



通过强制网络门户的用户控制

- [强制网络门户身份源](#)，第 1 页
- [关于主机名重定向](#)，第 2 页
- [强制网络门户的许可证要求](#)，第 2 页
- [强制网络门户的要求和必备条件](#)，第 2 页
- [强制网络门户指南和限制](#)，第 2 页
- [如果为用户控制配置强制网络门户](#)，第 5 页
- [强制网络门户身份源故障排除](#)，第 16 页
- [强制网络门户的历史](#)，第 17 页

强制网络门户身份源

强制网络门户是系统支持的授权身份源之一。强制网络门户是一种主动身份验证方法，其中用户可以使用受管设备验证网络登录。

通常使用强制网络门户要求身份验证访问互联网，或者访问受限制的内部资源；可以选择配置对资源的访客访问。在系统对强制网络门户用户进行身份验证后，会根据访问控制规则处理其用户流量。强制网络门户仅会对 HTTP 和 HTTPS 流量执行身份验证。



注释 必须先对 HTTPS 流量进行加密，然后强制网络门户才能执行身份验证。

强制网络门户还记录失败的身份验证尝试。如果尝试失败，则不会将新用户添加到数据库的用户列表中。强制网络门户报告的身份验证活动失败的用户活动类型是**身份验证失败的用户 (Failed Auth User)**。

从强制网络门户获取的身份验证数据可用于用户感知和用户控制。

相关主题

[如果为用户控制配置强制网络门户](#)，第 5 页

关于主机名重定向

(仅限 Snort 3。)主动身份验证身份规则会使用其配置的接口重定向到强制网络门户端口。由于重定向通常是指向 IP 地址，因此用户会收到不受信任的证书错误，并且由于此行为类似于中间人攻击，因此用户可能不愿意接受不受信任的证书。

为避免此问题，您可以将强制网络门户配置为使用完全限定域名(FQDN)。使用正确配置的证书时，用户不会收到不受信任的证书错误，并且身份验证将更加无缝，且看起来更加安全。

相关主题

[重定向到主机名网络规则条件](#)

强制网络门户的许可证要求

威胁防御 许可证

Any

经典许可证

控制

强制网络门户的要求和必备条件

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

强制网络门户指南和限制

在身份策略中配置和部署强制网络门户时，来自指定领域的用户会使用威胁防御来进行身份验证，以访问您的网络。



注释 如果远程接入 VPN 用户已通过作为安全网关的受管设备进行主动身份验证，则不会执行强制网络门户主动身份验证，即便身份策略中配置了该验证方式。

需要路由接口

只有配置了路由接口的设备，才能执行强制网络门户主动身份验证。如果要为强制网络门户配置规则，并且您的强制网络门户设备包含内联接口和路由接口，则必须在访问控制策略中配置接口规则条件，以便仅针对设备上的路由接口。

如果访问控制策略引用的身份策略包含一个或多个强制网络门户身份规则，并且您在管理一个或多个配置了路由接口的设备的管理中心上部署策略，则策略部署成功且路由接口执行主动身份验证。

强制网络门户和策略

在身份策略中配置强制网络门户并在身份规则中调用主动身份验证。身份策略与访问控制策略相关联。

您可以在访问控制策略的**主动身份验证**选项卡页面上配置一些强制网络门户身份策略设置，并在与访问控制策略关联的身份规则中配置其余部分。

主动身份验证规则具有**主动身份验证规则操作**或**被动身份验证规则操作**，并且如果无法建立**被动或 VPN 识别**，则使用**主动身份验证**已选中。不管上述哪种情况，系统都会透明地启用或禁用 TLS/SSL 解密，从而重启 Snort 进程。



注意 在禁用了 TLS/SSL 解密（即，当访问控制策略不包括 **an SSL 策略** 时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅[Snort 重启流量行为](#)。

当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何 Microsoft 用户都将被识别为“未知”。为避免用户被识别为未知，请将领域配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

要确保系统下载领域中的所有用户，请确保组位于领域配置的可用组列表中。

有关同步用户和组的详细信息，请参阅[同步用户和组](#)。

强制网络门户要求和限制

请注意以下要求和限制：

- 系统每秒最多支持 20 次强制网络门户登录。
- 对于计入最大登录尝试次数的失败登录尝试，失败登录尝试之间存在最长五分钟的时间限制。该五分钟限制不可配置。

（最大登录尝试次数显示在连接事件中：[分析 > 连接 > 事件](#)。）

如果失败登录之间的间隔时间超过五分钟，则用户将被重定向到强制网络门户进行身份验证，而不会被指定为登录失败的用户或访客用户，也不会报告给管理中心。

- 强制网络门户不会协商 TLS v1.0 连接。
仅支持 TLS v1.1、v1.2 和 TLS 1.3 连接。
- 您不能对强制网络门户使用领域序列。
- 确保用户注销的唯一方法是关闭并重新打开浏览器。除非发生这种情况，否则在某些情况下，用户可以注销强制网络门户，并且能够在不使用同一浏览器再次进行身份验证的情况下访问网络。
- 如果为父域创建了领域，并且受管设备检测到有用户登录到该父域的子域，则受管设备不会检测用户的后续注销。
- 必须允许流量流向计划用于强制网络门户的设备的 IP 地址和端口。
- 要对 HTTPS 流量执行强制网络门户主动身份验证，必须使用 **an SSL** 策略解密来自要对其进行身份验证的用户的流量。您无法解密受管设备上强制网络门户用户的 Web 浏览器和强制网络门户后台守护程序之间的连接中的流量；此连接用于对强制网络门户用户进行身份验证。
- 要限制允许流经受管设备的非 HTTP 或 HTTPS 流量的量，您应在身份策略的 **端口** 选项卡页面中输入典型的 HTTP 和 HTTPS 端口。

受管设备在确定传入请求未使用 HTTP 或 HTTPS 协议时，会将先前未发现的用户从 **待定** 更改为 **未知**。受管设备将用户从 **待定** 状态更改为其他状态之后，访问控制、服务质量和 SSL 策略便可以应用到该流量。如果您的其他策略不允许非 HTTP 或 HTTPS 流量，则在强制网络门户身份策略上配置端口可以防止允许不需要的流量流经受管设备。

- 当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何 Microsoft 用户都将被识别为“未知”。为避免用户被识别为未知，请将领域配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

要确保系统下载领域中的所有用户，请确保组位于领域配置的可用组列表中。

有关详细信息，请参阅[同步用户和组](#)。

Kerberos 必备条件

如果使用 Kerberos 身份验证，则受管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置受管设备主机名。有关详细信息，请参阅 Microsoft 文档网站上的此类文章：[Active Directory 中计算机、域、站点和 OU 的命名约定](#)。

DNS 必须向主机名返回 64KB 或更少的响应；否则，测试连接 AD 连接失败。此限制在两个方向上都适用，将在 [RFC 6891 第 6.2.5 节](#)中讨论。

如果为用户控制配置强制网络门户

开始之前

要使用强制网络门户进行主动身份验证，必须设置一个 Microsoft AD 或 LDAP 领域（但非领域序列）、访问控制策略、一个身份策略、一个 an SSL 策略，并将身份和 SSL 策略与访问控制策略关联。最后，必须将这些策略部署到受管设备。此主题介绍这些任务的高度概要。

例如，整个过程从[配置强制网络门户第 1 部分：创建网络主体](#)，第 6 页开始。

首先，请执行以下任务：

- 确认您的管理中心使用已配置的路由接口管理一台或多台设备。
- 要将加密身份验证用于强制网络门户，要么创建一个 PKI 对象，要么使证书数据和密钥可在用于访问管理中心的机器上使用。要创建 PKI 对象，请参阅[PKI](#)。

过程

步骤 1 按照以下主题中所述，创建并启用 Microsoft AD 领域：

- [创建 Active Directory 领域和领域目录](#)
- [同步用户和组](#)

强制网络门户不支持领域序列。

当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何 Microsoft 用户都将被识别为“未知”。为避免用户被识别为未知，请将领域配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

要确保系统下载领域中的所有用户，请确保组位于领域配置的可用组列表中。

有关详细信息，请参阅[同步用户和组](#)。

步骤 2（可选。）要将强制网络门户重定向到主机而不是 IP 地址，请创建具有关联的受信任证书颁发机构的网络对象。

请参阅[配置强制网络门户第 1 部分：创建网络主体](#)，第 6 页

步骤 3 为强制网络门户创建包含主动身份验证规则的身份策略。

在使用强制网络门户执行身份验证后，该身份策略将在您的领域访问资源内启用所选用户。

有关详细信息，请参阅[配置强制网络门户第 2 部分：创建身份策略](#)，第 8 页。

步骤 4 为强制网络门户配置允许强制网络门户端口（默认情况下为 TCP 885）上的流量的访问控制规则。

您可以为要使用的强制网络门户选择任何可用的 TCP 端口。无论选择哪个端口，都必须创建一条允许该端口上的流量的规则。

有关详细信息，请参阅[配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则](#)，第 10 页。

步骤 5 再添加一条访问控制规则，以允许所选领域中的用户使用强制网络门户访问资源。

这样，用户可使用强制网络门户进行身份验证。

有关详细信息，请参阅[配置强制网络门户第 4 部分：创建用户访问控制规则](#)，第 11 页。

步骤 6 为未知用户配置 an SSL 策略 策略和解密 - 重签策略，以使强制网络门户用户能够使用 HTTPS 协议访问网页。

仅当 HTTPS 流量在流量发送到强制网络门户之前被解密的情况下，强制网络门户才能进行用户身份验证。系统将强制网络门户视为未知用户。

有关详细信息，请参阅[配置强制网络门户第 5 部分：创建 TLS/SSL 解密-重签策略](#)，第 12 页。

步骤 7 将身份和 SSL 策略 与第 3 步的访问控制策略相关联。

这是最后一步，此后系统即可使用强制网络门户进行用户身份验证。

有关详细信息，请参阅[配置强制网络门户第 6 部分：将身份和 SSL 策略 与访问控制策略关联起来](#)，第 13 页。

下一步做什么

请参阅[配置强制网络门户第 1 部分：创建网络主体](#)，第 6 页。

相关主题

[排除强制网络门户中的应用](#)，第 15 页

[PKI](#)

[强制网络门户身份源故障排除](#)，第 16 页

[Snort 重新启动场景](#)

配置强制网络门户第 1 部分：创建网络主体

此任务讨论如何开始将强制网络门户配置为身份源。

威胁防御 功能历史记录：

- 7.1- 您可以选择将强制网络门户身份验证请求重定向到完全限定域名。

开始之前

（仅限 Snort 3。）此任务是可选的。使用 DNS 服务器创建完全限定的主机名（FQDN）。如果您之前从未使用过例如 [此类](#) 资源，可以咨询此类资源。在 管理中心的其中一个受管服务器上指定路由接口的 IP 地址。

有关网络对象的详细信息，请参阅 [重定向到主机名网络规则条件](#)。

过程

- 步骤 1 如果尚未这样子，请登录 管理中心。
- 步骤 2 请点击 **对象 > 对象管理**。
- 步骤 3 展开 **PKI**。
- 步骤 4 点击 **内部证书**。
- 步骤 5 点击 **Add Internal Cert**。
- 步骤 6 在 **名称** 字段中，输入名称以标识受信任 CA（例如，**MyCaptivePortal**）。
- 步骤 7 在 **证书数据** 字段中，粘贴证书或使用 **浏览** 按钮查找证书。
证书公用名必须与您想要强制网络门户用户进行身份验证的 FDQN 完全匹配。
- 步骤 8 在 **密钥** 字段中，粘贴证书的私钥或使用 **浏览** 按钮查找证书。
- 步骤 9 如果证书已加密，请选中 **已加密** 复选框并在相邻字段中输入密码。
- 步骤 10 点击 **保存 (Save)**。
- 步骤 11 点击 **网络 (Network)**。
- 步骤 12 从页面顶部的列表中，点击 **添加对象**。
- 步骤 13 在 **名称** 字段中，输入名称以标识对象（例如，**MyCaptivePortalNetwork**）。
- 步骤 14 点击 **FDQN**，然后在字段中输入强制网络门户的 FDQN 的名称。
- 步骤 15 点击 **查找选项**。

下图显示了一个示例。

New Network Object ?

Name

Description

Network
 Host Range Network FQDN

Note:
You can use FQDN network objects in access, prefilter and translated destination in NAT rules only.

Lookup:

Allow Overrides

步骤 16 点击保存 (Save)。

下一步做什么

[配置强制网络门户第 2 部分：创建身份策略，第 8 页](#)

配置强制网络门户第 2 部分：创建身份策略

开始之前

此由多个部分组成的程序展示如何使用默认 TCP 端口 885 以及将 管理中心 服务器证书用于强制网络门户和 TLS/SSL 解密来设置强制网络门户。本示例中的每个部分介绍启用强制网络门户来执行主动身份验证所需的一项任务。

如果您遵循此程序中的所有步骤，则可以将强制网络门户配置为供您的域中的用户使用。您可以选择执行在程序的各个部分中介绍的其他任务。

有关完整程序的概述，请参阅[如果为用户控制配置强制网络门户，第 5 页](#)。

过程

步骤 1 如果尚未登录, 请登录 管理中心。

步骤 2 依次点击策略 > 访问控制 > 身份, 然后创建或编辑身份策略。

步骤 3 (可选。) 点击添加类别, 为强制网络门户身份规则添加类别, 然后为该类别输入一个名称。

步骤 4 点击主动身份验证 (Active Authentication)。

步骤 5 从列表中选择适当的 服务器证书, 或者点击 添加 (+) 以添加证书。

注释 强制网络门户 不支持使用数字签名算法 (DSA) 或椭圆曲线数字签名算法 (ECDSA) 证书。

步骤 6 从 重定向到主机名 字段中, 点击之前创建的网络对象。

步骤 7 在端口字段中输入 885, 然后指定最大登录尝试次数。

步骤 8 (可选。) 选择主动身份验证响应页面, 如强制网络门户字段, 第 14 页中所述。

下图显示了一个示例。

Rules	Active Authentication	Identity Source
Server Certificate *	<input type="text" value="CaptivePortalCert"/>	+
Redirect to Host Name ⓘ	<input type="text" value="CaptivePortalNetwork"/>	+ ▲ Supported only in Snort 3.0 and above.
Port *	<input type="text" value="885"/>	(885 or 1025 - 65535)
Maximum login attempts *	<input type="text" value="3"/>	(0 or greater. Use 0 to indicate unlimited login attempts)

Active Authentication Response Page

This page will be displayed if a user triggers an identity rule with HTTP Response Page as the Authentication Type.

* Required when using Active Authentication

步骤 9 点击保存 (Save)。

步骤 10 点击规则 (Rules)。

步骤 11 点击 添加规则 以添加新的强制网络门户身份策略规则, 或者点击 编辑 (✎) 以编辑现有规则。

步骤 12 为规则输入名称 (Name)。

步骤 13 从操作列表中, 选择主动身份验证。

步骤 14 点击 领域和设置。

步骤 15 从领域 (Realms) 列表中, 选择要用于用户身份验证的领域。

不支持领域序列。

步骤 16 (可选。) 选中如果身份验证无法识别用户, 则识别为访客。有关详细信息, 请参阅强制网络门户字段, 第 14 页。

步骤 17 从列表中选择身份验证协议。

步骤 18 (可选。) 要豁免强制网络门户中的特定应用流量, 请参阅排除强制网络门户中的应用, 第 15 页。

- 步骤 19 向规则（端口、网络等）添加条件，如[身份规则条件](#)中所述。
- 步骤 20 点击 **Add**。
- 步骤 21 在该页面顶部，点击**保存**。

下一步做什么

继续执行[配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则](#)，第 10 页。

配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则

该程序的这一部分显示如何创建访问控制规则，以允许强制网络门户使用 TCP 端口 885（它是强制网络门户的默认端口）与客户端通信。如果您希望，也可以选择另一个端口，但该端口必须与您在[配置强制网络门户第 2 部分：创建身份策略](#)，第 8 页中选择的端口匹配。

开始之前

有关整个强制网络门户配置的概述，请参阅[如果为用户控制配置强制网络门户](#)，第 5 页。

过程

- 步骤 1 如果尚未登录，请登录 [管理中心](#)。
- 步骤 2 如果尚未进行此操作，则请创建强制网络门户证书，如[PKI](#)中所述。
- 步骤 3 依次点击 [策略](#) > [访问控制](#) > [访问控制](#) 然后创建或编辑访问控制策略。
- 步骤 4 点击**添加规则**。
- 步骤 5 为规则输入名称 (**Name**)。
- 步骤 6 从操作列表中选择**允许**。
- 步骤 7 点击**端口**。
- 步骤 8 从所选目标端口字段下的协议列表中，选择 **TCP**。
- 步骤 9 在端口字段中，输入 **885**。
- 步骤 10 点击端口字段旁边的**添加**。
下图显示了一个示例。

The screenshot shows the 'Add Rule' configuration page. The 'Name' field is 'Captive portal rule', 'Action' is 'Allow', and 'Time Range' is 'None'. The 'Ports' tab is selected, showing a list of available ports (AOL, Bittorrent, DNS_over_TCP, DNS_over_UDP, FTP, HTTP, HTTPS, IMAP) and two empty boxes for 'Selected Source Ports' and 'Selected Destination Ports'. At the bottom, the 'Protocol' is set to 'TCP (6)' and the 'Port' field contains '885', with an 'Add' button highlighted by a red circle.

步骤 11 点击页面底部的添加。

下一步做什么

继续执行[配置强制网络门户第 4 部分：创建用户访问控制规则](#)，第 11 页。

配置强制网络门户第 4 部分：创建用户访问控制规则

该过程的此部分讨论如何添加访问控制规则，以使领域中的用户能够使用强制网络门户进行身份验证。

开始之前

有关整个强制网络门户配置的概述，请参阅[如果为用户控制配置强制网络门户](#)，第 5 页。

过程

- 步骤 1** 在规则编辑器中，点击添加规则。
- 步骤 2** 为规则输入名称 (Name)。
- 步骤 3** 从操作列表中选择允许。
- 步骤 4** 点击“用户”。
- 步骤 5** 在可用领域列表中，点击要允许的领域。
- 步骤 6** 如果没有显示领域，则请点击刷新 (🔄)。
- 步骤 7** 在可用用户列表中，选择要添加到规则的用户，然后点击添加到规则。

- 步骤 8** (可选。) 向访问控制策略添加条件，如[身份规则条件](#)中所述。
- 步骤 9** 点击 **Add**。
- 步骤 10** 在访问控制规则页面上，点击**保存**。
- 步骤 11** 在策略编辑器中，设置规则位置。点击并拖动，或使用右键点击菜单剪切并粘贴。规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。流量匹配的第一条规则是处理该流量的规则。适当的规则顺序可减少处理网络流量所需的资源，并防止规则抢占。

下一步做什么

继续执行[配置强制网络门户第 5 部分：创建 TLS/SSL 解密-重签策略](#)，第 12 页。

配置强制网络门户第 5 部分：创建 TLS/SSL 解密-重签策略

程序的此部分介绍如何创建 an SSL 策略，以在流量到达强制网络门户之前解密和重签流量。强制网络门户仅可对解密的流量进行身份验证。

开始之前

有关整个强制网络门户配置的概述，请参阅[如果为用户控制配置强制网络门户](#)，第 5 页。

过程

- 步骤 1** 如果尚未登录，请登录 [管理中心](#)。
- 步骤 2** 如果尚未进行此操作，则请创建证书对象，以 TLS/SSL 流量进行解密，如 [PKI](#)中所述。
- 步骤 3** 依次点击 **策略 (Policies) > 访问控制 (Access Control) > SSL策略 > 访问控制 > SSL**。
- 步骤 4** 点击新建策略。
- 步骤 5** 为策略输入名称，然后选择默认操作。默认操作将在[SSL 策略 默认操作](#)中讨论。
- 步骤 6** 点击**保存 (Save)**。
- 步骤 7** 点击添加规则。
- 步骤 8** 为规则输入名称 (**Name**)。
- 步骤 9** 从操作列表中，选择解密 - 放弃。
- 步骤 10** 从使用列表中，选择 PKI 对象。
- 步骤 11** 点击“用户”。
- 步骤 12** 在可用领域列表上方，点击刷新 (🔄)。
- 步骤 13** 在可用领域列表中，点击特殊身份。
- 步骤 14** 在可用用户列表中，点击未知。
- 步骤 15** 点击添加至规则。

下图显示了一个示例。

步骤 16 （可选。）设置其他选项，如[TLS/SSL 规则 条件](#)中所述。

步骤 17 点击 **Add**。

步骤 18 在该页面顶部，点击**保存**。

下一步做什么

继续执行[配置强制网络门户第 6 部分：将身份和 SSL 策略与访问控制策略关联起来](#)，第 13 页。


配置强制网络门户第 6 部分：将身份和 SSL 策略与访问控制策略关联起来

该程序的这一部分讨论如何将身份策略和 TLS/SSL 解密 - 重新签名规则与您先前创建的访问控制规则关联起来。在此之后，用户可以使用强制网络门户进行身份验证。

开始之前

有关整个强制网络门户配置的概述，请参阅[如果为用户控制配置强制网络门户](#)，第 5 页。

过程

步骤 1 点击策略 > 访问控制 > 访问控制，然后按照[配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则](#)，第 10 页中所述编辑您创建的访问控制策略。如果显示视图（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 2 创建新的访问控制策略，或者编辑现有策略。

步骤 3 在该页面顶部，点击**身份策略**旁边的链接。

步骤 4 从该列表中，选择身份策略的名称，然后在该页面顶部，点击**保存**。

步骤 5 重复前面的步骤，以使强制网络门户 SSL 策略与访问控制策略相关联。

步骤 6 如果尚未进行此操作，则请将受管设备作为该策略的目标，如[设置访问控制策略的目标设备](#)中所述。

下一步做什么

- 将身份和访问控制策略部署到受管设备，如[部署配置更改](#)中所述。
- 监控用户活动，如《[Cisco Secure Firewall Management Center 管理指南](#)》中使用工作流程所述。

强制网络门户字段

使用以下字段，在身份策略的**主动身份验证**选项卡页面上配置强制网络门户设置。另请参阅[身份规则字段](#)和[排除强制网络门户中的应用](#)，第 15 页。

服务器证书 (Server Certificate)

强制网络门户后台守护程序显示的内部证书。



注释 强制网络门户 不支持使用数字签名算法 (DSA) 或椭圆曲线数字签名算法 (ECDSA) 证书。

端口

要用于强制网络门户连接的端口号。您必须使用 TCP 端口来设置访问控制规则，以便用于强制网络门户，然后将身份策略与该访问控制策略相关联。有关详细信息，请参阅[配置强制网络门户第 3 部分：创建 TCP 端口访问控制规则](#)，第 10 页。

最大登录尝试次数 (Maximum login attempts)

系统拒绝用户登录请求前允许的最大失败登录尝试的次数。

跨防火墙共享主动身份验证会话

选中此复选框可在访问控制策略与此身份策略关联的受管设备之间共享会话。

主动身份验证响应页面 (Active Authentication Response Page)

要向强制网络门户用户显示的系统提供或自定义 HTTP 响应页面。在身份策略主动身份验证设置中选择**主动身份验证响应页面**后，还必须使用**HTTP 响应页面**配置一个或更多个身份规则作为**身份验证协议**。

系统提供的 HTTP 响应页面包括**用户名 (Username)** 和**密码 (Password)** 字段，以及用于允许用户以访客身份访问网络的**以访客身份登录 (Login as guest)** 按钮。要显示单点登录方法，请配置自定义 HTTP 响应页面。

选择以下选项：

- 要使用通用响应，请选择**系统提供**。可以点击 **视图** (👁) 以查看此页面的 HTML 代码。
- 要创建自定义响应，请选择**自定义**。将显示一个具有系统提供的代码的窗口，您可以替换或修改该代码。完成时，保存更改。可以通过点击 **编辑** (✎) 来编辑自定义页面。

相关主题

[内部证书对象](#)

排除强制网络门户中的应用

您可以选择应用（通过其 HTTP 用户-代理 字符串标识）并免于对它们执行强制网络门户主动身份验证。这允许所选应用的流量在未经身份验证的情况下通过身份策略。



注释 此列表中仅显示带有用户代理排除标记的应用。

过程

步骤 1 如果尚未登录，请登录 **管理中心**。

步骤 2 请点击 **策略 > 访问控制 > 身份**。

步骤 3 编辑包含强制网络门户规则的身份策略。

步骤 4 在 **领域和设置** 选项卡页面上，展开 **HTTP 用户代理排除**。

- 在第一列中，选中要过滤应用的每个项目旁边的复选框，然后选择一个或多个应用，然后点击 **添加到规则**。

复选框与 ANDed 在一起。

- 要减少显示的过滤器，请在 **按名称搜索** 字段中键入搜索字符串；这对类别和标记尤其有用。要清除搜索，请点击 **清除** (X)。
- 要刷新过滤器列表并清除所有所选过滤器，请点击 **重新加载** (C)。

注释 该列表每次显示 100 个应用。

步骤 5 从可用应用列表中选择要添加到过滤器的应用：

- 要减少显示的应用，请在 **按名称搜索** 字段中输入搜索字符串。要清除搜索，请点击 **清除** (X)。
- 使用位于列表底部的页码可浏览各个可用应用的列表。
- 要刷新应用列表并清除所有所选应用，请点击 **重新加载** (C)。

步骤 6 添加所选应用以免除外部身份验证。可以点击并拖动，也可以点击添加到规则 (**Add to Rule**)。由此则得到您所选的应用过滤器组合。

下一步做什么

- 继续配置身份规则，如[创建身份规则](#)中所述。

强制网络门户身份源故障排除

有关其他相关故障排除信息，请参阅[领域和用户下载故障排除](#)和[用户控制故障排除](#)。

如果您遇到强制网络门户证问题，请检查以下事项：

- 强制网络门户托管设备上的时间必须与管理中心上的时间同步。
- 如果您已配置 DNS 解析并创建了身份规则来执行 **Kerberos**（或 **HTTP** 协商，如果希望 Kerberos 作为选项）强制网络门户，则必须配置 DNS 服务器来解析强制网络门户设备的完全限定域名 (FQDN)。FQDN 必须与您配置 DNS 时提供的主机名匹配。
有关详细信息，请参阅[关于主机名重定向](#)，第 2 页。
- 如果使用 Kerberos 身份验证，则受管设备的主机名必须少于 15 个字符（这是 Windows 设置的 NetBIOS 限制）；否则，强制网络门户身份验证失败。您在设置设备时设置受管设备主机名。
有关详细信息，请参阅 Microsoft 文档网站上的此类文章：[Active Directory 中计算机、域、站点和 OU 的命名约定](#)。
- DNS 必须向主机名返回 64KB 或更少的响应；否则，测试连接 AD 连接失败。此限制在两个方向上都适用，将在 [RFC 6891 第 6.2.5 节](#)中讨论。
- 如果强制网络门户配置正确，但重定向到 IP 地址或完全限定域名 (FQDN) 失败，请禁用终端安全软件。此类软件可能会干扰重定向。
- 如果您选择 **Kerberos**（或 **HTTP** 协商，如果您要将 Kerberos 作为一个选项）作为身份规则的身份验证类型，则您选择的领域必须配置 **AD 加入用户名** 和 **AD 加入密码**，以便执行 Kerberos 强制网络门户主动身份验证。
- 如果选择 **HTTP 基本身份验证** 作为身份规则中的身份验证类型，则您的网络上的用户可能不会注意到其会话超时。大多数 Web 浏览器会从 HTTP 基本身份验证登录中缓存凭证，并在旧会话超时后使用这些凭证无缝开始新会话。
- 如果您的管理中心和受管设备之间的连接失败，则无法在停机期间识别设备报告的所有强制网络门户登录，除非以前查看过这些用户并已将他们下载到管理中心。无法识别的用户在管理中心上记录为“未知”(Unknown) 未知用户。停机时间过后，系统将根据身份策略中的规则重新识别和处理“未知”(Unknown) 用户。
- 如果要用于强制网络门户的设备包含内联接口和路由接口，则必须在强制网络门户身份规则中配置区域条件，以便仅针对强制网络门户设备上的路由接口。

- 受管设备的主机名必须少于 15 个字符，Kerberos 身份验证才能成功。
- 确保用户注销的唯一方法是关闭并重新打开浏览器。除非发生这种情况，否则在某些情况下，用户可以注销强制网络门户，并且能够在不使用同一浏览器再次进行身份验证的情况下访问网络。
- 活动 FTP 会话在事件中显示为 **Unknown** 用户。此为正常现象，因为在活动 FTP 中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关活动 FTP 的详细信息，请参阅 [RFC 959](#)。
- 当强制网络门户对与身份规则匹配的用户进行身份验证时，Active Directory 或 LDAP 组中尚未下载的任何 Microsoft 用户都将被识别为“未知”。为避免用户被识别为未知，请将领域配置为下载您希望通过强制网络门户进行身份验证的所有组中的用户。未知用户根据关联的访问控制策略处理；如果访问控制策略配置为阻止未知用户，则会阻止这些用户。

要确保系统下载领域中的所有用户，请确保组位于领域配置的可用组列表中。

有关详细信息，请参阅[同步用户和组](#)。

强制网络门户的历史

特性	Version	详细信息
主机名重定向	7.1.0	（仅限 Snort3）—你可以使用一个网络对象，其中包含强制网络门户可用于主动认证请求的接口的完全限定主机名（FQDN）。
访客登录。	6.1.0	用户可以使用强制网络门户以访客身份登录。
强制网络门户。	6.0	引入的功能。可以使用强制网络门户要求用户在浏览器窗口出现提示时输入其凭证。映射还允许策略基于用户或用户组。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。