提供程序

为了使ISE-PIC能够向订用服务的使用者（用户）提供身份信息，您必须首先配置ISE-PIC探测器，它连接到身份提供程序。

下表提供了有关ISE-PIC中所有提供程序和探测类型的详细信息。有关Active Directory的详细信息，请参阅 Active Directory 作为探测器和提供程序。

您可以定义下列提供程序类型：

表 *1:* 提供程序类型

提供程序类型（探测器）	说明	源系统（提供程序）	技术	收集的用户身份信息	文档链接
Active Directory (AD)	用于从中接收用户信息的高度安全而精确且最常用的源。 作为探测器，AD 运用 WMI 技术传送经过身份验证的用户身份。 此外，AD 本身而不是探测器，而是用作其他探测器从中检索用户数据的源系统（提供程序）。	Active Directory 域控制器	WMI	• 用户名 • IP 地址 • 域 (Domain)	Active Directory 作为探测器和提供程序
代理	Active Directory 域控制器或成员服务器上安装的本地 32 位应用。代理探测器是将 Active Directory 用于用户身份信息的一种快速高效的解决方案。		域控制器或成员服务器上安装的代理。	• 用户名 • IP 地址 • 域 (Domain)	Active Directory 代理，第 3 页
终端	除其他已配置的探测器以外，始终在后台运行，以便验证用户是否仍然处于连接状态。		WMI	用户是否仍然处于连接状态	终端探测器，第 35 页
SPAN	位于网络交换机上，以便侦听网络流量并根据 Active Directory 数据提取用户身份信息。		交换机上安装的 SPAN，以及 Kerberos 消息	• 用户名 • IP 地址 • 域 (Domain)	SPAN，第 11 页

提供程序类型（探测器）	说明	源系统（提供程序）	技术	收集的用户身份信息	文档链接
API 提供程序	使用 ISE-PIC 提供的 RESTful API 服务从编程为与 RESTful API 客户端进行通信的任何系统收集用户身份信息。	编程为与 REST API 客户端进行通信的任何系统。	RESTful API。以 JSON 格式发送到用户的用户身份。	• 用户名 • IP 地址 • 端口范围 • 域	API 提供程序，第 7 页
系统日志	解析系统日志消息和检索用户身份，包括 MAC 地址。	• 常规系统日志消息提供程序 • DHCP 服务器	系统日志消息	• 用户名 • IP 地址 • MAC 地址 • 域	系统日志提供程序，第 13 页

注释 pxGrid 会每秒为会话主题发送 200 个事件，以避免客户端过载。如果发布方发送的事件超过 200 个，则额外的事件将排队并在下一批中发送。

如果 pxGrid 在很长一段时间内持续收到每秒超过 200 个事件，它可能会消耗比平时更多的内存来存储积压的事件。这可能会影响 pxGrid 的性能。

- Active Directory 代理，第 3 页
- API 提供程序，第 7 页
- SPAN，第 11 页
- 系统日志提供程序，第 13 页
- 过滤被动身份服务，第 34 页
- 终端探测器，第 35 页

Active Directory 代理

从ISE-PIC，在 Active Directory (AD) 域控制器 (DC) 或成员服务器上的任意位置（根据配置）安装本地 32 位应用（即域控制器 (DC) 代理），以从 AD 检索用户身份信息，然后将这些身份发送给已配置的用户。代理探测器是将 Active Directory 用于用户身份信息的一种快速高效的解决方案。代理可安装在单独的域中，也可安装在 AD 域中，并且一旦安装，它们就会每分钟提供一次 ISE-PIC 的状态更新。

代理可由 ISE-PIC 自动安装和配置，您也可以手动对其进行安装。安装时，会发生以下情况：

- 代理及其关联文件安装在以下路径：**Program Files/Cisco/Cisco ISE PassiveID Agent**
- 系统将安装一个名为 **PICAgent.exe.config** 的配置文件，其中会指示代理的日志记录级别。您可以从该配置文件内手动更改日志记录级别。
- CiscoISEPICAgent.log 文件与所有日志记录消息一起存储。
- nodes.txt 文件包含部署中可与代理进行通信的所有节点的列表。代理会访问列表中的第一个节点。如果无法访问该节点，代理将根据列表中节点的顺序继续尝试通信。对于手动安装，必须打开文件并输入节点 IP 地址。（手动或自动）安装完成后，便只能通过手动更新该文件来对其进行更改。打开文件，然后根据需要添加、更改或删除节点 IP 地址。
- 思科 ISE PassiveID 代理服务在机器上运行，您可从“Windows 服务”对话框管理该机器。
- ISE-PIC 最多支持 100 个域控制器，而每个代理最多可以监控 10 个域控制器。要监控 100 个域控制器，必须配置 10 个代理。
- 仅在 Windows Server 2008 及更高版本上支持 Active Directory 代理。如果无法安装代理，则对被动身份服务使用 Active Directory 探测器。有关详细信息，请参阅Active Directory 作为探测器和提供程序。

注释 即使您在成员服务器上运行 AD 代理，它也仍会在 Active Directory 中查询登录请求。

自动安装并部署 Active Directory 代理

配置代理提供程序以监控域控制器的用户身份时，代理必须安装在成员服务器或域控制器上。代理可由 ISE-PIC 自动安装，也可以手动对其进行安装。自动或手动安装后，必须配置已安装的代理来监控指定域控制器，而非默认 WMI。以下流程说明了如何自动安装并配置代理以监控域控制器。

开始之前

- 从服务器端对相关 DNS 服务器配置反向查找。有关 ISE-PIC 的 DNS 服务器配置要求的详细信息，请参阅 DNS 服务器
- 确保在指定用于代理的机器上更新 Microsoft .NET Framework，最低更新至版本 4.0。有关 .NET Framework 的详细信息，请参阅 https://www.microsoft.com/net/framework。
- 创建 AD 加入点，并至少添加一个域控制器。有关创建加入点的详细信息，请参阅Active Directory 作为探测器和提供程序。

  对 AD、代理、SPAN 和系统日志探测器使用 AD 用户组。有关 AD 组的详细信息，请参阅配置 Active Directory 用户组。

步骤 1 选择**提供程序 (Providers)** > **代理 (Agents)**。

步骤 2 要添加新客户端，请从表的顶部单击**添加 (Add)**。

步骤 3 要创建新代理并将其自动安装到您在此配置中指示的主机上，请选择**部署新代理 (Deploy New Agent)**。

步骤 4 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅Active Directory 代理设置 ， 第 6 页。

步骤 5 单击**部署 (Deploy)**。
代理将根据您在配置中指示的域自动安装到主机上，并保存设置。代理现在显示在“Agents”(代理)表格中，并可应用于监控指定域控制器，如以下步骤所述。

步骤 6 选择**提供程序 (Providers)** > **Active Directory** 以查看当前配置的所有接入点。

步骤 7 单击您要从中启用所创建代理的接入点的链接。

步骤 8 选择**被动 ID (Passive ID)** 选项卡以配置您作为前提条件的一部分而添加的域控制器。

步骤 9 选择您要通过所创建代理来监控的域控制器，然后单击**编辑 (Edit)**。

步骤 10 从**协议 (Protocol)** 下拉列表中，选择**代理 (Agent)**。

步骤 11 从**代理 (Agent)** 下拉列表中选择您创建的代理。输入您创建的代理的用户名和密码凭证（如果有），然后单击**保存 (Save)**。

手动安装并部署 Active Directory 代理

配置代理提供程序以监控域控制器的用户身份时，代理必须安装在成员服务器或域控制器上。代理可由 ISE-PIC 自动安装，也可以手动对其进行安装。自动或手动安装后，必须配置已安装的代理来监控指定域控制器，而非默认 WMI。以下流程说明了如何手动安装并配置代理以监控域控制器。

开始之前

- 从服务器端对相关 DNS 服务器配置反向查找。有关 ISE-PIC 的 DNS 服务器配置要求的详细信息，请参阅 DNS 服务器
- 确保在指定用于代理的机器上更新 Microsoft .NET Framework，最低更新至版本 4.0。有关 .NET Framework 的详细信息，请参阅 https://www.microsoft.com/net/framework。
- 创建 AD 加入点，并至少添加一个域控制器。有关创建加入点的详细信息，请参阅Active Directory 作为探测器和提供程序。

  对 AD、代理、SPAN 和系统日志探测器使用 AD 用户组。有关 AD 组的详细信息，请参阅配置 Active Directory 用户组。

步骤 1 选择**提供程序 (Providers)** > **代理 (Agents)**。

步骤 2 点击**下载代理 (Download Agent)** 以下载 **`picagent-installer.zip`** 文件进行手动安装。
此文件将下载至标准 Windows 下载文件夹。

步骤 3 将此 zip 文件置于指定主机并运行安装。

步骤 4 从 ISE-PIC GUI 中，同样依次选择**提供程序 (Providers)** > **代理 (Agents)**。

步骤 5 要配置新代理，请从表的顶部点击**添加 (Add)**。

步骤 6 要配置已在主机上安装的代理，请选择**注册现有代理 (Register Existing Agent)**。

步骤 7 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅#unique_52。

步骤 8 单击**保存**。
系统会保存代理设置。代理现在显示在“Agents”(代理)表格中，并可应用于监控指定域控制器，如以下步骤所述。

步骤 9 依次选择**提供程序 (Providers)** > **Active Directory** 以查看当前配置的所有接入点。

步骤 10 点击您要从中启用所创建代理的接入点的链接。

步骤 11 选择**被动 ID (Passive ID)** 选项卡以配置您作为先决条件的一部分而添加的域控制器。

步骤 12 选择您要通过所创建代理来监控的域控制器，然后点击**编辑 (Edit)**。

步骤 13 从**协议 (Protocol)** 下拉列表中，选择**代理 (Agent)**。

步骤 14 从**代理 (Agent)** 下拉列表中选择您创建的代理。输入您为代理创建的任何用户名和密码凭证，然后点击**保存 (Save)**

卸载代理

可以直接从 Windows 轻松（手动）卸载自动或手动安装的代理。

步骤 1 在 Windows 对话框中，转至**程序和功能**。

步骤 2 在已安装程序的列表中，查找并选择思科 ISE 被动 ID 代理。

步骤 3 点击**卸载**。

Active Directory 代理设置

允许 ISE-PIC 在网络中的指定主机上自动安装代理，以从不同的域控制器 (DC) 检索用户身份信息并向 ISE-PIC 订户提供此信息。

要创建和管理代理，请依次选择**提供程序 (Providers)** > **代理 (Agents)**。请参阅自动安装并部署 Active Directory 代理 ， 第 4 页。

表 *2:*“代理”*(Agents)*窗口

字段名称	说明
名称	您配置的代理名称。
主机	安装代理的主机的完全限定域名。
监控	此为指定代理所监控的域控制器的逗号分隔列表。

表 *3:* 新建代理 *(Agents New)*

字段	说明
“部署新代理”(Deploy New Agent) 或“注册现有代理”(Register Existing Agent)	• “部署新代理”(Deploy New Agent)：在指定主机上安装新代理。 • “注册现有代理”(Register Existing Agent)：在主机上手动安装代理，然后从此屏幕为 ISE-PIC 配置此代理以启用服务。
名称	输入可用于轻松识别代理的名称。
说明	输入可用于轻松识别代理的说明。
主机 **FQDN**	此为已安装代理（注册现有代理）或将要安装代理（自动部署）的主机的完全限定域名。
用户名	输入用户名以访问要安装代理的主机。ISE-PIC 将使用这些凭证为您安装代理。
密码	输入用户密码以访问要安装代理的主机。ISE-PIC 将使用这些凭证为您安装代理。

API 提供程序

通过思科 ISE-PIC 中的“API 提供程序”功能，可将用户身份信息从自定义程序或从终端服务器 (TS) 代理推送到内置的 ISE-PIC REST API 服务。通过此方式，可以自定义网络中的可编程客户端，以将从任何网络访问控制 (NAC) 系统收集到的用户身份发送到服务。此外，通过思科 ISE-PIC API 提供程序，还可与网络应用（例如 Citrix 服务器上的 TS 代理，其中所有用户都具有同一 IP 地址但分配有唯一端口）接合。

例如，在 Citrix 服务器上运行的用于为根据 Active Directory (AD) 服务器进行身份验证的用户提供身份映射的代理可向 ISE-PIC 发送 REST 请求，请求只要有新用户登录或注销便添加或删除用户会话。然后，ISE-PIC 获取从客户端传送的用户身份信息（包括 IP 地址和已分配的端口），并将其发送到预配置用户，例如思科 Firepower 管理中心 (FMC)。

ISE-PIC REST API 框架通过 HTTPS 协议实施 REST 服务（无需客户端证书验证），并以 JSON (JavaScript Object Notation) 格式传送用户身份信息。有关 JSON 的详细信息，请参阅 http://www.json.org/ 。

ISE-PIC REST API 服务会解析用户身份，此外还会将该信息映射到端口范围，以便区分同时登录到一个系统的不同用户。每次将端口分配给用户时，API 都会向 ISE-PIC 发送一条消息。

REST API 提供程序流程

配置了从 ISE-PIC 到自定义客户端的网桥后（通过将该客户端声明为 ISE-PIC 的提供程序，并使该特定自定义程序 (客户端) 能够发送 RESTful 请求），ISE-PIC REST 服务便通过以下方式进行工作：

1. 对于客户端身份验证，思科ISE-PIC需要身份验证令牌。客户端机器上的自定义程序在发起联系时发送身份验证令牌的请求，然后ISE-PIC每次都会通知先前令牌已到期。系统会返回令牌以响应请求，从而启用客户端和 ISE-PIC 服务之间的持续通信。
2. 用户登录到网络中后，客户端便会检索用户身份信息，并使用 API 添加命令将该信息发布到 ISE-PIC REST 服务。
3. 思科 ISE-PIC 接收并映射用户身份信息。
4. 思科 ISE-PIC 向用户发送已映射的用户身份信息。
5. 只要有必要，自定义机器即可发送用于移除用户信息的请求，方法是发送“删除 API”调用并包含在发送“添加”调用后作为响应接收到的用户 ID。

在 ISE-PIC 中使用 REST API 提供程序

按照以下步骤激活 ISE-PIC 中的 REST 服务：

1. 配置客户端。有关详细信息，请参阅客户端用户文档。
2. 确保您已正确配置 DNS 服务器，包括从 ISE-PIC 配置客户端机器的反向查找。有关 ISE-PIC 的 DNS 服务器配置要求的详细信息，请参阅 DNS 服务器
3. 请参阅为 被动身份服务 配置与 ISE-PIC REST 服务的桥接 ， 第 8 页。

> **注释** 要将 API 提供程序配置为使用 TS 代理，请在创建从 ISE-PIC 到该代理的网桥时添加 TS 代理信息，然后参考 TS 代理文档以获取有关发送 API 调用的信息。

4. 生成身份验证令牌并向 API 服务发送添加和删除请求。

为 被动身份服务 配置与 ISE-PIC REST 服务的桥接

为了使 ISE-PIC REST API 服务能够从特定客户端接收信息，必须首先从 ISE-PIC 定义该特定客户端。您可以定义多个具有不同 IP 地址的 REST API 客户端。

开始之前

- 确保您已正确配置 DNS 服务器，包括从思科 ISE-PIC 配置客户端机器的反向查找。有关思科 ISE-PIC 的 DNS 服务器配置要求的详细信息，请参阅DNS 服务器

步骤 1 系统将显示“API 提供程序”表，包括每个现有客户端的状态信息。

步骤 2 要添加新客户端，请从表的顶部单击**添加 (Add)**。

步骤 3 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅API 提供程序设置 ， 第 9 页。

步骤 4 单击**提交 (Submit)**。

系统将保存客户端配置，并其屏幕会显示更新后的“API提供程序”表。客户端现在可以将发布内容发送到ISE-PIC REST 服务。

下一步做什么

设置自定义客户端，以将身份验证令牌和用户身份发布到ISE-PIC REST 服务。请参阅将 API 调用发送到 ISE-PIC REST 服务 ， 第 9 页。

将 API 调用发送到 ISE-PIC REST 服务

开始之前

为 被动身份服务 配置与 ISE-PIC REST 服务的桥接 ， 第 8 页

步骤 1 在浏览器的地址栏中输入思科 ISE URL（例如 *https://<ise hostname or ip address>/admin/*）

步骤 2 在以下位置中输入已从 **API 提供程序 (API Providers)** 窗口中指定并配置的用户名和密码。有关详细信息，请参阅为 被动身份服务 配置与 ISE-PIC REST 服务的桥接 ， 第 8 页。

步骤 3 按 **Enter** 键。

步骤 4 在目标节点的“URL 地址”(URL Address) 字段中输入 API 调用。

步骤 5 点击**发送**以发出 API 调用。

下一步做什么

请参阅 API 调用 ， 第 10 页以获取有关不同 API 调用、其架构及其结果的更多信息和详细信息。

API 提供程序设置

注释 可以使用请求调用来检索完整的 API 定义和对象架构，如下所示：

- 对于完整 API 规范 (wadl) - https://YOUR_ISE:9094/application.wadl
- 对于 API 模型和对象架构 - https://YOUR_ISE:9094/application.wadl/xsd0.xsd

表 *4: API* 提供程序设置

字段	说明
名称	输入此客户端的用于快速轻松地将其与其他客户端进行区分的唯一名称。
说明	输入此客户端的明确说明。

字段	说明
状态	选择**已启用 (Enabled)** 以使客户端能够在完成配置时立即与 REST 服务进行交互。
主机/IP	输入客户端主机器的 IP 地址。确保您已正确配置 DNS 服务器，包括从 ISE-PIC 配置客户端机器的反向查找。
用户名	创建在发布到REST服务时要使用的唯一用户名。
密码	创建在发布到 REST 服务时要使用的唯一密码。

API 调用

这些 API 调用用于通过思科 ISE-PIC 来管理 被动身份服务 的用户身份事件。

目的：生成身份验证令牌

- **请求**

  POST

  https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken

  请求应包含 BasicAuth 授权报头。提供先前从 ISE-PIC GUI 创建的 API 提供程序凭证。有关详细信息，请参阅API 提供程序设置，第 9 页。

- **响应报头**

  该报头包含 X-auth-access-token。这是发布其他 REST 请求时要使用的令牌。

- **响应正文**

  HTTP 204 No Content

目的：添加用户

- **请求**

  POST

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity

  在发布请求标头中添加 X-auth-access-token，例如，标头：X-auth-access-token，值：f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- **响应报头**

  201创建

- **响应正文**

  {

"user": "<username>",
"srcPatRange": {
"userPatStart": <user PAT start value>,
"userPatEnd": <user PAT end value>,
"patRangeStart": <PAT range start value>
},
"srcIpAddress": "<src IP address>",
"agentInfo": "<Agent name>",
"timestamp": "<ISO_8601 format i.e. “YYYY-MM-DDTHH:MM:SSZ" >",
"domain": "<domain>"
}

- 注
  - 可在以上 JSON 中删除 srcPatRange 以创建单个 IP 用户绑定。
  - 响应正文包含“ID”，这是所创建的用户会话绑定的唯一标识符。发送 DELETE 请求时使用此 ID，以指示应删除哪个用户。
  - 此响应还包含自链接，这是此新创建的用户会话绑定的 URL。

目的：删除用户

- 请求

  DELETE

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>

  在 <id> 中，输入从“添加”响应接收到的 ID。

  在删除请求报头中添加 X-auth-access-token，例如，报头：X-auth-access-token，值：f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- 响应报头

  200 OK

- 响应正文

  响应正文包含有关已删除的用户会话绑定的详细信息。

SPAN

SPAN通过它可快速轻松地启用思科 ISE-PIC 以侦听网络和检索用户信息，而不必将 Active Directory 配置为直接使用思科 ISE-PIC。SPAN 嗅探网络流量（专门检查 Kerberos 消息），提取 Active Directory

也已存储的用户身份信息，并将该信息发送到 ISE-PIC。然后，ISE-PIC 解析信息，最终将用户名、IP 地址和域名传送到您也已从 ISE-PIC 配置的用户。

为了使 SPAN 侦听网络和提取 Active Directory 用户信息，ISE-PIC 和 Active Directory 必须连接到网络上的同一交换机。这样，SPAN 便可以从 Active Directory 复制并镜像所有用户身份数据。

使用 SPAN，将通过以下方式检索用户信息：

1. 用户终端登录网络。
2. 登录和用户数据存储在 Kerberos 消息中。
3. 一旦用户登录且用户数据通过交换机进行传递，SPAN 就会镜像网络数据。
4. 思科 ISE-PIC 侦听网络以获取用户信息，并从交换机检索镜像的数据。
5. 思科 ISE-PIC 解析用户信息并更新被动 ID 映射。
6. 思科 ISE-PIC 将已解析的用户信息传送到用户。

使用 SPAN

开始之前

要使 ISE-PIC 从网络交换机接收 SPAN 流量，必须先定义侦听此交换机的节点和节点接口。可以配置 SPAN 以侦听安装的不同 ISE-PIC 节点。对于每个节点，只能配置一个接口来侦听网络，用于侦听的接口只能专用于 SPAN。

此外，您必须牢记：

- 确保已在网络上配置 Active Directory。
- 在同样连接至 Active Directory 的网络中的交换机上运行 CLI，以确保交换机可以与 ISE-PIC 通信。
- 配置交换机以从 AD 镜像网络。
- 配置专用于 SPAN 的ISE-PIC网络接口卡 (NIC)。此 NIC 仅用于 SPAN 流量。
- 通过命令行界面，确保激活专用于 SPAN 的 NIC。
- 创建仅将 Kerberos 流量发送到 SPAN 端口的 VACL。

步骤 1 选择**提供程序 (Providers)** > **SPAN**以配置 SPAN。

步骤 2 注释　我们建议 GigabitEthernet0 网卡 (NIC) 保持可用，并选择任何其他可用 NIC 来配置 SPAN。GigabitEthernet0 用于系统管理。

输入有意义的说明（可选），选择状态**已启用 (Enabled)**，并选择将用于侦听网络交换机的节点和相关 NIC。有关详细信息，请参阅SPAN 设置，第 13 页。

步骤 3 单击**保存**。

系统将保存 SPAN 配置， ISE-PIC 现在主动侦听网络流量。

SPAN 设置

从已部署的每个节点，通过在客户端网络上安装 SPAN，可快速轻松地配置 ISE-PIC 以接收用户身份。

表 *5: SPAN* 设置

字段	说明
说明	输入唯一说明以向您提醒当前启用的节点和接口。
状态	选择**已启用**可在完成配置时立即启用客户端。
接口 NIC (Interface NIC)	为 ISE-PIC 选择一个或两个节点，然后对于每个选定节点，选择用于侦听网络以获取信息的节点接口。 **注释** 我们建议将 GigabitEthernet0 NIC 保持可用，并选择任何其他可用 NIC 来配置 SPAN。GigabitEthernet0 用于系统管理。

系统日志提供程序

ISE-PIC 会解析来自任何传送系统日志消息的任何客户端（身份数据提供程序）的系统日志消息，包括常规系统日志消息 （来自 InfoBlox、Blue Coat、BlueCat 和 Lucent 等提供程序）以及 DHCP 系统日志消息，并发送回用户身份信息，包括 MAC 地址。然后将此映射的用户身份数据传送到用户。

您可以指定接收用户身份数据的系统日志客户端（请参阅配置系统日志客户端， 第 14 页）。配置提供程序时，您必须指定连接方法（TCP 或 UDP）以及要用于解析的系统日志模板。

注释 当所配置的连接类型为 TCP 时，如果消息报头存在问题且无法解析主机名，则 ISE-PIC 会尝试将数据包中接收到的 IP 地址与已为 ISE-PIC 中的系统日志消息配置的提供程序列表中任何提供程序的 IP 地址进行匹配。要查看此列表，请选择**提供程序 (Providers)** > **系统日志提供程序(Syslog Providers)**。我们建议您检查消息报头并根据需要进行自定义，以便保证解析成功。有关自定义报头的详细信息，请参阅自定义系统日志报头， 第 20 页。

系统日志探测器会将接收到的系统日志消息发送到ISE-PIC解析器，该解析器会映射用户身份信息，并将该信息发布到ISE-PIC。然后，ISE-PIC将已解析和已映射的用户身份信息传送到ISE-PIC用户。

注释 DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便 ISE-PIC 可以首先检查在本地会话目录（从“实时会话”(Live Sessions) 中显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。

要从 ISE-PIC 解析用户身份的系统日志消息，请执行以下操作：

- 配置要从中接收用户身份数据的系统日志客户端。请参阅配置系统日志客户端，第 14 页。
- 自定义单个消息报头。请参阅自定义系统日志报头，第 20 页。
- 通过创建模板来自定义消息正文。请参阅自定义系统日志消息正文，第 19 页。
- 在将系统日志客户端配置为用于解析的消息模板时使用 ISE-PIC 中预定义的消息模板，或者基于这些预定义的模板自定义报头或正文模板。请参阅使用系统日志预定义消息模板，第 23 页。

配置系统日志客户端

为了使思科 ISE-PIC 能够从特定客户端侦听系统日志消息，必须首先从思科 ISE-PIC 定义该特定客户端。您可以使用不同 IP 地址定义多个提供程序。

步骤 1 系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

步骤 2 要配置新系统日志客户端，请从表的顶部单击**添加 (Add)**。

步骤 3 填写所有必填字段（请参阅系统日志设置，第 14 页以获取更多详细信息），并在必要时创建消息模板（请参阅自定义系统日志消息正文，第 19 页以获取更多详细信息），以便正确配置客户端。

步骤 4 单击**提交 (Submit)**。

系统日志设置

配置思科 ISE-PIC 以通过来自特定客户端的系统日志消息接收用户身份，包括 MAC 地址。您可以使用不同 IP 地址定义多个提供程序。

表 6: 系统日志提供程序

字段名称	说明
名称	输入用于快速轻松地区分此已配置客户端的唯一名称。
说明	此系统日志提供程序的有意义说明。
状态	选择**已启用**可在完成配置时立即启用客户端。

字段名称	说明
主机	输入主机器的 FQDN。
连接类型	输入 UDP 或 TCP 以指示 ISE-PIC 用于侦听系统日志消息的通道。 注释 当所配置的连接类型为 TCP 时，如果消息报头存在问题且无法解析主机名，则思科 ISE 会尝试将数据包中接收到的 IP 地址与已为思科 ISE 中的系统日志消息配置的提供程序列表中任何提供程序的 IP 地址进行匹配。 要查看此列表，请依次选择 **提供程序 (Providers)** > **系统日志提供程序 (Syslog Providers)**。我们建议您检查消息报头并根据需要进行自定义，以便确保解析成功。有关自定义报头的详细信息，请参阅自定义系统日志报头，第 20 页。

字段名称	说明
模板	

字段名称	说明
	模板指示精确正文消息结构，以便解析器可以识别应解析、映射和传送的系统日志消息中的信息段。 例如，模板可以指示用户名的确切位置，以便解析器能够在接收到的每条消息中查找用户名。 从此字段中，指示要使用的模板（适用于系统日志消息的正文），以便识别并正确解析系统日志消息。 从预定义下拉列表中进行选择，或者点击**新建**以创建自己的自定义模板。有关创建新模板的详细信息，请参阅自定义系统日志消息正文，第 19 页。大多数预定义模板都使用正则表达式，并且自定义模板也应使用正则表达式。 **注释** 只能编辑或删除自定义模板，而无法修改下拉列表中的预定义系统模板。 ISE-PIC 当前提供下列预定义 DHCP 提供程序模板： • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP **注释** DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便思科 ISE 可以首先检查在本地会话目录（从“实时会话”(Live Sessionss) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。 如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。 思科 ISE 提供下列预定义常规系统日志提供程序

字段名称	说明
	模板： • ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN 有关模板的信息，请参阅使用系统日志预定义消息模板，第 23 页。
默认域	如果在特定用户的系统日志消息中未识别域，则会将此默认域自动分配给用户，以便确保为所有用户都分配域。 通过默认域或通过从消息中解析的域，会将用户名附加到 username@domain，从而包含该域，以便获取有关用户和用户组的详细信息。

自定义系统日志消息结构（模板）

模板指示精确消息结构，以便解析器可以识别应解析、映射和传送的系统日志消息中的信息段。例如，模板可以指示用户名的确切位置，以便解析器能够在接收到的每条消息中查找用户名。模板可确定新增和删除映射消息的受支持结构。

通过思科 ISE-PIC，您可以自定义单个消息报头和多个正文结构以供 ISE-PIC 解析器使用。

模板应包含正则表达式，用于定义用户名、IP 地址、MAC 地址和域的结构，以使 ISE-PIC 解析器能够正确识别消息是要添加还是删除用户身份映射，以及正确解析用户详细信息。

自定义消息模板时，可以选择基于 ISE-PIC 中预定义的消息模板进行自定义，参考这些预定义选项中使用的正则表达式和消息结构。有关预定义模板、正则表达式、消息结构、示例等的详细信息，请参阅使用系统日志预定义消息模板，第 23 页。

可以自定义：

- 单个消息报头 -自定义系统日志报头，第 20 页
- 多个消息正文 - 自定义系统日志消息正文，第 19 页。

注释 DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便思科 ISE 可以首先检查在本地会话目录（从“实时会话”(Live Sessionss) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。

无法将正确匹配、分析和映射 DHCP 消息中的详细信息所需的延迟应用于自定义模板，因此不建议对 DHCP 消息模板进行自定义。请改为使用任何预定义 DHCP 模板。

自定义系统日志消息正文

通过思科 ISE-PIC，您可以自定义将由 ISE-PIC 解析器解析的自有系统日志消息模板（通过自定义消息正文）。模板应包含正则表达式，以定义用户名、IP 地址、MAC 地址和域的结构。

注释 DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便思科 ISE 可以首先检查在本地会话目录（从“实时会话”(Live Sessionss) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。

无法将正确匹配、分析和映射 DHCP 消息中的详细信息所需的延迟应用于自定义模板，因此不建议对 DHCP 消息模板进行自定义。请改为使用任何预定义 DHCP 模板。

从系统日志客户端配置屏幕中创建和编辑系统日志消息正文模板。

注释 您只能编辑自己的自定义模板。无法更改系统提供的预定义模板。

步骤 1 系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

步骤 2 单击**添加(Add)**以添加新系统日志客户端，或者单击**编辑 (Edit)** 来更新已配置的客户端。有关配置和更新系统日志客户端的详细信息，请参阅配置系统日志客户端，第 14 页。

步骤 3 在**系统日志提供程序 (Syslog Providers)** 窗口中，单击**新建 (New)** 以创建新消息模板。要编辑现有模板，请从下拉列表中选择该模板，然后单击**编辑 (Edit)**。

步骤 4 填写所有必填字段。

有关如何正确输入值的信息，请参阅系统日志自定义模板设置和示例，第 21 页。

步骤 5 单击**测试 (Test)** 以根据所输入的字符串正确解析消息。

步骤 6 单击**保存 (Save)**。

自定义系统日志报头

系统日志报头还包含消息源于的主机名。如果思科 ISE-PIC 消息解析器未识别系统日志消息，则可能需要通过配置前置于主机名的分隔符来自定义消息报头，从而使思科 ISE-PIC 能够正确识别主机名并解析消息。有关此屏幕中的字段的更多详细信息，请参阅系统日志自定义模板设置和示例，第 21 页。只要接收到消息，便会将自定义报头配置保存并添加到解析器所使用的报头类型。

注释 只能自定义单个报头。自定义报头后，在单击**自定义报头 (Custom Header)** 并创建模板时，将仅保存最新配置。

步骤 1 系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

步骤 2 单击**自定义报头 (Custom Header)** 以打开“系统日志自定义报头”(Syslog Custom Header) 屏幕。

步骤 3 在**粘贴示例系统日志 (Paste sample syslog)** 字段中，输入系统日志消息中报头格式的示例。例如，从其中一条消息复制并粘贴以下报头：**<181>Oct 10 15:14:08 Cisco.com**。

步骤 4 在**分隔符 (Separator)** 字段中，指示单词是以空格还是制表符分隔。

步骤 5 在**报头中的主机名位置 (Position of hostname in header)** 字段中，指示报头中表示主机名的位置。例如，在以上提供的报头中，主机名是报头中的第四个单词。输入 4 可指示此位置。

主机名 (Hostname) 字段根据前三个字段中指示的详细信息来显示主机名。例如，如果**粘贴示例系统日志**中的报头示例如下：

<181>Oct 10 15:14:08 Cisco.com

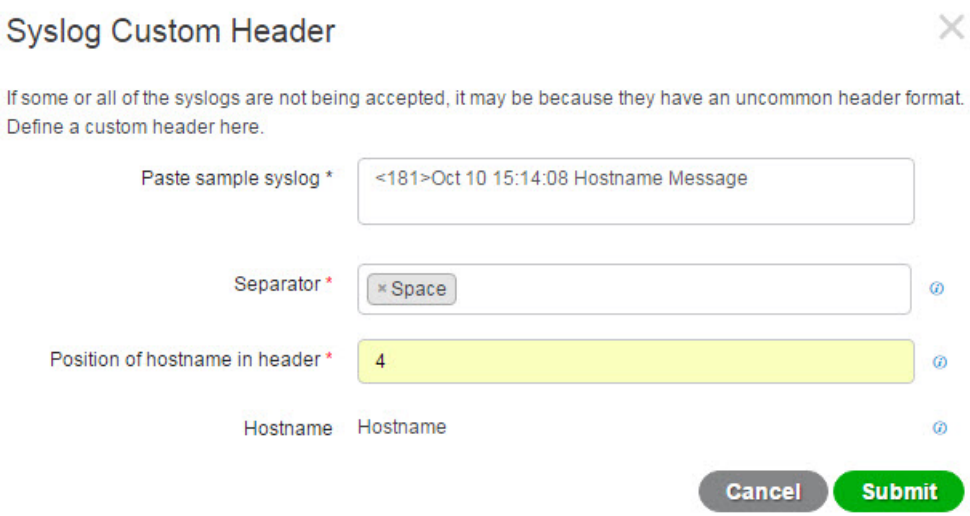
分隔符指示为**空格**，并且**报头中的主机名位置**输入为 4。

主机名将自动显示为 Cisco.com，这是**粘贴示例系统日志**字段中粘贴的报头短语中的第四个单词。

如果未正确显示主机名，请检查您已在**分隔符 (Separator)** 和**报头中的主机名位置 (Position of hostname in header)** 字段中输入的数据。

此示例与以下截屏相同：

图 *1:* 自定义系统日志报头



步骤 6 单击**提交 (Submit)**。
只要接收到消息，便会将自定义报头配置保存并添加到解析器所使用的报头类型。

系统日志自定义模板设置和示例

通过思科ISE-PIC，您可以自定义将由ISE-PIC解析器解析的自有系统日志消息模板。自定义模板确定了新增和删除映射消息的受支持结构。模板应包含正则表达式，用于定义用户名、IP地址、MAC地址和域的结构，以使 ISE-PIC 解析器能够正确识别消息是要添加还是删除用户身份映射，以及正确解析用户详细信息。

注释 大多数预定义模板都使用正则表达式。自定义模板也应使用正则表达式。

系统日志报头部分

您可以通过配置前置于主机名的分隔符来自定义系统日志探测器可识别的单个报头。

下表介绍可在自定义系统日志报头中包含的不同部分和字段。有关正则表达式的详细信息，请参阅表 9: 自定义模板的正则表达式，第 23 页。

表 7: 系统日志自定义报头

字段	说明
粘贴示例系统日志	输入系统日志消息中的报头格式的示例。例如，复制并粘贴以下报头： **<181>Oct 10 15:14:08 Hostname Message**
分隔符	指示单词是以空格还是制表符分隔。
报头中的主机名位置	指示报头中表示主机名的位置。例如，在以上提供的报头中，主机名是报头中的第四个单词。输入 4 可指示此位置。
主机名 (Hostname)	根据前三个字段中指示的详细信息来显示主机名。例如，如果**粘贴示例系统日志**中的报头示例如下： <181>Oct 10 15:14:08 Hostname Message 分隔符指示为**空格**，并且**报头中的主机名位置**输入为 4。 **主机名**将自动显示为 Hostname。 如果未正确显示主机名，请检查您已在**分隔符**和**报头中的主机名位置**字段中输入的数据。

消息正文的系统日志模板部分和说明

下表介绍可在自定义系统日志消息模板中包含的不同部分和字段。有关正则表达式的详细信息，请参阅表 9: 自定义模板的正则表达式，第 23 页。

表 8: 系统日志模板

部件	字段	说明
	名称	用于识别此模板的用途的唯一名称。
映射操作	新映射	描述与此模板配合用于添加新用户的映射类型的正则表达式。例如，在此字段中输入“logg on from”可指示已登录到 F5 VPN 的新用户。
	已删除的映射	描述与此模板配合用于删除用户的映射类型的正则表达式。例如，在此字段中输入“sess disconnect”可指示应为 ASA VPN 删除的用户。

部件	字段	说明
用户数据	IP 地址	指示要捕获的 IP 地址的正则表达式。 例如，对于 Bluecat 消息，要捕获此 IP 地址范围内的用户的身份，请输入： (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][(
	用户名	指示要捕获的用户名格式的正则表达式。
	域	指示要捕获的域的正则表达式。
	MAC 地址	指示要捕获的 MAC 地址格式的正则表达式。

正则表达式示例

要解析消息，请使用正则表达式。此部分提供正则表达式示例，以便解析 IP 地址、用户名和添加映射消息。

例如，使用正则表达式解析以下消息：

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

正则表达式按下表中进行定义。

表 *9:* 自定义模板的正则表达式

部件	正则表达式
IP 地址	Address <([^\s]+)>|address ([^\s]+)
用户名	User <([^\s]+)>| Username = ([^\s]+)
添加映射消息	(%ASA-4-722051|%ASA-6-713228)

使用系统日志预定义消息模板

系统日志消息具有包含报头和消息正文的标准结构。

本节介绍了思科 ISE-PIC 提供的预定义模板，包括根据消息源支持的报头以及受支持正文结构的内容详细信息。

此外，您可以使用系统中未预定义的源的自定义正文内容来创建自己的模板。本节还介绍了自定义模板的受支持结构。解析消息时，除系统中预定义的报头以外，您还可以配置要使用的单个自定义报头，并且可为消息正文配置多个自定义模板。有关自定义报头的详细信息，请参阅自定义系统日志报头，第 20 页。有关自定义正文的详细信息，请参阅自定义系统日志消息正文，第 19 页。

注释 大多数预定义模板都使用正则表达式，并且自定义模板也应使用正则表达式。

消息报头

有两种可由解析器识别的报头类型：适用于所有消息类型（新增和删除）和适用于所有客户端机器。这些报头如下：

- <171>Host message
- <171>Oct 10 15:14:08 Host message

收到后，系统将解析报头以获取主机名，它可以是 IP 地址、主机名或完整 FQDN。

此外，还可以自定义报头。要自定义报头，请参阅自定义系统日志报头，第 20 页。

系统日志 ASA VPN 预定义模板

ASA VPN 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 23 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 ASA VPN 正文消息。

正文消息	解析示例
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] 注释 从此消息类型解析的 IP 地址是私有 IP 地址，如消息中所示。
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] 注释 从此消息类型解析的 IP 地址是 IPv4 地址。

删除映射正文消息

解析器支持的 ASA VPN 删除映射消息如此部分所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[UserA,10.1.1.1]

正文消息
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason

正文消息
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

系统日志 Bluecat 预定义模板

支持的系统日志消息格式和 Bluecoat 类型如下所述。

报头

如使用系统日志预定义消息模板，第 23 页中所述，对于所有客户端，解析器支持的报头都相同。

新映射正文消息

Bluecat 系统日志的新映射支持的消息如本部分所述。

收到正文消息后，如下解析正文以获取用户详细信息：

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

正文
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

删除映射消息

Bluecat 没有已知的删除映射消息。

系统日志 F5 VPN 预定义模板

F5 VPN 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 23 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 F5 VPN 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[user=UserA,ip=172.16.0.12]

正文
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security [nnnnn]：[UserA @ vendor-abcr] User UserA login on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz \

删除映射消息

目前没有支持的 F5 VPN 删除消息。

系统日志 Infoblox 预定义模板

Infoblox 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 23 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 ASA VPN 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

正文消息
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

删除映射消息

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

- 如果包含 MAC 地址：

  [00:0c:29:a2:18:34,10.0.10.100]

- 如果不包含 MAC 地址：

  [10.0.10.100]

正文消息
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

系统日志 Linux DHCPd3 预定义模板

Linux DHCPd3 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板 ， 第 23 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射消息

如下表所述，解析器可识别不同的 Linux DHCPd3 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

正文消息
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

删除映射正文消息

解析器支持的 Linux DHCPd3 删除映射消息如此部分所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[00:0c:29:a2:18:34 ,10.0.10.100]

正文消息
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

系统日志 MS DHCP 预定义模板

MS DHCP 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 23 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

解析器可识别不同的 MS DHCP 正文消息，如下表所述。

接收后，解析器会通过搜索逗号 (,) 来分隔数据，然后解析这些格式的消息，如以下示例所示：

[macAddress=000C29912E5D,ip=10.0.10.123]

正文消息
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,0x4D53465420352E30,MSFT,5.0

删除映射正文消息

解析器解析的 MS DHCP 支持的删除映射消息如此部分所述。

接收后，解析器会通过搜索逗号 (,) 来分隔数据，然后解析这些格式的消息，如以下示例所示：

[macAddress=000C29912E5D,ip=10.0.10.123]

正文消息
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0

系统日志 SafeConnect NAC 预定义模板

SafeConnect NAC 支持的系统日志消息格式和类型如下所述。

报头

如使用系统日志预定义消息模板，第 23 页中所述，对于所有客户端，解析器支持的报头都相同。

新映射正文消息

解析器可识别不同的 SafeConnect NAC 正文消息，如下表所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

正文消息
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

删除映射消息

目前没有 Safe Connect 支持的删除消息。

系统日志 Aerohive 预定义模板

Aerohive 支持的系统日志消息格式和类型如下所述。

信头

如使用系统日志预定义消息模板，第 23 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 Aerohive 正文消息。

从正文解析的详细信息包括用户名和 IP 地址。用于解析的正则表达式如以下示例所示：

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

收到正文消息后，如下解析正文以获取用户详细信息：

[UserA,10.5.50.52]

正文消息
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

删除映射消息

系统当前不支持从 Aerohive 删除映射消息。

系统日志 Blue Coat 预定义模板 - 主代理、代理 SG、Squid Web 代理

系统支持 Blue Coat 的以下消息类型：

- BlueCoat 主代理
- BlueCoat 代理 SG
- BlueCoat Squid Web 代理

支持的系统日志消息格式和 Bluecoat 消息类型如下所述。

信头

如使用系统日志预定义消息模板，第 23 页中所述，对于所有客户端，解析器支持的信头都相同。

新映射正文消息

解析器可识别不同的 Blue Coat 正文消息，如下表所述。

收到正文消息后，如下解析正文以获取用户详细信息：

[UserA,192.168.10.24]

正文消息（此示例摘自 **BlueCoat** 代理 **SG** 消息）
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

下表介绍了每个客户端用于新映射消息的不同正则表达式结构。

客户端	正则表达式
BlueCoat 主代理	新映射 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,}:{1,2}){1,7}[a-zA-Z0-9]{1,})\s** 用户名 **\s\-\s([a-zA-Z0-9_]+)\s\-\s**
BlueCoat 代理 SG	新映射 **(\-\sPROXIED){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,}:{1,2}){1,7}[a-zA-Z0-9]{1,}|::[a-zA-Z0-9_]+)\s** 用户名 **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**
BlueCoat Squid Web 代理	新映射 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,}:{1,2}){1,7}[a-zA-Z0-9]{1,})\sTCP** 用户名 **\s([a-zA-Z0-9\._]+)\s\-\/**

删除映射消息

Blue Coat 客户端支持删除映射消息，但当前没有提供相关示例。

下表介绍了每个客户端用于删除映射消息的不同的已知正则表达式结构示例。

客户端	正则表达式
BlueCoat 主代理	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat 代理 SG	当前无可用示例。
BlueCoat Squid Web 代理	**(TCP_MISS|TCP_NC_MISS){1}**

系统日志 ISE 和 ACS 预定义模板

侦听 ISE 或 ACS 客户端时，解析器将接收以下消息类型：

- 通过身份验证：当用户经 ISE 或 ACS 进行身份验证后，通过身份验证消息将发出以通知身份验证已成功，并包含用户详细信息。系统将解析此消息，并保存此消息中的用户详细信息和会话 ID。
- 记帐启动和记帐更新消息（新映射）：从 ISE 或 ACS 接收的记帐启动或记帐更新消息将进行解析，并包含在通过身份验证消息中保存的用户详细信息和会话 ID，然后映射用户。
- 记帐停止（删除映射）：从 ISE 或 ACS 接收后，用户应设将从系统中删除。

ISE 和 ACS 支持的系统日志消息格式与类型如下所述。

通过身份验证消息

通过身份验证类型支持以下消息。

- 标题

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例如：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 正文

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=1.1.1.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- 解析示例

  仅解析用户名和会话 ID。

  [UserA,5]

记帐启动/更新（新映射）消息

新映射支持以下消息。

- 标题

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例如：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 正文

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- 解析示例

  解析的详细信息包括用户名、成帧的 IP 地址以及 MAC 地址（如果消息中包括）。

  [UserA,10.0.0.16]

删除映射消息

删除映射支持以下消息。

- 标题

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例如：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 正文

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- 解析示例

  解析的详细信息包括用户名、成帧的 IP 地址以及 MAC 地址（如果消息中包括）。

  [UserA,10.0.0.16]

系统日志 Lucent QIP 预定义模板

Lucent QIP 支持的系统日志消息格式和类型如下所述。

报头

如使用系统日志预定义消息模板，第 23 页中所述，对于所有客户端，解析器支持的报头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 Lucent QIP 正文消息。

这些消息的正则表达式结构如下：

DHCP_GrantLease|:DHCP_RenewLease

收到正文消息后，如下解析正文以获取用户详细信息：

[00:0C:29:91:2E:5D,10.0.0.11]

正文消息
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

删除映射正文消息

这些消息的正则表达式结构如下所示：

删除租约:|DHCP 自动释放:

收到正文消息后，如下解析正文以获取用户详细信息：

[10.0.0.11]

正文消息
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

过滤被动身份服务

您可以根据用户名称或 IP 地址过滤某些用户。例如，如果 IT 服务中的管理员登录到终端以帮助该终端的常规用户，则可以过滤掉管理员活动，从而在“实时会话”中不显示管理员活动，而是仅显示该终端的常规用户。实时会话显示映射过滤器未过滤掉的被动身份服务组件。您可以按照需要添加很多过滤器。“OR”逻辑运算符适用于过滤器之间。如果在单个过滤器中同时指定两个字段，则在这两个字段之间使用“AND”逻辑运算符。

步骤 1 选择**提供程序 (Providers)** > **映射过滤器 (Mapping Filters)**。

步骤 2 单击**添加 (Add)**，输入您想要过滤的用户的用户名和 Ip 地址，然后单击**提交 (Submit)**。

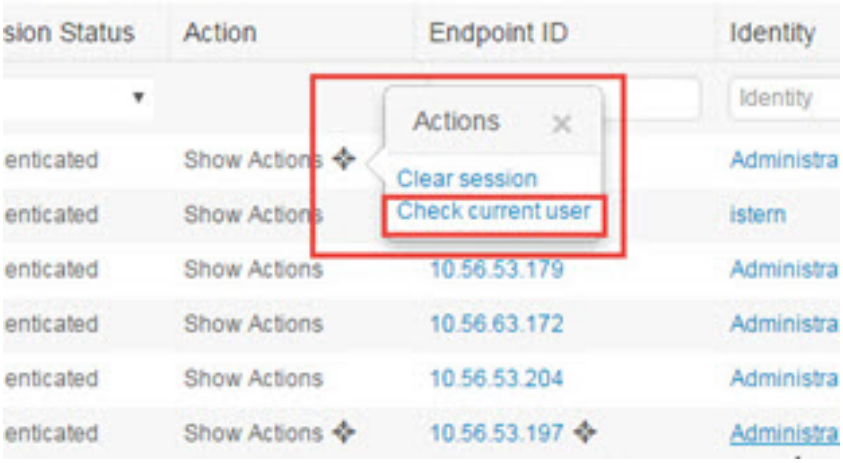
终端探测器

除可以配置的自定义提供程序以外，安装时默认在 ISE-PIC 中启用终端探测器，并且始终在后台运行。终端探测器会定期检查每个特定用户是否仍已登录到系统。

注释 为了确保终端在后台运行，您必须首先配置初始 Active Directory 加入点，并确保选择**存储凭证**。有关配置终端探测器的详细信息，请参阅使用终端探测器，第 36 页。

要手动检查终端状态，请转至**实时会话 (Live Sessions)**，从**操作 (Actions)** 列单击**显示操作 (Show Actions)**，然后选择**检查当前用户 (Check current user)**，如下图所示。

图 *2:* 检查当前用户



有关终端用户状态以及手动运行检查的详细信息，请参阅实时会话。

当终端探测器识别用户已连接时，如果自上次为特定终端更新会话已经过 4 小时，则它将检查该用户是否仍已登录并收集以下数据：

- MAC 地址
- 操作系统版本

根据此检查，探测器将执行以下操作：

- 当用户仍处于登录状态时，探测器将使用“活动用户”(Active User) 状态更新思科 ISE-PIC。
- 当用户已注销时，会话状态更新为“已终止”，15 分钟后，将从会话目录中删除用户。
- 当无法联系用户时（例如，当防火墙阻止联系或者终端已关闭时），状态更新为“无法访问”，并且用户策略将确定如何处理用户会话。终端将保持处于会话目录中。

使用终端探测器

开始之前

安装 ISE-PIC 后，默认情况下会启用终端探测器。要启用和禁用探测器，请首先确保您已配置下列各项：

- 终端必须具有与端口 445 的网络连接。
- 从 ISE-PIC 配置初始 Active Directory 加入点。有关加入点的详细信息，请参阅 Active Directory 作为探测器和提供程序。

注释 为了确保终端在后台运行，您必须首先配置初始 Active Directory 加入点，通过它可使终端探测器即便在 Active Directory 未完全配置时也能够运行。

步骤 1 选择**提供程序 (Providers)** > **终端探测器 (Endpoint Probes)**。

步骤 2 选择**已启用 (Enabled)** 或**已禁用 (Disabled)**。
屏幕不会更改。但是，探测器根据选择进行启用或禁用，如果已启用，则此时正在后台运行并收集数据。