是否已注册到 MDM 服务器的标志。	Boolean	`true | false`
所有权	设备所有权类别（例如，**Employee Owned**（归员工所有））。	字符串	`byod`
合规性	指示设备是否符合您定义的合规策略的合规状态。	字符串	是
标签	使您能够标记设备的标签。每个标签必须用逗号隔开。	字符串	`GuestAccount,SatelliteOffice`

4. **Save**（保存）更改。

STEP 5 | 在受管 Chromebook 上对 Android 版 GlobalProtect 应用程序实施策略。

- 在受管 Chromebook 上使用 Android 特有的 **Host Info**（主机信息）Create HIP objects（创建 HIIP 对象）。然后在任何主机信息配置文件 (HIP) 配置文件中将其用作匹配条件。

© 2019 Palo Alto Networks, Inc.

- 使用 HIP 配置文件作为策略规则中的匹配条件来实施相应安全策略。默认情况下，应用程序收集信息数据类别，以帮助识别主机的安全状态。

始终打开 *VPN* 配置

采用始终打开 VPN 配置时，应确保 GlobalProtect 的安全连接始终打开。GlobalProtect 应用在用户登录时将连接至 GlobalProtect 门户以提交用户和主机信息并检索代理配置。在应用从门户接收到代理配置后，将自动连接并建立到代理配置中所指定 GlobalProtect 网关的 VPN 隧道。

有关如何通过受支持的移动设备管理系统来配置始终打开 VPN 配置的信息，请参阅以下部分：

- 使用 AirWatch 配置始终打开 VPN 配置
- 使用 Microsoft Intune 配置始终打开 VPN 配置
- 使用 MobileIron 配置始终打开 VPN 配置
- 使用 Google 管理控制台配置始终打开 VPN 设置

使用 **AirWatch** 配置始终打开 **VPN** 配置

AirWatch 是一种企业移动性管理平台，使您可以从中央控制台管理移动端点。GlobalProtect 应用在防火墙和 AirWatch 受管移动端点之间提供设备级或应用级安全连接。使用 GlobalProtect 作为安全连接，可以持续检查流量，在移动端点上强制实施预防威胁的网络安全策略。

有关如何通过 AirWatch 配置始终打开 VPN 配置的信息，请参阅以下部分：

- 使用 AirWatch 为 iOS 端点配置始终打开 VPN 配置
- 使用 AirWatch 为 Windows 10 UWP 端点配置始终打开 VPN 配置

使用 *AirWatch* 为 *iOS* 端点配置始终打开 *VPN* 配置

采用始终打开 VPN 配置时，应确保 GlobalProtect 的安全连接始终打开。应始终通过 VPN 隧道路由与 GlobalProtect 网关上所配置特定筛选条件（端口和 IP 地址等）相匹配的流量。

要使用 AirWatch 为 iOS 端点配置始终打开 VPN 配置，请按以下步骤操作：

STEP 1 | 下载 GlobalProtect iOS 应用。

- 使用 AirWatch 部署 GlobalProtect 移动应用。
- 用户还可直接从 App Store 下载 GlobalProtect 应用。

在中国，可从 Apple App Store 获取 *GlobalProtect iOS* 应用程序。

STEP 2 | 从 AirWatch 控制台，修改现有 Apple iOS 配置文件，或添加新的配置文件。

1. 选择 **Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件），然后 **ADD**（添加）新配置文件。
2. 从平台列表选择 **iOS**。

© 2019 Palo Alto Networks, Inc.

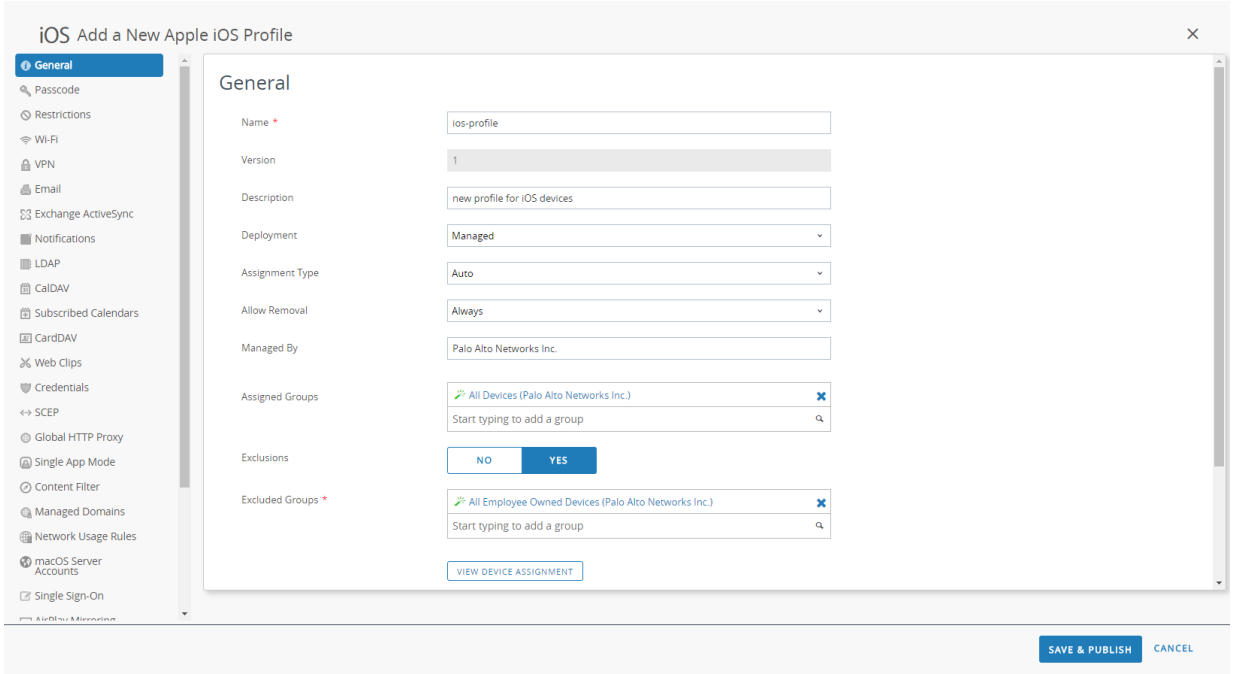
STEP 3 | **配置General（常规）设置：**

1. 输入配置文件的 **Name**（名称）。
2. （可选）输入指定配置文件用途的简短**Description**（说明）。
3. （可选）选择**Deployment**（部署）方法，该方法指示是否在取消注册时自动删除配置文件 —— **Managed**（受管）（删除配置文件）或**Manual**（手动）（配置文件仍保持已安装状态，直至被最终用户删除）。
4. （可选）选择 **Assignment Type**（分配类型）以决定如何将配置文件部署到端点。选择 **Auto**（自动）以自动将配置文件部署到所有终端，选择 **Optional**（可选）使最终用户能够从自助服务门户 (SSP) 安装配置文件或手动将配置文件部署到单个端点，或者选择 **Compliance**（合规）以在最终用户违反适用于该端点的合规性策略时部署该配置文件。

© 2019 Palo Alto Networks, Inc.

5. （可选）选择是否想要最终用户 **Allow Removal**（允许删除）配置文件。选择 **Always**（总是）使最终用户能够随时手动删除配置文件，选择 **Never**（决不）阻止最终用户删除配置文件，或者选择 **With Authorization**（授权）以使最终用户能够在管理员的授权下移除配置文件。选择 **With Authorization**（授权）添加要求的密码。
6. （可选）在 **Managed By**（管理者）字段中，输入具有配置文件管理权限的组织组。
7. （可选）在 **Assigned Groups**（分配组）字段中，添加想要为其添加配置文件的智能组。此字段包含一个创建新智能组的选项，智能组可使用最低 OS 版本、设备型号、所有权类别、组织组等的规格进行配置。
8. （可选）指示是否想要在此配置文件的分配中包含任何 **Exclusions**（排除）。如果选择 **Yes**（是），则显示 **Excluded Groups**（排除组）字段，让您可以选择希望从此配置文件分配中排除的智能组。
9. （可选）如果启用 **Install only on devices inside selected areas**（仅在选定区域安装设备）选项，则配置文件只能安装在指定地理围栏或 iBeacon 区域内的端点上。出现提示时，在 **Assigned Geofence Areas**（分配的地理围栏区域）字段内添加地理围栏或 iBeacon 区域。
10. （可选）如果 **Enable Scheduling and install only during selected time periods**（仅在选定时间段内启动计划和安装），则可以在配置文件安装时应用时间表（**Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles Settings**（配置文件设置）> **Time Schedules**（时间表）），这将限制配置文件在端点上进行安装的时间段。出现提示时，在 **Assigned Schedules**（分配的计划）字段内输入计划名称。
11. （可选）选择想要从所有端点删除配置文件的 **Removal Date**（删除日期）。

© 2019 Palo Alto Networks, Inc.

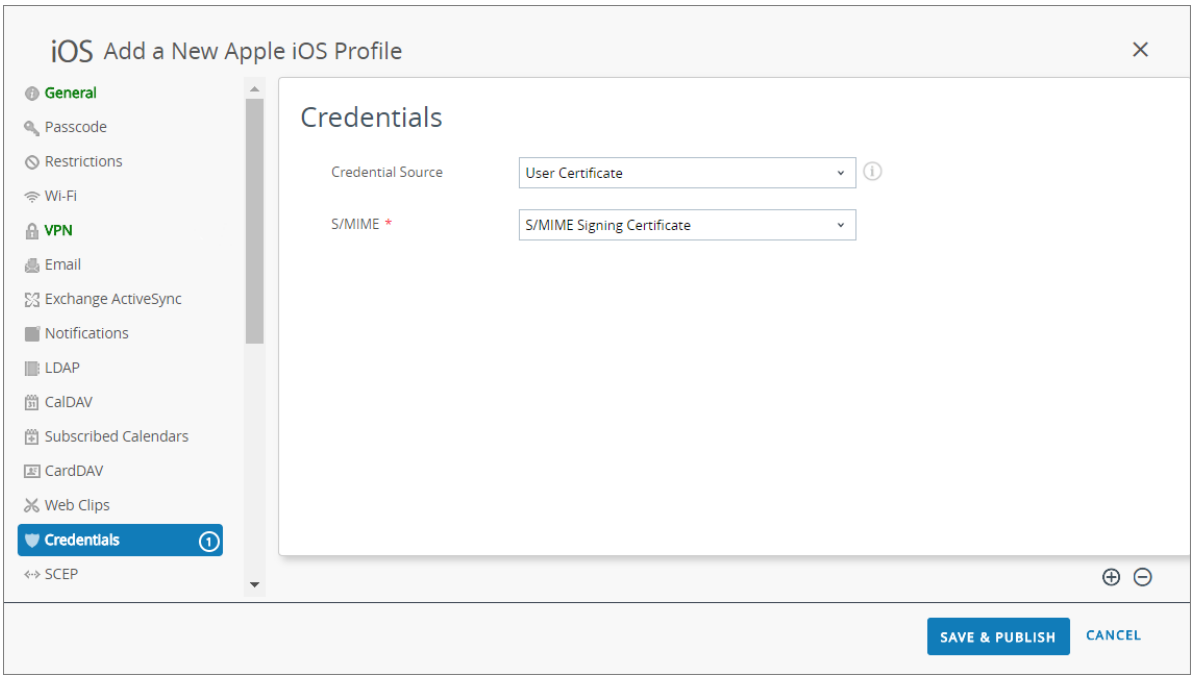


© 2019 Palo Alto Networks, Inc.

STEP 4 | （可选）如果需要客户端证书身份验证才能部署 GlobalProtect，则配置 **Credentials**（凭据）设置：

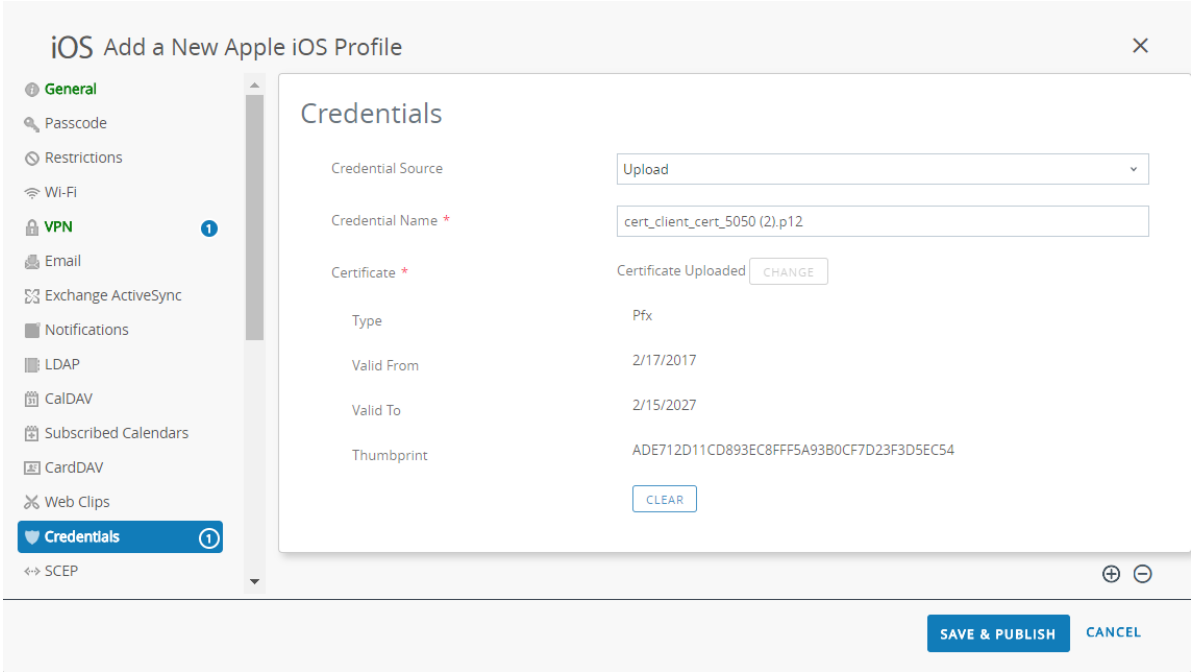
> 从 *iOS 12* 开始，如果要将客户端证书用于 *GlobalProtect* 客户端身份验证，则必须将客户端证书部署为从 *MDM* 服务器推送的 *VPN* 配置文件组成部分。如果使用任何其他方法从 *MDM* 服务器部署客户端证书，则 *GlobalProtect* 应用将无法使用此证书。

- 要从 AirWatch 用户中提取客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **User Certificate**（用户证书）。
  2. 选择 **S/MIME Signing Certificate**（**S/MIME** 签名证书）（默认）。



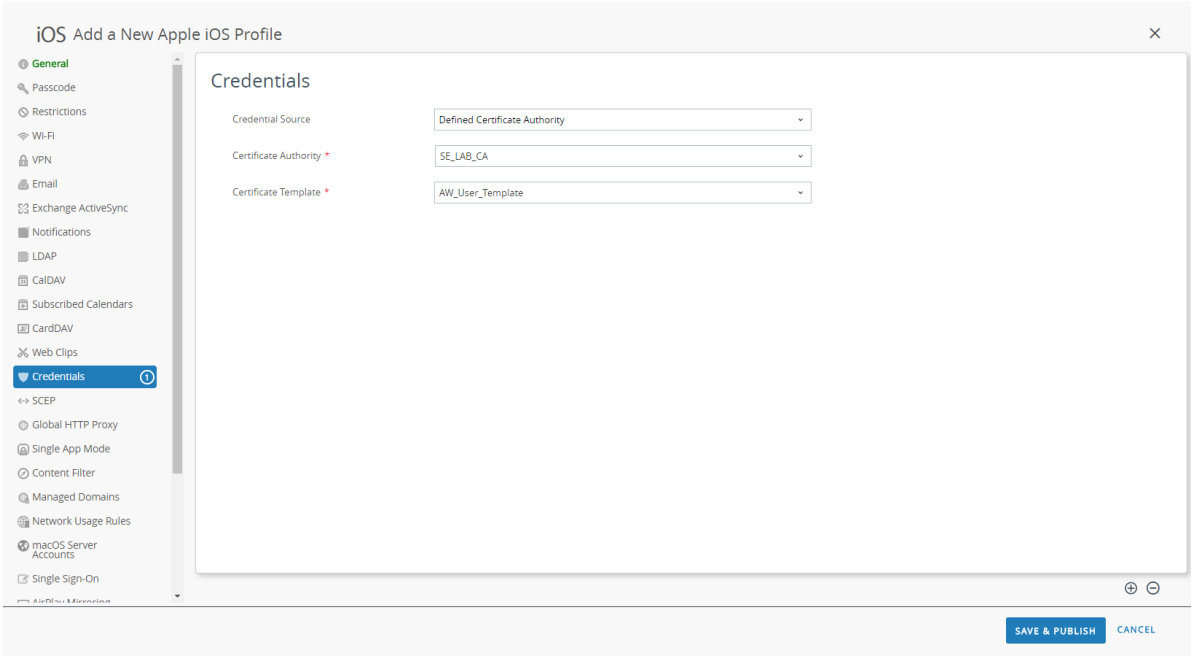
- 要手动上传客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **Upload**（上传）。
  2. 输入 **Credential Name**（凭据名称）。
  3. 单击 **UPLOAD**（上传），找到并选定想要上传的证书。
  4. 证书选定后，单击 **SAVE**（保存）。

© 2019 Palo Alto Networks, Inc.



- 要使用预定义证书颁发机构和模板：
  1. 设置 **Credential Source**（凭据来源）为 **Defined Certificate Authority**（定义的证书颁发机构）。
  2. 选择想要从其获取证书的 **Certificate Authority**（证书颁发机构）。
  3. 选择用于证书颁发机构的 **Certificate Template**（证书模板）。

© 2019 Palo Alto Networks, Inc.

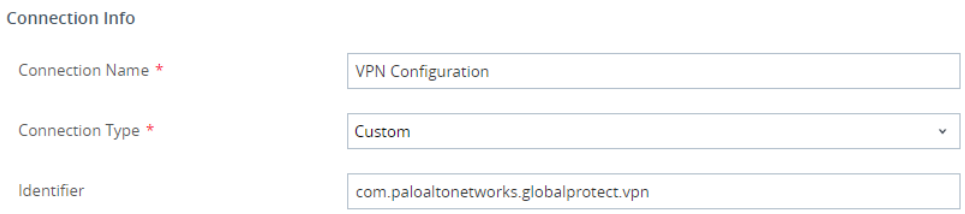


© 2019 Palo Alto Networks, Inc.

STEP 5 | 配置 VPN 设置：

1. 输入端点显示的 **Connection Name**（连接名称）。
2. 选择网络 **Connection Type**（连接类型）：
   - 对于 4.1.x 及更低版本的 GlobalProtect 应用，请选择 **Palo Alto Networks GlobalProtect**。
   - 对于 5.0 及更高版本的 GlobalProtect 应用，请选择 **Custom**（自定义）。
3. （可选）如果将 **Connection Type**（连接类型）设置为 **Custom**（自定义），则在 **Identifier**（标识符）字段内输入以下绑定 ID (**com.paloaltonetworks.globalprotect.vpn**) 以识别 GlobalProtect 应用程序。

   如果您直接从中国版 *Apple App Store* 下载了 *GlobalProtect* 应用程序，请在 *Identifier*（标识符）字段内输入绑定 *ID* (***com.paloaltonetworks.globalprotect.vpncn***)。

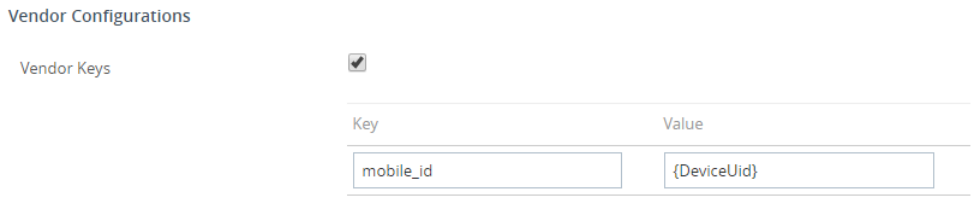


4. 在 **Server**（服务器）字段中，输入用户要连接的 GlobalProtect 门户的主机名或 IP 地址。
5. （可选）输入 VPN **Account**（账户）的用户名，单击 **+** 按钮查看您可插入的支持查找值。
6. （可选）在 **Disconnect on idle**（闲置时断开连接） 字段中，指定在 GlobalProtect 应用停止通过 VPN 隧道路由流量后，端点从此应用注销所花费的时间（秒）。
7. 在身份验证区域，选择用户 **Authentication**（身份验证）方法：**Password**（密码）、**Certificate**（证书）、**Password + Certificate**（密码 + 证书）。
8. 出现提示时，输入 **Password**（密码）并/或选择 GlobalProtect 用于验证用户身份的 **Identity Certificate**（身份证书）。**Identity Certificate**（身份证书）与您在 **Credentials**（凭据）设置内配置的证书一致。
9. 按需启用 **VPN** 并使用新的按需密钥。
10. 使用 操作配置按需规则：连接。
11. （可选）选择 **Proxy**（代理）类型，并配置相关设置。

STEP 6 | （可选）（从 5.0 版本的 GlobalProtect 应用开始）如果 GlobalProtect 配置需要 HIP 与 MDM 集成，则指定唯一设备标识符 (UDID) 属性。

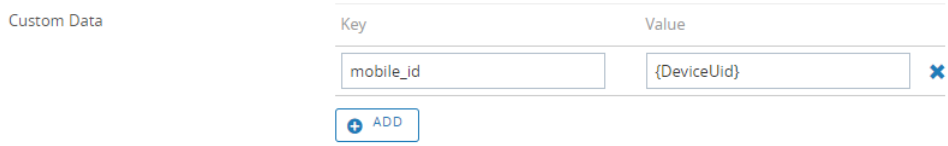
GlobalProtect 支持与 MDM 集成，以从 MDM 服务器获取用于基于 HIP 的策略实施的移动设备属性。为了让 GlobalProtect 集成起作用，GlobalProtect 应用必须向 GlobalProtect 网关展示端点 UDID。GlobalProtect 应用可通过 UDID 属性检索并使用基于 MDM 的部署中的 UDID 信息。若要从配置文件中删除 UDID 属性，则可以不再使用 MDM 集成。GlobalProtect 应用生成新的 UDID，但此 UDID 不能用于集成。

- 如果使用 **Palo Alto Networks GlobalProtect** 网络 **Connection Type**（连接类型），则前往 **VPN** 设置，并启用供应商配置区域的 **Vendor Keys**（供应商表项）。设置 **Key**（表项）为 **`mobile_id`**，**Value**（值）设置为 **`{DeviceUid}`**。



© 2019 Palo Alto Networks, Inc.

- 如果使用 **Custom**（自定义）网络 **Connection Type**（连接类型），则前往 **VPN** 设置，并在连接信息区域内 **ADD**（添加） **Custom Data**（自定义数据）。设置 **Key**（表项）为 **`mobile_id`**，**Value**（值） 设置为 **`{DeviceUid}`**。



STEP 7 | **SAVE & PUBLISH**（保存并发布）更改。

使用 *AirWatch* 为 *Windows 10 UWP* 端点配置始终打开 *VPN* 配置

采用始终打开 VPN 配置时，应确保 GlobalProtect 的安全连接始终打开。应始终通过 VPN 隧道路由与 GlobalProtect 网关上所配置特定筛选条件（端口和 IP 地址等）相匹配的流量。对于更严格的安全要求，可启用 VPN 锁定，强制安全连接始终启用的同时在应用未连接情况下禁用网络访问。此配置类似于您一般在 GlobalProtect 门户配置中配置的 **Enforce GlobalProtect for Network Access**（强制执行 **GlobalProtect** 进行网络访问）。

由于 *AirWatch* 并不将 *GlobalProtect* 列为 *Windows* 端点的官方连接提供程序，所以您必须选择备用 *VPN* 提供程序，编辑 *GlobalProtect* 应用设置，并按照下列工作流所述将配置导回 *VPN* 配置文件。

要使用 AirWatch 为 Windows 10 UWP 端点配置始终打开 VPN 配置，请按以下步骤操作：

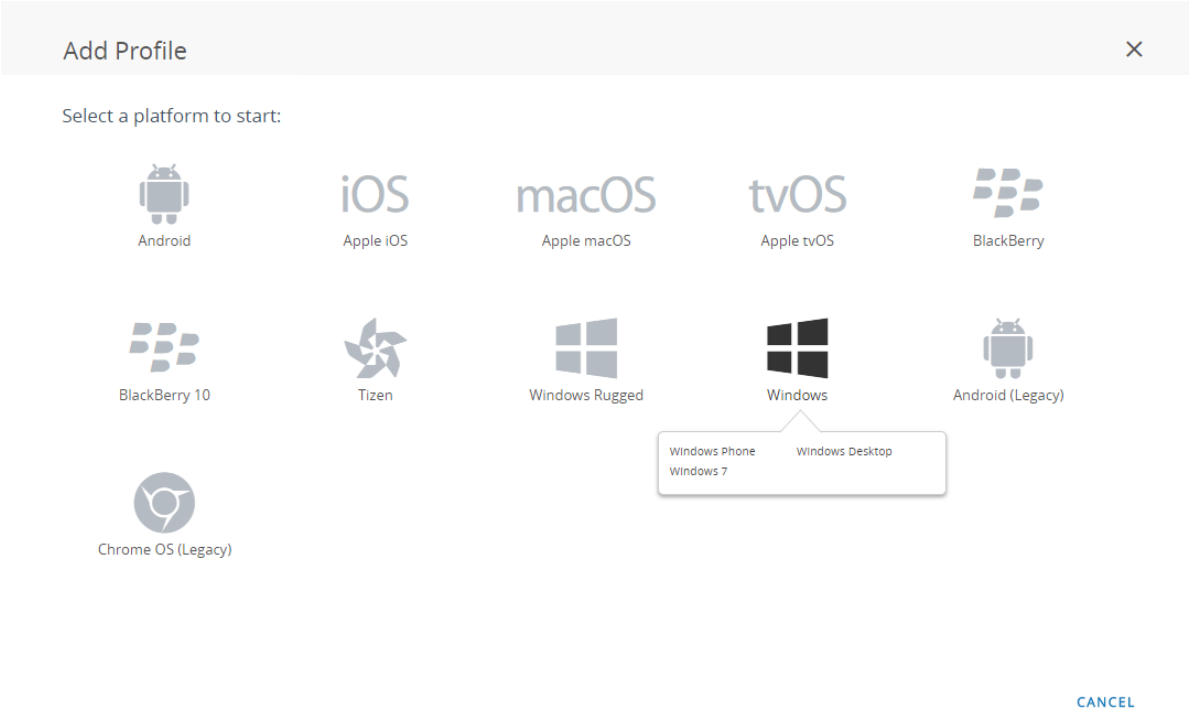
STEP 1 | 下载 GlobalProtect Windows 10 UWP 应用：

- 使用 AirWatch 部署 GlobalProtect 移动应用。
- 用户还可直接从 Microsoft Store 下载 GlobalProtect 应用。

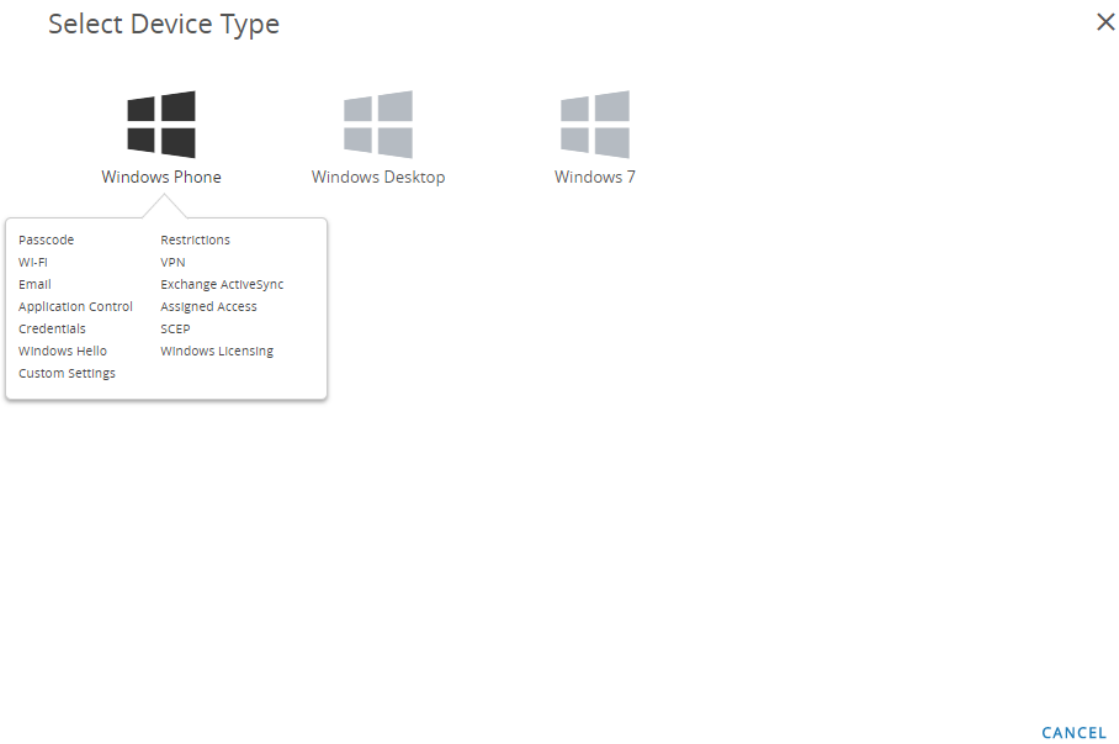
STEP 2 | 从 AirWatch 控制台，修改现有 Windows 10 UWP 配置文件，或添加新的配置文件。

1. 选择 **Devices**（设备） > **Profiles & Resources**（配置文件和资源） > **Profiles**（配置文件），然后 **ADD**（添加）新配置文件。
2. 选择 **Windows** 作为平台，**Windows Phone** 作为设备类型。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.



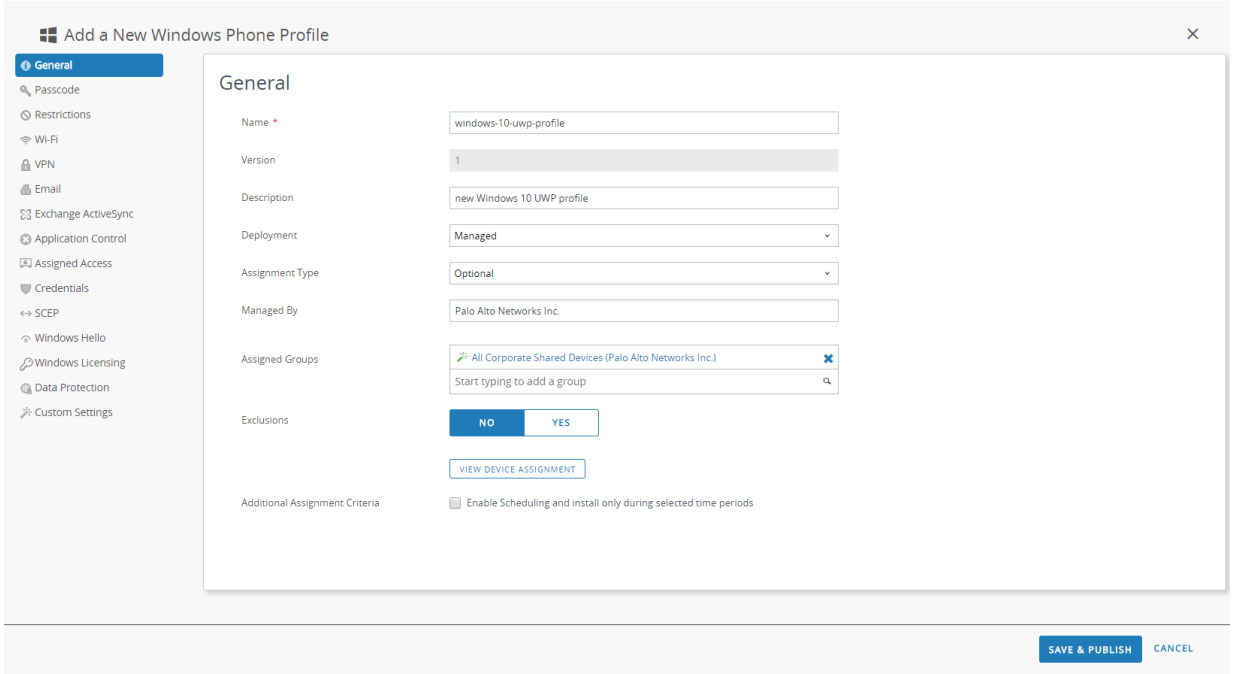
STEP 3 | **配置General（常规）设置：**

1. 输入配置文件的 **Name**（名称）。
2. （可选）输入指定配置文件用途的简短**Description**（说明）。
3. （可选）设置 **Deployment**（部署）方法为 **Managed**（受管理），以便在取消注册时自动删除配置文件。
4. （可选）选择 **Assignment Type**（分配类型）以决定如何将配置文件部署到端点。选择 **Auto**（自动）以自动将配置文件部署到所有终端，选择 **Optional**（可选）使最终用户能够从自助服务门户 (SSP) 安装配置文件或手动将配置文件部署到单个端点，或者选择 **Compliance**（合规）以在最终用户违反适用于该端点的合规性策略时部署该配置文件。
5. （可选）在 **Managed By**（管理者）字段中，输入具有配置文件管理权限的组织组。

© 2019 Palo Alto Networks, Inc.

6. （可选）在 **Assigned Groups**（分配组）字段中，添加想要为其添加配置文件的智能组。此字段包含一个创建新智能组的选项，智能组可使用最低 OS 版本、设备型号、所有权类别、组织组等的规格进行配置。
7. （可选）指示是否想要在此配置文件的分配中包含任何 **Exclusions**（排除）。如果选择 **Yes**（是），则显示 **Excluded Groups**（排除组）字段，让您可以选择希望从此配置文件分配中排除的智能组。
8. （可选）如果 **Enable Scheduling and install only during selected time periods**（仅在选定时间段内启动计划和安装），则可以在配置文件安装时应用时间表（**Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles Settings**（配置文件设置）> **Time Schedules**（时间表）），这将限制配置文件在端点上进行安装的时间段。出现提示时，在 **Assigned Schedules**（分配的计划）字段内输入计划名称。

© 2019 Palo Alto Networks, Inc.

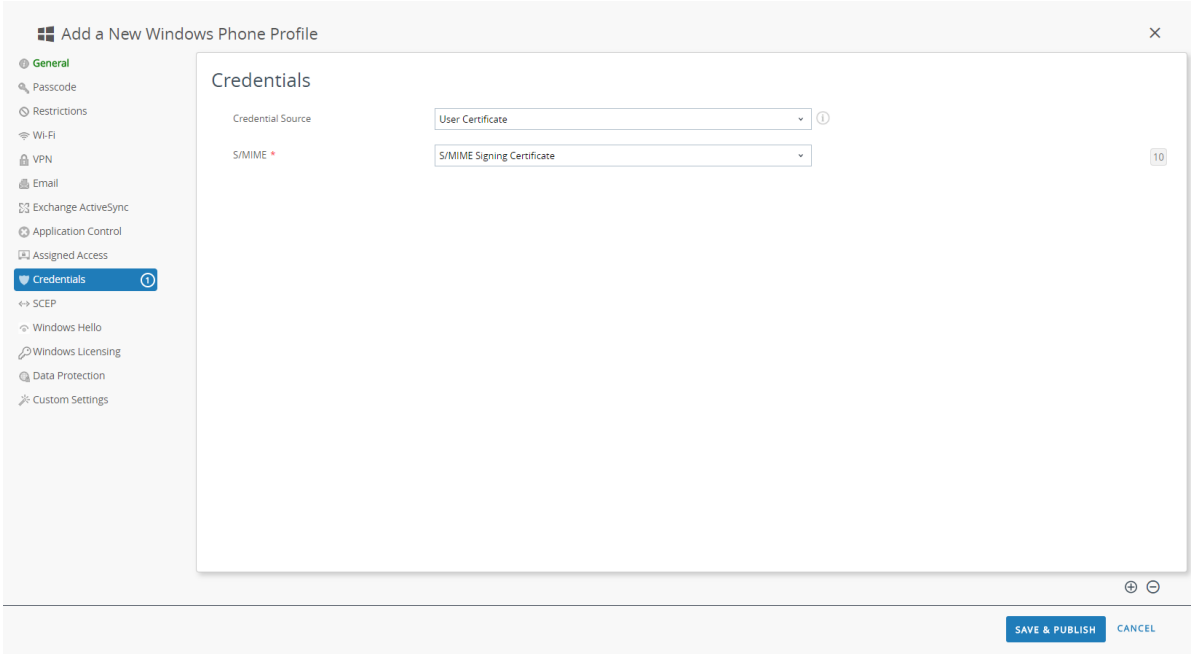


© 2019 Palo Alto Networks, Inc.

STEP 4 | （可选）如果需要客户端证书身份验证才能部署 GlobalProtect，则配置 **Credentials**（凭据）设置：

- 要从 AirWatch 用户中提取客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **User Certificate**（用户证书）。
  2. 选择 **S/MIME Signing Certificate**（**S/MIME** 签名证书）（默认）。

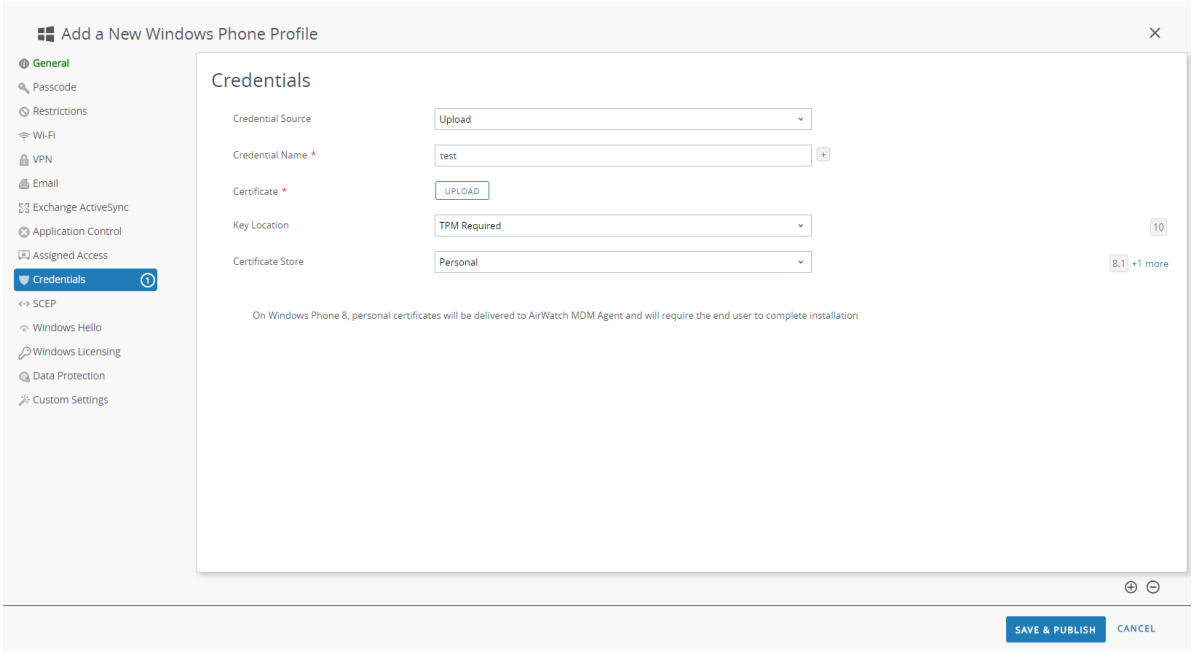
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

- 要手动上传客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **Upload**（上传）。
  2. 输入 **Credential Name**（凭据名称）。
  3. 单击 **UPLOAD**（上传），找到并选定想要上传的证书。
  4. 证书选定后，单击 **SAVE**（保存）。
  5. 选择想要保存证书私钥的 **Key Location**（表项位置）：
     - **TPM Required**（需要 **TPM**）—在可信平台模块中保存私钥。如果端点无可信平台模块，则无法安装私钥。
     - **TPM If Present**（如果存在 **TPM**）—如果端点有可用的可信平台模块，则将私钥保存在其内。如果端点无可信平台模块，则将私钥保存在端点软件内。
     - **Software**（软件）—将私钥保存在端点软件内。
     - **Passport**（通行证）—将私钥保存在 Microsoft 通行证中。要启用此选项，必须在端点上安装 AirWatch Protection Agent 。
  6. 将 **Certificate Store**（证书存储库）设置为 **Personal**（个人）。

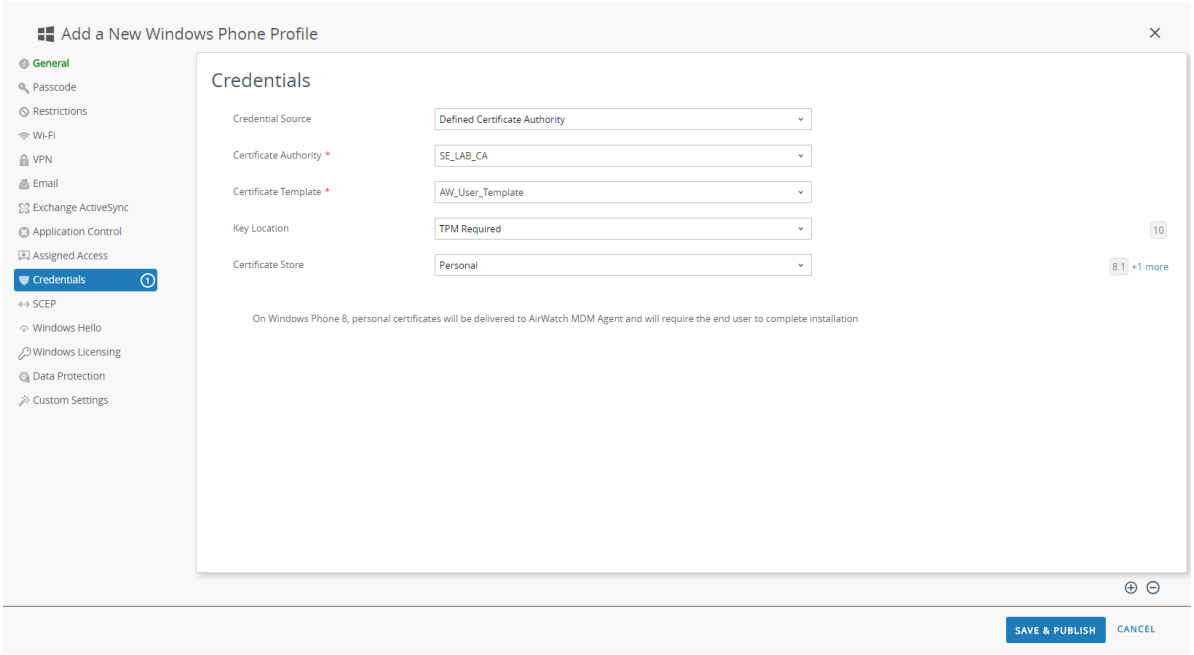
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

- 要使用预定义证书颁发机构和模板：
  1. 设置 **Credential Source**（凭据来源）为 **Defined Certificate Authority**（定义的证书颁发机构）。
  2. 选择想要从其获取证书的 **Certificate Authority**（证书颁发机构）。
  3. 选择用于证书颁发机构的 **Certificate Template**（证书模板）。
  4. 选择想要保存证书私钥的 **Key Location**（表项位置）：
     - **TPM Required**（需要 **TPM**）—在可信平台模块中保存私钥。如果端点无可信平台模块，则无法安装私钥。
     - **TPM If Present**（如果存在 **TPM**）—如果端点有可用的可信平台模块，则将私钥保存在其内。如果端点无可信平台模块，则将私钥保存在端点软件内。
     - **Software**（软件）—将私钥保存在端点软件内。
     - **Passport**（通行证）—将私钥保存在 Microsoft 通行证中。要启用此选项，必须在端点上安装 AirWatch Protection Agent。
  5. 将 **Certificate Store**（证书存储库）设置为 **Personal**（个人）。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

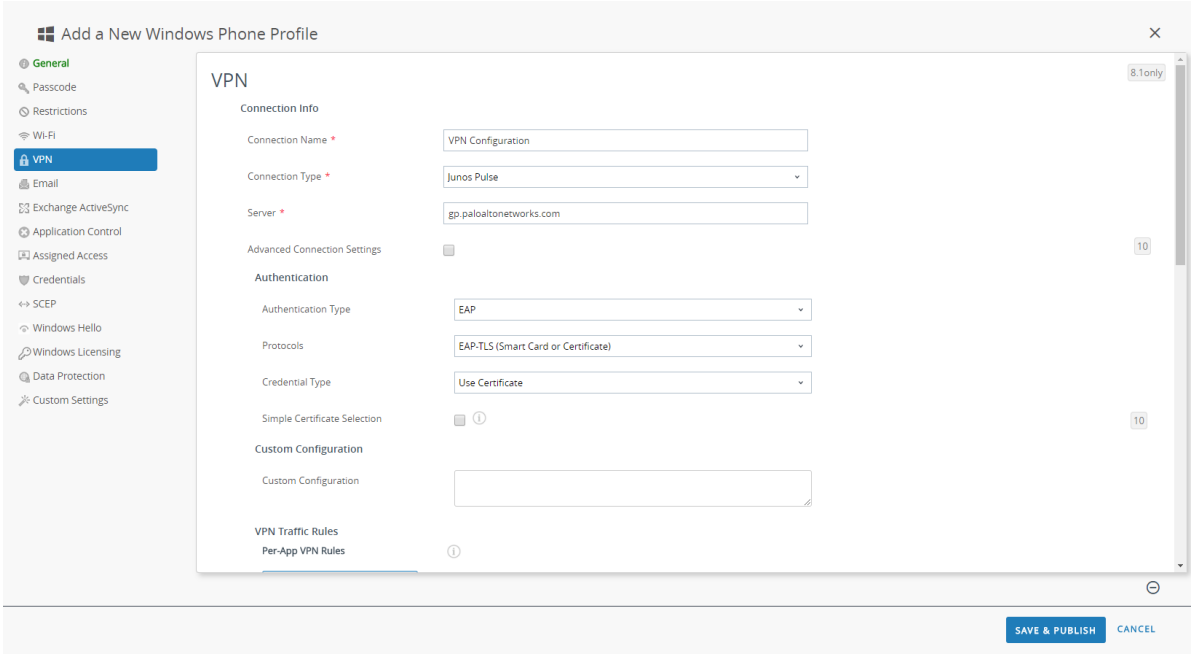
STEP 5 | **配置 VPN 设置：**

1. 输入端点显示的 **Connection Name**（连接名称）。
2. 选择备用提供程序 **Connection Type(连接类型)**（勿选择**IKEv2**、**L2TP**、**PPTP** 或 **Automatic**（自动），因为其没有 GlobalProtect VPN 配置文件所需的相关联供应商设置）。

   必须选择备用供应商，因为 AirWatch 尚未将 GlobalProtect 列为 Windows 端点的官方连接提供程序。

3. 在 **Server**（服务器）字段中，输入用户要连接的 GlobalProtect 门户的主机名或 IP 地址。
4. 在身份验证区域，选择用于指定最终用户身份验证时使用的方法的 **Authentication Type**（身份验证类型）。

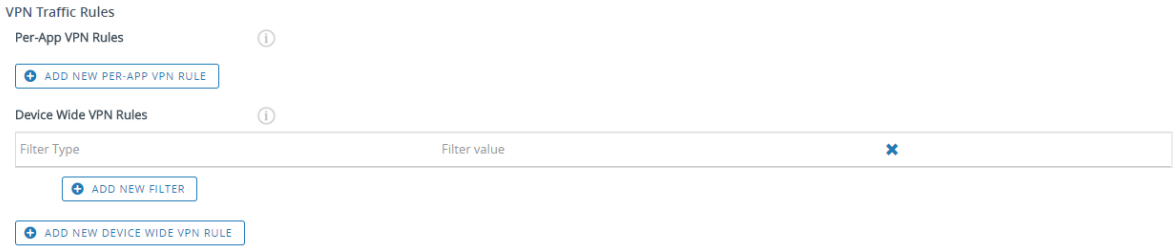
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

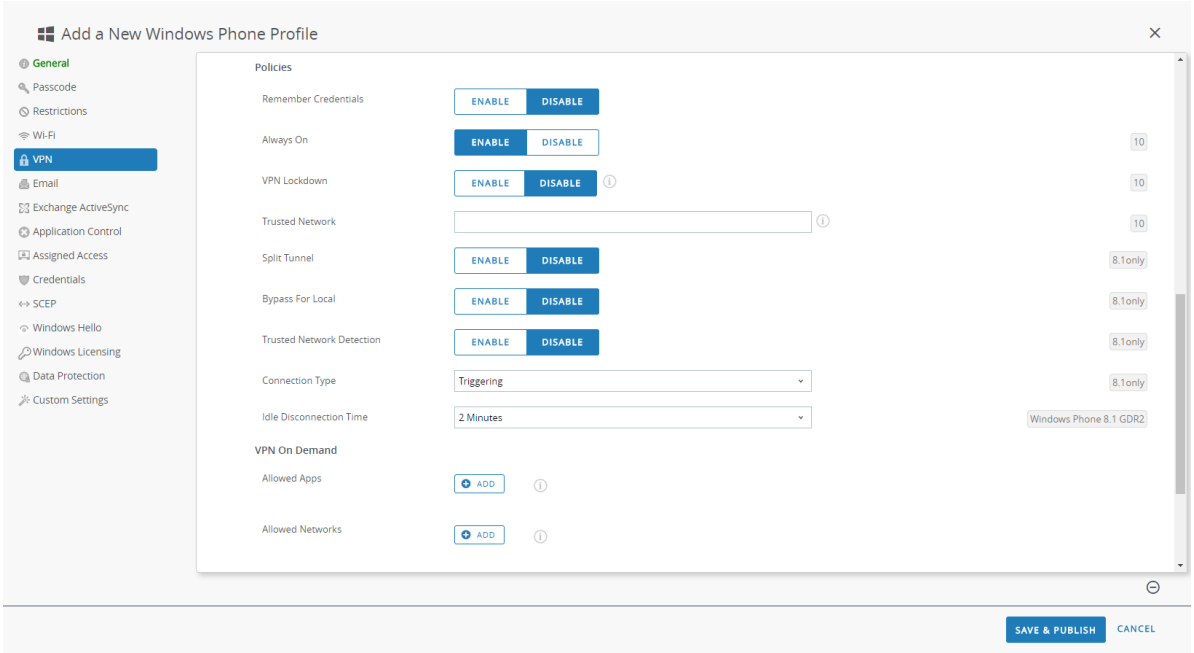
5. （可选）要允许 GlobalProtect 保存用户凭据，请在“策略”区域 **ENABLE**（启用）**Remember Credentials**（记住凭据）选项。
6. （可选）在“VPN 流量规则”区域，**ADD NEW DEVICE WIDE VPN RULE**（添加新设备宽 **VPN** 规则），以通过 VPN 隧道发送与特定路由匹配的流量。这些规则不受应用限制，但可在整个端点进行评估。如果流量与特定匹配条件相匹配，则通过 VPN 隧道进行路由。

   要添加匹配条件，请单击 **ADD NEW FILTER**（添加新筛选条件），然后输入 **Filter Type**（筛选条件类型）和相应的 **Filter Value**（筛选条件值）。



7. 要始终维持 GlobalProtect 连接，请在策略区域配置下列任一选项：
   - **ENABLE**（启用）**Always On**（始终打开），强制安全连接始终可用。
   - **ENABLE**（启用）**VPN Lockdown**（**VPN** 锁定），强制安全连接始终启用，并在应用未连接时禁用网络访问。AirWatch 中的 **VPN Lockdown**（**VPN** 锁定）选项类似于您在 GlobalProtect 门户配置中配置的 **Enforce GlobalProtect for Network Access**（为网络访问强制执行 **GlobalProtect**）。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

8. （可选）如果要 GlobalProtect 仅在检测到可信网络连接时才连接，则指定 **Trusted Network**（可信网络）地址。

STEP 6 | **SAVE & PUBLISH**（保存并发布）更改。

STEP 7 | 要设置连接类型提供程序为 GlobalProtect，请以 XML 格式编辑 VPN 配置文件。

> 要最大程度减少在原始 *XML* 中的额外编辑次数，请在导出配置之前检查 *VPN* 配置文件中的设置。如果在导出 *VPN* 配置文件后需要更改设置，可在原始 *XML* 中进行更改；或者，可更新 *VPN* 配置文件中的设置后重复执行此步骤。

1. 在 **Devices**（设备）> **Profiles**（配置文件）> **List View**（列表视图）中，选择在之前步骤中添加的新配置文件旁的单选按钮，然后选择表格顶部的 **</>XML**。AirWatch 将打开配置文件的 XML 视图。
2. **Export**（导出）配置文件，然后在所选的文本编辑器中打开。
3. 为 GlobalProtect 编辑以下设置：

- 在指定 `PluginPackageFamilyName` 的 `LoclURI` 元素中，将元素更改为：

  ```
  <LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/
  PluginPackageFamilyName</LocURI>
  ```

- 在随后的 `Data` 元素中，将值更改为：

  ```
  <Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>
  ```

1. 保存对所导出配置文件的更改。
2. 返回 AirWatch，选择 **Devices**（设备）> **Profiles**（配置文件）> **List View**（列表视图）。
3. 创建并命名新配置文件（选择 **ADD**（添加）> **Add Profile**（添加配置文件）> **Windows** > **Windows Phone**）。
4. 选择 **Custom Settings**（自定义设置）> **Configure**（配置），然后复制粘贴所编辑的配置。
5. **SAVE & PUBLISH**（保存并发布）更改。

STEP 8 | 要清除原始配置文件，选择 **Devices**（设备）> **Profiles**（配置文件）> **List View**（列表视图），然后选择 **More Actions**（更多操作）> **Deactivate**（停用）。AirWatch 将该配置文件移至非活动列表。

STEP 9 | 测试配置。

使用 **Microsoft Intune** 配置始终打开 **VPN** 配置

Microsoft Intune 是一种基于云的企业移动性管理平台，使您可以从中心位置管理移动端点。GlobalProtect 应用在防火墙和 Microsoft Intune 受管移动端点之间提供设备级或应用级安全连接。使用 GlobalProtect 作为安全连接，可以持续检查流量，在移动端点上强制实施预防威胁的网络安全策略。

有关如何通过 Microsoft Intune 配置始终打开 VPN 配置的信息，请参阅以下部分：

- 使用 Microsoft Intune 为 iOS 端点配置始终打开 VPN 配置
- 使用 Microsoft Intune 为 Windows 10 UWP 端点配置始终打开 VPN 配置

使用 *Microsoft Intune* 为 *iOS* 端点配置始终打开 *VPN* 配置

采用始终打开 VPN 配置时，应确保 GlobalProtect 的安全连接始终打开。应始终通过 VPN 隧道路由与 GlobalProtect 网关上所配置特定筛选条件（端口和 IP 地址等）相匹配的流量。

要使用 Microsoft Intune 为 iOS 端点配置始终打开 VPN 配置，请按以下步骤操作：

STEP 1 | 下载 GlobalProtect iOS 应用。

- 使用 Microsoft Intune 部署 GlobalProtect 移动应用。
- 用户还可直接从 App Store 下载 GlobalProtect 应用。

© 2019 Palo Alto Networks, Inc.

STEP 2 | （可选）如果部署需要基于证书的身份验证，则配置证书配置文件。

STEP 3 | 创建新的 iOS VPN 配置文件。

- 设置 **Platform**（平台）为 **iOS**。

STEP 4 | 为 iOS 端点配置始终打开 VPN 设置。

- 设置 **Connection type**（连接类型）为 **Palo Alto Networks GlobalProtect**。

使用 *Microsoft Intune* 为 *Windows 10 UWP* 端点配置始终打开 *VPN* 配置

采用始终打开 VPN 配置时，应确保 GlobalProtect 的安全连接始终打开。应始终通过 VPN 隧道路由与 GlobalProtect 网关上所配置特定筛选条件（端口和 IP 地址等）相匹配的流量。

要使用 Microsoft Intune 为 Windows 10 UWP 端点配置始终打开 VPN 配置，请按以下步骤操作：

STEP 1 | 下载 GlobalProtect Windows 10 UWP 应用：

- 使用 Microsoft Intune 部署 GlobalProtect 移动应用。
- 用户还可直接从 Microsoft Store 下载 GlobalProtect 应用。

STEP 2 | （可选）如果部署需要基于证书的身份验证，则配置证书配置文件。

STEP 3 | 创建新的 Windows 10 UWP VPN 配置文件。

- 设置 **Platform**（平台）为 **Windows 10 and later**（**Windows 10** 及更高版本）。

STEP 4 | 为 Windows 10 UWP 端点配置始终打开 VPN 设置。

- 设置 **Connection type**（连接类型）为 **Palo Alto Networks GlobalProtect**。
- 启用 **Always On**（始终打开）VPN。

使用 **MobileIron** 配置始终打开 **VPN** 配置

MobileIron 是一种企业移动性管理平台，使您可以从中央控制台管理移动端点。GlobalProtect 应用在防火墙和 MobileIron 受管移动端点之间提供设备级或应用级安全连接。使用 GlobalProtect 作为安全连接，可以持续检查流量，在移动端点上强制实施预防威胁的网络安全策略。

有关如何通过 MobileIron 配置始终打开 VPN 配置的信息，请参阅以下部分：

- 使用 MobileIron 为 iOS 端点配置始终打开 VPN 配置
- 使用 MobileIron 为安卓端点配置始终打开 VPN 配置

使用 *MobileIron* 为 *iOS* 端点配置始终打开 *VPN* 配置

采用始终打开 VPN 配置时，应确保 GlobalProtect 的安全连接始终打开。应始终通过 VPN 隧道路由与 GlobalProtect 网关上所配置特定筛选条件（端口和 IP 地址等）相匹配的流量。

要使用 MobileIron 为 iOS 端点配置始终打开 VPN 配置，请按以下步骤操作：

STEP 1 | 下载 GlobalProtect iOS 应用。

- 使用 MobileIron 部署 GlobalProtect 移动应用。
- 用户还可直接从 App Store 下载 GlobalProtect 应用。

STEP 2 | （可选）如果部署需要基于证书的身份验证，请添加证书配置，然后 配置证书设置。

STEP 3 | 添加始终打开 VPN 配置。

- 设置配置类型为 **Always On VPN**（始终打开 **VPN**）。

© 2019 Palo Alto Networks, Inc.

STEP 4 | 为 iOS 配置始终打开 VPN 设置。

使用 *MobileIron* 为安卓端点配置始终打开 *VPN* 配置

采用始终打开 VPN 配置时，应确保 GlobalProtect 的安全连接始终打开。应始终通过 VPN 隧道路由与 GlobalProtect 网关上所配置特定筛选条件（端口和 IP 地址等）相匹配的流量。

要使用 MobileIron 为 Android 端点配置始终打开 VPN 配置，请按以下步骤操作：

STEP 1 | 下载 GlobalProtect 安卓应用。

- 使用 MobileIron 部署 GlobalProtect 移动应用。
- 用户还可直接从 Google Play 下载 GlobalProtect 应用。

STEP 2 | （可选）如果部署需要基于证书的身份验证，请添加证书配置，然后 配置证书设置。

STEP 3 | 添加始终打开 VPN 配置。

- 设置配置类型为 **Always On VPN**（始终打开 **VPN**）。

STEP 4 | 为安卓配置始终打开 VPN 设置。

使用 **Google** 管理控制台配置始终打开 **VPN** 设置

Google 管理控制台是一种基于云的企业移动性管理平台，使您可以从中央控制台管理 Chromebook。GlobalProtect 应用在防火墙和受 Google 管理控制台管理的 Chromebook 之间提供设备级或应用级安全连接。使用 GlobalProtect 作为安全连接，可以持续检查流量，在移动端点上强制实施预防威胁的网络安全策略。

使用 *Google* 管理控制台为 *Chromebook* 配置始终打开 *VPN* 设置

Chromebook 通过 Android 版 GlobalProtect 应用扩展支持，支持“始终打开 VPN”。采用始终打开 VPN 配置时，应确保 GlobalProtect 的安全连接始终打开。应始终通过 VPN 隧道路由与 GlobalProtect 网关上所配置特定筛选条件（端口和 IP 地址等）相匹配的流量。通过让最终用户在其 Chromebook 上运行 Android 版 GlobalProtect 应用，可以确保他们始终连接至 GlobalProtect 并可以确保持续安全性。

- *Android* 版 *GlobalProtect* 应用仅支持在某些 Chromebook 上使用。
- 不支持 *Android* 应用程序的 *Chromebook* 必须继续使用 *Chrome* 的 *GlobalProtect* 应用。但是，这些 *Chromebook* 将不支持“始终打开 *VPN*”。
- 如果 *Android* 版 *GlobalProtect* 应用安装于 *Chromebook* 上用于“始终打开 *VPN*”功能，则不得在相同的 *Chromebook* 上安装 *Chrome* 版 *GlobalProtect* 应用。

要使用 Google 管理控制台为 Chromebook 配置始终打开 VPN 配置，请按以下步骤操作。

以下步骤仅适用于使用 Google 管理控制台在受管 Chromebook 上部署 Android 版 GlobalProtect 应用程序。AirWatch 目前不支持受管 Chromebook 上 Android 版 GlobalProtect 应用的“始终打开 VPN”配置。

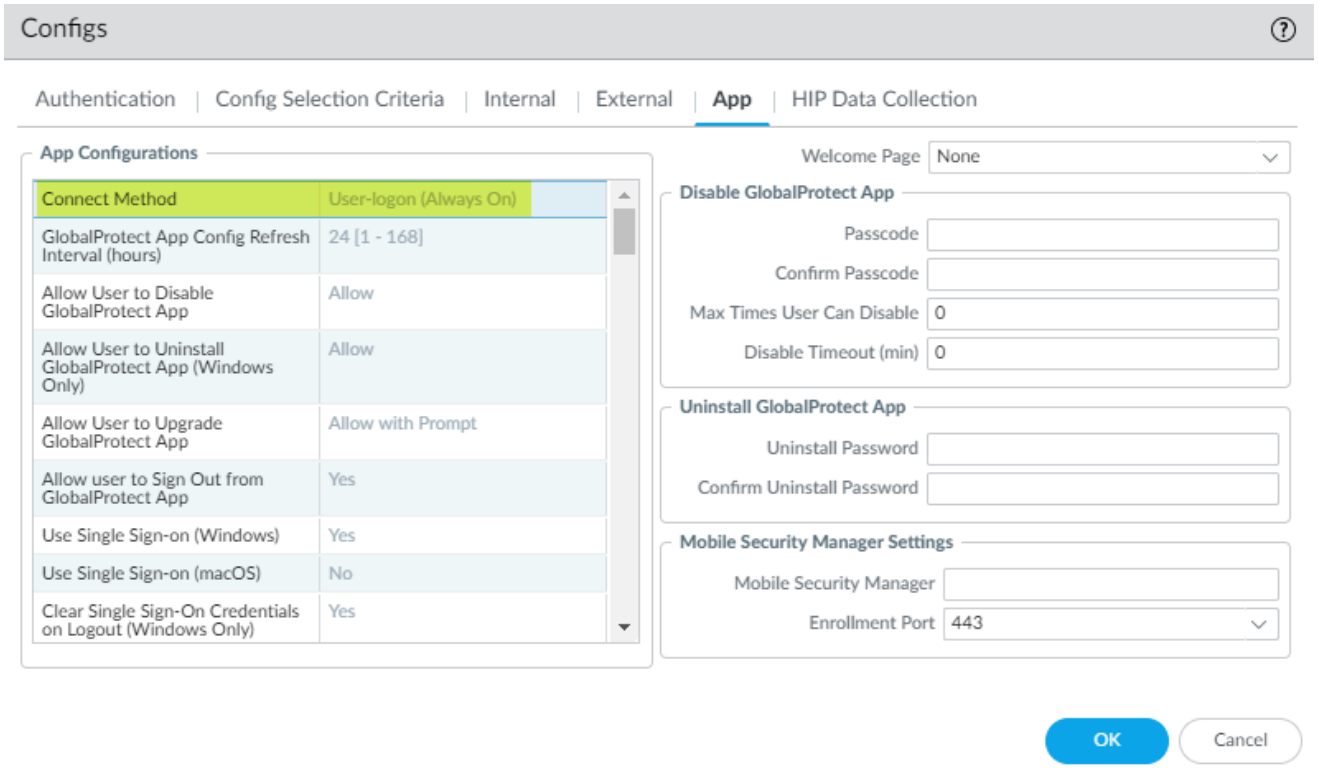
STEP 1 | 从您的 Palo Alto Networks 防火墙， 设置 GlobalProtect 门户访问权限。

STEP 2 | 定义 GlobalProtect 代理配置。

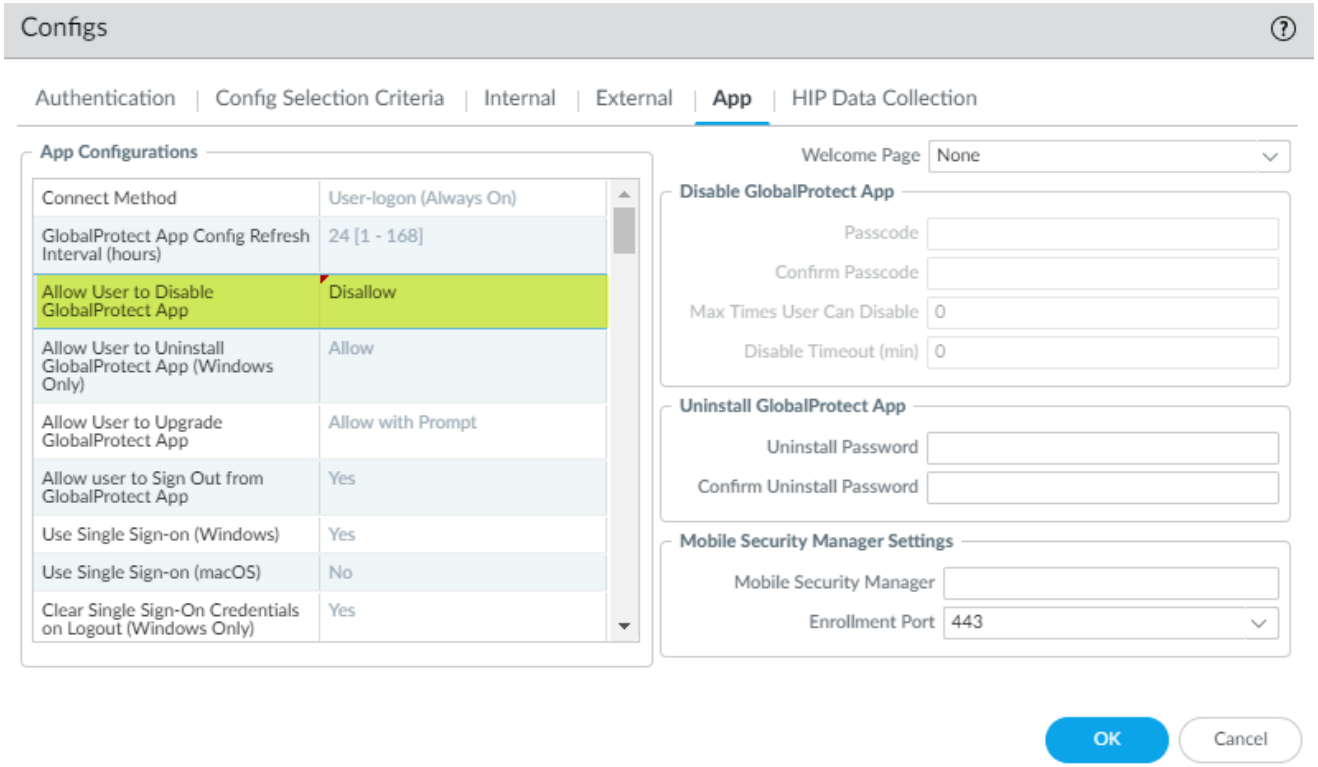
STEP 3 | 自定义 GlobalProtect 应用程序。

- 要配置 GlobalProtect 连接为始终打开，将 **Connect Method**（连接方法）设为 **User-logon (Always On)**（用户登录（始终打开））。

© 2019 Palo Alto Networks, Inc.



- 要防止用户禁用 GlobalProtect 应用，将 **Allow User to Disable GlobalProtect App**（允许用户禁用 **GlobalProtect** 应用）选项设置为 **Disallow**（不允许）。



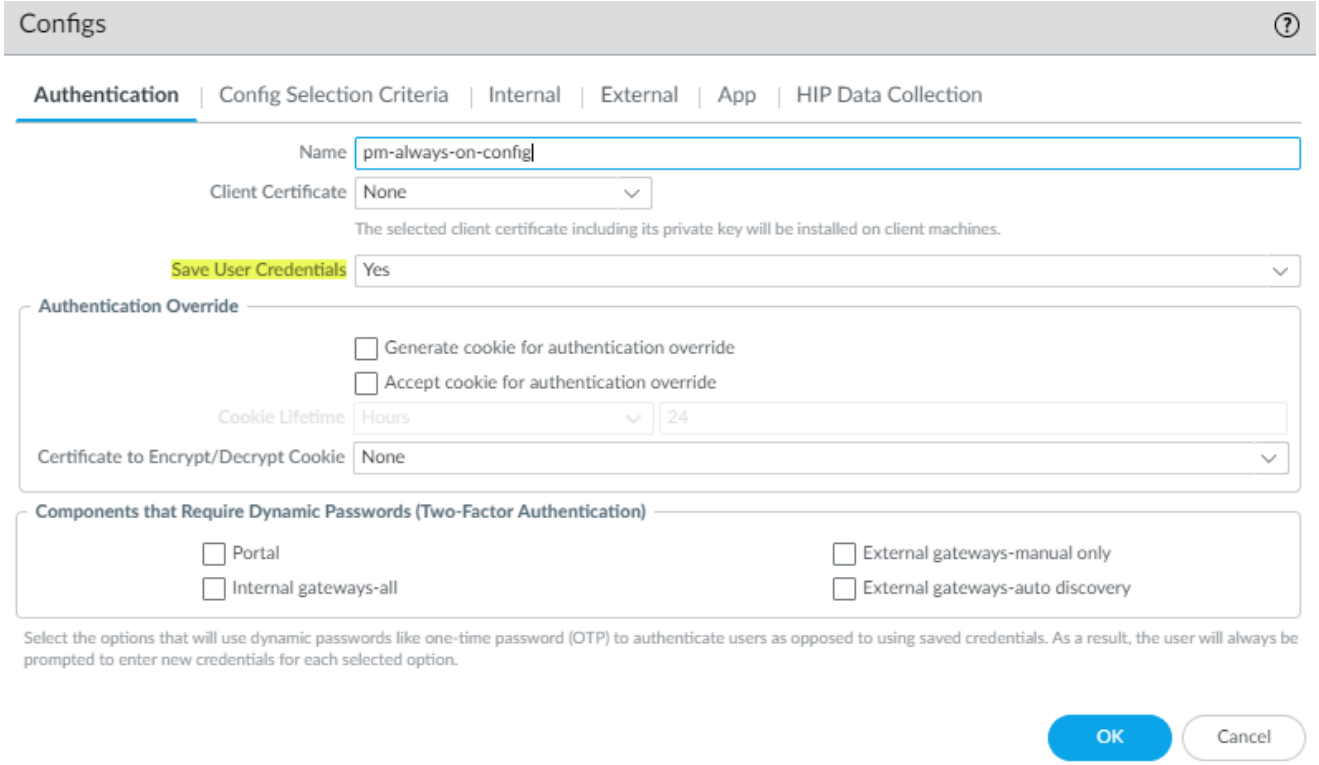
STEP 4 | 启用 GlobalProtect 的透明身份验证。

© 2019 Palo Alto Networks, Inc.

要阻止用户跳过 GlobalProtect 身份验证提示并在断开 GlobalProtect 时绕过 GlobalProtect 连接，则为透明身份验证配置以下选项之一：

- 让用户通过客户端证书身份验证进行 GlobalProtect 的透明身份验证。
- 允许 GlobalProtect 应用保存透明登录的用户和密码。

  1. 从您的门户代理配置（**Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）> *<agent-config>*）中选择 **Authentication**（身份验证）。
  2. 将 **Save User Credentials**（保存用户凭据）选项设为 **Yes**（是）。



  3. 单击 **OK**（确定）两次，以保存门户代理配置。

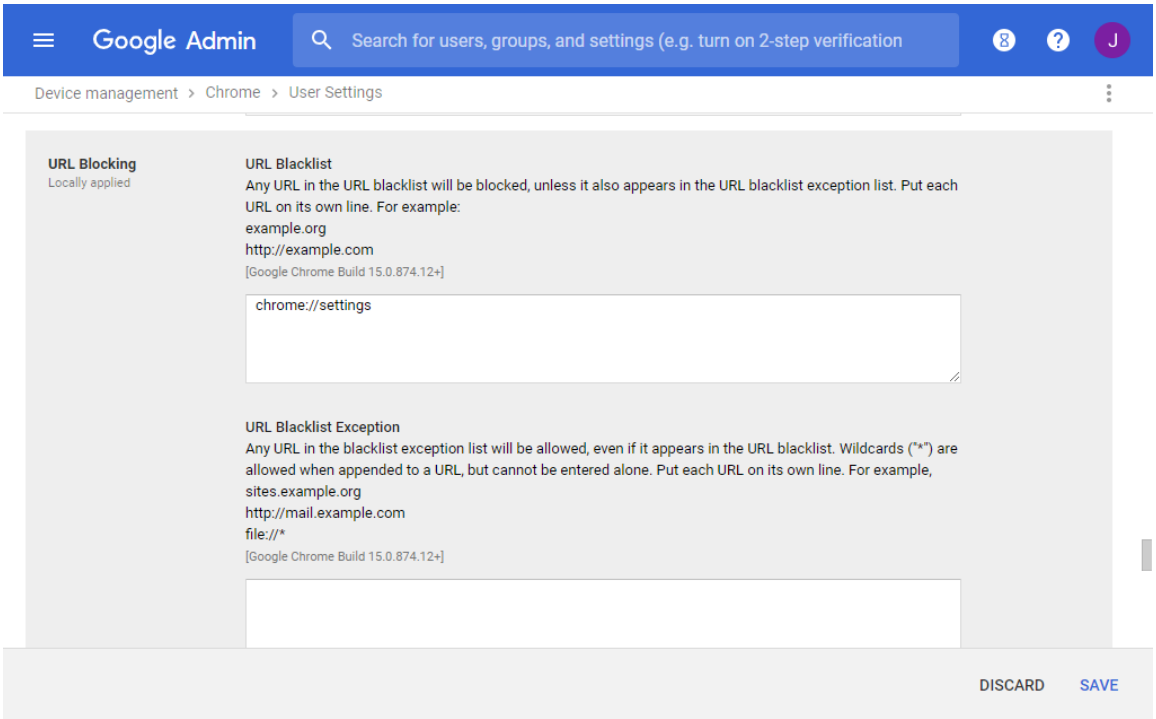
STEP 5 | 在防火墙上 **Commit**（提交）更改。

STEP 6 | 通过 Chrome OS VPN 设置，阻止 Chromebook 用户绕过 GlobalProtect。

1. 以管理员身份登录到 Google 管理控制台。
2. 使用 Google 管理控制台在受管 Chromebook 上为 Android 部署 GlobalProtect 应用在所有受管 Chromebook 上。
3. 将 Chrome 设置 (`chrome://settings`) 加入黑名单以阻止用户修改任何 VPN 设置：

   1. 选择 **Device Management**（设备管理）> **Chrome management**（**Chrome** 管理）> **User Settings**（用户设置）。
   2. 在 Content（内容）> URL Blocking（URL 阻止）区域的 **URL Blacklist**（**URL** 黑名单）文本框中输入 `chrome://settings`。

© 2019 Palo Alto Networks, Inc.



4. **Save**（保存）更改。

用户发起远程访问 *VPN* 配置

在远程访问（按需）VPN 配置中，用户必须手动启动 GlobalProtect 应用，以建立安全的 GlobalProtect 连接。GlobalProtect 应用在用户登录时将连接至 GlobalProtect 门户以提交用户和主机信息并检索代理配置。在应用从门户接收到代理配置后，将连接并建立到代理配置中所指定 GlobalProtect 网关的 VPN 隧道。

有关如何通过受支持的移动设备管理系统配置用户发起远程访问 VPN 配置的信息，请参阅以下部分：

- 使用 AirWatch 配置用户发起远程访问 VPN 配置
- 使用 Microsoft Intune 配置用户发起远程访问 VPN 配置
- 使用 MobileIron 配置用户发起远程访问 VPN 配置

© 2019 Palo Alto Networks, Inc.

使用 **AirWatch** 配置用户发起远程访问 **VPN** 配置

AirWatch 是一种企业移动性管理平台，使您可以从中央控制台管理移动端点。GlobalProtect 应用在 AirWatch 受管移动端点和防火墙之间提供设备级或应用级安全连接。使用 GlobalProtect 作为安全连接，可以持续检查流量，在移动端点上强制实施预防威胁的网络安全策略。

有关如何通过 AirWatch 配置用户发起远程访问 VPN 配置的信息，请参阅以下部分：

- 使用 AirWatch 为 iOS 端点配置用户发起远程访问 VPN 配置
- 使用 AirWatch 为 Windows 10 UWP 端点配置用户发起远程访问 VPN 配置

使用 *AirWatch* 为 *iOS* 端点配置用户发起远程访问 *VPN* 配置

在远程访问（按需）VPN 配置中，用户必须手动启动应用，以建立安全的 GlobalProtect 连接。应仅在用户发起并建立连接后通过 VPN 隧道路由与 GlobalProtect 网关上配置的特定筛选条件（端口和 IP 地址等）相匹配的流量。

要使用 AirWatch 为 iOS 端点配置用户发起远程访问 VPN 配置，请按以下步骤操作：

STEP 1 | 下载 GlobalProtect iOS 应用。

- 使用 AirWatch 部署 GlobalProtect 移动应用。
- 用户还可直接从 App Store 下载 GlobalProtect 应用。

在中国，可从 Apple App Store 获取 *GlobalProtect iOS* 应用程序。

STEP 2 | 从 AirWatch 控制台，修改现有 Apple iOS 配置文件，或添加新的配置文件。

1. 选择 **Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件），然后 **ADD**（添加）新配置文件。
2. 从平台列表选择 **iOS** 。

© 2019 Palo Alto Networks, Inc.

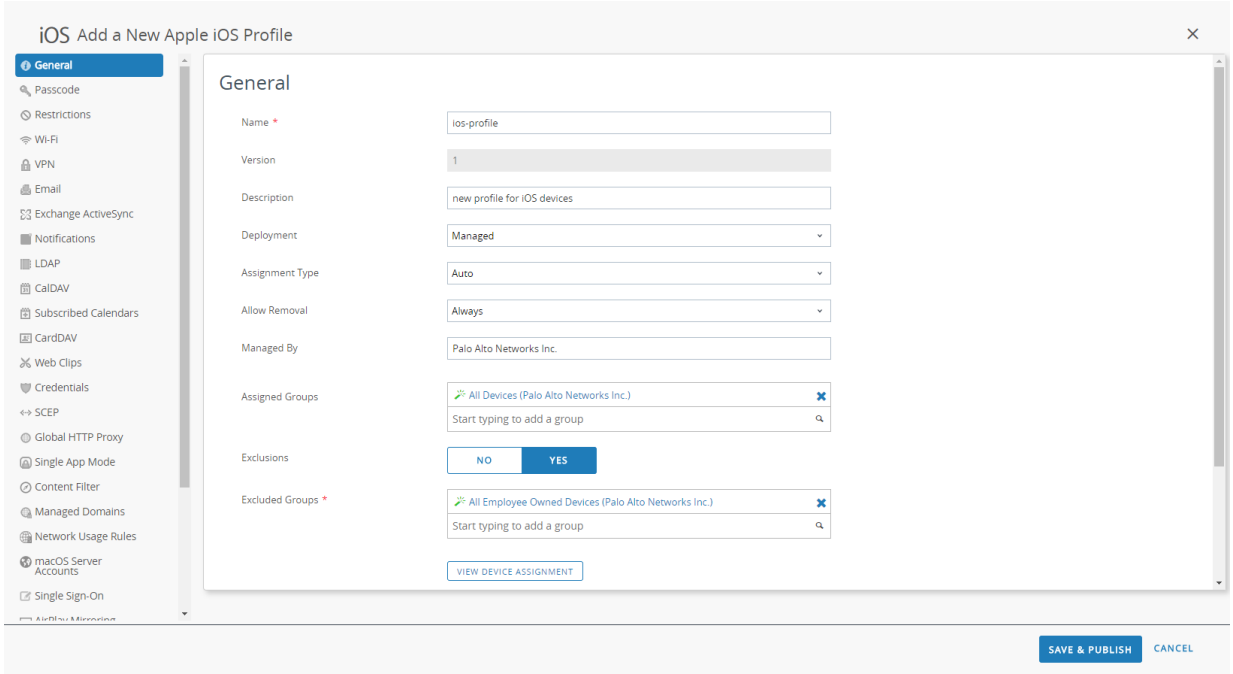
STEP 3 | 配置**General**（常规）设置：

1. 输入配置文件的 **Name**（名称）。
2. （可选）输入指定配置文件用途的简短**Description**（说明）。
3. （可选）选择**Deployment**（部署）方法，该方法指示是否在取消注册时自动删除配置文件 —— **Managed**（受管）（删除配置文件）或**Manual**（手动）（配置文件仍保持已安装状态，直至被最终用户删除）。
4. （可选）选择 **Assignment Type**（分配类型）以决定如何将配置文件部署到端点。选择 **Auto**（自动）以自动将配置文件部署到所有终端，选择 **Optional**（可选）使最终用户能够从自助服务门户 (SSP) 安装配置文件或手动将配置文件部署到单个端点，或者选择 **Compliance**（合规）以在最终用户违反适用于该端点的合规性策略时部署该配置文件。

© 2019 Palo Alto Networks, Inc.

5. （可选）选择是否想要最终用户 **Allow Removal**（允许删除）配置文件。选择 **Always**（总是）使最终用户能够随时手动删除配置文件，选择 **Never**（决不）阻止最终用户删除配置文件，或者选择 **With Authorization**（授权）以使最终用户能够在管理员的授权下移除配置文件。选择 **With Authorization**（授权）添加要求的密码。
6. （可选）在 **Managed By**（管理者）字段中，输入具有配置文件管理权限的组织组。
7. （可选）在 **Assigned Groups**（分配组）字段中，添加想要为其添加配置文件的智能组。此字段包含一个创建新智能组的选项，智能组可使用最低 OS 版本、设备型号、所有权类别、组织组等的规格进行配置。
8. （可选）指示是否想要在此配置文件的分配中包含任何 **Exclusions**（排除）。如果选择 **Yes**（是），则显示 **Excluded Groups**（排除组）字段，让您可以选择希望从此配置文件分配中排除的智能组。
9. （可选）如果启用 **Install only on devices inside selected areas**（仅在选定区域安装设备）选项，则配置文件只能安装在指定地理围栏或 iBeacon 区域内的端点上。出现提示时，在 **Assigned Geofence Areas**（分配的地理围栏区域）字段内添加地理围栏或 iBeacon 区域。
10. （可选）如果 **Enable Scheduling and install only during selected time periods**（仅在选定时间段内启动计划和安装），则可以在配置文件安装时应用时间表（**Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles Settings**（配置文件设置）> **Time Schedules**（时间表）），这将限制配置文件在端点上进行安装的时间段。出现提示时，在 **Assigned Schedules**（分配的计划）字段内输入计划名称。
11. （可选）选择想要从所有端点删除配置文件的 **Removal Date**（删除日期）。

© 2019 Palo Alto Networks, Inc.



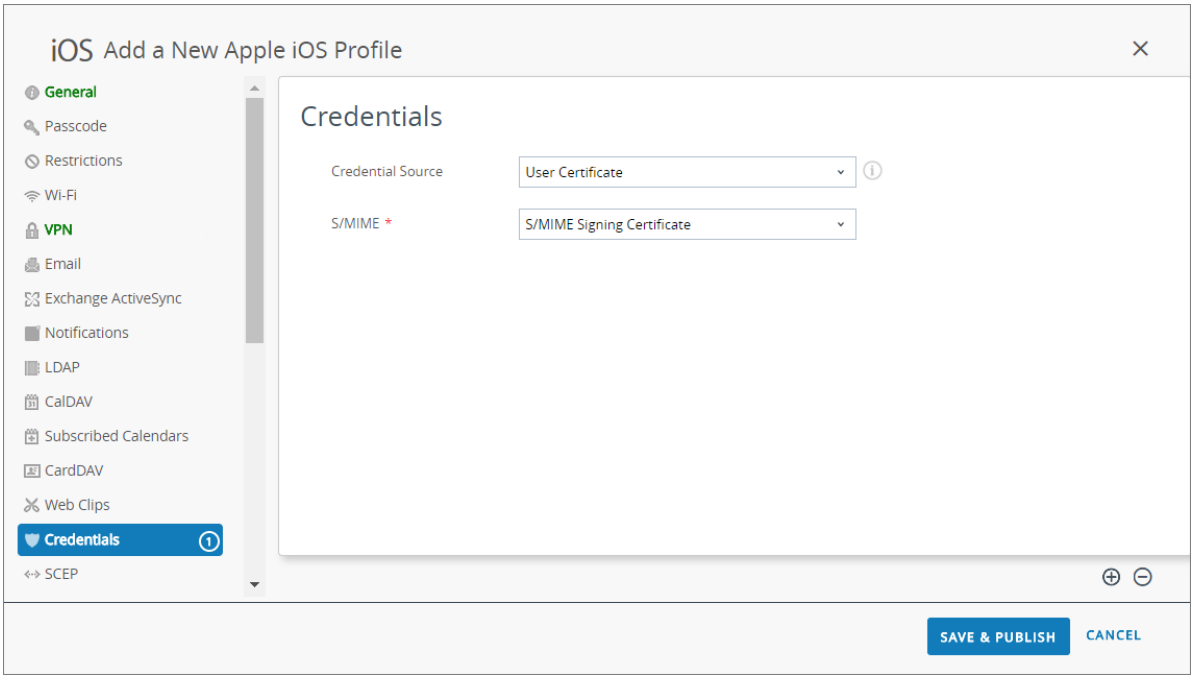
© 2019 Palo Alto Networks, Inc.

STEP 4 | 配置 **Credentials**（凭据）设置：

iOS 端点上所有远程访问 *VPN* 配置均需要基于证书的身份验证。

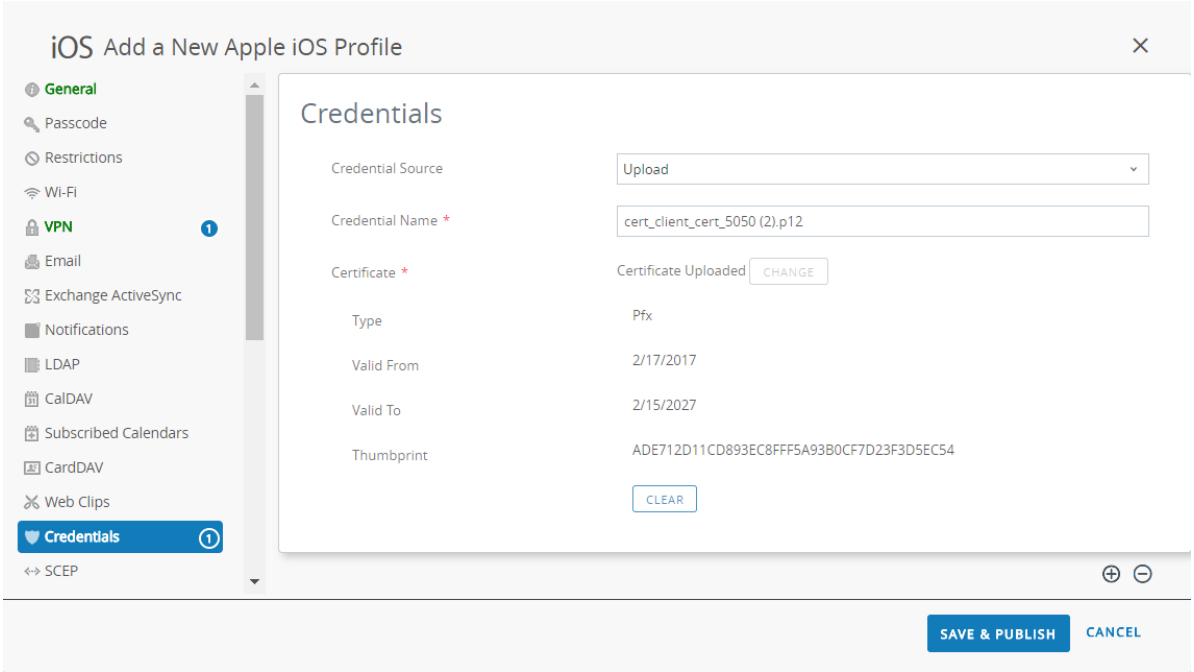
从 *iOS 12* 开始，如果要将客户端证书用于 *GlobalProtect* 客户端身份验证，则必须将客户端证书部署为从 *MDM* 服务器推送的 *VPN* 配置文件组成部分。如果使用任何其他方法从 *MDM* 服务器部署客户端证书，则 *GlobalProtect* 应用将无法使用此证书。

- 要从 AirWatch 用户中提取客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **User Certificate**（用户证书）。
  2. 选择 **S/MIME Signing Certificate**（**S/MIME** 签名证书）（默认）。



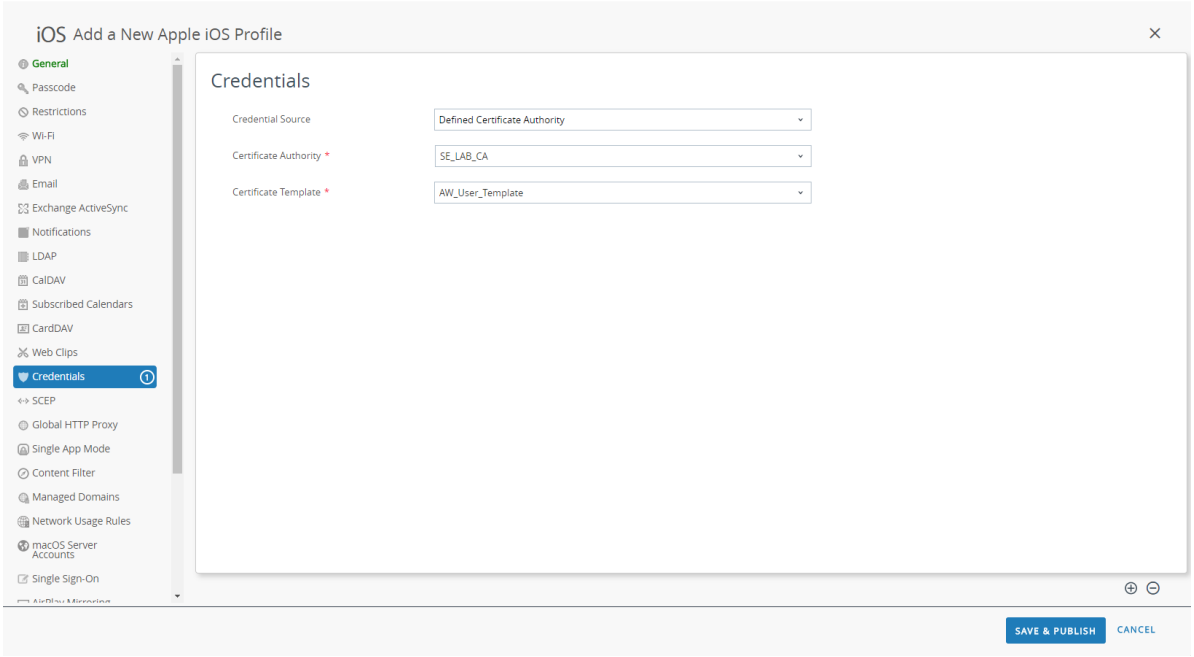
- 要手动上传客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **Upload**（上传）。
  2. 输入 **Credential Name**（凭据名称）。
  3. 单击 **UPLOAD**（上传），找到并选定想要上传的证书。
  4. 证书选定后，单击 **SAVE**（保存）。

© 2019 Palo Alto Networks, Inc.



- 要使用预定义证书颁发机构和模板：
  1. 设置 **Credential Source**（凭据来源）为 **Defined Certificate Authority**（定义的证书颁发机构）。
  2. 选择想要从其获取证书的 **Certificate Authority**（证书颁发机构）。
  3. 选择用于证书颁发机构的 **Certificate Template**（证书模板）。

© 2019 Palo Alto Networks, Inc.

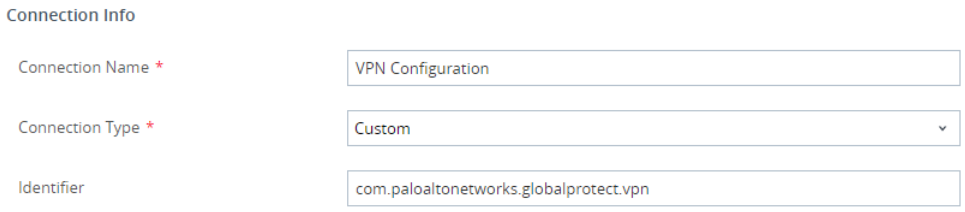


© 2019 Palo Alto Networks, Inc.

STEP 5 | 配置 VPN 设置：

1. 输入端点显示的 **Connection Name**（连接名称）。
2. 选择网络 **Connection Type**（连接类型）：
   - 对于 4.1.x 及更低版本的 GlobalProtect 应用，请选择 **Palo Alto Networks GlobalProtect**。
   - 对于 5.0 及更高版本的 GlobalProtect 应用，请选择 **Custom**（自定义）。
3. （可选）如果将 **Connection Type**（连接类型）设置为 **Custom**（自定义），则在 **Identifier**（标识符）字段内输入以下绑定 ID (**com.paloaltonetworks.globalprotect.vpn**) 以识别 GlobalProtect 应用程序。

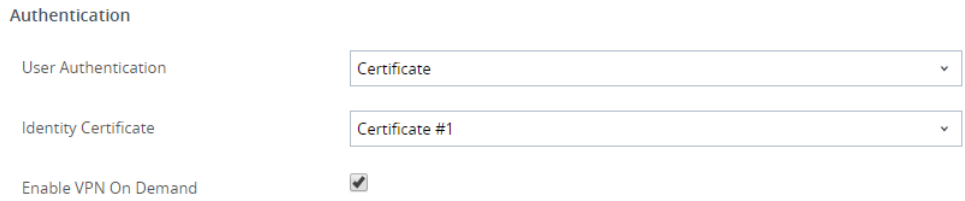
   如果您直接从中国版 *Apple App Store* 下载了 *GlobalProtect* 应用程序，请在 *Identifier*（标识符）字段内输入绑定 *ID* ***(com.paloaltonetworks.globalprotect.vpncn)***。



4. 在 **Server**（服务器）字段中，输入用户要连接的 GlobalProtect 门户的主机名或 IP 地址。
5. （可选）输入 VPN **Account**（账户）的用户名，单击 **+** 按钮查看您可插入的支持查找值。
6. （可选）在 **Disconnect on idle**（闲置时断开连接）字段中，指定在 GlobalProtect 应用停止通过 VPN 隧道路由流量后，端点从此应用注销所花费的时间（秒）。
7. 在身份验证区域，设置用户 **Authentication**（身份验证）方法为 **Certificate**（证书）。

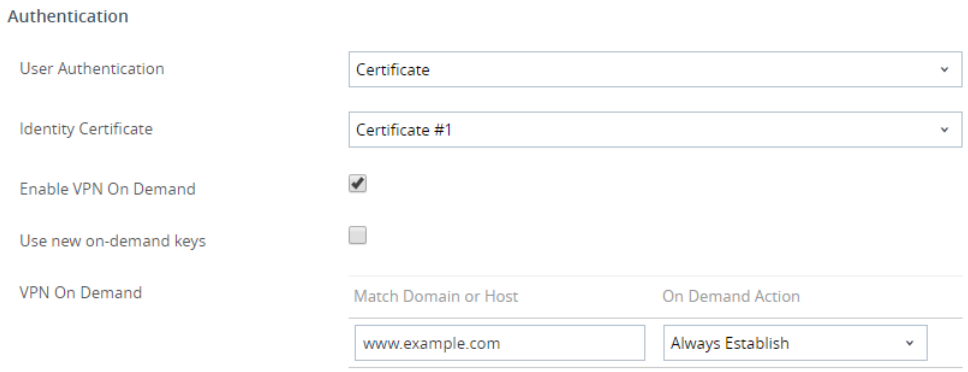
   iOS 端点上所有远程访问 VPN 配置均需要基于证书的身份验证。

8. 出现提示时，输入 GlobalProtect 用于验证用户身份的 **Identity Certificate**（身份证书）。**Identity Certificate**（身份证书）与您在 **Credentials**（凭据）设置内配置的证书一致。
9. 必须启用 **Enable VPN On Demand**（按需启用 **VPN**）（默认设置）。

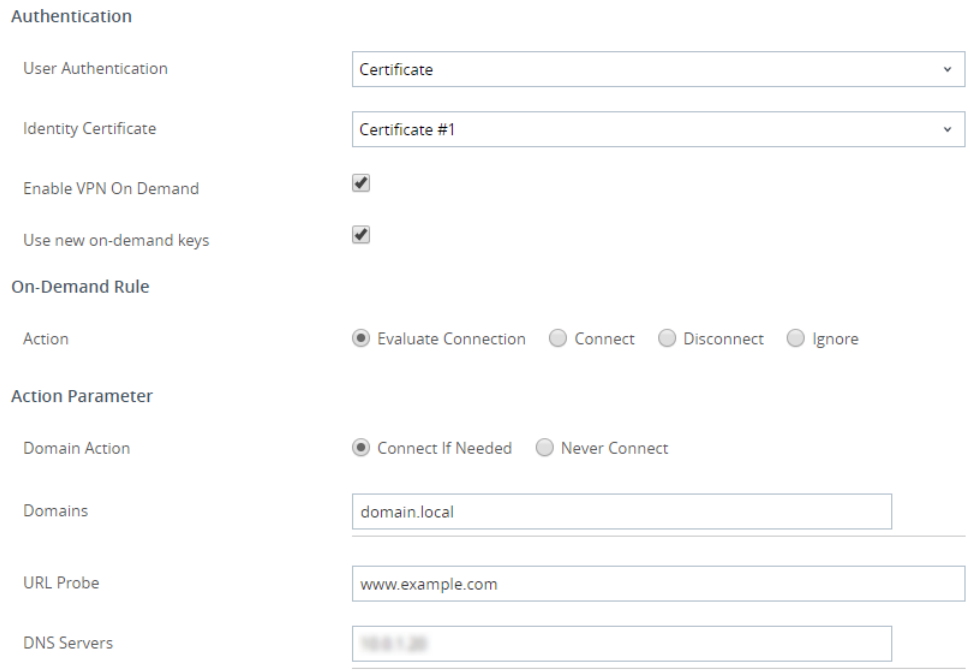


10. （可选）配置旧版 **VPN On-Demand**（按需 **VPN**）连接规则：
    - **Match Domain or Host**（匹配域或主机）— 输入在用户访问时可触发 GlobalProtect 建立连接的域或主机名。
    - **On Demand Action**（按需操作）— 设置 **On Demand Action**（按需操作）为**Establish if Needed**（必要时建立）或 **Always Establish**（始终建立），以便仅在用户无法直接访问指定域或主机名时建立 GlobalProtect 连接。设置 **On Demand Action**（按需操作）为**Never Establish**（从不建立），防止在用户访问特定域或主机名时建立 GlobalProtect 连接。如果连接已经就绪，则可以继续使用。

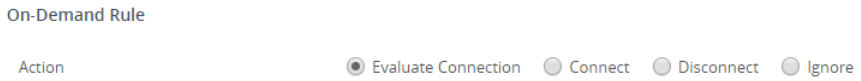
© 2019 Palo Alto Networks, Inc.



11. （可选）启用 GlobalProtect 应用为 **Use new on-demand keys**（使用新的按需表项），以设置更精细的按需连接规则。可以通过单击 **ADD RULE**（添加规则）添加多个规则。



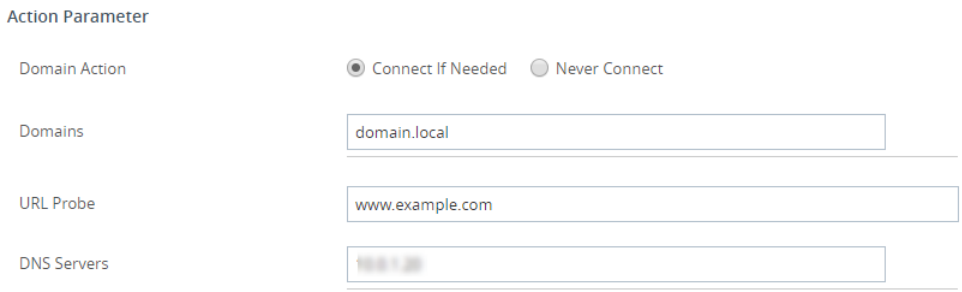
- 在按需规则区域，根据定义的条件选择适用于 GlobalProtect 连接的 **Action**（操作）：
  - **Evaluate Connection**（评估连接）— 根据网络和连接设置自动建立 GlobalProtect 连接。每当用户尝试连接到域时，都会进行评估。
  - **Connect**（连接）— 自动建立 GlobalProtect 连接。
  - **Disconnect**（断开连接）— 自动禁用 GlobalProtect，并阻止 GlobalProtect 重新建立连接。
  - **Ignore**（忽略）— 保留现有 GlobalProtect 连接，并在断开后阻止 GlobalProtect 重新建立连接。



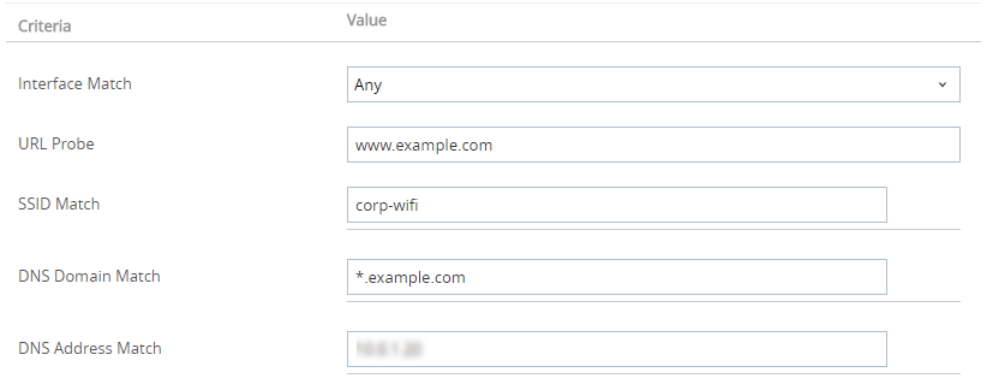
- （可选）如果将按需连接规则的 **Action**（操作）设置为 **Evaluate Connection**（评估连接），则还必须配置操作参数，以便在连接评估时，如果域名解析失败，指定 GlobalProtect 是否能够尝试重新建立连接（例如，如果 DNS 服务器由于超时而无法响应）。可以通过单击 **ADD ACTION PARAMETERS**（添加操作参数）添加多个参数。

© 2019 Palo Alto Networks, Inc.

- 设置 **Domain Action**（域操作）为 **Connect if Needed**（必要时连接），以启用 GlobalProtect 重新建立连接，或是 **Never Connect**（从不连接），以阻止 GlobalProtect 重新建立连接。
- 输入使用此 **Action Parameter**（操作参数）的 **Domains**（域）。
- （可选）如果设置 **Domain Action**（域操作）为 **Connect if Needed**（必要时连接），则输入想在 **URL Probe**（**URL** 探测）字段中探测的 HTTP 或 HTTPS URL。如果无法解析 URL 主机名，则无法访问服务器，或是如果服务器无法响应 200 HTTP 状态代码，则建立 GlobalProtect 连接。
- （可选）如果设置 **Domain Action**（域操作）为 **Connect if Needed**（必要时连接），则输入用于解析指定**Domains**（域）的 **DNS Servers**（**DNS** 服务器）IP 地址（内部或可信外部）。如果无法访问 DNS 服务器，则建立 GlobalProtect 连接。



- 配置可匹配按需连接规则的下列条件。如果端点匹配所有指定条件，则按需连接规则适用于此端点。
  - **Interface Match**（接口匹配）— 指定可匹配端点网络适配器的连接类型：**Any**（任何）、**Ethernet**、**Wi-Fi**、**Cellular**。
  - **URL Probe**（**URL** 探测）— 输入要匹配的 HTTP 或 HTTPS URL。如果匹配成功，则返回 200 HTTP 状态代码。
  - **SSID Match**（**SSID** 匹配）— 输入要匹配的网络 SSID。可以通过单击添加 (+) 按钮添加多个网络 SSID。要匹配成功，端点必须至少与一个指定网络 SSID 相匹配。
  - **DNS Domain Match**（**DNS** 域匹配）— 输入要匹配的 DNS 搜索域。此外，还可以匹配包含所有子域的通配符记录（例如 `*.example.com`）。
  - **DNS Address Match**（**DNS** 地址匹配）— 输入要匹配的 DNS 服务器 IP 地址。可以通过单击添加 (+) 按钮添加多个 DNS 服务器 IP 地址。此外，还可以匹配包含所有不带 IP 地址的 DNS 服务器的单个通配符记录（例如 `17.*`）。要匹配成功，端点上列出的所有 DNS 服务器 IP 地址必须匹配指定的 DNS 服务器 IP 地址。



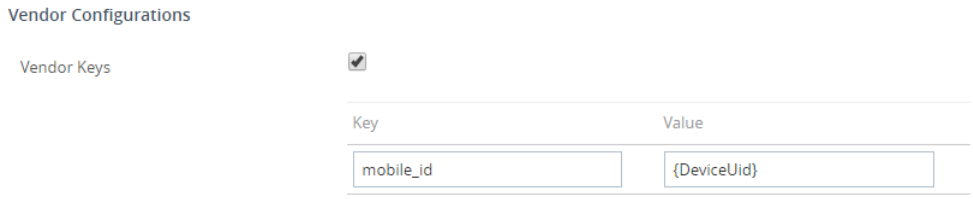
12. （可选）选择 **Proxy**（代理）类型，并配置相关设置。

STEP 6 | （可选）（从 5.0 版本的 GlobalProtect 应用开始）如果 GlobalProtect 配置需要 HIP 与 MDM 集成，则指定唯一设备标识符 (UDID) 属性。

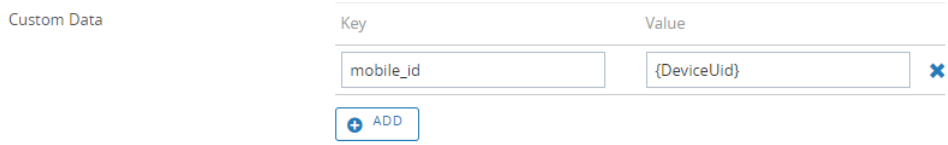
© 2019 Palo Alto Networks, Inc.

GlobalProtect 支持与 MDM 集成，以从 MDM 服务器获取用于基于 HIP 的策略实施的移动设备属性。为了让 GlobalProtect 集成起作用，GlobalProtect 应用必须向 GlobalProtect 网关展示端点 UDID。GlobalProtect 应用可通过 UDID 属性检索并使用基于 MDM 的部署中的 UDID 信息。若要从配置文件中删除 UDID 属性，则可以不再使用 MDM 集成。GlobalProtect 应用生成新的 UDID，但此 UDID 不能用于集成。

- 如果使用 **Palo Alto Networks GlobalProtect** 网络 **Connection Type**（连接类型），则前往 **VPN** 设置，并启用供应商配置区域的 **Vendor Keys**（供应商表项）。设置 **Key**（表项）为 **`mobile_id`**，**Value**（值）设置为 **`{DeviceUid}`**。



- 如果使用 **Custom**（自定义）网络 **Connection Type**（连接类型），则前往 **VPN** 设置，并在连接信息区域内 **ADD**（添加）**Custom Data**（自定义数据）。设置 **Key**（表项）为 **`mobile_id`**，**Value**（值）设置为 **`{DeviceUid}`**。



STEP 7 | **SAVE & PUBLISH**（保存并发布）更改。

使用 *AirWatch* 为 *Windows 10 UWP* 端点配置用户发起远程访问 *VPN* 配置

在远程访问（按需）VPN 配置中，用户必须手动启动应用，以建立安全的 GlobalProtect 连接。应仅在用户发起并建立连接后通过 VPN 隧道路由与 GlobalProtect 网关上配置的特定筛选条件（端口和 IP 地址等）相匹配的流量。

由于 *AirWatch* 并不将 *GlobalProtect* 列为 *Windows* 端点的官方连接提供程序，所以您必须选择备用 *VPN* 提供程序，编辑 *GlobalProtect* 应用设置，并按照下列工作流所述将配置导回 *VPN* 配置文件。

要使用 AirWatch 为 Windows 10 UWP 端点配置用户发起远程访问 VPN 配置，请按以下步骤操作：

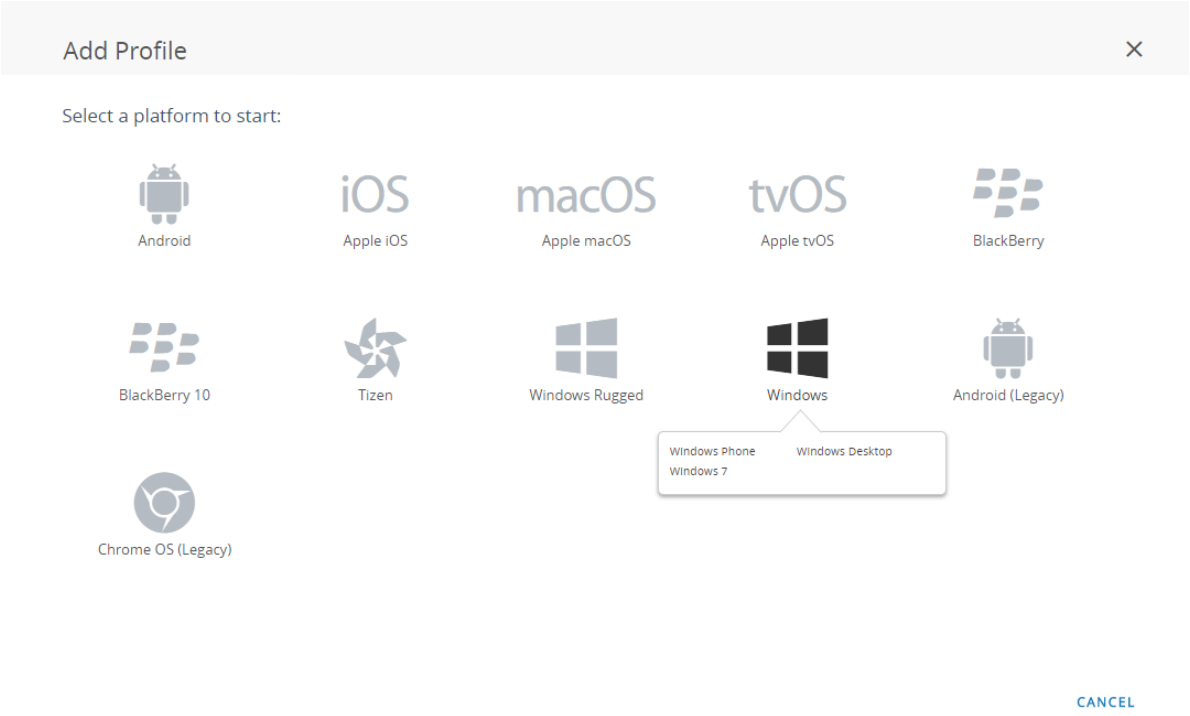
STEP 1 | 下载 GlobalProtect Windows 10 UWP 应用：

- 使用 AirWatch 部署 GlobalProtect 移动应用。
- 用户还可直接从 Microsoft Store 下载 GlobalProtect 应用。

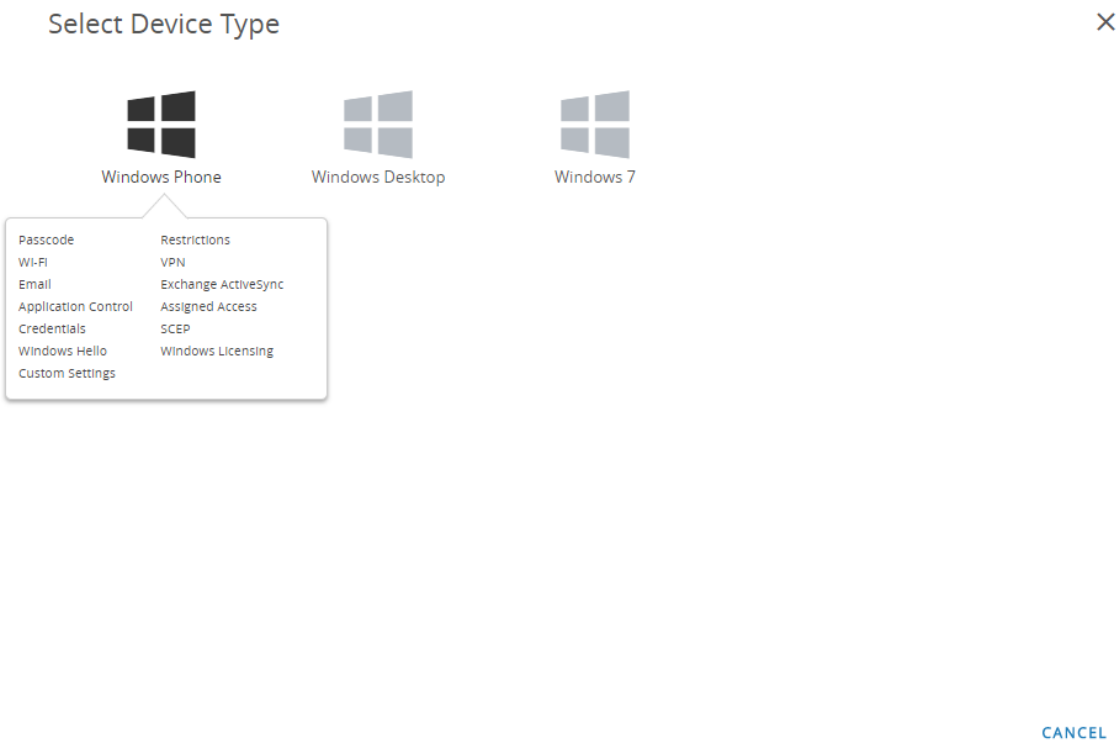
STEP 2 | 从 AirWatch 控制台，修改现有 Windows 10 UWP 配置文件，或添加新的配置文件。

1. 选择 **Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件），然后 **ADD**（添加）新配置文件。
2. 选择 **Windows** 作为平台，**Windows Phone** 作为设备类型。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.



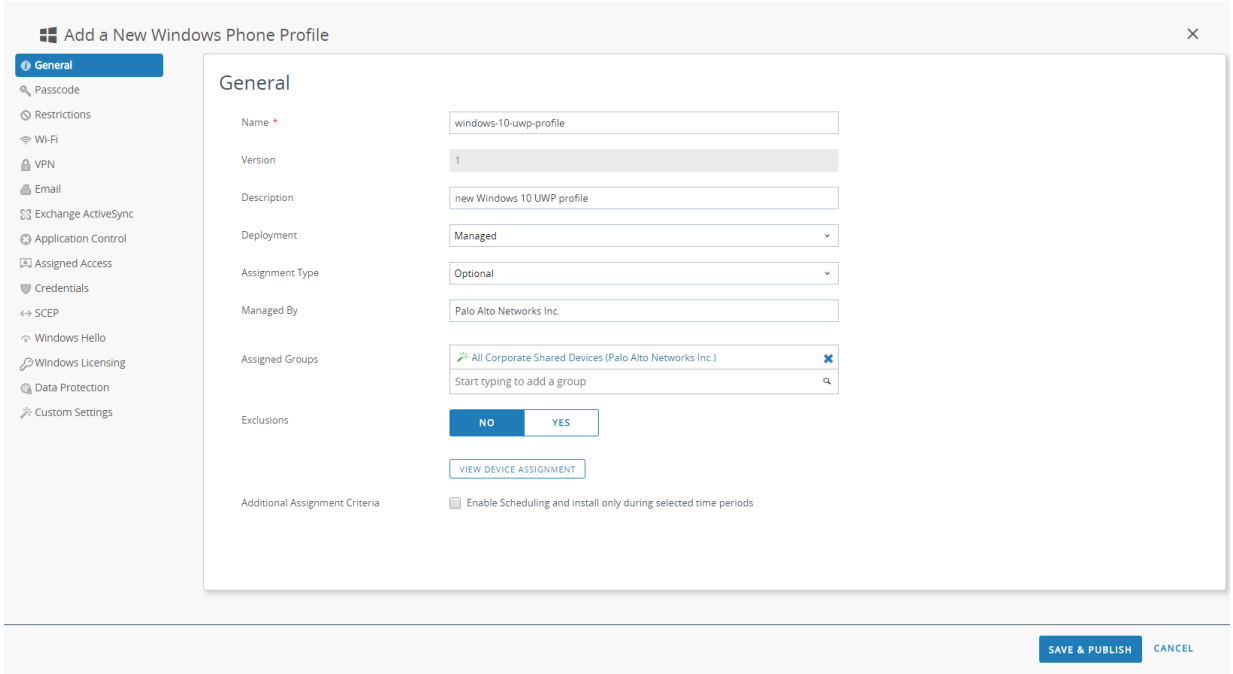
STEP 3 | **配置General（常规）设置：**

1. 输入配置文件的 **Name**（名称）。
2. （可选）输入指定配置文件用途的简短**Description**（说明）。
3. （可选）设置 **Deployment**（部署）方法为 **Managed**（受管理），以便在取消注册时自动删除配置文件。
4. （可选）选择 **Assignment Type**（分配类型）以决定如何将配置文件部署到端点。选择 **Auto**（自动）以自动将配置文件部署到所有终端，选择 **Optional**（可选）使最终用户能够从自助服务门户 (SSP) 安装配置文件或手动将配置文件部署到单个端点，或者选择 **Compliance**（合规）以在最终用户违反适用于该端点的合规性策略时部署该配置文件。
5. （可选）在 **Managed By**（管理者）字段中，输入具有配置文件管理权限的组织组。

© 2019 Palo Alto Networks, Inc.

6. （可选）在 **Assigned Groups**（分配组）字段中，添加想要为其添加配置文件的智能组。此字段包含一个创建新智能组的选项，智能组可使用最低 OS 版本、设备型号、所有权类别、组织组等的规格进行配置。
7. （可选）指示是否想要在此配置文件的分配中包含任何 **Exclusions**（排除）。如果选择 **Yes**（是），则显示 **Excluded Groups**（排除组）字段，让您可以选择希望从此配置文件分配中排除的智能组。
8. （可选）如果 **Enable Scheduling and install only during selected time periods**（仅在选定时间段内启动计划和安装），则可以在配置文件安装时应用时间表（**Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles Settings**（配置文件设置）> **Time Schedules**（时间表）），这将限制配置文件在端点上进行安装的时间段。出现提示时，在 **Assigned Schedules**（分配的计划）字段内输入计划名称。

© 2019 Palo Alto Networks, Inc.

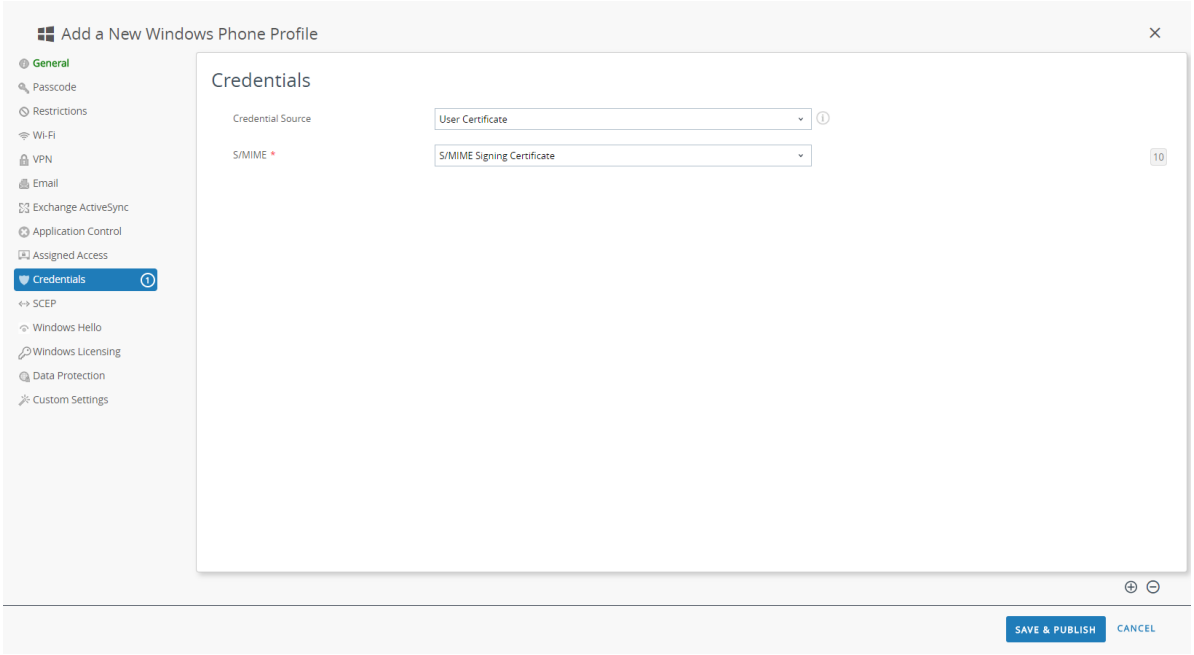


© 2019 Palo Alto Networks, Inc.

STEP 4 | （可选）如果需要客户端证书身份验证才能部署 GlobalProtect，则配置 **Credentials**（凭据）设置：

- 要从 AirWatch 用户中提取客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **User Certificate**（用户证书）。
  2. 选择 **S/MIME Signing Certificate**（**S/MIME** 签名证书）（默认）。

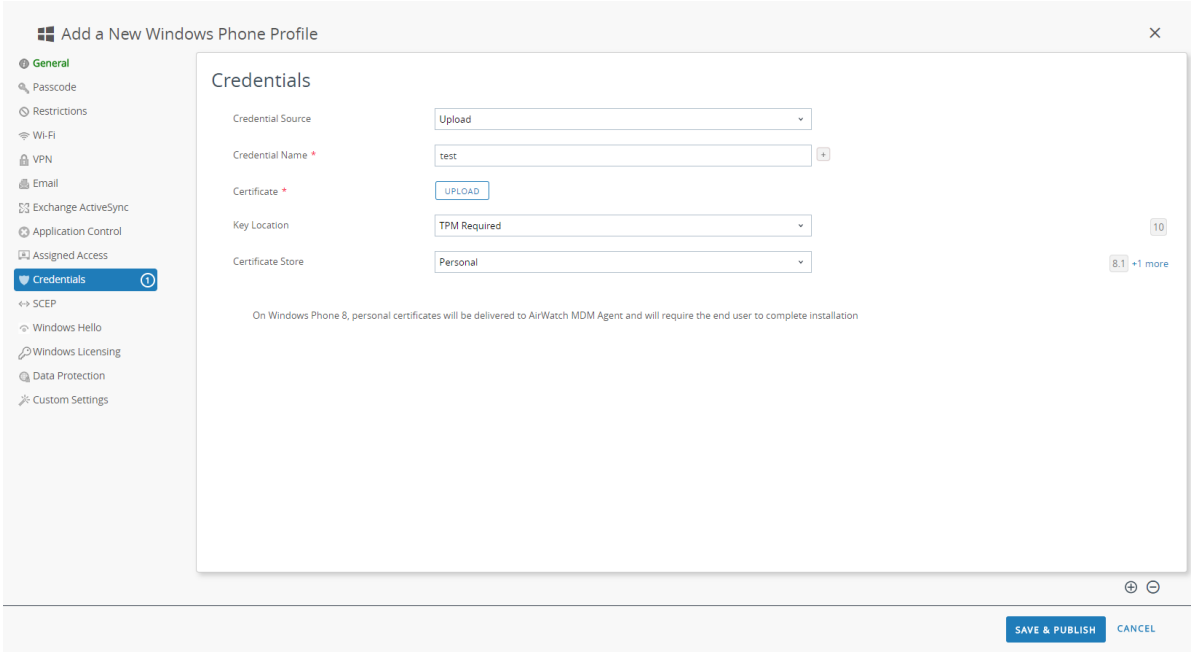
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

- 要手动上传客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **Upload**（上传）。
  2. 输入 **Credential Name**（凭据名称）。
  3. 单击 **UPLOAD**（上传），找到并选定想要上传的证书。
  4. 证书选定后，单击 **SAVE**（保存）。
  5. 选择想要保存证书私钥的 **Key Location**（表项位置）：
     - **TPM Required**（需要 **TPM**）—在可信平台模块中保存私钥。如果端点无可信平台模块，则无法安装私钥。
     - **TPM If Present**（如果存在 **TPM**）—如果端点有可用的可信平台模块，则将私钥保存在其内。如果端点无可信平台模块，则将私钥保存在端点软件内。
     - **Software**（软件）—将私钥保存在端点软件内。
     - **Passport**（通行证）—将私钥保存在 Microsoft 通行证中。要启用此选项，必须在端点上安装 AirWatch Protection Agent 。
  6. 将 **Certificate Store**（证书存储库）设置为 **Personal**（个人）。

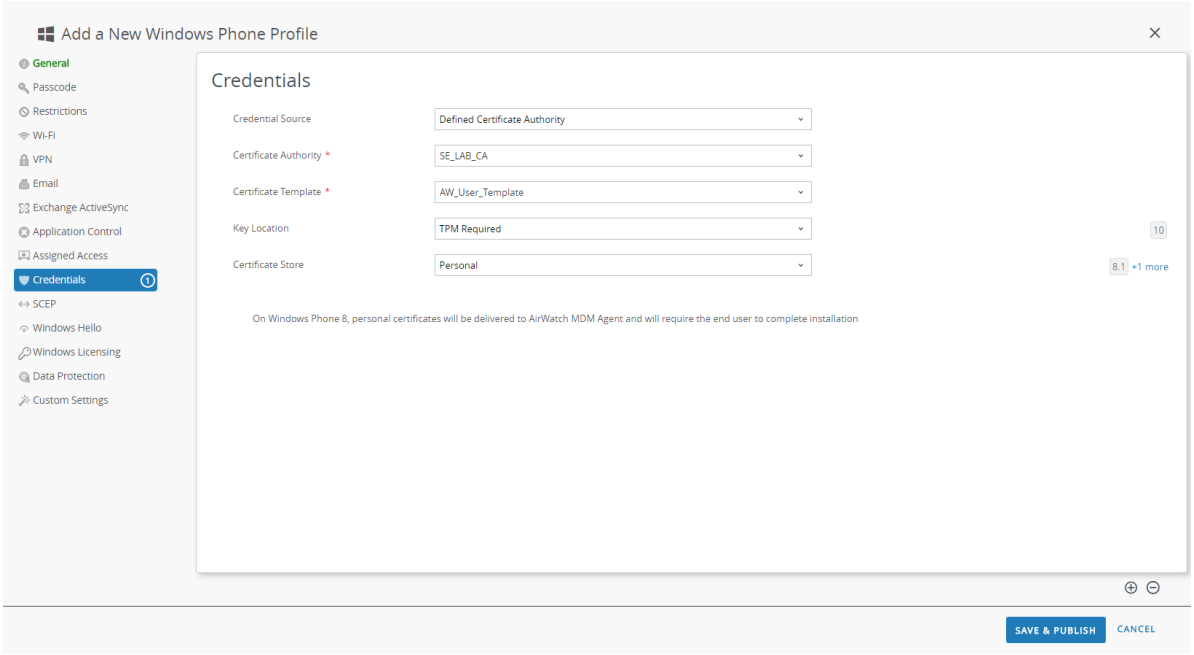
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

- 要使用预定义证书颁发机构和模板：
  1. 设置 **Credential Source**（凭据来源）为 **Defined Certificate Authority**（定义的证书颁发机构）。
  2. 选择想要从其获取证书的 **Certificate Authority**（证书颁发机构）。
  3. 选择用于证书颁发机构的 **Certificate Template**（证书模板）。
  4. 选择想要保存证书私钥的 **Key Location**（表项位置）：
     - **TPM Required**（需要 **TPM**）—在可信平台模块中保存私钥。如果端点无可信平台模块，则无法安装私钥。
     - **TPM If Present**（如果存在 **TPM**）—如果端点有可用的可信平台模块，则将私钥保存在其内。如果端点无可信平台模块，则将私钥保存在端点软件内。
     - **Software**（软件）—将私钥保存在端点软件内。
     - **Passport**（通行证）—将私钥保存在 Microsoft 通行证中。要启用此选项，必须在端点上安装 AirWatch Protection Agent。
  5. 将 **Certificate Store**（证书存储库）设置为 **Personal**（个人）。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

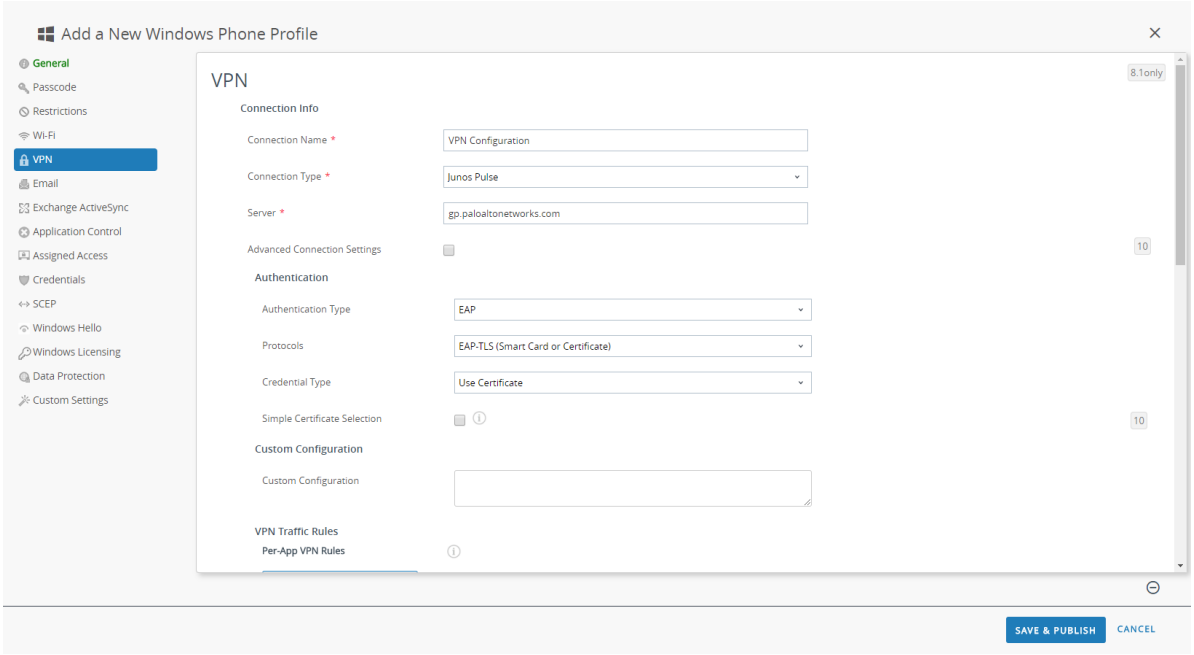
STEP 5 | **配置 VPN 设置：**

1. 输入端点显示的 **Connection Name**（连接名称）。
2. 选择备用提供程序 **Connection Type(连接类型)**（勿选择**IKEv2**、**L2TP**、**PPTP** 或 **Automatic**（自动），因为其没有 GlobalProtect VPN 配置文件所需的相关联供应商设置）。

   必须选择备用供应商，因为 AirWatch 尚未将 GlobalProtect 列为 Windows 端点的官方连接提供程序。

3. 在 **Server**（服务器）字段中，输入用户要连接的 GlobalProtect 门户的主机名或 IP 地址。
4. 在身份验证区域，选择用于指定最终用户身份验证时使用的方法的 **Authentication Type**（身份验证类型）。

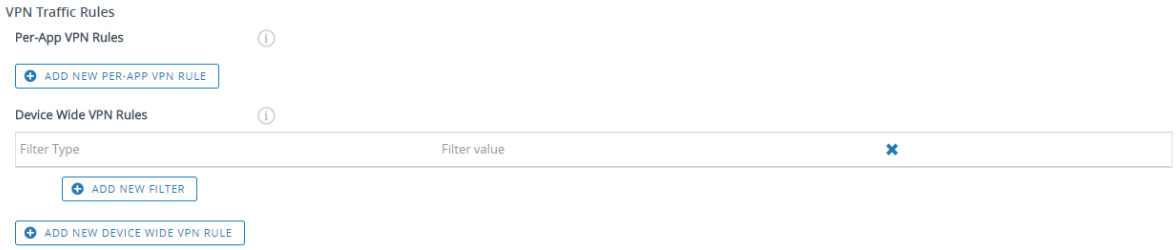
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

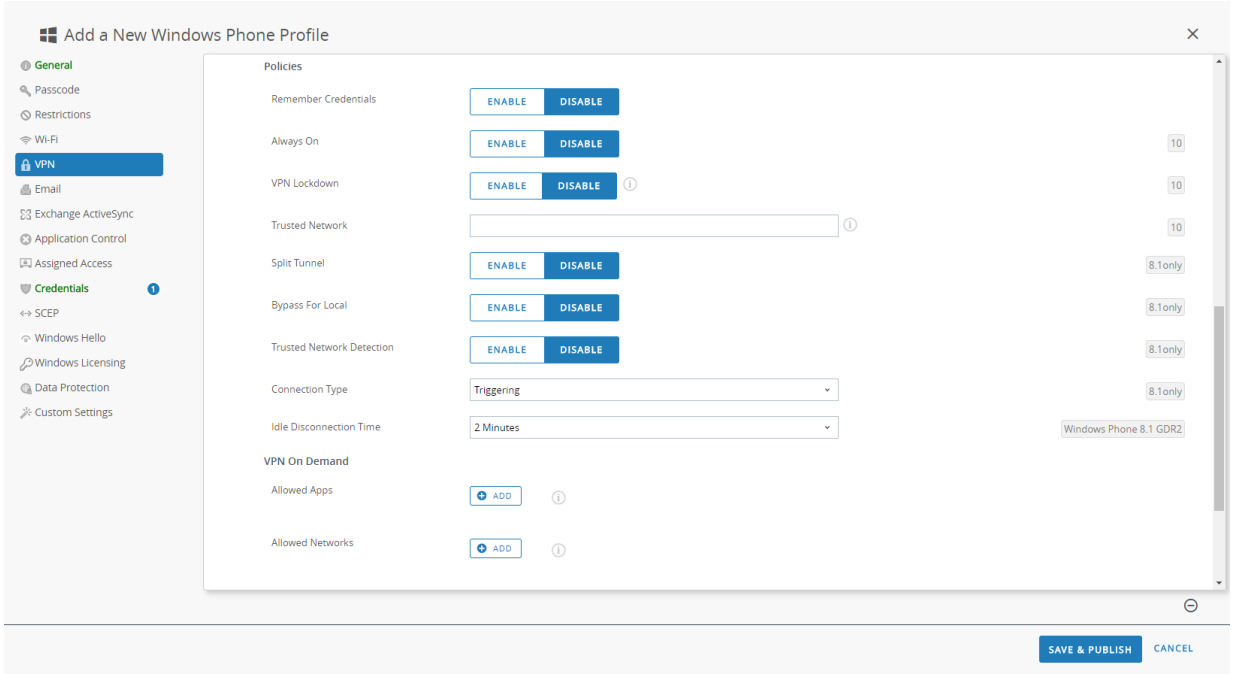
5. （可选）要允许 GlobalProtect 保存用户凭据，请在“策略”区域 **ENABLE**（启用）**Remember Credentials**（记住凭据）选项。
6. （可选）在“VPN 流量规则”区域，**ADD NEW DEVICE WIDE VPN RULE**（添加新设备宽 **VPN** 规则），以通过 VPN 隧道发送与特定路由匹配的流量。这些规则不受应用限制，但可在整个端点进行评估。如果流量与特定匹配条件相匹配，则通过 VPN 隧道进行路由。

   单击 **ADD NEW FILTER**（添加新的筛选条件），添加匹配条件。出现提示时，输入 **Filter Type**（筛选条件类型）和相应的 **Filter Value**（筛选条件值）。



7. 要确保此配置文件使用按需连接方法，则在策略区域配置以下设置：
   - **DISABLE**（禁用）**Always On**（始终打开）。若此字段 **ENABLED**（已启用），则始终打开安全连接。
   - **DISABLE**（禁用）**VPN Lockdown**（**VPN** 锁定）。如果此字段为 **ENABLED**（已启用），则始终打开并连上安全连接，并在应用未连接时禁用网络访问。AirWatch 中的 **VPN Lockdown**（**VPN** 锁定）选项类似于您在 GlobalProtect 门户配置中配置的 **Enforce GlobalProtect for Network Access**（为网络访问强制执行 **GlobalProtect**）。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

STEP 6 | **SAVE & PUBLISH**（保存并发布）更改。

STEP 7 | 要设置连接类型提供程序为 GlobalProtect，请以 XML 格式编辑 VPN 配置文件。

> 要最大程度减少在原始 *XML* 中的额外编辑次数，请在导出配置之前检查 *VPN* 配置文件中的设置。如果在导出 *VPN* 配置文件后需要更改设置，可在原始 *XML* 中进行更改；或者，可更新 *VPN* 配置文件中的设置后重复执行此步骤。

1. 在 **Devices**（设备）> **Profiles**（配置文件）> **List View**（列表视图）中，选择在之前步骤中添加的新配置文件旁的单选按钮，然后选择表格顶部的 **</>XML**。AirWatch 将打开配置文件的 XML 视图。
2. **Export**（导出）配置文件，然后在所选的文本编辑器中打开。
3. 为 GlobalProtect 编辑以下设置：

- 在指定 `PluginPackageFamilyName` 的 `LoclURI` 元素中，将元素更改为：

  ```
  <LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/
  PluginPackageFamilyName</LocURI>
  ```

- 在随后的 `Data` 元素中，将值更改为：

  ```
  <Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>
  ```

1. 保存对所导出配置文件的更改。
2. 返回 AirWatch，选择 **Devices**（设备）> **Profiles**（配置文件）> **List View**（列表视图）。
3. 创建（选择 **Add**（添加）> **Add Profile**（添加配置文件）> **Windows** > **Windows Phone**）并命名新配置文件。
4. 选择 **Custom Settings**（自定义设置）> **Configure**（配置），然后复制粘贴所编辑的配置。
5. **Save & Publish**（保存并发布）更改。

STEP 8 | 要清除原始配置文件，选择 **Devices**（设备）> **Profiles**（配置文件）> **List View**（列表视图），然后选择 **More Actions**（更多操作）> **Deactivate**（停用）。AirWatch 将该配置文件移至非活动列表。

STEP 9 | 测试配置。

使用 **Microsoft Intune** 配置用户发起远程访问 **VPN** 配置

Microsoft Intune 是一种基于云的企业移动性管理平台，使您可以从中心位置管理移动端点。GlobalProtect 应用在防火墙和 Microsoft Intune 受管移动端点之间提供设备级或应用级安全连接。使用 GlobalProtect 作为安全连接，可以持续检查流量，在移动端点上强制实施预防威胁的网络安全策略。

有关如何通过 Microsoft Intune 配置用户发起远程访问 VPN 配置的信息，请参阅以下部分：

- 使用 Microsoft Intune 为 iOS 端点配置用户发起远程访问 VPN 配置

使用 *Microsoft Intune* 为 *iOS* 端点配置用户发起远程访问 *VPN* 配置

在远程访问（按需）VPN 配置中，用户必须手动启动应用，以建立安全的 GlobalProtect 连接。应仅在用户发起并建立连接后通过 VPN 隧道路由与 GlobalProtect 网关上配置的特定筛选条件（端口和 IP 地址等）相匹配的流量。

要使用 Microsoft Intune 为 iOS 端点配置用户发起远程访问 VPN 配置，请遵守以下步骤：

STEP 1 | 下载 GlobalProtect iOS 应用。

- 使用 Microsoft Intune 部署 GlobalProtect 移动应用。
- 用户还可直接从 App Store 下载 GlobalProtect 应用。

STEP 2 | （可选）如果部署需要基于证书的身份验证，则配置证书配置文件。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 创建新的 iOS VPN 配置文件。

- 设置 **Platform**（平台）为 **iOS**。

STEP 4 | 为 iOS 端点配置按需（远程访问）VPN 设置。

- 设置 **Connection type**（连接类型）为 **Palo Alto Networks GlobalProtect**。
- 在 VPN 自动设置区域，启用 **On-demand VPN**（按需 **VPN**），以配置用于控制何时发起 VPN 连接的条件规则。

使用 **MobileIron** 配置用户发起远程访问 **VPN** 配置

MobileIron 是一种企业移动性管理平台，使您可以从中央控制台管理移动端点。GlobalProtect 应用在防火墙和 MobileIron 受管移动端点之间提供设备级或应用级安全连接。使用 GlobalProtect 作为安全连接，可以持续检查流量，在移动端点上强制实施预防威胁的网络安全策略。

有关如何通过 MobileIron 配置用户发起远程访问 VPN 配置的信息，请参阅以下部分：

- 使用 MobileIron 为 iOS 端点配置用户发起远程访问 VPN 配置

使用 *MobileIron* 为 *iOS* 端点配置用户发起远程访问 *VPN* 配置

在远程访问（按需）VPN 配置中，用户必须手动启动应用，以建立安全的 GlobalProtect 连接。应仅在用户发起并建立连接后通过 VPN 隧道路由与 GlobalProtect 网关上配置的特定筛选条件（端口和 IP 地址等）相匹配的流量。

要使用 MobileIron 为 iOS 端点配置用户发起远程访问 VPN 配置，请遵守以下步骤：

STEP 1 | 下载 GlobalProtect iOS 应用。

- 使用 MobileIron 部署 GlobalProtect 移动应用。
- 用户还可直接从 App Store 下载 GlobalProtect 应用。

STEP 2 | 添加证书配置文件，然后配置证书设置。

所有按需 *VNP* 配置均需要基于证书的身份验证。

STEP 3 | 添加按需（远程访问）VPN 配置。

- 设置配置类型为 **VPN On Demand**（按需 **VPN**）。

STEP 4 | 为 iOS 配置按需 VPN 设置。

- 设置 **Connection Type**（连接类型）为 **Palo Alto Networks GlobalProtect**，然后配置相关设置。

每应用 *VPN* 配置

在每应用 VPN 配置中，可指定哪些受管应用可通过 GlobalProtect VPN 隧道发送流量。非受管应用将继续直接连接到互联网，而非 GlobalProtect VPN 隧道。

有关如何通过受支持的移动设备管理系统配置每应用 VPN 配置的信息，请参阅以下部分：

- 使用 AirWatch 配置每应用 VPN 配置
- 使用 Microsoft Intune 配置每应用 VPN 配置
- 使用 MobileIron 配置每应用 VPN 配置

使用 **AirWatch** 配置每应用 **VPN** 配置

AirWatch 是一种企业移动性管理平台，使您可以从中央控制台管理移动端点。GlobalProtect 应用在 AirWatch 受管移动端点和防火墙之间提供设备级或应用级安全连接。使用 GlobalProtect 作为安全连接，可以持续检查流量，在移动端点上强制实施预防威胁的网络安全策略。

© 2019 Palo Alto Networks, Inc.

有关如何通过 AirWatch 配置每应用 VPN 配置的信息，请参阅以下部分：

- 使用 AirWatch 为 iOS 端点配置每应用 VPN 配置
- 使用 AirWatch 为安卓端点配置每应用 VPN 配置
- 使用 AirWatch 为 Windows 10 UWP 端点配置每应用 VPN 配置

使用 *AirWatch* 为 *iOS* 端点配置每应用 *VPN* 配置

使用 AirWatch 配置 GlobalProtect VPN 访问，可从您的受管移动端点上启用对内部资源的访问权限。在每应用 VPN 配置中，可指定哪些受管应用可通过 VPN 隧道路由流量。非受管应用将继续直接连接到 Internet，而非 VPN 隧道。

要使用 AirWatch 为 iOS 端点配置每应用 VPN 配置，请按以下步骤操作：

STEP 1 | 下载 GlobalProtect iOS 应用：

- 使用 AirWatch 部署 GlobalProtect 移动应用。
- 用户还可直接从 App Store 下载 GlobalProtect 应用。

在中国，可从 Apple App Store 获取 *GlobalProtect iOS* 应用程序。

STEP 2 | 从 AirWatch 控制台，修改现有 Apple iOS 配置文件，或添加新的配置文件。

1. 选择 **Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件），然后 **ADD**（添加）新配置文件。
2. 从平台列表选择 **iOS**。

© 2019 Palo Alto Networks, Inc.

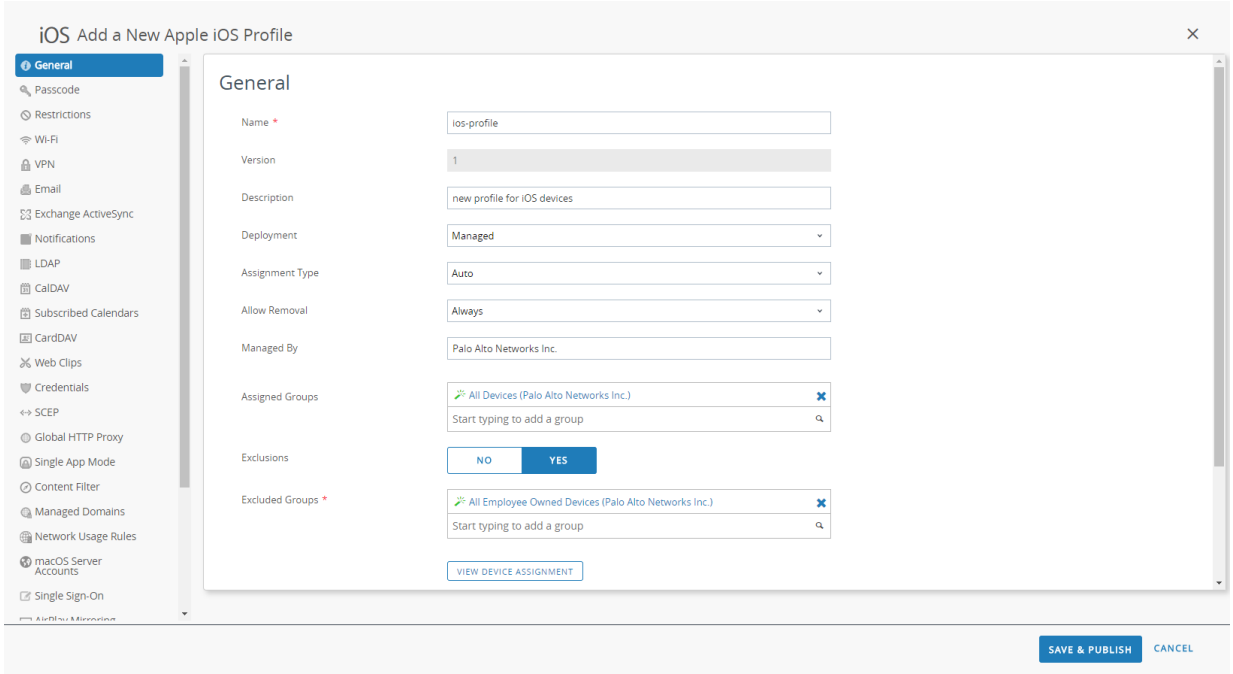
STEP 3 | **配置General（常规）设置：**

1. 输入配置文件的 **Name**（名称）。
2. （可选）输入指定配置文件用途的简短**Description**（说明）。
3. （可选）选择**Deployment**（部署）方法，该方法指示是否在取消注册时自动删除配置文件 —— **Managed**（受管）（删除配置文件）或**Manual**（手动）（配置文件仍保持已安装状态，直至被最终用户删除）。
4. （可选）选择 **Assignment Type**（分配类型）以决定如何将配置文件部署到端点。选择 **Auto**（自动）以自动将配置文件部署到所有终端，选择 **Optional**（可选）使最终用户能够从自助服务门户 (SSP) 安装配置文件或手动将配置文件部署到单个端点，或者选择 **Compliance**（合规）以在最终用户违反适用于该端点的合规性策略时部署该配置文件。

© 2019 Palo Alto Networks, Inc.

5. （可选）选择是否想要最终用户 **Allow Removal**（允许删除）配置文件。选择 **Always**（总是）使最终用户能够随时手动删除配置文件，选择 **Never**（决不）阻止最终用户删除配置文件，或者选择 **With Authorization**（授权）以使最终用户能够在管理员的授权下移除配置文件。选择 **With Authorization**（授权）添加要求的密码。
6. （可选）在 **Managed By**（管理者）字段中，输入具有配置文件管理权限的组织组。
7. （可选）在 **Assigned Groups**（分配组）字段中，添加想要为其添加配置文件的智能组。此字段包含一个创建新智能组的选项，智能组可使用最低 OS 版本、设备型号、所有权类别、组织组等的规格进行配置。
8. （可选）指示是否想要在此配置文件的分配中包含任何 **Exclusions**（排除）。如果选择 **Yes**（是），则显示 **Excluded Groups**（排除组）字段，让您可以选择希望从此配置文件分配中排除的智能组。

© 2019 Palo Alto Networks, Inc.



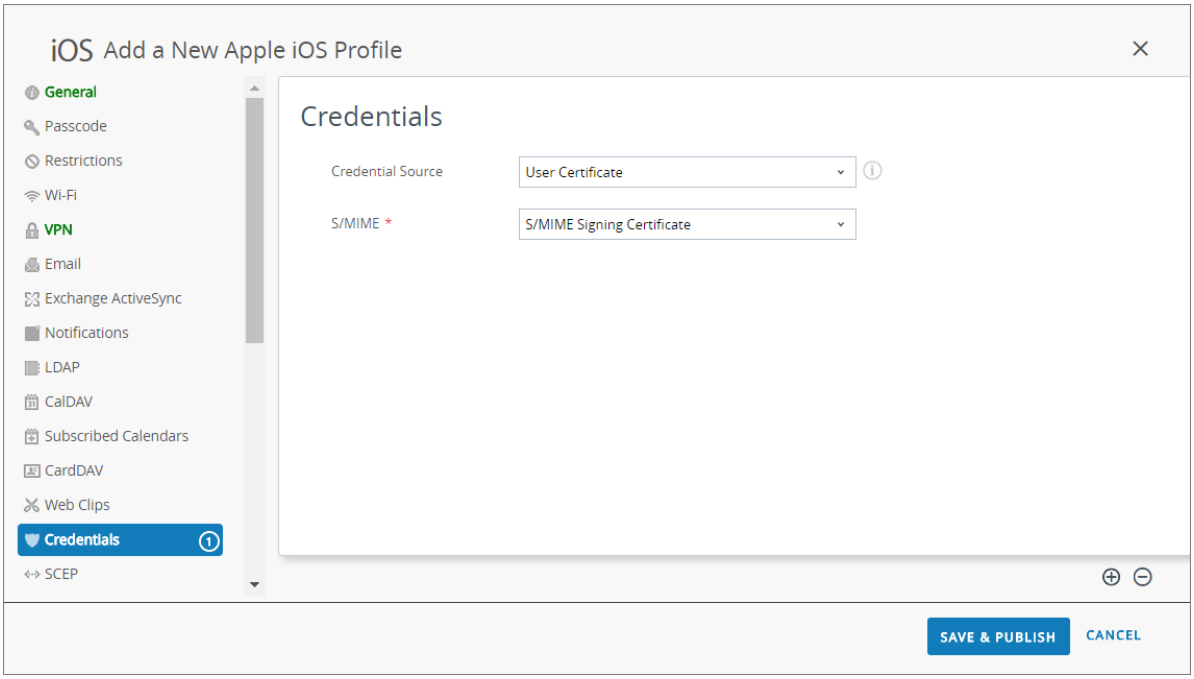
© 2019 Palo Alto Networks, Inc.

STEP 4 | 配置 **Credentials**（凭据）设置：

所有每应用 *VNP* 配置均需要基于证书的身份验证。

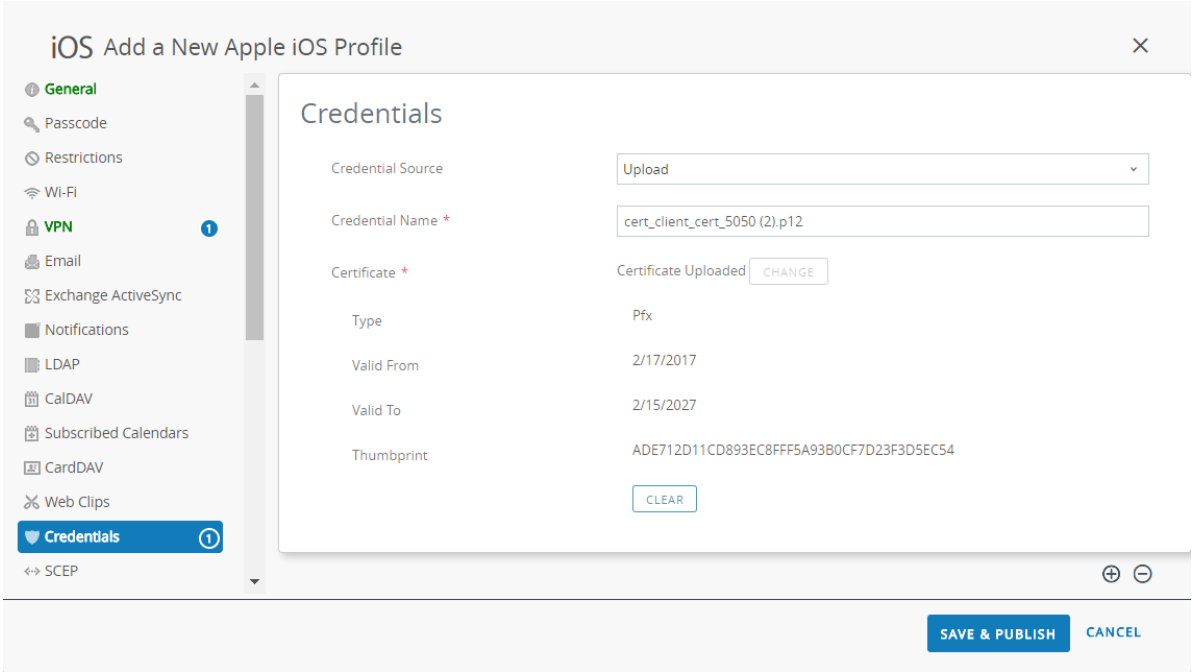
从 *iOS 12* 开始，如果要将客户端证书用于 *GlobalProtect* 客户端身份验证，则必须将客户端证书部署为从 *MDM* 服务器推送的 *VPN* 配置文件组成部分。如果使用任何其他方法从 *MDM* 服务器部署客户端证书，则 *GlobalProtect* 应用将无法使用此证书。

- 要从 AirWatch 用户中提取客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **User Certificate**（用户证书）。
  2. 选择 **S/MIME Signing Certificate**（**S/MIME** 签名证书）（默认）。



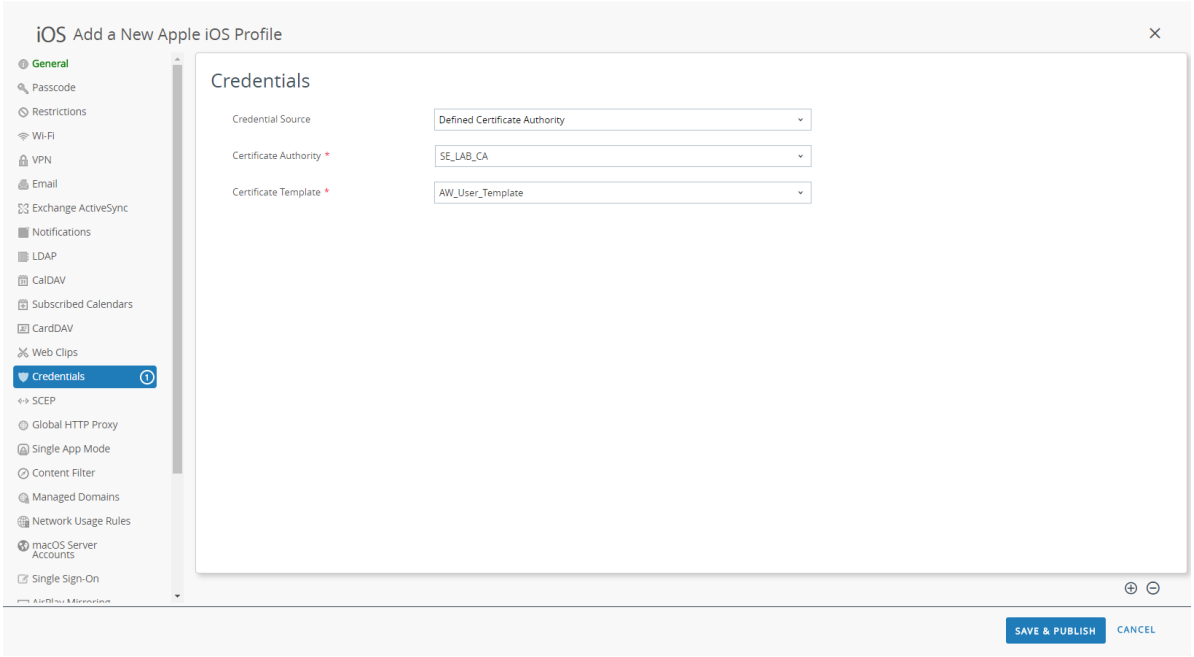
- 要手动上传客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **Upload**（上传）。
  2. 输入 **Credential Name**（凭据名称）。
  3. 单击 **UPLOAD**（上传），找到并选定想要上传的证书。
  4. 证书选定后，单击 **SAVE**（保存）。

© 2019 Palo Alto Networks, Inc.



- 要使用预定义证书颁发机构和模板：
  1. 设置 **Credential Source**（凭据来源）为 **Defined Certificate Authority**（定义的证书颁发机构）。
  2. 选择想要从其获取证书的 **Certificate Authority**（证书颁发机构）。
  3. 选择用于证书颁发机构的 **Certificate Template**（证书模板）。

© 2019 Palo Alto Networks, Inc.

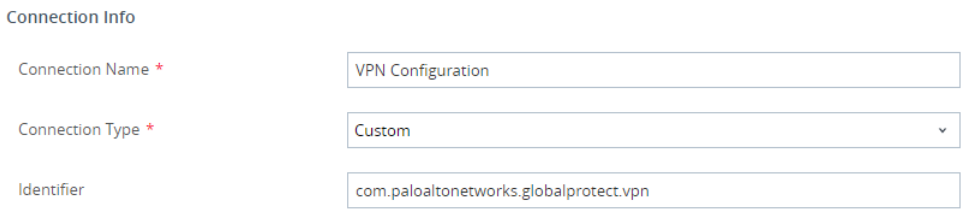


© 2019 Palo Alto Networks, Inc.

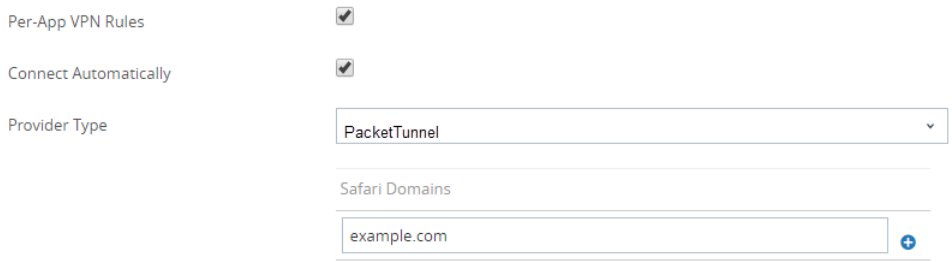
STEP 5 | 配置 VPN 设置：

1. 输入端点显示的 **Connection Name**（连接名称）。
2. 选择网络 **Connection Type**（连接类型）：
   - 对于 4.1.x 及更低版本的 GlobalProtect 应用，请选择 **Palo Alto Networks GlobalProtect**。
   - 对于 5.0 及更高版本的 GlobalProtect 应用，请选择 **Custom**（自定义）。
3. （可选）如果将 **Connection Type**（连接类型）设置为 **Custom**（自定义），则在 **Identifier**（标识符）字段内输入以下绑定 ID (**com.paloaltonetworks.globalprotect.vpn**) 以识别 GlobalProtect 应用程序。

   如果您直接从中国版 *Apple App Store* 下载了 *GlobalProtect* 应用程序，请在 *Identifier*（标识符）字段内输入绑定 *ID* (***com.paloaltonetworks.globalprotect.vpncn***)。



4. 在 **Server**（服务器）字段中，输入用户要连接的 GlobalProtect 门户的主机名或 IP 地址。
5. （可选）输入 VPN **Account**（账户）的用户名，单击 **+** 按钮查看您可插入的支持查找值。
6. （可选）在 **Disconnect on idle**（闲置时断开连接） 字段中，指定在 GlobalProtect 应用停止通过 VPN 隧道路由流量后，端点从此应用注销所花费的时间（秒）。
7. 启用 **Per App VPN**（每应用 **VPN**）将受管应用的所有流量路由通过 GlobalProtect VPN 隧道。
   - 使 GlobalProtect **Connect Automatically**（自动连接）到指定的 **Safari Domains**（**Safari** 域）。可以通过单击添加 (+) 按钮添加多个 **Safari Domains**（**Safari** 域）。
   - 设置 **Provider Type**（提供程序类型），以指示流量如何通过隧道 — 在应用层或 IP 层。使用 PacketTunnel。

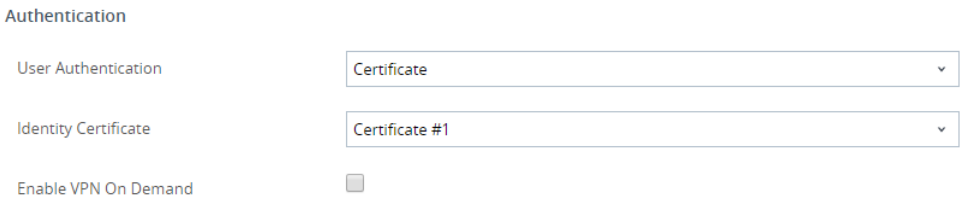


8. 在身份验证区域，设置用户 **Authentication**（身份验证）方法为 **Certificate**（证书）。

   所有每应用 *VNP* 配置均需要基于证书的身份验证。

9. 出现提示时，输入 GlobalProtect 用于验证用户身份的 **Identity Certificate**（身份证书）。**Identity Certificate**（身份证书）与您在 **Credentials**（凭据）设置内配置的证书一致。

© 2019 Palo Alto Networks, Inc.

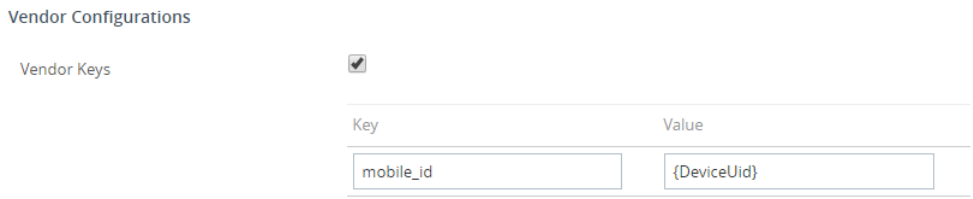


10. （可选）选择 **Proxy**（代理）类型，并配置相关设置。

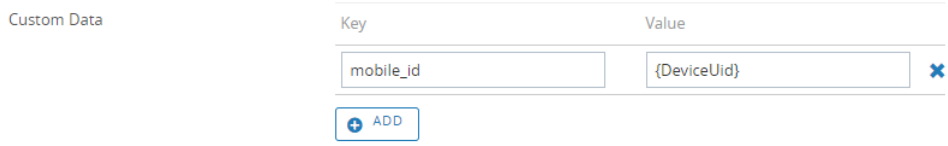
STEP 6 | （可选）（从 5.0 版本的 GlobalProtect 应用开始）如果 GlobalProtect 配置需要 HIP 与 MDM 集成，则指定唯一设备标识符 (UDID) 属性。

GlobalProtect 支持与 MDM 集成，以从 MDM 服务器获取用于基于 HIP 的策略实施的移动设备属性。为了让 GlobalProtect 集成起作用，GlobalProtect 应用必须向 GlobalProtect 网关展示端点 UDID。GlobalProtect 应用可通过 UDID 属性检索并使用基于 MDM 的部署中的 UDID 信息。若要从配置文件中删除 UDID 属性，则可以不再使用 MDM 集成。GlobalProtect 应用生成新的 UDID，但此 UDID 不能用于集成。

- 如果使用 **Palo Alto Networks GlobalProtect** 网络 **Connection Type**（连接类型），则前往 **VPN** 设置，并启用供应商配置区域的 **Vendor Keys**（供应商表项）。设置 **Key**（表项）为 **`mobile_id`**，**Value**（值）设置为 **`{DeviceUid}`**。



- 如果使用 **Custom**（自定义）网络 **Connection Type**（连接类型），则前往 **VPN** 设置，并在连接信息区域内 **ADD**（添加）**Custom Data**（自定义数据）。设置 **Key**（表项）为 **`mobile_id`**，**Value**（值）设置为 **`{DeviceUid}`**。



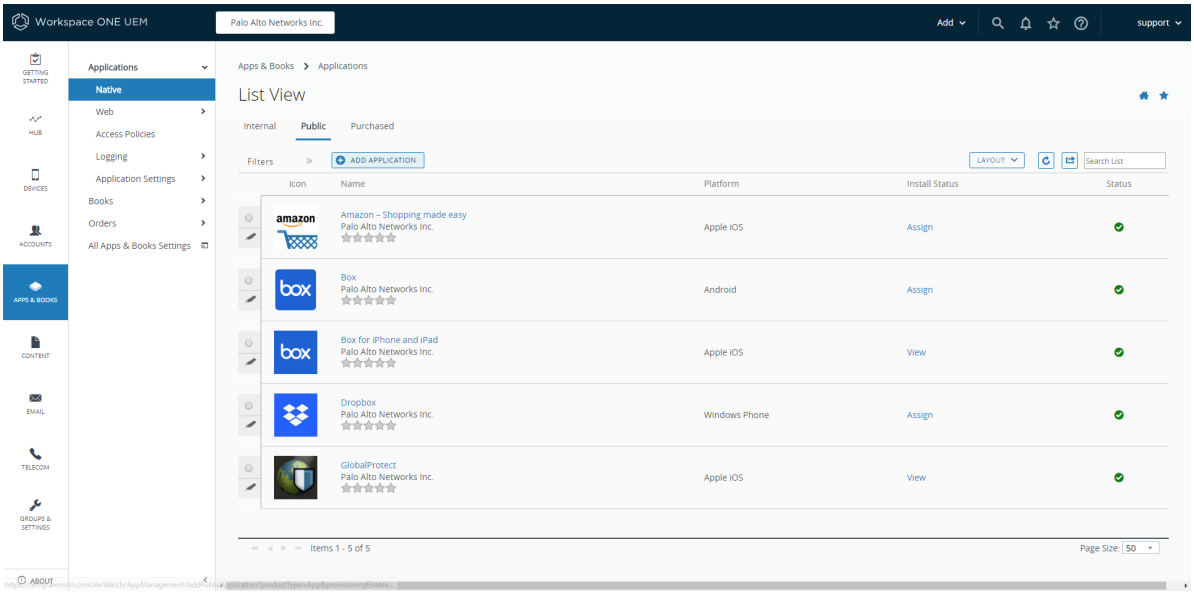
STEP 7 | **SAVE & PUBLISH**（保存并发布）更改。

STEP 8 | 为新的受管应用配置每应用 VPN 设置，或修改已有受管应用的设置。

为应用配置设置并启用每应用 VPN 后，可将此应用发布到一组用户，让此应用通过 GlobalProtect VPN 隧道发送流量。

1. 选择 **APPS & BOOKS**（应用和书籍）> **Applications**（应用）> **Native**（本机）> **Public**（公共）。
2. 要添加新应用，选择 **ADD APPLICATION**（添加应用程序）。要修改已有应用的设置，在公共应用列表（列表视图）中找到应用，然后选择此行旁边的操作菜单中的编辑图标（ ）。

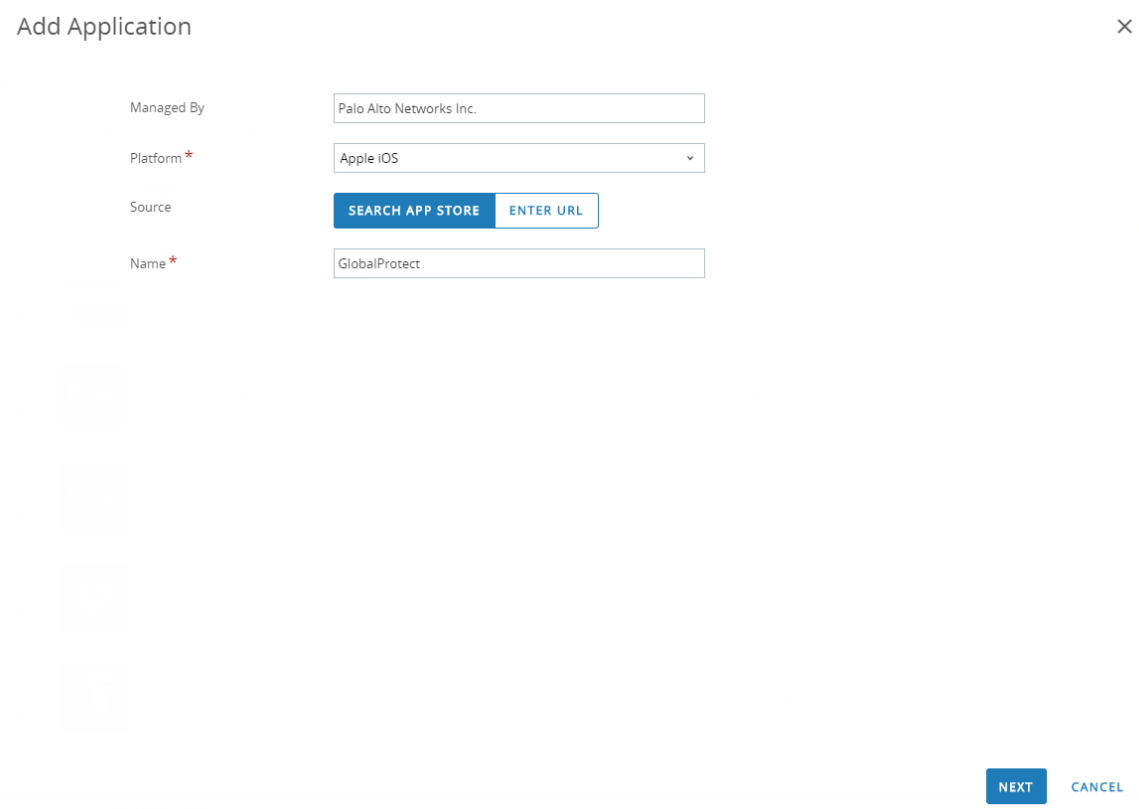
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

3. 在 **Managed By**（管理者）字段中，选择将管理此应用的组织组。
4. 设置 **Platform**（平台）为 **Apple iOS**。
5. 选择用于定位应用的首选 **Source**（来源）：
   - **SEARCH APP STORE**（搜索应用商店）—输入应用 **Name**（名称）。
   - **ENTER URL**（输入 **URL**）—输入此应用的 App Store URL（例如，要添加 Box 应用，输入 https://itunes.apple.com/us/app/box-for-iphone-and-ipad/id290853822?mt=8&uo=4)。

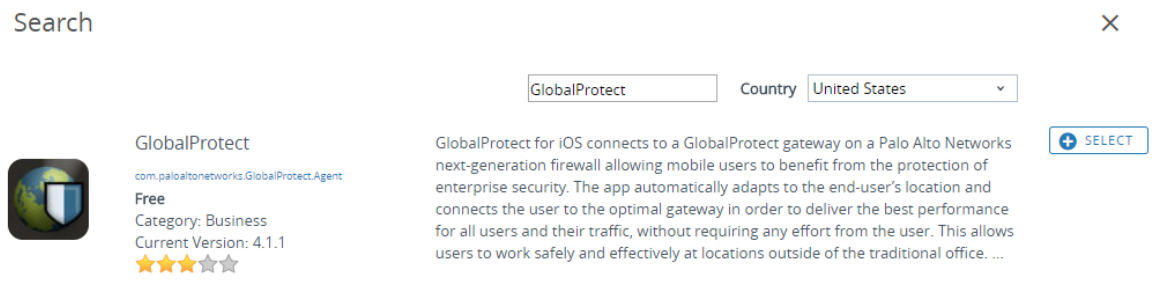
© 2019 Palo Alto Networks, Inc.



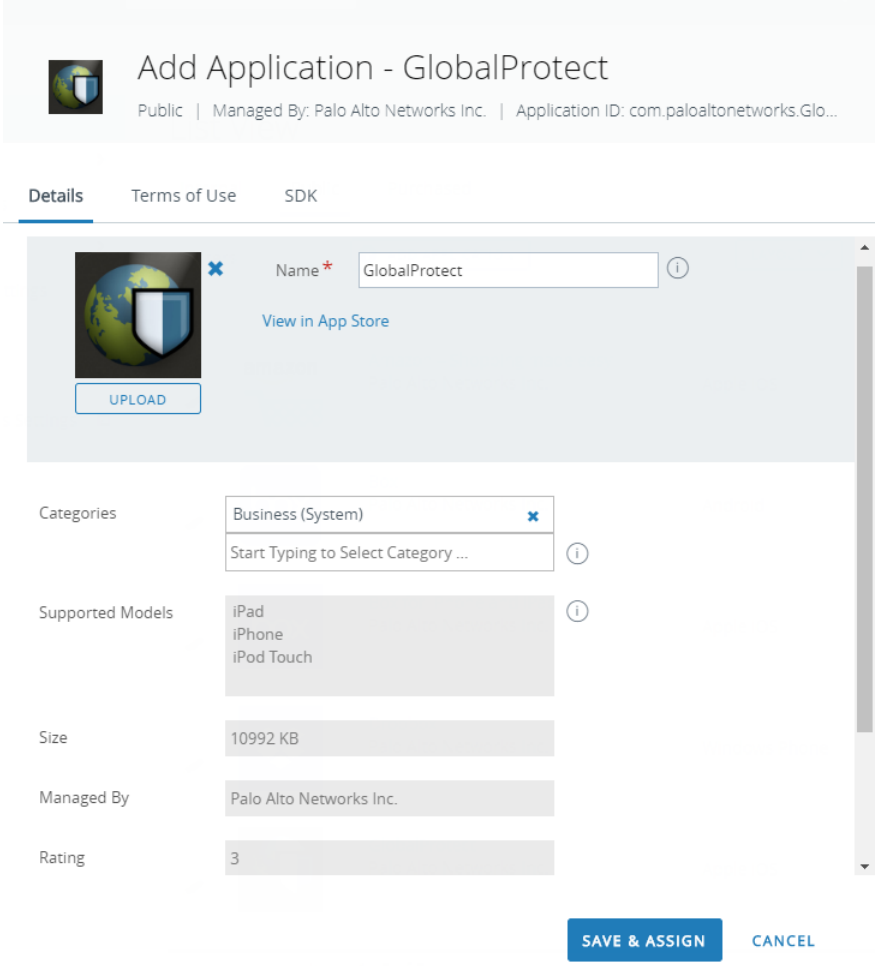
© 2019 Palo Alto Networks, Inc.

6. 单击 **NEXT**（下一步）。

   如果选择搜索 App Store，您还必须从搜索结果列表中 **SELECT**（选择）应用。



7. 在添加应用程序对话框中，应用 **Name**（名称）必须正确。此名称将出现在 AirWatch 应用目录中。
8. （可选）将应用分配到预定义或自定义 **Categories**（类别）中，以便通过 AirWatch 应用目录轻松访问。

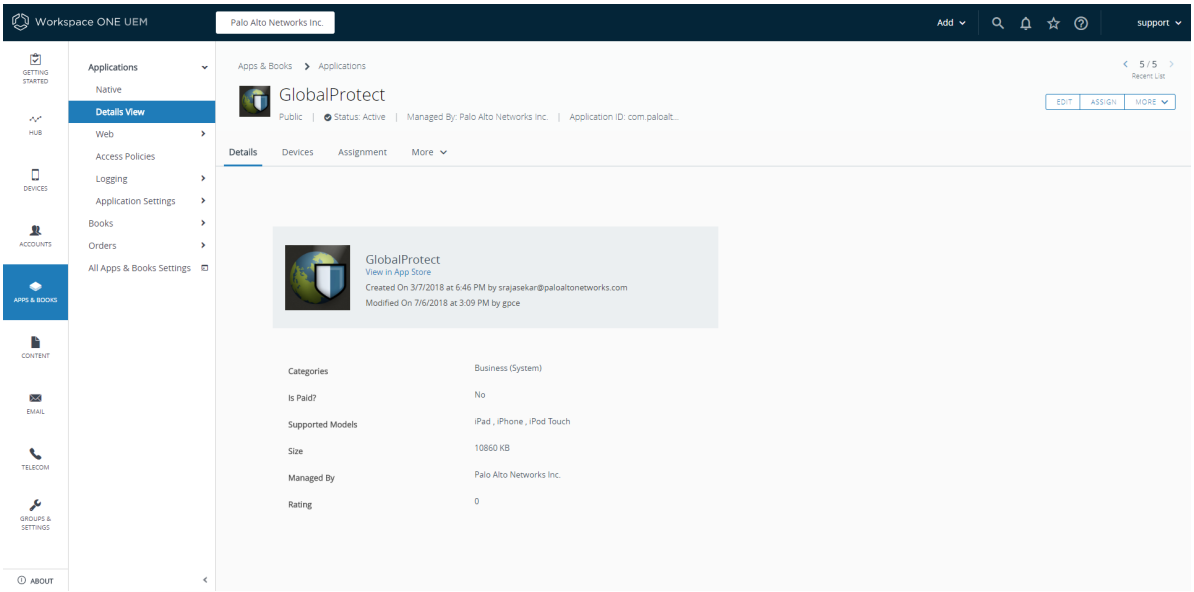


9. **SAVE & ASSIGN**（保存并分配）新应用。

© 2019 Palo Alto Networks, Inc.

10.从公共应用列表（列表视图）中选择新添加的应用。
11.从 **Applications**（应用） > **Details View**（详细视图）中，单击屏幕右上角的 **ASSIGN**（分配）。

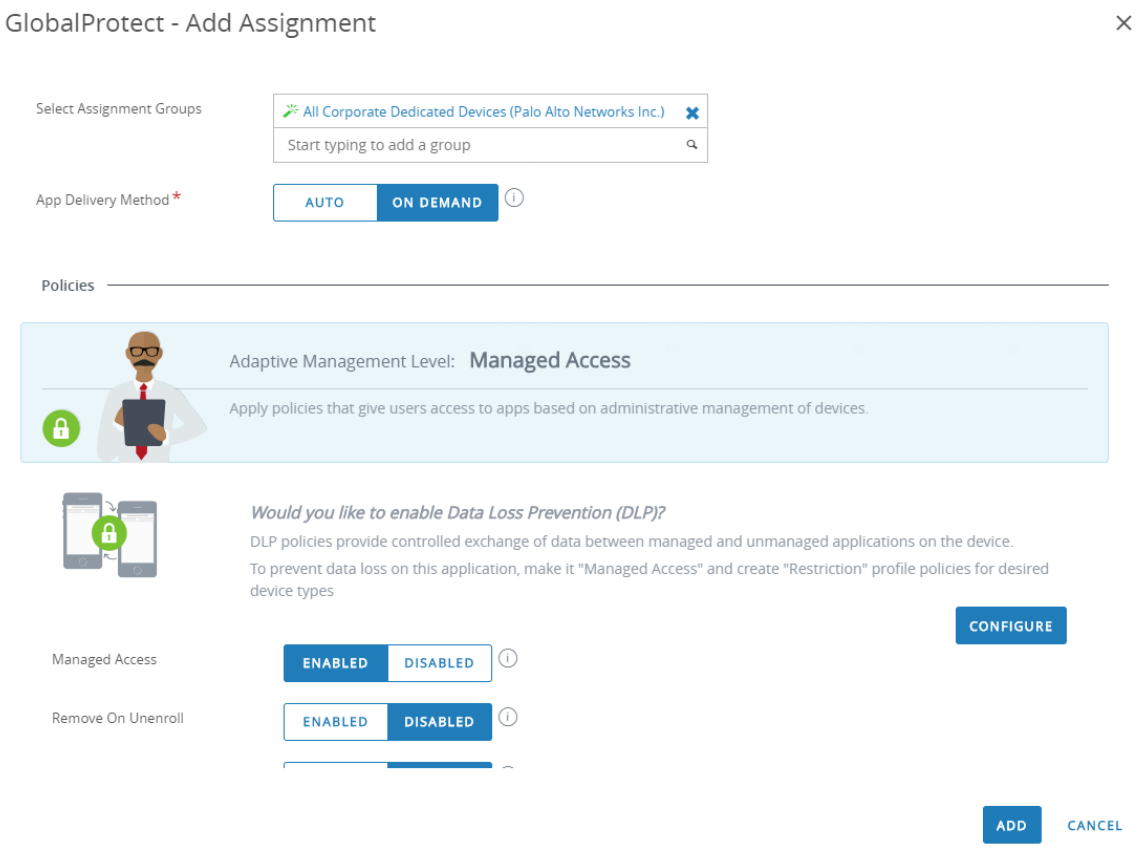
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

12. 选择 **Assignments**（分配），然后单击 **ADD ASSIGNMENT**（添加分配），以添加有权访问此应用的智能组。
    1. 在 **Select Assignment Groups**（选择分配组） 字段中，选择想要获得此应用访问权的智能组。
    2. 选择 **App Delivery Method**（应用交付方法）。如果选择 **AUTO**（自动），则应用将自动部署到指定智能组。如果选择 **ON DEMAND**（按需），则必须手动部署此应用。
    3. 设置 **Managed Access**（受管访问）选项为 **ENABLED**（已启用）。选择此选项后，用户可以根据应用的管理策略访问此应用。
    4. 根据需要配置其他设置。
    5. **Add**（添加）新分配。

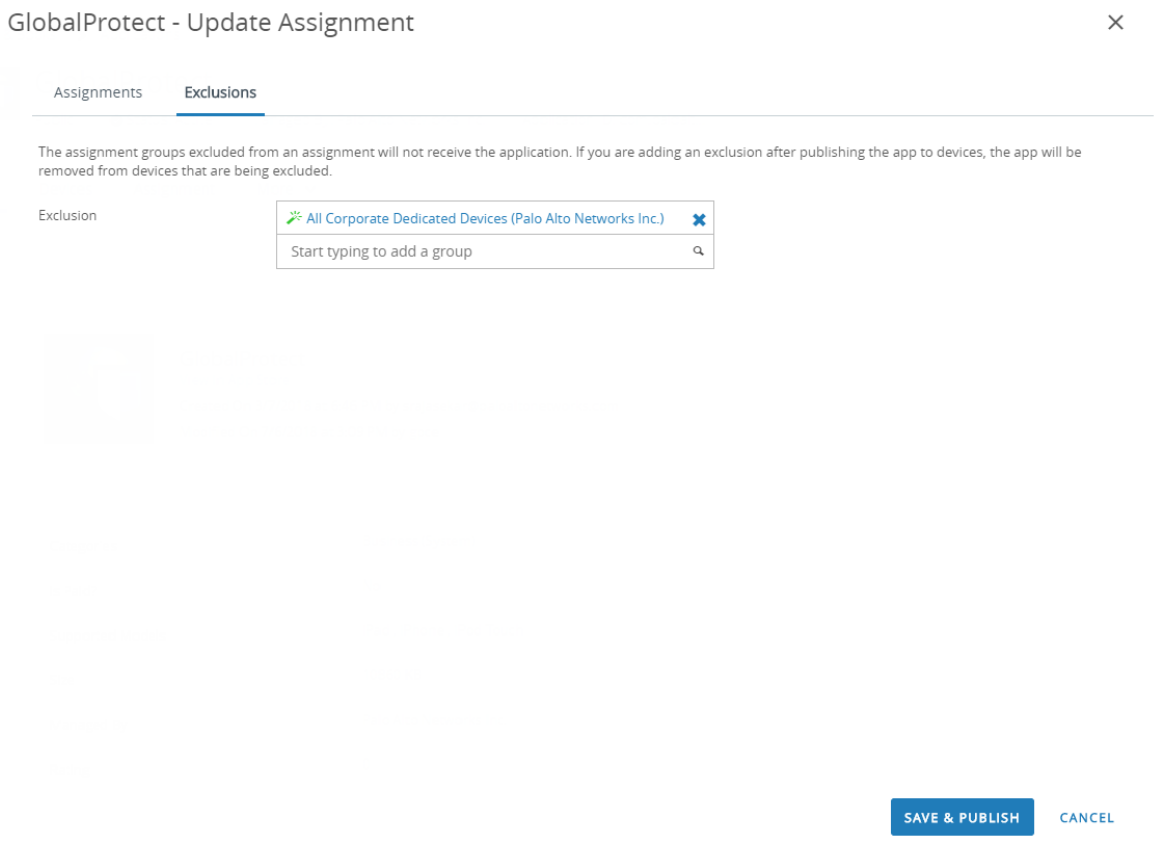
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

13. （可选）要排除某些智能组访问此应用的权限，请选择 **Exclusions**（排除），然后选择想要从 **Exclusion**（排除）字段排除的智能组。

© 2019 Palo Alto Networks, Inc.



14.**SAVE & PUBLISH**（保存并发布）该配置到分配的智能组。

© 2019 Palo Alto Networks, Inc.

使用 *AirWatch* 为安卓端点配置每应用 *VPN* 配置

使用 AirWatch 配置 GlobalProtect VPN 访问，可从您的受管移动端点上启用对内部资源的访问权限。在每应用 VPN 配置中，可指定哪些受管应用可通过 GlobalProtect VPN 隧道发送流量。非受管应用将继续直接连接到互联网，而非 GlobalProtect VPN 隧道。

要使用 AirWatch 为 Android 端点配置每应用 VPN 配置，请按以下步骤操作：

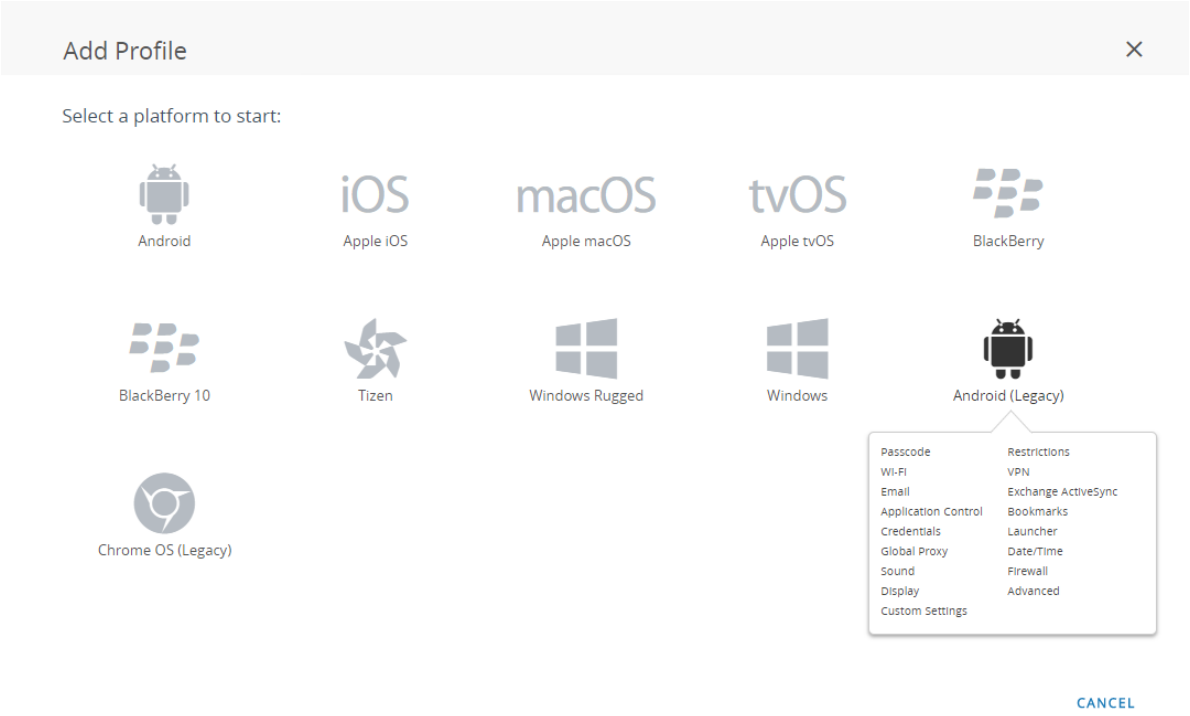
STEP 1 | 下载 GlobalProtect Android 应用：

- 使用 AirWatch 部署 GlobalProtect 移动应用。
- 用户还可直接从 Google Play 下载 GlobalProtect 应用。

STEP 2 | 从 AirWatch 控制台，修改现有安卓配置文件，或添加新的配置文件。

1. 选择 **Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件），然后 **ADD**（添加）新配置文件。
2. 从平台列表选择**Android (Legacy)**。

© 2019 Palo Alto Networks, Inc.



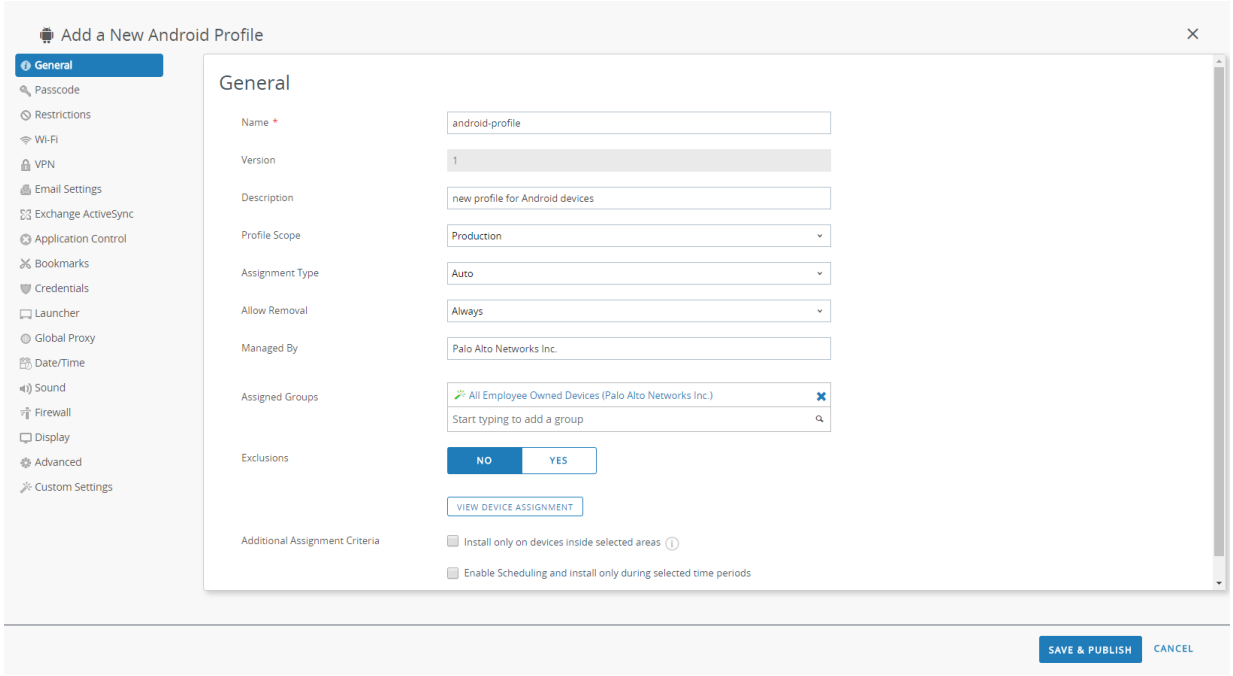
STEP 3 | 配置**General**（常规）设置：

1. 输入配置文件的 **Name**（名称）。
2. （可选）输入指定配置文件用途的简短**Description**（说明）。
3. （可选）选择 **Profile Scope**（配置文件范围），**Production**（生产）、**Staging**（分级）或 **Both**（两者）。
4. （可选）选择 **Assignment Type**（分配类型）以决定如何将配置文件部署到端点。选择 **Auto**（自动）以自动将配置文件部署到所有终端，选择 **Optional**（可选）使最终用户能够从自助服务门户 (SSP) 安装配置文件或手动将配置文件部署到单个端点，或者选择 **Compliance**（合规）以在最终用户违反适用于该端点的合规性策略时部署该配置文件。

© 2019 Palo Alto Networks, Inc.

5. （可选）选择是否想要最终用户 **Allow Removal**（允许删除）配置文件。选择 **Always**（总是）使最终用户能够随时手动删除配置文件，选择 **Never**（决不）阻止最终用户删除配置文件，或者选择 **With Authorization**（授权）以使最终用户能够在管理员的授权下移除配置文件。选择 **With Authorization**（授权）添加要求的密码。
6. （可选）在 **Managed By**（管理者）字段中，输入具有配置文件管理权限的组织组。
7. （可选）在 **Assigned Groups**（分配组）字段中，添加想要为其添加配置文件的智能组。此字段包含一个创建新智能组的选项，智能组可使用最低 OS 版本、设备型号、所有权类别、组织组等的规格进行配置。
8. （可选）指示是否想要在此配置文件的分配中包含任何 **Exclusions**（排除）。如果选择 **Yes**（是），则显示 **Excluded Groups**（排除组）字段，让您可以选择希望从此配置文件分配中排除的智能组。

© 2019 Palo Alto Networks, Inc.



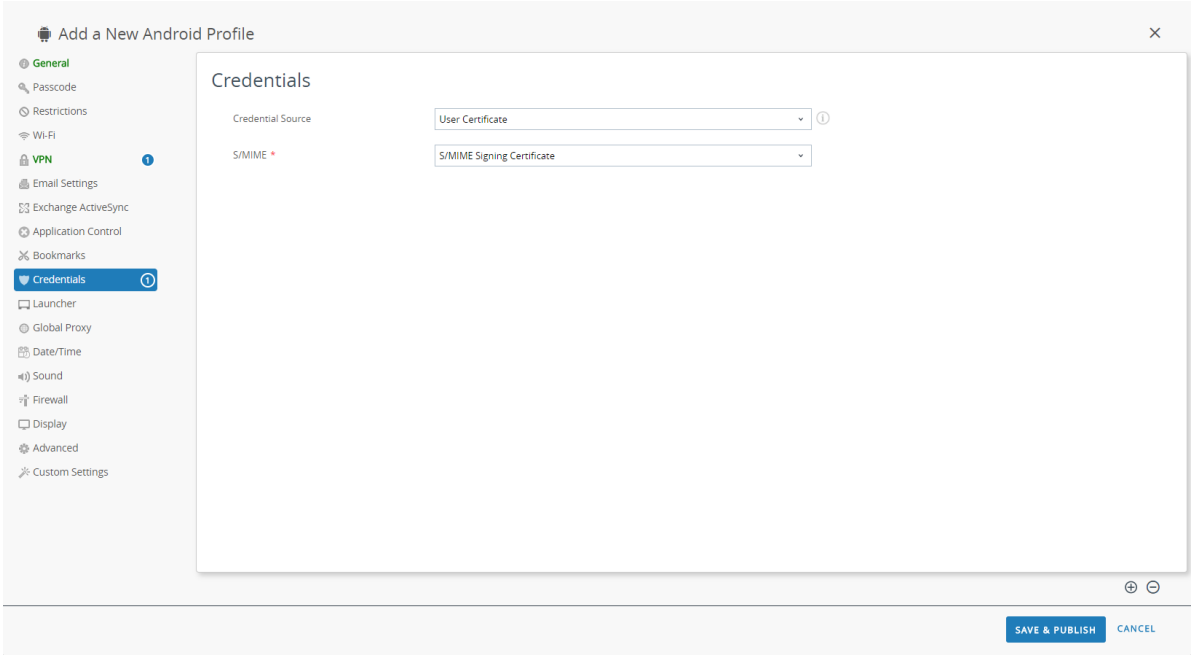
© 2019 Palo Alto Networks, Inc.

STEP 4 | **配置 Credentials（凭据）设置：**

所有每应用 *VNP* 配置均需要基于证书的身份验证。

- 要从 AirWatch 用户中提取客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **User Certificate**（用户证书）。
  2. 选择 **S/MIME Signing Certificate**（**S/MIME** 签名证书）（默认）。

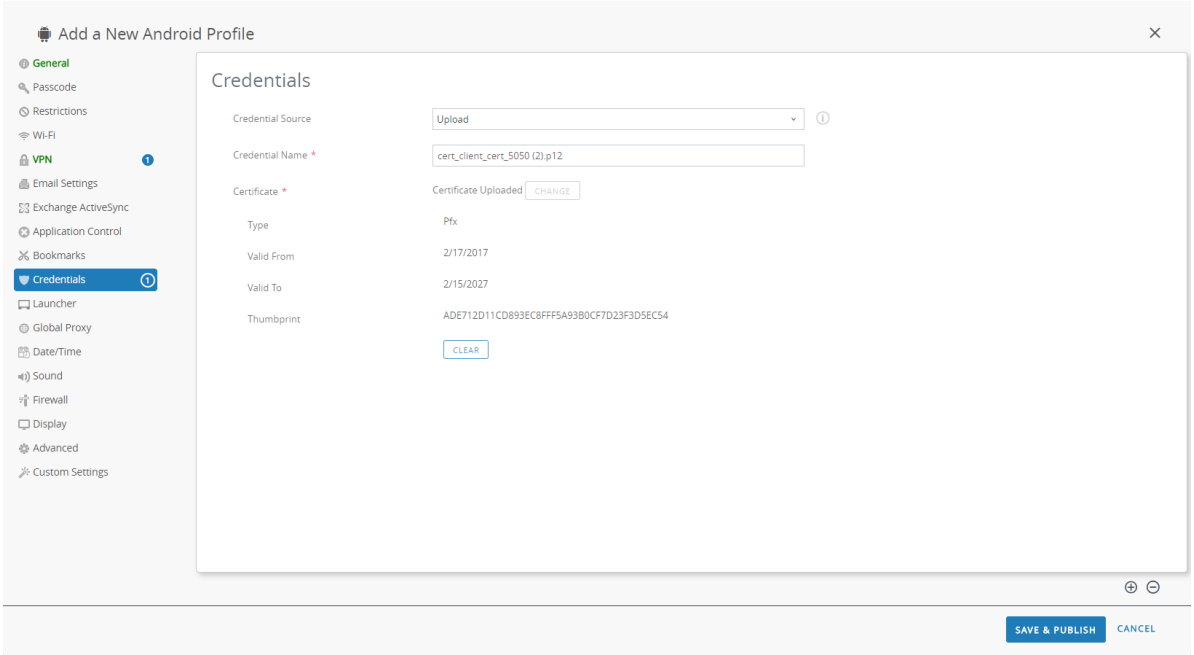
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

- 要手动上传客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **Upload**（上传）。
  2. 输入 **Credential Name**（凭据名称）。
  3. 单击 **UPLOAD**（上传），找到并选定想要上传的证书。
  4. 证书选定后，单击 **SAVE**（保存）。

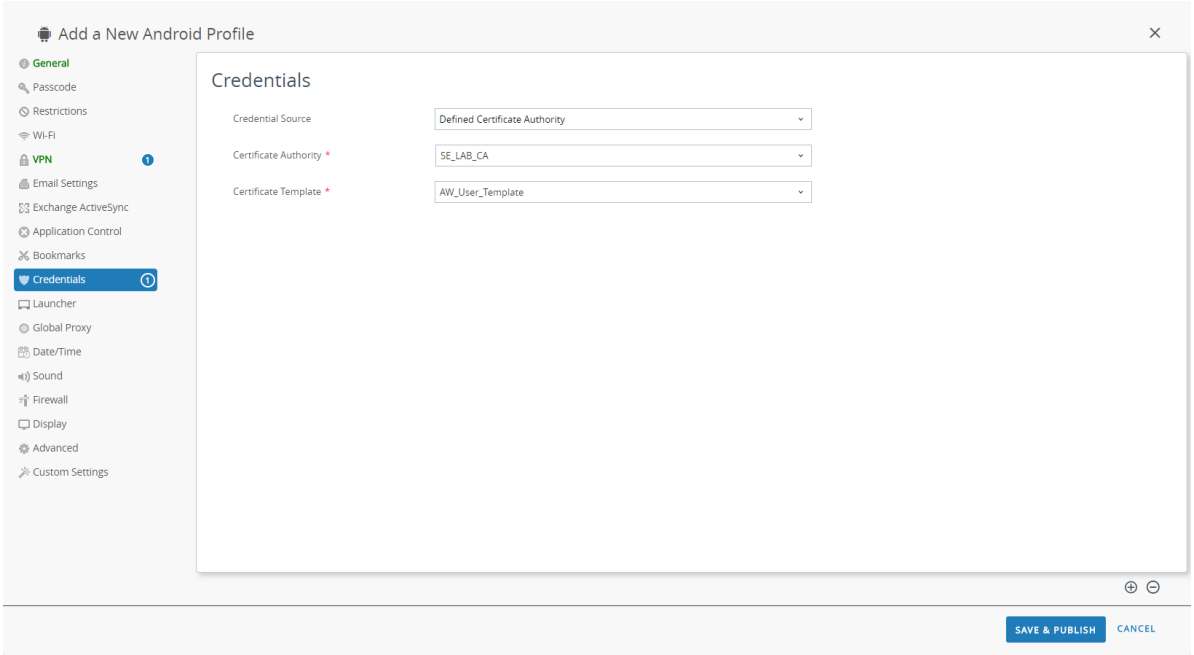
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

- 要使用预定义证书颁发机构和模板：
  1. 设置 **Credential Source**（凭据来源）为 **Defined Certificate Authority**（定义的证书颁发机构）。
  2. 选择想要从其获取证书的 **Certificate Authority**（证书颁发机构）。
  3. 选择用于证书颁发机构的 **Certificate Template**（证书模板）。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

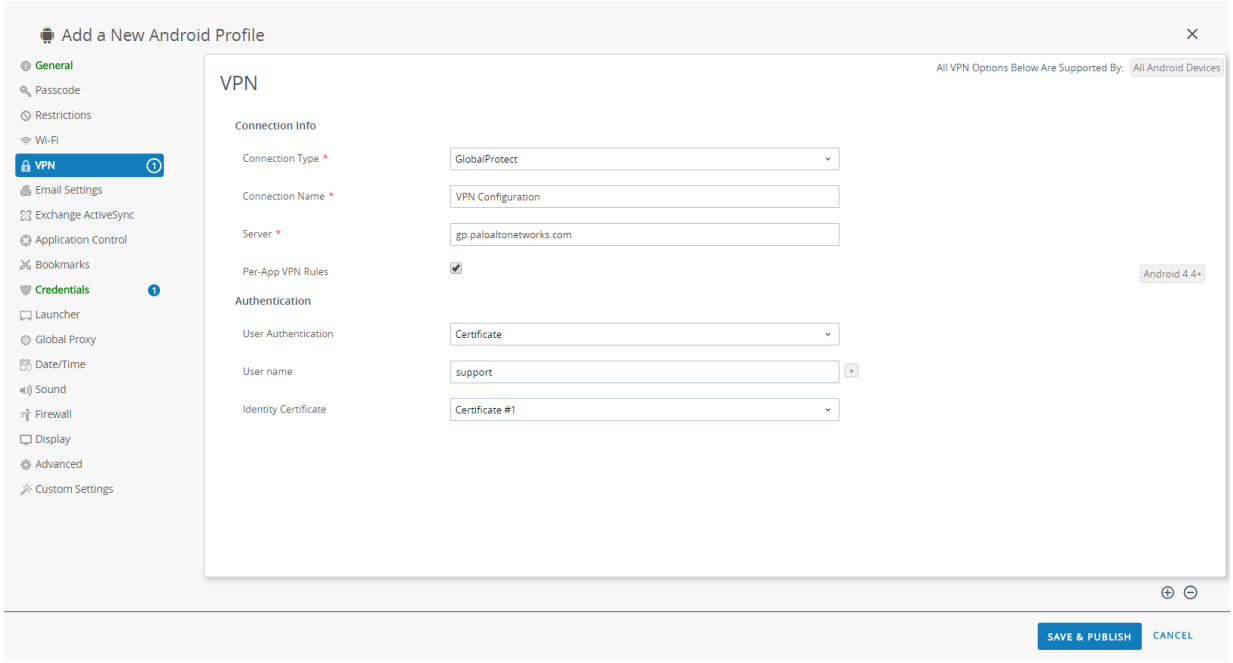
STEP 5 | **配置 VPN 设置：**

1. 设置网络 **Connection Type**（连接类型） 为 **GlobalProtect**。
2. 输入端点显示的 **Connection Name**（连接名称）。
3. 在 **Server**（服务器）字段中，输入用户要连接的 GlobalProtect 门户的主机名或 IP 地址。
4. 启用 **Per App VPN**（每应用 **VPN**）将受管应用的所有流量路由通过 GlobalProtect VPN 隧道。
5. 在身份验证区域，设置 **User Authentication**（用户身份验证）方法为 **Certificate**（证书）。

   所有每应用 *VNP* 配置均需要基于证书的身份验证。

6. 输入 VPN 帐户的 **User name**（用户名）或单击 **+** 按钮查看您可插入的支持查找值。
7. 出现提示时，输入 GlobalProtect 用于验证用户身份的 **Identity Certificate**（身份证书）。**Identity Certificate**（身份证书）与您在 **Credentials**（凭据）设置内配置的证书一致。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

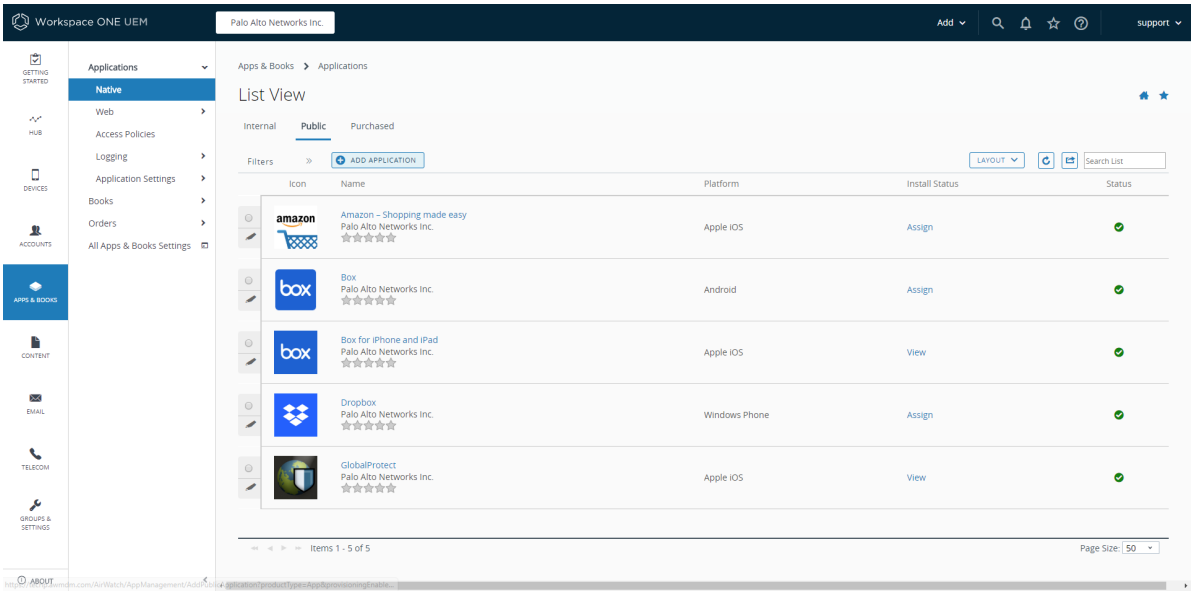
STEP 6 | **SAVE & PUBLISH**（保存并发布）更改。

STEP 7 | 为新的受管应用配置每应用 VPN 设置，或修改已有受管应用的设置。

为应用配置设置并启用每应用 VPN 后，可将此应用发布到一组用户，让此应用通过 GlobalProtect VPN 隧道发送流量。

1. 选择 **APPS & BOOKS**（应用和书籍）> **Applications**（应用）> **Native**（本机）> **Public**（公共）。
2. 要添加新应用，选择 **ADD APPLICATION**（添加应用程序）。要修改已有应用的设置，在公共应用列表（列表视图）中找到应用，然后选择此行旁边的操作菜单中的编辑图标（ ）。

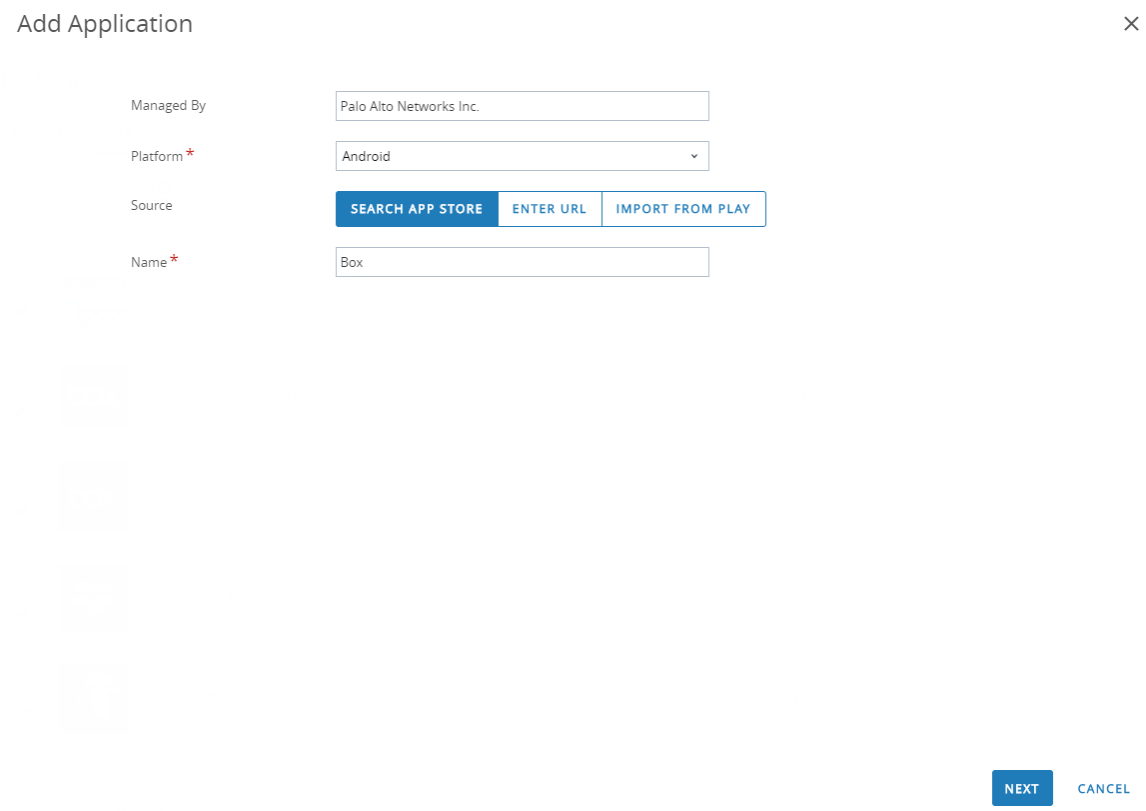
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

3. 在 **Managed By**（管理者）字段中，选择将管理此应用的组织组。
4. 设置 **Platform**（平台）为 **Android**。
5. 选择用于定位应用的首选 **Source**（来源）：
   - **SEARCH APP STORE**（搜索应用商店）—输入应用 **Name**（名称）。
   - **ENTER URL**（输入 **URL**）—输入此应用的 Google Play Store URL（例如，要按 URL 搜索 Box 应用，输入https://play.google.com/store/apps/details?id=com.box.android)。
   - **IMPORT FROM PLAY**（从 **Play** 导入）—从 Google Play 导入公司核准的应用。

© 2019 Palo Alto Networks, Inc.

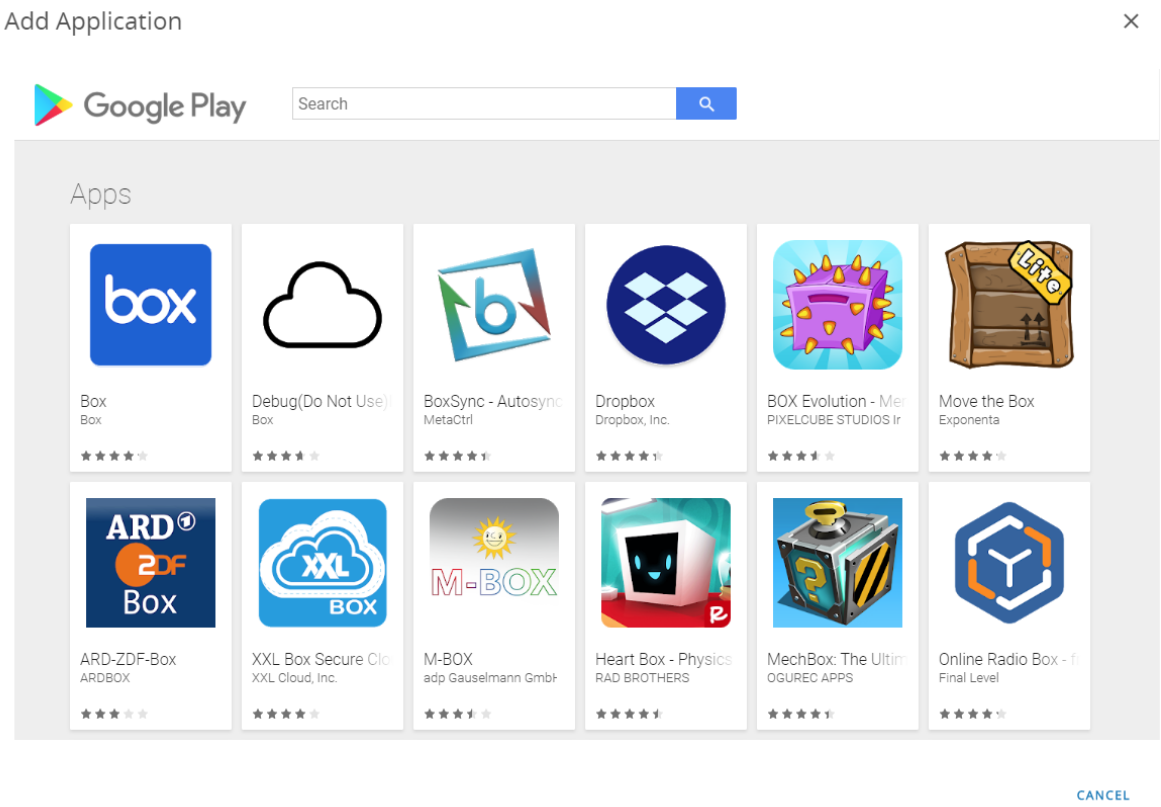


6. 单击 **NEXT**（下一步）。

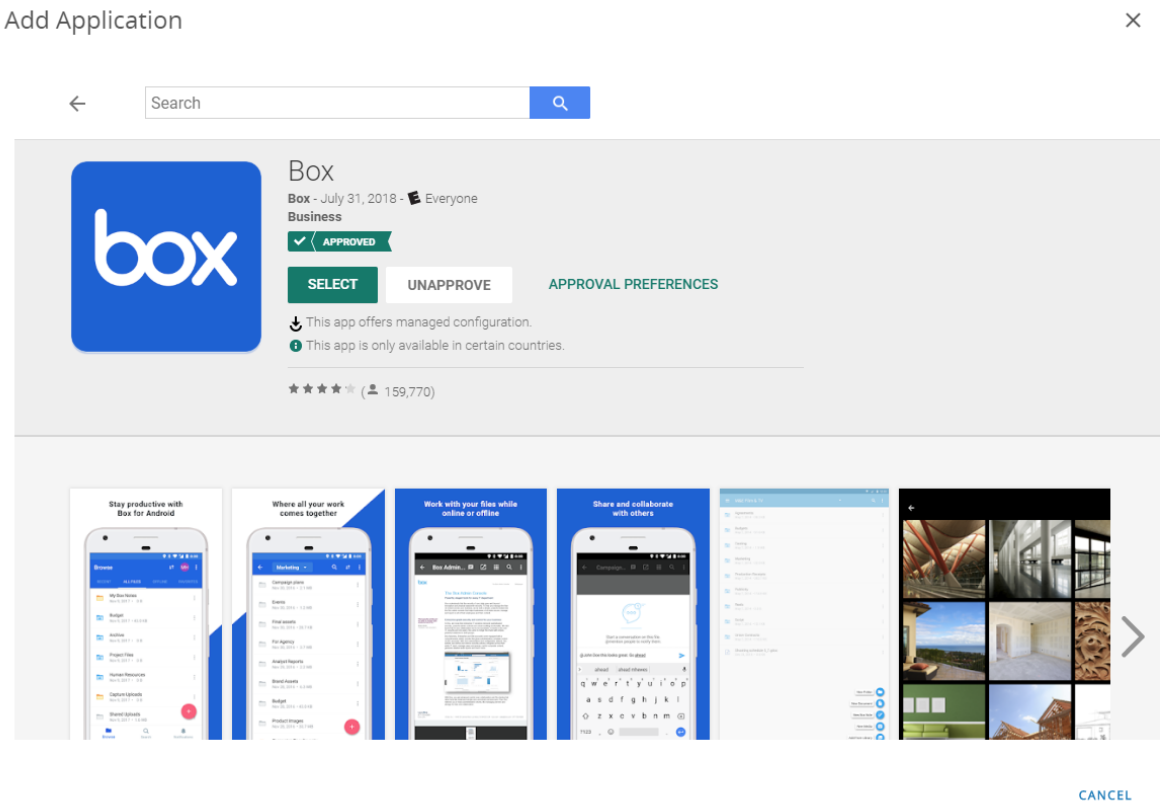
© 2019 Palo Alto Networks, Inc.

如果选择搜索 Google Play，请单击搜索结果列表中的应用图标。如果公司尚未核准此应用，则必须 **APPROVE**（核准）此应用。核准应用后，**SELECT**（选择） 此应用。

© 2019 Palo Alto Networks, Inc.

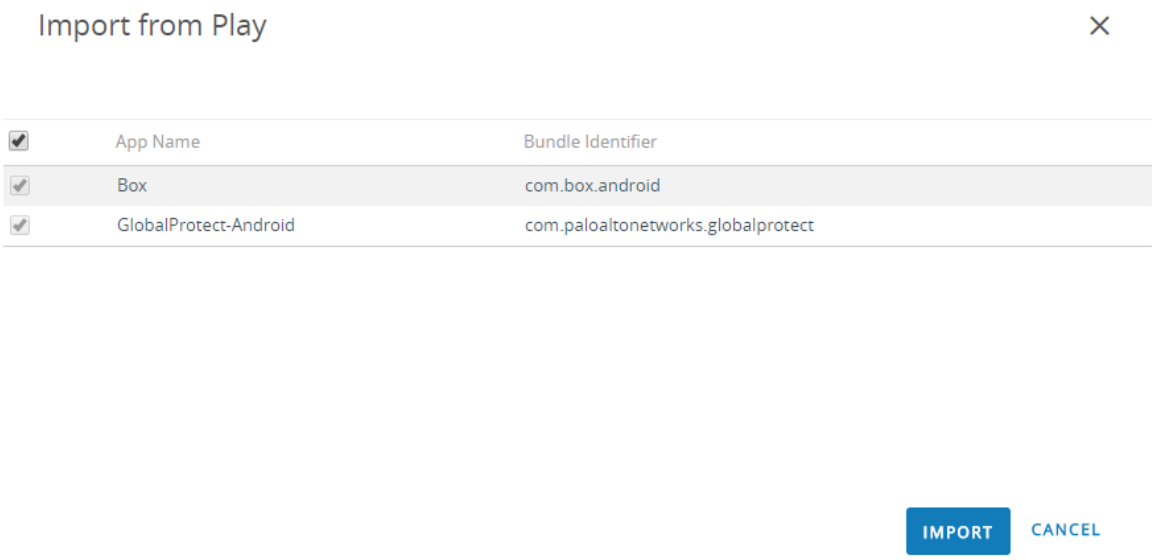


© 2019 Palo Alto Networks, Inc.



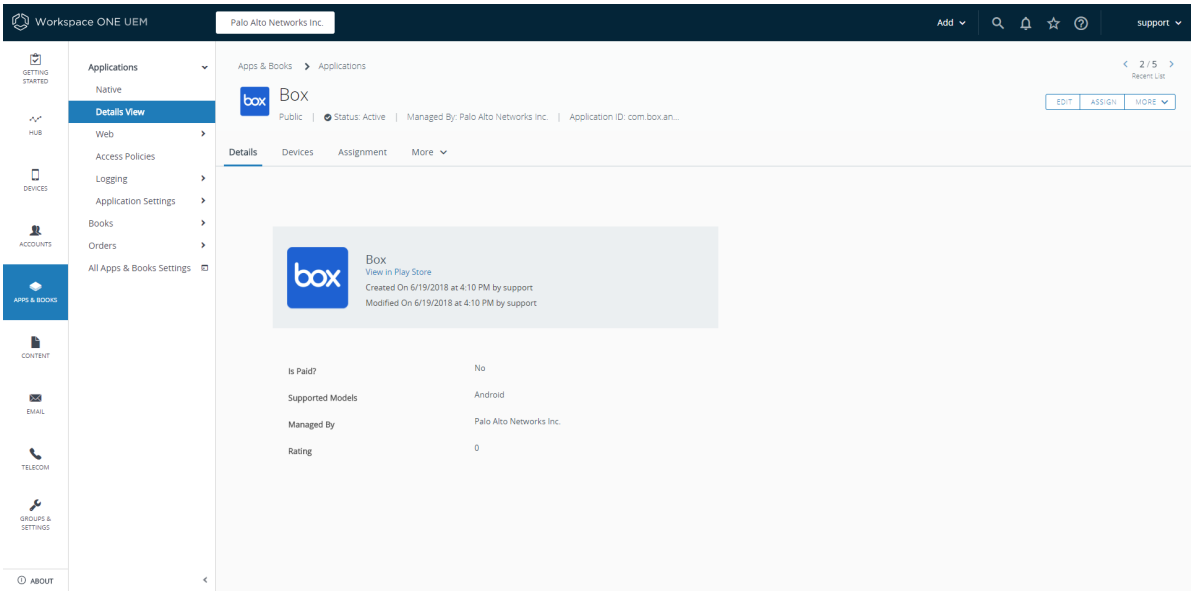
© 2019 Palo Alto Networks, Inc.

如果选择从 Google Play 导入应用，必须从核准公司应用列表中选择此应用，然后单击 **IMPORT**（导入）。如果在列表中看不到此应用，联系您的 Android for Work 管理员批准此应用。



7. 从公共应用列表（列表视图）中选择新添加的应用。
8. 从 **Applications**（应用）> **Details View**（详细视图）中，单击屏幕右上角的 **ASSIGN**（分配）。

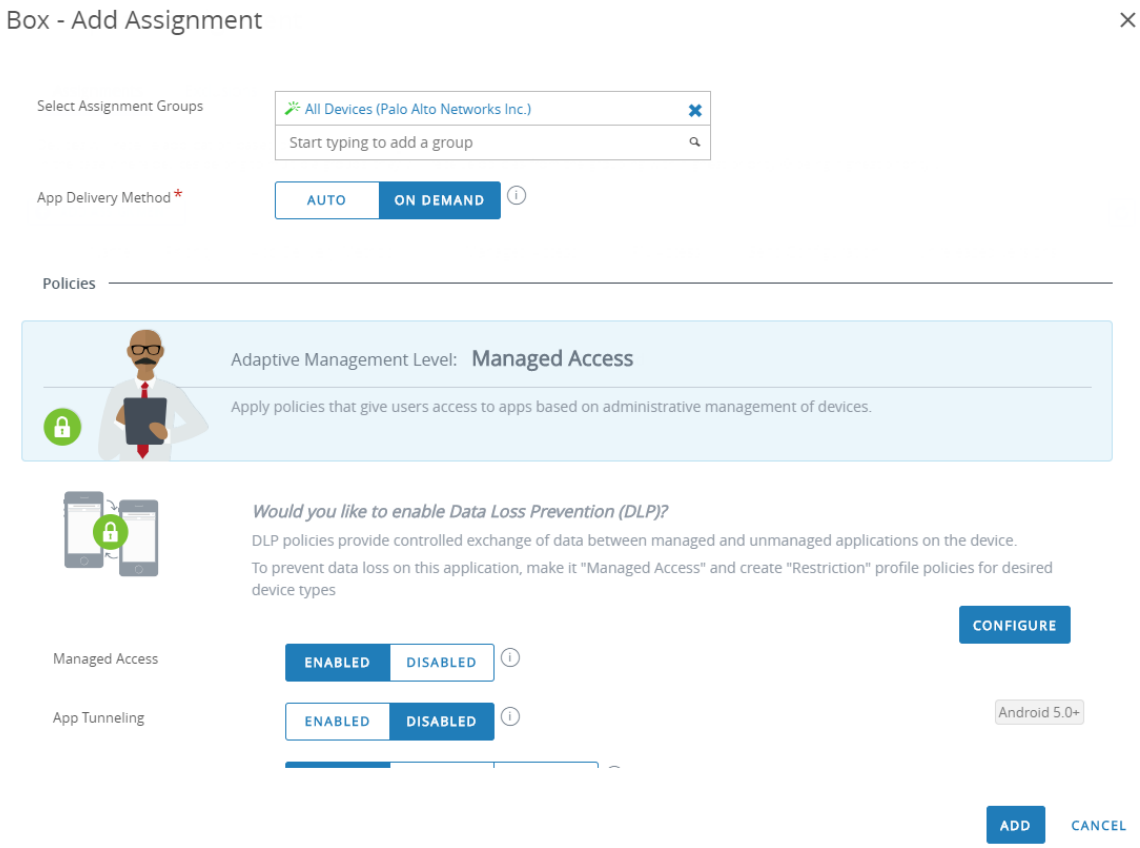
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

9. 选择 **Assignments**（分配），然后单击 **ADD ASSIGNMENT**（添加分配），以添加有权访问此应用的智能组。
    1. 在 **Select Assignment Groups**（选择分配组） 字段中，选择想要获得此应用访问权的智能组。
    2. 选择 **App Delivery Method**（应用交付方法）。如果选择 **AUTO**（自动），则应用将自动部署到指定智能组。如果选择 **ON DEMAND**（按需），则必须手动部署此应用。
    3. 设置 **Managed Access**（受管访问）选项为 **ENABLED**（已启用）。选择此选项后，用户可以根据应用的管理策略访问此应用。
    4. 根据需要配置其他设置。
    5. **Add**（添加）新分配。

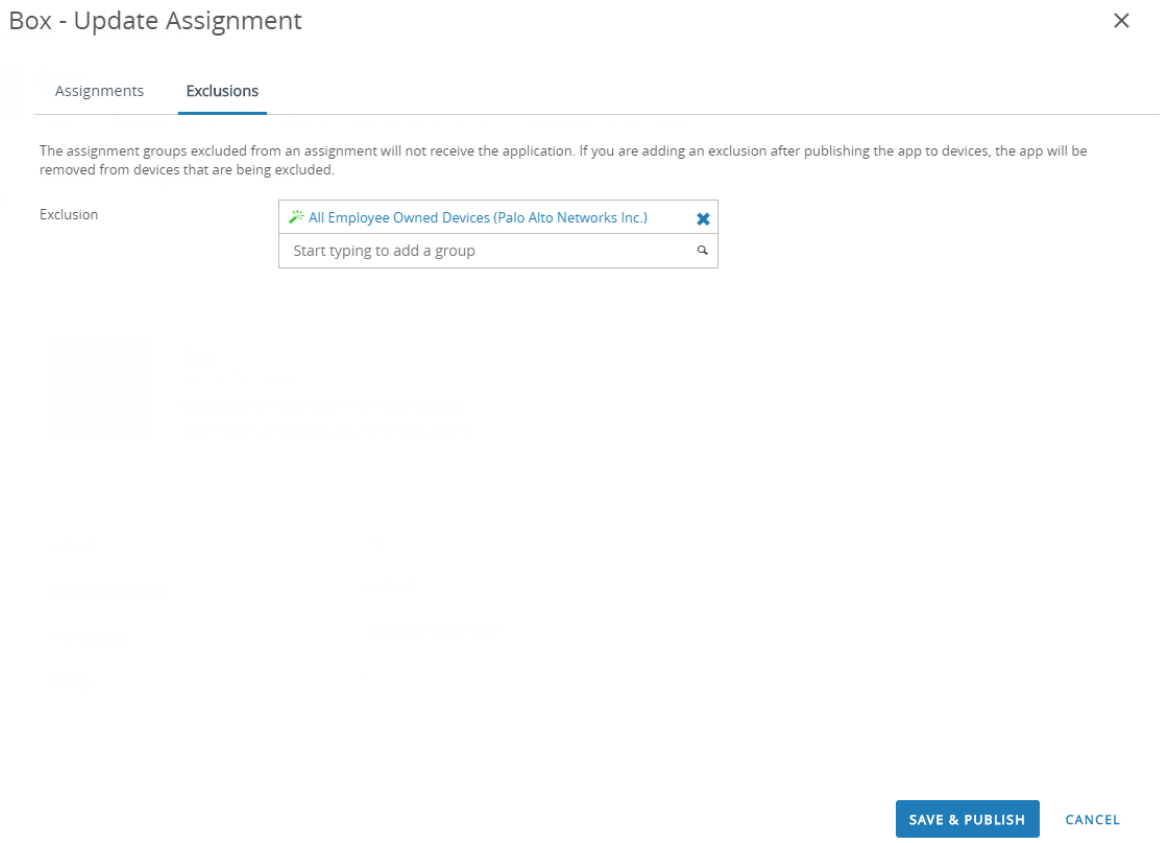
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

10. （可选）要排除某些智能组访问此应用的权限，请选择 **Exclusions**（排除），然后选择想要从 **Exclusion**（排除）字段排除的智能组。

© 2019 Palo Alto Networks, Inc.



11.**SAVE & PUBLISH**（保存并发布）该配置到分配的智能组。

© 2019 Palo Alto Networks, Inc.

使用 *AirWatch* 为 *Windows 10 UWP* 端点配置每应用 *VPN* 配置

使用 AirWatch 配置 GlobalProtect VPN 访问，可从您的受管移动端点上启用对内部资源的访问权限。在每应用 VPN 配置中，可指定哪些受管应用可通过 GlobalProtect VPN 隧道发送流量。非受管应用将继续直接连接到互联网，而非 GlobalProtect VPN 隧道。

由于 *AirWatch* 并不将 *GlobalProtect* 列为 *Windows* 端点的官方连接提供程序，所以您必须选择备用 *VPN* 提供程序，编辑 *GlobalProtect* 应用设置，并按照下列工作流所述将配置导回 *VPN* 配置文件。

要使用 AirWatch 为 Windows 10 UWP 端点配置每应用 VPN 配置，请按以下步骤操作：

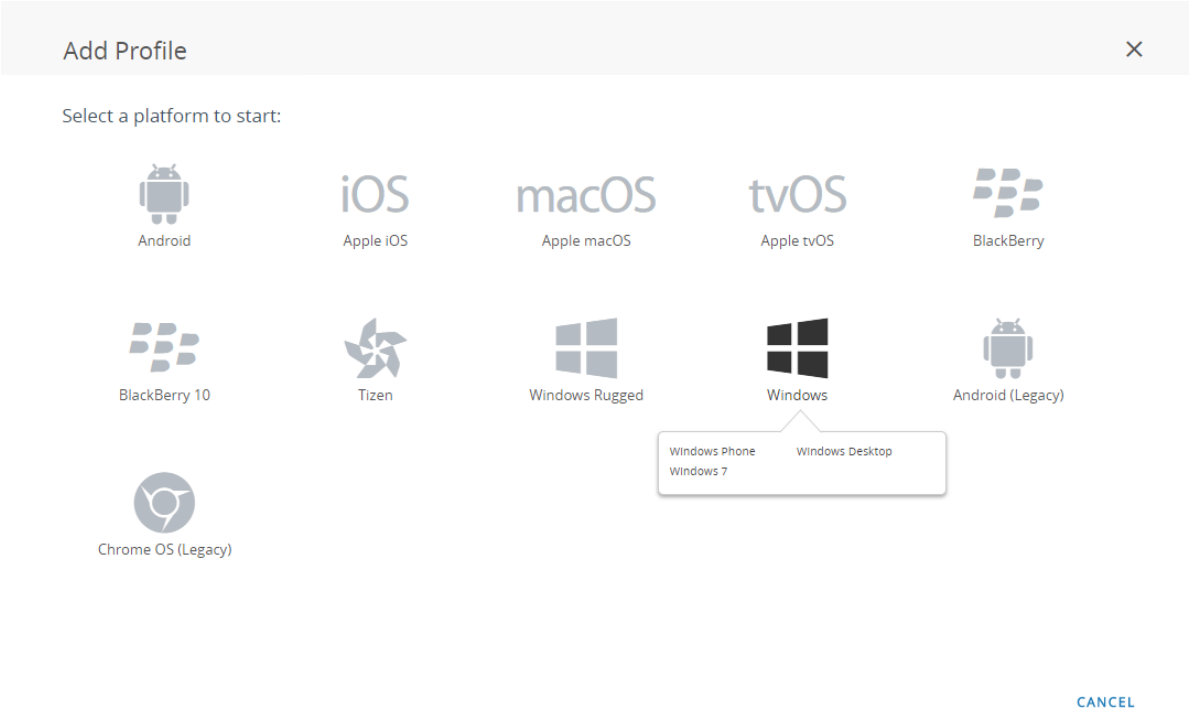
STEP 1 | 下载 GlobalProtect Windows 10 UWP 应用：

- 使用 AirWatch 部署 GlobalProtect 移动应用。
- 用户还可直接从 Microsoft Store 下载 GlobalProtect 应用。

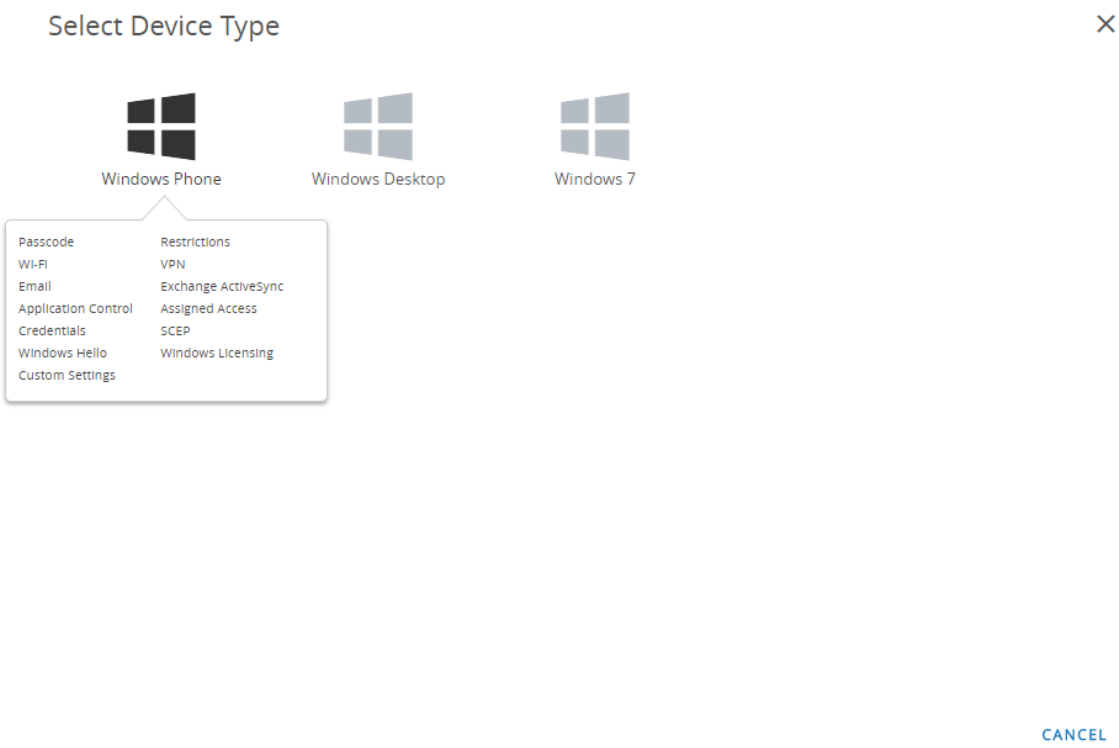
STEP 2 | 从 AirWatch 控制台，修改现有 Windows 10 UWP 配置文件，或添加新的配置文件。

1. 选择 **Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件），然后 **ADD**（添加）新配置文件。
2. 选择 **Windows** 作为平台，**Windows Phone** 作为设备类型。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.



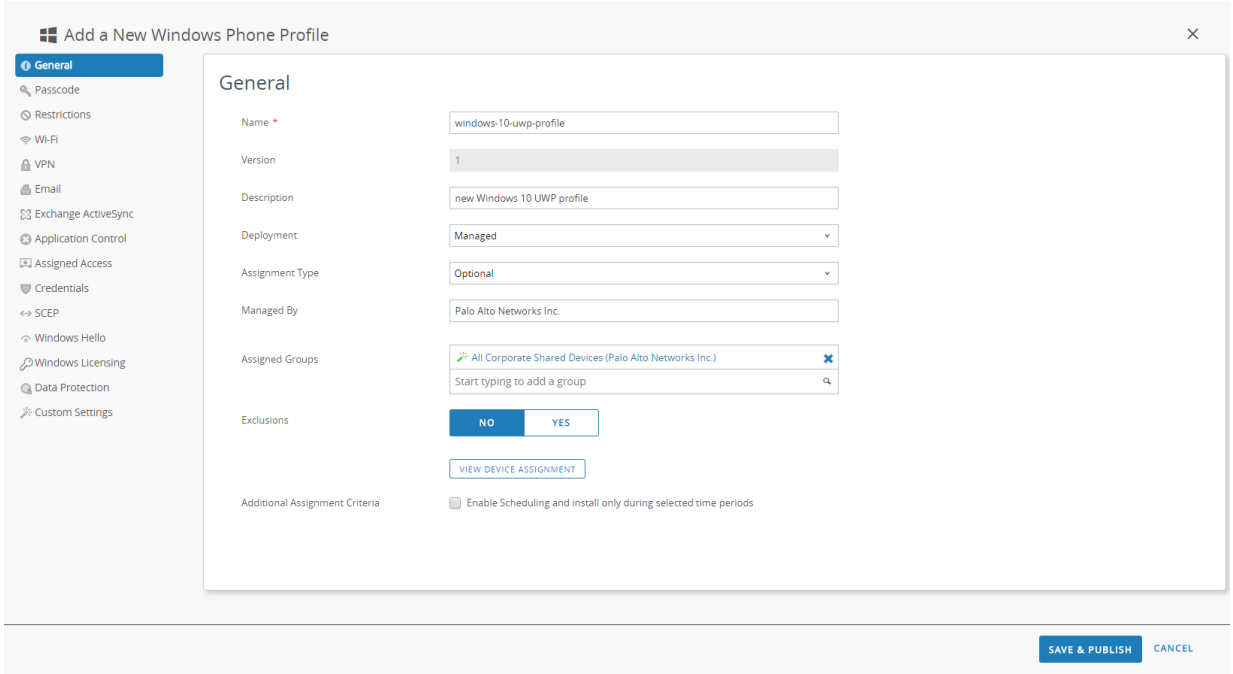
STEP 3 | 配置**General**（常规）设置：

- 输入配置文件的 **Name**（名称）。
- （可选）输入指定配置文件用途的简短**Description**（说明）。
- （可选）设置 **Deployment**（部署）方法为 **Managed**（受管理），以便在取消注册时自动删除配置文件。
- （可选）选择 **Assignment Type**（分配类型）以决定如何将配置文件部署到端点。选择 **Auto**（自动）以自动将配置文件部署到所有终端，选择 **Optional**（可选）使最终用户能够从自助服务门户 (SSP) 安装配置文件或手动将配置文件部署到单个端点，或者选择 **Compliance**（合规）以在最终用户违反适用于该端点的合规性策略时部署该配置文件。
- （可选）在 **Managed By**（管理者）字段中，输入具有配置文件管理权限的组织组。

© 2019 Palo Alto Networks, Inc.

- （可选）在 **Assigned Groups**（分配组）字段中，添加想要为其添加配置文件的智能组。此字段包含一个创建新智能组的选项，智能组可使用最低 OS 版本、设备型号、所有权类别、组织组等的规格进行配置。
- （可选）指示是否想要在此配置文件的分配中包含任何 **Exclusions**（排除）。如果选择 **Yes**（是），则显示 **Excluded Groups**（排除组）字段，让您可以选择希望从此配置文件分配中排除的智能组。

© 2019 Palo Alto Networks, Inc.



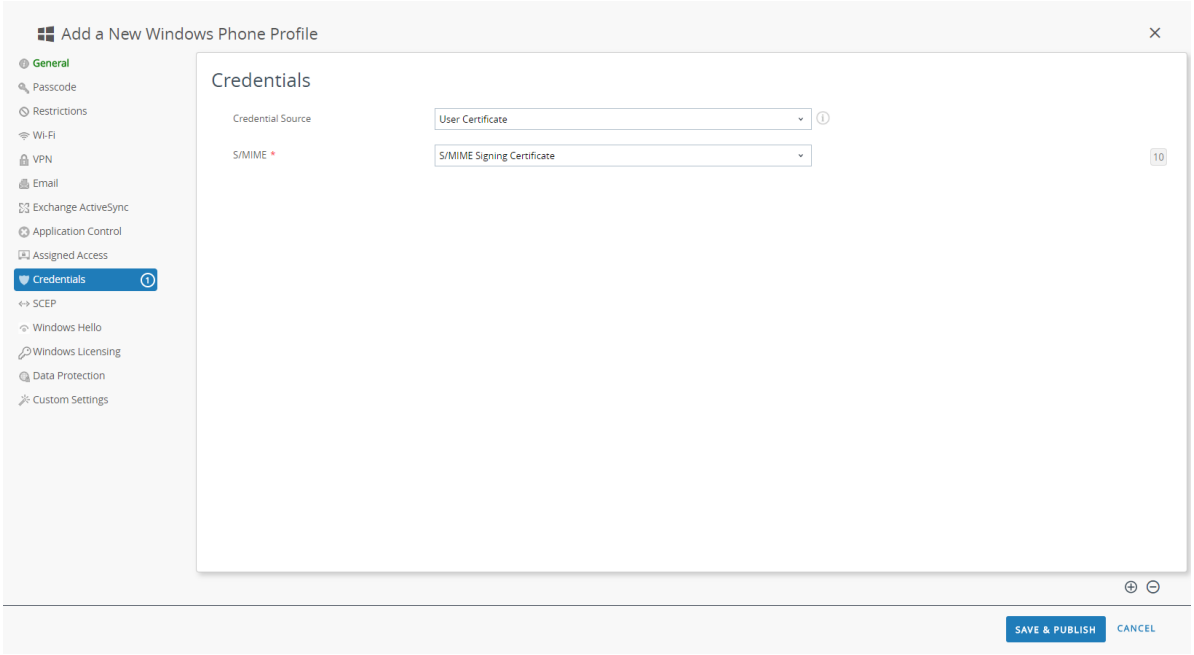
© 2019 Palo Alto Networks, Inc.

STEP 4 | **配置 Credentials（凭据）设置：**

所有每应用 *VNP* 配置均需要基于证书的身份验证。

- 要从 AirWatch 用户中提取客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **User Certificate**（用户证书）。
  2. 选择 **S/MIME Signing Certificate**（**S/MIME** 签名证书）（默认）。

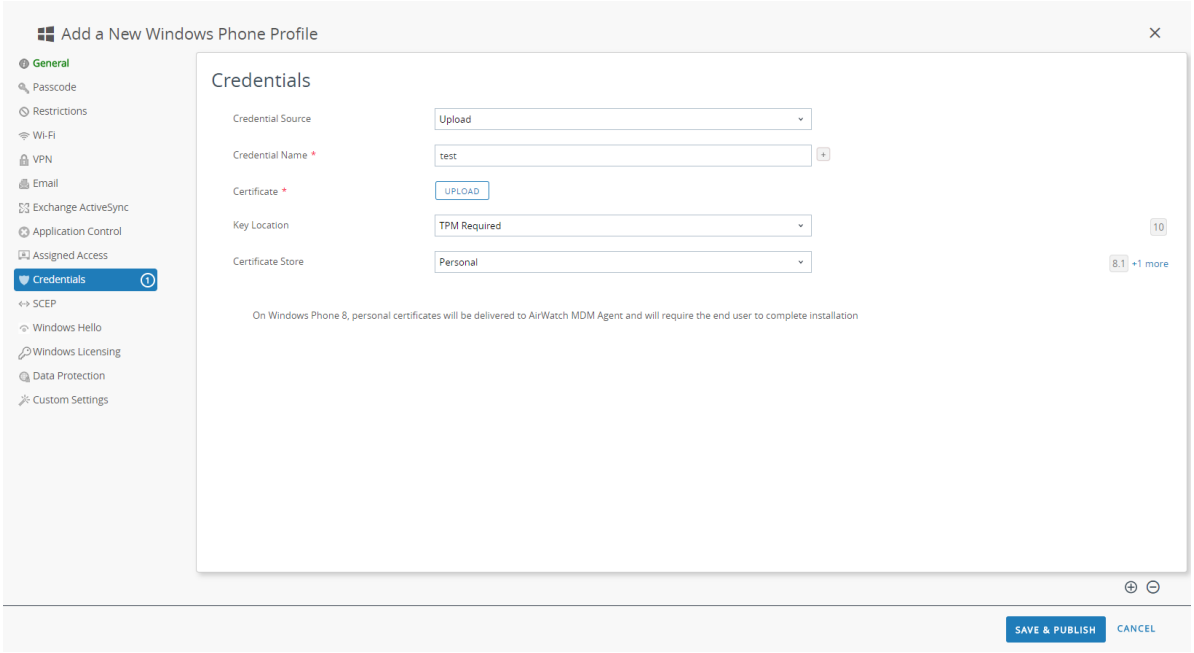
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

- 要手动上传客户端证书：
  1. 设置 **Credential Source**（凭据来源）为 **Upload**（上传）。
  2. 输入 **Credential Name**（凭据名称）。
  3. 单击 **UPLOAD**（上传），找到并选定想要上传的证书。
  4. 证书选定后，单击 **SAVE**（保存）。
  5. 选择想要保存证书私钥的 **Key Location**（表项位置）：
     - **TPM Required**（需要 **TPM**）—在可信平台模块中保存私钥。如果端点无可信平台模块，则无法安装私钥。
     - **TPM If Present**（如果存在 **TPM**）—如果端点有可用的可信平台模块，则将私钥保存在其内。如果端点无可信平台模块，则将私钥保存在端点软件内。
     - **Software**（软件）—将私钥保存在端点软件内。
     - **Passport**（通行证）—将私钥保存在 Microsoft 通行证中。要启用此选项，必须在端点上安装 AirWatch Protection Agent 。
  6. 将 **Certificate Store**（证书存储库）设置为 **Personal**（个人）。

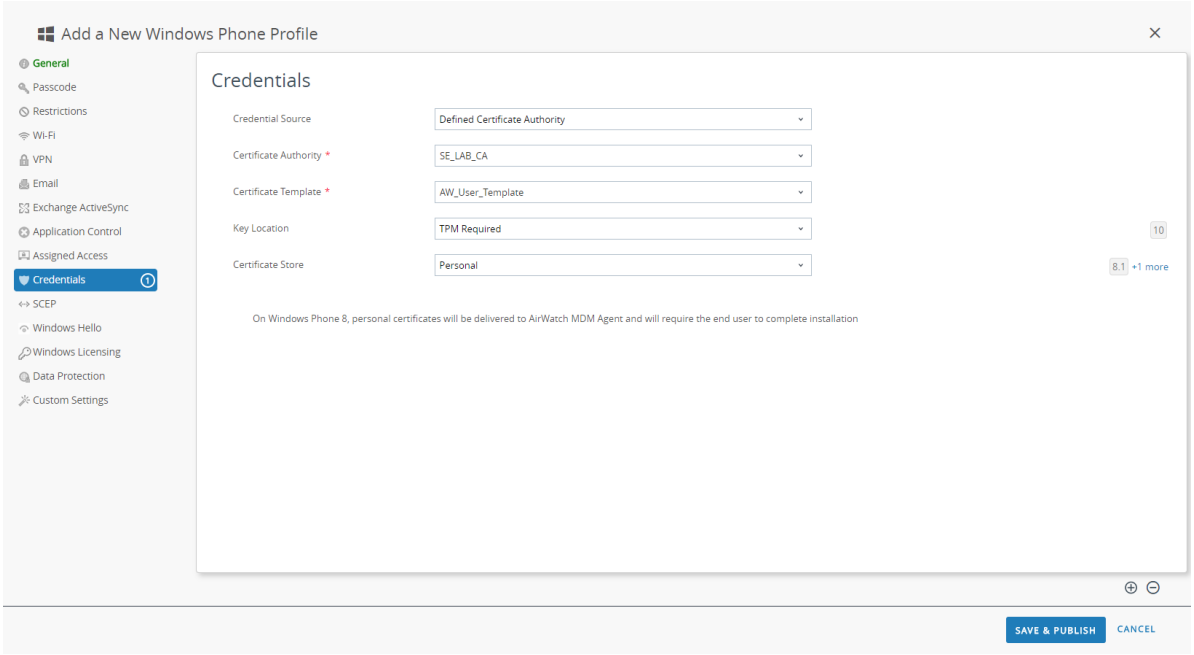
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

- 要使用预定义证书颁发机构和模板：
  1. 设置 **Credential Source**（凭据来源）为 **Defined Certificate Authority**（定义的证书颁发机构）。
  2. 选择想要从其获取证书的 **Certificate Authority**（证书颁发机构）。
  3. 选择用于证书颁发机构的 **Certificate Template**（证书模板）。
  4. 选择想要保存证书私钥的 **Key Location**（表项位置）：
     - **TPM Required**（需要 **TPM**）—在可信平台模块中保存私钥。如果端点无可信平台模块，则无法安装私钥。
     - **TPM If Present**（如果存在 **TPM**）—如果端点有可用的可信平台模块，则将私钥保存在其内。如果端点无可信平台模块，则将私钥保存在端点软件内。
     - **Software**（软件）—将私钥保存在端点软件内。
     - **Passport**（通行证）—将私钥保存在 Microsoft 通行证中。要启用此选项，必须在端点上安装 AirWatch Protection Agent。
  5. 将 **Certificate Store**（证书存储库）设置为 **Personal**（个人）。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

STEP 5 | **配置 VPN 设置：**

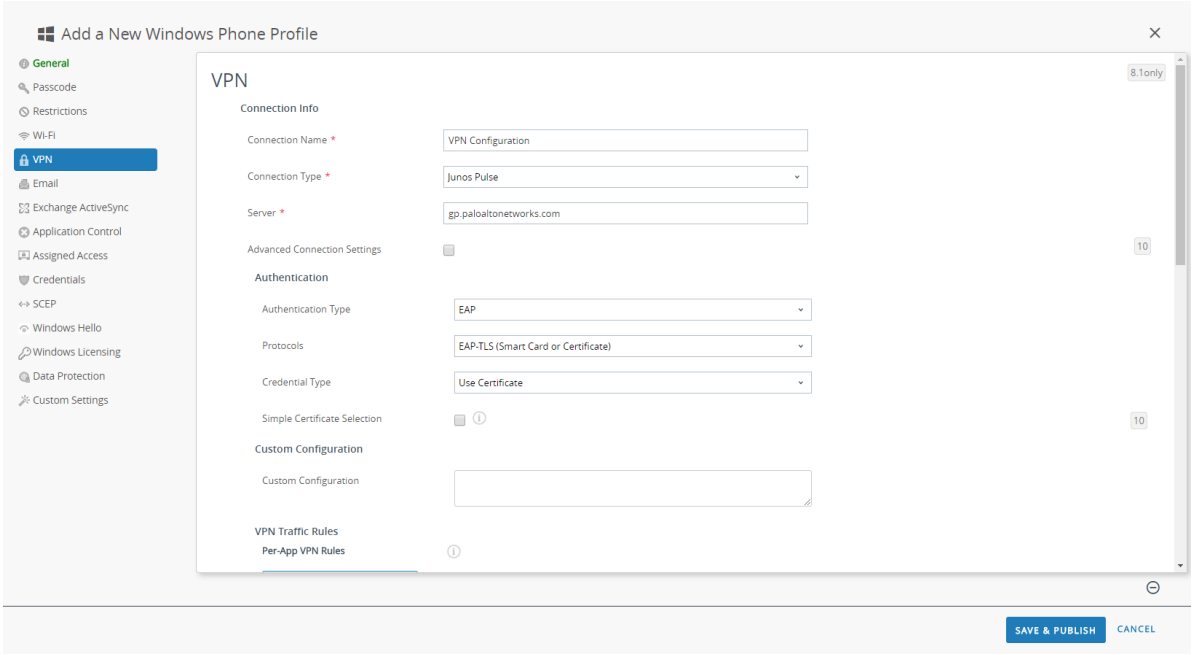
1. 输入端点显示的 **Connection Name**（连接名称）。
2. 选择备用提供程序 **Connection Type(连接类型)**（勿选择**IKEv2**、**L2TP**、**PPTP** 或 **Automatic**（自动），因为其没有 GlobalProtect VPN 配置文件所需的相关联供应商设置）。

   必须选择备用供应商，因为 AirWatch 尚未将 GlobalProtect 列为 Windows 端点的官方连接提供程序。

3. 在 **Server**（服务器）字段中，输入用户要连接的 GlobalProtect 门户的主机名或 IP 地址。
4. 在身份验证区域，选择用于指定最终用户身份验证时使用的方法的基于证书的 **Authentication Type**（身份验证类型）。

   所有每应用 VNP 配置均需要基于证书的身份验证。

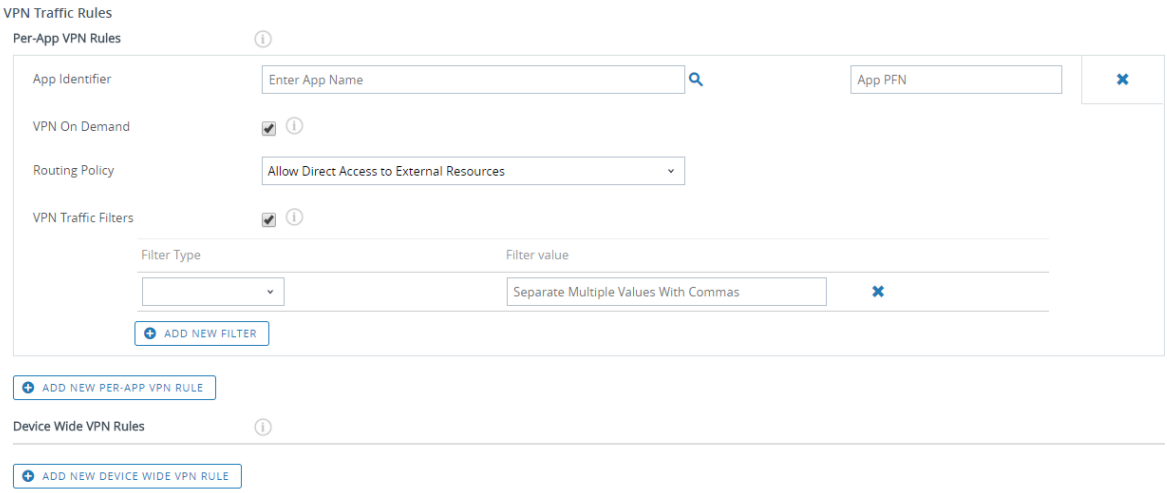
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

5. （可选）要允许 GlobalProtect 保存用户凭据，请在“策略”区域 **ENABLE**（启用）**Remember Credentials**（记住凭据）选项。
6. 在 VPN 流量规则区域，**ADD NEW PER-APP VPN RULE**（添加新的每应用 **VPN** 规则），以指定适用于特定旧版应用（通常为 .exe 文件）或新版应用（通常从 Microsoft Store 下载）的规则。
   1. （可选）**VPN On Demand**（按需启用 **VPN**），允许 GlobalProtect 在应用发布时自动建立连接。
   2. 选择 **Routing Policy**（路由策略），以指定是否需要通过 VPN 隧道发送应用流量。
   3. （可选）配置特定 **VPN Traffic Filters**（**VPN** 流量筛选条件），以便仅在匹配所定义的匹配条件（IP 地址和端口等）时通过 VPN 隧道路由应用流量。

      单击 **ADD NEW FILTER**（添加新的筛选条件），添加匹配条件。出现提示时，输入 **Filter Name**（筛选条件名称）和相应的 **Filter Value**（筛选条件值）。



STEP 6 | **SAVE & PUBLISH**（保存并发布）更改。

STEP 7 | 为新的受管应用配置每应用 VPN 设置，或修改已有受管应用的设置。

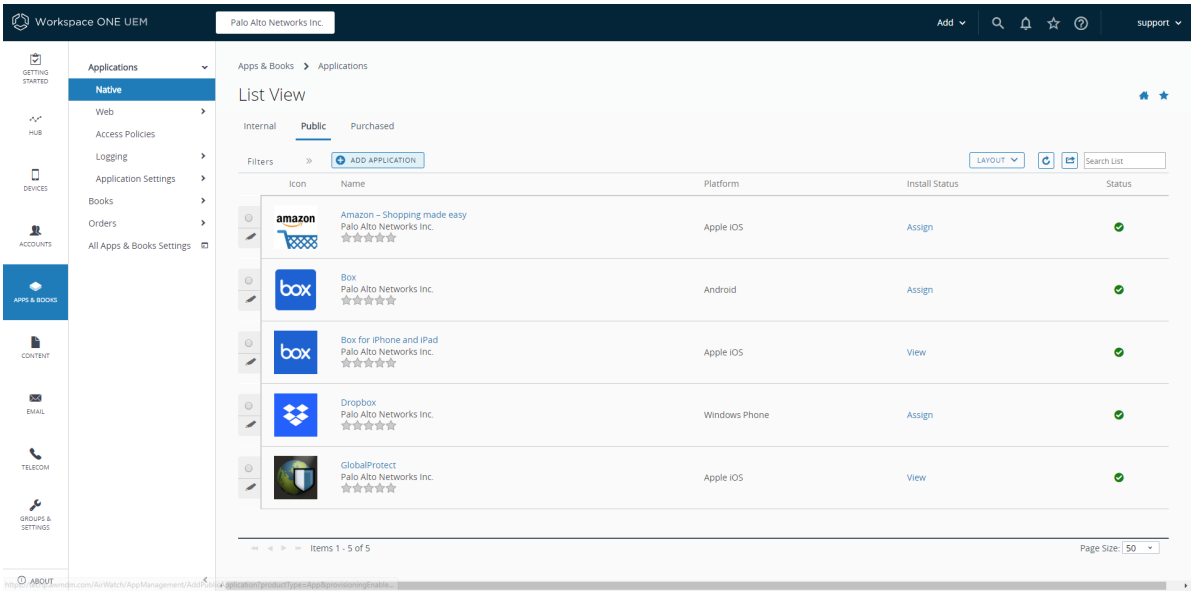
为应用配置设置并启用每应用 VPN 后，可将此应用发布到一组用户，让此应用通过 GlobalProtect VPN 隧道发送流量。

1. 选择 **APPS & BOOKS**（应用和书籍）> **Applications**（应用）> **Native**（本机）> **Public**（公共）。

© 2019 Palo Alto Networks, Inc.

2. 要添加新应用，选择 **ADD APPLICATION**（添加应用程序）。要修改已有应用的设置，在公共应用列表中找到应用，然后选择此行旁边的操作菜单中的编辑图标 ( )。

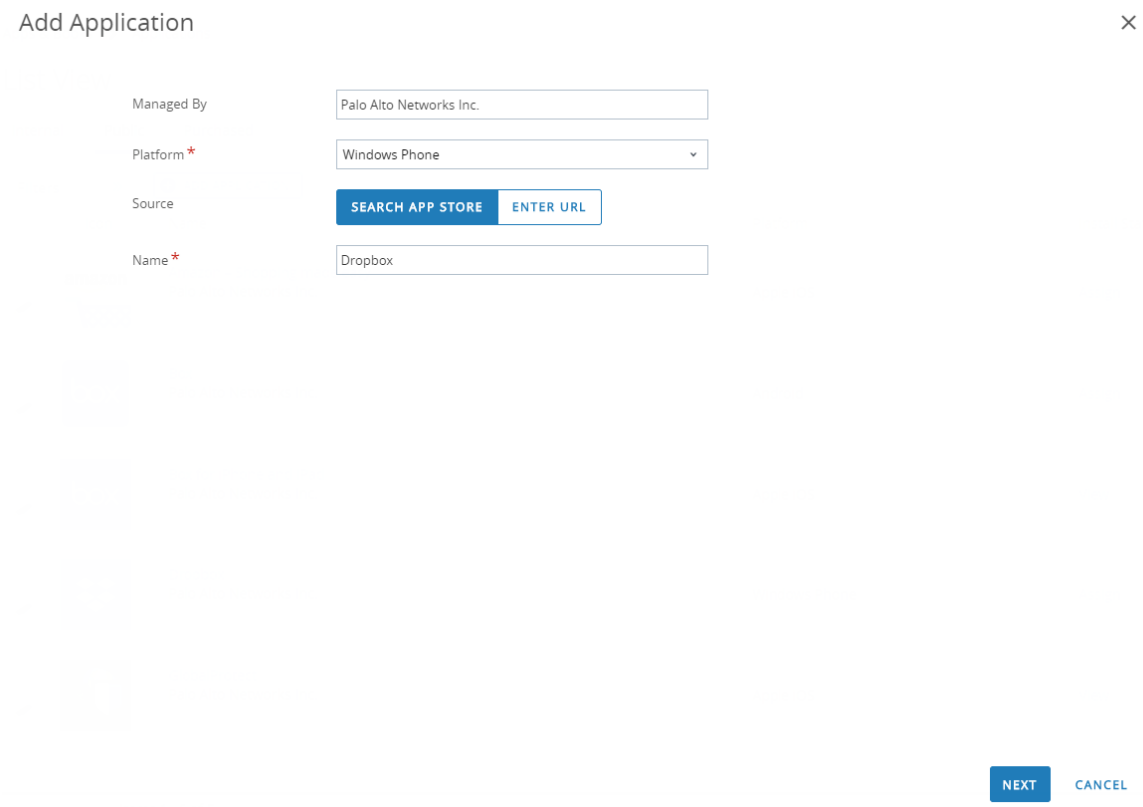
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

3. 在 **Managed By**（管理者）字段中，选择将管理此应用的组织组。
4. 设置 **Platform**（平台）为 **Windows Phone**。
5. 选择用于定位应用的首选 **Source**（来源）：
   - **SEARCH APP STORE**（搜索应用商店）—输入应用 **Name**（名称）。
   - **ENTER URL**（输入 **URL**）—输入此应用的 Microsoft Store URL（例如，要按 URL 搜索 Dropbox 移动应用，输入 https://www.microsoft.com/en-us/p/dropbox-mobile/9wzdncrfj0pk）。

© 2019 Palo Alto Networks, Inc.

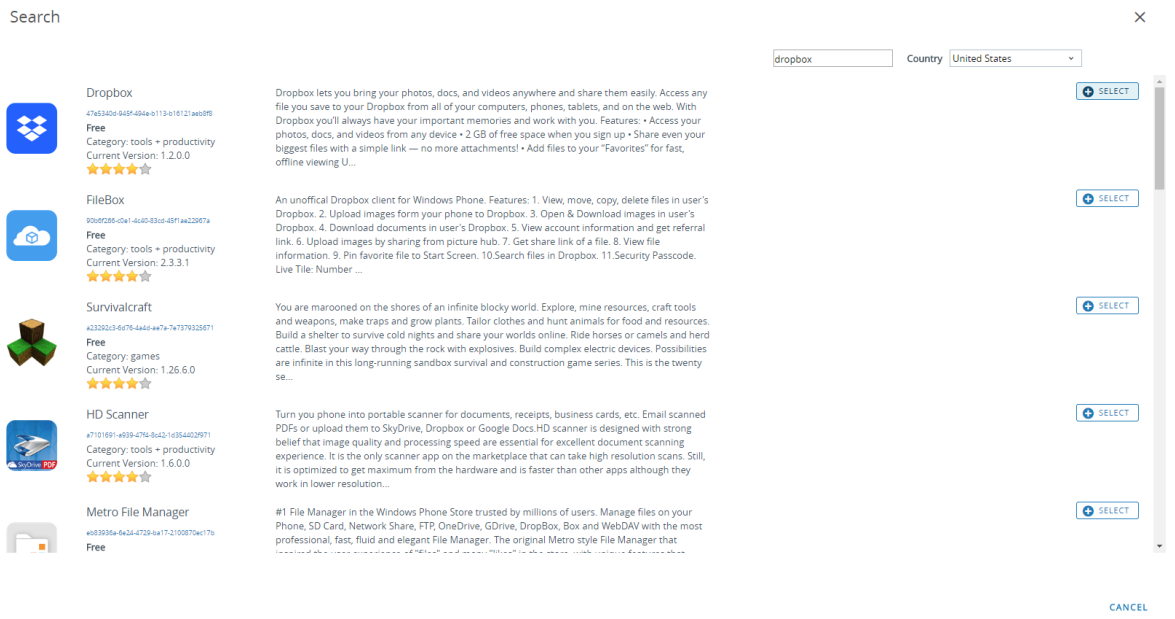


© 2019 Palo Alto Networks, Inc.

6. 单击 **NEXT**（下一步）。

   如果选择搜索 Microsoft Store，您必须从搜索结果列表中 **SELECT**（选择）应用。

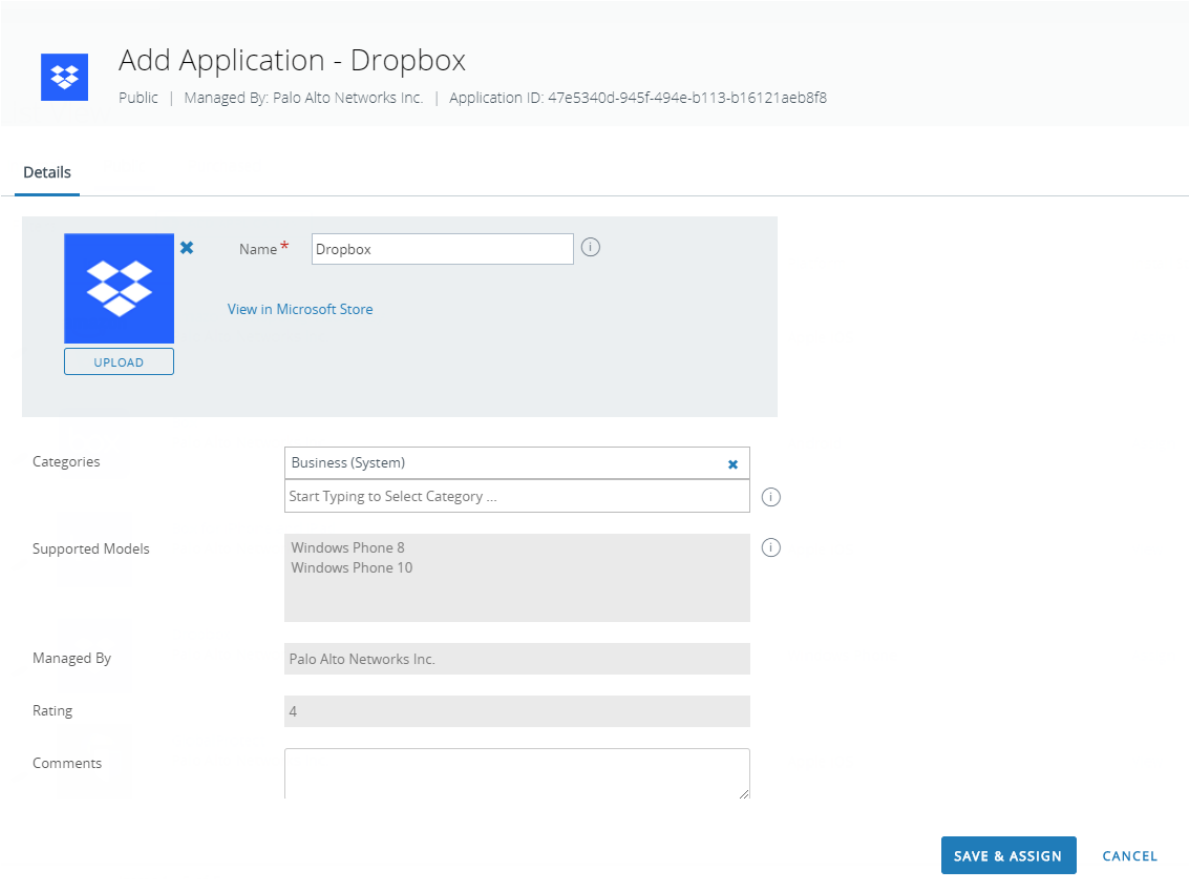
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

7. 在添加应用程序对话框中，应用 **Name**（名称）必须正确。此名称将出现在 AirWatch 应用目录中。
8. （可选）将应用分配到预定义或自定义 **Categories**（类别）中，以便通过 AirWatch 应用目录轻松访问。

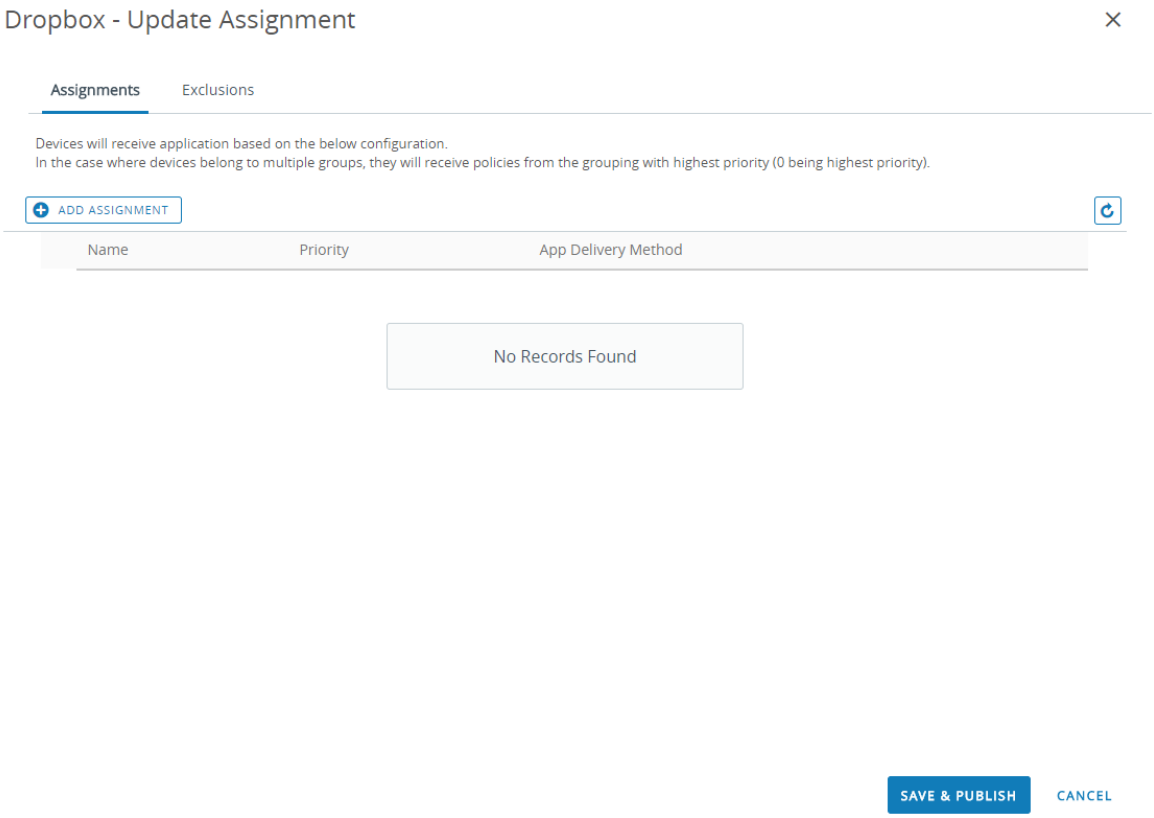
© 2019 Palo Alto Networks, Inc.



9. **SAVE & ASSIGN**（保存并分配）新应用。

© 2019 Palo Alto Networks, Inc.

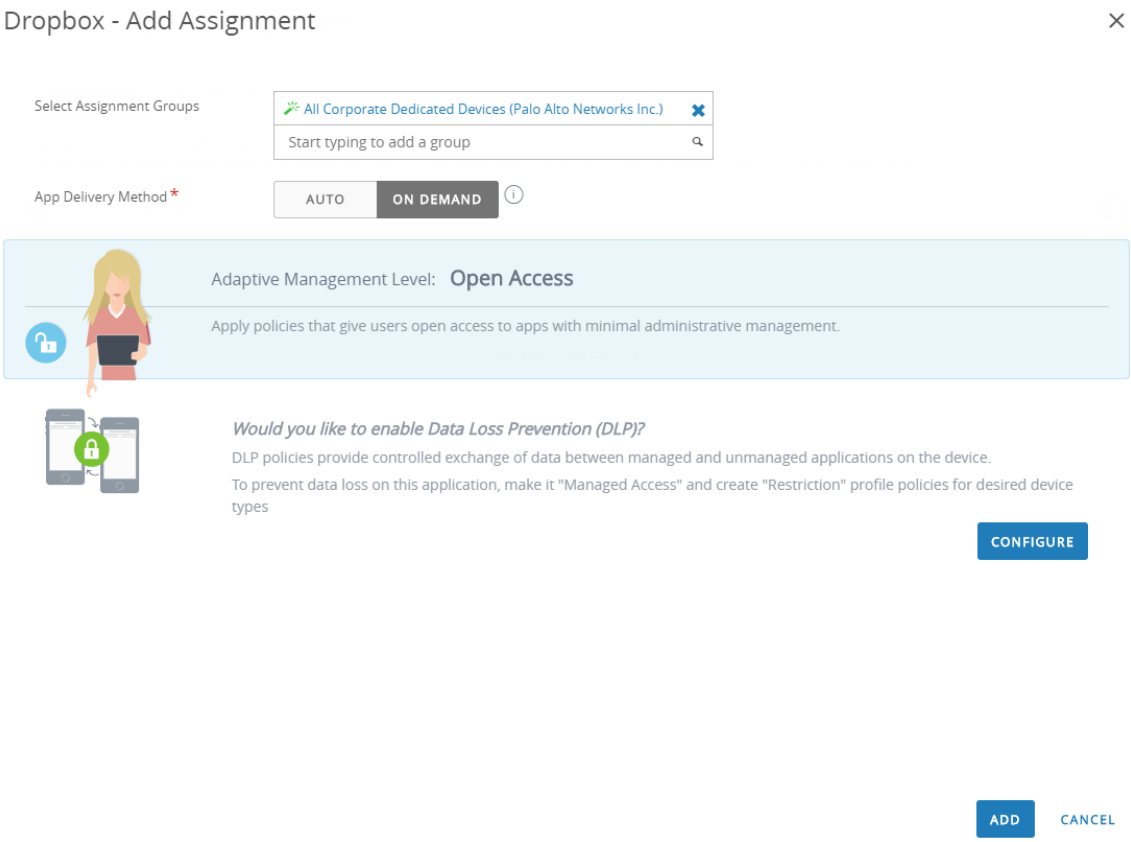
10. 在更新分配对话框中，选择 **Assignments**（分配），然后单击 **ADD ASSIGNMENT**（添加分配），以添加有权访问此应用的智能组。



© 2019 Palo Alto Networks, Inc.

1. 在 **Select Assignment Groups**（选择分配组） 字段中，选择想要获得此应用访问权的智能组。
2. 选择 **App Delivery Method**（应用交付方法）。如果选择 **AUTO**（自动），则应用将自动部署到指定智能组。如果选择 **ON DEMAND**（按需），则必须手动部署此应用。
3. **Add**（添加）新分配。

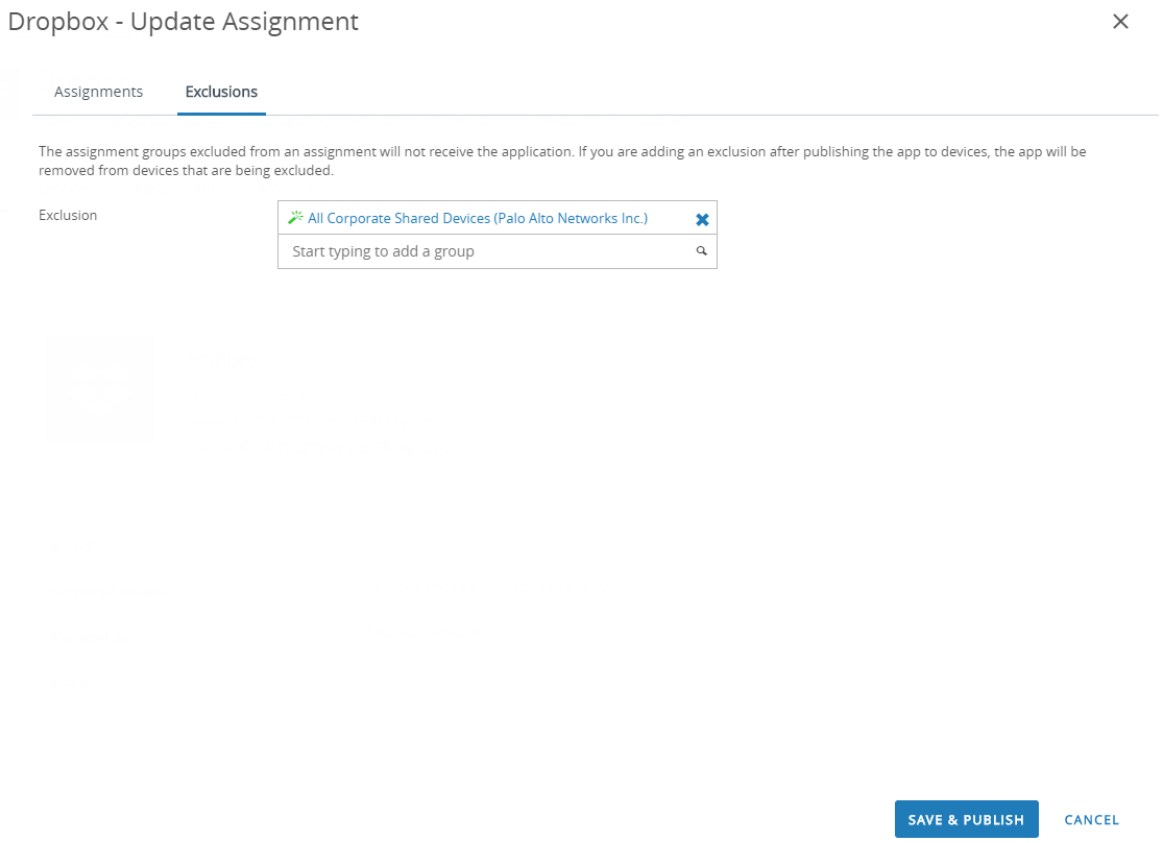
© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

11. （可选）要排除某些智能组访问此应用的权限，请选择 **Exclusions**（排除），然后选择想要从 **Exclusion**（排除）字段排除的智能组。

© 2019 Palo Alto Networks, Inc.



12.**SAVE & PUBLISH**（保存并发布）该配置到分配的智能组。

© 2019 Palo Alto Networks, Inc.

STEP 8 | 要设置连接类型提供程序为 GlobalProtect，请以 XML 格式编辑 VPN 配置文件。

> 要最大程度减少在原始 *XML* 中的额外编辑次数，请在导出配置之前检查 *VPN* 配置文件中的设置。如果在导出 *VPN* 配置文件后需要更改设置，可在原始 *XML* 中进行更改；或者，可更新 *VPN* 配置文件中的设置后重复执行此步骤。

1. 在 **Devices**（设备）> **Profiles**（配置文件）> **List View**（列表视图）中，选择在之前步骤中添加的新配置文件旁的单选按钮，然后选择表格顶部的 **</>XML**。AirWatch 将打开配置文件的 XML 视图。
2. **Export**（导出）配置文件，然后在所选的文本编辑器中打开。
3. 为 GlobalProtect 编辑以下设置：

- 在指定 `PluginPackageFamilyName` 的 `LoclURI` 元素中，将元素更改为：

  `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`
- 在随后的 `Data` 元素中，将值更改为：

  `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

1. 保存对所导出配置文件的更改。
2. 返回 AirWatch，选择 **Devices**（设备）> **Profiles**（配置文件）> **List View**（列表视图）。
3. 创建（选择 **Add**（添加）> **Add Profile**（添加配置文件）> **Windows** > **Windows Phone**）并命名新配置文件。
4. 选择 **Custom Settings**（自定义设置）> **Configure**（配置），然后复制粘贴所编辑的配置。
5. **Save & Publish**（保存并发布）更改。

STEP 9 | 要清除原始配置文件，选择 **Devices**（设备）> **Profiles**（配置文件）> **List View**（列表视图），然后选择 **More Actions**（更多操作）> **Deactivate**（停用）。AirWatch 将该配置文件移至非活动列表。

STEP 10 | 测试配置。

使用 **Microsoft Intune** 配置每应用 **VPN** 配置

Microsoft Intune 是一种基于云的企业移动性管理平台，使您可以从中心位置管理移动端点。GlobalProtect 应用在防火墙和 Microsoft Intune 受管移动端点之间提供设备级或应用级安全连接。使用 GlobalProtect 作为安全连接，可以持续检查流量，在移动端点上强制实施预防威胁的网络安全策略。

有关如何通过 Microsoft Intune 配置每应用 VPN 配置的信息，请参阅以下部分：

- 使用 Microsoft Intune 为 iOS 端点配置每应用 VPN 配置
- 使用 Microsoft Intune 为 Windows 10 UWP 端点配置每应用 VPN 配置

使用 *Microsoft Intune* 为 *iOS* 端点配置每应用 *VPN* 配置

使用 Microsoft Intune 配置 GlobalProtect VPN 访问，可从您的受管移动端点上启用对内部资源的访问权限。在每应用 VPN 配置中，可指定哪些受管应用可通过 VPN 隧道路由流量。非受管应用将继续直接连接到 Internet，而非 VPN 隧道。

要使用 Microsoft Intune 为 iOS 端点配置每应用 VPN 配置，请按以下步骤操作：

STEP 1 | 下载 GlobalProtect iOS 应用。

- 使用 Microsoft Intune 部署 GlobalProtect 移动应用。
- 用户还可直接从 App Store 下载 GlobalProtect 应用。

STEP 2 | 添加应用到 Microsoft Intune。

分配、监控、配置或保护应用之前，必须将其添加到 Microsoft Intune。

© 2019 Palo Alto Networks, Inc.

- 设置 **App type**（应用类型）为 **iOS**。
- 添加 iOS 商店应用到 Microsoft Intune。

STEP 3 | 为 iOS 设置每应用 VPN 配置。

- 创建每应用 VPN 配置文件时，将 **Platform**（平台）设置为 **iOS**，**Connection type**（连接类型）设置为 **Palo Alto Networks GlobalProtect**。
- 关联应用至 VPN 配置文件时，从 **VPNS** 下拉列表中选择每应用 VPN 配置文件。

使用 *Microsoft Intune* 为 *Windows 10 UWP* 端点配置每应用 *VPN* 配置

使用 Microsoft Intune 配置 GlobalProtect VPN 访问，可从您的受管移动端点上启用对内部资源的访问权限。在每应用 VPN 配置中，可指定哪些受管应用可通过 VPN 隧道路由流量。非受管应用将继续直接连接到 Internet，而非 VPN 隧道。

要使用 Microsoft Intune 为 Windows 10 UWP 端点配置每应用 VPN 配置，请按以下步骤操作：

STEP 1 | 下载 GlobalProtect Windows 10 UWP 应用：

- 使用 Microsoft Intune 部署 GlobalProtect 移动应用。
- 用户还可直接从 Microsoft Store 下载 GlobalProtect 应用。

STEP 2 | 配置证书配置文件。

所有每应用 *VNP* 配置均需要基于证书的身份验证。

STEP 3 | 创建新的 Windows 10 UWP VPN 配置文件。

- 设置 **Platform**（平台）为 **Windows 10 and later**（**Windows 10** 及更高版本）。

STEP 4 | 为 Windows 10 UWP 端点配置每应用 VPN 设置。

- 设置 **Connection type**（连接类型）为 **Palo Alto Networks GlobalProtect**。
- 在应用和流量规则区域，设置 **Associate WIP or apps with this VPN**（关联 **WIP** 或应用至此 **VPN**）选项为 **Associate apps with this connection**（关联应用至此连接）。**Enable**（启用）**Restrict VPN connection to these apps**（限制这些应用的 **VPN** 连接）选项，然后 **Add**（添加）想要使用 VPN 连接的关联应用。

使用 **MobileIron** 配置每应用 **VPN** 配置

MobileIron 是一种企业移动性管理平台，使您可以从中央控制台管理移动端点。GlobalProtect 应用在防火墙和 MobileIron 受管移动端点之间提供设备级或应用级安全连接。使用 GlobalProtect 作为安全连接，可以持续检查流量，在移动端点上强制实施预防威胁的网络安全策略。

有关如何通过 MobileIron 配置每应用 VPN 配置的信息，请参阅以下部分：

- 使用 MobileIron 为 iOS 端点配置每应用 VPN 配置

使用 *MobileIron* 为 *iOS* 端点配置每应用 *VPN* 配置

使用 MobileIron 配置 GlobalProtect VPN 访问，可从您的受管移动端点上启用对内部资源的访问权限。在每应用 VPN 配置中，可指定哪些受管应用可通过 VPN 隧道路由流量。非受管应用将继续直接连接到 Internet，而非 VPN 隧道。

要使用 MobileIron 为 iOS 端点配置每应用 VPN 配置，请按以下步骤操作：

STEP 1 | 下载 GlobalProtect iOS 应用。

- 使用 MobileIron 部署 GlobalProtect 移动应用。

© 2019 Palo Alto Networks, Inc.

- 用户还可直接从 App Store 下载 GlobalProtect 应用。

STEP 2 | 添加证书配置文件，然后配置证书设置。

所有每应用 *VNP* 配置均需要基于证书的身份验证。

STEP 3 | 添加每应用 VPN 配置。

- 设置配置类型为 **Per-app VPN**（每应用 **VPN**）。

STEP 4 | 为 iOS 配置每应用 VPN 设置。

- 设置 **Connection Type**（连接类型）为 **Palo Alto Networks GlobalProtect**，然后配置相关设置。

启用 *App Scan* 与 *WildFire* 集成

通过在 AirWatch 中启用 App Scan，您可利用有关应用的 WildFire 威胁情报检测安卓端点上的恶意软件。启用时，AirWatch 代理将安装在安卓端点上的应用列表发送至 AirWatch。这在注册和随后的任意端点检入期间都会发生。然后，AirWatch 定期查询 WildFire 判定结果，并可基于判定结果对端点采取合规操作。

STEP 1 | 在开始之前，请获取 WildFire API 密钥。如果还没有 API 密钥，请联系“支持”。

STEP 2 | 从 AirWatch 选择 **Groups & Settings**（组和设置）> **All Settings**（所有设置）> **Apps**（应用）> **App Scan** > **Third Party Integration**（第三方集成）。

STEP 3 | 选择 **Current Setting**：**Override**（当前设置：覆盖）。

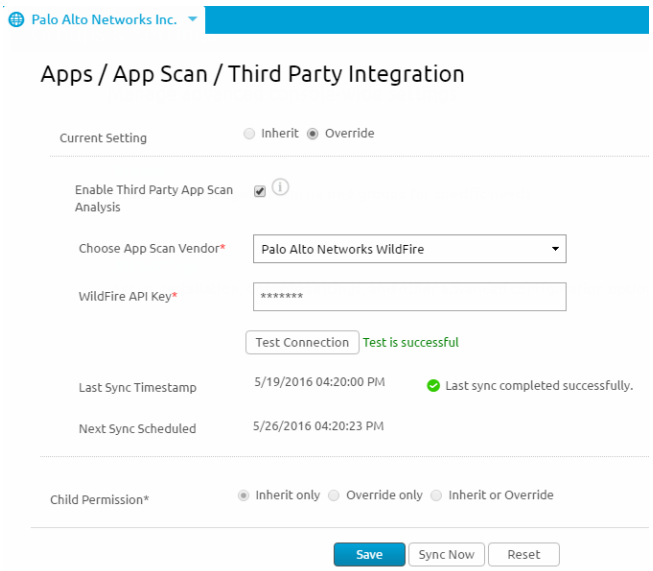
STEP 4 | 选择 **Enable Third Party App Scan Analysis**（启用第三方 **App Scan** 分析）以启用 AirWatch 与 WildFire 之间通信。

STEP 5 | 从 **Choose App Scan Vendor**（选择 **App Scan** 供应商）下拉列表中选择 **Palo Alto Networks WildFire**。

STEP 6 | 输入您的 WildFire API 密钥。

STEP 7 | 单击 **Test Connection**（测试连接）以确保 AirWatch 可与 WildFire 通信。如果测试失败，验证是否连接至互联网，重新输入 API 密钥，然后重新尝试。

© 2019 Palo Alto Networks, Inc.



STEP 8 | **Save**（保持）更改。AirWatch 将调度与 WildFire 进行通信的同步任务，以获得应用程序哈希值的最新判定结果，同时定期运行该任务。单击 **Sync Now**（立即同步）启动与 WildFire 的手动同步。

在用于 *macOS* 端点的 *GlobalProtect* 应用程序中抑制通知

macOS 上的 GlobalProtect 应用程序支持两种类型的扩展：内核（运行 macOS Catalina 10.15.3 或更早版本的 macOS 设备）和系统（运行 macOS Catalina 10.15.4 或更高版本和 GlobalProtect app 5.1.4 或更高版本的 macOS 设备）。如果您已在 GlobalProtect 网关上配置了拆分隧道，或者实施 GlobalProtect 连接以访问网络（请参阅 GlobalProtect 应用程序自定义），则会在 GlobalProtect 应用程序中显示一条通知消息。该消息提示用户启用 macOS 中的内核扩展或系统扩展，当用户访问启用了这些功能的 GlobalProtect 应用程序时，这些扩展被阻止加载。

要允许 GlobalProtect 应用程序用户在不收到通知的情况下自动加载内核扩展或系统扩展，可以使用受支持的移动设备管理系统 (MDM) 为该扩展（如 Airwatch）创建策略。

请参阅以下部分了解如何抑制 macOS 端点上的 GlobalProtect 应用程序通知：

- 在用于 macOS 端点的 GlobalProtect 应用程序中启用内核扩展
- 在用于 macOS 端点的 GlobalProtect 应用程序中启用系统扩展

在用于 macOS 端点的 GlobalProtect 应用程序中启用内核扩展

从 macOS 10.13 开始，Apple 引入了一项软件变更，要求用户在使用内核扩展之前必须先获得批准。

用户可以在 macOS 上手动启用内核扩展（**System Preferences**（系统首选项）> **Security&Privacy**（安全与隐私），并选择 **Allow**（允许）内核扩展），还能使用任何合格的 MDM 供应商创建策略并自动批准内核扩展。Apple Technical Note TN2450（苹果技术说明 TN2450）描述了此进程。

以下工作流已使用 Airwatch 进行了测试。

STEP 1 | 创建内核扩展策略。

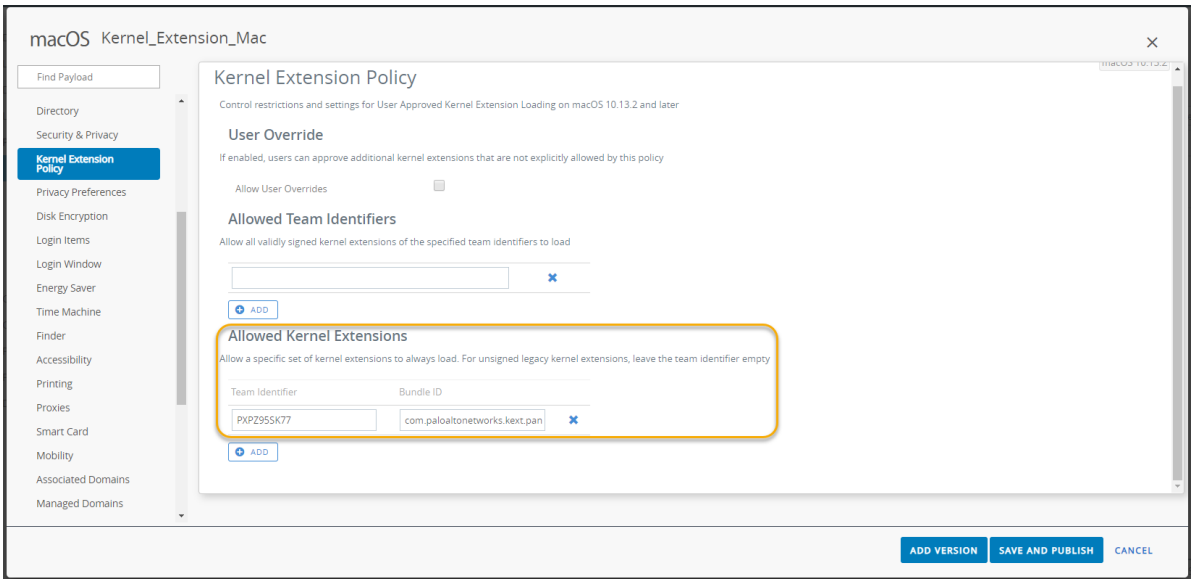
1. 以管理员身份登录 AirWatch。
2. 选择 **Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件），然后从下拉列表中选择 **Add**（添加）> **Add Profile**（添加配置文件）。
3. 在 **Add Profile**（添加配置文件）区域，单击 **Apple macOS**，然后单击 **Device Profile**（设备配置文件）图标。
4. 在 **General**（常规）区域中，指定配置文件的名称。

© 2019 Palo Alto Networks, Inc.

您还可以在列表中选择现有内核扩展配置文件（**Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件））。

STEP 2 | 添加内核扩展并将相关策略分发到 macOS 设备。

1. 选择 **Kernel Extension Policy**（内核扩展策略）。
2. 输入 GlobalProtect 应用程序使用的 **Team Identifier**（团队标识符）(**PXPZ95SK77**)。
3. 输入 **Bundle ID**（包 **ID**）(**com.paloaltonetworks.kext.pangpd**)。



4. 单击 **Save and Publish**（保存并发布）保存更改。

在用于 **macOS** 端点的 **GlobalProtect** 应用程序中启用系统扩展

从 macOS 10.15.4 开始，苹果限制了对内核扩展的支持。GlobalProtect 应用程序将使用系统扩展而非内核扩展。用户必须先批准系统扩展，然后才能使用它们。

您不仅可以启用系统扩展，还可以在 *GlobalProtect*应用程序中启用网络扩展，以阻止 *Network Extensions Configuration*（网络扩展配置）弹出提示（用于拆分隧道和实施 *GlobalProtect* 连接以访问网络等功能）。您可以通过 *Jamf Pro* 等移动设备管理系统 *(MDM)* 自动加载网络扩展，而不会接收弹出提示。有关如何使用 Jamf Pro 启用系统和网络扩展的信息，请参阅知识库文章：https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAW8。

使用以下步骤将配置文件配置为使用 AirWatch 自动批准系统扩展。在使用 AirWatch 测试此配置后，您可以使用任何合格的 MDM 供应商来创建和实施此配置文件。

STEP 1 | 创建系统扩展配置文件。

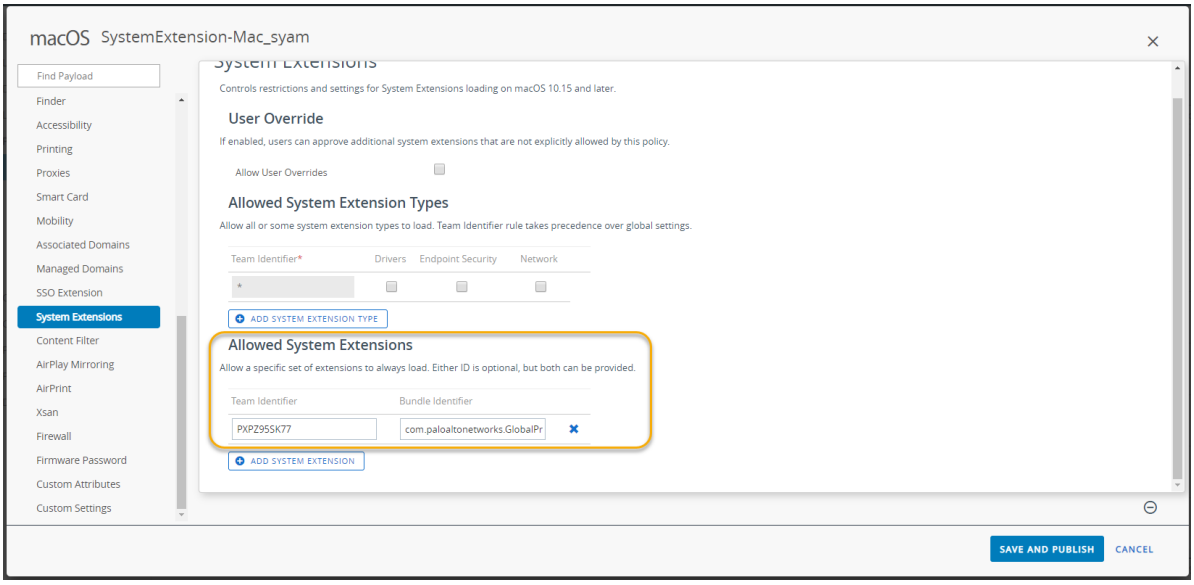
1. 以管理员身份登录 AirWatch。
2. 选择 **Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件），然后从下拉列表中选择 **Add**（添加）> **Add Profile**（添加配置文件）。
3. 在 **Add Profile**（添加配置文件）区域，单击 **Apple macOS**，然后单击 **Device Profile**（设备配置文件）图标。
4. 在 **General**（常规）区域中，指定配置文件的名称。

   您还可以在列表中选择现有系统扩展配置文件（**Devices**（设备）> **Profiles & Resources**（配置文件和资源）> **Profiles**（配置文件））。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 添加系统扩展。

1. 选择 **System Extensions**（系统扩展）。
2. 输入 GlobalProtect 应用程序使用的 **Team Identifier**（团队标识符）(**PXPZ95SK77**)。
3. 输入 **Bundle Identifier**（包标识符）(**com.paloaltonetworks.GlobalProtect.client.extension**)



4. 单击 **Save and Publish**（保存并发布）保存更改。

使用其他第三方 MDM 管理 GlobalProtect 应用

如果未使用受支持的第三方 MDM 供应商，则可以使用其他第三方 MDM 系统部署和管理 GlobalProtect 应用：

- 配置 GlobalProtect iOS 应用
  - 示例：GlobalProtect iOS 应用设备级别 VPN 配置
  - 示例：GlobalProtect iOS 应用应用级别 VPN 配置
- 配置 GlobalProtect 安卓应用
  - 示例：设置 VPN 配置
  - 示例：删除 VPN 配置

配置 *GlobalProtect iOS* 应用

尽管第三方 MDM 系统可让您推送配置设置以访问企业资源和提供实施端点限制的机制，但它无法保护移动端点与服务之间的连接。要使应用程序能够建立安全连接，您必须在端点上启用 VPN 支持。

下表描述了可使用第三方 MDM 系统配置的典型设置。

设置	说明	值
连接类型	策略启用的连接类型。	自定义 `SSL`
标识符	自定义 SSL VPN 标识符（反向 DNS 格式）。	`com.paloaltonetworks.globalprotect.vpn`

© 2019 Palo Alto Networks, Inc.

设置	说明	值
服务器	GlobalProtect 门户的主机名称或 IP 地址。	**<hostname or IP address>** 例如：**gp.paloaltonetworks.com**
帐户	验证连接的用户帐户。	**<username>**
用户身份验证	连接身份验证类型。	证书 | 密码
凭据	（仅证书用户身份验证）验证连接的凭据。	**<credential>** 例如：**clientcredial.p12**
按需启用 VPN	（可选）将建立此连接和按需操作的域和主机名： • 始终建立连接 • 从不建立连接 • 根据需要建立连接	**<domain and hostname and the on-demand action>** 例如： gp.acme.com; Never establish

示例：**GlobalProtect iOS** 应用设备级别 **VPN** 配置

以下示例显示了包含 VPN 载荷的 XML 配置，您可用其验证 GlobalProtect iOS 应用的设备级别 VPN 配置。

```
<?xml version="1.0"
encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Configures VPN settings, including authentication.</string>
<key>PayloadDisplayName</key>
<string>VPN (Sample Device Level VPN)</string>
<key>PayloadIdentifier</key>
<string>Sample Device Level VPN.vpn</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadType</key>
<string>com.apple.vpn.managed</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011d</string>
<key>UserDefinedName</key>
<string>Sample Device Level VPN</string>
<key>Proxies</key>
<dict/>
<key>VPNType</key>
<string>VPN</string>
<key>VPNSubType</key>
<string>com.paloaltonetworks.GlobalProtect.vpnplugin</string>
<key>IPv4</key>
<dict>
```


© 2019 Palo Alto Networks, Inc.

```
<key>OverridePrimary</key>
<integer>0</integer>
</dict>
<key>VPN</key>
<dict>
<key>RemoteAddress</key>
<string>cademogp.paloaltonetworks.com</string>
<key>AuthName</key>
<string></string>
<key>DisconnectOnIdle</key>
<integer>0</integer>
<key>OnDemandEnabled</key>
<integer>1</integer>
<key>OnDemandRules</key>
<array>
<dict>
<key>Action</key>
<string>Connect</string>
</dict>
</array>
<key>AuthenticationMethod</key>
<string>Password</string>
</dict>
<key>VendorConfig</key>
<dict>
<key>AllowPortalProfile</key>
<integer>0</integer>
<key>FromAspen</key>
<integer>1</integer>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>Sample Device Level VPN</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadDescription</key>
<string>Profile Description</string>
<key>PayloadIdentifier</key>
<string>Sample Device Level VPN</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011c</string>
<key>PayloadRemovalDisallowed</key>
<false/>
</dict>
</plist>
```

示例：**GlobalProtect iOS** 应用应用级别 **VPN** 配置

以下示例显示了包含 VPN 载荷的 XML 配置，您可用其验证 GlobalProtect iOS 应用的应用级别 VPN 配置。

```
<?xml version="1.0"
encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
```


© 2019 Palo Alto Networks, Inc.

```
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Configures VPN settings, including authentication.</string>
<key>PayloadDisplayName</key>
<string>VPN (Sample App Level VPN)</string>
<key>PayloadIdentifier</key>
<string>Sample App Level VPN.vpn</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadType</key>
<string>com.apple.vpn.managed.applayer</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>VPNUUID</key>
<string>cGFuU2FtcGxlIEFwcCBMZXZlbCBWUE52cG5TYW1wbGUgQXBwIExldmVsIFZQTg==</
string>
<key>SafariDomains</key>
<array>
<string>*.paloaltonetworks.com</string>
</array>
<key>PayloadUUID</key>
<string>54370008-205f-7c59-0000-01a1</string>
<key>UserDefinedName</key>
<string>Sample App Level VPN</string>
<key>Proxies</key>
<dict/>
<key>VPNType</key>
<string>VPN</string>
<key>VPNSubType</key>
<string>com.paloaltonetworks.GlobalProtect.vpnplugin</string>
<key>IPv4</key>
<dict>
<key>OverridePrimary</key>
<integer>0</integer>
</dict>
<key>VPN</key>
<dict>
<key>RemoteAddress</key>
<string>cademogp.paloaltonetworks.com</string>
<key>AuthName</key>
<string></string>
<key>OnDemandMatchAppEnabled</key>
<integer>1</integer>
<key>OnDemandEnabled</key>
<integer>1</integer>
<key>DisconnectOnIdle</key>
<integer>0</integer>
<key>AuthenticationMethod</key>
<string>Password</string>
</dict>
<key>VendorConfig</key>
<dict>
<key>OnlyAppLevel</key>
<integer>1</integer>
<key>AllowPortalProfile</key>
<integer>0</integer>
<key>FromAspen</key>
<integer>1</integer>
</dict>
</dict>
```


© 2019 Palo Alto Networks, Inc.

```
</array>
<key>PayloadDisplayName</key>
<string>Sample App Level VPN</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadDescription</key>
<string>Profile Description</string>
<key>PayloadIdentifier</key>
<string>Sample App Level VPN</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011c</string>
<key>PayloadRemovalDisallowed</key>
<false/>
</dict>
</plist>
```

配置 *GlobalProtect* 安卓应用

可从支持 Android For Work 应用数据限制的任何第三方移动设备 (MDM) 系统在 Android For Work 端点上部署和配置 GlobalProtect 应用。

在安卓端点上，根据在 GlobalProtect 网关上配置的访问路由，将流量路由通过 VPN 隧道。从管理 Android for Work 端点的第三方 MDM，可进一步定义路由通过 VPN 隧道的流量。

如果端点属于企业所有，端点所有人管理整个端点，包括在此端点上安装的所有应用。默认情况下，根据在网关上定义的访问路由，安装的所有应用可通过 VPN 隧道发送流量。

如果是自带设备 (BYOD) 环境，端点不属于企业所有，使用工作配置文件区分业务应用和个人应用。默认情况下，根据在网关上定义的访问路由，只有工作配置文件中的受管应用才能通过 VPN 隧道发送流量。在端点个人部分安装的应用不能通过工作配置文件中安装的受管 GlobalProtect 应用设置的 VPN 隧道发送流量。

要路由甚至更少应用的流量，可启用按应用 VPN，这样 GlobalProtect 只路由来自特定受管应用的流量。对于按应用 VPN，您可以为特定受管应用程序设置是否让流量通过 VPN 隧道路由的允许列表或阻止列表。

作为 VPN 配置的一部分，还可指定用户如何连接 VPN。将 VPN 连接方法配置为 **user-logon**（用户登录）时，GlobalProtect 应用将自动建立连接。将 VPN 连接方法配置为 **on-demand**（按需）时，用户必须手动启动连接。

在 *MDM* 中定义的 *VPN* 连接方法的优先级高于在 *GlobalProtect* 门户配置中定义的连接方法。

删除 VPN 配置会自动将 GlobalProtect 应用恢复到原始配置设置。

要配置 GlobalProtect 安卓应用，配置以下安卓应用限制。

密钥	值类型	说明	示例
门户	字符串	门户的 IP 地址或完全限定域名 (FQDN)。	`10.1.8.190`
用户名	字符串	用户的用户名。	`john`
密码	字符串	用户的密码。	`Passwd!234`

© 2019 Palo Alto Networks, Inc.

密钥	值类型	说明	示例
mobile_id	字符串	第三方 MDM 服务配置用于唯一标识移动设备的移动 ID 。GlobalProtect 使用此移动 ID 检索设备信息。	**5188a8193be43f42d332dde5cb2c941e**
证书	字符串 (Base64)	用于对代理和门户进行身份验证的客户端证书。	**DAFDSaweEWQ23wDSAFD**...
client_certificate_passphrase	字符串	与客户端证书相关联的密钥。	**PA$$W0RD$123**
app_list	字符串	每应用 VPN 配置。字符串以允许列表或阻止列表开头，后面是以分号隔开的一组应用程序名称。允许列表指定将使用 VPN 隧道进行网络通信的应用程序。不在允许列表中或未明确列入阻止列表的任何其他应用程序的网络流量将不会通过 VPN 隧道。	允许列表 **|** 阻止列表：**com.google.calendar; com.android.email; com.android.chrome**
connect_method	字符串	用户登录通过其 Windows 凭证自动将用户连接到 GlobalProtect 门户，或是按需手动将用户与网关相连接。	**user-logon | on-demand**
remove_vpn_config_via_restriction	Boolean	永久删除所有 GlobalProtect VPN 配置信息。	**true | false**

示例：设置 **VPN** 配置

```
private static String RESTRICTION_PORTAL
= "portal";
private static String RESTRICTION_USERNAME = "username";
private static String RESTRICTION_PASSWORD = "password";
private static String RESTRICTION_CONNECT_METHOD = "connect_method";
private static String RESTRICTION_CLIENT_CERTIFICATE
= "client_certificate";
private static String RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE
= "client_certificate_passphrase";
private static String RESTRICTION_APP_LIST = "app_list";
private static String RESTRICTION_REMOVE_CONFIG =
 "remove_vpn_config_via_restriction";

Bundle config = new Bundle();
config.putString(RESTRICTION_PORTAL, "192.168.1.1");
config.putString(RESTRICTION_USERNAME, "john");
config.putString(RESTRICTION_PASSWORD, "Passwd!234");
config.putString(RESTRICTION_CONNECT_METHOD, "user-logon");
config.putString(RESTRICTION_CLIENT_CERTIFICATE, "DAFDSaweEWQ23wDSAFD....");
config.putString(RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE,
"PA$$W0RD$123");
config.putString(RESTRICTION_APP_LIST, "allow
 list:com.android.chrome;com.android.calendar");

DevicePolicyManager dpm = (DevicePolicyManager)
getSystemService(Context.DEVICE_POLICY_SERVICE);
```


© 2019 Palo Alto Networks, Inc.

```
dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.getComponentName(this),
"com.paloaltonetworks.globalprotect", config);
```

示例：删除 VPN 配置

```
Bundle config = new Bundle();
config.putBoolean(RESTRICTION_REMOVE_CONFIG, true );
DevicePolicyManager dpm = (DevicePolicyManager)
getSystemService(Context.DEVICE_POLICY_SERVICE);
dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.
getComponentName(this),"com.paloaltonetworks.globalprotect",
config);
```

用于 *IoT* 设备的 *GlobalProtect*

通过用于 IoT 的 GlobalProtect，您可以保护来自 IoT 设备的流量并将安全策略实施扩展到您的 IoT 设备。在为 IoT 设置 GlobalProtect 后，GlobalProtect 应用程序使用客户端证书和（可选）用户名与密码进行 GlobalProtect 门户或网关身份验证。身份验证成功后，GlobalProtect 应用程序将建立一个 IPSec 隧道。如果使用 IPSec 的连接失败，您可以将 GlobalProtect 应用程序配置为回退到 SSL 隧道。请参阅 Palo Alto Networks 兼容性矩阵，以获取 IoT 设备操作系统支持的功能列表。

> 满足 IoT 要求的 GlobalProtect
> 为 IoT 设备配置 GlobalProtect 门户和网关
> 在 Android 上安装用于 IoT 的 GlobalProtect
> 在 Raspbian 上安装用于 IoT 的 GlobalProtect
> 在 Ubuntu 上安装用于 IoT 的 GlobalProtect
> 在 Windows 上安装用于 IoT 的 GlobalProtect

满足 IoT 要求的 GlobalProtect

用于 IoT 的 GlobalProtect 具有以下要求：

- Prisma 访问或 GlobalProtect 订阅
- 防火墙正在运行 PAN-OS 10.0（立即升级）
- 下列操作系统之一：
  - Android
  - Raspbian
  - Ubuntu
  - Windows IoT 企业版
- 128MB RAM
- 4GB 内存
- x86 和 ARMv7 或 ARMv5 处理器
- 使用 CLI 或 WebDM 中的快照应用程序包进行安装

© 2019 Palo Alto Networks, Inc.

为 IoT 设备配置 GlobalProtect 门户和网关

STEP 1 | 查看 满足 IoT 要求的 GlobalProtect。

STEP 2 | 配置 GlobalProtect 网关以支持用于 IoT 的 GlobalProtect 应用程序。

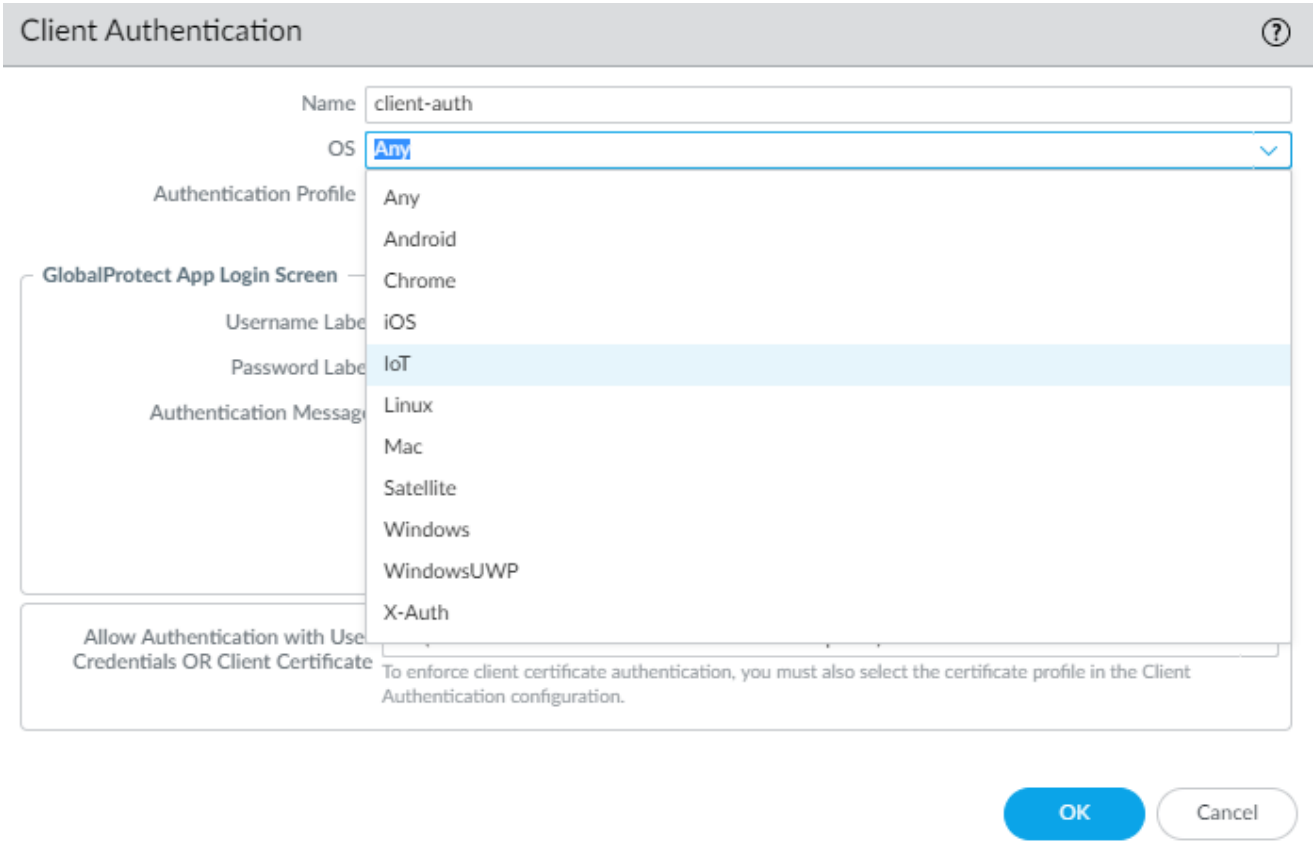
1. 完成设置 GlobalProtect 网关的前提任务。
2. 为每个支持适用于 IoT 的 GlobalProtect 应用程序的网关安装 GlobalProtect 订阅。如果使用 Prisma 访问，则不需要 GlobalProtect 订阅。
3. 为您的 IoT 设备自定义网关配置：

   配置网关时，可以指定专门应用于 IoT 的客户端身份验证设置。例如，您可以将 Windows 和 macOS 端点配置为使用双因素身份验证，并要求 IoT 设备使用基于证书的身份验证。

   您还可以配置受支持的网络和客户端设置，例如特定 IP 池、访问路由和用于 IoT 设备的拆分隧道。

   1. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关），然后选择或 **Add**（添加）一个网关配置。
   2. 为 IoT 设备添加客户端身份验证配置：

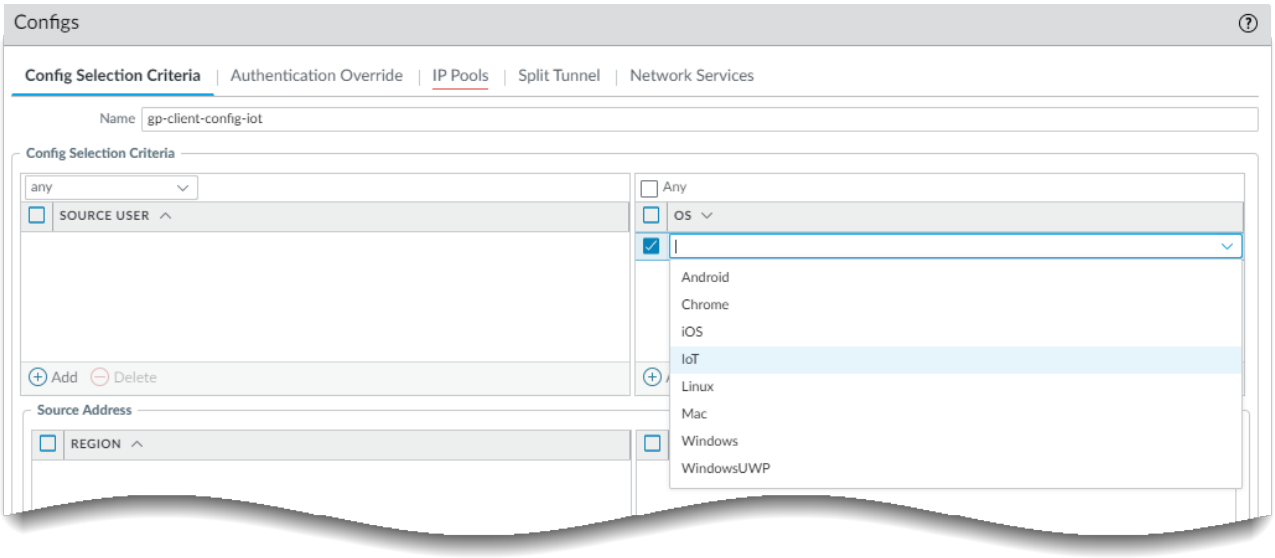
      1. 选择 **Authentication**（身份验证）并 **Add**（添加）一个新的客户端身份验证配置。
      2. 输入一个 **Name**（名称）以标识客户端身份验证配置，将 **OS**（操作系统）设置为 **IoT**，指定用于对此网关上用户进行身份验证的身份验证配置文件。选择启用客户端证书身份验证的配置文件。



      3. 单击 **OK**（确定）。
3. 要配置仅适用于 IoT 端点的特定客户端设置，请配置新客户端设置配置：

© 2019 Palo Alto Networks, Inc.

1. 选择 **Agent**（代理）并 **Add**（添加）一个新的客户端设置配置。
2. 根据需要配置客户端身份验证设置。
3. 选择 **User/User Group**（用户/用户组），然后 **Add**（添加）操作系统，再选择 **IoT**。



4. 单击 **OK**（确定）。

4. 单击 **OK**（确定）。
5. **Commit**（提交）配置。

STEP 3 | 配置门户以支持适用于 IoT 设备的 GlobalProtect 应用程序。

要支持 IoT 设备，必须配置 GlobalProtect 应用程序可以连接的一个或多个网关，然后配置门户和应用程序设置。门户将配置信息和有关可用网关的信息发送到应用程序。从 GlobalProtect 门户接收到配置后，应用程序会发现客户端配置中列出的网关，并选择最佳网关。使用以下工作流配置 GlobalProtect 门户，以支持适用于 IoT 设备的 GlobalProtect 应用程序。

1. 如果尚未完成此操作，请完成设置 GlobalProtect 门户的前提任务。
2. 定义适用于 IoT 设备的客户端设置以进行门户身份验证。
   1. 选择 **Network**（网络）> **GlobalProtect** > **Portal**（门户），然后选择门户配置。
   2. 配置用户访问门户时应用于 IoT 设备的客户端身份验证设置：
      1. 选择 **Authentication**（身份验证），然后 **Add**（添加）一个新的客户端身份验证配置。
      2. 输入一个 **Name**（名称）以标识客户端身份验证配置，将 **OS**（操作系统）设置为 **IoT**，指定用于对此门户上用户进行身份验证的身份验证配置文件。选择启用客户端证书身份验证的配置文件。
3. 为 IoT 设备自定义代理配置。

   修改现有配置还是创建新配置取决于您的环境。例如，若使用特定于操作系统的网关或希望收集特定于 IoT 设备的主机信息，请考虑创建新的代理配置。

   有关受支持功能的信息，请参阅 Palo Alto Networks 兼容性矩阵，以获取 IoT 设备操作系统支持的功能列表。

   1. 定义 GlobalProtect 代理配置：
   2. 选择 **Agent**（代理），然后选择一个现有的或**Add**（添加）一个新的门户代理配置。
   3. 为 IoT 设备配置身份验证设置。
   4. 选择 **User/User Group**（用户/用户组），然后添加 **OS**（操作系统），再选择 **IoT**。
   5. 指定采用此配置的用户可连接至的外部网关。

© 2019 Palo Alto Networks, Inc.

6. （可选）选择 **App**（应用程序）并自定义适用于 IoT 的 GlobalProtect 应用程序门户设置。GlobalProtect 应用程序会丢弃任何不适用于 IoT 的设置。有关操作系统支持的功能列表，请参阅 Palo Alto Networks 兼容性矩阵，以获取 IoT 设备操作系统支持的功能列表。
7. 双击 **OK**（确定）。
8. **Commit**（提交）配置。

4. 在 IoT 设备上实施策略（**Objects**（对象） > **GlobalProtect** > **HIP Objects**（**HIP** 对象））。

   现在，您可以使用特定于 IoT 设备的主机信息创建 HIP 对象，并将其用于任何 HIP 配置文件中的匹配条件。然后，可以在策略规则中使用 HIP 配置文件作为匹配条件，以实施相应安全策略。

   1. 选择 **General**（常规） > **Host Info**（主机信息） > **OS**（操作系统）.
   2. 选择 **Contains**（包含） > **IoT**。
   3. 单击 **OK**（确定）。
   4. 根据需要创建其他 HIP 对象。
   5. 配置基于 HIP 的策略实施。

STEP 4 | 为 IoT 安装并设置 GlobalProtect 应用程序。

使用为 IoT 设备操作系统提供的说明。

- 在 Android 上安装用于 IoT 的 GlobalProtect
- 在 Raspbian 上安装用于 IoT 的 GlobalProtect
- 在 Ubuntu 上安装用于 IoT 的 GlobalProtect
- 在 Windows 上安装用于 IoT 的 GlobalProtect

© 2019 Palo Alto Networks, Inc.

在 Android 上安装用于 IoT 的 GlobalProtect

要在 Android 设备上使用用于 IoT 的 GlobalProtect，必须将应用程序和 GlobalProtect 配置作为系统应用程序构建到 Android 操作系统映像中。要使 GlobalProtect 在无头模式下运行，必须使用 GlobalProtect 应用程序包部署预配置文件。

STEP 1 | 添加 GlobalProtect.apk 作为 Android 操作系统映像中的预构建系统应用程序。

1. 从 Support Site（支持站点）选择 **Updates**（更新）> **Software Updates**（软件更新），然后下载 GlobalProtect APK。
2. 解码 `android_src_tree_root/packages/app/` 目录中的 APK 文件。

   解码器将应用程序解压到 GlobalProtect 文件夹中。
3. 在 GlobalProtect 文件夹中，创建 `Android.mk` 文件。此文件定义编码器将用于构建系统的源和共享库。

   编辑文件以包含以下内容：

```
LOCAL_PATH := $(call my-dir)
include $(CLEAR_VARS)
LOCAL_MODULE_TAGS := optional
LOCAL_MODULE := GlobalProtect
LOCAL_SRC_FILES := $(LOCAL_MODULE).apk
LOCAL_MODULE_CLASS := APPS
LOCAL_MODULE_SUFFIX := $(COMMON_ANDROID_PACKAGE_SUFFIX)
LOCAL_CERTIFICATE := PRESIGNED
include $(BUILD_PREBUILT)
```

4. 对于 `android_src_tree_root/vendor/` 中的任何其他 MK 文件，请添加以下行：

```
PRODUCT_PACKAGES += GlobalProtect
```

5. 将 libgpjni.so 添加到 `/system/lib` 或 `/system/lib64` 中，具体取决于 IoT 设备支持的 CPU 架构。用 apktool 解码 GlobalProtect.apk 之后，可以从 lib 目录中检索 libgpjni.so 文件。

STEP 2 | 修改 Android 框架源代码以预授权 VPN 连接的权限请求弹出窗口。

编辑 `android_src_tree_root/frameworks/base/services/core/java/com/android/server/connectivity/Vpn.java` 文件以包含以下代码段：

```
private boolean isVpnUserPreConsented(String packageName) {

    if ("com.paloaltonetworks.globalprotect".equals(packageName)){
        Log.v(TAG, "IoT, isVpnUserPreConsented always true");
    return true;
    }
    AppOpsManager appOps =
        (AppOpsManager) mContext.getSystemService(Context.APP_OPS_SERVICE);

    // Verify that the caller matches the given package and has permission
 to activate VPNs.
    return
 appOps.noteOpNoThrow(AppOpsManager.OP_ACTIVATE_VPN,Binder.getCallingUid(),
        packageName) == AppOpsManager.MODE_ALLOWED;
    }
}
```


© 2019 Palo Alto Networks, Inc.

STEP 3 | 对于 Android 8.0 及更高版本，自定义 Android 行为以抑制通知栏中的 GlobalProtect 图标。

编辑 `android_src_tree_root/frameworks/base/services/core/java/com/android/server/am/ActiveServices.java` 文件以包含以下代码段。

```
if ( r.packageName.equals("com.paloaltonetworks.globalprotect") ) {
    Slog.d(TAG, "not to show the foreground service running notification for
 IoT");
} else {
    r.postNotification();
}
```

STEP 4 | 配置要为 Android IoT 设备预先部署的 VPN 设置。

1. 以如下格式创建配置文件 (`globalprotect.conf`) 并编辑 GlobalProtect 门户的 IP 地址和身份验证设置：用户名和密码，或客户端证书路径 (client-cert-path) 和密码短语文件 (client-cert-passphrase)。

   基于用户名和密码的身份验证

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
    <PanSetup>
                <Portal>192.168.1.23</Portal>
    </PanSetup>
        <Settings>
                <head-less>yes</head-less>
                <os-type>IoT</os-type>
                <username>user1</username>
                <password>mypassw0rd</password>
                <log-path-service>/home/gptest/Desktop/data/gps</log-path-
service>
                <log-path-agent>/home/gptest/Desktop/data/gpadata</log-
path-agent>
        </Settings>
</GlobalProtect>
```

   基于客户端证书的身份验证

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
    <PanSetup>
                <Portal>192.168.1.23</Portal>
    </PanSetup>
        <Settings>
                <head-less>yes</head-less>
                <os-type>IoT</os-type>
                <client-cert-path>/home/gptest/Desktop/data/
pan_client_cert.pfx</client-cert-path>
                <client-cert-passphrase>/home/gptest/Desktop/data/
pan_client_cert_passcode.dat</client-cert-passphrase>
                <username>user1</username>
                <password>paloalto</password>
                <log-path-service>/home/gptest/Desktop/data/gps</log-path-
service>
                <log-path-agent>/home/gptest/Desktop/data/gpadata</log-
path-agent>
        </Settings>
```


© 2019 Palo Alto Networks, Inc.

```
</GlobalProtect>
```

2. 以 Base64 格式编码 `globalprotect.conf` 文件，并将其保存到 `android_src_tree_root/system/config/` 目录。

   如果需要，可以将文件保存到其他位置。但是，必须在 `android_src_tree_root/assets/gp_conf_location.txt` 文件中编辑此配置的位置。

STEP 5 | 构建 GlobalProtect APK 文件。

STEP 6 | 签署 GlobalProtect APK 文件。

STEP 7 | 将新操作系统作为系统映像的一部分推送到 Android 设备上，然后将新操作系统推送到 Android 设备上。

© 2019 Palo Alto Networks, Inc.

在 Raspbian 上安装用于 IoT 的 GlobalProtect

要在 Raspbian 设备上安装用于 IoT 的 GlobalProtect，请完成以下步骤。

用于 *Raspbian* 和 *Ubuntu* 上 *IoT* 的 *GlobalProtect* 仅支持基于 *Arm* 的架构。

STEP 1 | 从 Support Site（支持站点）选择 **Updates**（更新）> **Software Updates**（软件更新），然后从操作系统下载 GlobalProtect 包。

STEP 2 | 安装用于 IoT 的 GlobalProtect 应用程序。

在 IoT 设备上使用 **sudo dpkg -i GlobalProtect_deb_arm<*version*>.deb** 命令安装软件。

```
sudo dpkg -i GlobalProtect_deb_arm-5.1.0.0-84.deb
```

要在之后卸载该软件，请使用 ***sudo dpkg -P globalprotect*** 命令。

STEP 3 | 配置要为 Raspbian IoT 设备预先部署的 VPN 设置。

1. 在 `client-cert` 路径中，以 pcks12 格式导入证书，并以 .pfx 扩展名保存文件（例如，**pan_client_cert.pfx**）。
2. 在 `client-cert-passphrase` 路径中，保存扩展名为 .dat 的通行码文件（例如，**pan_client_cert_passcode.dat**）
3. 在 `log-path-service` 路径中，如果没有使用 PanGPS 的默认路径（例如，`/opt/paloaltonetworks/globalprotect`），请确保 `log-setting` 路径文件夹与 `opt/paloaltonetworks` 下的 globalprotect 文件夹具有相同特权。
4. 以如下格式创建 `/opt/paloaltonetworks/globalprotect/pangps.xml` 预部署配置文件，并编辑 GlobalProtect 门户的 IP 地址和身份验证设置：用户名和密码，或客户端证书路径 (**client-cert-path**) 和密码短语文件 (**client-cert-passphrase**)。您还可以指定一个可选文件夹，在其中存储 GlobalProtect 服务 (**log-path-service**) 和代理 (**log-path-agent**) 日志。

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
 <PanSetup>
          <Portal>192.168.1.160</Portal>       //pre-deployed portal address
</PanSetup>
 <PanGPS>
 </PanGPS>
 <Settings>
         <portal-timeout>5</portal-timeout>
         <connect-timeout>5</connect-timeout>
         <receive-timeout>30</receive-timeout>
         <os-type>IoT</os-type>             //pre-deployed OS type for IoT.
 If this tag does not present, GP will automatic detect the OS type.
         <head-less>yes</head-less>       //pre-deployed head-less mode
         <username>abc</username>    //optional pre-deployed username
         <password>xyz</password>       //optional pre-deployed password
         <client-cert-path>cli_cert_path</client-cert-path>       //optional
 pre-deployed client certificate file(p12) path
```


© 2019 Palo Alto Networks, Inc.

```
        <client-cert-passphrase>cli_cert_passphrase_path< /client-cert-
passphrase>       //optional pre-deployed client certificate passphrase file
 path
        <log-path-service>/tmp/gps</log-path-service>  //optional pre-
deployed log folder for PanGPS
        <log-path-agent>/tmp/gpa</log-path-agent>      //optional pre-
deployed log folder for PanGPA and globalprotect CLI
 </Settings>
</GlobalProtect>
```

STEP 4 | 重启 GlobalProtect 进程以使预部署配置生效。

STEP 5 | 部署 IoT 设备后，可以根据需要使用 **globalprotect collect-log** 命令收集日志。

```
user@raspbianhost:~/Desktop/data$ globalprotect collect-log
The support file is saved to /home/gptest/.GlobalProtect/
GlobalProtectLogs.tgz
```

STEP 6 | （可选）如果身份验证方法是用户名/密码和客户端证书身份验证组合，请确保客户端证书的 **CommonName** 与用户名匹配。

© 2019 Palo Alto Networks, Inc.

在 Ubuntu 上安装用于 IoT 的 GlobalProtect

要在 Ubuntu 设备上安装用于 IoT 的 GlobalProtect，请完成以下步骤。

用于 *Raspbian* 和 *Ubuntu* 上 *IoT* 的 *GlobalProtect* 仅支持基于 *Arm* 的架构。

STEP 1 | 从 Support Site（支持站点）选择 **Updates**（更新）> **Software Updates**（软件更新），然后从操作系统下载 GlobalProtect 包。

STEP 2 | 安装用于 IoT 的 GlobalProtect 应用程序。

在 IoT 设备上使用 **sudo dpkg -i GlobalProtect_deb *<version>*.deb** 命令安装软件。

```
user@linuxhost:~$ sudo dpkg -i GlobalProtect_deb-4.1.0.0-19.deb
```

要在之后卸载该软件，请使用 ***sudo dpkg -P globalprotect*** 命令。

STEP 3 | 配置要为 Ubuntu IoT 设备预先部署的 VPN 设置。

1. 在 `client-cert` 路径中，以 pcks12 格式导入证书，并以 .pfx 扩展名保存文件（例如，**pan_client_cert.pfx**）。
2. 在 `client-cert-passphrase` 路径中，保存扩展名为 .dat 的通行码文件（例如，**pan_client_cert_passcode.dat**）
3. 在 `log-path-service` 路径中，如果没有使用 PanGPS 的默认路径（例如，`/opt/paloaltonetworks/globalprotect`），请确保 `log-setting` 路径文件夹与 `opt/paloaltonetworks` 下的 globalprotect 文件夹具有相同特权。
4. 以如下格式创建 `/opt/paloaltonetworks/globalprotect/pangps.xml` 预部署配置文件，并编辑 GlobalProtect 门户的 IP 地址和身份验证设置：用户名和密码，或客户端证书路径 (**client-cert-path**) 和密码短语文件 (**client-cert-passphrase**)。您还可以指定一个可选文件夹，在其中存储 GlobalProtect 服务 (**log-path-service**) 和代理 (**log-path-agent**) 日志。

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
 <PanSetup>
          <Portal>192.168.1.160</Portal>       //pre-deployed portal address
</PanSetup>
 <PanGPS>
 </PanGPS>
 <Settings>
         <portal-timeout>5</portal-timeout>
         <connect-timeout>5</connect-timeout>
         <receive-timeout>30</receive-timeout>
         <os-type>IoT</os-type>             //pre-deployed OS type for IoT.
 If this tag does not present, GP will automatic detect the OS type.
         <head-less>yes</head-less>       //pre-deployed head-less mode
         <username>abc</username>    //optional pre-deployed username
         <password>xyz</password>       //optional pre-deployed password
         <client-cert-path>cli_cert_path</client-cert-path>       //optional
 pre-deployed client certificate file(p12) path
```


© 2019 Palo Alto Networks, Inc.

```
        <client-cert-passphrase>cli_cert_passphrase_path< /client-cert-
passphrase>       //optional pre-deployed client certificate passphrase file
 path
        <log-path-service>/tmp/gps</log-path-service>  //optional pre-
deployed log folder for PanGPS
        <log-path-agent>/tmp/gpa</log-path-agent>      //optional pre-
deployed log folder for PanGPA and globalprotect CLI
 </Settings>
</GlobalProtect>
```

STEP 4 | 重启 GlobalProtect 进程以使预部署配置生效。

STEP 5 | 部署 IoT 设备后，可以根据需要使用 **globalprotect collect-log** 命令收集日志。

```
user@linuxhost:~$ globalprotect collect-log
The support file is saved to /home/gptest/.GlobalProtect/
GlobalProtectLogs.tgz
```

STEP 6 | （可选）如果身份验证方法是用户名/密码和客户端证书身份验证组合，请确保客户端证书的 **CommonName** 与用户名匹配。

© 2019 Palo Alto Networks, Inc.

在 Windows 上安装用于 IoT 的 GlobalProtect

运行 Windows 10 IoT 的设备可以使用 GlobalProtect 应用程序。使用组织的分发方法（如 Microsoft 系统中心配置管理器 (SCCM)）在运行 Windows 10 IoT 企业版的 IoT 设备上部署和安装 GlobalProtect 应用程序。

GlobalProtect Windows IoT 部署支持基于证书的身份验证。您必须在其本地计算机存储区中的每台 IoT 设备上安装用于身份验证的证书。如果一台 IoT 设备具有多个相同根 CA 的证书，GlobalProtect 将使用 IoT 设备本地计算机存储区中的第一个证书进行身份验证；请确保证书在设备中的顺序正确。

以下各部分介绍如何在运行 Windows IoT 的设备上安装 GlobalProtect 应用程序：

- 在 IoT 设备上下载并安装 MSIEXEC 文件
- 修改 IoT 设备上的注册表项（On-Demand（按需）或 Always On（始终打开））
- 修改 IoT 设备上的注册表项（Always On with Pre-logon（预登录时始终打开））

在 IoT 设备上下载并安装 MSIEXEC 文件

您可以下载并安装 `msiexec.exe` 文件到您的 IoT 设备，以安装适用于 **On-Demand**（按需）连接方法或 **Always On**（始终打开）连接方法的 GlobalProtect 应用程序。使用相同方法部署 msiexec.exe 文件，就如在非-IoT 设备上一样。

修改 IoT 设备上的注册表项（On-Demand（按需）或 Always On（始终打开））

必须将操作系统类型指定为 IoT，将设备类型指定为 headless（无头），并指定门户地址。也可以指定用户名和密码。如果不指定用户名和密码，GlobalProtect 将使用基于证书的身份验证。

对于 **On-Demand**（按需）连接方法或 **Always On**（始终打开）连接方法，可以使用以下安装方法：

- 指定操作系统类型（必需）：

  Registry subkey（注册表子项）：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name（名称）：os-type（操作系统类型）

  Type（类型）：REG_SZ

  Data（数据）：IoT
- 指定无头 IoT 设备（必需）：

  Registry subkey（注册表子项）：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name（名称）：head-less（无头）

  Type（类型）：REG_SZ

  Data（数据）：yes（是）
- 指定门户地址（必需）：

  Registry subkey（注册表子项）：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  名称：门户

  Type（类型）：REG_SZ

  Data（数据）：输入 GlobalProtect 门户的 IP 地址或 FQDN。

© 2019 Palo Alto Networks, Inc.

- 指定用户名（可选）：

  Registry subkey（注册表子项）：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name（名称）：username（用户名）

  Type（类型）：REG_SZ

  Data（数据）：输入用于 IoT 设备的用户名。
- 指定密码（可选）：

  Registry subkey（注册表子项）：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name（名称）：password（密码）

  Type（类型）：REG_SZ

  Data（数据）：输入用于 IoT 设备的密码。

修改 IoT 设备上的注册表项（Always On with Pre-logon（预登录时始终打开））

必须指定门户地址、预登录超时值和仅服务值。必须删除 GlobalProtect 值，以防止 IoT 设备在系统重启时自动启动应用程序接口。预登录 VPN 隧道不会关联用户名，因为用户尚未登录。

对于 **Pre-logon (Always On)**（预登录（始终打开））连接方法，可以使用以下安装方法：

- 指定门户地址（必需）：

  Registry subkey（注册表子项）：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  名称：门户

  Type（类型）：REG_SZ

  Data（数据）：输入 GlobalProtect 门户的 IP 地址或 FQDN。
- 指定预登录值（必需）：

  Registry subkey（注册表子项）：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  名称：Prelogon

  Type（类型）：REG_SZ

  Data（数据）：1
- 指定仅服务值（必需）：

  Registry subkey（注册表子项）：`\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name（名称）：service-only（仅服务）

  Type（类型）：REG_SZ

  Data（数据）：yes（是）
- 删除 GlobalProtect 值（必需）：

  Registry subkey（注册表子项）：`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

  名称：GlobalProtect

© 2019 Palo Alto Networks, Inc.

Type（类型）：REG_SZ

© 2019 Palo Alto Networks, Inc.

主机信息

尽管您可能在企业网络边界拥有严格的安全机制，但是您的网络的安全性实际上跟访问它的端点不相上下。随着当今的劳动力变得越来越具有移动性，导致经常需要从不同地点（如机场、咖啡厅和酒店）和通过各种端点（包括公司配备和个人拥有）访问企业资源，您必须在逻辑上将网络安全扩展到各个端点，以确保全面和一致的安全实施。GlobalProtect™ 主机信息配置文件 (HIP) 功能可让您收集有关端点安全状态的信息，例如端点是否已安装最新的安全修补程序和防病毒定义、是否已启用磁盘加密功能、端点是否已越狱或获取 Root 权限或是否正在运行贵公司所需的特定软件，并根据遵循定义的主机策略决定是否允许或拒绝访问特定主机。

以下部分提供了有关在策略实施中使用主机信息的信息。

> 关于主机信息
> 配置基于 HIP 的策略实施
> 从端点收集应用程序和流程数据
> 重新分发 HIP 报告
> 阻止设备访问
> 配置 Windows User-ID 代理以收集主机信息
> 使用主机信息隔离设备

关于主机信息

GlobalProtect 应用程序的其中一项工作是收集有关正在其上运行的主机的信息。应用程序在成功建立连接后会将此主机的信息提交到 GlobalProtect 网关。网关根据定义的所有 HIP 对象和 HIP 配置文件匹配应用程序提交的此原始主机信息。如果网关找到匹配，则将会在 HIP 匹配日志中生成一个条目。此外，如果网关在策略规则中找到 HIP 配置文件匹配，则将会实施相应的安全策略。

HIP 检查在应用程序连接到网关时执行，且在连接到 GlobalProtect 代理后，每小时执行一次后续检查。一旦之前的 HIP 检查发生变化，GlobalProtect 代理会请求获取更新后的 HIP 报告。网关上每个端点都只保留最新 HIP 报告。

使用策略实施的主机信息配置文件可启用粒度安全功能，确保远程主机能够访问得到充分维护的关键资源，并且保证遵循安全标准之后才允许访问网络资源。例如，在允许访问最敏感的数据系统前，您可能要确保主机访问在其硬盘驱动器上已启用加密功能的数据。如果端点系统已启用加密功能，则您可以通过创建安全规则实施此策略只允许访问应用程序。此外，对于不符合此规则的端点，您可以创建通知消息告知用户拒绝他们访问的原因并将其链接到文件共享位置，他们可以在此位置访问尚未安装加密软件的安装程序（当然，允许用户访问必须创建相应安全规则的文件共享，才能允许访问拥有特定 HIP 配置文件匹配的主机的特殊共享）。

- GlobalProtect 应用收集哪些数据？
- GlobalProtect 应用程序在每种操作系统上会收集哪些数据？
- 网关如何使用主机信息实施策略？
- 用户如何知道其系统是否合规？
- 如何查看端点的状态？

GlobalProtect 应用收集哪些数据？

默认情况下，GlobalProtect 应用收集有关正在端点上运行的最终用户安全包的供应商特定数据（如 OPSWAT 全球合作伙伴计划编制），并将此数据报告给 GlobalProtect 网关以供策略实施使用。有关 GlobalProtect 可通过使用指定的 OPSWAT SDK 进行检测的第三方供应商产品的详细信息，请参阅 GlobalProtect OPSWAT 支持表格。

由于安全软件必须不断完善才可确保保护最终用户，因此 GlobalProtect 网关许可证也可让您获取适用于 GlobalProtect 数据文件的动态更新，以及适用于每个数据包的最新修补程序和软件版本。

默认情况下，应用将收集有关以下信息类别的数据，以帮助确定主机的安全状态：

表 **8:** 表：数据收集类别

类别	收集的数据
通用	有关主机本身的信息，包括主机名、登录域、操作系统、应用版本，而且对于 Windows 系统，还应包括本机所属的域。 对于 *Windows* 端点域，*GlobalProtect* 应用收集为 `ComputerNameDnsDomain` 定义的域，即分配给本地计算机或与其相关联的群集的 *DNS* 域。此数据是在 *HIP* 匹配日志详细信息（*Monitor*（监控）> *Logs*（日志）> *HIP Match*（*HIP* 匹配））中为 *Windows* 端点*Domain*（域）显示的数据。

© 2019 Palo Alto Networks, Inc.

类别	收集的数据
移动设备	有关移动设备的信息，包括设备名称、登录域、操作系统、应用程序版本以及设备连接到的网络信息。此外，GlobalProtect 还会收集设备是否已经破解或越狱的信息。 要收集移动设备属性并在 *HIP* 执行策略中使用这些属性，*GlobalProtect* 需要借助 *MDM* 服务器。*GlobalProtect* 目前支持 *HIP* 与 *AirWatch MDM* 服务器的集成。 对于由 AirWatch 管理的设备，GlobalProtect 应用程序收集的主机信息可以通过 AirWatch 服务收集的附加信息进行补充。有关可从 AirWatch 检索的属性列表，请参阅配置 Windows User-ID 代理以收集主机信息。
补丁程序管理	有关在主机上启用和/或安装的修补程序管理软件以及是否缺少任何修补程序的信息。 如果想要将缺失修补程序的 *Severity*（严重性）值配置为 *HIP* 对象中的匹配条件（*Objects*（对象）> *GlobalProtect* > *HIP Objects*（*HIP* 对象）> *<hip-object>* > *Patch Management*（修补程序管理）> *Criteria*（条件）），请使用 *GlobalProtect* 严重性值与 *OPSWAT* 严重性等级之间的以下映射来了解每个值的含义： • ***0*** — 低 • ***1*** — 中等 • ***2*** — 严重 • ***3*** — 非常严重
防火墙	有关在主机上安装和/或启用的任何防火墙的信息。
防恶意软件	有关在端点上启用和/或安装的任何防病毒或反间谍软件、是否启用实时保护、病毒定义版本、上次扫描时间、供应商和产品名称的信息。 GlobalProtect 使用 OPSWAT 技术来检测和评估端点上的第三方安全应用程序。通过与 OPSWAT OESIS 框架集成，GlobalProtect 使您能够评估端点的合规状态。例如，您可以定义用于验证端点是否存在源于特定供应商的特定抗病毒软件版本的 HIP 对象和 HIP 配置文件，也可确保具有最新病毒定义文件。 *OPSWAT* 无法检测用于 *macOS* 端点上 *Gatekeeper* 安全功能的以下 防恶意软件信息： • 引擎版本 • 定义版本 • 日期 • 上次扫描
磁盘备份	有关是否已安装磁盘备份软件、最后备份时间以及软件的供应商和产品名称的信息。
磁盘加密	有关是否已安装磁盘加密软件、为加密配置的驱动器和/或路径以及软件的供应商和产品名称的信息。

© 2019 Palo Alto Networks, Inc.

类别	收集的数据
数据丢失保护	有关是否为防止企业网络丢失或在潜在的不安全设备上存储敏感企业信息安装和/或启用数据丢失防护 (DLP) 软件的信息。此信息只能从 Windows 端点收集。
证书	关于端点上安装的计算机证书信息。
自定义检查	关于指定注册表项（仅限 Windows）、属性列表 (plist)、（仅限 macOS）或操作系统进程和用户控件应用程序进程是否存在的信息。

您可以在某些主机上排除收集某些类别的信息（以缩短 CPU 周期和加快响应时间）。为此，请在门户上创建代理配置，然后排除您不感兴趣的类别（**Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）> *<agent-config>* > **Data Collection**（数据收集））。例如，如果您不打算根据端点是否运行磁盘备份软件来创建策略，则可以排除该类别以防止应用程序收集任何有关磁盘备份的信息。

此外，您还可以排除在个人端点上收集的信息，以便提供用户隐私。例如，可以包括排除在不是由第三方移动设备管理器管理的端点上安装的应用列表。

GlobalProtect 应用程序在每种操作系统上会收集哪些数据？

GlobalProtect 应用程序收集数据以帮助标识和检索在基于 HIP 的策略实施中使用的设备主机信息配置文件 (HIP)。

- GlobalProtect 应用程序会在 Windows 上收集哪些数据？
- GlobalProtect 应用程序在 macOS 设备上收集哪些数据？
- GlobalProtect 应用程序会在 Windows UWP 设备上收集哪些数据？
- GlobalProtect 应用程序会在 Android 设备上收集哪些数据？
- GlobalProtect 应用程序会在 iOS 设备上收集哪些数据？
- GlobalProtect 应用程序会在 Linux 设备上收集哪些数据？

GlobalProtect 应用程序会在 *Windows* 上收集哪些数据？

下表描述了 GlobalProtect 应用程序在 Windows 设备上为基于 HIP 的策略实施所收集的由防火墙生成的数据：

HIP 报告属性	说明
Report Generation Time（报告生成时间）	HIP 报告生成的日期和时间。
用户名	用于登录到 VPN 的用户名。
User IP Address（用户 **IP** 地址）	用户 Windows 设备的 IP 地址。
Machine Name（计算机名称）	Windows 设备的主机名和序列号。
域	Windows 设备上的字段为空。
OS	目标操作系统的应用程序名称和供应商名称。

© 2019 Palo Alto Networks, Inc.

HIP 报告属性	说明
主机 **ID**	GlobalProtect 分配用于识别主机的唯一主机 ID。Windows 设备上的主机 ID 值为计算机 GUID。计算机 GUID 存储在 Windows 注册表 (HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid)中。
客户端版本	当前安装的 GlobalProtect 应用程序版本号。
Network Interface（网络接口）	其中为网络接口标识了下列设置： • **Interface**（接口）— Windows 设备上检测到的网络接口类型。 • **MAC Address**（**MAC** 地址）— MAC 地址是指分配给 Windows 设备上各个网络接口的唯一硬件标识符。 • **IP Address**（**IP** 地址）— 分配给 Windows 设备上各个网络接口的 IP 地址。
防恶意软件	有关在设备上启用或安装的任何防病毒或防间谍软件、是否在主机上启用实时防病毒或防间谍保护、病毒定义版本、上次扫描时间以及供应商和产品名称的信息。
磁盘备份	有关设备磁盘备份状态的信息，例如，是否已在主机上安装磁盘备份软件、上次备份时间以及软件的供应商和产品名称。
磁盘加密	有关设备磁盘加密状态的信息，例如，是否已在主机上安装磁盘加密软件、检查磁盘加密以确定是否匹配的驱动器或路径、加密位置的状态以及软件的供应商或产品名称。
补丁程序管理	有关在主机上启用或安装的补丁程序管理软件、主机是否检测到缺少补丁程序和所指定严重性级别值的信息。有关各个值的详细信息，请参阅补丁程序管理类别。
防火墙	有关主机上是否启用或安装防火墙软件的信息。
数据丢失保护	有关 Windows 设备上数据丢失保护(DLP)软件状态的信息，以防止公司信息离开公司网络，或是存储到可能不安全的设备上。
自定义检查	有关 GlobalProtect 应用程序从 Windows 设备收集 Windows 注册表的信息。您可以启用自定义检查以从 Windows 设备收集数据，从而指导应用程序收集特定注册表信息（注册表项和注册表项值）。所收集信息的类型可以包括是否已在设备上安装应用程序，或该应用程序的特定特性或属性。

GlobalProtect 应用程序在 *macOS* 设备上收集哪些数据？

下表描述了 GlobalProtect 应用程序在 macOS 设备上为基于 HIP 的策略实施所收集的由防火墙生成的数据：

HIP 报告属性	说明
Report Generation Time（报告生成时间）	HIP 报告生成的日期和时间。
用户名	用于登录到 VPN 的用户名。

© 2019 Palo Alto Networks, Inc.

HIP 报告属性	说明
User IP Address（用户 **IP** 地址）	用户 macOS 设备的 IP 地址。
Machine Name（计算机名称）	macOS 设备的主机名和序列号。
域	macOS 设备上的字段为空。
OS	目标操作系统的应用程序名称和供应商名称。
主机 **ID**	GlobalProtect 分配用于识别主机的唯一主机 ID。主机 ID 值是第一个内置物理网络接口的 MAC 地址。
客户端版本	当前安装的 GlobalProtect 应用程序版本号。
Network Interface（网络接口）	其中为网络接口标识了下列设置： • **Interface**（接口）— macOS 设备上检测到的网络接口类型。 • **MAC Address**（**MAC** 地址）— MAC 地址是指分配给 macOS 设备上各个网络接口的唯一硬件标识符。 • **IP Address**（**IP** 地址）— 分配给 macOS 设备上各个网络接口的 IP 地址。
防恶意软件	有关在设备上启用或安装的任何防病毒或防间谍软件、是否在主机上启用实时防病毒或防间谍保护、病毒定义版本、上次扫描时间以及供应商和产品名称的信息。
磁盘备份	有关设备磁盘备份状态的信息，例如，是否已在主机上安装磁盘备份软件、上次备份时间以及软件的供应商和产品名称。
磁盘加密	有关设备磁盘加密状态的信息，例如，是否已在主机上安装磁盘加密软件、检查磁盘加密以确定是否匹配的驱动器或路径、加密位置的状态以及软件的供应商或产品名称。
补丁程序管理	有关在主机上启用或安装的补丁程序管理软件、主机是否检测到缺少补丁程序和所指定严重性级别值的信息。有关各个值的详细信息，请参阅补丁程序管理类别。
防火墙	有关主机上是否启用或安装防火墙软件的信息。
自定义检查	有关 GlobalProtect 应用程序从 macOS 设备收集 WmacOS 属性列表(plist)的信息。您可以启用自定义检查以从 macOS 设备收集数据，从而指导应用程序收集特定 plist 信息（plist 和 plist 项）。所收集信息的类型可以包括是否已在设备上安装应用程序，或该应用程序的特定特性或属性。

GlobalProtect 应用程序会在 *Windows UWP* 设备上收集哪些数据？

下表描述了 GlobalProtect 应用程序在 Windows UWP 设备上为基于 HIP 的策略实施所收集的由防火墙生成的数据：

© 2019 Palo Alto Networks, Inc.

HIP 报告属性	说明
Report Generation Time（报告生成时间）	HIP 报告生成的日期和时间。
用户名	用于登录到 VPN 的用户名。
User IP Address（用户 **IP** 地址）	用户 Windows UWP 设备的 IP 地址。
Machine Name（计算机名称）	Windows UWP 设备的主机名和序列号。
域	Windows UWP 设备上的字段为空。
OS	目标操作系统的应用程序名称和供应商名称。
主机 **ID**	GlobalProtect 分配用于识别主机的唯一主机 ID。Windows UWP 设备上的主机 ID 值为计算机 GUID。
客户端版本	当前安装的 GlobalProtect 应用程序版本号。
Network Interface（网络接口）	其中为网络接口标识了下列设置： • **Interface**（接口）— Windows UWP 设备上检测到的网络接口类型。 • **MAC Address**（**MAC** 地址）— MAC 地址是指分配给 Windows UWP 设备上各个网络接口的唯一硬件标识符。 • **IP Address**（**IP** 地址）— 分配给 Windows UWP 设备上各个网络接口的 IP 地址。

GlobalProtect 应用程序会在 *Android* 设备上收集哪些数据？

下表描述了 GlobalProtect 应用程序在 Android 设备上为基于 HIP 的策略实施所收集的由防火墙生成的数据：

Chromebook 上的 Android 版 GlobalProtect 应用程序使用相同的 HIP 报告属性。

HIP 报告属性	说明
Report Generation Time（报告生成时间）	HIP 报告生成的日期和时间。
用户名	用于登录到 VPN 的用户名。
User IP Address（用户 **IP** 地址）	用户 Android 设备的 IP 地址。
Machine Name（计算机名称）	Android 设备的主机名和序列号。
域	Android 设备上的字段为空。
序列号	Android 设备的序列号。

© 2019 Palo Alto Networks, Inc.

HIP 报告属性	说明
受管	表示 Android 设备是否受管的值。如果此值为 **Yes**（是），则设备受管。如果此值为 **No**（否），则设备不受管。
OS	目标操作系统的应用程序名称和供应商名称。
主机 **ID**	GlobalProtect 分配用于标识主机的唯一字母数字字符串，长度为 16 个字符。主机 ID 值是 Android 设备上的 Android ID。
客户端版本	当前安装的 GlobalProtect 应用程序版本号。
WiFi SSID	有关网络连接的特定信息，例如 Android 设备上的 **WiFi SSID**。
Network Interface（网络接口）	其中为网络接口标识了下列设置： • **Interface**（接口）— Android 设备上检测到的网络接口类型。 • **MAC Address**（**MAC** 地址）— MAC 地址是指分配给 Android 设备上各个网络接口的唯一硬件标识符。 • **IP Address**（**IP** 地址）— 分配给 Android 设备上各个网络接口的 IP 地址。
移动设备	有关移动设备的信息，包括设备名称、登录域、操作系统、应用程序版本以及设备所连接的网络的相关信息。
标记	启用后可与其他基于 MDM 的属性进行匹配的标记。
Device Compliance（设备合规性）	**Rooted/Jailbroken**（破解/越狱）属性用于确定已通过破解或越狱的方式取得管理权限的 Android 设备的合规状态。针对受影响的设备，可从操作系统中移除或绕过此安全策略。
MDM Attributes（**MDM** 属性）	在将 GlobalProtect 部署与 MDM 供应商集成时，Android 设备的 GlobalProtect 应用程序可以从 MDM 系统中获取下列数据属性和标记： • **udid**— Android 设备的唯一设备标识符 (UDID)。 • **managed-by-mdm**— 指示 Android 设备是否受管的值。如果此值为 **Yes**（是），则 Android 设备受管。如果此值为 **No**（否），则 Android 设备不受管。 • **tag**（标记）— 启用后可与其他基于 MDM 的属性进行匹配的标记。 • **compliance**（合规性）— 指示 Android 设备是否符合您定义的合规策略的合规状态。 • **ownership**（所有权）— Android 设备的所有权类别（例如，**Employee Owned**（归员工所有））。此值附加于 HIP 报告中的 **Tag**（标记）属性。

GlobalProtect 应用程序会在 *iOS* 设备上收集哪些数据？

下表描述了 GlobalProtect 应用程序在 iOS 设备上为基于 HIP 的策略实施所收集的由防火墙生成的数据：

HIP 报告属性	说明
Report Generation Time（报告生成时间）	HIP 报告生成的日期和时间。

© 2019 Palo Alto Networks, Inc.

HIP 报告属性	说明
用户名	用于登录到 VPN 的用户名。
User IP Address（用户 **IP** 地址）	用户 iOS 设备的 IP 地址。
Machine Name（计算机名称）	iOS 设备的主机名和序列号。
域	iOS 设备上的字段为空。
序列号	iOS 设备上的字段为空。
受管	指示 iOS 设备是否受管的值。如果此值为 **Yes**（是），则设备受管。如果此值为 **No**（否），则设备不受管。
OS	目标操作系统的应用程序名称和供应商名称。
主机 **ID**	GlobalProtect 分配用于标识主机的唯一 ID。主机 ID 值是 iOS 设备上的 UDID。
客户端版本	当前安装的 GlobalProtect 应用程序版本号。
WiFi SSID	有关网络连接的信息，例如 iOS 设备上的 **WiFi SSID**。
Network Interface（网络接口）	其中为网络接口标识了下列设置： • **Interface**（接口）— iOS 设备上检测到的网络接口类型。 • **MAC Address**（**MAC** 地址）— MAC 地址是指分配给 iOS 设备上各个网络接口的唯一硬件标识符。 • **IP Address**（**IP** 地址）— 分配给 iOS 设备上各个网络接口的 IP 地址。
移动设备	有关移动设备的信息，包括设备名称、登录域、操作系统、应用程序版本以及设备所连接的网络的相关信息。
Device Compliance（设备合规性）	以下属性用于确定 iOS 设备的合规状态： • **Rooted/Jailbroken**（破解/越狱）— 已通过破解或越狱的方式取得管理权限的 iOS 设备的状态。针对受影响的设备，可从操作系统中移除或绕过此安全策略。 • **Disk Encryption Not Set**（未设置磁盘加密）—已启用磁盘加密的 iOS 设备的状态。 • **Passcode Not Set**（未设置密码）— 已设置为使用密码的 iOS 设备的状态。 • **Has Malware**（有恶意软件）— 安装有感染恶意软件的应用程序的 iOS 设备状态。
MDM Attributes（**MDM** 属性）	在将 GlobalProtect 部署与 MDM 供应商集成时，iOS设备的 GlobalProtect 应用程序可以从 MDM 系统中获取下列数据属性和标记： • **udid**— iOS 设备的唯一设备标识符 (UDID)。 • **managed-by-mdm**— 指示 iOS 设备是否受管的值。如果此值为 **Yes**（是），则 iOS 设备受管。如果此值为 **No**（否），则 iOS 设备不受管。 • **tag**（标记）— 启用后可与其他基于 MDM 的属性进行匹配的标记。

© 2019 Palo Alto Networks, Inc.

HIP 报告属性	说明
	• **compliance**（合规性）—指示 iOS 设备是否符合您定义的合规策略的合规状态。 • **ownership**（所有权）— iOS 设备的所有权类别（例如，**Employee Owned**（归员工所有））。此值附加于 HIP 报告中的 **Tag**（标记）属性。

GlobalProtect 应用程序会在 *Linux* 设备上收集哪些数据？

下表描述了 GlobalProtect 应用程序在 Linux 设备上为基于 HIP 的策略实施所收集的由防火墙生成的数据（XML 格式）：

HIP 报告属性	说明
`user-name`（用户名）	用于登录到 VPN 的用户名。
`IP` 地址	用户 Linux 设备的 IP 地址。
`generate-time`（生成时间）	HIP 报告生成的日期和时间。
`host-info`（主机信息）	为配置主机信息，需激活下列选项： • `managed`（受管）— 指示 Linux 设备是否受管的值。如果此值为 **Yes**（是），则设备受管。如果此值为 **No**（否），则设备不受管。 • `serial-number`（序列号）— Linux 设备的序列号。 • `client-version`（客户端版本）— 当前安装的 GlobalProtect 应用程序版本号。 • `os`（操作系统）—目标操作系统的应用程序名称。 • `os-vendor`（操作系统供应商）— 目标操作系统的供应商名称。 • `domain`（域名）— Linux 设备的域名。 • `host-name`（主机名）— Linux 设备的主机名。 • `host-id`（主机 `ID`）— GlobalProtect 分配用于识别主机的唯一 ID。主机 ID 值是 Linux 设备的产品 UDID。
`network-interface`（网络接口）	其中为网络接口标识了下列设置： • `inteface`（接口）— Linux 设备上检测到的网络接口类型。 • `mac-address`（`MAC` 地址）— MAC 地址是指分配给 Linux 设备上各个网络接口的唯一硬件标识符。 • `ip-address`（`IP` 地址）— 分配给 Linux 设备上各个网络接口的 IP 地址。
`anti-malware`（防恶意软件）	有关在设备上启用或安装的任何防病毒或防间谍软件、是否在主机上启用实时防病毒或防间谍保护、病毒定义版本、上次扫描时间以及供应商和产品名称的信息。
`disk-backup`（磁盘备份）	有关设备磁盘备份状态的信息，例如，是否已在主机上安装磁盘备份软件、上次备份时间以及软件的供应商和产品名称。
`disk-encryption`（磁盘加密）	有关设备磁盘加密状态的信息，例如，是否已在主机上安装磁盘加密软件、检查磁盘加密以确定是否匹配的驱动器或路径、加密位置的状态以及软件的供应商或产品名称。

© 2019 Palo Alto Networks, Inc.

HIP 报告属性	说明
防火墙	有关主机上是否启用或安装防火墙软件的信息。
patch-management（补丁程序管理）	有关在主机上启用或安装的补丁程序管理软件、主机是否检测到缺少补丁程序和所指定严重性级别值的信息。有关各个值的详细信息，请参阅补丁程序管理类别。

网关如何使用主机信息实施策略？

尽管应用可获得有关从门户下载的客户端配置收集的信息，但您可以在网关上通过创建 HIP 对象和 HIP 配置文件定义需要监控和/或用于策略实施的主机属性：

- **HIP** 对象 — 提供匹配条件以筛选出您需要使用的主机信息，从而通过代理报告的原始数据实施策略。例如，尽管原始主机数据可能包括有关端点上安装的若干防病毒软件包的信息，但是您可能仅对贵组织中需要的某个特定应用程序感兴趣。在这种情况下，您将创建 HIP 对象以匹配您有兴趣实施的特定应用程序。

  确定您需要的 HIP 对象的最佳方式是确定您将如何使用所收集的主机信息来实施策略。请记住，HIP 对象自身仅仅是构建块，使您可以创建在安全策略中使用的 HIP 配置文件。因此，您可能希望保持对象简化，与一个对象匹配，例如，是否存在特定类型的必需软件、特定域中的成员身份或者是否存在特定端点操作系统。如此，您将能够灵活创建非常精细（且非常强大）的 HIP 扩充策略。
- **HIP** 配置文件 — 结合求值的 HIP 对象集合用于监控或安全策略实施。创建 HIP 配置文件时，可以使用布尔逻辑来合并先前创建的 HIP 对象（以及其他 HIP 配置文件），例如，当按照生成的 HIP 配置文件对通信流进行评估时，可能匹配，也可能不匹配。如果存在匹配项，那么将执行对应的策略规则。如果没有匹配项，将按照下一个规则来对通信流进行评估（与任何其他策略匹配标准一样）。

与流量日志不同 — 只有策略匹配时才会创建日志条目 — HIP 匹配日志在每当应用提交的原始数据与定义的 HIP 对象和/或 HIP 配置文件匹配时才会生成条目。在将 HIP 配置文件附加到安全策略前，这使得 HIP 匹配日志成为用于在网络上监控一段时间内端点状态的优良资源，帮助您确定您认为需要实施的真正策略。有关如何创建 HIP 对象和 HIP 配置文件并将它们用作策略匹配条件的详细信息，请参阅配置基于 HIP 的策略实施。

用户如何知道其系统是否合规？

默认情况下，最终用户不会提供有关所做策略决策的任何信息，作为实施启用 HIP 安全规则的结果。但是，您可以通过配置 HIP 通知消息启用此功能显示特定 HIP 配置文件匹配和/或不匹配的时间。

至于决定显示消息的时间（即在用户配置与策略的 HIP 配置文件匹配时还是在不匹配时显示），在很大程度上取决于您的策略和用户的 HIP 匹配（或非匹配）方法。也就是说，匹配意味着就能够完全访问您的网络资源？或者，意味着因出现不合规问题而限制访问您的网络资源？

例如，需要考虑以下各种情景：

- 如果尚未安装所需的企业防病毒和反间谍软件包，可以创建 HIP 配置文件进行匹配。在这种情况下，您可能要为匹配 HIP 配置文件的用户创建 HIP 通知消息告知他们需要安装软件（并且，可以提供指向文件共享位置的链接，他们在该位置可以访问相应软件的安装程序）。
- 如果已经安装相同的应用程序，可以创建匹配的 HIP 配置文件。在这种情况下，您可能要为不匹配配置文件的用户创建消息，并将他们引导至安装包的位置。

有关如何创建 HIP 对象和 HIP 配置文件并将它们用作定义 HIP 通知消息的详细信息，请参阅配置基于 HIP 的策略实施。

© 2019 Palo Alto Networks, Inc.

如何查看端点的状态？

每当将端点连接到 GlobalProtect 时，应用都会将其 HIP 数据提供给网关。然后，网关使用此数据确定与主机匹配的 HIP 对象和/或 HIP 配置文件。对于每个匹配，它都会生成 HIP 匹配日志条目。与流量日志不同 — 只有策略匹配时才会创建日志条目 — HIP 匹配日志在每当应用提交的原始数据与定义的 HIP 对象和/或 HIP 配置文件匹配时才会生成条目。在将 HIP 配置文件附加到安全策略前，这使得 HIP 匹配日志成为用于在网络上监控一段时间内端点状态的优良资源，帮助您确定您认为需要实施的真正策略。

因为只有在当主机状态与所创建的 HIP 对象匹配时才会生成 HIP 匹配日志，因此为了全面查看端点状态，对于与符合特定状态（对于安全策略实施目的）和不合规（对于可见性）的端点匹配的 HIP 日志，可能需要创建多个 HIP 对象。例如，假设您想要防止没有安装防病毒或防间谍软件的端点连接到网络。在这种情况下，您可能需要创建与已安装特定防病毒或防间谍软件的主机匹配的 HIP 对象。通过在 HIP 配置文件中包括此对象并将其附加到允许从 VPN 区域访问的安全策略规则，您可以确保只能连接使用防病毒或防间谍软件保护的主机。

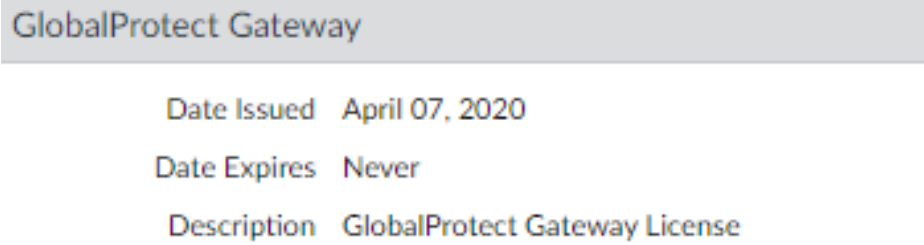
在此示例中，您将无法在 HIP 匹配日志中查看哪些端点不符合此要求。如果您希望查看没有安装防病毒或防间谍软件的端点的日志以便可以跟踪这些用户，则也可以创建与没有安装防病毒或防间谍软件条件相匹配的 HIP 对象。由于此对象仅用于日志记录目的，因而您不需要将其添加到 HIP 配置文件或附加到安全策略规则。

© 2019 Palo Alto Networks, Inc.

配置基于 HIP 的策略实施

要在策略实施中使用主机信息，您必须完成下列步骤。有关 HIP 功能的详细信息，请参阅关于主机信息。有关为设备收集的数据的更多详细信息，请参阅 GlobalProtect 应用程序在每种操作系统上会收集哪些数据？。

STEP 1 | 验证用于 HIP 检查的许可证是否正确。

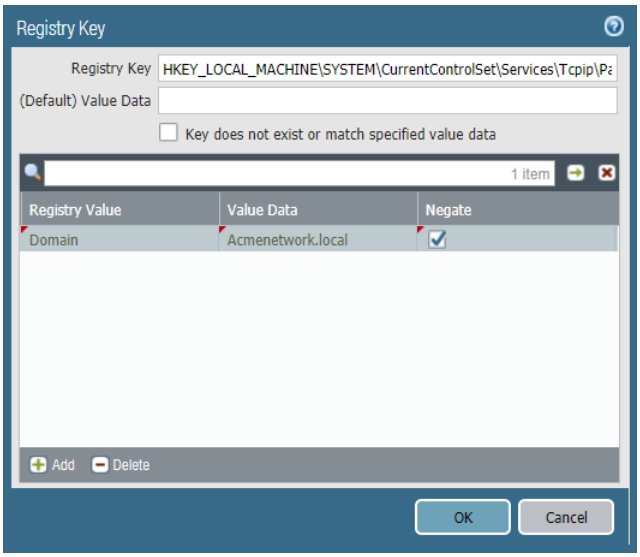


要使用 HIP 功能，您必须购买并在将要执行 HIP 检查的每个网关上安装 GlobalProtect 订阅许可证。要在每个门户和网关上验证许可证的状态，请选择**Device**（设备）> **Licenses**（许可证）。

如果您没有所需的许可证，请联系您的 Palo Alto Networks 销售工程师或经销商。有关许可证的详细信息，请参阅关于 GlobalProtect 许可证。

STEP 2 | （可选）定义您希望应用程序收集的所有自定义主机信息。例如，如果您有任何必需应用程序未包含在用于创建 HIP 对象的供应商和/或产品列表中，则您可以创建自定义检查可让您确定是否已安装应用程序（具有对应的注册表或 plist 项），或者是否正在运行（具有对应的运行进程）。

> *步骤 2 和 3 均假设您已经完成 GlobalProtect 门户配置。如果您尚未配置门户，有关说明请参阅设置 GlobalProtect 门户访问权限。*



1. 在托管 GlobalProtect 门户的防火墙上，选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）。
2. 选择要修改的门户配置。
3. 在 **Agent**（代理）选项卡上，选择您要添加到自定义 HIP 检查的代理配置，或单击 **Add**（添加）以创建新的配置。

© 2019 Palo Alto Networks, Inc.

4. 选择 **HIP Data Collection**（**HIP** 数据收集），然后启用选项以 **Collect HIP Data**（收集 **HIP** 数据）。
5. 在 **Custom Checks**（自定义检查）下，定义您要从正运行此代理配置的主机收集的数据，如下所示：
   - 要收集有关特定注册表项的信息：在 **Windows** 选项卡上，**Add**（添加）要在**Registry Key**（注册表项）区域收集数据的 **Registry Key**（注册表项）的名称。要限制于收集特定 **Registry Value**（注册表值）的数据，**Add**（添加）并定义该特定注册表值。单击 **OK**（确定）以保存设置。
   - 要收集有关正在运行进程的信息：选择相应的选项卡（**Windows** 或 **Mac**），然后 **Add**（添加）进程至 **Process List**（进程列表）。输入您希望应用程序收集有关其信息的进程的名称。
   - 要收集有关特定属性列表的信息：在 **Mac**选项卡上，**Add**（添加）要收集其数据的 **Plist**。要限制于收集特定表项值的数据， **Add**（添加）**Key**（表项）值。单击 **OK**（确定）以保存设置。
6. 如果使用新代理配置，请根据定义 GlobalProtect 代理配置。
7. 单击 **OK**（确定）保存配置。
8. **Commit**（提交）更改。

STEP 3 | （可选）排除收集类别。

1. 在托管 GlobalProtect 门户的防火墙上，选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）。
2. 选择要修改的门户配置。
3. 在 **Agent**（代理）选项卡上，选择要从中排除类别的代理配置，或 **Add**（添加）新代理配置。
4. 选择 **Data Collection**（数据收集），然后验证 **Collect HIP Data**（收集 **HIP** 数据）是否启用。
5. 在 **Exclude Categories**（排除类别）下，**Add**（添加）一个新的排除类别。
6. 从下拉列表中选择要排除的 **Category**（类别）。
7. （可选）如果您要在选定类别中排除特定供应商和/或产品（而非排除整个类别），请单击 **Add**（添加）。在“编辑供应商”对话框中，选择想要排除的 **Vendor**（供应商），然后单击 **Add**（添加）从该供应商中排除特定产品。在定义供应商完成后，单击 **OK**（确定）。您可以在排除列表中添加多个供应商和产品。
8. 针对要排除的每个类别，请重复步骤 5-7。
9. 如果使用新代理配置，请根据定义 GlobalProtect 代理配置。
10. 单击 **OK**（确定）保存配置。
11. **Commit**（提交）更改。

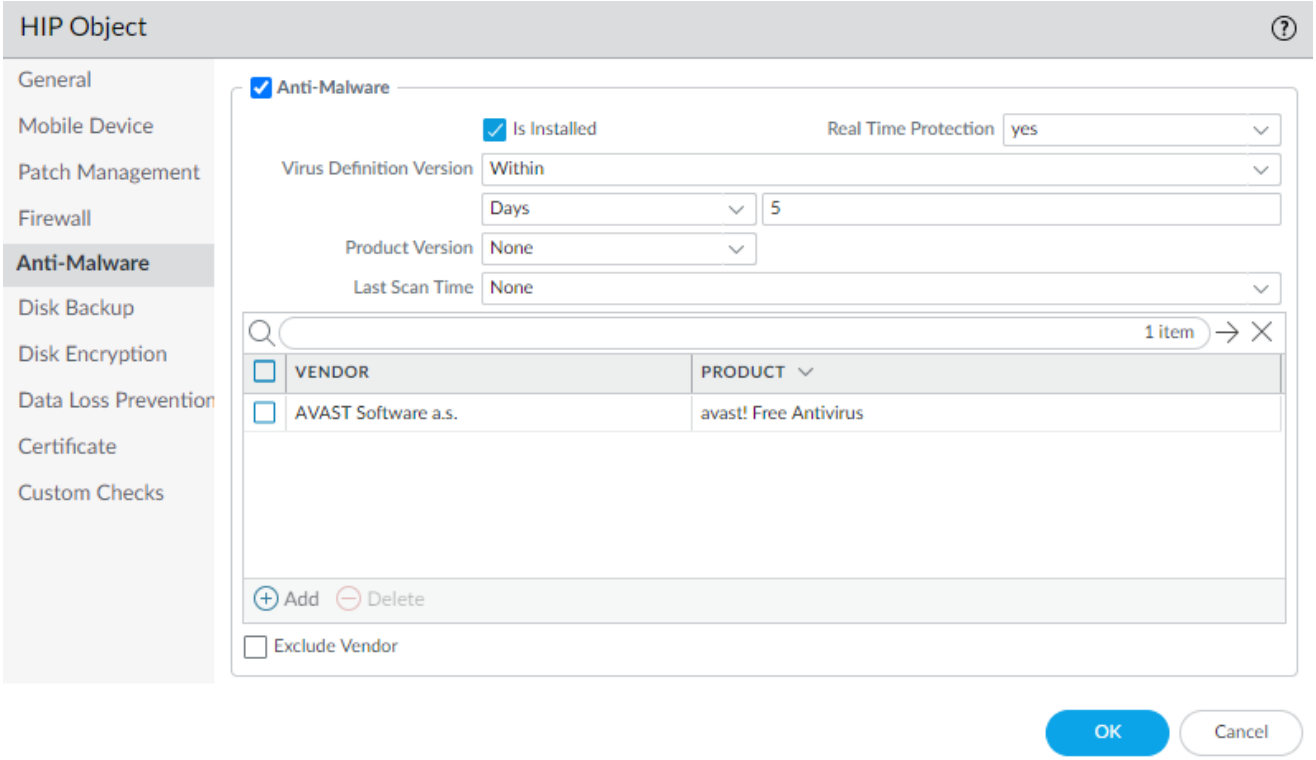
STEP 4 | 创建 HIP 对象以筛选应用程序所收集的原始主机数据。

确定您需要的 HIP 对象的最佳方式是确定您将如何使用所收集的主机信息来实施策略。请记住，HIP 对象自身仅仅是构建块，使您可以创建在安全策略中使用的 HIP 配置文件。因此，您可能希望保持对象简化，与一个项目匹配，例如，是否存在特定类型的必需软件、特定域中的成员身份或者是否存在特定端点操作系统。如此，您将能够灵活创建非常精细（且非常强大）的 HIP 扩充策略。

有关特定 *HIP* 类别或字段的详细信息，请参阅联机帮助。

1. 在托管 GlobalProtect 网关的防火墙上（或者，如果您打算在多个网关之间共享 HIP 对象，则在 Panorama 上），选择 **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象），然后 **Add**（添加）一个新 HIP 对象。
2. 输入对象的 **Name**（名称）。
3. 选择与您感兴趣匹配的主机信息类别相对应的选项卡，然后选中该复选框启用根据类别匹配的对象。例如，要创建对象查找有关防病毒软件或防间谍软件的信息，可以选择 **Antivirus**（防病毒）选项卡，然后选中 **Antivirus**（防病毒）复选框以启用相应的字段。填写完成下列字段以定义所需的匹配条件。例如，下面的图像显示了如何创建是否与所安装的 AVAST 免费防病毒软件应用程序匹配、已经启用 **Real Time Protection**（实时保护）和拥有在最近 5 天内更新的病毒定义的 HIP 对象。

© 2019 Palo Alto Networks, Inc.



对于您要根据该对象匹配的每个类别，请重复此步骤。有关详细信息，请参阅表：数据收集类别。

4. （可选）配置标记以匹配所有权类别或端点的合规状态。

   例如，您可以创建一个标记来匹配员工个人拥有的端点，以便您能阻止用户访问其个人端点上的敏感网络资源。

   用于 Windows 的 User-ID 代理可查询 MDM 服务器，以获取以下信息：

   - 移动设备合规状态。
   - 移动设备所属的智能组（所有权类别）。

   User-ID 代理将此信息转换为可合并到 HIP 报告的标记。您可以基于这些标记值创建 HIP 对象，以便为网络中的端点实施基于 HIP 的安全策略。更多信息，请参阅配置 Windows User-ID 代理以收集主机信息。

   1. 选择 **Mobile Device**（移动设备）复选框以启用配置 **Mobile Device**（移动设备）设置。
   2. 在 **Device**（设备）选项卡上，从 **Tag**（标记）下拉列表中选择匹配运算符（例如 **Contains**（包含）或 **Is Not**（不是））。
   3. （可选）出现提示时，输入以下其中一个所有权类别值：

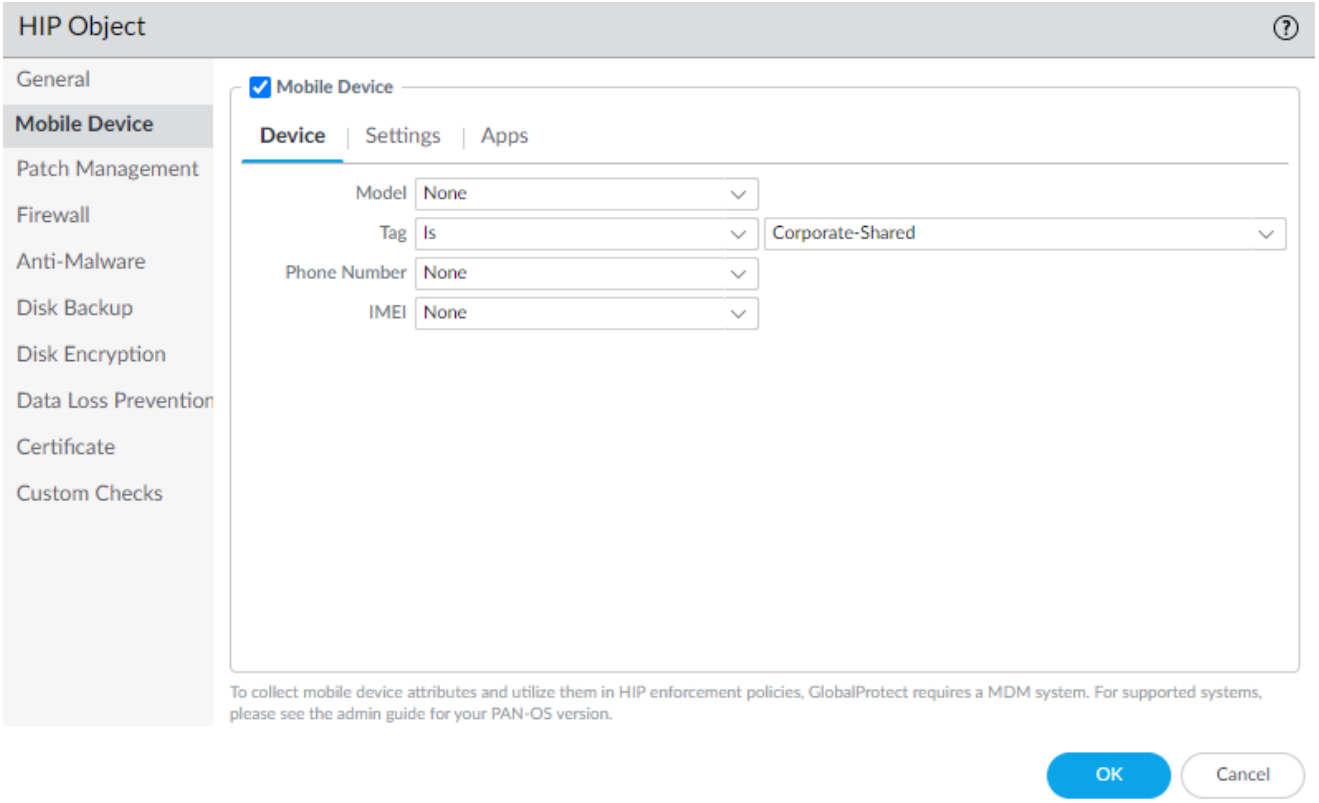
      所有权类别显示端点拥有者。

      - 员工所有
      - 公司专用
      - 公司共享
   4. （可选）出现提示时，输入以下其中一个合规状态值：

      合规状态显示的是端点是否与您定义的安全策略相符。

© 2019 Palo Alto Networks, Inc.

- 合规
- 不合规
- 无法使用



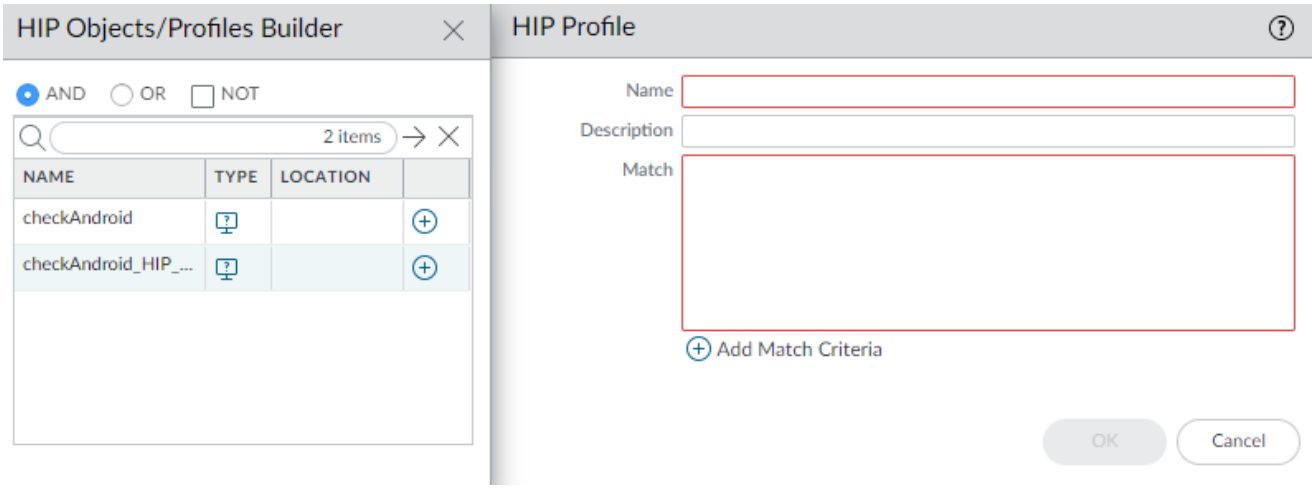
5. 单击 **OK**（确定）保存 HIP 对象。
6. 重复这些步骤可创建所需的每个额外的 HIP 对象。
7. **Commit**（提交）更改。

STEP 5 | 创建您要在策略中使用的 HIP 配置文件。

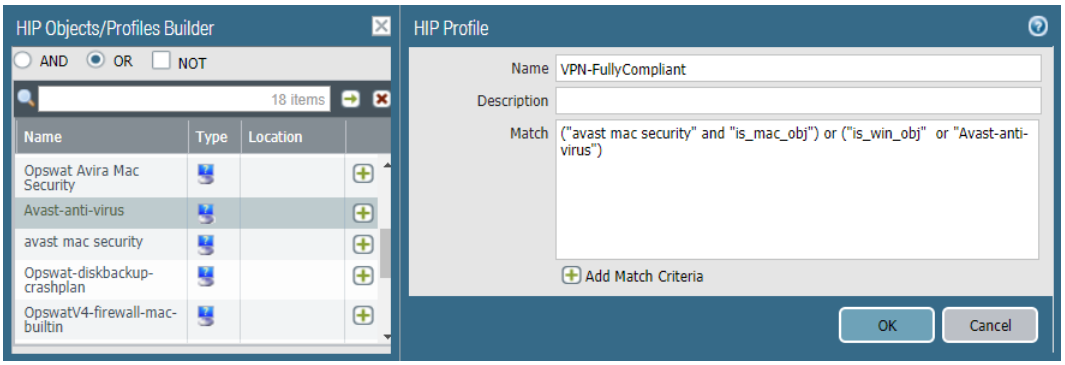
创建 HIP 配置文件时，可以使用布尔逻辑来合并先前创建的 HIP 对象（以及其他 HIP 配置文件），例如，当按照生成的 HIP 配置文件对通信流进行评估时，可能匹配，也可能不匹配。如果存在匹配项，那么将实施对应的策略规则；如果没有匹配项，将按照下一个规则来对流进行评估（与任何其他策略匹配条件一样）。

1. 在托管 GlobalProtect 网关的防火墙上（或者，如果您打算在多个网关之间共享 HIP 配置文件，则在 Panorama 上），选择 **Objects**（对象）> **GlobalProtect** > **HIP Profiles**（**HIP** 配置文件），然后 **Add**（添加）一个新 HIP 配置文件。
2. 输入 **Name**（名称）和 **Description**（说明）以标识配置文件。
3. 单击 **Add Match Criteria**（添加匹配标准）可打开 HIP 对象/配置文件生成器。
4. 选择要用作匹配条件的 HIP 对象或配置文件，然后单击添加图标 (⊕) 以将其移动到“HIP 配置文件”对话框上的 **Match**（匹配）文本框。如果您希望仅当对象中的条件对于流不成立时，HIP 配置文件才作为匹配项评估对象，请在添加对象之前选中 **NOT**（非）复选框。

© 2019 Palo Alto Networks, Inc.



5. 继续为您在生成的配置文件添加匹配条件，确保在每个加法之间选中相应的布尔运算符单选按钮（**AND**（与）或 **OR**（或））（如果适用，请再次使用 **NOT**（非）复选框）。
6. 如果在创建复杂的布尔表达式，必须手动在匹配文本框中的适当位置中添加圆括号，以确保使用需要的逻辑来对 HIP 配置文件进行求值。例如，下面的 HIP 配置文件匹配以下流量：来自具有 FileVault 磁盘加密（对于 macOS 系统）或 TrueCrypt 磁盘加密（对于 Windows 系统）的主机；属于必需域；并且安装有 Symantec 防病毒客户端：



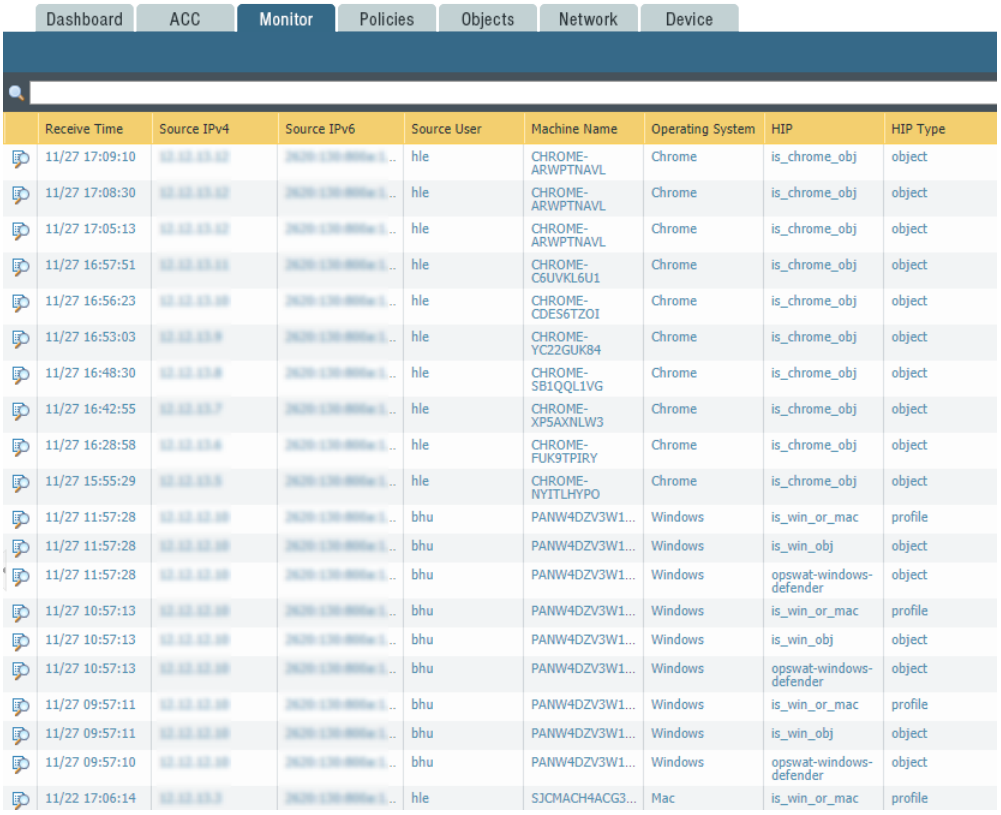
7. 在添加完所有匹配条件后，单击 **OK**（确定）以保存配置文件。
8. 重复这些步骤可创建您所需的每个额外的 HIP 配置文件。
9. **Commit**（提交）更改。

STEP 6 | 验证您创建的 HIP 对象和 HIP 配置文件是否与 GlobalProtect 流量按预期匹配。

将监控 *HIP* 对象和配置文件视为用来监控主机端点的安全状态和活动的一种手段。通过监控一段时间内的主机信息，您将能够更好地了解出现安全和合规性问题的位置，从而引导您创建有用的策略。有关详细信息，请参阅如何查看端点的状态？

在 GlobalProtect 用户连接的网关上，选择 **Monitor**（监控）> **Logs**（日志）> **HIP Match**（**HIP** 匹配）。在评估应用程序根据定义的 HIP 对象和 HIP 配置文件报告的原始 HIP 数据时，此日志将会显示网关确定的所有匹配项。与其他日志不同，HIP 匹配不需要记录安全策略匹配。

© 2019 Palo Alto Networks, Inc.



Receive Time	Source IPv4	Source IPv6	Source User	Machine Name	Operating System	HIP	HIP Type
11/27 17:09:10	[illegible]	[illegible]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 17:08:30	[illegible]	[illegible]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 17:05:13	[illegible]	[illegible]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 16:57:51	[illegible]	[illegible]	hle	CHROME-C6UVKL6U1	Chrome	is_chrome_obj	object
11/27 16:56:23	[illegible]	[illegible]	hle	CHROME-CDES6TZOI	Chrome	is_chrome_obj	object
11/27 16:53:03	[illegible]	[illegible]	hle	CHROME-YC22GUK84	Chrome	is_chrome_obj	object
11/27 16:48:30	[illegible]	[illegible]	hle	CHROME-SB1QQL1VG	Chrome	is_chrome_obj	object
11/27 16:42:55	[illegible]	[illegible]	hle	CHROME-XP5AXNLW3	Chrome	is_chrome_obj	object
11/27 16:28:58	[illegible]	[illegible]	hle	CHROME-FUK9TPIRY	Chrome	is_chrome_obj	object
11/27 15:55:29	[illegible]	[illegible]	hle	CHROME-NYITLHYPO	Chrome	is_chrome_obj	object
11/27 11:57:28	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 11:57:28	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 11:57:28	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/27 10:57:13	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 10:57:13	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 10:57:13	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/27 09:57:11	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 09:57:11	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 09:57:10	[illegible]	[illegible]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/22 17:06:14	[illegible]	[illegible]	hle	SJCMACH4ACG3...	Mac	is_win_or_mac	profile

STEP 7 | 在包含 GlobalProtect 用户的源区域上启用 User-ID 发送请求需要基于 HIP 的访问控件。您必须启用 User-ID，即使您不使用用户标识功能或防火墙不会生成任何 HIP 匹配日志条目。

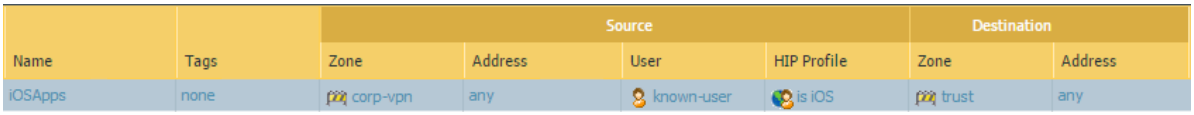
1. 选择**Network**（网络）> **Zones**（区域）。
2. 单击您想要在其中启用 User-ID 的区域**Name**（名称）。
3. **Enable User Identification**（启用用户标识），然后单击 **OK**（确定）。

Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	User ID Enabled
corp-vpn	layer3	ethernet1/2 tunnel.1			✓

STEP 8 | 在网关上创建启用 HIP 的安全规则。

作为最佳做法，您应创建安全规则，并在添加 HIP 配置文件前根据源和目标条件测试它们是否与流量匹配。通过执行此操作，您将能够更好地确定启用 HIP 的规则在策略内的正确位置。

1. 选择 **Policies**（策略）> **Security**（安全），然后选择您要添加 HIP 配置文件的规则。
2. 在 **Source**（源）选项卡上，请务必确保 **Source Zone**（源区域）是启用用户 ID 的区域。
3. 在 **Source Device**（源设备）的 **Source**（源）选项卡上，**Add**（添加）用于标识设备的 **HIP Profiles**（**HIP** 配置文件）（您最多可向规则添加 63 个 HIP 配置文件）。
4. 单击 **OK**（确定）保存规则。
5. **Commit**（提交）更改。



Name	Tags	Source				Destination	
		Zone	Address	User	HIP Profile	Zone	Address
iOSApps	none	corp-vpn	any	known-user	is iOS	trust	any

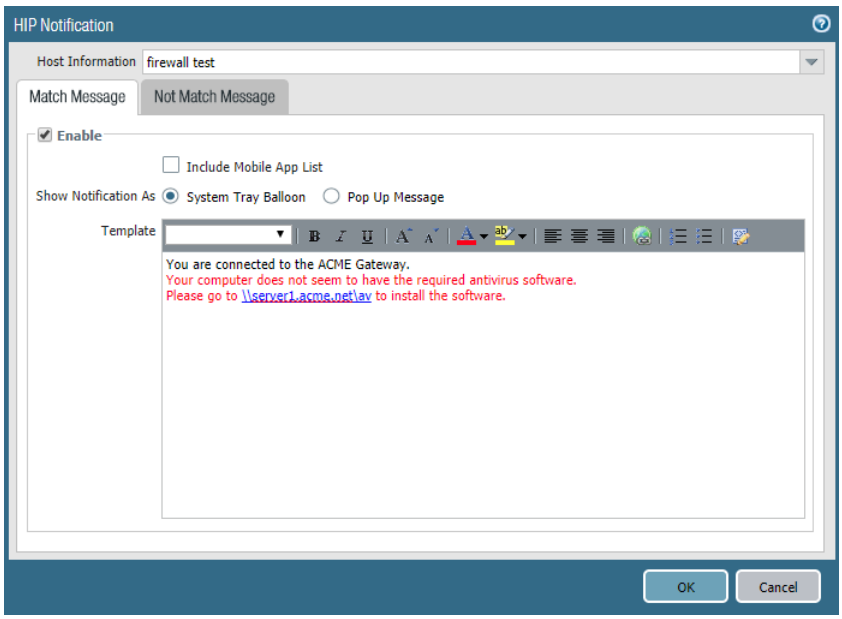
© 2019 Palo Alto Networks, Inc.

STEP 9 | 定义在实施含有 HIP 配置文件的安全规则时最终用户可以看到的通知消息。

至于决定想要显示通知消息的时间（即在用户配置与策略的 HIP 配置文件匹配时还是在不匹配时显示），在很大程度上取决于您的策略和用户的 HIP 匹配（或非匹配）方法。也就是说，匹配意味着就能够完全访问您的网络资源？或者，意味着因出现不合规问题而限制访问您的网络资源？

例如，如果尚未安装所需的企业防病毒和反间谍软件包，则假设您可以创建 HIP 配置文件进行匹配。在这种情况下，您可能要为匹配 HIP 配置文件的用户创建 HIP 通知消息告知他们需要安装软件。或者，如果您的 HIP 配置文件已匹配（如果已安装相同的应用程序），则您可能要为不匹配配置文件的用户创建消息。

1. 在托管 GlobalProtect 网关的防火墙上，选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）。
2. 选择想要为其添加 HIP 通知消息的网关配置。
3. 选择 **Agent**（代理）> **HIP Notification**（**HIP** 通知），然后单击 **Add**（添加）。
4. 从 **Host Information**（主机信息）下拉列表中选择此消息应用到的 HIP 配置文件。
5. 根据您是否希望匹配相应的 HIP 配置文件时，或是在不匹配时显示消息，选择 **Match Message**（匹配消息）或 **Not Match Message**（不匹配消息）。在某些情况下，您可能要为匹配和不匹配创建消息，取决于匹配的对象和策略的目标。
6. **Enable**（启用） **Match Message**（匹配消息）或 **Not Match Message**（不匹配消息），然后选择是否想要将消息显示为 **Pop Up Message**（弹出消息）或 **System Tray Balloon**（系统托盘气球）。
7. 在 **Template**（模板）文本框中输入消息文本，然后单击 **OK**（确定）。文本框提供了文本的 WYSIWYG 视图和 HTML 源视图，您可以使 **Source Edit**（源编辑）图标在这两个视图之间切换。此外，工具栏还提供了用于格式化文本和创建指向外部文档的超链接的各种选项，例如将用户直接连接到可下载所需软件程序的 URL 的链接。



8. 为您要定义的每个消息重复执行此程序。
9. **Commit**（提交）更改。

STEP 10 | 验证您的 HIP 配置文件是否按预期运行。

您可以使用 流量日志监控命中 HIP 启用策略的流量：

1. 在托管网关的防火墙上，选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）。
2. 对日志进行筛选，以便只显示与包含您感兴趣监控的 HIP 配置文件规则匹配的流量。例如，要搜索与名为“iOS Apps”的安全规则匹配的流量，您可以在过滤器文本框中输入 **(rule eq 'iOS Apps')**，如下所示：

© 2019 Palo Alto Networks, Inc.

(rule eq 'iOS Apps')

		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port
		02/08 17:47:25	end	l3-trust	l3-untrust	10.31.32.4	paloaltonetwork\...	17.154.66.16	443
		02/08 17:47:25	end	l3-trust	l3-untrust	10.31.32.4	paloaltonetwork\...	17.158.36.34	443
		02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
		02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
		02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
		02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
		02/08 17:47:21	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
		02/08 17:47:21	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
		02/08 17:47:08	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	107.20.172.241	443
		02/08 17:47:08	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	74.125.129.104	80
		02/08 17:47:07	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	17.167.193.105	443
		02/08 17:47:07	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	17.167.193.105	443

© 2019 Palo Alto Networks, Inc.

从端点收集应用程序和流程数据

Windows 注册表和 macOS plist 分别都可用于配置和存储 Windows 和 macOS 操作系统设置。您可以创建自定义检查以便确定是否安装了应用程序（拥有相应的注册表或 plist 项），或者应用程序是否在 Windows 或 macOS 端点上运行（拥有相应的运行进程）。启用自定义检查指示 GlobalProtect 应用程序收集特定注册表信息（Windows 端点的注册表项和注册表项值）和首选项列表 (plist) 信息（macOS 端点的 plist 和 plist 项）。定义要在 GlobalProtect 应用程序收集的原始主机信息数据包括的自定义检查中收集的数据，然后在应用程序连接时提交到 GlobalProtect 网关。

要监控使用自定义检查收集的数据，可以创建 HIP 对象。然后，可以将 HIP 对象添加到 HIP 配置文件，以便使用所收集的数据来匹配端点流量和执行安全规则。网关可以使用 HIP 对象（与在自定义检查中所定义的数据匹配）筛选应用程序所提交的原始主机信息。当网关将端点数据与 HIP 对象进行相匹配时，将会为数据生成 HIP 匹配日志条目。HIP 配置文件也允许网关将所收集的数据与安全规则进行相匹配。如果将 HIP 配置文件用作安全策略规则的匹配条件，网关将会在匹配流量上执行安全规则。

使用以下步骤可启用自定义检查以便从 Windows 和 macOS 端点收集数据。此工作流包括为自定义检查创建 HIP 对象和 HIP 配置文件的可选步骤，允许您将端点数据用作安全策略的匹配条件，以便监控、识别并对流量采取措施。

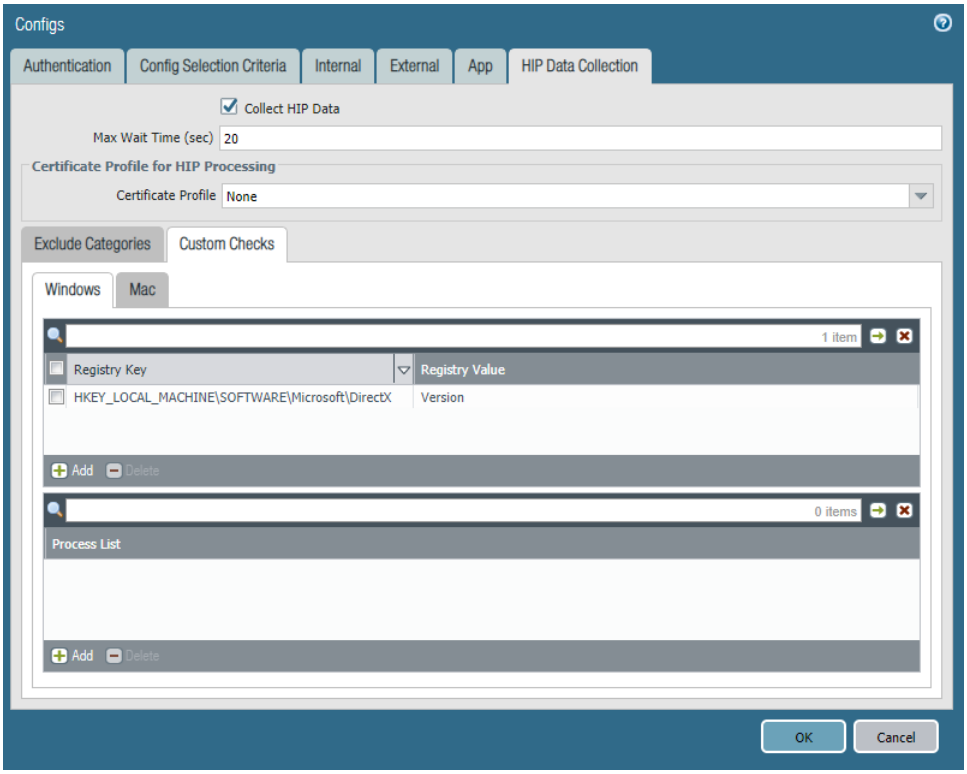
有关直接从 *Windows* 注册表或全局 *macOS plist* 定义应用程序设置的详细信息，请参阅以透明方式部署应用设置。

STEP 1 | 启用 GlobalProtect 应用程序从 Windows 端点收集 Windows 注册表信息或从 macOS 端点收集 Plist 信息。所收集信息的类型可以包括是否已在端点上安装应用程序，或该应用程序的特定特性或属性。

从 Windows 端点收集数据：

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）。
2. 选择现有门户配置或 **Add**（添加）新配置。
3. 在 **Agent**（代理）选项卡上，选择要修改的代理配置或 **Add**（添加）新配置。
4. 选择 **HIP Data Collection**（**HIP** 数据收集）。
5. 启用 GlobalProtect 应用以 **Collect HIP Data**（收集 **HIP** 数据）。
6. 选择 **Custom Checks**（自定义检查）> **Windows**，然后 **Add**（添加）想要收集有关其信息的 **Registry Key**（注册表项）。如果要限制收集注册表项所包含的值的数据，应添加相应的 **Registry Value**（注册表值）。

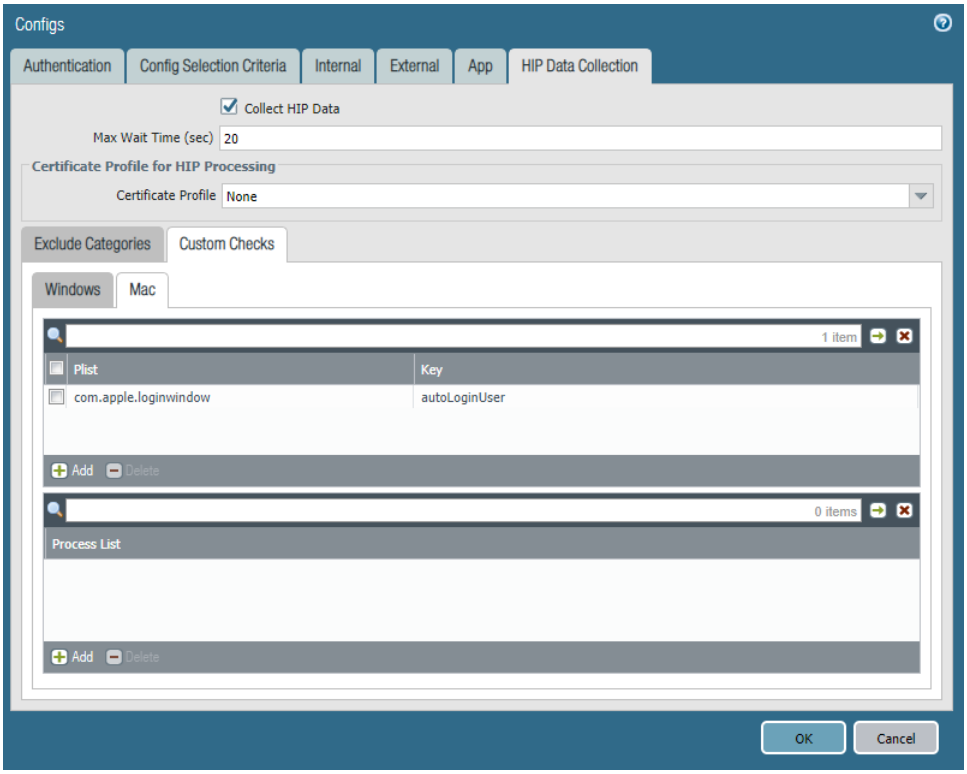
© 2019 Palo Alto Networks, Inc.



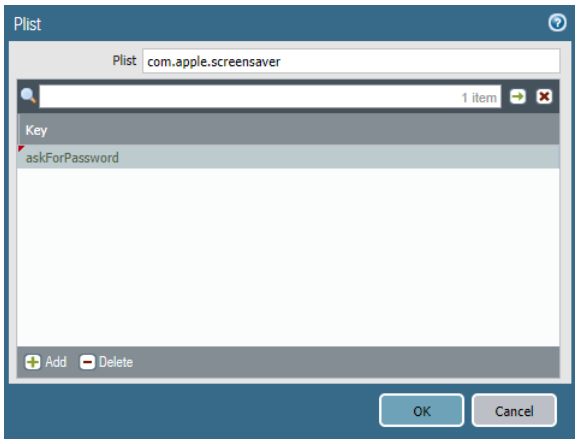
从 macOS 端点收集数据：

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）。
2. 选择现有门户配置或 **Add**（添加）新配置。
3. 在 **Agent**（代理）选项卡上，选择要修改的代理配置或 **Add**（添加）新配置。
4. 选择 **HIP Data Collection**（**HIP** 数据收集）。
5. 启用 GlobalProtect 应用以 **Collect HIP Data**（收集 **HIP** 数据）。
6. 选择 **Custom Checks**（自定义检查）> **Mac**，然后 **Add**（添加）想要收集有关其信息 **Plist** 和相应的 **Key**（表项）以确定是否安装应用程序。

© 2019 Palo Alto Networks, Inc.



例如，**Add**（添加）**Plist** `com.apple.screensaver` 和 **Key**（表项）`askForPassword`，以收集有关在屏幕保护程序开始后唤醒 macOS 端点是否需要密码的信息：



STEP 2 | （可选）检查在端点上是否正在运行特定进程。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）。
2. 选择现有门户配置或 **Add**（添加）新配置。
3. 在 **Agent**（代理）选项卡上，选择要修改的代理配置或 **Add**（添加）新配置。
4. 选择 **HIP Data Collection**（**HIP** 数据收集）。
5. 启用 GlobalProtect 应用以 **Collect HIP Data**（收集 **HIP** 数据）。
6. 选择 **Custom Checks**（自定义检查）> **Windows** 或 **Mac**。
7. 将想要收集有关其信息的进程的名称 **Add**（添加）到 **Process List**（进程列表）。

STEP 3 | 保存自定义检查。

单击 **OK**（确定）并 **Commit**（提交）更改。

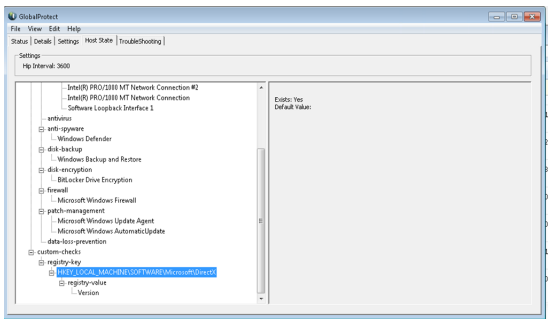
© 2019 Palo Alto Networks, Inc.

STEP 4 | 验证 GlobalProtect 应用程序是否正在从端点收集在自定义检查中定义的数据。

对于 Windows 端点：

1. 单击系统托盘图片，启动用于 Windows 端点的 GlobalProtect 应用程序。GlobalProtect 状态面板打开。
2. 单击设置 (

)图标，打开设置菜单。
3. 选择**Settings**（设置），打开 **GlobalProtect Settings**（**GlobalProtect** 设置）面板。
4. 选择 **Host Profile**（主机配置文件）选项卡，查看 GlobalProtect 正在从端点收集的信息。检验 **custom-checks**（自定义检查）下拉列表是否显示收集需要定义的数据。



对于 macOS 端点：

1. 单击系统托盘图片，启动用于 macOS 端点的 GlobalProtect 应用程序。GlobalProtect 状态面板打开。
2. 单击设置 (

)图标，打开设置菜单。
3. 选择**Settings**（设置），打开 **GlobalProtect Settings**（**GlobalProtect** 设置）面板。
4. 选择 **Host Profile**（主机配置文件）选项卡，查看 GlobalProtect 正在从端点收集的信息。检验 **custom-checks**（自定义检查）下拉列表是否显示收集需要定义的数据。

STEP 5 | （可选）创建 HIP 对象以与注册表项 (Windows) 或 plist (macOS) 相匹配，允许您筛选从 GlobalProtect 应用程序收集的原始主机信息，从而监控自定义检查的数据。

使用为自定义检查数据定义的 HIP 对象，网关可以将应用程序提交的原始数据与 HIP 对象进行匹配并为该数据生成 HIP 匹配日志条目（**Monitor**（监控）> **HIP Match**（**HIP** 匹配））。

对于 Windows 和 macOS 端点：

1. 选择 **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）。
2. 选择现有 HIP 对象或 **Add**（添加）新的配置文件。
3. 在 **Custom Checks**（自定义检查）选项卡上，选择复选框以启用 **Custom Checks**（自定义检查）。

仅对于 Windows 端点：

1. 要检查用于特定注册表项的 Windows 端点，选择 **Custom Checks**（自定义检查）> **Registry Key**（注册表项），然后 **Add**（添加）要相匹配的注册表项。出现提示时，输入 **Registry Key**（注册表项），然后配置以下选项之一：
   - 要匹配注册表项的默认值数据，输入 **(Default) Value Data**（（默认）值数据）。
   - 要匹配没有指定注册表项的端点，选择 **Key does not exist or match the specified value data**（密钥不存在或与指定的值数据不匹配）。

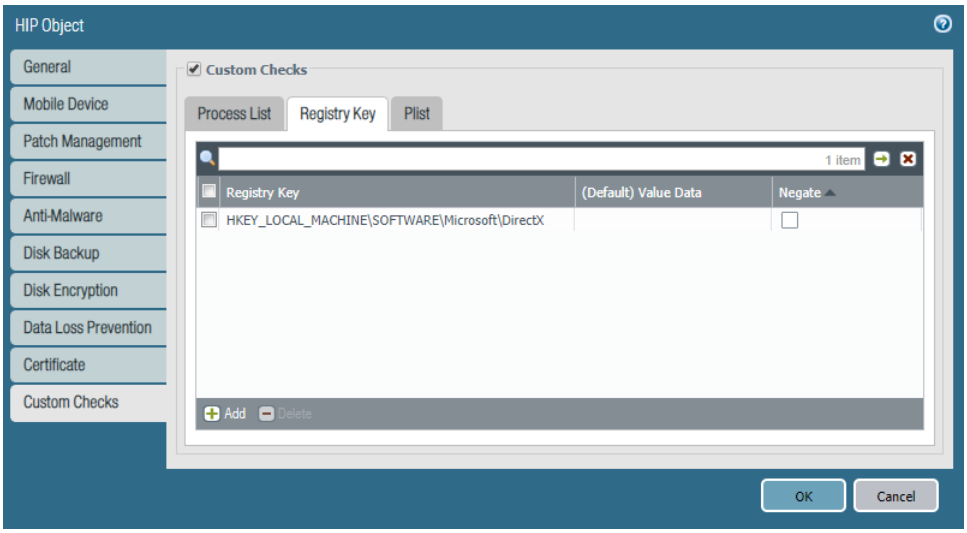
不得同时配置 *(Default) Value Data*（（默认）值数据）和 *Key does not exist or match the specified value data*（密钥不存在或与指定的值数据不匹配）选项。

© 2019 Palo Alto Networks, Inc.

2. 要匹配注册表项内特定值，选择 **Custom Checks**（自定义检查）> **Registry Key**（注册表项），然后 **Add**（添加）要匹配的注册表项。根据提示输入 **Registry Key**（注册表项）。点击 **Add**（添加），然后配置以下选项之一：
   - 要在注册表项内匹配特定值，请输入 **Registry Value**（注册表值）和对应的 **Value Data**（值数据）。
   - 要匹配没有特定注册表值的端点，请输入与 **Registry Value**（注册表值），然后选中 **Negate**（求反）复选框。

   要使用此选项，不得为 *Registry Key*（注册表项）输入任何 *Value Data*（值数据）。

   如果为注册表项添加一个以上的注册表值，*GlobalProtect* 网关将检查端点是否有指定的注册表值。

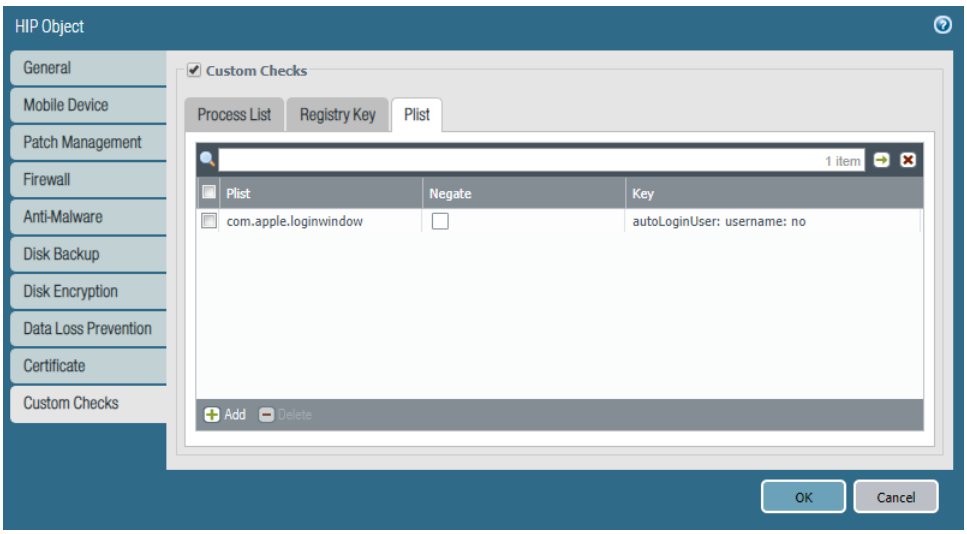


3. 单击 **OK**（确定）保存 HIP 对象。您可以 **Commit**（提交）更改，以便在下一次设备检入时查看 **HIP Match**（**HIP** 匹配）日志中的数据或继续执行步骤 6。

仅对于 macOS 端点：

1. 要检查 macOS 端点是否有特定 plist，请选择 **Plist**，然后 **Add**（添加）您想要检查的 plist。按照输入 **Plist** 的名称。如果您想要匹配没有指定 Plist 的 macOS 端点，启用 **Plist** 不存在选项。
2. 要匹配 plist 内的特定键值对，请选择 **Plist**，然后 **Add**（添加）您想要检查的 plist。出现提示时，输入 **Plist** 的名称，然后 **Add**（添加）一个 **Key**（键）和对应的 **Value**（值）以匹配。或者，如果您想要识别没有特定项和值的端点，可以在添加 **Key**（表项）和 **Value**（值）后选择 **Negate**（求反）。

© 2019 Palo Alto Networks, Inc.



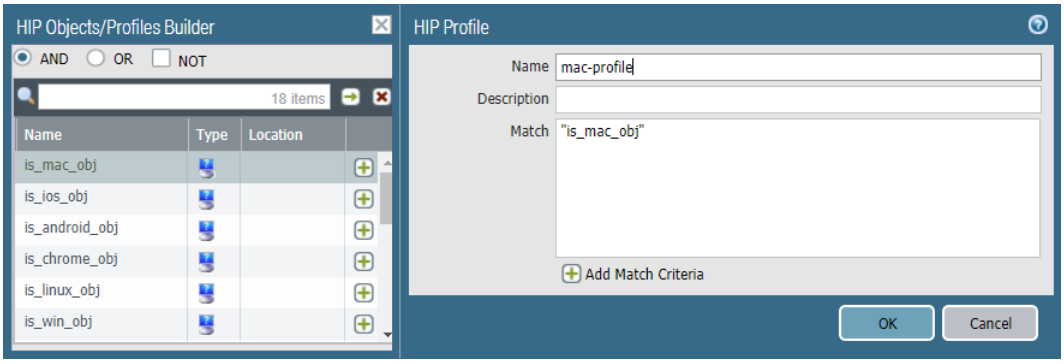
3. 单击 **OK**（确定）保存 HIP 对象。您可以 **Commit**（提交）更改，以便在下一次设备检入时查看 **HIP Match**（**HIP** 匹配）日志中的数据或继续执行步骤 6。

STEP 6 | （可选）创建 HIP 配置文件以允许根据流量评估 HIP 对象。

可以将 HIP 配置文件添加到安全策略作为与该策略匹配的流量的额外检查。当将流量与 HIP 配置文件进行匹配时，将会在流量上执行安全策略规则。

有关创建 HIP 配置文件的详细信息，请参阅配置基于 HIP 的策略实施。

1. 选择 **Objects**（对象）> **GlobalProtect** > **HIP Profile**（**HIP** 配置文件）。
2. 选择现有 HIP 配置文件或 **Add**（添加）新的配置文件。
3. 单击 **Add Match Criteria**（添加匹配标准）可打开 HIP 对象/配置文件生成器。
4. 选择要用作匹配条件的 **HIP object**（**HIP** 对象），然后单击添加（ ）图标以将其移动到“HIP 配置文件”的 **Match**（匹配）区域。
5. 将对象添加到新 HIP 配置文件后，单击 **OK**（确定），然后 **Commit**（提交）。



STEP 7 | 将 HIP 配置文件添加到安全策略，以便可以使用通过自定义检查收集的数据来进行匹配和对流量执行措施。

选择 **Policies**（策略）> **Security**（安全），然后选择现有的安全策略或 **Add**（添加）新的安全策略。在 **User**（用户）选项卡上，将 **HIP Profiles**（**HIP** 配置文件）**Add**（添加）到策略。有关安全策略组件和使用安全策略进行匹配并对流量执行措施的详细信息，请参阅安全策略。

© 2019 Palo Alto Networks, Inc.

重新分发 HIP 报告

要确保一致的主机信息配置文件 (HIP) 策略实施并简化策略管理，您可以分发从 GlobalProtect 应用接收的 HIP 报告，并将其发送至内部或外部 GlobalProtect 网关以及其他网关、防火墙、专属日志收集器 (DLC) 和企业内部的 Panorama 设备。HIP 报告再分发在以下情况中非常有用：

- 您希望将一致的策略应用至内部和外部 GlobalProtect 网关。
- 您希望对经过多个防火墙的特定用户流量应用一致的 HIP 策略。

要重新分发 HIP 报告，可按照用于 重新分发 User-ID 信息的部署建议和最佳做法操作。

使用下列步骤配置 HIP 报告再分发。

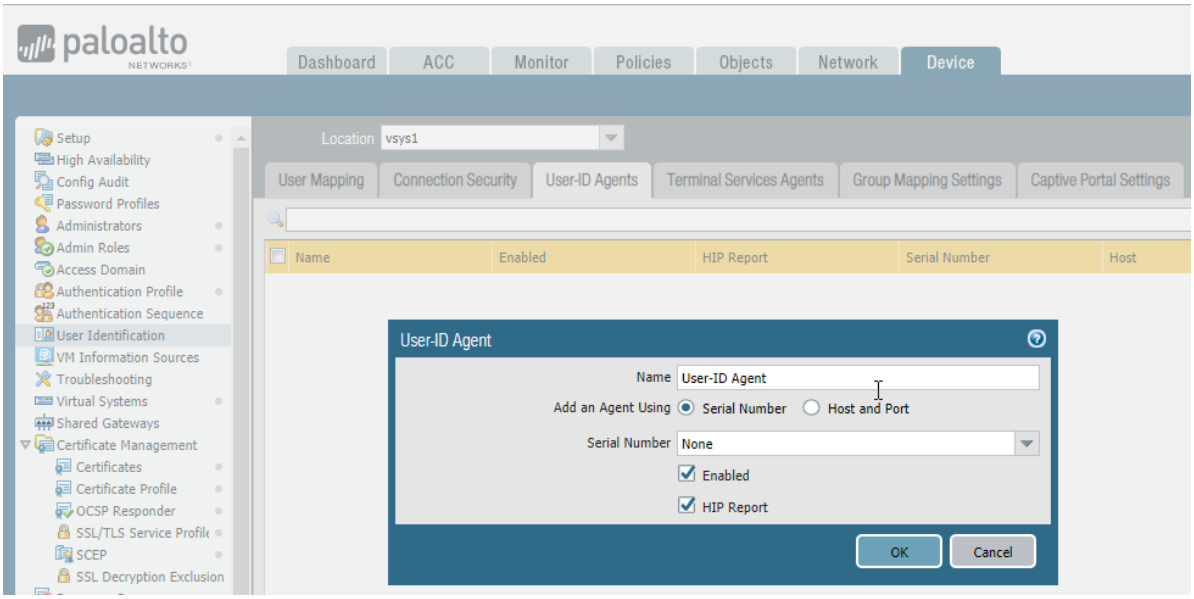
STEP 1 | 配置基于 HIP 的策略实施 用于您的网关和防火墙。

STEP 2 | 配置 HIP 报告再分发。

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **User-ID Agents**（**User-ID** 代理）。
2. 选择现有 User-ID 代理或 **Add**（添加）新的 User-ID 代理。

   代理必须为 *Palo Alto Networks* 下一代防火墙、*GlobalProtect* 网关、*DLC* 或 *Panorama* 设备。

3. 选择 **HIP Report**（**HIP** 报告）。



4. 单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 如果您使用 GlobalProtect 防火墙或网关分发 HIP 报告，请确保您用于重新分发 HIP 报告的防火墙或网关组映射设置与配置了 User-ID 的防火墙或网关的以下属性相匹配。

如果您使用 *Panorama* 设备或 *DLC* 分发 *HIP* 报告，则跳过此步骤。

- 在 HIP 报告再分发防火墙或网关上配置用户属性，以匹配 User-ID 防火墙或网关上的用户属性。

  例如，如果用于 HIP 报告再分发的防火墙或网关拥有 **Primary attribute**（主属性）的 sAMAccountName 和 **Alternate Username 1**（备用用户名 **1**）用户主体名称 (UPN)，请确保在配置了 User-ID 的防火墙或网关上配置相同的值。

  属性无需采用相同的顺序；例如，如果 *HIP* 报告再分发防火墙有 *Primary attribute*（主属性）的 *sAMAccountName* 和 *Alternate Username 1*（备用用户名 *1*）的 *UPN*，则您可以通过 *Alternate Username*（备用用户名）的 *sAMAccountName* 和 *Primary attribute 1*（主属性 *1*）的 *UPN* 配置 *User-ID* 防火墙。
- 如果您的部署在组映射中有用户域配置，则在 HIP 报告再分发防火墙或网关上配置用户域属性，以匹配 User-ID 防火墙或网关上的用户域属性。用户域属性在所有防火墙和网关上必须保持一致。
- 在 HIP 报告再分发防火墙或网关上，配置普通用户组（连接相同身份验证服务器并检索相同用户组的防火墙和网关上的用户组），以匹配 User-ID 防火墙或网关上的用户组。

STEP 4 | 按照您用于重新分发 User-ID 信息至受管防火墙的工作流程，重新分发 HIP 报告至您的受管 Panorama 设备、网关、防火墙和虚拟系统。

© 2019 Palo Alto Networks, Inc.

阻止端点访问

如果用户遗失了提供 GlobalProtect 网络访问权限的端点、该端点被盗或用户离职，您可通过将该端点置于阻止列表中来阻止该端点获取网络访问权限。

阻止列表位于逻辑网络位置本地（vsys，例如 1），每个位置可最多容纳 1,000 个端点。因此，您可为承载 GlobalProtect 部署的每个位置创建单独的阻止列表。

STEP 1 | 确定要阻止的端点的主机 ID。

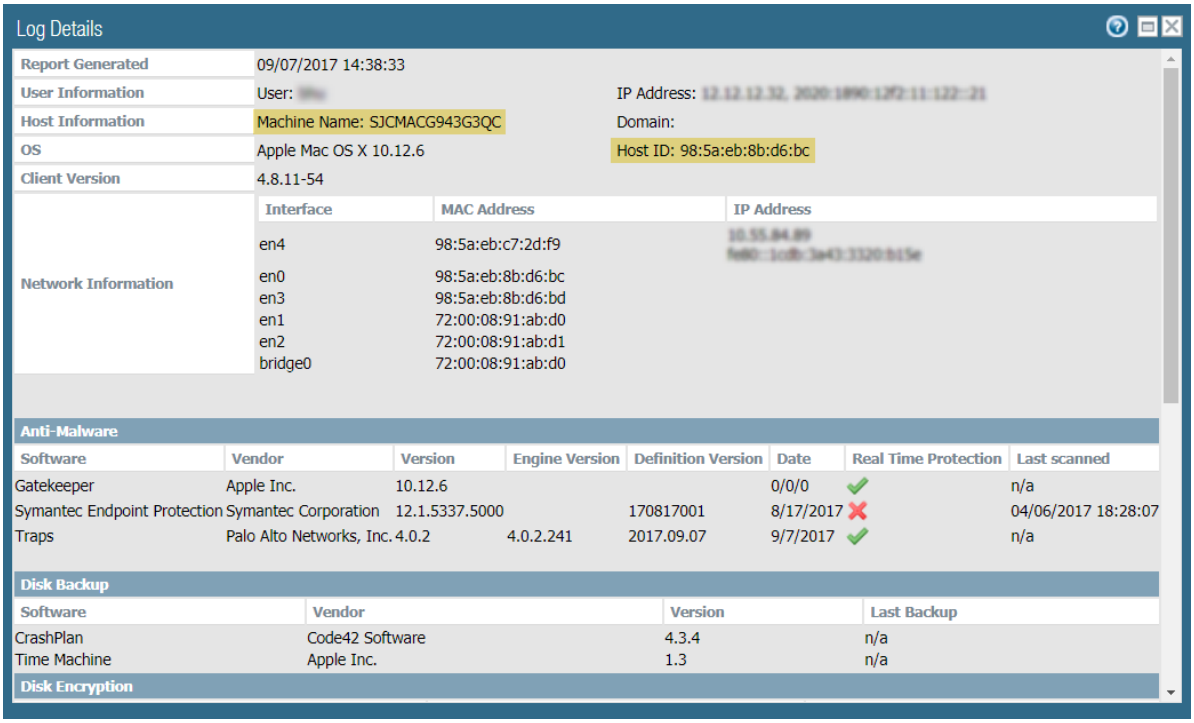
主机 ID 是 GlobalProtect 分配用于标识主机的唯一 ID。主机 ID 值因端点类型而异：

- Windows — 存储在 Windows 注册表中的机器 GUID (HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid)
- macOS — 第一个内置物理网络接口的 MAC 地址
- Android — Android ID
- iOS — UDID
- Chrome — GlobalProtect 分配的唯一字母数字字符串，长度为 32 个字符

如果您不知道主机 ID，则可以将 User-ID 与 HIP 匹配日志中的主机 ID 相关联：

1. 选择 **Monitor**（监控）> **Logs**（日志）> **HIP Match**（**HIP** 匹配）。
2. 过滤与端点关联的源用户的 HIP 匹配日志。
3. 打开 HIP 匹配日志并确定 **OS** > **Host ID**（主机 **ID**）下的主机 ID，并可选择确定 **Host Information**（主机信息）> **Machine Name**（机器名称）下的主机名。

© 2019 Palo Alto Networks, Inc.



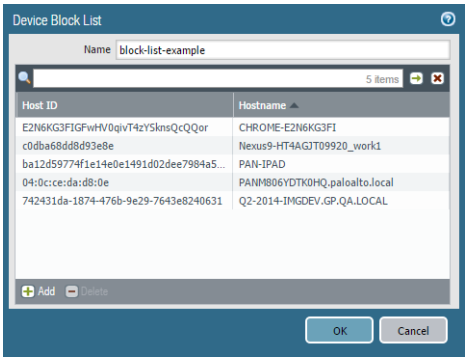
STEP 2 | 创建设备阻止列表。

不可使用 *Panorama* 模板推送设备阻止列表至防火墙。

1. 选择 **Network**（网络）> **GlobalProtect** > **Device Block List**（设备阻止列表），**Add**（添加）设备阻止列表。
2. 为列表输入描述性 **Name**（名称）。
3. 对于具有多个虚拟系统 (vsys) 的防火墙，请选择可提供配置文件的 **Location**（位置）（vsys 或 **Shared**（共享））。

STEP 3 | 添加设备至阻止列表。

© 2019 Palo Alto Networks, Inc.



1. **Add**（添加）端点。为您要阻止的端点输入主机 ID（必需）和主机名（可选）。
2. 根据需要 **Add**（添加）其他端点。
3. 单击 **OK**（确定）以保存并激活阻止列表。

该设备阻止列表无需提交，即时激活。

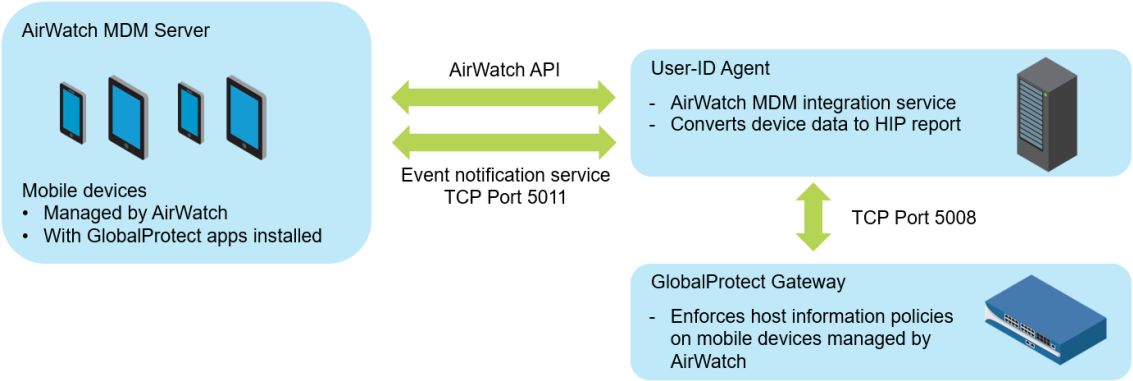
© 2019 Palo Alto Networks, Inc.

配置 Windows User-ID 代理以收集主机信息

基于 Windows 的 User-ID 代理已扩展为支持新的 AirWatch MDM 集成服务。通过此服务，GlobalProtect 可以使用由服务收集的主机信息在由 AirWatch 管理的设备上实施基于 HIP 的策略。作为基于 Windows 的 User-ID 代理的一部分，AirWatch MDM 集成服务使用 AirWatch API 从 VMware AirWatch 管理的移动端点收集信息，并将这些数据转换为主机信息。

对于由 *AirWatch* 管理的 *Android* 端点，此功能支持 *Android for Work* 端点，但不支持其他类型的 *Android* 端点。

- MDM 集成概述
- 收集的信息
- 系统要求
- 配置 GlobalProtect 以检索主机信息
- 解决 MDM 集成服务问题



MDM 集成概述

基于 Windows 的 User-ID 代理包含的 MDM 集成服务会向 AirWatch MDM 服务器进行完整的 HIP 查询，以检索移动设备的完整主机信息。移动设备上的 GlobalProtect 应用程序也会将 HIP 信息发送到网关，网关将合并来自 GlobalProtect 应用程序和 MDM 集成服务的 HIP 信息。当运行 GlobalProtect 应用程序的移动设备连接到 GlobalProtect 网关时，GlobalProtect 可以将安全策略应用到主机信息配置文件。

您可以配置 MDM 集成服务以定期获取 AirWatch 设备信息，并将其推送到 GlobalProtect 网关。此外，该服务还可以监控 AirWatch 事件通知，并在发生 AirWatch 事件（例如，合规性更改）时获取更新的设备信息。

收集的信息

下表显示如何将从 AirWatch 管理的端点收集的信息转换为 HIP 报告属性。映射自动完成。

AirWatch 属性	HIP 报告属性
设备信息	
系列号	serial-number
Mac 地址	wifimac

© 2019 Palo Alto Networks, Inc.

AirWatch 属性	HIP 报告属性
Imei	IMEI
操作系统	version
模型	model
设备友好名称	devname
IsSupervised	supervised
Udid（唯一设备标识符）	udid
用户名	user
上次注册时间	enroll-time
平台	os
注册状态	managed-by-mdm
上次显示时间	last-checkin-time
合规性状态 （User-ID 代理 8.0.3 及更高版本）	合规 不合规 无法使用
所有权 （User-ID 代理 8.0.3 及更高版本）	员工所有 公司专用 公司共享
安全信息	
DataProtectionEnabled	disk-encrypted
IsPasscodePresent	passcode-set
IsPasscodeCompliant	passcode-compliant
网络信息	
DataRoamingEnabled	data-roaming
GPS 坐标	
纬度	latitude
经度	longitude
采样时间	last-location-time

© 2019 Palo Alto Networks, Inc.

AirWatch 属性	HIP 报告属性
应用程序详细信息	
应用名称	appname
版本	version
应用程序标识符	package

系统要求

AirWatch MDM 集成服务需要以下软件：

软件	最低支持版本
User-ID 代理	8.0.1
PAN-OS	7.1.0
适用于 Android 的 GlobalProtect 应用程序	4.0.0
适用于 iOS 的 GlobalProtect 应用	4.0.1
AirWatch 服务器	8.4.7.0
Windows Server	2008 和 2012 2016（包含用户 ID 代理 8.0.4 和 PAN-OS 8.0.4 ）

配置 GlobalProtect 以检索主机信息

按照以下说明配置 GlobalProtect 以从 AirWatch 管理的设备中检索主机信息。

STEP 1 | 安装 User-ID 代理。User-ID 代理必须位于能够安全连接到 VMware AirWatch 移动设备管理 (MDM) 系统的位置。

AirWatch MDM 集成服务包含在基于 Windows 的 User-ID 代理中。

STEP 2 | 在基于 Windows 的 User-ID 代理和 GlobalProtect 网关之间配置 SSL 身份验证。

当您配置 SSL 身份验证时，请确保：

- 在基于 Windows 的 User-ID 代理上配置的服务器证书具有与 User-ID 代理主机的主机名/IP 地址相同的公用名称 (CN)。
- 服务器证书由防火墙信任（包含在防火墙的 MDM 配置中的可信 CA 列表中）。
- 必须将防火墙上配置的 MDM 客户端证书的根证书颁发机构 (CA) 证书导入 Windows 服务器的 Windows 信任存储区。

1. 获取服务器证书和私钥，以便在基于 Windows 的 User-ID 代理和 GlobalProtect 网关之间进行身份验证。证书包必须是包含 PEM 证书，完整证书链和私钥的 PEM 格式。

© 2019 Palo Alto Networks, Inc.

2. 打开基于 Windows 的 User-ID 代理并选择 **Server Certificate**（服务器证书）。
3. **Add**（添加）服务器证书。

- **Browse**（浏览）到证书文件并 **Open**（打开）该文件以将证书上载到基于 Windows 的 User-ID 代理。
- 输入整数的 **Private Key Password**（私钥密码）。
- 单击 **OK**（确定）。

代理验证证书是否有效，并将私钥的加密密码存储在主机的 Windows 证书库中。

如果安装成功，则会在 **Server Certificate**（服务器证书）标签中显示关于证书的详细信息（包括常用名称、到期日期和颁发者）。

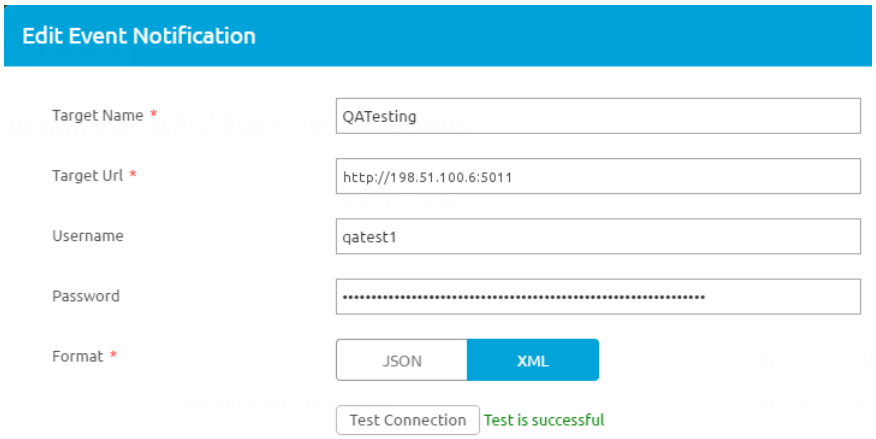
1. 重新启动基于 Windows 的 User-ID 代理。

STEP 3 | 在基于 Windows 的 User-ID 代理上配置 MDM 集成服务。

1. 在基于 Windows 的 User-ID 代理上选择 **MDM Integration**（**MDM** 集成）服务。
2. 为TCP 通信指定一个 **Gateway Connection TCP Port**（网关连接 **TCP** 端口）。基于 Windows 的 User-ID 代理在此端口侦听所有与 MDM 相关的消息。默认端口为 5008。要更改端口，请指定从 1 至 65535 之间的数字。
3. 在 **Setup**（设置）选项卡上，单击 **Edit**（编辑）。
4. 为 **MDM Vendor**（**MDM** 供应商）选择 **AirWatch**。

STEP 4 | 指定 **MDM Event Notification**（**MDM** 事件通知）监控和收集 AirWatch 事件的设置（例如，设备注册、设备擦除和合规性更改）。发生事件时，MDM 集成服务从 AirWatch API 获取更新的设备信息，并将此信息推送到所有已配置的 GlobalProtect 网关。

对于 *MDM Event Notification*（*MDM* 事件通知），请确保您在此处输入的值也在 *AirWatch* 控制台的 *Groups & Settings*（群组和设置）> *All Settings*（所有设置）> *System*（系统）> *Advanced*（高级）> *API* > *Event Notifications*（事件通知）下进行了配置。

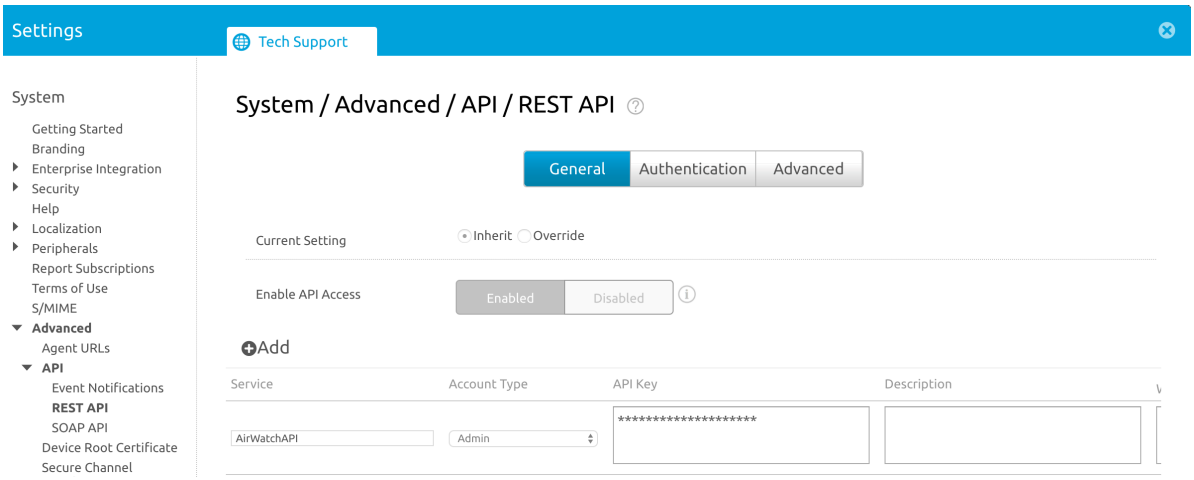


- 设置 **TCP Port**（**TCP** 端口）以便与事件通知服务进行通信。使用此格式：`http://<external_hostname>/<ip_address>:<port>`，其中 `<ip-address>` 是 MDM 集成服务的 IP 地址。默认端口为 5011。要更改端口，请指定从 1 至 65535 之间的数字。
- 对于事件通知，输入验证传入请求所需的 **Username**（用户名）和 **Password**（密码）凭据。
- 输入 **Permitted IP**（允许的 **IP**）访问 MDM 事件的地址。这是发布 MDM 事件的 IP 地址的逗号分隔列表。例如，AirWatch 服务器的 IP 地址。请联系您的 AirWatch 支持团队，获取有关指定哪些 IP 地址的指导。

STEP 5 | 添加 **MDM API Authentication**（**MDM API** 身份验证）设置，以便与 AirWatch API 连接。

© 2019 Palo Alto Networks, Inc.

- 输入基于 Windows 的 User-ID 代理将连接的 AirWatch MDM 服务器的 **Server Address**（服务器地址）。例如，`api.awmdm.com`。
- 输入访问 AirWatch MDM API 所需的 **Username**（用户名）和 **Username**（密码）凭据。
- 输入 **Tenant Code**（租户代码）。这是访问 AirWatch MDM API 所需的唯一十六进制代码数字。在 AirWatch 控制台上，您可以在 **System**（系统）> **Advanced**（高级）> **API** > **REST API** > **API Key**（**API** 密钥）中找到租户代码。



- 输入 **Mobile Device State Retrieval Interval**（移动设备状态检索间隔）。此设置控制从 AirWatch 管理的设备检索主机信息的频率。默认间隔为 30 分钟。要更改该时间间隔，请指定从 1 至 600 之间的数字。

STEP 6 | **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

STEP 7 | 点击 **Test Connection**（测试连接）以确保基于 Windows 的 User-ID 代理可以连接到 AirWatch API。

STEP 8 | 将 GlobalProtect 网关配置为与 MDM 集成服务通信，以检索由 AirWatch 管理的设备的 HIP 报告。

1. 在 PAN-OS Web 界面中，选择 **Network**（网络）> **GlobalProtect** > **MDM**。
2. **Add**（添加）以下有关 MDM 集成服务的信息。

- **Name**（名称）— 输入 MDM 集成服务的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
- （可选）选择网关所属的虚拟系统。
- **Server**（服务器）— 输入网关进行连接以检索 HIP 报告的 Airwatch MDM 集成服务接口的 IP 地址或 FQDN。确保您具有此接口的服务路由。
- **Connection Port**（连接端口）— 输入 MDM 集成服务侦听 HIP 报告请求的连接端口。默认端口为 5008。要更改端口，请指定从 1 至 65535 之间的数字。
- **Client Certificate**（客户端证书）— 选择在建立 HTTPS 连接时网关要呈递给 MDM 集成服务的客户端证书。您可以从下拉列表中选择客户端证书，也可以导入新客户端证书。**Certificate Purpose**（证书目的）必须表明它是客户端身份验证证书。

客户端证书的根证书颁发机构 (CA) 证书必须导入到安装了 User-ID 代理的 Windows 服务器的 Windows 信任存储区中。

1. **Add**（添加）与安装在 MDM 集成服务主机上的服务器证书关联的根 CA 证书。您需要根 CA 证书和服务器证书来建立网关和 MDM 集成服务之间的安全连接。您可以从下拉列表中选择一个根 CA 证书，也可以 *Import*（导入）一个新证书。
2. 单击 **OK**（确定）。
3. **Commit**（提交）更改。

STEP 9 | 检查您的连接，确保将 AirWatch 设备数据传输到 GlobalProtect。

1. 打开基于 Windows 的 User-ID 代理并选择 **MDM Integration**（**MDM** 集成）> **Mobile Devices**（移动设备）。您应该看到由 AirWatch 管理的所有设备的唯一设备 ID 和用户名的列表。
2. （可选）您可以 **Filter**（过滤）该列表以找到具体的 **Mobile Device**（移动设备）。
3. （可选）。在设备 ID 列表中选择一个设备，然后单击 **Retrieve Device State**（检索设备状态）以提取有关设备的最新信息，并查看它如何映射到 GlobalProtect 网关的主机信息配置文件。

解决 MDM 集成服务问题

如果遇到事件通知问题或 AirWatch REST API 验证问题，请按照这些说明进行操作。

- MDM 集成服务未收到 AirWatch MDM 服务器的事件通知。
  1. 设置 **Debug**（调试）选项（在 **File**（文件）菜单中）以 **Debug**（调试）或 **Verbose**（详细列出）。
  2. 转到 Windows 服务器上的 User-ID 代理安装文件夹，然后打开 `MaDebug` 文件。查找类似于以下内容的消息：

```
The address x.x.x.x
is not in the permitted ip list for event notifications.
```

  3. 添加此 IP 地址作为一个 **Permitted IP**（允许的 **IP**）地址（**MDM Integration**（**MDM** 集成）> **Setup**（设置）> **Permitted IP**（允许的 **IP**））。

- 对 Airwatch REST API 的身份验证不成功。

  确保：

© 2019 Palo Alto Networks, Inc.

- 用于 MDM 集成服务对 AirWatch MDM 服务进行身份验证的凭据有效。
- 用于访问 Airwatch REST API 的用户帐户对 AirWatch 管理的移动设备和用户具有 API 访问权限，至少有只读权限。
- 该 **Tenant Code**（租户代码）（API 密钥）与用户帐户正确关联。删除所有未使用的 API 密钥。

© 2019 Palo Alto Networks, Inc.

使用主机信息隔离设备

GlobalProtect 允许您手动或自动添加受影响设备到隔离列表。隔离设备后，您可以使用 GlobalProtect 阻止用户从该设备登录到网络。您还可以限制流向受影响设备、从受影响设流出或受影响设备之间的流量。如果使用 Panorama 设备，您还可以重新分发隔离设备信息到其他下一代防火墙。使用下列主题了解如何隔离设备（包括 GlobalProtect 订阅许可证要求）以及如何重新分发隔离信息。

- 识别并隔离受影响的设备 — 概述和许可证要求
- 查看隔离设备信息
- 从隔离列表中手动添加并删除设备
- 自动隔离设备
- 使用 GlobalProtect 和安全策略阻止访问隔离设备
- 从 Panorama 重新分发设备隔离信息

识别并隔离受影响的设备 — 概述和许可证要求

通过 GlobalProtect，您可以通过识别带主机 ID（或者是序列号，而非源 IP 地址）的受影响设备，阻止受影响设备访问网络。此功能更适用于根据 IP 地址阻止受影响端点访问网络，因为一旦设备 IP 地址发生更改（例如，如果用户将其端点从工作位置移至家里），基于 IP 地址的安全策略就会允许端点返回到网络。

将设备识别为受影响（例如，如果设备遭受恶意软件的攻击，且正在执行命令和控制操作）后，您可以手动添加设备的主机 ID 到隔离列表，并配置 GlobalProtect 以防止用户从隔离设备连接到 GlobalProtect 网关。此外，您还可以使用带安全策略或 HIP Match（HIP 匹配）日志设置的日志转发配置文件自动隔离设备。

开始隔离设备之前，请务必确保您的 GlobalProtect 用户使用的 GlobalProtect 应用程序最低版本为 5.1。此外，防火墙上还必须拥有一个有效的 GlobalProtect 订阅许可证，以便防火墙将受影响设备添加到隔离列表中。此功能的 GlobalProtect 订阅许可证要求的实施如下表所述。

- 防火墙需要 GlobalProtect 订阅许可证来手动或自动添加设备到隔离列表。如果在没有许可证的情况下尝试添加设备，将会收到一条错误消息，如下所示：`The device cannot be quarantined.You must have a valid GlobalProtect subscription to add the device to the quarantine list.`（设备无法隔离。您必须拥有有效的 `GlobalProtect` 订阅以将设备添加到隔离列表。）

  但是，您可以在没有许可证的情况下删除隔离列表中的隔离设备。
- 如果您的 GlobalProtect 订阅许可证过期，隔离列表会被保留，不会被删除。

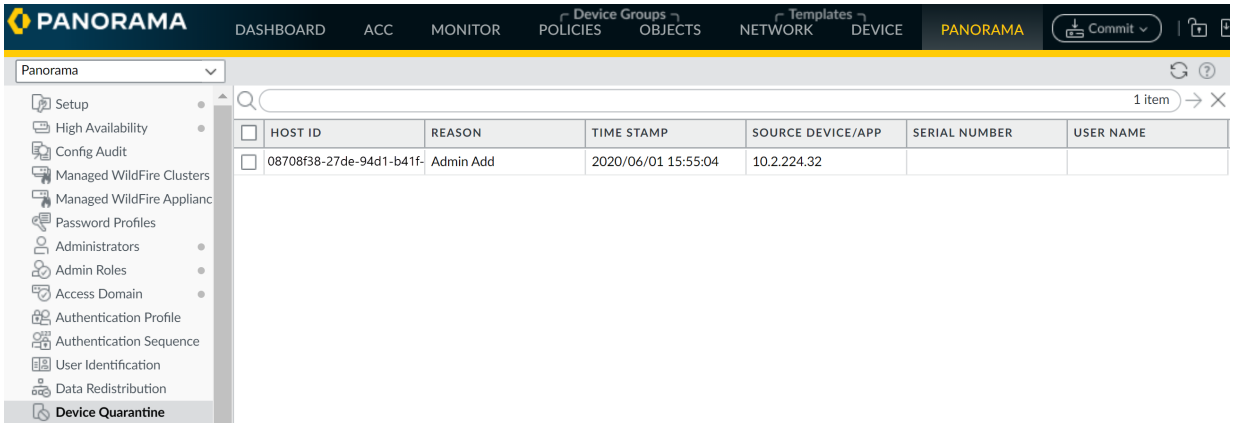
  GlobalProtect 每小时执行一次许可证检查。
- 如果您没有有效的 GlobalProtect 许可证，且满足以下条件之一，一旦提交更改，您的防火墙或 Panorama 将会显示一条警告消息：
  - 您已选择数据重新分发代理中的 **Quarantine List**（隔离列表）。
  - 您已选择 **Quarantine**（隔离）作为 **Log Forwarding Profile**（日志转发配置文件）的内置操作。

查看隔离设备信息

您可以从 **Device Quarantine**（设备隔离）页面查看隔离设备信息。如果您从下一代防火墙或 Panorama 设备进行查看，则该页面的位置可能有所不同。

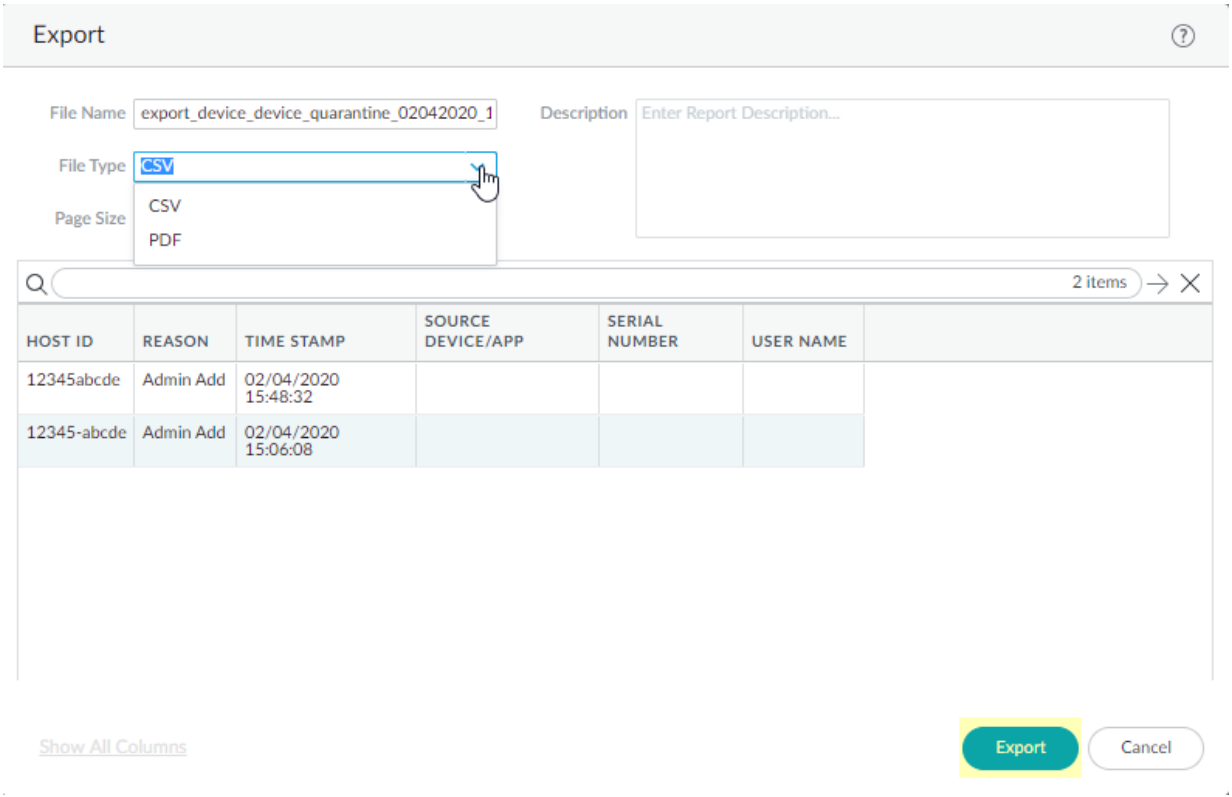
- 在下一代防火墙中，通过选择**Device**（设备）> **Device Quarantine**（设备隔离）以查看隔离设备列表。
- 在 Panorama 设备中，通过选择**Panorama** > **Device Quarantine**（设备隔离）查看 **Device**（设备）> **Device Quarantine**（设备隔离）。

© 2019 Palo Alto Networks, Inc.



- 您还可以从 ACC 查看 GlobalProtect 隔离活动。ACC 的 **GlobalProtect Quarantine Activity**（**GlobalProtect 隔离活动**）选项卡中包含窗格 **GlobalProtect Quarantine Activity**（**GlobalProtect 隔离活动**），其中会显示隔离设备的图表视图。使用图表顶部的切换键，根据导致 GlobalProtect 隔离设备的操作、GlobalProtect 隔离设备的原因、以及隔离设备的位置查看隔离设备。
- 若要导出 pdf 或 csv 文件格式的隔离设备列表，请选择 **Device Quarantine**（设备隔离）页面底部的 **PDF/CSV**，然后打开 **Export**（导出）页面。

© 2019 Palo Alto Networks, Inc.

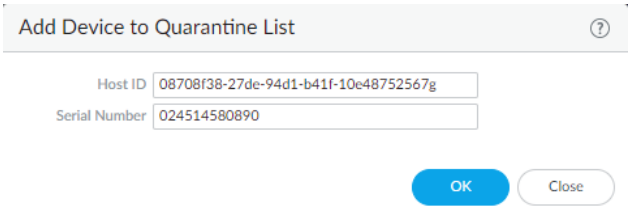


从隔离列表中手动添加并删除设备

您可以通过使用 API，从“隔离”页面，或是从 GlobalProtect、Threat（威胁）、Traffic（流量）或 Unified（统一）日志手动添加设备。此外，您还可以从隔离列表中手动删除设备，步骤如下所示。

- 若要从 **Device Quarantine**（设备隔离）页面手动添加设备到隔离列表，请选择**Device**（设备）> **Device Quarantine**（设备隔离）或 **Panorama** > **Device Quarantine**（设备隔离），然后 **Add**（添加）设备。

  添加设备 **Host ID**（主机 **ID**）或是 **Serial Number**（序列号）。GlobalProtect 使用主机 ID 识别设备。

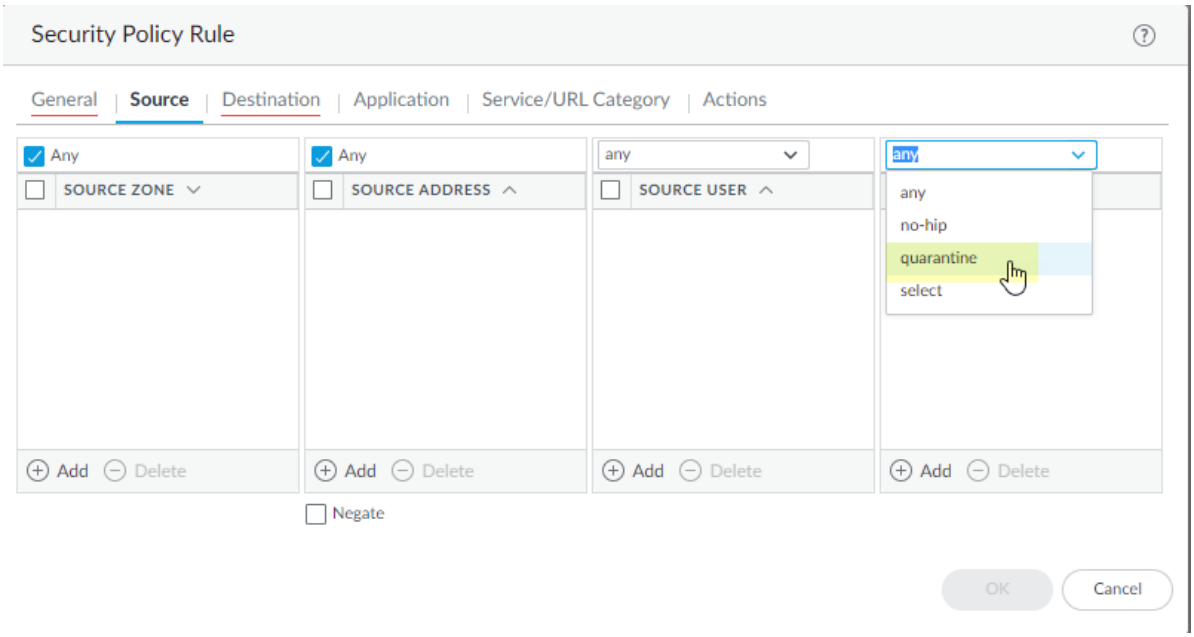


- 若要从 GlobalProtect、Threat（威胁）、Traffic（流量）或 Unified（统一）日志添加设备到隔离列表，请完成下列步骤。

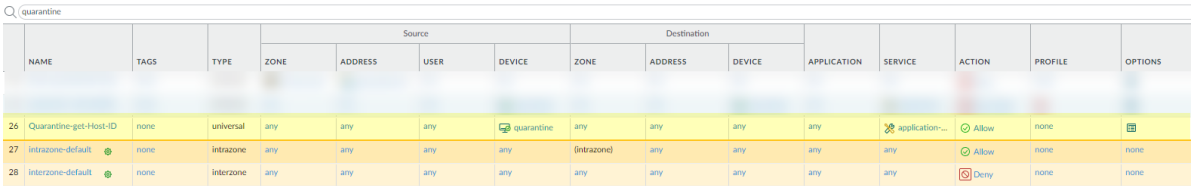
© 2019 Palo Alto Networks, Inc.

1. （仅限威胁、流量和统一日志）要添加主机 ID 信息到流量、威胁和统一日志，请选择**Policies**（策略）> **Security**（安全），**Add**（添加）安全策略规则；然后选择 **Quarantine**（隔离）设备作为 **Source**（源）流量的**Source Device**（源设备）。

   添加设备到隔离列表时，需要使用主机 ID。一旦用户使用 GlobalProtect 应用程序连接到网络，GlobalProtect 就会自动添加连接端点的主机 ID 信息到 GlobalProtect 日志。为使 GlobalProtect 自动添加主机 ID 信息到“流量”、“威胁”或“统一”日志，必须添加已选择 **Quarantine**（隔离）设备充当源流量的策略规则。



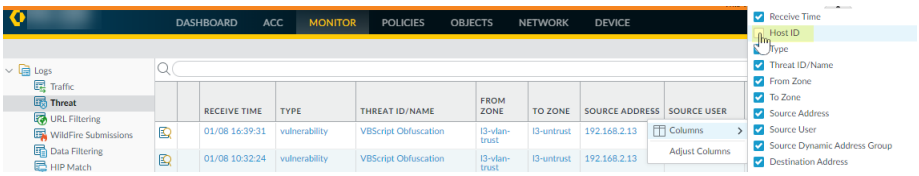
为确保可添加您要（手动或自动）隔离的所有设备的主机 *ID*，请创建允许所有流量的安全策略，并指定 *Quarantine*（隔离）设备作为 *Source Device*（源设备）。无论您将此策略置于策略列表的哪个位置，都不会影响它的作用。



2. 右键单击与设备关联的 **Host ID**（主机 **ID**），然后单击 **Block Device**（阻止设备）。

如果 **Host ID**（主机 **ID**）列没有显示，请选择任何列的标题，然后选择 **Host ID**（主机 **ID**）字段以显示主机 ID。

© 2019 Palo Alto Networks, Inc.



- 若要创建 API 以手动添加设备，请参阅PAN-OS 和 Panorama API 使用指南中的说明。

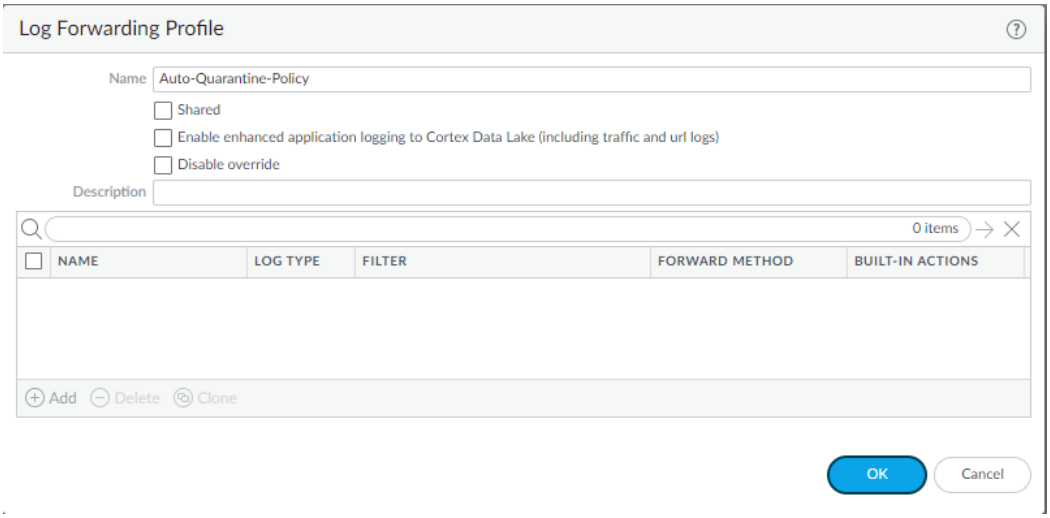
- 在管理员对设备执行修复后，您可以通过选择**Device**（设备）> **Device Quarantine**（设备隔离）（下一代防火墙）或 **Panorama** > **Device Quarantine**（设备隔离）（Panorama 设备），然后选择一个或多个设备，最后选择 **Delete**（删除），以从列表中删除设备。

自动隔离设备

您可以使用带安全策略规则或 HIP 匹配日志设置的日志转发配置文件自动隔离设备。

- 若要使用日志转发配置文件隔离设备，请完成下列步骤。

  1. 选择 **Object**（对象）> **Log Forwarding**（日志转发），然后 **Add**（添加）新的日志转发配置文件或选择现有配置文件进行修改。



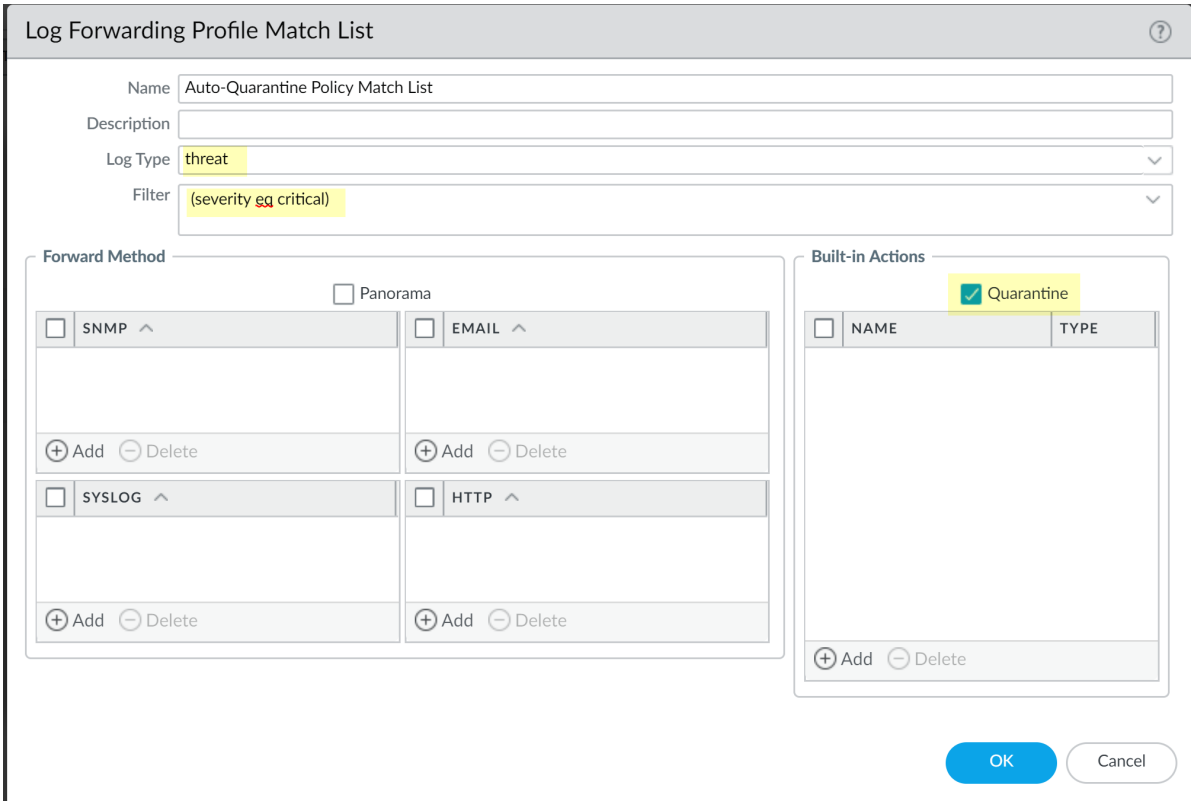
  2. **Add**（添加）**Log Forwarding Profile Match List**（日志转发配置文件匹配列表），然后在 **Built-in Actions**（内置操作）部分中选择 **Quarantine**（隔离）。

     指定 **GlobalProtect**、**Threat**（威胁）或 **Traffic**（流量）的 **Log Type**（日志类型）。

     如果指定 *Threat*（威胁）或 *Traffic*（流量）的 *Log Type*（日志类型），请务必通过创建一个安全策略规则且其中具有作为 *Source*（源）流量 *Source Device*（源设备）的 *Quarantine*（隔离）设备，将主机 *ID* 与某个设备关联，以便添加主机 *ID*。如果没有主机 *ID*，就无法添加设备到隔离列表。

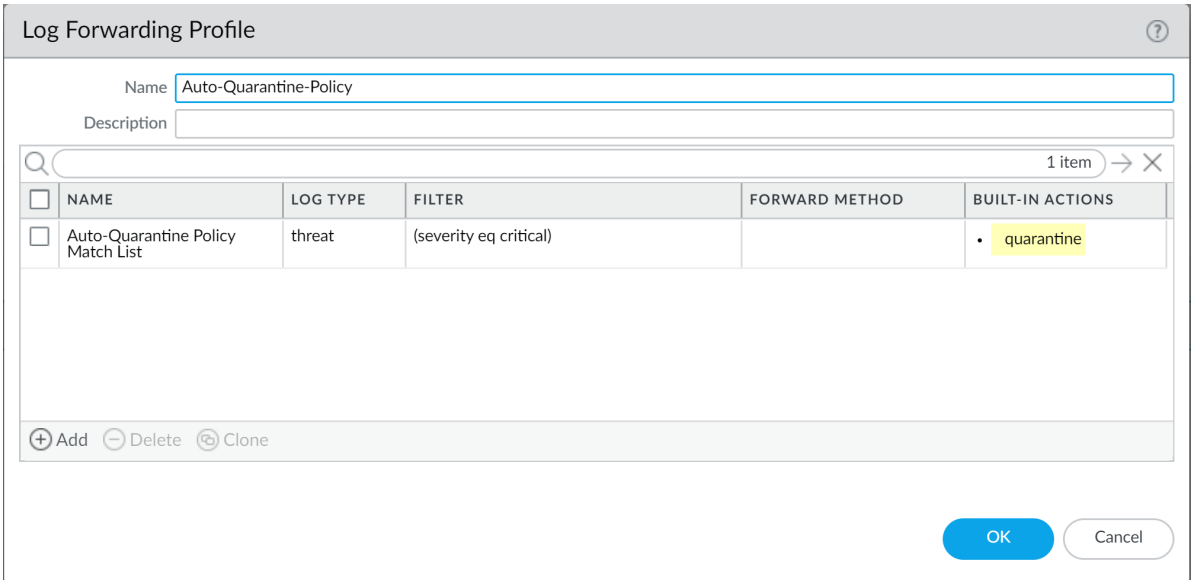
     在下例中，使用了 **Threat**（威胁）的**Log Type**（日志类型），且严重性级别是“严重”。将此配置文件添加到安全策略后，如果这些标准都匹配，那么，防火墙会将设备从此流量起始位置添加到隔离列表。

© 2019 Palo Alto Networks, Inc.

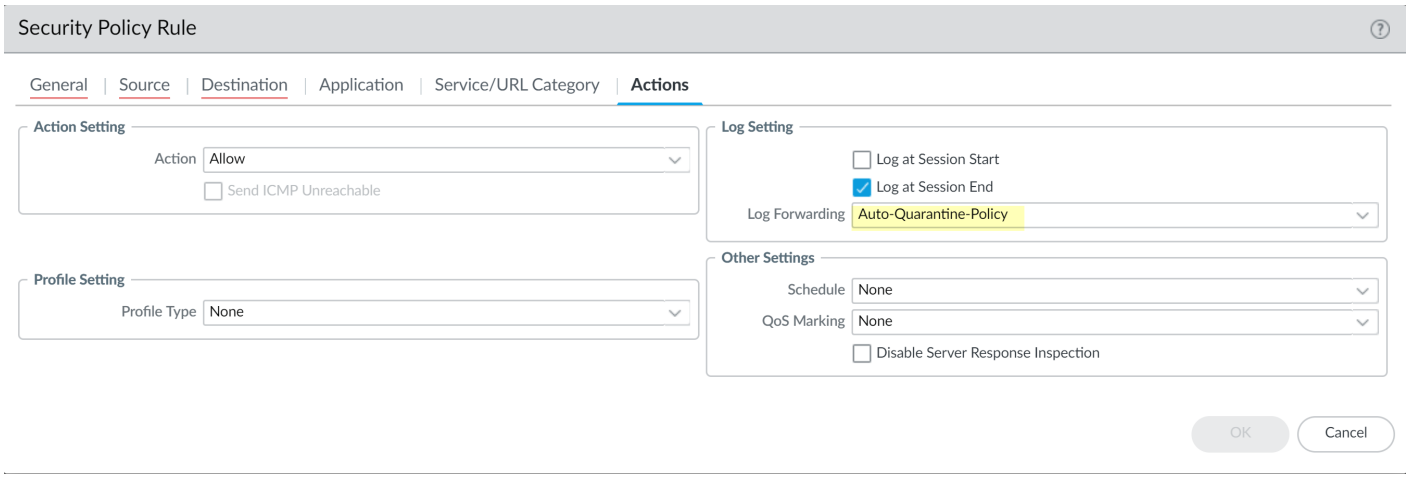


添加匹配列表后，日志转发配置文件将在 **Built-In Actions**（内置操作）项下显示 **Quarantine**（隔离）。

© 2019 Palo Alto Networks, Inc.



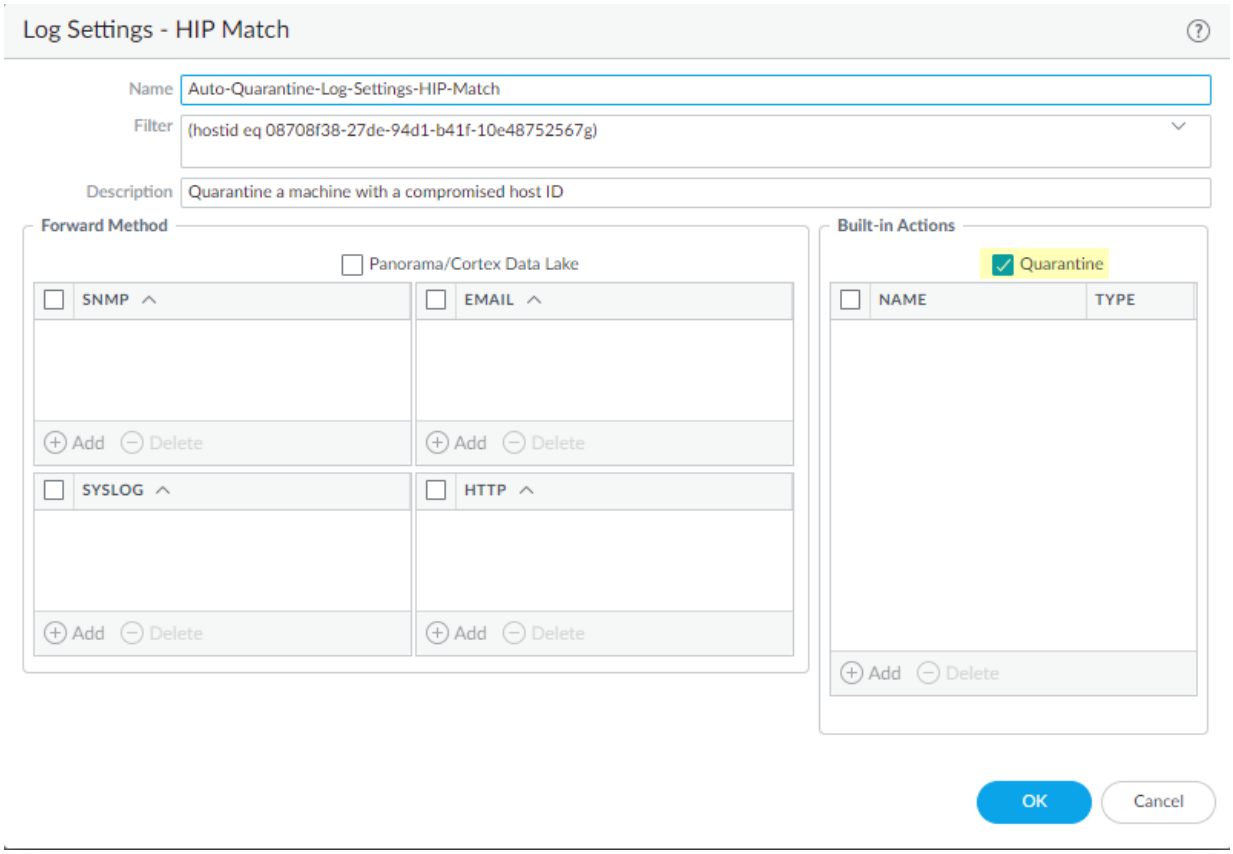
3. 选择 **Policies**（策略）> **Security**（安全），并 **Add**（添加）安全策略。
4. 选择 **Actions**（操作），然后选择您所创建的 **Log Forwarding profile**（日志转发配置文件）。



- 若要使用 HIP 匹配日志设置自动隔离设备，请选择 **Device**（设备）> **Log Settings**（日志设置）> **HIP Match**（HIP 匹配），然后 **Add**（添加）**Built-In Actions**（内置操作）为 **Quarantine**（隔离）的日志设置。

  在下面的日志设置中，**Filter**（筛选器）使用的主机 ID 为 08708f38-27de-94d1-b41f-10e48752567g。如果 HIP 匹配日志找到此主机 ID 的匹配项，此日志设置会将该设备添加到隔离列表。与日志转发配置文件不同的是，您无需将此日志设置添加到安全策略以使其生效。

© 2019 Palo Alto Networks, Inc.

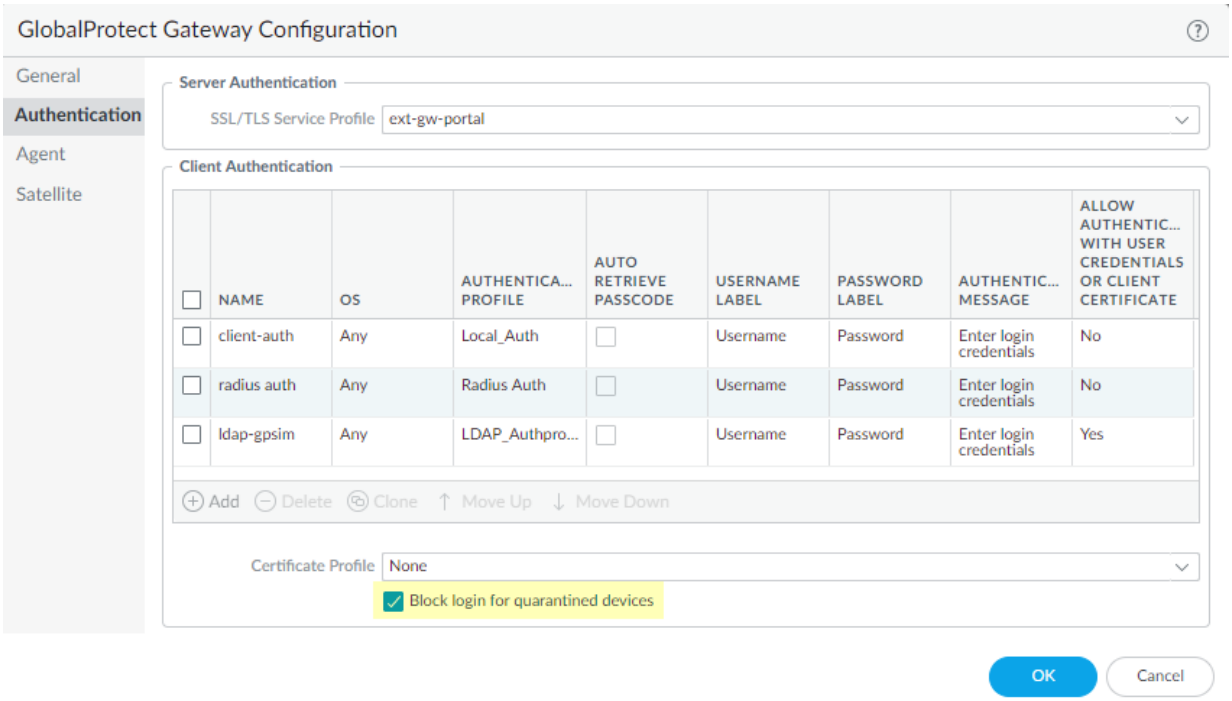


使用 GlobalProtect 和安全策略阻止访问隔离设备

您可以通过配置网关身份验证，阻止用户从隔离设备登录到 GlobalProtect。此外，您还可以通过指定安全策略规则中的选项，阻止隔离设备在网络中发送或接收流量。完成下列任务以阻止 GlobalProtect 用户访问隔离设备，或是管理隔离设备的网络访问。

- 若要阻止用户从隔离设备登录到 GlobalProtect，请配置 GlobalProtect 网关身份验证（**Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *gateway-configuration*（网关配置）> **Authentication**（身份验证）），然后选择 **Block login for quarantined devices**（阻止隔离设备登录）。

© 2019 Palo Alto Networks, Inc.



如果用户尝试从隔离设备登录到已启用 **Block login for quarantined devices**（阻止隔离设备登录）的网关，GlobalProtect 应用程序将通知用户该设备已被隔离，用户无法从该设备登录。如果未启用此设置，用户将收到通知，但是仍能从隔离设备登录。

- 若要通过安全策略规则阻止从隔离设备的访问，请为源或目标流量指定 **Quarantine**（隔离）选项，然后指定可阻止隔离设备的操作。

  若在安全策略规则中指定 **Quarantine**（隔离），意味着规则将使用隔离列表中的设备用作匹配标准，无论您是将 **Quarantine**（隔离）设备指定为 **Source**（源）流量的 **Source Device**（源设备）还是 **Destination**（目标）流量的 **Destination Device**（目标设备）。下例中显示了 **Quarantine**（隔离）的源 **Device**（设备）、HQ 服务器的目标 IP 地址、以及 **Deny**（拒绝）操作。通过此安全策略规则，隔离列表中的所有设备均无法访问 HQ 服务器。

为使策略或防火墙中的隔离设备生效，*GlobalProtect* 用户必须能从隔离设备成功登录到 *GlobalProtect*，且防火墙必须知悉此登录事件。如果防火墙配置为 *GlobalProtect* 网关，那么，用户可以从隔离设备登录到此网关，以验证策略中的设备。用户从隔离设备成功登录到网关后，网关将实施策略，您可以 重新分发隔离设备信息，且还能在网络中任何防火墙或网关的策略中实施。如果用户已被阻止，不能登录到网关（例如，如果您已在网关配置

© 2019 Palo Alto Networks, Inc.

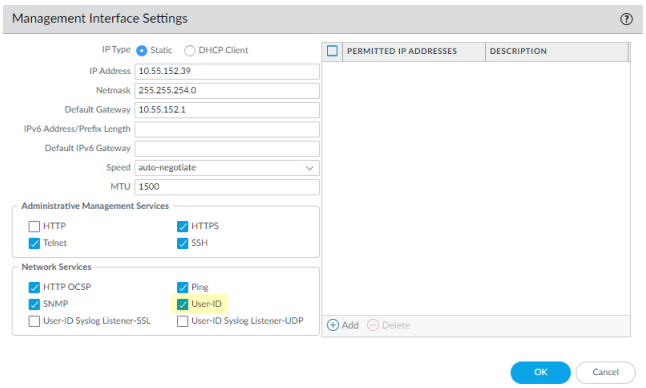
中选择 *Block login for quarantined devices*（阻止隔离设备登录）），那么，该登录就不被视为成功登录。

从 Panorama 重新分发设备隔离信息

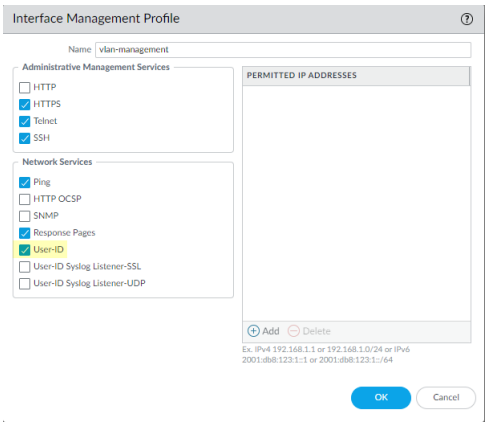
如果使用 Panorama 设备管理您的下一代防火墙，您可以在 **Panorama** > **Device Quarantine**（设备隔离）中创建适用于所有防火墙的隔离列表，并分发该信息到您的托管防火墙。重新分发设备隔离信息的方式与重新分发 User-ID 信息的方式相同。完成下列步骤，以从 Panorama 重新分发隔离信息。

STEP 1 | 如果尚未这样操作，请在代理服务器上启用 User-ID。

- 如果重新分发代理服务器使用管理接口，请选择 **Device**（设备）> **Setup**（设置）> **Interfaces**（接口）> **Management**（管理），然后选择 **User-ID**。



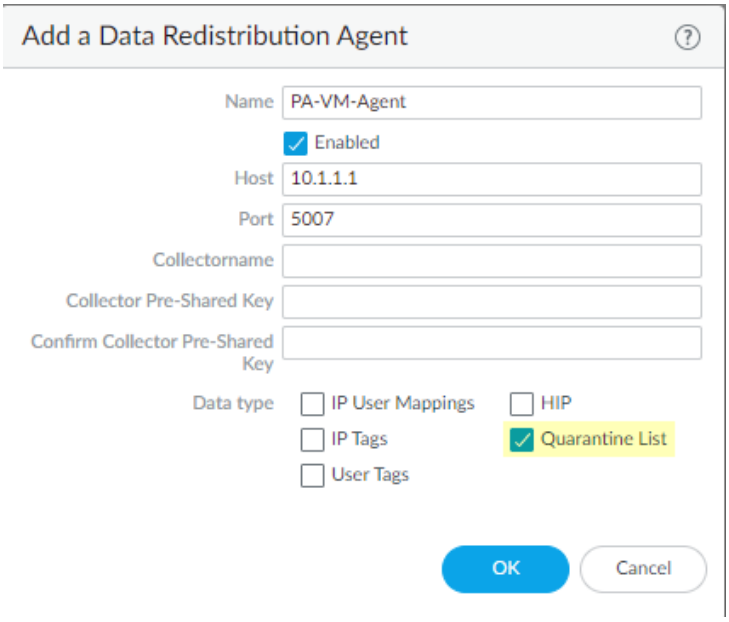
- 如果重新分发代理使用数据面板上的接口（例如，以太网或 VLAN 接口），请选择 **Network**（网络）> **Interface Mgmt**（接口管理），然后选择现有管理配置文件或 **Add**（添加）新的管理配置文件，最后选择 **User-ID**。



STEP 2 | 若要创建数据重新分发代理，请选择**Panorama** > **Data Redistribution**（数据重新分发）并 **Add**（添加）代理。

下例显示的是数据重新分发代理，其中 Panorama 将 **Quarantine List**（隔离列表）信息分发给 IP 地址为 10.1.1.1、端口为 5007 的防火墙。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

认证

当您启用 FIPS-CC 模式时，Windows 和 macOS 端点的 GlobalProtect™ 应用满足联邦信息处理标准 (FIPS 140-2) 和通用标准 (CC) 要求。这些安全认证确保了一系列的标准安全保障和功能，且美国政府机构和其他国内和国际管制行业通常会要求这样的安全认证。有关产品证书和第三方验证的更多详细信息，请参阅 Palo Alto Networks 认证页面。

有关如何在 FIPS-CC 模式下，对 Windows 和 macOS 端点的 GlobalProtect 应用进行配置和故障排除的信息，请参见以下章节：

> 启用并验证 FIPS-CC 模式
> FIPS-CC 安全功能
> FIPS-CC 故障排除模式

启用并验证 FIPS-CC 模式

您可以通过以下方法，启用并验证 GlobalProtect 应用的 FIPS-CC 模式：

- 通过 Windows 注册表启用并验证 FIPS-CC 模式
- 通过 macOS 属性列表启用并验证 FIPS-CC 模式

要修改 *Windows* 注册表或 *macOS plist*，您必须拥有 *Windows* 或 *macOS* 中的管理员帐户。

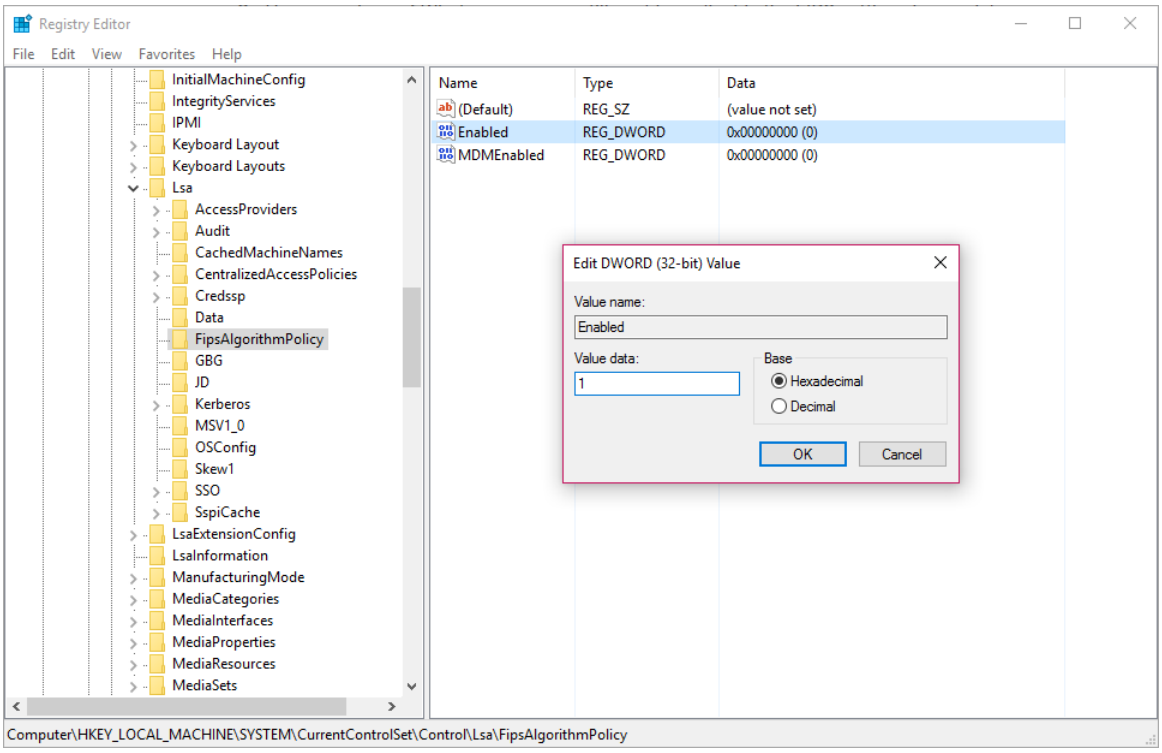
通过 Windows 注册表启用并验证 FIPS-CC 模式

在 Windows 端点上，使用以下步骤通过 Windows 注册表启用并验证 GlobalProtect™ 的 FIPS-CC 模式：

STEP 1 | 为 Windows 操作系统启用 FIPS 模式。

要为 GlobalProtect 启用 FIPS-CC 模式，您必须先为 Windows 启用 FIPS 模式，以确保您的 Windows 端点兼容 FIPS 140-2。

1. 启动命令提示符。
2. 输入 **`regedit`** 以打开 Windows 注册表。
3. 在 Windows 注册表中，请转到：`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\`。
4. 右键单击 **Enabled**（已启用）注册表值，然后 **Modify**（修改）。
5. 要启用 FIPS 模式，将 **Value Data**（值数据）设为 **`1`**。默认值 **0** 表示 FIPS 模式已禁用。



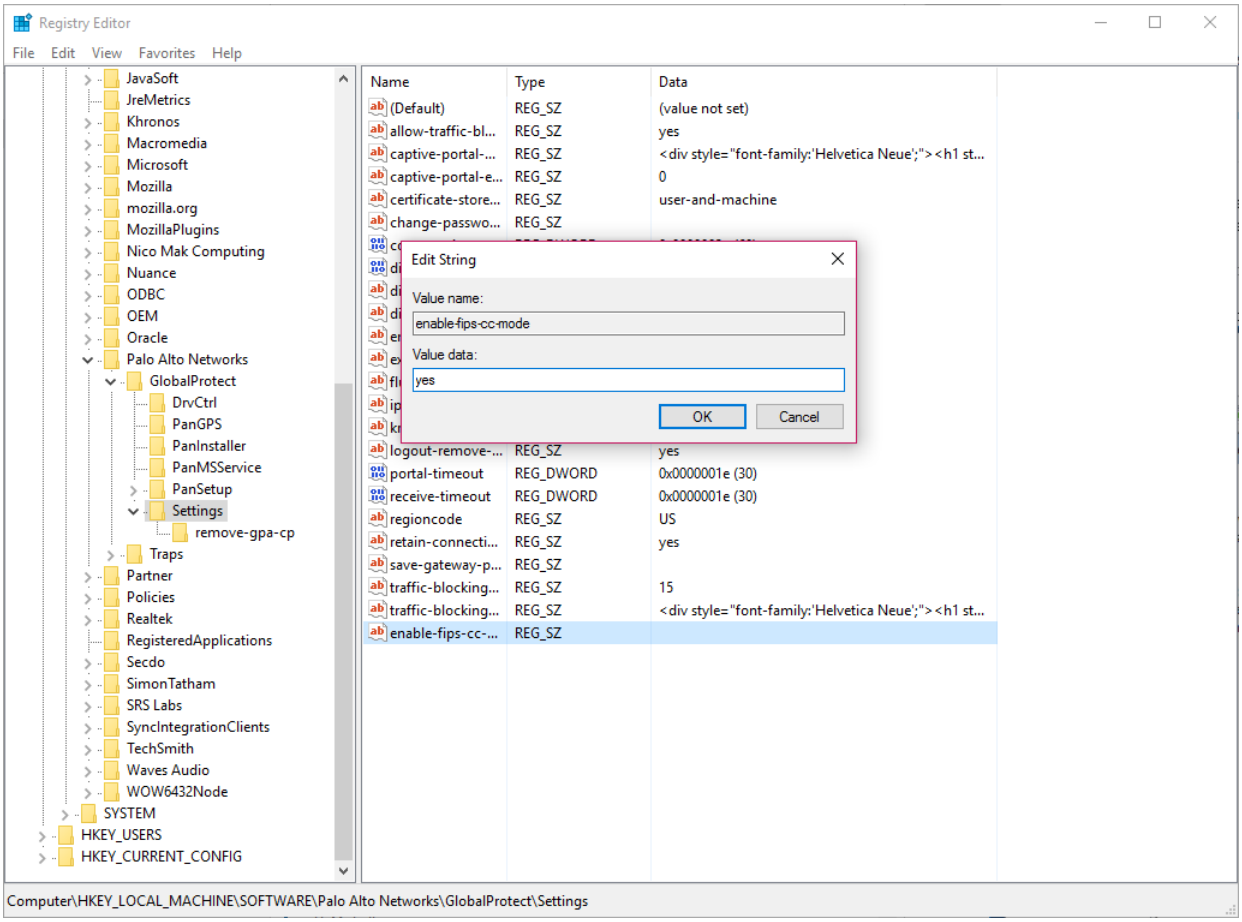
6. 单击 **OK**（确定）。
7. 重新启动您的端点。

STEP 2 | 启用 GlobalProtect 的 FIPS-CC 模式。

© 2019 Palo Alto Networks, Inc.

启用 *FIPS-CC* 模式后您将无法再禁用。要在非 *FIPS-CC* 模式下运行 *GlobalProtect*，最终用户必须先卸载然后重新安装 *GlobalProtect* 应用。这将从 *Windows* 注册表中清除所有 *FIPS-CC* 模式设置。

1. 启动命令提示符。
2. 输入 **`regedit`** 以打开 Windows 注册表。
3. 在 Windows 注册表中，请转到：`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\`。
4. 单击 **Edit**（编辑），然后选择 **New**（新）> **String Value**（字符串值）。
5. 按照提示，将新注册表值的 **Name**（名称）指定为 **`enable-fips-cc-mode`**。
6. 右键单击新注册表值，然后 **Modify**（修改）。
7. 要启用 FIPS-CC 模式，将 **Value Data**（值数据）设为 **`yes`**（是）。
8. 单击 **OK**（确定）。

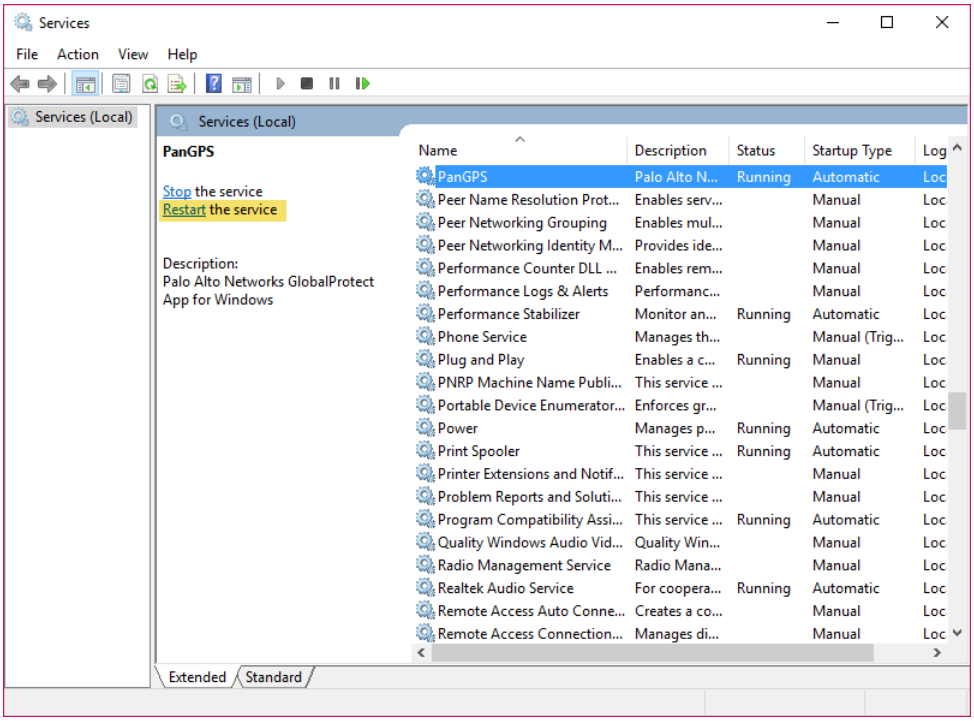


STEP 3 | 重新启动 GlobalProtect。

要启用 GlobalProtect 应用以在 FIPS-CC 模式中初始化，您必须通过以下方法之一重新启动：

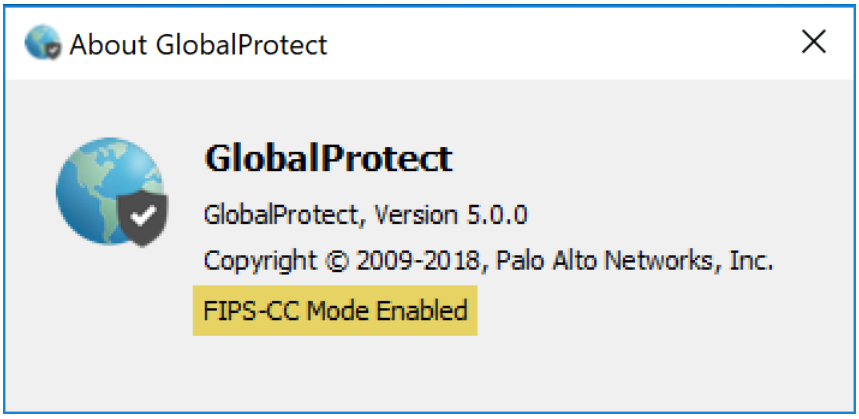
- 重新启动您的端点。
- 重新启动 GlobalProtect 应用程序和 GlobalProtect 服务 (PanGPS)：
  1. 启动命令提示符。
  2. 输入 **`services.msc`** 以打开 Windows 服务管理器。
  3. 从“服务”列表中，选择 **PanGPS**。
  4. **Restart**（重新启动）服务。

© 2019 Palo Alto Networks, Inc.



STEP 4 | 确认已在您的 GlobalProtect 应用上启用 FIPS-CC 模式。

1. 使用 GlobalProtect 应用程序
2. 从状态面板中，打开设置对话框 ( )。
3. 选择 **About**（关于）。
4. 验证 FIPS-CC 模式是否已启用。如果 FIPS-CC 模式已启用，About（关于）对话框会显示 `FIPS-CC Mode Enabled`（`FIPS-CC` 模式启用）状态。



通过 macOS 属性列表启用并验证 FIPS-CC 模式

在 macOS 端点上，使用以下步骤通过 macOS plist（属性列表）以启用并验证 GlobalProtect™ 的 FIPS-CC 模式：

> 要为 *GlobalProtect* 启用 *FIPS-CC* 模式，您的 *macOS* 端点必须兼容 *FIPS 140-2*。默认状态下，*macOS* 操作系统的 *FIPS* 模式在运行 *macOS 10.8* 和更高版本的端点上自动启用。

STEP 1 | 打开 GlobalProtect plist 文件，找到 GlobalProtect 应用程序自定义设置。

© 2019 Palo Alto Networks, Inc.

1. 启动 plist 编辑器，如 Xcode。
2. 在 plist 编辑器中，打开以下 plist 文件：`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`。
3. 找到 GlobalProtect Settings 字典：`/Palo Alto Networks/GlobalProtect/Settings`。

   如果 Settings 词典不存在，创建一个。将每个注册表项作为字符串添加到 Settings 词典。

STEP 2 | 启用 GlobalProtect 的 FIPS-CC 模式。

启用 *FIPS-CC* 后您将无法再禁用。要在非 *FIPS-CC* 模式下运行 *GlobalProtect*，最终用户必须先卸载然后重新安装 *GlobalProtect* 应用。这将从 *macOS plist* 中清除所有 *FIPS-CC* 模式设置。

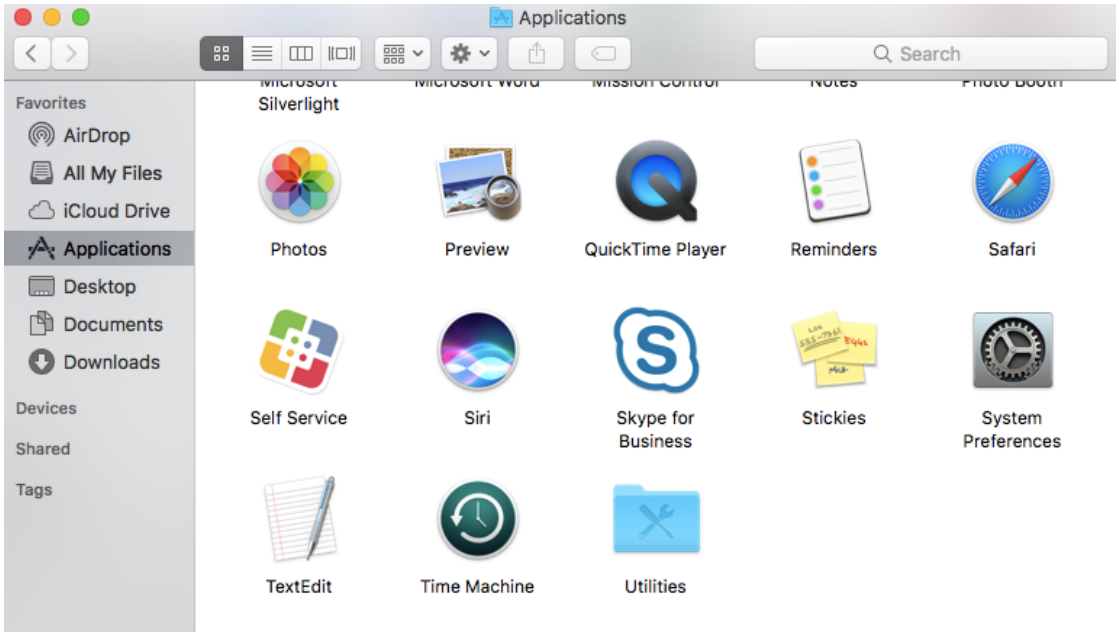
在 Settings 词典中，添加以下键值对以启用 FIPS-CC 模式：

```
<key>enable-fips-cc-mode</key>
<string>yes</string>
```

STEP 3 | 重新启动 GlobalProtect。

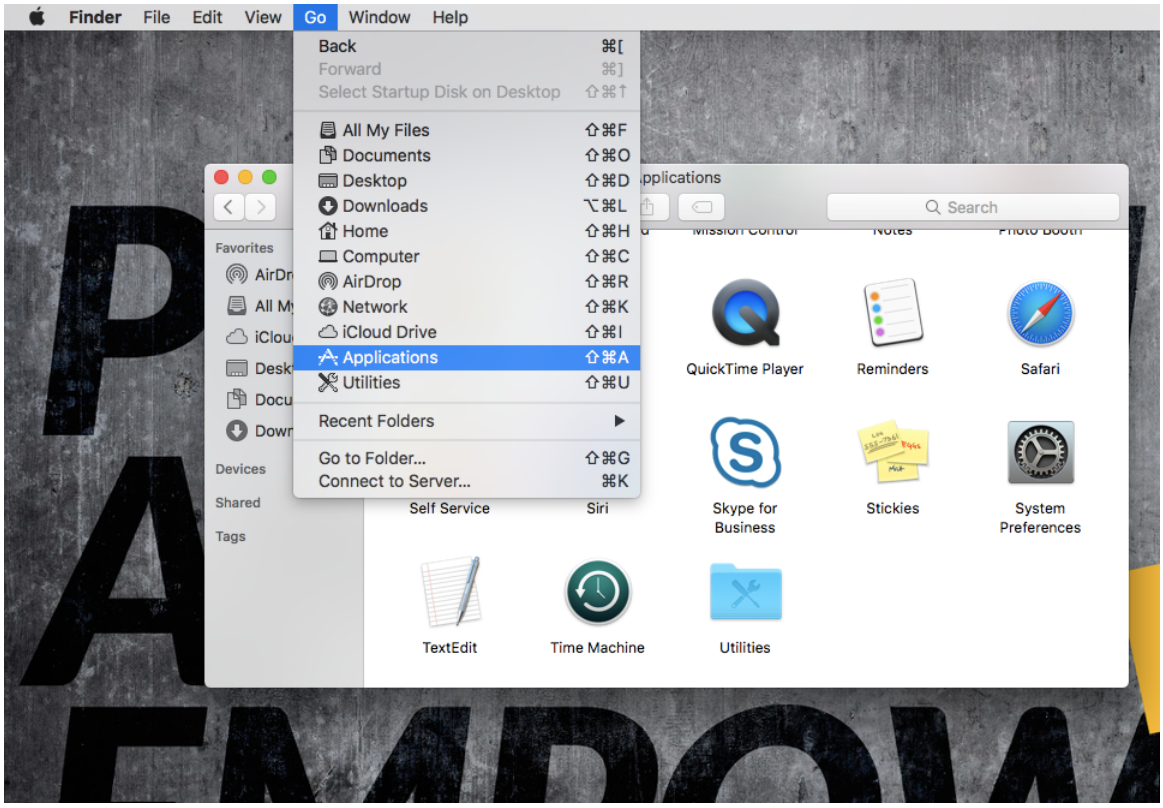
要启用 GlobalProtect 应用以在 FIPS-CC 模式中初始化，您必须通过以下方法之一重新启动：

- 重新启动您的端点。
- 重新启动 GlobalProtect 应用程序和 GlobalProtect 服务 (PanGPS)：
  1. 启动 Finder。
  2. 打开“应用程序”文件夹：
     - 从 Finder 侧边栏中选择 **Applications**（应用程序）。



     - 如果在 Finder 侧边栏中没有看到 **Applications**（应用程序），则从 Finder 菜单栏中选择 **Go**（前往）> **Applications**（应用程序）。

© 2019 Palo Alto Networks, Inc.



要在 *Finder* 侧边栏中显示 *Applications*（应用程序），倾从 *Finder* 菜单栏中选择 *Finder* > *Preferences*（首选项）。从 *Finder*“首选项”中，选择 *Sidebar*（侧边栏），然后启用选项以显示 *Applications*（应用程序）。

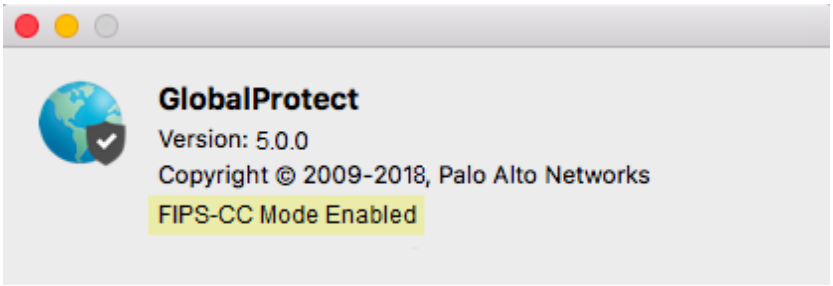
3. 打开“实用程序”文件夹。
4. 启动“终端”。
5. 执行以下命令：

```
username>$ launchctl unload -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangpa.plist
username>$ launchctl unload -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangps.plist
username>$ launchctl load -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangpa.plist
username>$ launchctl load -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangps.plist
```

STEP 4 | 确认已在您的 GlobalProtect 应用上启用 FIPS-CC 模式。

1. 使用 GlobalProtect 应用程序
2. 从状态面板中，打开设置对话框（⚙）。
3. 选择 **About**（关于）。
4. 验证 FIPS-CC 模式是否已启用。如果 FIPS-CC 模式已启用，About（关于）对话框会显示 `FIPS-CC Mode Enabled`（`FIPS-CC` 模式启用）状态。

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

FIPS-CC 安全功能

当您为 GlobalProtect 启用 FIPS-CC 模式时，将在 Windows 和 macOS 端点上为所有 GlobalProtect 应用强制实施以下安全功能：

- 您必须通过 TLS 或 IPSec 加密 GlobalProtect 应用和网关之间的所有 VPN 隧道。
- 当您配置 IPSec VPN 隧道时，您必须选择在 IPSec 设置期间显示的密码套件选项。
- 当您配置 IPSec VPN 隧道时，您可以指定以下加密算法之一：
  - AES-CBC-128（通过 SHA1 身份验证算法）
  - AES-GCM-128
  - AES-GCM-256
- 服务器和客户端证书都必须使用以下签名算法之一：
  - RSA 2048 位（或以上）
  - ECDSA P-256
  - ECDSA P-384
  - ECDSA P-521

  此外，您必须使用 SHA256、SHA384 或 SHA512 的签名散列算法。

© 2019 Palo Alto Networks, Inc.

FIPS-CC 故障排除模式

如果您在启用 FIPS-CC 模式时遇到问题，请参阅以下部分以解决这些问题：

- 查看并收集 GlobalProtect 日志
- 解决 FIPS-CC 模式问题

查看并收集 GlobalProtect 日志

您可以在 GlobalProtect™ 日志中，查看关于 FIPS-CC 问题的更多详细信息。

使用以下步骤查看或收集 GlobalProtect 日志：

STEP 1 | 使用 GlobalProtect 应用程序

STEP 2 | 从状态面板中，打开设置对话框 ( )。

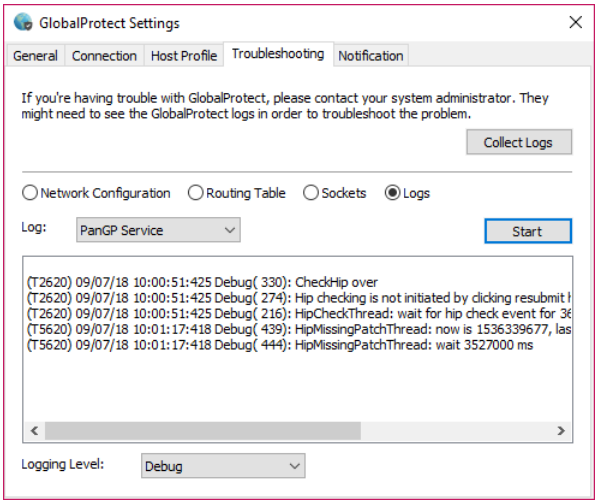
STEP 3 | 选择 **Settings**（设置）。

STEP 4 | 从 GlobalProtect 设置面板中选择 **Troubleshooting**（故障排除）。

STEP 5 | 选择 **Logging Level**（日志记录级别）。

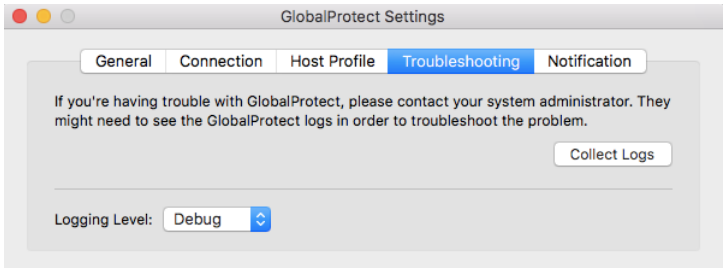
STEP 6 | （可选 — 仅限 Windows）查看您的 GlobalProtect 日志：

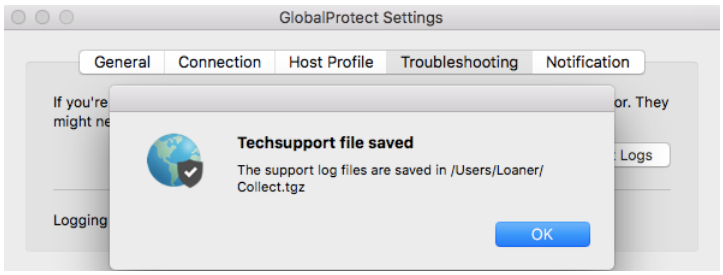
1. 选择 **Logs**（日志）。
2. 选择 **Log**（日志）类型。
3. **Start**（开始）收集日志。



STEP 7 | （可选）**Collect Logs**（收集日志）以发送给您的 GlobalProtect 管理员进行故障排除。

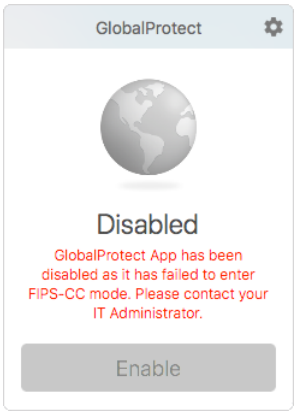
© 2019 Palo Alto Networks, Inc.



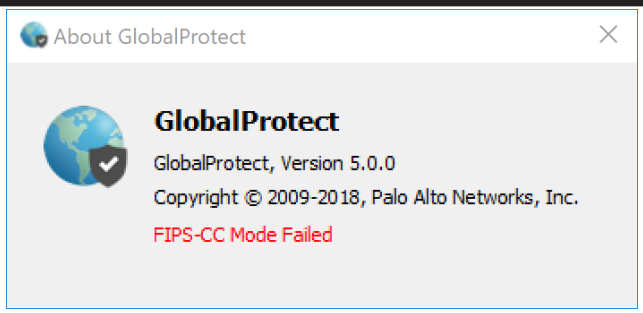


解决 FIPS-CC 模式问题

下表列出了可能的 FIPS-CC 模式问题和相应解决办法。如果您遇到下文中未提到的问题，请联系您的 GlobalProtect™ 管理员获得故障排除协助。

问题	说明	解决办法
由于 FIPS 开机自检或完整性测试失败，GlobalProtect 应用在 FIPS-CC 模式下初始化失败。	启用 FIPS-CC 模式后，在应用初始化和系统或应用重启时，GlobalProtect 应用执行 FIPS 开机自检和完整性测试。如果任一测试失败，GlobalProtect 应用程序将被禁用，且 About（关于）窗口显示 `FIPS-CC Mode Failed`（`FIPS-CC` 模式失效）错误消息： 	重新启动应用以清除错误条件。如果问题继续，卸载并重新安装应用。

© 2019 Palo Alto Networks, Inc.

问题	说明	解决办法
		
由于 FIPS 条件自检失败，GlobalProtect 应用无法在 FIPS-CC 模式下建立连接。	GlobalProtect 应用在 FIPS-CC 模式下初始化后，将执行 FIPS 条件自检。如果自检失败，GlobalProtect 应用将终止会话，并保持断开。	要建立 GlobalProtect 连接，您必须重新向 GlobalProtect 门户验证身份。

如果 *GlobalProtect* 无法在 *FIPS-CC* 模式下初始化或连接，您可以访问 *GlobalProtect* 设置面板的 *Troubleshooting*（故障排除）选项卡，查看并收集日志以便排除故障。*GlobalProtect* 正确连接前，所有其他选项卡不可用。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 快速配置

下列章节提供有关配置部分常见 GlobalProtect™ 部署的分步说明：

> 远程访问 VPN（身份验证配置文件）
> 远程访问 VPN（证书配置文件）
> 带双重身份验证的远程访问 VPN
> 始终打开 VPN 配置
> 使用预登录远程访问 VPN
> GlobalProtect 多网关配置
> 适用于内部 HIP 验证和基于用户的访问的 GlobalProtect
> 内部和外部网关混合配置
> 强制网络门户和对网络访问强制执行 GlobalProtect

有关如何使用 GlobalProtect 更改活动目录密码的信息，请参阅知识库文章：https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGYCA0。

远程访问 VPN（身份验证配置文件）

在适用于远程访问的 GlobalProtect VPN 中，GlobalProtect 门户和网关均配置于 **ethernet1/2** 上，因此该接口为 GlobalProtect 用户连接的物理接口。当用户连接并成功验证至门户和网关后，端点便会通过其虚拟适配器建立隧道，并已在与网关 tunnel.2 配置相关的 IP 池中为其分配 IP 地址（在本例中，即为 10.31.32.3-10.31.32.118）。由于 GlobalProtect VPN 隧道将在单独的 **corp-vpn** 区域内终止，因此便可查看连接流量并为远程用户自定义安全策略。

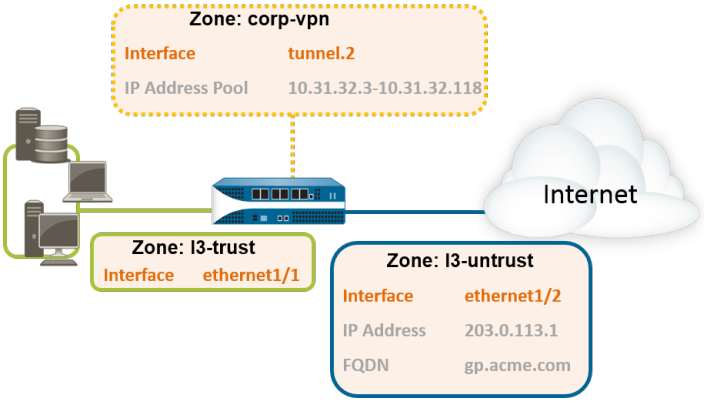


图 **5:** 适用于远程访问的 **GlobalProtect VPN**

STEP 1 | 为 GlobalProtect 创建接口和区域。

为所有接口配置使用 *default*（默认）虚拟路由器以免创建域间路由。

- 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）。将 **ethernet1/2** 配置为 IP 地址为 203.0.113.1 的第三层以太网接口，然后将其分配给 **l3-untrust Security Zone**（安全区域）和默认 **Virtual Router**（虚拟路由器）。
- 创建用于将 IP 地址 **203.0.113.1** 映射至**gp.acme.com** 的 DNS“A”记录。
- 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），然后 **Add**（添加）**tunnel.2**接口。**Add**（添加）隧道接口至名为 **corp-vpn** 的新 **Security Zone**（安全区域），然后将其分配给默认 **Virtual Router**（虚拟路由器）。
- 在 **corp-vpn** 区域内启用“用户标识”。

STEP 2 | 创建安全策略以在 **corp-vpn** 区域和 **l3-trust** 区域之间启用流量，以便访问内部资源。

1. 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）新规则。
2. 在本例中，您可以使用以下设置定义规则：
   - **Name**（名称）（**General**（常规）选项卡）— VPN 访问
   - **Source Zone**（源区域）（**Source**（源）选项卡）— corp-vpn
   - **Destination Zone**（目标区域）（**Destination**（目标）选项卡）—l3-trust

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 3 | 使用下列方法之一为承载 GlobalProtect 门户和网关的接口获取服务器证书：

- （建议）导入来自众所周知的第三方 CA 的服务器证书。

© 2019 Palo Alto Networks, Inc.

- 使用门户中的根 CA 生成自签名服务器证书。

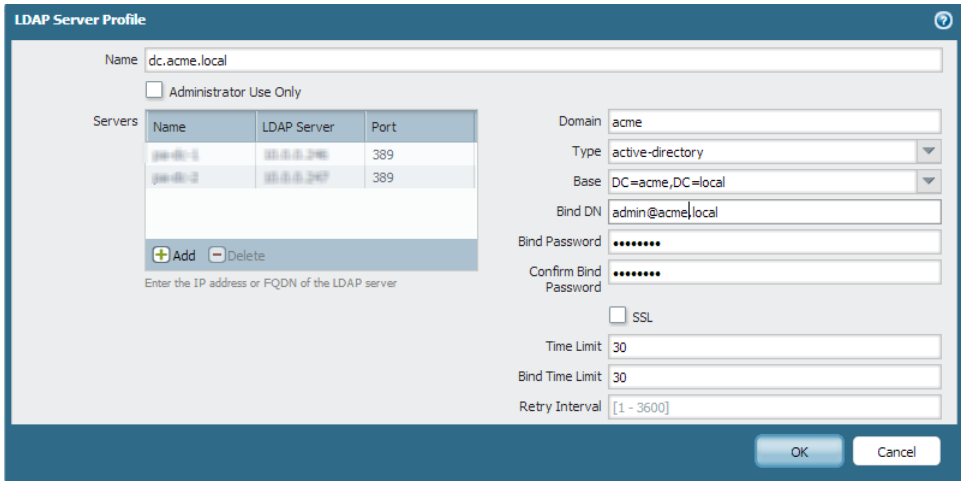
选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）以按下列方法管理证书：

- 获取服务器证书。由于门户和网关位于同一接口，因此这两个组件可共用同一服务器证书。
- 证书的公用名 (CN) 必须与 FQDN `gp.acme.com` 相符。
- 要使用户连接至门户而不收到证书错误，请使用来自公共 CA 的服务器证书。

STEP 4 | 创建服务器配置文件。

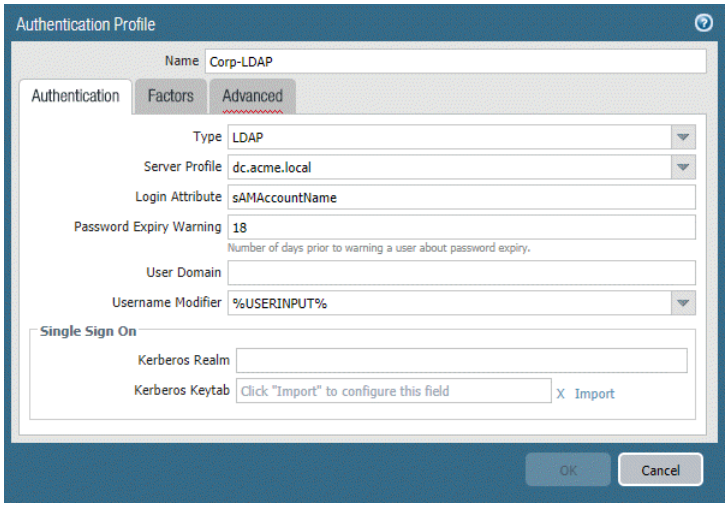
服务器配置文件将指导防火墙如何连接至身份验证服务。支持本地、RADIUS、SAML、Kerberos 和 LDAP 身份验证方法。本示例介绍针对 Active Directory 对用户进行身份验证的 LDAP 身份验证配置文件。

创建用于连接至 LDAP 服务器的服务器配置文件（**Device**（设备）> **Server Profiles**（服务器配置文件）> **LDAP**）。



STEP 5 |（可选）创建身份验证配置文件。

将服务器配置文件附加到身份验证配置文件（**Device**（设备）> **Authentication Profile**（身份验证配置文件））。



STEP 6 | 配置 GlobalProtect 网关。

© 2019 Palo Alto Networks, Inc.

选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关），然后**Add**（添加）下列配置：

Interface（接口）— `ethernet1/2`

IP 地址 — `203.0.113.1`

Server Certificate（服务器证书）— `GoDaddy` 颁发的 `GP-server-cert.pem`

Authentication Profile（身份验证配置文件）— `Corp-LDAP`

Tunnel Interface（隧道接口）— `tunnel.2`

IP Pool（IP 池）— `10.31.32.3 - 10.31.32.118`

STEP 7 | 配置 GlobalProtect 门户。

选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户），然后**Add**（添加）下列配置：

1. 设置 GlobalProtect 门户访问权限：

   Interface（接口）— `ethernet1/2`

   IP 地址 — `203.0.113.1`

   Server Certificate（服务器证书）— `GoDaddy` 颁发的 `GP-server-cert.pem`

   Authentication Profile（身份验证配置文件）— `Corp-LDAP`
2. 定义 GlobalProtect 客户端身份验证配置：

   Connect Method（连接方法）— `On-demand`（用户手动启动的连接）

   External Gateway Address（外部网关地址）— `gp.acme.com`

STEP 8 | 部署 GlobalProtect 应用程序软件。

选择 **Device**（设备）> **GlobalProtect Client**（**GlobalProtect** 客户端）。遵循在门户上载入应用更新的步骤。

STEP 9 | （可选）启用对 GlobalProtect 移动应用的使用。

购买并安装 GlobalProtect 订阅（**Device**（设备）> **Licenses**（许可证））以启用该应用。

STEP 10 | 保存 GlobalProtect 配置。

单击 **Commit**（提交）。

© 2019 Palo Alto Networks, Inc.

远程访问 VPN（证书配置文件）

采用证书身份验证时，用户须提供能够识别其连接至 GlobalProtect 门户或网关的有效客户端证书。若要验证客户端证书是否有效，门户或网关将通过使用 SSL 握手期间交换的证书验证消息，检查客户端是否拥有证书私钥。此外，客户端证书将通过证书链**Issuer**（颁发机构）字段指定的证书颁发机构 (CA) 签名。除了证书本身之外，门户或网关还可使用证书配置文件来确定发送证书的用户是否为向其签发证书的用户。

当客户端证书为唯一身份验证方法时，用户提供的证书须在某一证书字段中包含用户名。通常，该用户名对应于证书“主题”字段中的公用名 (CN)。

身份验证成功后，GlobalProtect 应用将与网关建立隧道，并从采用该网关的隧道配置的 IP 池中为其分配 IP 地址。要对 **corp-vpn** 域中的会话启用基于用户的策略强制，须将证书中的用户名映射至网关分配的 IP 地址。如果安全策略要求使用域名加用户名，则须将证书配置文件中指定的域值附加到用户名。

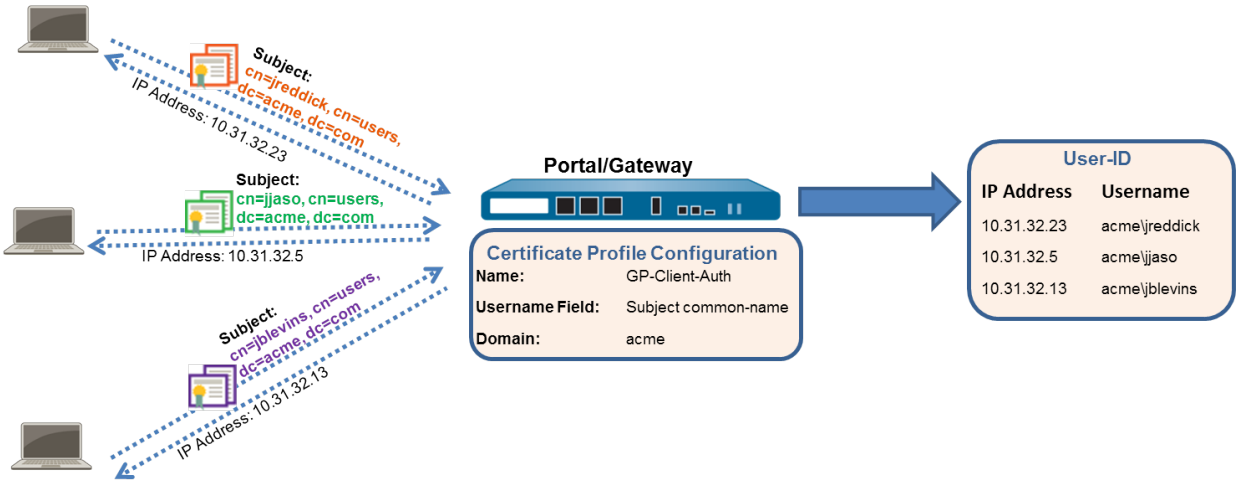


图 **6: GlobalProtect** 客户端证书身份验证配置

该快速配置使用与用于远程访问的 GlobalProtect VPN 相同的拓扑结构。两者间的唯一配置差别在于不针对外部身份验证服务器对用户进行验证，而仅使用客户端证书身份验证。

STEP 1 | 为 GlobalProtect 创建接口和区域。

为所有接口配置使用 *default*（默认）虚拟路由器以免创建域间路由。

- 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）。将 **ethernet1/2** 配置为 IP 地址为 **203.0.113.1** 的第三层以太网接口，然后将其分配给 **l3-untrust Security Zone**（安全区域）和默认 **Virtual Router**（虚拟路由器）。
- 创建用于将 IP 地址 **203.0.113.1** 映射至**gp.acme.com** 的 DNS“A”记录。

© 2019 Palo Alto Networks, Inc.

- 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），然后 **Add**（添加）**tunnel.2**接口。添加隧道接口至名为 `corp-vpn` 的新 **Security Zone**（安全区域），然后将其分配给默认 **Virtual Router**（虚拟路由器）。
- 在 **`corp-vpn`** 区域内启用“用户标识”。

STEP 2 | 创建安全策略以在 **`corp-vpn`** 区域和 **`l3-trust`** 区域之间启用流量，以便访问内部资源。

1. 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）新规则。
2. 在本例中，您可以使用以下设置定义规则：
   - **Name**（名称）（**General**（常规）选项卡）— **`VPN Access`**
   - **Source Zone**（源区域）（**Source**（源）选项卡）— **`corp-vpn`**
   - **Destination Zone**（目标区域）（**Destination**（目标）选项卡）— **`l3-trust`**

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 3 | 使用下列方法之一为承载 GlobalProtect 门户和网关的接口获取服务器证书：

- （建议）导入来自众所周知的第三方 CA 的服务器证书。
- 使用门户中的根 CA 生成自签名服务器证书。

选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）以按下列方法管理证书：

- 获取服务器证书。由于门户和网关位于同一接口，因此这两个组件可共用同一服务器证书。
- 证书的公用名 (CN) 必须与 FQDN `gp.acme.com` 相符。
- 要使用户连接至门户而不收到证书错误，请使用来自公共 CA 的服务器证书。

STEP 4 | 向 GlobalProtect 客户端和端点颁发客户端证书。

1. 使用企业 PKI 或公共 CA 向所有 GlobalProtect 用户颁发唯一客户端证书。
2. 在端点的个人证书存储库中安装证书。

STEP 5 | 创建客户端证书配置文件。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。**Add**（添加）新的证书配置文件，然后输入配置文件 **Name**（名称），例如 **`GP-client-cert`**。
2. 从 **Username Field**（用户名字段）下拉列表中选择 **Subject**（主题）。
3. **CA Certificates**（**CA** 证书）区域，**Add**（添加）已发行客户端证书的 CA 证书。双击 **OK**（确定）。

STEP 6 | 配置 GlobalProtect 网关。

请参阅用于远程访问的 GlobalProtect VPN 中显示的拓扑图。

选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关），然后**Add**（添加）下列配置：

Interface（接口）— **`ethernet1/2`**

IP 地址 — **`203.0.113.1`**

Server Certificate（服务器证书）— **`GoDaddy`** 颁发的 **`GP-server-cert.pem`**

Certificate Profile（证书配置文件）— **`GP-client-cert`**

Tunnel Interface（隧道接口）— **`tunnel.2`**

IP Pool（**IP** 池）— **`10.31.32.3 - 10.31.32.118`**

© 2019 Palo Alto Networks, Inc.

STEP 7 | 配置 GlobalProtect 门户。

选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户），然后**Add**（添加）下列配置：

1. 设置 GlobalProtect 门户访问权限：

   Interface（接口）— `ethernet1/2`

   IP 地址 — `203.0.113.1`

   Server Certificate（服务器证书）— `GoDaddy` 颁发的 `GP-server-cert.pem`

   Certificate Profile（证书配置文件）— `GP-client-cert`
2. 定义 GlobalProtect 代理配置：

   Connect Method（连接方法）— `On-demand`（用户手动启动的连接）

   External Gateway Address（外部网关地址）— `gp.acme.com`

STEP 8 | 部署 GlobalProtect 应用程序软件。

选择 **Device**（设备）> **GlobalProtect Client**（**GlobalProtect** 客户端）。遵循在门户上载入应用更新的步骤。

STEP 9 | （可选）启用对 GlobalProtect 移动应用的使用。

购买并安装 GlobalProtect 订阅（**Device**（设备）> **Licenses**（许可证））以启用该应用。

STEP 10 | 保存 GlobalProtect 配置。

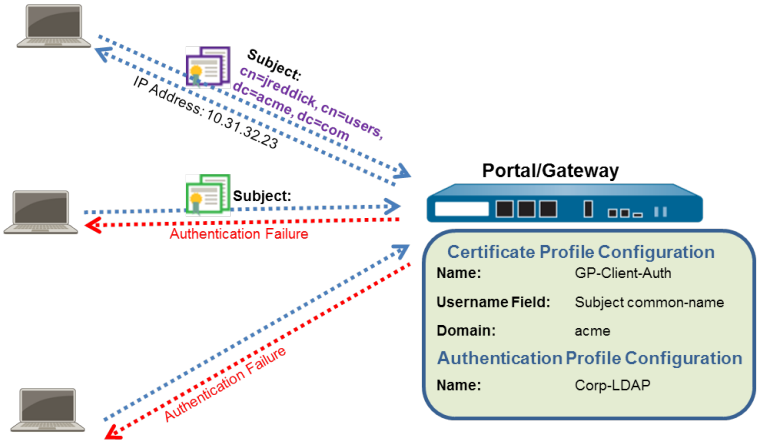
单击 **Commit**（提交）。

© 2019 Palo Alto Networks, Inc.

带双重身份验证的远程访问 VPN

如果为 GlobalProtect 门户或网关配置了身份验证配置文件和证书配置文件（二者组合可提供双重身份验证），最终用户必须在获取访问权限之前成功通过采用这两种配置文件的身份验证。对于门户身份验证，即表示须在端点建立初始门户连接前为其预部署证书。此外，用户提供的证书须与证书配置文件中的定义相符。

- 如果证书配置文件未指定用户名字段（**Username Field**（用户名字段）被设为 **None**（无）），则客户端证书无需包含用户名。在此情况下，用户须在针对身份验证配置文件进行验证时提供用户名。
- 如果证书配置文件指定了用户名，则用户提供的证书须在对应字段中包含用户名。例如，如果证书配置文件指定用户名字段为 **Subject**（主题），则用户提供的证书须在公用名字段中包含值，否则身份验证将失败。此外，当用户名字段为必需项时，证书用户名字段中的值将被自动填充为用户尝试输入凭据以验证至身份验证配置文件时的用户名。如果不想强制用户通过证书中的用户名进行身份验证，则请勿在证书配置文件中指定用户名字段。



该快速配置使用与用于远程访问的 GlobalProtect VPN 相同的拓扑结构。但采用此配置时，用户须针对证书配置文件和身份验证配置文件进行验证。有关特定类型的双重身份验证的更多详细信息，请参阅下列主题：

- 使用证书和身份验证配置文件启用双重身份验证
- 使用一次性密码 (OTP) 启用双重身份验证
- 使用智能卡启用双重身份验证
- 使用软件令牌应用程序启用双因素身份验证

根据以下步骤配置带双重身份验证的远程 VPN 访问。

STEP 1 | 为 GlobalProtect 创建接口和区域。

为所有接口配置使用 *default*（默认）虚拟路由器以免创建域间路由。

- 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）。将 **ethernet1/2** 配置为 IP 地址为 `203.0.113.1` 的 **Layer3**（第三层）以太网接口，然后将其分配给 `l3-untrust` **Security Zone**（安全区域）和默认 **Virtual Router**（虚拟路由器）。
- 创建用于将 IP 地址 `203.0.113.1` 映射至`gp.acme.com` 的 DNS“A”记录。
- 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），然后 **Add**（添加）**tunnel.2**接口。添加隧道接口至名为 `corp-vpn` 的新 **Security Zone**（安全区域），然后将其分配给默认 **Virtual Router**（虚拟路由器）。
- 在 `corp-vpn` 区域内启用“用户标识”。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 创建安全策略以在 `corp-vpn` 区域和 `l3-trust` 区域之间启用流量，以便访问内部资源。

1. 选择 **Policies**（策略）> **Security**（安全），然后单击 **Add**（添加）以创建新规则。
2. 在本例中，您可以使用以下设置定义规则：
   - **Name**（名称）（**General**（常规）选项卡）— `VPN Access`
   - **Source Zone**（源区域）（**Source**（源）选项卡）— `corp-vpn`
   - **Destination Zone**（目标区域）（**Destination**（目标）选项卡）— `l3-trust`

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 3 | 使用下列方法之一为承载 GlobalProtect 门户和网关的接口获取服务器证书：

- （建议）导入来自众所周知的第三方 CA 的服务器证书。
- 使用门户中的根 CA 生成自签名服务器证书。

选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）以按下列方法管理证书：

- 获取服务器证书。由于门户和网关位于同一接口，因此这两个组件可共用同一服务器证书。
- 证书的公用名 (CN) 必须与 FQDN `gp.acme.com` 相符。
- 要使用户连接至门户而不收到证书错误，请使用来自公共 CA 的服务器证书。

STEP 4 | 向 GlobalProtect 客户端和端点颁发客户端证书。

1. 使用企业 PKI 或公共 CA 向所有 GlobalProtect 用户颁发唯一客户端证书。
2. 在端点的个人证书存储库中安装证书。

STEP 5 | 创建客户端证书配置文件。

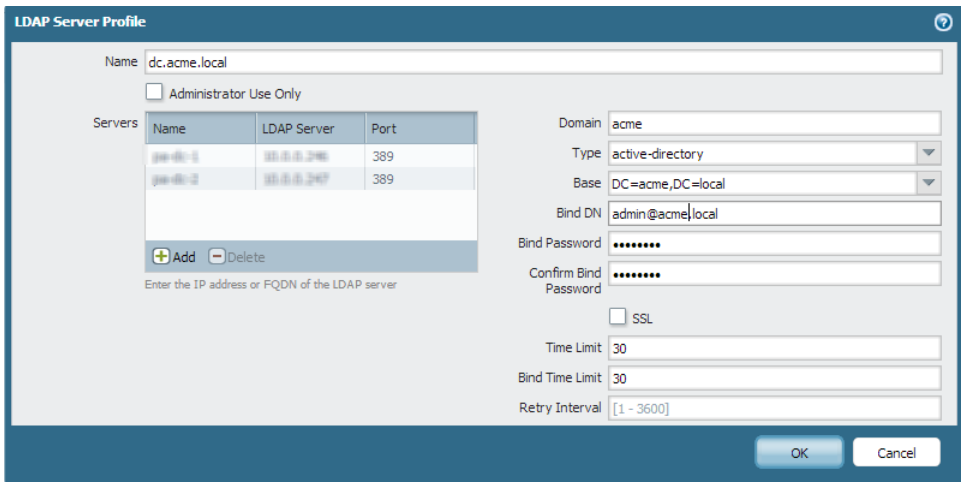
1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。**Add**（添加）新的证书配置文件，然后输入配置文件 **Name**（名称），例如 `GP-client-cert`。
2. 指定在何处获取用于验证最终用户的用户名：
   - 从用户 — 如果想要最终用户在验证至身份验证配置文件中指定的服务时提供用户名，则请选择无作为用户名字段。
   - 从证书 — 如果要从证书中提取用户名，请选择主题作为用户名字段。如果采用此选项，则当提示用户登录到门户或网关时，证书中包含的 CN 将自动填充用户名字段。用户需要使用该用户名登录。
3. **CA Certificates**（**CA** 证书）区域，**Add**（添加）已发行客户端证书的 CA 证书。双击 **OK**（确定）。

STEP 6 | 创建服务器配置文件。

服务器配置文件将指导防火墙如何连接至身份验证服务。支持本地、RADIUS、SAML、Kerberos 和 LDAP 身份验证方法。本示例介绍针对 Active Directory 对用户进行身份验证的 LDAP 身份验证配置文件。

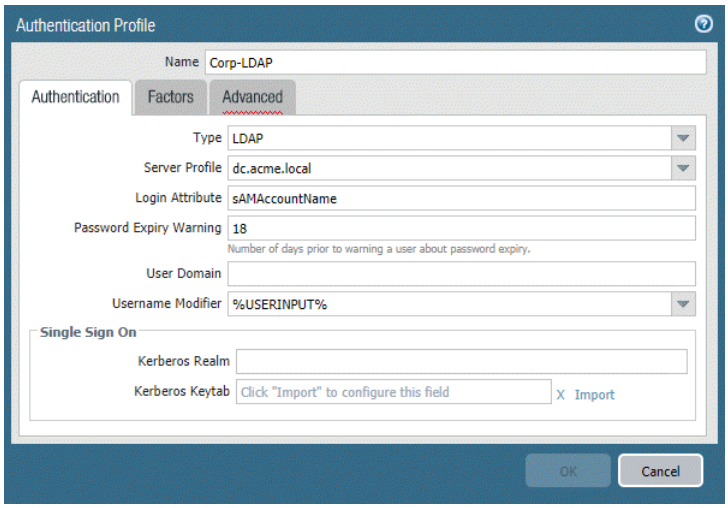
创建用于连接至 LDAP 服务器的服务器配置文件（**Device**（设备）> **Server Profiles**（服务器配置文件）> **LDAP**）。

© 2019 Palo Alto Networks, Inc.



STEP 7 | （可选）创建身份验证配置文件。

将服务器配置文件附加到身份验证配置文件（**Device**（设备）**Authentication Profile**（身份验证配置文件））。



STEP 8 | 配置 GlobalProtect 网关。

请参阅用于远程访问的 GlobalProtect VPN 中显示的拓扑图。

选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关），然后**Add**（添加）下列配置：

Interface（接口）— `ethernet1/2`

IP 地址 — `203.0.113.1`

Server Certificate（服务器证书）— `GoDaddy` 颁发的 `GP-server-cert.pem`

Certificate Profile（证书配置文件）— `GP-client-cert`

Authentication Profile（身份验证配置文件）— `Corp-LDAP`

Tunnel Interface（隧道接口）— `tunnel.2`

IP Pool（**IP** 池）— `10.31.32.3 - 10.31.32.118`

STEP 9 | 配置 GlobalProtect 门户。

© 2019 Palo Alto Networks, Inc.

选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户），然后**Add**（添加）下列配置：

1. 设置 GlobalProtect 门户访问权限：

   Interface（接口）— `ethernet1/2`

   IP 地址 — `203.0.113.1`

   Server Certificate（服务器证书）— `GoDaddy` 颁发的 `GP-server-cert.pem`

   Certificate Profile（证书配置文件）— `GP-client-cert`

   Authentication Profile（身份验证配置文件）— `Corp-LDAP`
2. 定义 GlobalProtect 代理配置：

   Connect Method（连接方法）— `On-demand`（用户手动启动的连接）

   External Gateway Address（外部网关地址）— `gp.acme.com`

STEP 10 | 部署 GlobalProtect 应用程序软件。

选择 **Device**（设备）> **GlobalProtect Client**（**GlobalProtect** 客户端）。遵循在门户上载入应用更新的步骤。

STEP 11 | （可选）以透明方式部署应用设置。

作为从门户配置部署应用设置的备用方法，可直接从 Windows 注册表或全局 macOS plist 定义设置。可部署的设置包括指定门户 IP 地址，或者让 GlobalProtect 在用户登录端点并连接 GlobalProtect 门户前发起 VPN 隧道。还可使用 MSIEXEC 安装程序配置设置，这仅限 Windows 端点。更多信息，请参阅自定义应用设置。

STEP 12 | （可选）启用对 GlobalProtect 移动应用的使用。

购买并安装 GlobalProtect 订阅（**Device**（设备）> **Licenses**（许可证））以启用该应用。

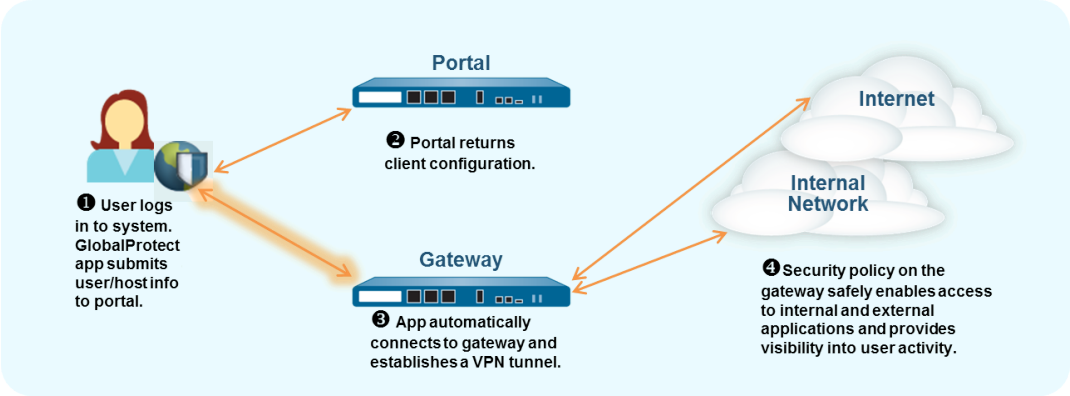
STEP 13 | 保存 GlobalProtect 配置。

单击 **Commit**（提交）。

© 2019 Palo Alto Networks, Inc.

始终打开 VPN 配置

采用“始终打开”GlobalProtect 配置时，应用程序在用户登录时将连接至 GlobalProtect 门户以提交用户和主机信息并接收客户端配置。应用程序随后将自动连接并建立一条 VPN 隧道，其连接到门户提供的客户端配置指定网关，如下图所示：



要将下列远程访问 VPN 配置之一切换至“始终打开”配置，您可以更改连接方法：

- 远程访问 VPN（身份验证配置文件）
- 远程访问 VPN（证书配置文件）
- 带双重身份验证的远程访问 VPN

按照下列步骤将远程访问 VPN 配置切换至“始终启用”配置。

STEP 1 | 选择 **Network**（网络）> **GlobalProtect** > **Portal**（门户），然后选择门户配置。

STEP 2 | 选择要修改的代理配置中的 **Agent**（代理）选项卡。

STEP 3 | 选择 **App**（应用程序），然后设置 **Connect Method**（连接方法）为 **User-logon (Always On)**（用户登录（始终启用））。

STEP 4 | 单击 **OK**（确定）以保存代理配置。

STEP 5 | 针对要修改的每个代理配置，请重复步骤 2-4。

STEP 6 | 单击**OK**（确定）以保存门户配置，然后**Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

使用预登录远程访问 VPN

Pre-logon（预登录）是在用户登录之前建立 VPN 隧道的一种连接方法。预登录的目的是对端点（而非用户）进行身份验证，进而使域脚本和所选择的其他任务能够在端点启动时立即运行。机器证书使端点能够建立至 GlobalProtect 网关的 VPN 隧道。IT 管理员的一般做法是在划分用户端点时安装机器证书。

由于用户尚未登录，所以预登录 VPN 隧道不存在用户名关联。要让端点可访问信任区域的资源，必须创建与预登录用户匹配的安全策略。此类策略应仅允许访问启动系统所需的基础服务，例如 DHCP、DNS、Active Directory（如要更改过期的密码）、抗病毒软件或操作系统更新服务。在网关对用户进行身份验证之后，GlobalProtect 应用将 VPN 隧道被重新分配给该用户（防火墙上的 IP 地址映射从预登录端点更改为经认证用户）。

适用于 Windows 7 和 Windows 10 端点的 GlobalProtect 凭据提供程序登录屏幕还会在用户登录之前显示登录前连接状态，允许最终用户确定其是否可以在登录时访问网络资源。如果 GlobalProtect 应用将端点作为内部进行检查，则登录屏幕将显示 内部登录前连接状态。如果 Globalprotect 应用将端点作为外部进行检查，则登录屏幕将显示 已连接或 未连接登录前连接状态。

Windows 端点与具有预登录功能的 *macOS* 端点的行为不同。对于 *macOS* 操作系统，当用户登录时，为预登录创建的隧道断开，转而创建新隧道。

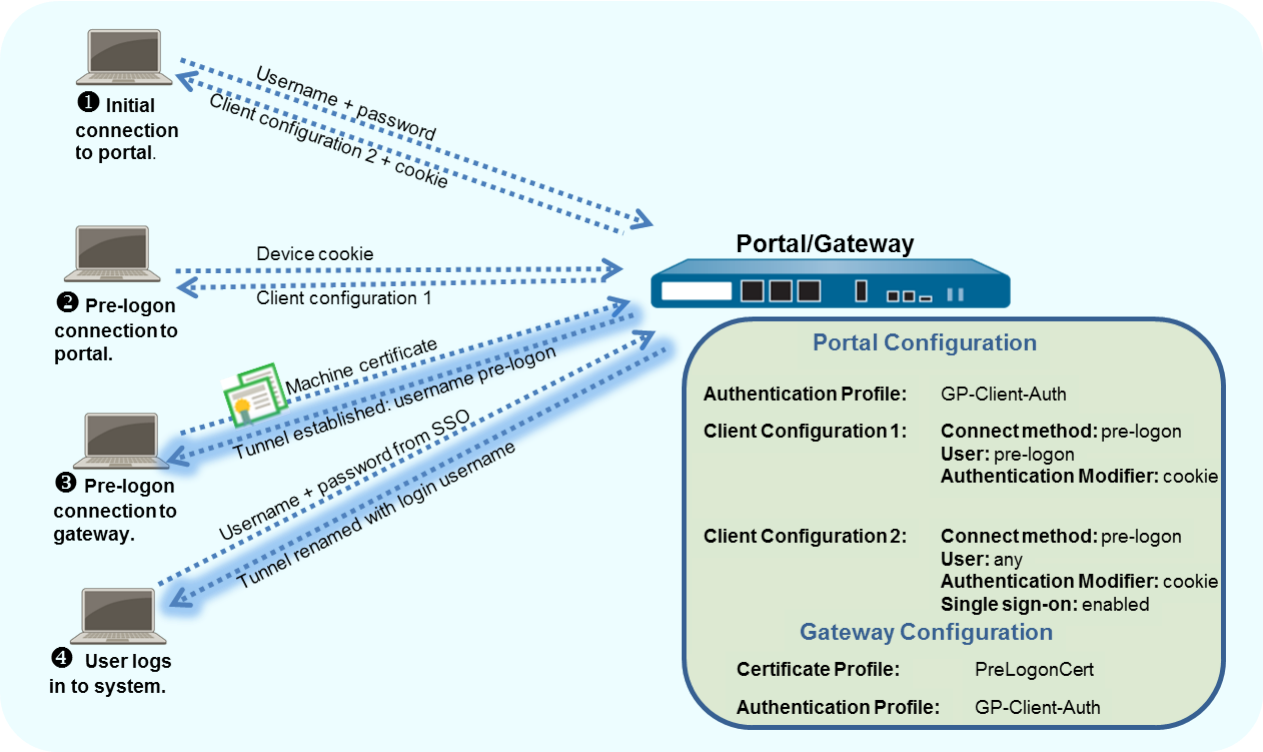
当用户请求建立新连接时，门户使用身份验证配置文件对用户进行身份验证。门户还可使用对客户端证书进行验证的可选证书配置文件（如果其配置包含客户端证书）。在此情况下，证书必须识别用户。执行身份验证后，门户确定端点的 GlobalProtect 配置是否最新的。如果门户的配置改变，则将更新的配置推送至端点。

如果门户或网关配置包含基于 Cookie 的身份验证，则门户或网关在端点安装加密 Cookie。之后，门户或网关使用该 Cookie 验证用户和刷新代理配置。如果代理配置文件包含结合 Cookie 身份验证的预登录连接方法，GlobalProtect 组件可使用 Cookie 进行预登录。

如果用户从未登录端点（例如无外设端点），或者用户以前未登录的系统需要预登录连接，您可以允许端点发起一个预登录隧道，而无需先连接到门户以下载预登录配置。为此，您必须在 Windows 注册表或 macOS plist 中创建一些表项来覆盖此默认行为。

然后，GlobalProtect 端点将连接至配置中指定的门户，并使用其机器证书对端点进行身份验证（如网关上所配置证书配置文件中指定的）和建立 GlobalProtect 连接。随后，当最终用户登录至机器时，如果在代理配置中启用了单点登录 (SSO)，则在用户登录时将捕获用户名和密码。如果在代理配置中未启用 SSO，或是端点不支持 SSO（例如，macOS 系统），用户凭据必须保存在应用中（**Save User Credentials**（保存用户凭据）选项必须设置为 **Yes**（是））。在对网关进行身份验证成功后，可以重命名隧道 (Windows) 或重建 (macOS)，以及执行基于用户和组的策略。

© 2019 Palo Alto Networks, Inc.



这个例子使用的是用于远程访问的 GlobalProtect VPN 中所述的 GlobalProtect 拓扑结构。

STEP 1 | 为 GlobalProtect 创建接口和区域。

为所有接口配置使用 *default*（默认）虚拟路由器以免创建域间路由。

- 例如，选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）选项卡，然后配置以下设置：
  1. 选择 **ethernet1/2**。
  2. 从 **Interface Type**（接口类型）下列列表中选择 **Layer 3**（第 3 层）。
  3. 在 **Config**（配置）选项卡上，**Assign interface to**（分配接口至）默认 **Virtual Router**（虚拟路由器）和 **`13-untrust`** **Security Zone**（安全区域）。
  4. 在 **IPv4** 选项卡上，单击 **Add**（添加）以选择 IP 地址 **`203.0.113.1`**（或映射至 **`203.0.113.1`** 的对象）或添加 **New Address**（新地址）来创建新对象和地址映射（地址类型保留为 **Static**（静态））。例如，创建用于将 IP 地址 **`203.0.113.1`** 映射至 **`gp.acme.com`** 的 DNS“A”记录。
- 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道）并 **Add**（添加）新隧道接口。
  1. 对于 **Interface Name**（接口名称），请输入 **`tunnel.2`**。
  2. 在 **Config**（配置）选项卡上，**Assign interface to**（分配接口至）名为 **`corp-vpn`** 的新 **Security Zone**（安全区域）和默认 **Virtual Router**（虚拟路由器）。
- 在 **`corp-vpn`** 区域内启用“用户标识”。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 创建安全策略规则。

此配置需要以下策略（**Policies**（策略）> **Security**（安全））：

1. **Add**（添加）可让预登录用户访问启动端点所需基础服务（例如身份验证服务、DNS、DHCP 和 Microsoft 更新）的规则。
2. **Add**（添加）一个规则来拒绝预登录用户访问所有其他目的地和应用程序。
3. **Add**（添加）任何其他规则来使不同的用户或用户组能够访问特定的目标和应用程序。按照最佳实践互联网网关安全策略建议创建这些规则。

STEP 3 | 使用下列方法之一为承载 GlobalProtect 门户和网关的接口获取服务器证书：

- （建议）导入来自众所周知的第三方 CA 的服务器证书。
- 使用门户中的根 CA 生成自签名服务器证书。

选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）以按下列标准管理证书：

- 获取服务器证书。由于门户和网关位于同一接口，因此这两个组件可共用同一服务器证书。
- 证书的公用名 (CN) 必须与 FQDN `gp.acme.com` 相符。
- 要使端点连接至门户而不收到证书错误，请使用来自公共 CA 的服务器证书。

STEP 4 | 为所有连接至 GlobalProtect 的端点生成机器证书，然后将其导入至每个机器的个人证书存储库中。

尽管可为所有端点生成自签名证书，但最佳做法是使用个人的公钥基础结构 (PKI) 向端点颁发和分发证书。

1. 向 GlobalProtect 客户端和端点颁发客户端证书。
2. 在端点的个人证书存储库中安装证书。（Windows 端点上的本地计算机存储库或 macOS 端点上的系统密钥链）

STEP 5 | 从已颁布机器证书的 CA 中将可信根 CA 证书导入至门户和网关上：

无需导入私钥。

1. 下载 Base64 格式的 CA 证书。
2. 按下列步骤将证书导入至承载门户或网关的所有防火墙上：
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后 **Import**（导入）证书。
   2. 输入 **Certificate Name**（证书名称），该名称可将证书标识为您的客户端 CA 证书。
   3. **Browse**（浏览）到从 CA 下载的 **Certificate File**（证书文件）。
   4. 将 **File Format**（文件格式）设置为**Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**）。
   5. 单击 **OK**（确定）以保存您的证书。
   6. 在 **Device Certificates**（设备证书）选项卡上，选择要刚导入的证书。
   7. 选择 **Trusted Root CA**（可信根 **CA**）复选框，然后单击 **OK**（确定）。

STEP 6 | 在每个承载 GlobalProtect 网关的防火墙上，创建证书配置文件以标识用于验证机器证书的 CA 证书。

如果您计划在用户登录系统时使用客户端证书身份验证对用户进行身份验证，且颁发客户端证书的 CA 证书与已颁发机器证书的 CA 证书不同，请务必在证书配置文件中同时引用这两个证书。

© 2019 Palo Alto Networks, Inc.

1. 选择 **Device**（设备）> **Certificates**（证书）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），并 **Add**（添加）新的证书配置文件。
2. 输入 **Name**（名称）以标识配置文件，例如 `PreLogonCert`。
3. 将 **Username Field**（用户名字段）设置为 **None**（无）。
4. （可选）如果还使用客户端证书在用户登录时对其进行身份验证，且颁发客户端证书的 CA 证书与颁发机器证书的 CA 证书不同，则还应添加前一种证书。
5. 在 **CA Certificates**（**CA** 证书）字段，**Add**（添加）CA 证书。
6. 选择在步骤 5 导入的可信根 **CA Certificate**（**CA** 证书），然后单击 **OK**（确定）。
7. 单击 **OK**（确定）保存配置文件。

STEP 7 | 配置 GlobalProtect 网关。

请参阅用于远程访问的 GlobalProtect VPN 中显示的拓扑图。

虽然须为预登录访问网关创建证书配置文件，但可以为已登录用户使用客户端证书身份验证或基于身份验证配置文件的验证。在本示例中，所用的 LDAP 配置文件为用于将用户验证至门户的同一配置文件。

1. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关），然后 **Add**（添加）下列网关配置：

   Interface（接口）— `ethernet1/2`

   IP 地址 — `203.0.113.1`

   Server Certificate（服务器证书）— `GoDaddy` 颁发的 `GP-server-cert.pem`

   Certificate Profile（证书配置文件）— `PreLogonCert`

   Authentication Profile（身份验证配置文件）— `Corp-LDAP`

   Tunnel Interface（隧道接口）— `tunnel.2`

   IP Pool（**IP** 池）— `10.31.32.3 - 10.31.32.118`
2. **Commit**（提交）网关配置。

STEP 8 | 配置 GlobalProtect 门户。

配置 **Device**（设备）详情（联网参数、身份验证服务配置文件以及身份验证服务器证书）。

选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户），然后 **Add**（添加）下列门户配置：

设置 GlobalProtect 门户访问权限：

Interface（接口）— `ethernet1/2`

IP 地址 — `203.0.113.1`

Server Certificate（服务器证书）— `GoDaddy` 颁发的 `GP-server-cert.pem`

Certificate Profile（证书配置文件）— `None`

Authentication Profile（身份验证配置文件）— `Corp-LDAP`

STEP 9 | 为预登录用户和已登录用户定义 GlobalProtect 代理配置。

若要预登录用户在登录前后访问相同网关，请使用单一配置。

若要预登录用户在登录前后被导向不同网关，请创建两个配置文件。在第一个配置的 **User/User Group**（用户/用户组）中，选择 **pre-logon**（预登录）筛选器。对于预登录，门户首先对端点而非用户进行身份验证，以建立连接（即使预登录参数与用户相关联）。接着，当用户登录时，门户对用户进行身份验证。

在门户对用户进行身份验证后，其将部署第二个配置。在此情况下，**User/User Group**（用户/用户组）为 **any**（任意）。

© 2019 Palo Alto Networks, Inc.

最佳做法是，在第二个配置中启用 *SSO* 以确保当用户登录至端点时立即将正确的用户名报告至网关。如果未启用 *SSO*，则会使用 *Agent*（代理）设置面板中保存的用户名。

选择 **GlobalProtect** 门户配置窗口的 **Agent**（代理）选项卡（**Network**（网络）> **GlobalProtect** > **Portals**（门户）> **<portal-config>**（门户配置）），然后 **Add**（添加）下列其中一个配置：

- 在预登录用户登录前后使用相同网关：

Use single sign-on（使用单点登录）— **`enabled`**

Connect Method（连接方法）— 预登录

External Gateway Address（外部网关地址）— **`gp1.acme.com`**

User/User Group（用户/用户组）— **`any`**

Authentication Override（身份验证覆盖）— Cookie 身份验证以对用户进行透明身份验证和配置刷新

- 在预登录用户登录前后分别使用单独网关：

第一个代理配置：

Connect Method（连接方法）— 预登录

External Gateway Address（外部网关地址）— **`gp1.acme.com`**

User/User Group（用户/用户组）— 预登录

Authentication Override（身份验证覆盖）— Cookie 身份验证以对用户进行透明身份验证和配置刷新

第二个代理配置：

Use single sign-on（使用单点登录）— **`enabled`**

Connect Method（连接方法）— 预登录

External Gateway Address（外部网关地址）— **`gp2.acme.com`**

User/User Group（用户/用户组）— **`any`**

Authentication Override（身份验证覆盖）— Cookie 身份验证以对用户进行透明身份验证和配置刷新

确保预登录配置位于配置列表的第一项。如果未处于第一项，请将其选中并单击 **Move Up**（上移）。

STEP 10 | 保存 GlobalProtect 配置。

单击 **Commit**（提交）。

STEP 11 | （可选）如果用户从未登录端点（例如无头端点），或者用户以前未登录的端点需要预登录连接，在端点上创建 **`Prelogon`** 注册表项。

您还必须预部署默认门户 *IP* 地址。

有关注册表设置的详细信息，请参阅以透明方式部署应用设置。

1. 转到以下 Windows 注册表位置以查看 GlobalProtect 设置列表：

   `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

2. 选择 **Edit**（编辑）> **New**（新）> **String Value**（字符串值），以创建以下注册表条目：
   - 创建名为 **`Prelogon`** 且值为 **`1`** 的 **String Value**（字符串值）。该设置让 GlobalProtect 在用户登录端点前发起一个连接。

© 2019 Palo Alto Networks, Inc.

- 创建名称为 **`Portal`** 的 **String Value**（字符串值），其中指定 GlobalProtect 端点默认门户的 IP 地址或主机名。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 多网关配置

在以下 GlobalProtect 多网关拓扑中，已将第二个外部网关添加至配置。在此拓扑中，您必须配置其他防火墙以承载第二个 GlobalProtect 网关。在添加由门户部署的客户端配置时，还可以为不同的客户端配置指定不同的网关，或允许访问所有网关。

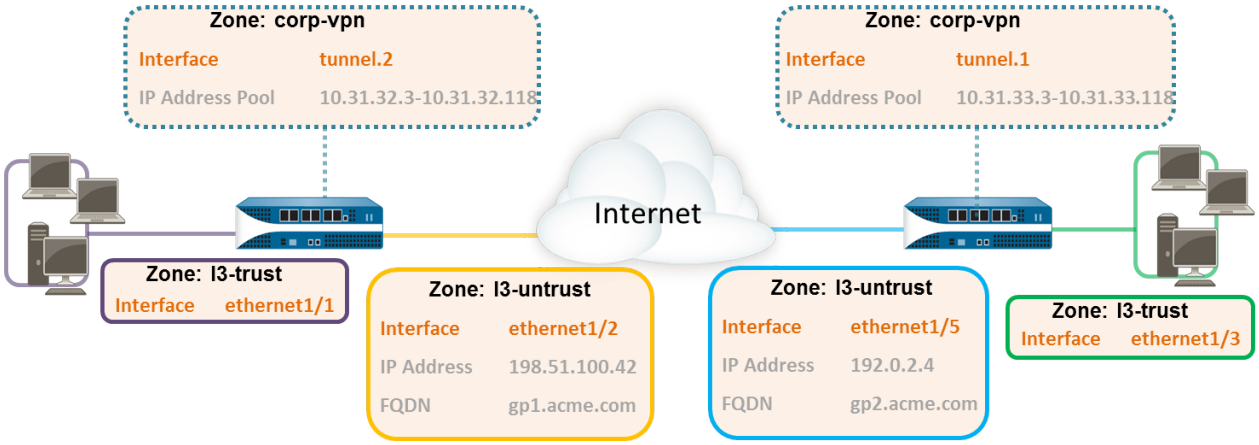


图 7: **GlobalProtect** 多网关拓扑

如果客户端配置包含多个网关，则应用将尝试连接至其客户端配置中所列的全部网关。应用将使用优先级和响应时间来决定要连接的网关。当较高优先级网关的响应时间长于所有网关的平均响应时间时，应用才连接至较低优先级网关。有关详细信息，请参阅多网关配置中的网关优先级。

STEP 1 | 为 GlobalProtect 创建接口和区域。

采用此配置时，须在承载网关的所有防火墙上设置接口。

为所有接口配置使用 *default*（默认）虚拟路由器以免创建域间路由。

在承载门户/网关 (gw1) 的防火墙上：

- 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择 **ethernet1/2**。
- 将 **ethernet1/2** 配置为 IP 地址为 `198.51.100.42` 的第三层以太网接口，然后将其分配给 `l3-untrust` **Security Zone**（安全区域）和 `default` **Virtual Router**（虚拟路由器）。
- 创建将 IP 地址 `198.51.100.42` 映射到 `gp1.acme.com` 的 DNS“A”记录。
- 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），然后 **Add**（添加）`tunnel.2` 接口。添加接口至名为 `corp-vpn` 的新 **Security Zone**（安全区域）。将其分配给 `default`**Virtual Router**（虚拟路由器）。
- 在 `corp-vpn` 区域内启用“用户标识”。

在承载第二个网关 (gw2) 的防火墙上：

- 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择 **ethernet1/5**。

© 2019 Palo Alto Networks, Inc.

- 将 **ethernet1/5** 配置为 IP 地址为 **192.0.2.4** 的第 3 层接口，然后将其分配给 **l3-untrust Security Zone**（安全区域）和默认 **Virtual Router**（虚拟路由器）。
- 创建用于将 IP 地址 **192.0.2.4** 映射至 **gp2.acme.com** 的 DNS“A”记录。
- 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），然后 **Add**（添加）**tunnel.1** 接口。添加接口至名为 **corp-vpn** 的新 **Security Zone**（安全区域）。将其分配给默认 **Virtual Router**（虚拟路由器）。
- 在 **corp-vpn** 区域内启用“用户标识”。

STEP 2 | 如果最终用户要使用其移动端点上的 GlobalProtect 应用或是您计划使用启用了 HIP 的安全策略，需要在每个网关上购买并安装 GlobalProtect 订阅。

购买 GlobalProtect 订阅并收到激活代码后，按下列方法在承载门户的防火墙上安装该许可证：

1. 选择 **Device**（设备）> **Licenses**（许可证）。
2. 选择 **Activate feature using authorization code**（使用授权代码激活功能）。
3. 系统提示时，输入 **Authorization Code**（授权代码），然后单击 **OK**（确定）。
4. 验证是否已成功激活许可证：

STEP 3 | 在托管 GlobalProtect 网关的每个防火墙中，创建安全策略。

此配置需要策略规则在 **corp-vpn** 区域和 **l3-trust** 区域之间启用通信流，以便访问内部资源（**Policies**（策略）> **Security**（安全））。

STEP 4 | 使用下列推荐方法之一为承载 GlobalProtect 门户和 GlobalProtect 网关的所有接口获取服务器证书：

- （在承载门户或门户/网关的防火墙上）导入来自众所周知的第三方 CA 的服务器证书。
- （在仅承载网关的防火墙上）使用门户中的根 CA 生成自签名服务器证书。

在承载门户/网关或网关的每个防火墙上，选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）以按下列方法管理证书：

- 为承载 portal/gw1 的接口获取服务器证书。由于门户和网关位于同一接口上，因此须使用同一服务器证书。证书的 CN 必须与 FQDN `gp1.acme.com` 相符。要使端点连接至门户而不收到证书错误，请使用来自公共 CA 的服务器证书。
- 为承载 gw2 的接口获取服务器证书。由于该接口仅承载网关，因此可使用自签名证书。证书公用名 (CN) 必须与 FQDN `gp2.acme.com` 相匹配。

STEP 5 | 定义如何将用户验证至门户和网关。

您可以按需使用证书配置文件和/或身份验证配置文件的组合以确保门户和网关的安全。门户及各网关也可使用不同的身份验证方案。请参阅下列章节以了解分步说明：

- 设置外部身份验证（身份验证配置文件）
- 设置客户端证书身份验证（证书配置文件）
- 设置双重身份验证（基于令牌或 OTP）

随后，需应用门户和网关配置中定义的证书配置文件和/或身份验证配置文件。

STEP 6 | 配置 GlobalProtect 网关。

以下示例介绍如何配置 GlobalProtect 多网关拓扑中所示的 gp1 和 gp2。

在托管 gp1 的防火墙上，选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）。配置以下网关设置：

© 2019 Palo Alto Networks, Inc.

Interface（接口）— `ethernet1/2`

IP 地址 — `198.51.100.42`

Server Certificate（服务器证书）— `GP1-server-cert.pem issued by GoDaddy`

Tunnel Interface（隧道接口）— `tunnel.2`

IP Pool（**IP** 池）— `10.31.32.3 - 10.31.32.118`

在托管 gp2 的防火墙上，选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）。配置以下网关设置：

Interface（接口）— `ethernet1/2`

IP 地址 — `192.0.2.4`

Server Certificate（服务器证书）— 自签名证书 `GP2-server-cert.pem`

Tunnel Interface（隧道接口）— `tunnel.1`

IP 池 — `10.31.33.3 - 10.31.33.118`

STEP 7 | 配置 GlobalProtect 门户。

选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）.配置以下门户设置：

1. 设置 GlobalProtect 门户访问权限：

   Interface（接口）— `ethernet1/2`

   IP 地址 — `198.51.100.42`

   Server Certificate（服务器证书）— `GP1-server-cert.pem issued by GoDaddy`
2. 定义 GlobalProtect 代理配置：

   需创建的客户端配置数取决于特定的访问需求，其中包括是否需要基于用户/组的策略和/或已启用 HIP 的策略强制。

STEP 8 | 部署 GlobalProtect 代理软件。

选择 **Device**（设备）> **GlobalProtect Client**（**GlobalProtect** 客户端）。

在此例中，遵循在门户上载入应用更新的步骤。

STEP 9 | 保存 GlobalProtect 配置。

在承载门户和网关的防火墙上 **Commit**（提交）配置 。

© 2019 Palo Alto Networks, Inc.

适用于内部 HIP 验证和基于用户的访问的 GlobalProtect

与用户 ID 和/或 HIP 验证协同使用时，内部网关可提供一种按用户和/或设备状态来辨识和控制通信的安全、精确方法，从而替代其他网络访问控制 (NAC) 服务。在需要进行身份验证以访问关键资源的敏感环境下，内部网关十分有用。

采用仅含内部网关的配置时，须将所有端点配置为用户登录（始终启用）模式，而不支持按需模式。此外，建议将所有客户端配置设为使用单一登录 (SSO)。另外，由于内部主机无需与网关建立隧道连接，因此将使用端点上物理网络适配器的 IP 地址。

采用此快速配置时，内部网关将用于强制执行基于组的策略。这些策略分别允许“工程”组的用户访问内部源控制和漏洞数据库，以及“财经”组的用户访问 CRM 应用程序。所有经验证的用户均可访问内部 Web 资源。此外，网关上配置的 HIP 配置文件还将检查所有主机以确保符合内部维护要求，例如是否已安装最新的安全修补程序，是否已启用磁盘加密，或是否已安装必要软件。

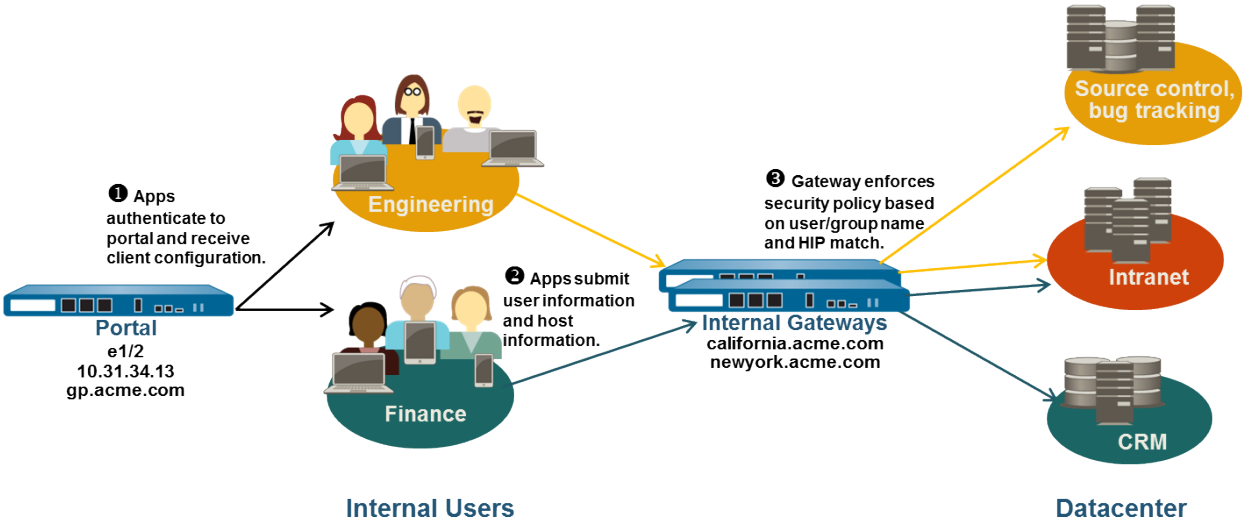


图 **8: GlobalProtect** 内部网关配置

使用下列步骤配置 GlobalProtect 内部网关。

STEP 1 | 为 GlobalProtect 创建接口和区域。

采用此配置时，须在承载门户和/或网关的所有防火墙上设置接口。由于此配置仅使用内部网关，因此须在内部网络的接口上配置门户和网关。

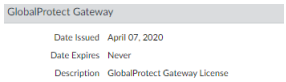
为所有接口配置使用 *default*（默认）虚拟路由器以免创建域间路由。

© 2019 Palo Alto Networks, Inc.

在承载门户/网关的每个防火墙上：

1. 选择某一以太网端口以承载门户/网关，然后配置 IP 地址位于 `l3-trust` **Security Zone**（安全区域）中的第 3 层接口（**Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网））。
2. 在 `l3-trust` 区域内 **Enable User Identification**（启用用户标识）。

STEP 2 | 如果您的任何一名最终用户将通过其移动设备访问 GlobalProtect 应用程序，或者您计划使用启用了 HIP 的安全策略，请为承载内部网关的每个防火墙购买并安装 GlobalProtect 订阅。



购买 GlobalProtect 订阅并收到激活代码后，按下列方法在承载网关的防火墙上安装 GlobalProtect 订阅：

1. 选择 **Device**（设备）> **Licenses**（许可证）。
2. 选择 **Activate feature using authorization code**（使用授权代码激活功能）。
3. 系统提示时，输入 **Authorization Code**（授权代码），然后单击 **OK**（确定）。
4. 验证是否已成功激活许可证。

如果您没有所需的许可证，请联系您的 Palo Alto Networks 销售工程师或经销商。有关许可证的详细信息，请参阅关于 GlobalProtect 许可证。

STEP 3 | 为 GlobalProtect 门户和所有 GlobalProtect 网关获取服务器证书。

为首次连接至门户，端点须信任用户颁发门户服务器证书的根 CA 证书。您既可以在首次连接到门户前在门户上使用自签名证书并将根 CA 证书部署至端点，也可从受信 CA 为门户获取服务器证书。

可在网关上使用自签名证书。

推荐的操作流程如下：

1. 在承载门户的防火墙上：
   1. 导入来自众所周知的第三方 CA 的服务器证书。
   2. 创建用于向 GlobalProtect 组件颁发自签名证书的根 CA 证书。
   3. 使用门户中的根 CA 生成自签名服务器证书。为所有网关重复执行此步骤。
2. 在承载内部网关的每个防火墙上，部署自签名服务器证书。

STEP 4 | 定义如何将用户验证至门户和网关。

您可以按需使用证书配置文件和/或身份验证配置文件的组合以确保门户和网关的安全。门户及各网关也可使用不同的身份验证方案。请参阅下列章节以了解分步说明：

- 设置外部身份验证（身份验证配置文件）
- 设置客户端证书身份验证（证书配置文件）
- 设置双重身份验证（基于令牌或 OTP）

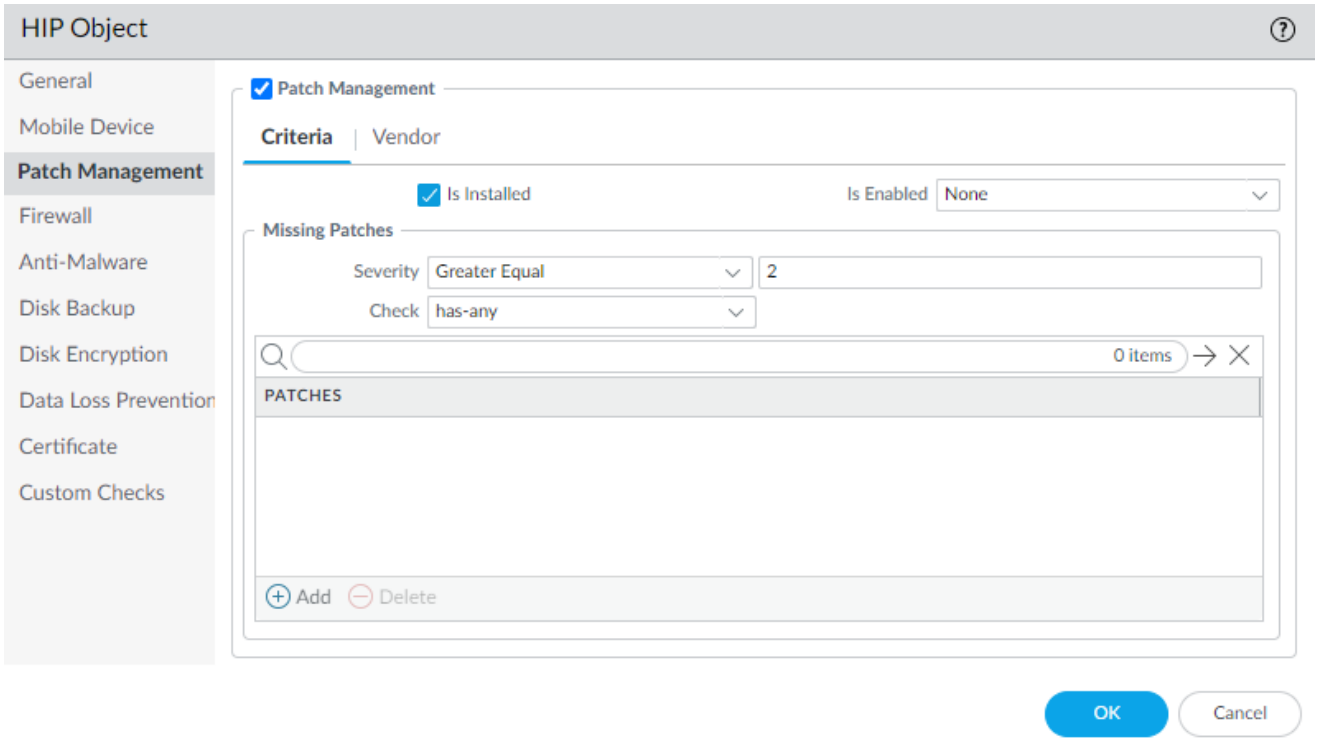
随后，需应用门户和网关配置中定义的证书配置文件和/或身份验证配置文件。

STEP 5 | 创建需对网关访问强制执行安全策略的 HIP 配置文件。

有关 HIP 匹配的详细信息，请参阅主机信息。

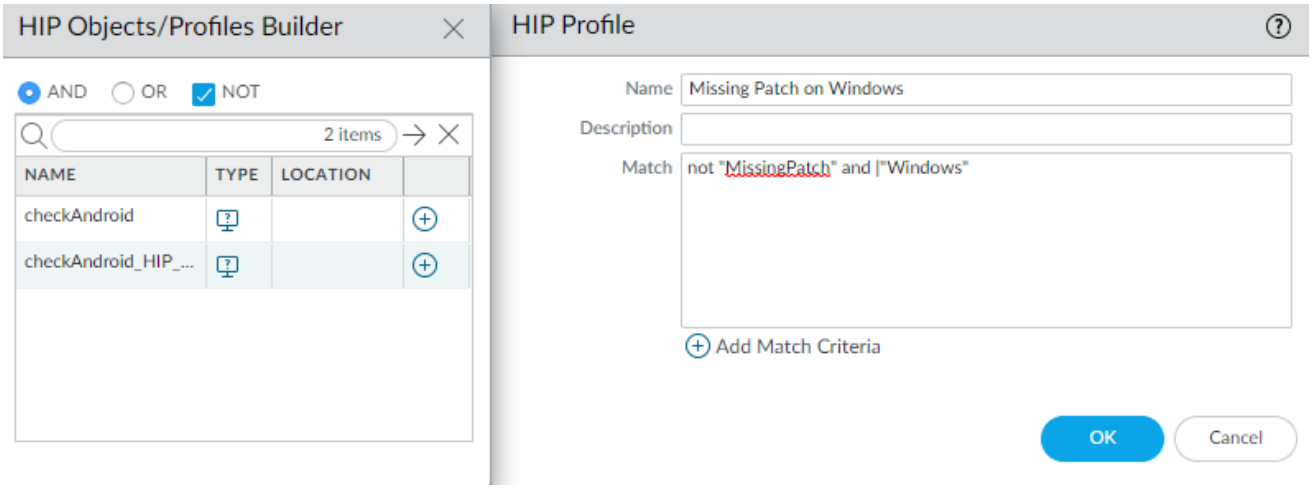
1. 创建 HIP 对象以筛选应用程序所收集的原始主机数据。例如，如果想阻止不需要最新必要修补程序的用户进行连接，则可创建 HIP 对象以验证是否已安装修补程序管理软件以及具有特定严重性的所有修补程序是否为最新。

© 2019 Palo Alto Networks, Inc.



2. 创建您要在策略中使用的 HIP 配置文件。

   例如，如果想确保仅安装了最新修补程序的 Windows 用户访问内部应用程序，则可附加下列 HIP 配置文件以匹配装有完整修补程序的主机：



STEP 6 | 配置内部网关。

选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关），然后选择现有内部网关或 **Add**（添加）新网关。配置以下网关设置：

- 接口
- **IP** 地址
- 服务器证书
- 身份验证配置文件和/或 配置文件

© 2019 Palo Alto Networks, Inc.

请注意，由于不需要隧道连接，因此无需在网关配置中设定客户端设置（除非想设置 HIP 通知）。有关创建网关配置的分步说明，请参阅配置 GlobalProtect 网关。

STEP 7 | 配置 GlobalProtect 门户。

> 虽然上述所有配置均可使用 *User-logon (Always On)*（用户登录（始终启用））或 *On-demand (Manual user initiated connection)*（按需（用户手动发起连接））连接方法，但由于内部网关配置须始终打开，因此需使用 *User-logon (Always On)*（用户登录（始终启用））连接方法。

选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户），然后选择现有门户或 **Add**（添加）新门户。配置以下门户：

1. 设置 GlobalProtect 门户访问权限：

   Interface（接口）— `ethernet1/2`

   IP Address（IP 地址）— `10.31.34.13`

   Server Certificate（服务器证书验证）— `GP-server-cert.pem issued by GoDaddy`，包含 `CN=gp.acme.com`
2. 定义 GlobalProtect 客户端身份验证配置：

   Use single sign-on（使用单点登录）— `enabled`

   Connect Method（连接方法）— `User-logon (Always On)`

   Internal Gateway Address（内部网关地址）— `california.acme.com, newyork.acme.com`

   User/User Group（用户/用户组）— `any`
3. **Commit**（提交）门户配置。

STEP 8 | 部署 GlobalProtect 应用程序软件。

选择 **Device**（设备）> **GlobalProtect Client**（**GlobalProtect** 客户端）。

在此例中，使用在门户上载入应用更新的步骤。

STEP 9 | 在网关上创建已启用 HIP 和/或基于用户/组的安全规则。

在本示例中，添加下列安全规则：

1. 选择 **Policies**（策略）> **Security**（安全），并单击 **Add**（添加）。
2. 在 **Source**（源）选项卡中，将 **Source Zone**（源区域）设置为 **l3-trust**。
3. 在 **User**（用户）选项卡中，添加要匹配的 HIP 配置文件和用户/组。
   - 在 **HIP Profiles**（**HIP** 配置文件）区域内单击 **Add**（添加），然后选择 HIP 配置文件 **MissingPatch**。
   - **Add**（添加） **Source User**（源用户）组（根据当前创建的规则，选择“财务”或“工程”）。
4. 单击 **OK**（确定）保存规则。
5. **Commit**（提交）网关配置。

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	CRM access	none	l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default	✓
2	Eng access	none	l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default	✓

© 2019 Palo Alto Networks, Inc.

内部和外部网关混合配置

在 GlobalProtect 内部和外部网关混合配置中，您可以为 VPN 访问和访问敏感内部资源分别配置网关。采用此配置时，GlobalProtect 应用将执行内部主机检测以确定其是位于内部还是外部网络。如果应用确定其位于外部网络，则会尝试连接至其客户端配置中所列的外部网关，并与具有最高优先级和最短响应时间的网关建立连接。

如果将所有外部网关配置为仅手动网关，但将 *GlobalProtect* 连接方法配置为 *User-Logon (Always On)*（用户登录（始终启用）或 *Pre-Logon (Always On)*（预登录（始终启用））），则 *GlobalProtect* 应用不会自动连接到任何外部网关。在外部用户手动建立网关连接之前，*GlobalProtect* 将保持 未连接状态。通过此行为，您可以部署 *GlobalProtect* 以导出内部用户的 *User-ID*，同时支持外部用户的 按需*VPN* 行为。

由于安全策略分别在各个网关上定义，因此可细粒度控制内、外部用户分别可访问的资源。此外，通过配置门户以根据用户/组成员资格或根据 HIP 配置文件匹配以部署不同的客户端配置，还可细粒度控制用户拥有访问权限的网关。

在本示例中，门户和所有三个网关（一个外部和两个内部网关）均部署于不同防火墙上。位于 gpvpn.acme.com 的外部网关可提供针对公司网络的远程 VPN 访问权限，内部网关则针对敏感的数据中心资源提供基于组成员资格的细粒度访问权限。此外，还使用 HIP 验证以确保访问数据中心的主机装有最新的安全修补程序。

© 2019 Palo Alto Networks, Inc.

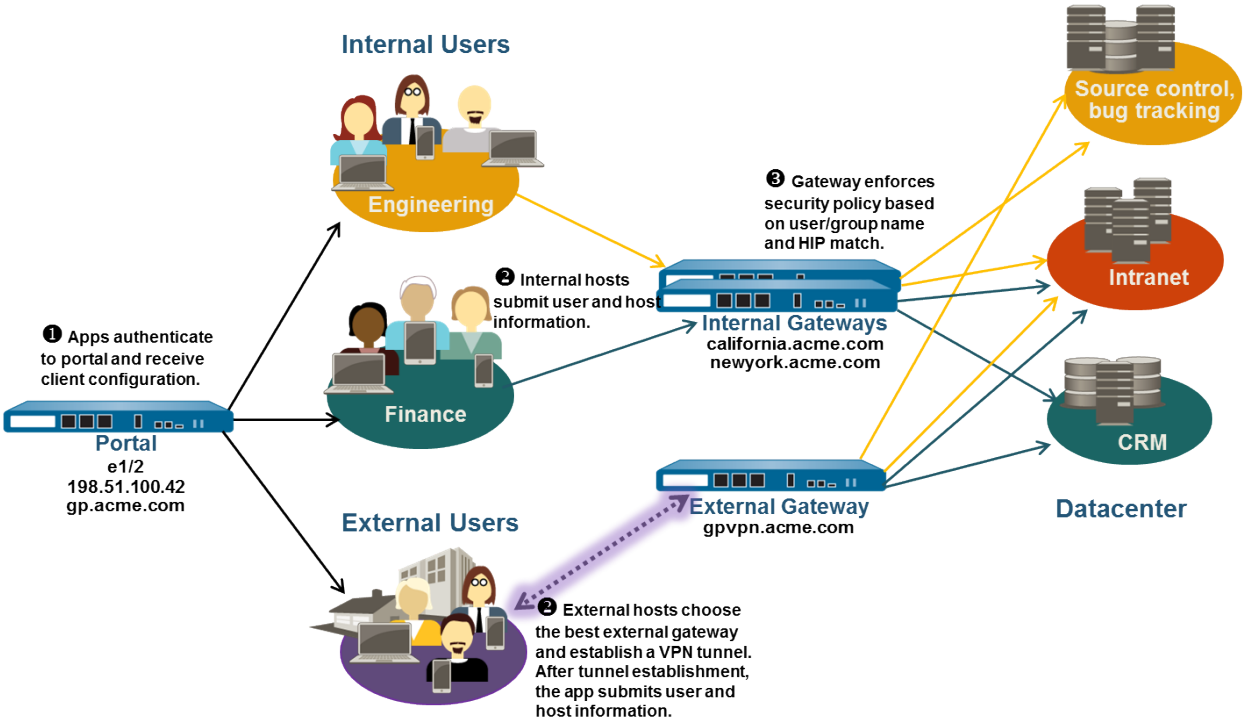


图 **9:** 带内外部网关的 **GlobalProtect** 部署

使用下列步骤混合配置内部和外部 GlobalProtect 网关。

STEP 1 | 为 GlobalProtect 创建接口和区域。

采用此配置时，须在承载门户和网关的所有防火墙上设置接口。

请勿在已配置 *GlobalProtect* 门户或网关的接口上附加允许 *HTTP*、*HTTPS*、*Telnet* 或 *SSH* 的接口管理配置文件，因为这样可以从 *Internet* 访问管理界面。按照安全管理访问的最佳实践确保您以防止成功攻击的方式保护对防火墙的管理访问权限。

为所有接口配置使用 *default*（默认）虚拟路由器以免创建域间路由。

在承载门户网关 (gp.acme.com) 的防火墙上：

- 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），将 **ethernet1/2** 配置为 IP 地址为 `198.51.100.42` 的第 3 层以太网接口。将其分配给 `l3-untrust` **Security Zone**（安全区域）和默认 **Virtual Router**（虚拟路由器）.
- 创建用于将 IP 地址 198.51.100.42 映射至 gp.acme.com 的 DNS“A”记录。

© 2019 Palo Alto Networks, Inc.

- 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），然后 **Add**（添加）**`tunnel.2`**接口。将其分配给名为 `corp-vpn` 的新 **Security Zone**（安全区域）和默认 **Virtual Router**（虚拟路由器）。
- 在 corp-vpn 区域内启用“用户标识”。

在承载外部网关 (gpvpn.acme.com) 的防火墙上：

- 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），将 **ethernet1/5** 配置为 IP 地址为 **`192.0.2.4`** 的第 3 层以太网接口。将其分配给 **`l3-untrust`** **Security Zone**（安全区域）和默认 **Virtual Router**（虚拟路由器）.
- 创建用于将 IP 地址 192.0.2.4 映射至 gpvpn.acme.com 的 DNS“A”记录。
- 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），然后 **Add**（添加）**`tunnel.3`** 接口。将其分配给名为 `corp-vpn` 的新 **Security Zone**（安全区域）和默认 **Virtual Router**（虚拟路由器）。
- 在 corp-vpn 区域内启用“用户标识”。

在承载内部网关（california.acme.com 和 newyork.acme.com）的防火墙上：

- 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），在内部网络上配置带 IP 地址的第三层以太网接口。将其分配给 **`l3-trust`** **Security Zone**（安全区域）和默认 **Virtual Router**（虚拟路由器）。
- 创建用于映射内部 IP 地址 california.acme.com 和 newyork.acme.com 的 DNS“A”记录。
- 在 l3-trust 区域内启用用户标识。

STEP 2 | 如果最终用户要使用其移动端点上的 GlobalProtect 应用或是您计划使用启用了 HIP 的安全策略，需要为承载网关（内部和外部）的每个防火墙购买并安装 GlobalProtect 订阅。

购买 GlobalProtect 订阅并收到激活代码后，在承载网关的防火墙上安装 GlobalProtect 订阅：

1. 选择 **Device**（设备）> **Licenses**（许可证）。
2. 选择 **Activate feature using authorization code**（使用授权代码激活功能）。
3. 系统提示时，输入 **Authorization Code**（授权代码），然后单击 **OK**（确定）。
4. 验证是否已成功激活许可证和订阅。

如果您没有所需的许可证，请联系您的 Palo Alto Networks 销售工程师或经销商。有关许可证的详细信息，请参阅关于 GlobalProtect 许可证。

STEP 3 | 为 GlobalProtect 门户和所有 GlobalProtect 网关获取服务器证书。

为首次连接至门户，端点须信任用户颁发门户服务器证书的根 CA 证书。

可在网关上使用自签名证书，并在客户端配置中将根 CA 证书部署至应用。最佳做法是在承载门户的防火墙上生成所有证书，然后将其部署至网关。

推荐的操作流程如下：

1. 在承载门户的防火墙上：
   1. 导入来自众所周知的第三方 CA 的服务器证书。
   2. 创建用于向 GlobalProtect 组件颁发自签名证书的根 CA 证书。
   3. 使用门户中的根 CA 生成自签名服务器证书。为所有网关重复执行此步骤。
2. 在承载内部网关的每个防火墙上：
   - 部署自签名服务器证书。

STEP 4 | 定义如何将用户验证至门户和网关。

© 2019 Palo Alto Networks, Inc.

您可以使用证书配置文件和/或身份验证配置文件的组合以确保门户和网关的安全。门户及各网关也可使用不同的身份验证方案。请参阅下列章节以了解分步说明：

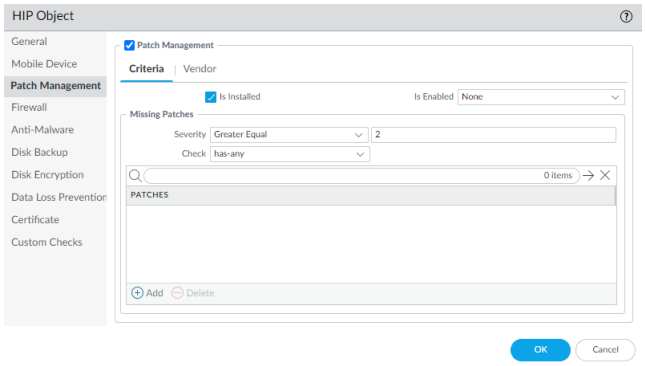
- 设置外部身份验证（身份验证配置文件）
- 设置客户端证书身份验证（证书配置文件）
- 设置双重身份验证（基于令牌或 OTP）

随后，需应用门户和网关配置中定义的证书配置文件和/或身份验证配置文件。

STEP 5 | 创建需对网关访问强制执行安全策略的 HIP 配置文件。

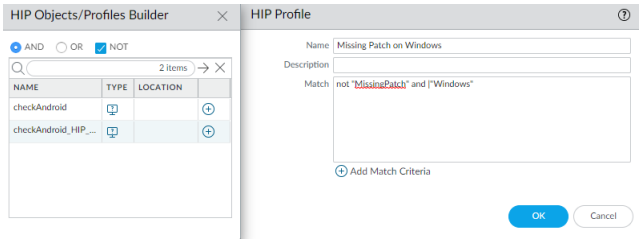
有关 HIP 匹配的详细信息，请参阅主机信息。

1. 创建 HIP 对象以筛选应用程序所收集的原始主机数据。例如，如果想阻止未安装最新的必要修补程序的用户，则可创建 HIP 对象以验证是否已安装修补程序管理软件以及具有特定严重性的所有修补程序是否为最新。



2. 创建您要在策略中使用的 HIP 配置文件。

   例如，如果想确保仅安装了最新修补程序的 Windows 端点访问内部应用程序，则可附加下列 HIP 配置文件以匹配装有完整修补程序的主机：



STEP 6 | 配置内部网关。

选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）并 **Add**（添加）带下列设置的网关配置：

- 接口
- **IP** 地址
- 服务器证书
- 身份验证配置文件和/或 配置文件

请注意，由于不需要隧道连接，因此无需在网关配置中设定客户端配置设置（除非想设置 HIP 通知）。有关创建网关配置的分步说明，请参阅配置 GlobalProtect 网关。

STEP 7 | 配置 GlobalProtect 门户。

虽然本示例介绍了如何创建将部署至所有应用的单个客户端配置，但也可为不同用途分别创建配置，然后根据用户/组名和/或运行应用的端点操作系统对其进行部署。

© 2019 Palo Alto Networks, Inc.

选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）并 **Add**（添加）下列门户配置：

1. 设置 GlobalProtect 门户访问权限：

   Interface（接口）— `ethernet1/2`

   IP Address（IP 地址）— `10.31.34.13`

   Server Certificate（服务器证书验证）— `GP-server-cert.pem issued by GoDaddy`，包含 `CN=gp.acme.com`
2. 定义 GlobalProtect 客户端身份验证配置：

   Internal Host Detection（内部主机检测）— `enabled`

   Use single sign-on（使用单点登录）— `enabled`

   Connect Method（连接方法）— `User-logon (Always On)`

   External Gateway Address（外部网关地址）— `gpvpn.acme.com`

   Internal Gateway Address（内部网关地址）— `california.acme.com, newyork.acme.com`

   User/User Group（用户/用户组）— 任意
3. **Commit**（提交）门户配置。

STEP 8 | 部署 GlobalProtect 应用程序软件。

选择 **Device**（设备）> **GlobalProtect Client**（**GlobalProtect** 客户端）。

在此例中，使用在门户上载入应用更新的步骤。

STEP 9 | 在每个网关上创建安全策略规则以便让 VPN 用户安全访问应用程序。

- 创建安全策略（**Policies**（策略）> **Security**（安全））以便在 corp-vpn 区域和 l3-trust 区域之间启用通信流。
- 创建已启用 HIP 和基于用户/组的策略规则以便细粒度访问内部数据中心资源。
- 对于可视性，请使用默认安全配置文件创建规则，以允许所有用户通过 Web 浏览方式访问 l3-untrust 域，从而保护您免遭已知威胁。

			Source				Destination					
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	CRM access	none	corp-vpn l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default		none
2	Eng access	none	corp-vpn l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default		none
3	GP access	none	corp-vpn l3-trust	any	any	any	l3-untrust	any	web-browsing	application-default		

STEP 10 | 保存 GlobalProtect 配置。

Commit（提交）您的门户和网关配置。

© 2019 Palo Alto Networks, Inc.

强制网络门户和对网络访问强制执行 GlobalProtect

在大部分实例中，移动用户都连接至启用了强制网络门户的 Wi-Fi 网络，如咖啡馆、机场和酒店使用的 Wi-Fi 网络。用户登录强制网络门户后，方可访问 Internet。用户可通过基于浏览器的强制网络门户登录页面，或基于 OS 的强制网络门户助手（使用名称和电子邮件地址作为标识符）进行登录。通过此配置，您可以限制用户登录强制网络门户的时间。如果用户成功登录，且可连接 Internet，GlobalProtect 应用程序将自动建立连接。如果用户未在指定的时间内登录，将阻止所有流量。

为了进一步降低网络遭受安全威胁的风险，您也可以对网络访问强制执行 GlobalProtect。当启用此选项时，在应用程序连接至 GlobalProtect 网关之前，GlobalProtect 将阻止所有网络流量。所有流量都需要经过 VPN 隧道以进行检查并执行策略，由此让您可以保持对您的用户流量的全面监视和控制。

根据强制网络门户是否存在，以及是否需要连接 GlobalProtect 以访问网络，用户必须遵照指定的工作流程以访问网络：

强制网络门户	对网络访问强制执行 GlobalProtect	工作流程
是	是	如需连接 GlobalProtect 以访问网络，且最终用户还必须登录强制网络门户以访问 Internet，那么他们必须采取以下步骤以访问网络： 1. 连接至 Wi-Fi 网络。 在连接至 Wi-Fi 网络后，GlobalProtect 会自动检测强制网络门户。如果管理员配置了强制网络门户检测消息，GlobalProtect 应用将通知您必须登录强制网络门户才能访问网络。 管理员也可以配置经过多长时间之后显示强制网络门户检测消息。 2. 使用下列选项之一登录强制网络门户： • 打开 Web 浏览器，以通过强制网络门户登录页面登录。 • 通过端点操作系统 (OS) 内置的原生强制网络门户助手登录。 如果强制网络门户登录成功，将可以访问 Internet，且 GlobalProtect 应用自动连接。如果应用未立即连接，且管理员配置了流量阻止通知消息以指示您必须连接至 GlobalProtect 才能访问网络，在建立连接之前将显示此消息。 管理员也可以配置经过多长时间之后显示流量阻止通知。 如果强制网络门户日志登录失败，且强制网络门户登录页面超时，或 GlobalProtect 无法建立连接，您将无法使用此网络。要重新启动门户网站登录并重新触发强制网络门户登录时限，启动 GlobalProtect 应用，然后从应用设置 ( ) 菜单选择 **Refresh Connection**（刷新连接）。
是	否	如果最终用户必须登录强制网络门户才能访问 Internet，但网络访问无需 GlobalProtect 连接，则他们必须采用下列步骤以访问网络： 1. 连接至 Wi-Fi 网络。

© 2019 Palo Alto Networks, Inc.

强制网络门户	对网络访问强制执行 GlobalProtect	工作流程
		在连接至 Wi-Fi 网络后，GlobalProtect 会自动检测强制网络门户。 2. 使用下列选项之一登录强制网络门户： • 打开 Web 浏览器，以通过强制网络门户登录页面登录。 • 通过端点操作系统 (OS) 内置的原生强制网络门户助手登录。 如果登录成功且可以访问 Internet，GlobalProtect 应用将自动连接。
否	是	如需 GlobalProtect 连接才能访问网络，而最终用户无需登录强制网络门户以访问 Internet，那么他们必须连接至 Wi-Fi 网络。一旦连接 Wi-Fi 且可访问 Internet，GlobalProtect 应用便会自动连接。 如果应用未立即连接，且管理员配置了流量阻止通知消息以指示您必须连接至 GlobalProtect 才能访问网络，在建立连接之前将显示此消息。如果 GlobalProtect 无法建立连接，您将无法访问网络。您必须通过断开然后重新连接至 Wi-Fi 网络、重新启动您的端点或刷新 GlobalProtect 连接的方式，重新启动网络发现。

使用下列步骤自定义强制网络门户设置，并指示网络访问是否需要 GlobalProtect 连接：

只有在为 *GlobalProtect* 配置了“始终打开”连接方式时，才配置 *Enforce GlobalProtect for Network Access*（对网络访问强制执行 *GlobalProtect*）选项。

STEP 1 | 设置 GlobalProtect 门户访问权限。

STEP 2 | 定义 GlobalProtect 代理配置。

STEP 3 | 自定义 GlobalProtect 应用程序。

- 为确保 GlobalProtect 连接始终打开，将 **Connect Method**（连接方法）设为 **User-logon (Always On)**（用户登录（始终打开））。
- 如果您的用户必须登录强制网络门户才能访问 Internet，则可以通过配置以下项目自定义强制网络门户设置：
  - 在 **Captive Portal Exception Timeout (sec)**（强制网络门户例外超时）（秒）字段中，输入用户可登录强制网络门户的时限（以秒为单位）（范围为 0 至 3600 秒；默认为 0 秒）。如果用户未在此时限内登录，强制网络门户登录页面超时，用户将被禁止访问网络。
  - 要启用 GlobalProtect 应用以在检测到强制网络门户时通知用户，将 **Display Captive Portal Detection Message**（显示强制网络门户检测消息）设置为 **Yes**（是）。
    - 在 **Captive Portal Notification Delay (sec)**（强制网络门户通知延迟）（秒）字段中，输入 GlobalProtect 应用显示强制网络门户检测消息的延迟时间（以秒为单位）（范围为 1 至 120 秒；默认为 5 秒）。在检测到强制网络门户后，GlobalProtect 将在可访问 Internet 之前启动此计时器。
    - 自定义 **Captive Portal Detection Message**（强制网络门户检测消息）以在 GlobalProtect 检测到强制网络门户时显示。
- 要强制所有网络流量通过 GlobalProtect VPN 隧道，请配置以下选项：
  - 将 **Enforce GlobalProtect for Network Access**（对网络访问强制执行 **GlobalProtect**）选项设为 **Yes**（是）。

© 2019 Palo Alto Networks, Inc.

- 要启用 GlobalProtect 应用以通知用户需要 GlobalProtect 连接才能访问网络，将 **Display Traffic Blocking Notification Message**（显示流量阻止通知消息）设为 **Yes**（是）。当可连接至 Internet，但尚未建立 GlobalProtect 连接之前，GlobalProtect 应用会显示此消息。
  - 在 **Traffic Blocking Notification Delay (sec)**（流量阻止通知延迟）（秒）字段中，输入 GlobalProtect 应用显示流量阻止通知消息的延迟时间（以秒为单位）（范围为 5 至 120 秒；默认为 15 秒）。在可连接至 Internet 后，GlobalProtect 将启动此计时器。
  - 自定义在网络访问需要 GlobalProtect 连接时显示的 **Traffic Blocking Notification Message**（流量阻止通知消息）。此消息必须在 512 个字符以内。

STEP 4 | **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 架构

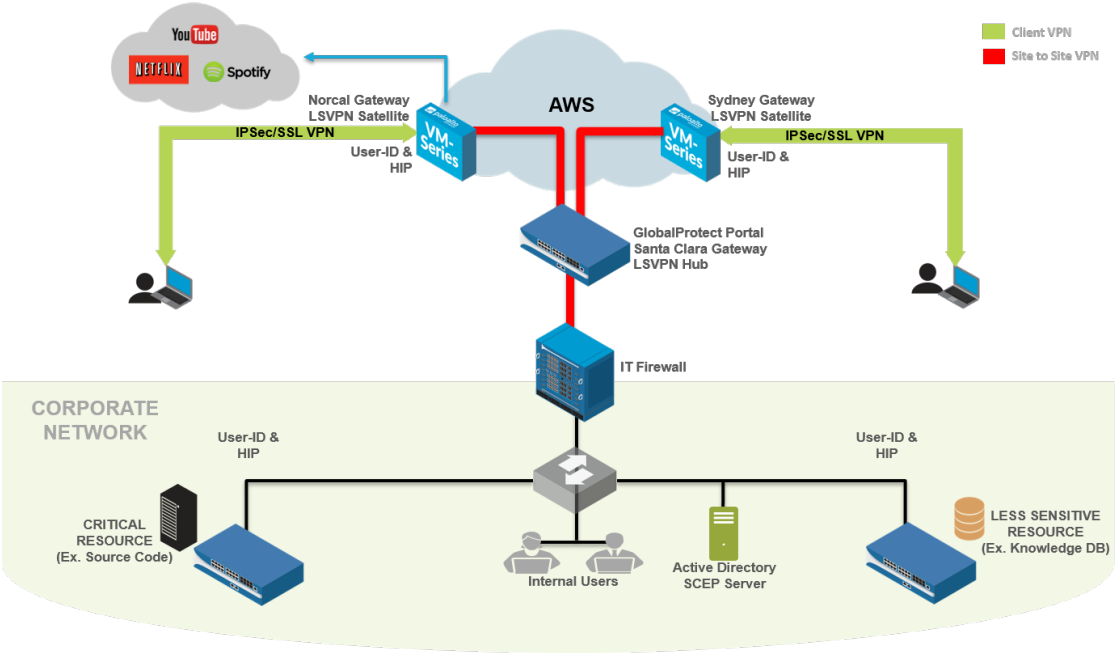
本节概述了用于部署 GlobalProtect™ 以保护 Internet 流量和安全访问公司资源的参考架构示例。

本节中所述的参考架构和指南提供了通用部署场景。在采用此架构之前，请确认公司安全性、基础结构可管理性以及最终用户体验要求，然后基于这些要求部署 GlobalProtect。

尽管这些要求可能因企业而异，但您可利用本文件中所述的通用原则和设计考量以及最佳实践配置指南来满足您的企业安全需求。

> GlobalProtect 参考架构拓扑
> GlobalProtect 参考架构功能
> GlobalProtect 参考架构配置

GlobalProtect 参考架构拓扑



- GlobalProtect 网络门户
- GlobalProtect 网关

GlobalProtect 网络门户

在本拓扑中，主机代管空间中的 PA-3020 作为 GlobalProtect 门户。

员工和承包商可使用由 Active Directory (AD) 和一次性密码 (OTP) 组合的双重身份验证 (2FA) 验证至门户。门户基于用户和组成员资格及操作系统部署 GlobalProtect 客户端配置。

通过配置适用于少部分或一组试用用户的单独门户客户端配置，可在向更广泛的用户群发布之前对功能进行测试。包含新功能（例如 PAN-OS 7.1 提供的强制执行 GlobalProtect 或简单证书注册协议 (SCEP)）的任何客户端配置及随后的内容更新首先在试用配置中启用，然后在向其他用户发布之前由试用用户对其进行验证。

GlobalProtect 门户还向 GlobalProtect 卫星推送配置。该配置包括卫星可连接并建立站点到站点隧道的 GlobalProtect 网关。

GlobalProtect 网关

前述主机代管空间中的 PA-3020 还可用作 GlobalProtect 网关（Santa Clara 网关）。在 Amazon Web 服务 (AWS) 和 Microsoft Azure 公共云中另部署有 10 个网关。部署有这些 AWS 和 Azure 网关的区域或 POP 位置基于全球员工的分布情况。

- **Santa Clara** 网关 — 员工和承包商可使用 2FA 验证至 Santa Clara 网关（主机代管空间中的 PA-3020）。该网关要求用户提供其 Active Directory 凭据和 OTP。由于该网关保护敏感性资源，因而被配置为仅手动网关。所以，用户不会自动连接至该网关，而必须手动选择连接。例如，当用户连接至并非仅手动网关的 AWS-Norcal 时，一些敏感内部资源是不可访问的。如要访问这些资源，用户必须手动切换并认证至 Santa Clara 网关。

© 2019 Palo Alto Networks, Inc.

此外，Santa Clara 网关被配置为来自 AWS 和 Azure 内网关的所有卫星连接的大型 VPN (LSVPN) 隧道终止点。Santa Clara 网关还被配置为设置至公司总部中 IT 防火墙的互联网协议安全 (IPSec) 隧道。通过此隧道可访问公司总部中的资源。

- **Amazon Web** 服务和 **Microsoft Azure** 中的网关 — 此类网关要求 2FA：客户端证书和 Active Directory 凭据。GlobalProtect 门户利用 GlobalProtect SCEP 功能分发此类网关需要验证的客户端证书。

  公共云中的此类网关还用作 GlobalProtect 卫星。它们与 GlobalProtect 门户通信、下载卫星配置并建立与 Santa Clara 网关的站点到站点隧道。GlobalProtect 卫星初次使用序列号进行身份验证，随后使用证书进行身份验证。
- 公司总部内部网关 — 在公司总部内部，三个防火墙用作 GlobalProtect 网关。这些防火墙为内部网关，无需端点设置隧道。用户可使用其 Active Directory 凭据验证至这些网关。这些内部网关使用 GlobalProtect 辨识用户 ID 和从端点收集主机信息配置文件 (HIP)。

要使最终用户尽可能获得无缝体验，可将这些内部网关配置为使用 *SCEP* 提供的证书或使用 *Kerberos* 服务票据对用户进行身份验证。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 参考架构功能

- 最终用户体验
- 管理和日志记录
- 监控和高可用性

最终用户体验

最终用户远程（公司网络外部）连接至 AWS 或 Azure 内网关之一。当配置 GlobalProtect 门户客户端时，为所有网关分配平等优先级。如此，用户连接的网关就取决于每个网关在隧道设置期间的 SSL 响应时间，该响应时间在端点计算。

例如，澳大利亚用户一般会连接至 AWS 悉尼网关。用户连接至 AWS 悉尼网关后，GlobalProtect 应用将端点的所有流量通过隧道传输至 AWS 悉尼防火墙进行检查。GlobalProtect 直接通过 AWS 悉尼网关将流量发送至公共互联网站点，并通过 AWS 悉尼网关与 Santa Clara 网关之间的站点到站点隧道将流量传输至公司资源，然后通过 IPsec 站点到站点隧道传输至公司总部。此架构设计用于减少用户在访问互联网时可能遭遇的任何延迟。如果 AWS 悉尼网关（或较接近悉尼的任何网关）不可及，则 GlobalProtect 应用会将互联网流量回传至公司总部内防火墙，从而导致延迟问题。

Active Directory 服务器驻留在公司网络内部。当远程用户进行远程身份验证时，GlobalProtect 应用通过 AWS/Azure 内的站点到站点隧道将身份验证请求发送至 Santa Clara 网关。然后，此网关通过 IPsec 站点到站点隧道将请求转发至公司总部内的 Active Directory 服务器。

如要缩短远程用户身份验证和隧道设置所花费的时间，可考虑复制 *Active Directory* 服务器并使其在 *AWS* 中可用。

公司网络内部的最终用户在登录后随即认证至三个内部网关。GlobalProtect 应用将 HIP 报告发送至这些内部网关。位于公司网络上的办公室内的用户必须满足用户 ID 和 HIP 要求方可访问任何工作资源。

管理和日志记录

在本部署中，您可利用部署在主机代管空间中的 Panorama 管理和配置所有防火墙。

为提供一致的安全性，AWS 和 Azure 中的所有防火墙使用相同的安全策略和配置。为简化网关配置，Panorama 还使用一个设备组和一个模板。在本部署中，所有网关将全部日志转发到 Panorama。这使您可以监控网络流量或解决中心位置的问题，而无需登录进每个防火墙。

当需要软件更新时，您可使用 Panorama 将软件更新部署至所有防火墙。Panorama 首先升级一个或两个防火墙，并在更新剩余防火墙之前验证升级是否成功。

监控和高可用性

要监控本部署中的防火墙，可使用 Nagios、开源服务器、网络和日志监控软件。将 Nagios 配置为定期验证门户和网关预登录页面的响应，并在响应与期望不符时发送警报。还可配置简单网络管理协议 (SNMP) 管理信息库 (MIB) 来监控网关用途。

在本部署中，仅有一个 GlobalProtect 门户实例。如果门户不可用，新用户（之前从未连接至门户）将无法连接至 GlobalProtect。但是，已有用户可使用缓存的门户客户端配置来连接至其中一个网关。

在 AWS 中被配置为 GlobalProtect 网关的多个虚拟机 (VM) 防火墙提供网关冗余。因此，无需将网关配置为高可用性 (HA) 对。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 参考架构配置

要使您的部署与参考架构一致，请检查下列配置检查表。

- 网关配置
- 门户配置
- 策略配置

网关配置

- 禁用拆分隧道为此，请确保在 **Agent**（代理）> **Client Settings**（客户端设置）> **Split Tunnel**（拆分隧道）设置中未指定访问路由。请参阅配置 GlobalProtect 网关。
- 通过 **Agent**（代理）> **Client Settings**（客户端设置）> **Split Tunnel**（拆分隧道）启用 **No direct access to local network**（不直接访问本地网络）。请参阅配置 GlobalProtect 网关。
- 使网关 **Accept cookie for authentication override**（接受 **Cookie** 以进行身份验证覆盖）。请参阅配置 GlobalProtect 网关。

门户配置

- 将 **Connect Method**（连接方法）配置为 **Always-on (User logon)**（始终启用（用户登录））请参阅自定义 GlobalProtect 应用。
- 设置 **Use Single Sign-On**（使用单点登录（仅限 Windows）为 **Yes**（是）。请参阅自定义 GlobalProtect 应用。
- 将门户配置为 **Save User Credentials**（保存用户凭据）（将值设为 **Yes**（是））。请参阅定义 GlobalProtect 代理配置。
- 使门户**Accept cookie for authentication override**（接受 **Cookie** 以进行身份验证覆盖）。请参阅定义 GlobalProtect 代理配置。
- 将 **Cookie Lifetime**（**Cookie** 生命周期）配置为 20 小时。请参阅定义 GlobalProtect 代理配置。
- 为网络访问 **Enforce GlobalProtect**（强制执行 **GlobalProtect**）。请参阅自定义 GlobalProtect 应用。
- 启用 为网络访问强制执行 **GlobalProtect**时，允许用户使用密码禁用 GlobalProtect 应用。请参阅自定义 GlobalProtect 应用。
- 配置 **Internal Host Detection**（内部主机检测）。请参阅定义 GlobalProtect 代理配置。
- 启用“数据收集”中的 **Collect HIP Data**（收集 **HIP** 数据）选项。请参阅定义 GlobalProtect 代理配置。
- 分发和安装用于 SSL 解密的 SSL 转发代理 CA 证书。请参阅定义 GlobalProtect 代理配置。

策略配置

- 将所有防火墙配置为使用基于最佳做法之互联网网关安全策略的安全策略和配置文件。在本参考部署中，这包括主机代管空间中的 Santa Clara 网关和 AWS/Azure 公共云中的网关。
- 对 AWS 和 Azure 中的所有网关启用 SSL 解密。
- 为 AWS 中的所有网关配置基于策略的转发规则，以通过 Santa Clara 网关将流量转发至特定网站。这确保 www.stubhub.com 和 www.lowes.com 等阻止来自 AWS IP 地址范围的流量的站点在用户连接至 AWS 中的网关时仍是可访问的。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 加密

> 关于 GlobalProtect 密码选择
> GlobalProtect 代理与网关之间的密码交换
> GlobalProtect 加密参考
> 用于建立 IPSec 隧道的密码
> SSL API

关于 GlobalProtect 密码选择

GlobalProtect 支持 IPSec 和 SSL 隧道模式。GlobalProtect 还支持启用并要求 GlobalProtect 应用程序始终先尝试建立 IPSec 隧道，然后回退到 SSL 隧道。通过 IPsec 隧道，GlobalProtect 应用程序使用 SSL/TLS 交换加密以及身份验证算法和密钥。GlobalProtect 用于保护 SSL/TLS 隧道的密码套件的选择取决于：

- 网关接受的 **SSL/TLS** 版本 GlobalProtect 门户和网关可以使用 SSL/TLS 配置文件来限制应用程序可用的密码套件列表。在防火墙上，通过指定证书和允许的协议版本来创建 SSL/TLS 配置文件，并将其与 GlobalProtect 门户和网关相关联。
- 网关的服务器证书算法 — 端点的操作系统确定 GlobalProtect 应用程序在其客户端 Hello 消息中包含的密码套件。只要 GlobalProtect 应用程序包含网关希望使用的密码套件，网关就会为 SSL 会话选择该密码套件。客户端 Hello 消息中密码套件的顺序不影响密码套件选择：网关选择基于 SSL/TLS 服务配置文件和网关服务器证书的算法及其首选列表中的密码套件。您从 GlobalProtect 网关验证配置中选择服务配置文件。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用与网关之间的密码交换

下图显示了创建 VPN 隧道时 GlobalProtect 网关和 GlobalProtect 应用之间的密码交换。

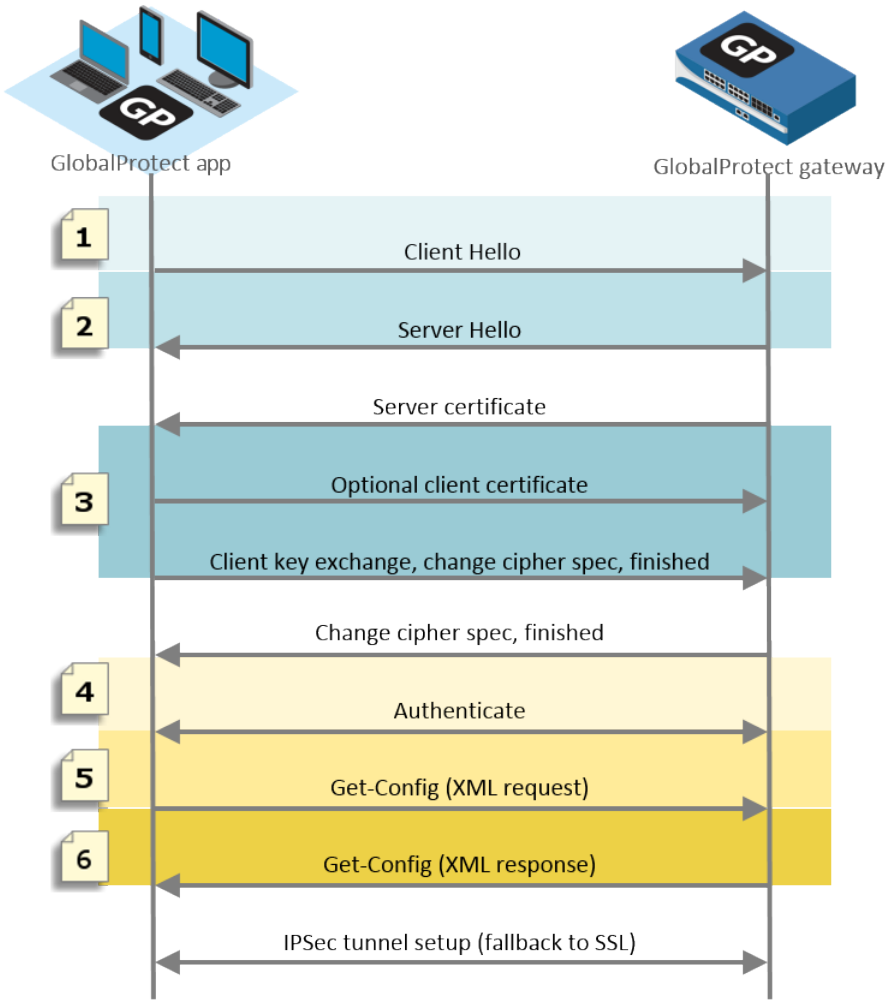


图 **10:** 应用与网关之间的密码交换

下表详细介绍了这些阶段。

表 **9:** 应用与网关之间的密码交换

通信阶段	说明
1 显示动态组定义的两个示例。客户 Hello	应用程序根据端点的操作系统提出一个密码套件列表。
2.服务器 Hello	网关选择应用程序提出的密码套件。当选择密码建立隧道时，网关会忽略应用程序建议的密码套件的数量和顺序，而是依赖网关服务器证书及其首选列表的 SSL/TLS 版本和算法（如关于 GlobalProtect 密码选择所述）。
3。可选客户端证书	网关可以选择请求应用程序的客户端证书以用于信任用户或端点的身份。

© 2019 Palo Alto Networks, Inc.

通信阶段	说明
4。SSL 会话	设置 SSL/TLS 会话后，应用程序将向网关进行身份验证并请求网关配置 (Get-Config-Request)。为了请求配置，应用程序建议加密和身份验证算法以及其他设置，例如隧道接口的首选 IP 地址。网关响应请求并根据 GlobalProtect IPSec 密码配置文件 (Get-Config-Response) 的配置选择要使用的加密和身份验证算法。

下表显示了 macOS 端点上的应用与网关之间密码交换的示例。

表 **10:** 示例：**macOS** 端点的密码交换

通信阶段	示例：macOS 端点
1 显示动态组定义的两个示例。客户 Hello	TLS 1.2 37 个密码套件（参考：macOS 端点上 GlobalProtect 应用支持的 TLS 密码）
2.服务器 Hello	• 当 GlobalProtect 使用 ECDSA 证书并接受 TLS 1.2 时，SSL 会话使用 ECDSA-AES256-CBC-SHA。 • 当 GlobalProtect 使用 RSA 证书并接受 TLS 1.2 时，SSL 会话使用 RSA-AES256-CBC-SHA256。
3。可选客户端证书	使用 ECDSA 或 RSA 签名并使用 SHA1，SHA256 或 SHA384 的客户端证书

4。SSL 会话	• SSL 会话使用 ECDSA-AES256-CBC-SHA或RSA-AES256-CBC-SHA256
	• Get-Config-Request
	  • 加密—AES-256-GCM、AES-128-GCM、AES-128-CBC
	  • 身份验证—SHA1 和 OS 类型、首选 IP 地址等
	• Get-Config-Response
	  • 客户端到服务器、服务器到客户端 SPI、加密密钥和身份验证密钥
	  • 隧道类型、端口、拆分隧道模式、IP 和 DNS 等

© 2019 Palo Alto Networks, Inc.

GlobalProtect 加密参考

- 引用：GlobalProtect 应用加密函数
- GlobalProtect 应用支持的 TLS 密码套件
- GlobalProtect 网关在 PAN-OS 8.1 中支持的 TLS 密码套件

参考资料：GlobalProtect 应用加密函数

GlobalProtect 应用使用 OpenSSL 库 1.0.1h 建立与 GlobalProtect 门户和 GlobalProtect 网关的安全通信。下表列出了需要加密函数的各个 GlobalProtect 应用函数，并介绍了 GlobalProtect 应用使用的加密密钥：

加密函数	密钥	使用情况
Winhttp (Windows) 和 NSURLConnection (macOS) aes256-sha	在 GlobalProtect 应用和 GlobalProtect 门户和/或网关之间为建立 HTTPS 连接协商的动态密钥。	用来在 GlobalProtect 应用和 GlobalProtect 门户与 GlobalProtect 网关之间建立 HTTPS 连接进行身份验证。
OpenSSL aes256-sha	在 SSL 握手期间在 GlobalProtect 应用和 GlobalProtect 网关之间协商的动态密钥。	用来在 GlobalProtect 应用和 GlobalProtect 网关之间建立 SSL 连接以便提交 HIP 报告、协商 SSL 隧道和发现网络。
IPsec 加密和身份验证 aes-128-sha1、aes-128-cbc、aes-128-gcm 和 aes-256-gcm	从 GlobalProtect 网关发送的会话密钥。	用来在 GlobalProtect 应用和 GlobalProtect 网关之间建立 IPSec 隧道。使用网络支持的最强算法（建议采用 AES-GCM）。 为保护数据完整性和真实性，aes-128-cbc 密码要求 SHA1 身份验证算法。由于 AES-GCM 加密算法 (aes-128-gcm 和 aes-256-gcm) 本身提供 ESP 完整性保护，对于这些密码而言，SHA1 身份验证算法将被忽略，即便在配置期间需要。

GlobalProtect 应用支持的 TLS 密码套件

以下部分提供了安装在各种端点操作系统上的 GlobalProtect 应用程序支持的 TLS 密码的示例。这些列表并不是所有支持的操作系统的详尽信息。

- 引用：macOS 端点上 GlobalProtect 代理支持的 TLS 密码
- 引用：Windows 7 端点上 GlobalProtect 代理支持的 TLS 密码
- 引用：Android 6.0.1 端点上由 GlobalProtect 代理支持的 TLS 密码
- 引用：iOS 10.2.1端点上 GlobalProtect 代理支持的 TLS 密码
- 引用：Chromebook 上由 GlobalProtect 代理支持的 TLS 密码

© 2019 Palo Alto Networks, Inc.

参考资料：*macOS* 端点上 *GlobalProtect* 应用支持的 *TLS* 密码

macOS 端点上 GlobalProtect 应用支持的 TLS 密码	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256 (0xc023)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
	TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
	TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
	TLS_RSA_WITH_RC4_128_SHA (0x0005)
	TLS_RSA_WITH_RC4_128_MD5 (0x0004)

参考资料：*Windows 7* 端点上 *GlobalProtect* 应用支持的 *TLS* 密码

Windows 7 端点上 GlobalProtect 应用支持的 TLS 密码	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384 (0xc02c)	

© 2019 Palo Alto Networks, Inc.

Windows 7 端点上 GlobalProtect 应用支持的 TLS 密码	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384 (0xc024)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256 (0xc023)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

参考资料：*Android 6.0.1* 端点上由 *GlobalProtect* 应用支持的 *TLS* 密码

适用于 Android 6.0.1 的 GlobalProtect 应用程序支持 20 个密码套件。

Android 6.0.1 端点上由 GlobalProtect 应用支持的 TLS 密码	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_RC4_128_SHA (0x0005)
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

© 2019 Palo Alto Networks, Inc.

参考资料：*iOS 10.2.1*端点上 *GlobalProtect* 应用支持的 *TLS* 密码

适用于 iOS 10.2.1 的 GlobalProtect 应用支持 19 个密码套件。

iOS 10.2.1端点上 GlobalProtect 应用支持的 TLS 密码	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384 (0xc02c)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384 (0xc024)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256 (0xc023)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

参考资料：*Chromebook* 上由 *GlobalProtect* 应用支持的 *TLS* 密码

适用于 Chrome OS 55.0.2883 的 GlobalProtect 应用程序支持 91 个密码套件。

Chromebook 上的 GlobalProtect 应用支持的 TLS 密码 (Chrome OS 55.0.2883)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0085)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384 (0xc02c)	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_DH_DSS_WITH_AES_256_GCM_SHA384 (0x00a5)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

© 2019 Palo Alto Networks, Inc.

Chromebook 上的 GlobalProtect 应用支持的 TLS 密码 (Chrome OS 55.0.2883)	
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3) TLS_DH_RSA_WITH_AES_256_GCM_SHA384 (0x00a1) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f) TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b) TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a) TLS_DH_RSA_WITH_AES_256_CBC_SHA256 (0x0069) TLS_DH_DSS_WITH_AES_256_CBC_SHA256 (0x0068) TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039) TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038) TLS_DH_RSA_WITH_AES_256_CBC_SHA (0x0037) TLS_DH_DSS_WITH_AES_256_CBC_SHA (0x0036) TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088) TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087) TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0086)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) TLS_DH_DSS_WITH_AES_128_GCM_SHA256 (0x00a4) TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2) TLS_DH_RSA_WITH_AES_128_GCM_SHA256 (0x00a0) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067) TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040) TLS_DH_RSA_WITH_AES_128_CBC_SHA256 (0x003f) TLS_DH_DSS_WITH_AES_128_CBC_SHA256 (0x003e) TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033) TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032) TLS_DH_RSA_WITH_AES_128_CBC_SHA (0x0031) TLS_DH_DSS_WITH_AES_128_CBC_SHA (0x0030) TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a) TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099) TLS_DH_RSA_WITH_SEED_CBC_SHA (0x0098) TLS_DH_DSS_WITH_SEED_CBC_SHA (0x0097)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) TLS_RSA_WITH_SEED_CBC_SHA (0x0096) TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041) TLS_RSA_WITH_IDEA_CBC_SHA (0x0007) TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007) TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c) TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002) TLS_RSA_WITH_RC4_128_SHA (0x0005) TLS_RSA_WITH_RC4_128_MD5 (0x0004) TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)

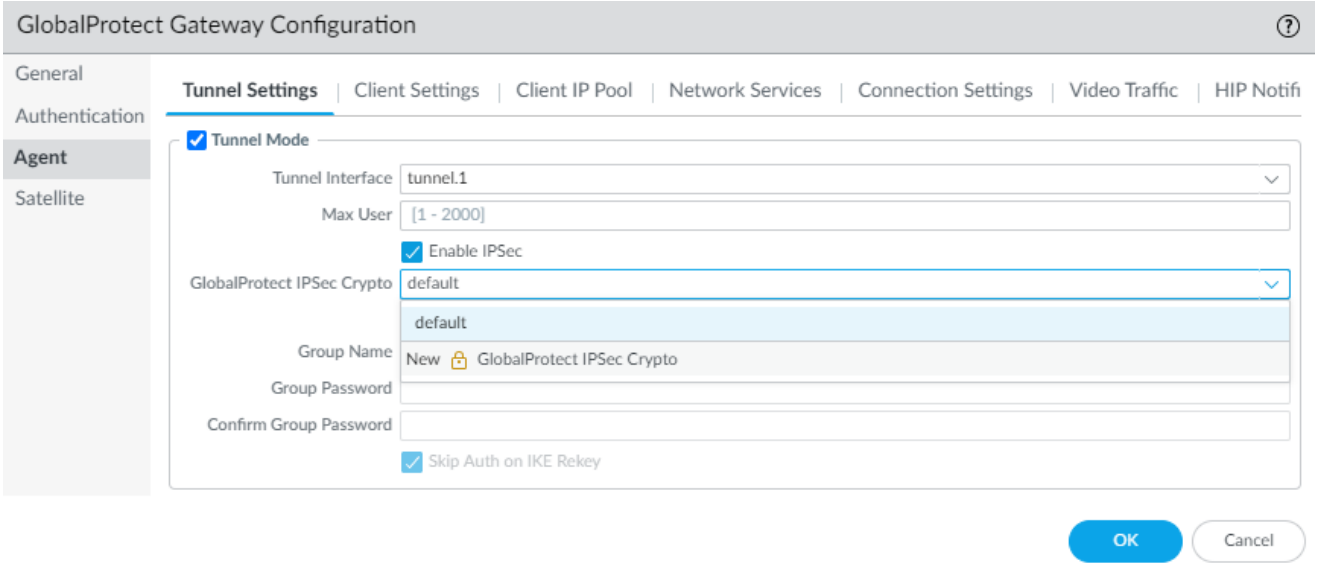
© 2019 Palo Alto Networks, Inc.

Chromebook 上的 GlobalProtect 应用支持的 TLS 密码 (Chrome OS 55.0.2883)	
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0044)	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0043)	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA (0x0010)
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0042)	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA (0x000d)
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)	TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)	TLS_DH_RSA_WITH_DES_CBC_SHA (0x000f)
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)	TLS_DH_DSS_WITH_DES_CBC_SHA (0x000c)
	TLS_RSA_WITH_DES_CBC_SHA (0x0009)
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

© 2019 Palo Alto Networks, Inc.

用于建立 IPsec 隧道的密码

GlobalProtect 可以限制和/或设置 GlobalProtect 应用可用于 IPsec 隧道的加密和身份验证算法的优先顺序。当您为 GlobalProtect 网关设置隧道时，可在配置的 **GlobalProtect IPSec Crypto**（**GlobalProtect IPSec** 加密）配置文件中定义算法和首选项（**Network**（网络）> **GlobalProtect** > **Gateways**（网关）> **<gateway-config>** > **GlobalProtect Gateway Configuration**（**GlobalProtect** 网关配置）> **Agent**（代理）> **Tunnel Settings**（隧道设置））。



当 GlobalProtect 应用通过 GlobalProtect 网关设置 SSL 会话时，用于此 SSL 会话的密码套件由网关上配置的 SSL/TLS 配置文件以及网关证书使用的算法类型管理。建立 SSL 会话之后，GlobalProtect 应用通过请求通过 SSL 进行配置来启动 VPN 隧道设置。

使用相同的 SSL 会话，GlobalProtect 网关会响应应用程序应使用的加密和身份验证算法、密钥和 SPI 来设置 IPsec 隧道。

建议使用 *AES-GCM* 以满足更安全的要求。为保护数据完整性和真实性，*aes-128-cbc* 密码要求 *SHA1* 身份验证算法。由于 *AES-GCM* 加密算法*(aes-128-gcm* 和 *aes-256-gcm)*本身提供 *ESP* 完整性保护，对于这些密码而言，*SHA1* 身份验证算法将被忽略，即便在配置期间需要。

您在网关上配置的 **GlobalProtect IPSec Crypto**（**GlobalProtect IPSec** 加密）配置文件决定用于设置 IPsec 隧道的加密和身份验证算法。GlobalProtect 网关使用配置文件中列出的匹配应用建议的第一个匹配加密算法进行响应。

然后，GlobalProtect 应用将尝试根据网关的响应建立隧道。

© 2019 Palo Alto Networks, Inc.

SSL API

GlobalProtect 使用 OpenSSL 和本地系统 API 来执行 SSL 握手。GlobalProtect 网关延迟测量（GlobalProtect 用于选择最佳网关）、网关注销以及发送 HIP 检查消息和报告传输等操作均通过使用 OpenSSL 库设置的 SSL 会话执行。网关预登录、登录和 get-config 之类的操作都是通过使用本地系统 API 设置的 SSL 会话完成的。