



# 用户身份概述

---

以下主题讨论用户身份：

- [关于用户身份，第 1 页](#)
- [思科防御协调器主机和用户限制，第 14 页](#)

## 关于用户身份

用户身份信息可以帮助识别政策违规、攻击或网络漏洞的来源，并跟踪它们到具体用户。例如，您可以确定：

- 谁拥有作为影响程度为“易受攻击”（级别 1：红色）的入侵事件的目标的主机。
- 谁发起了内部攻击或端口扫描。
- 谁正在尝试对指定主机进行未经授权的访问。
- 谁正在耗用异常大量的带宽。
- 谁尚未应用关键操作系统更新。
- 谁正在违反公司政策使用即时消息软件或 P2P 文件共享应用。
- 谁与您网络中的每个危害表现相关。

借助这些信息，可以使用 Firepower 系统的其他功能降低风险，执行访问控制以及采取措施防止中断他人的活动。这些功能还可以大大改善审核控制并提高合规性。

在配置用户身份源以收集用户数据后，您可以执行用户感知和用户控制。

### 相关主题

- [身份术语，第 2 页](#)
- [关于用户身份源，第 2 页](#)
- [身份部署，第 5 页](#)
- [如何设置身份策略，第 10 页](#)

## 身份术语

本主题讨论用户身份和用户控制的常用术语。

### 用户感知

使用身份源（如或 TS 代理）标识网络中的用户。通过用户感知，您可以从授权（例如 Active Directory）和非授权（基于应用）源中识别用户。要使用 Active Directory 作为身份源，必须配置领域和目录。有关详细信息，请参阅[关于用户身份源，第 2 页](#)。

### 用户控制

配置与访问控制策略关联的身份策略。（然后，身份策略将作为访问控制子策略引用。）身份策略指定身份源以及（可选）属于该源的用户和组。

通过将身份策略与访问控制策略相关联，可以确定在网络中是监控、信任、阻止还是允许流量中的用户或用户活动。有关详细信息，请参阅[访问控制策略](#)。

### 授权身份源

验证了用户登录的受信任服务器（例如，Active Directory）。您可以使用从授权登录获取的数据执行用户感知和用户控制。授权用户登录是从被动和主动身份验证中获取：

- 被动身份验证发生在用户通过外部源进行身份验证时。ISE/ISE-PIC 和 TS 代理是 Firepower 系统支持的被动身份验证方法。
- 主动身份验证发生在用户通过预先配置的受管设备进行身份验证时。强制网络门户和远程接入访问 VPN 是 Firepower 系统支持的主动身份验证方法。

### 非授权身份源

未知或不受信任的服务器已验证用户登录。基于流量的检测是 Firepower 系统唯一支持的未授权身份源。您可以使用从非授权登录获取的数据执行用户感知。

## 关于用户身份源

下表提供系统支持的用户身份源的简要概述。每个身份源都提供一个用户存储库以获取用户感知。然后，可以使用身份和访问控制策略来控制这些用户。

用户身份源	策略	服务器要求	类型	身份验证类型	用户感知?	用户控制?	有关详细信息，请参阅.....
ISE/ISE-PIC	身份	Microsoft Active Directory	授权登录	无源	是	是	<a href="#">ISE/ISE-PIC 身份源</a>
TS 代理	身份	Microsoft Windows 终端服务器	授权登录	无源	是	是	<a href="#">终端服务 (TS) 代理身份源</a>

用户身份源	策略	服务器要求	类型	身份验证类型	用户感知?	用户控制?	有关详细信息, 请参阅.....
强制网络门户	身份	OpenLDAP Microsoft Active Directory	授权登录	主用	是	是	<a href="#">强制网络门户身份源</a>
远程接入 VPN	身份	OpenLDAP 或 Microsoft Active 目录	授权登录	主用	是	是	<a href="#">远程接入 VPN 身份源</a>
	身份 (Identity)	RADIUS	授权登录	主用	是	否	
基于流量的检测	网络发现	n/a	非授权登录	n/a	是	否	<a href="#">基于流量的检测身份源</a>

当选择要部署的身份源时, 请考虑以下事项:

- 必须使用基于流量的检测来检测非 LDAP 用户登录。
- 必须使用基于流量的检测或强制网络门户来记录失败的登录或身份验证活动。如果登录或身份验证尝试失败, 则不会将新用户添加到数据库的用户列表中。
- 强制网络门户身份源需要具有路由接口的受管设备。您不能使用具有强制网络门户的内联 (也称为分路模式) 接口。

这些身份源的数据存储在 Cisco Secure Firewall Management Center 的用户数据库和用户活动数据库中。您可以配置管理中心服务器用户下载, 以将新用户数据定期自动下载到您的数据库中。

在使用所需的身份源配置身份规则之后, 必须将每个规则与访问控制策略相关联, 并将策略部署到受管设备, 策略才能产生效果。有关访问控制策略和部署的详细信息, 请参阅[将其他策略与访问控制相关联](#)。

有关用户身份的常规信息, 请参阅[关于用户身份, 第 1 页](#)。

## 用户身份的最佳实践

我们建议您在设置身份策略之前查看以下信息。

- 了解用户限制
- 每个 AD 域创建一个领域
- 运行状况监控
- 使用最新版本的 ISE/ISE-PIC, 两种类型的补救
- 6.7 中的用户代理支持丢弃

- 强制网络门户需要路由接口，多个单独的任务

### Active Directory、LDAP 和领域

Firepower 系统支持 Active Directory 或 LDAP 进行用户感知和控制。Active Directory 或 LDAP 存储库与 FMC 之间的关联被称为领域。您应为每个 LDAP 服务器或 Active Directory 域创建一个领域。有关支持版本的详细信息，请参阅[领域支持的服务器](#)。

LDAP 支持的唯一用户身份源是强制网络门户。要使用其他身份源（ISE/ISE-PIC 除外），您必须使用 Active Directory。

仅适用于 Active Directory：

- 为每个域控制器创建一个目录。  
有关详细信息，请参阅 [创建 Active Directory 领域和领域目录](#)
- 如果将所有 Active Directory 域和域控制器分别添加为领域和目录，则支持两个域之间存在信任关系的用户和组。  
有关详细信息，请参阅[领域和受信任的域](#)。

### 代理序列

代理序列 是一个或多个可用于与 LDAP、Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当 思科防御协调器（CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如，CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。）

虽然您可以使用一台受管设备作为代理序列，但我们强烈建议您设置两台或更多设备，以便在受管设备无法与 Active Directory 或 ISE / ISE-PIC 通信时，另一台受管设备可以接管。

### 使用最新版本的 ISE/ISE-PIC

如果您希望使用 ISE/ISE-PIC 身份源，则强烈建议您始终使用最新版本，以确保获得最新的功能和漏洞修复。

pxGrid 2.0（版本 2.6 补丁 6 或更高版本使用；或 2.7 补丁 2 或更高版本）还将 ISE/ISE-PIC 使用的补救从终端保护服务 (EPS) 更改为自适应网络控制 (ANC)。如果升级 ISE/ISE-PIC，您必须将中介策略从 EPS 迁移到 ANC。

有关使用 ISE/ISE-PIC 的更多信息，请参阅[ISE/ISE-PIC 指南和限制](#)。

要设置 ISE/ISE-PIC 身份源，请参阅[如何为用户控制配置 ISE/ISE-PIC](#)。

### 强制网络门户信息

强制网络门户是唯一可以使用 LDAP 或 Active Directory 的用户身份源。此外，必须将托管设备配置为使用路由接口。

其他准则可在[强制网络门户指南和限制](#)中找到。

设置强制网络门户需要执行多项独立任务。有关详细信息，请参阅[如果为用户控制配置强制网络门户](#)。

### TS 代理信息

需要 TS 代理用户身份源来识别 Windows 终端服务器上的用户会话。TS 代理软件必须安装在终端服务器计算机上，如《思科终端服务 (TS) 代理指南》中所述。此外，您必须将 TS 代理服务器上的时间与管理中心上的时间进行同步。

TS 代理数据显示在“用户” (Users)、“用户活动” (User Activity) 和“连接事件” (Connection Event) 表中，并可用于用户感知和用户控制。

有关详细信息，请参阅[TS 代理准则](#)。

### 将身份策略与访问控制策略相关联

在配置领域、目录和用户身份源后，您必须在身份策略中设置身份规则。要让策略生效，您必须将身份策略与访问控制策略相关联。

有关创建身份策略的详细信息，请参阅[创建身份策略](#)。

有关创建身份规则的详细信息，请参阅[创建身份规则](#)。

要将身份策略与访问控制策略相关联，请参阅[将其他策略与访问控制相关联](#)。

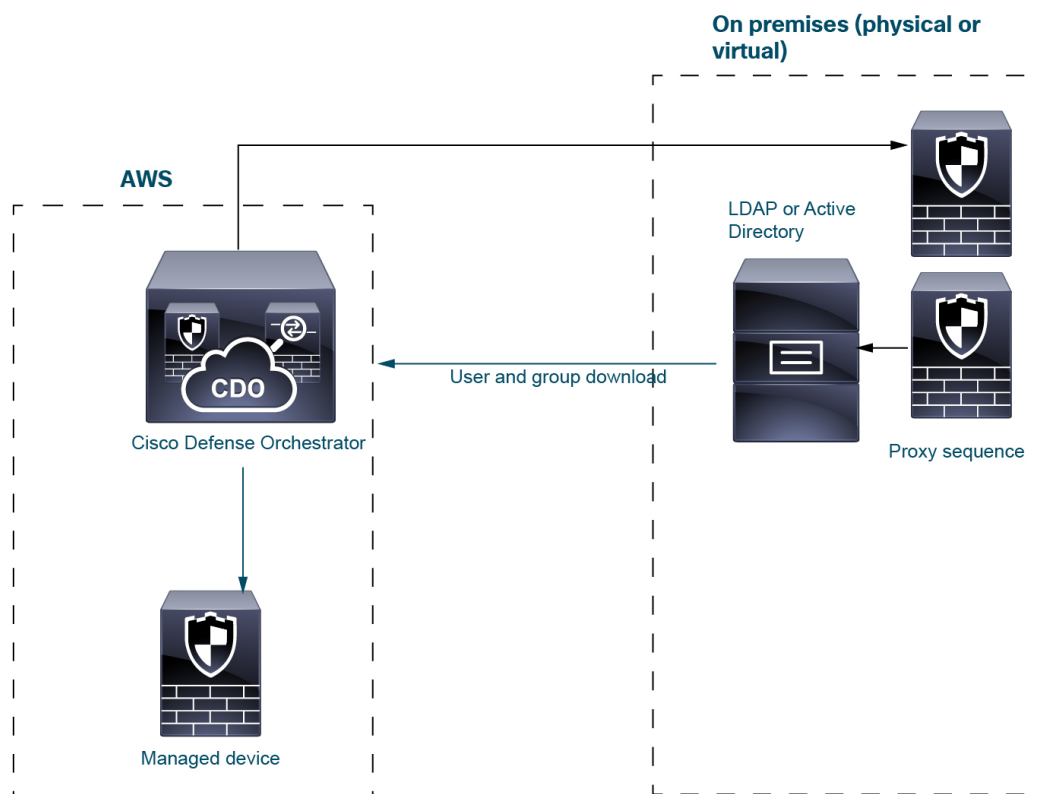
## 身份部署

系统从任何身份源检测到用户登录的用户数据时，会将登录用户与管理中心用户数据库中的用户列表进行比对。如果登录用户与现有用户匹配，则登录数据将会分配给该用户。如果登录信息与现有用户不匹配，则会创建新用户，除非登录信息位于 SMTP 流量中。SMTP 流量中不匹配的登录信息将被丢弃。

一旦用户被管理中心发现，用户所属的组就会与用户关联。

### 简单身份部署

本部分中讨论的示例部署基于下图所示的系统。



在上图中，CDO 和一个托管设备会被部署到 AWS，而其他设备位于本地。这些设备可以是物理设备，也可以是虚拟设备；它们只需要能够相互通信。

两个本地托管设备将用作代理序列。您还必须将这些设备添加到 CDO。

代理序列是一个或多个可用于与 LDAP、Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当思科防御协调器（CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如，CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。）

只有 TS 代理和强制网络门户需要 LDAP 或 Active Directory，如以下段落所述。

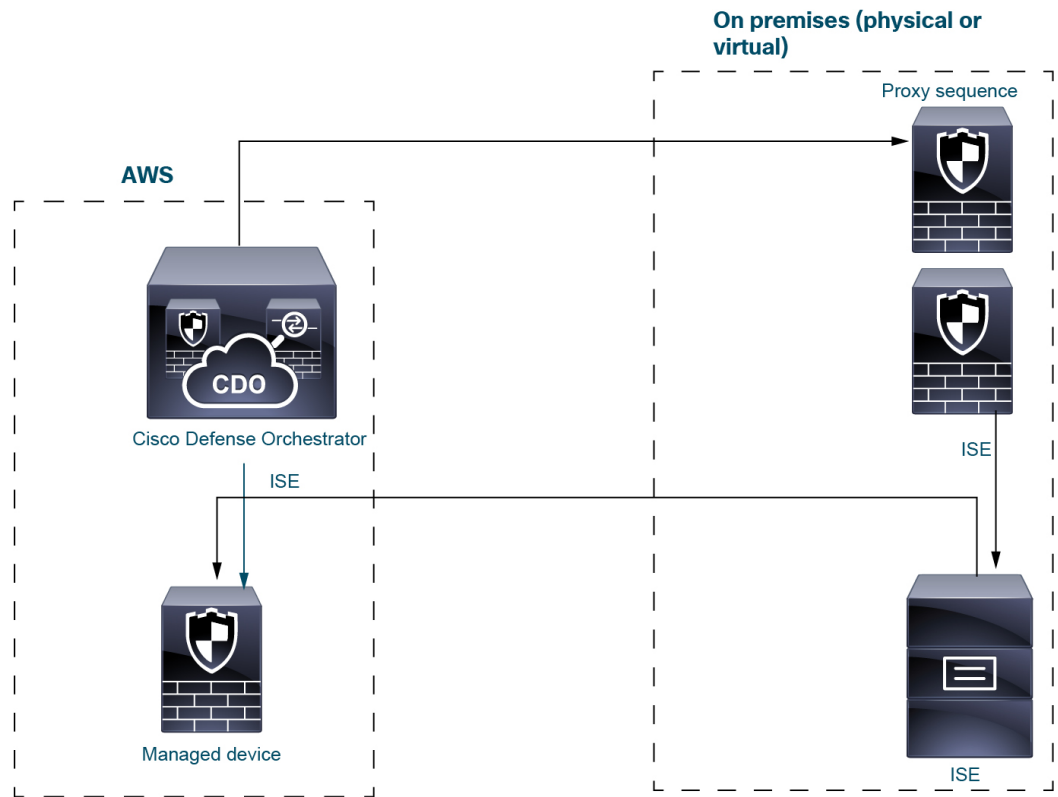
有关设置此类系统的详细信息，请参阅[如何设置身份策略](#)，第 10 页。

### ISE/ISE-PIC 身份源

部署 ISE/ISE-PIC 身份源时，如果 CDO 无法直接联系 ISE/ISE-PIC 服务器，CDO 会联系代理序列。用户、组和订用会从 ISE/ISE-PIC 服务器被发送到 AWS 中的托管设备。

您可以选择在 ISE/ISE-PIC 部署中使用 LDAP 服务器，但由于它是可选的，因此并未在下图中显示。

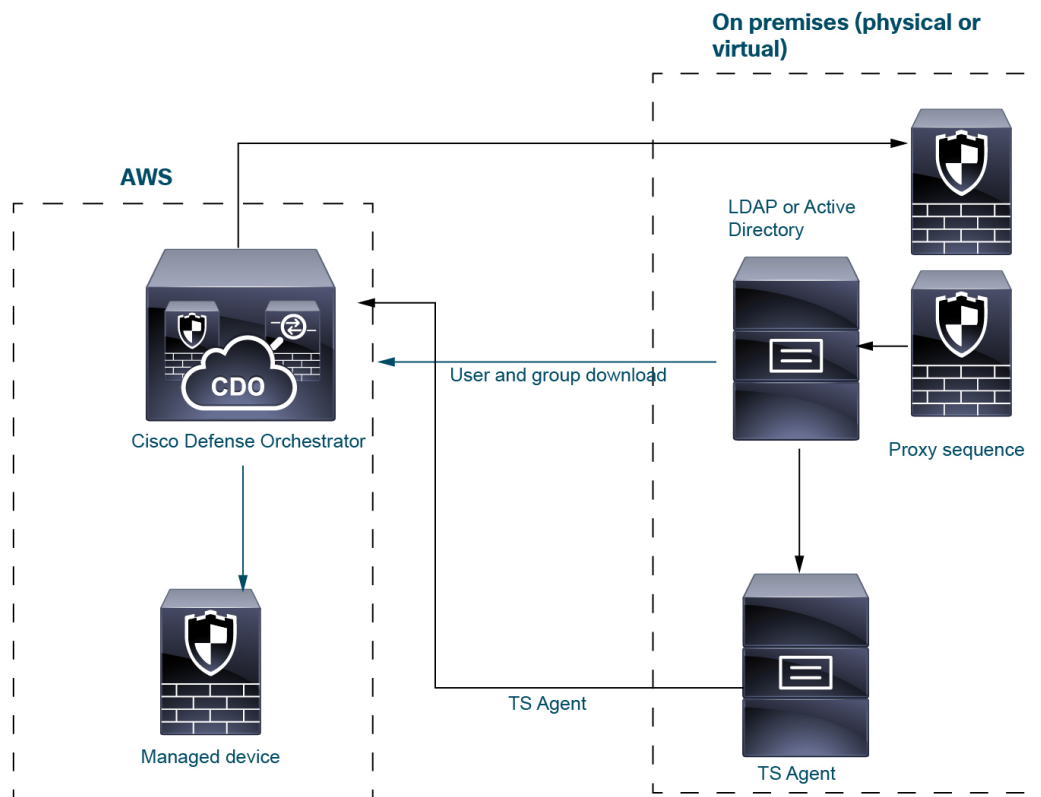
有关 ISE / ISE-PIC 的详细信息，请参阅[ISE/ISE-PIC 身份源](#)。



### TS 代理身份源

终端服务 (TS) 代理软件可在 Microsoft 服务器上运行，并会根据用户登录服务器所用的端口范围来发送 CDO 用户信息。TS 代理会从 LDAP 或 Active Directory 获取用户身份信息，然后将它们发送到 CDO。

有关 TS 代理身份源的详细信息，请参阅[终端服务 \(TS\) 代理身份源](#)。

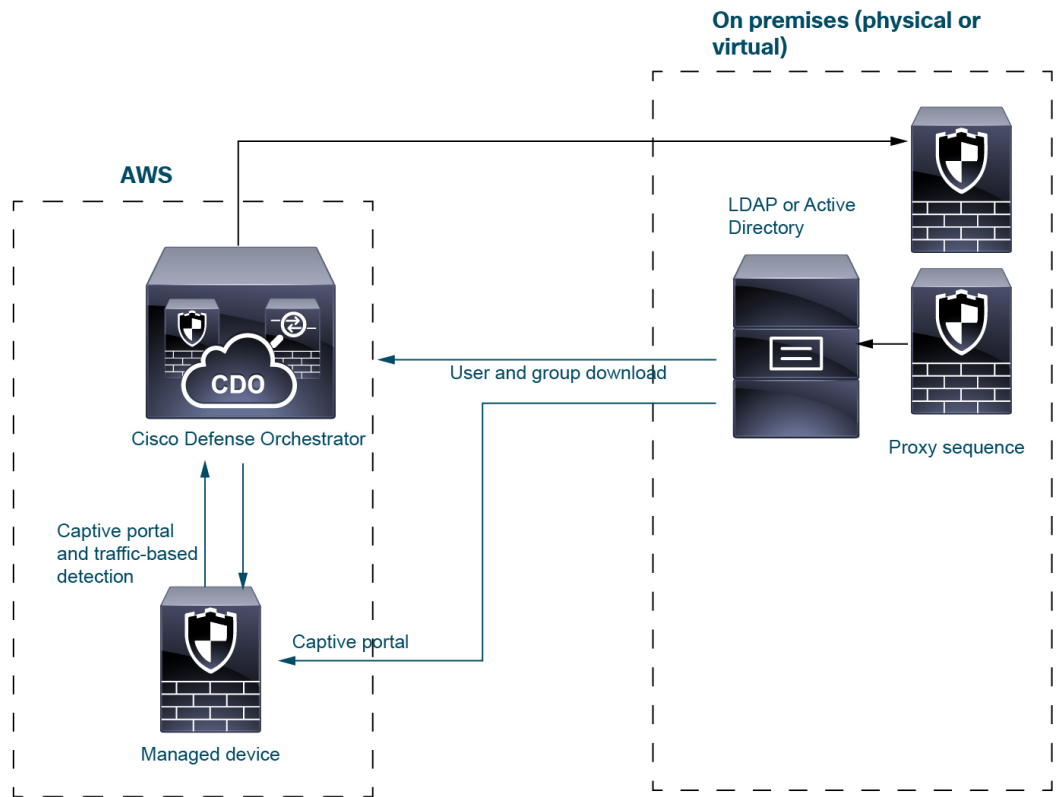


### 强制网络门户身份源

除 Active Directory 外，强制网络门户是唯一也支持 LDAP 的身份源。当用户尝试使用 AWS 中的托管设备通过 IP 地址或主机名来访问网络资源时，就会触发强制网络门户身份源。强制网络门户会使用代理序列从 LDAP 或 Active Directory 获取用户信息，然后将用户信息发送到 CDO。

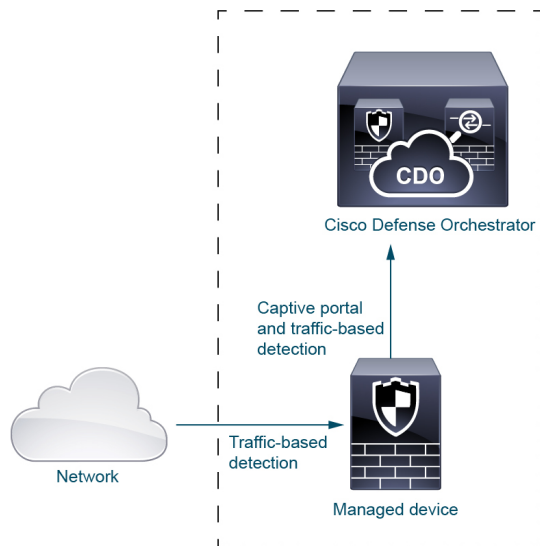
有关强制网络门户身份源的详细信息，请参阅[强制网络门户身份源](#)。





### 基于流量的检测

基于流量的检测仅用于检测网络上的应用，因此不需要使用像 Active Directory 这样的用户存储库或代理序列。有关详细信息，请参阅[关于主机、应用和用户数据的检测](#)。



## 如何设置身份策略

本主题提供了使用任何可用的用户身份源（TS代理、ISE/ISE-PIC、强制网络门户或远程接入VPN）设置身份策略的高级概述。

### 过程

	命令或操作	目的
步骤 1	（可选。）创建代理序列。	<p>代理序列 是一个或多个可用于与 LDAP、Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当思科防御协调器（CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如，CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。）</p> <p>虽然您可以使用一台受管设备作为代理序列，但我们强烈建议您设置两台或更多设备，以便在受管设备无法与 Active Directory 或 ISE / ISE-PIC 通信时，另一台受管设备可以接管。</p> <p>请参阅<a href="#">创建代理序列</a>。</p>
步骤 2	（可选。）创建领域和目录，林中包含要在用户控制中使用的用户的每个域都要创建一个领域。还为每个域控制器创建一个目录。只有具有相应 管理中心 领域和目录的用户和组才能用于身份策略中。	<p>如果满足以下任一条件，则创建领域、领域目录和代理序列为可选：</p> <ul style="list-style-type: none"> <li>• 您使用的 SGT ISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件。</li> <li>• 您仅使用身份策略来过滤网络流量。</li> <li>• 仅当您使用 思科防御协调器 (CDO) 且代理序列无法直接与 Active Directory 或 ISE/ISE-PIC 通信时才需要代理序列。</li> </ul> <p>领域是受信任的用户和组存储区，通常是 Microsoft Active Directory 存储库。管理中心会按您指定的间隔时间下载用户和组。您可以包括或排除用户和组来进行下载。</p> <p>请参阅<a href="#">创建 Active Directory 领域和领域目录</a>。有关创建领域的选项的详细信息，请参阅<a href="#">领域字段</a>。</p> <p>目录是一个 Active Directory 域控制器，它组织有关计算机网络的用户和网络共享的信息。Active Directory 控制器将为该领域提供</p>

	命令或操作	目的
		<p>目录服务。Active Directory 将跨域控制器分发用户和组对象，这些控制器是通过使用目录服务传播相互之间的本地更改的对等体。有关详细信息，请参阅 MSDN 上的 <a href="#">Active Directory 技术规范术语表</a>。</p> <p>您可以为某个领域指定多个目录，在这种情况下，每个域控制器都按该领域的目录选项卡页面上列出的顺序进行查询，以匹配进行用户控制的用户和组凭证。</p> <p><b>注释</b> 如果您计划配置 SGTISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件，则可自行决定是否配置领域或领域序列。</p>
步骤 3	从领域同步用户和组。	<p>要想能够控制用户和组，您必须将它们与管理中心同步。您可以随时将其与用户和组同步，也可以将系统配置为按指定的时间间隔进行同步。</p> <p>同步用户和组时，可以指定例外；例如，您可以从该领域的所有用户控制中排除“工程”组，也可以从应用于“工程”组的用户控制中排除用户 <code>joe.smith</code>。</p> <p>请参阅 <a href="#">同步用户和组</a></p>
步骤 4	(可选。) 创建领域序列。	<p>领域序列是一个有序的领域列表，如果用于身份策略中，则会导致系统按指定顺序搜索领域，以查找与规则匹配的用户。请参阅 <a href="#">创建领域序列</a>。</p>
步骤 5	创建检索用户和组数据的方法（身份源）。	<p>设置一个具有其独特配置的身份源，以便能够使用存储在该领域中的数据控制用户和组。身份源包括 TS 代理、网络强制门户或远程 VPN。请参见以下选项之一：</p> <ul style="list-style-type: none"> <li>• <a href="#">如果为用户控制配置强制网络门户</a></li> <li>• <a href="#">配置用户控制 ISE/ISE-PIC</a></li> <li>• <a href="#">配置用户控制 RA VPN</a></li> </ul>
步骤 6	创建身份策略。	<p>身份策略包含一个或多个身份规则，可选择按类别对其进行组织。请参阅 <a href="#">创建身份策略</a>。</p>

	命令或操作	目的
		<p><b>注释</b></p> <p>如果您计划配置 SGTISE 属性条件而不是用户、组、领域、终端位置或终端配置文件条件；或者，如果您只使用自己的身份策略来过滤网络流量，则可自行决定是否配置领域或领域序列。</p>
<b>步骤 7</b>	创建一个或多个身份规则。	身份规则使您能够指定许多匹配条件，包括身份验证类型、网络区域、网络或地理位置、领域、领域序列等。请参阅 <a href="#">创建身份规则</a> 。
<b>步骤 8</b>	请将您身份策略与访问控制策略关联起来。	访问控制策略将会过滤并（可选）检查流量。身份策略必须与访问控制策略相关联方可生效。请参阅 <a href="#">将其他策略与访问控制相关联</a> 。
<b>步骤 9</b>	将访问控制策略部署到至少一个受管设备。	要使用策略控制用户活动，必须将该策略部署到客户端所连接到的受管设备。请参阅 <a href="#">部署配置更改</a> 。
<b>步骤 10</b>	监控用户活动	<p>查看由用户身份源收集的会话列表或由用户身份源收集的用户信息列表。。</p> <p>如果满足以下所有条件，则不需要身份策略：</p> <ul style="list-style-type: none"> <li>• 您使用 ISE/ISE-PIC 身份源。</li> <li>• 您未在访问控制策略中使用用户或组。</li> <li>• 您在访问控制策略中使用安全组标记 (SGT)。有关详细信息，请参阅<a href="#">ISE SGT 与自定义 SGT 规则条件</a>。</li> </ul>

#### 相关主题

[配置基于流量的用户检测](#)

## 用户活动数据库

Cisco Secure Firewall Management Center 上的用户活动数据库包含已配置的所有身份源检测或报告的网络上的用户活动记录。系统会在以下情况下记录事件：

- 检测到单独的登录或注销时。
- 检测到新用户时。

- 系统管理员手动删除用户时。
- 系统检测到不在数据库中的用户，但因已达到用户限制而无法添加该用户时。
- 您解决与用户关联的危害表现，或者为用户启用或禁用危害表现规则时。



**注释** 如果 TS 代理监控与其他被动身份验证身份源（如 ISE/ISE-PIC）相同的用户，则管理中心会划分 TS 代理数据的优先级。如果 TS 代理和 ISE 报告来自同一 IP 地址的相同活动，则仅会将 TS 代理数据记录到管理中心。

可以使用 Cisco Secure Firewall Management Center 查看系统检测到的用户活动。（分析 (Analysis) > 用户 (Users) > 用户活动 (User Activity)。）

## 用户数据库

Cisco Secure Firewall Management Center 中的用户数据库包含所有已配置身份源检测或报告的每个用户的记录。您可以使用从授权源获取的数据进行用户控制。

有关受支持的非授权和授权身份源的详细信息，请参阅[关于用户身份源](#)，第 2 页。

如[用户限制](#)。达到此用户限制后，系统将基于其身份源对以前未检测到的用户数据划分优先级，如下所示：

- 如果新用户来自非授权身份源，则系统不会将该用户添加到数据库。要允许添加新用户，您必须手动或使用数据库清除删除用户。
- 如果新用户来自授权身份源，则系统会删除非活动时间最长的非授权用户，并将新用户添加到数据库。

如果身份源配置为排除特定用户名，则这些用户名的用户活动数据将不会报告给 Cisco Secure Firewall Management Center。这些已排除的用户名仍保留在数据库中，但不与 IP 地址关联。

如果已配置管理中心高可用性且主连接失败，则在故障切换停机期间无法识别强制网络门户、ISE/ISE-PIC、TS 代理、远程接入 VPN 报告的所有登录，即便以前查看过这些用户并已将他们下载到管理中心也是如此。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。



**注释** 如果 TS 代理监控与其他被动身份验证身份源（ISE/ISE-PIC）相同的用户，则管理中心会划分 TS 代理数据的优先级。如果 TS 代理和 ISE 报告来自同一 IP 地址的相同活动，则仅会将 TS 代理数据记录到管理中心。

系统检测到新用户会话时，用户会话数据会保留在用户数据库中，直至出现以下其中一种情形：

- 管理中心 的用户将手动删除用户会话。
- 某个身份源报告该用户会话的注销操作。

- 某个领域结束其用户会话超时：通过验证的用户、用户会话超时：未通过验证的用户或用户会话超时：访客用户设置指定的用户会话。

## 思科防御协调器主机和用户限制

### 云交付的防火墙管理中心 主机限制

当在监控网络中检测到与IP地址相关联的活动时，云交付的防火墙管理中心会将主机添加到网络映射，如网络发现策略中所定义。

云交付的防火墙管理中心可以在其主机数据库中存储最多 600,000 个主机，但我们的建议如下。

由 CDO 管理的设备数量	建议的主机数量
1-50	100,000
51-300	300,000
301-1000	600,000

您无法查看不在网络映射中的主机的情景数据。但是，您可以执行访问控制。例如，您可以对不在网络映射中的主机接收和发出的流量进行应用控制，即使您无法使用合规 allow 名单监控主机的网络合规性。



**注释** 系统分别从 IP 地址和 MAC 地址识别的主机对仅 MAC 主机进行计数。与一台主机关联的所有 IP 地址均视为一台主机共同计数。

#### 达到主机限制与删除主机

网络发现策略控制在您达到主机限制后检测到新主机时发生的情况；您可以丢弃新主机或替代非活动时间最长的主机。您也可以设置系统在主机处于非活动状态多长时间后将其从网络映射中删除的时间段。虽然您可以从网络映射中手动删除主机、整个子网或所有主机，但如果系统检测到与已删除主机相关的活动，它会重新添加该主机。

在多域部署中，每个分叶域都有自己的网络发现策略。因此，当系统发现新主机时，每个分叶域会管理自己的行为。

### 思科防御协调器云交付的防火墙管理中心用户限制

用户会在以下情况时被添加到云交付的防火墙管理中心用户数据库：

- 从领域下载用户。
- 强制网络门户或 RA-VPN 用户登录。

- 从任何身份源（例如，TS 代理）检测到用户。

云交付的防火墙管理中心可以在其主机数据库中存储最多 600,000 个用户，但我们的建议如下。

由 CDO 管理的设备数量	建议的用户数量
1-50	100,000
51-300	300,000
301-1000	600,000

仅授权用户才能使用访问控制策略进行用户控制。

云交付的防火墙管理中心可在其用户数据库中存储 600,000 个会话。

达到限制后，当系统检测到之前未检测到的新用户时，会根据其身份源确定用户数据的优先级：

- 如果新用户来自非授权源，则系统不会将该非授权用户添加到数据库。要允许添加新用户，您必须手动删除用户或清除数据库。
- 如果新用户来自授权身份源，则系统会删除非活动时间最长的非授权用户，并将新授权用户添加到数据库。

如果只有授权用户，则系统会删除非活动时间最长的授权用户，并将新用户添加到数据库。

故障排除信息可在[用户控制故障排除](#)中看到。



**提示** 请注意，如果使用的是基于流量的检测，则您可按协议限制客户日志记录，以最大程度低减少用户名干扰并保留数据库空间。例如，您可以防止系统添加在 AIM、POP3 和 IMAP 流量中发现的用户，因为您了解此流量来自您不想监控的特定承包商或访客。





## 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。