思科身份服务引擎 API 参考指南，版本 2.x

思科系统公司
www.cisco.com

思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站：
www.cisco.com/go/offices.

文本部件号：OL-26134-01

目 录

前言

思科身份服务引擎概述

思科身份服务引擎 (ISE) 是下一代身份和访问控制策略平台，可帮助企业执行策略规定、加强基础设施安全以及简化服务操作。凭借 Cisco ISE 的独特架构，企业可以通过把身份绑定到各种网络元素（包括访问交换机、无线局域网控制器 (WLC)、虚拟专用网络 (VPN) 网关和数据中心交换机），从网络、用户和设备收集实时背景信息，从而做出前瞻性的管理决策。

Cisco ISE 是思科安全组访问解决方案的关键组件。Cisco ISE 是一个统一的基于策略的访问控制解决方案具有以下：

- 将身份验证、授权、会计(AAA)、状态、分析和访客管理服务到设备
- 通过检查访问网络，包括 802.1X 环境的所有终端设备状态执行终端合规性
- 提供发现、分析、基于策略的布局和监控网络上的终端设备支持
- 在集中式和分布式部署中启用一致的策略，以实现根据实际需要交付服务
- 通过使用安全组标记 (SGT) 和安全组 (SG) 访问控制列表 (ACL) 使用高级实施功能，包括安全组访问 (SGA)
- 支持将多种部署方案从小型办公室扩展到大型企业环境的可扩展性

Cisco ISE 架构支持独立和分布式部署，允许您配置和管理您的从一个集中的门户的网络。有关 Cisco ISE 的功能的详细信息，请参阅《*思科身份服务引擎管理指南*》。

目的

此应用编程接口 (API) 参考指南提供支持的 API 提供的功能的仅短暂高级概述。此 API 参考指南的目的是为开发人员、系统或网络管理员或系统集成了基本的指导原则使用在 Cisco ISE 配置中概述的 API。

REST API 呼叫使用查询确定数据的以下类型的

- 活动会话的数量
- 活动会话的类型
- 活动会话的身份验证状态
- MAC 地址在使用中
- 在使用 NAS 的 IP 地址
- 节点版本和类型
- 节点会话失败的原因

外部 RESTful 服务 API 和相关 API 调用可用于对 Cisco ISE 资源执行 CRUD（创建、读取、更新、删除）操作。外部宁静的服务根据 HTTP 协议和其他方法。

备注 有关 Cisco ISE 网络及其节点和角色、操作概念或用法以及 Cisco ISE 用户界面使用方法的详细信息，请参阅《*思科身份服务引擎观礼指南*》。

受众

此 API 参考指南为管理网络环境中的 Cisco ISE 设备，系统集成可能要利用 API，或第三方合作伙伴与管理或排除 Cisco ISE 配置的责任的有经验的系统管理员使用。为使用此 API 参考指南的一个前提条件，您应该有故障排除和诊断工作有基本的了解和如何发出和解释 API 调用。

文档约定

本节概述约定使用在本文中。

注意 表示*读者应当小心*。您的某些操作可能会导致设备损坏或数据丢失。

备注 表示*读者需要注意的地方*。注释中包含有用的建议或包含对本手册中所没有的材料的引用。

此 API 参考指南使用以下约定表示指令和信息。

项目	约定
命令、关键字、特殊应选择在过程中的术语和选项	**粗体**
由您提供值和新或重要术语的变量	*斜体*
显示的会话和系统信息、路径和文件名	`screen` 字体
您输入的信息	**屏幕粗体**
您输入的变量	*屏幕斜体*
菜单项和按钮名称	**粗**体
表示菜单项按您选择其顺序选择。	**选项 > 网络首选项**

相关文档

本节在 Release - Specific 文档提供信息，以及 Platform - Specific 文档。

Cisco ISE 的一般产品信息位于 http://www.cisco.com/go/ise。最终用户文档位于 Cisco.com 上的 http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html。

Platform - Specific 文档

- Cisco Secure ACS
  http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html
- Cisco NAC 设备
  http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html
- Cisco NAC 分析器
  http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
- Cisco NAC 访客服务器
  http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html

获取文档和提交服务请求

关于如何获取文档、提交服务请求和收集其他信息的信息，请参阅每月的*思科产品文档更新*，其中还含有所有最新及修订的思科技术文档，此文档位于：

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

通过 Really Simple Syndication (RSS) 源的方式订阅*思科产品文档更新*，相关内容将通过阅读器应用直接发送至您的桌面。RSS 源是一项免费服务，思科目前支持 RSS 2.0 版本。

第 1 部分

Cisco ISE 监控 REST API

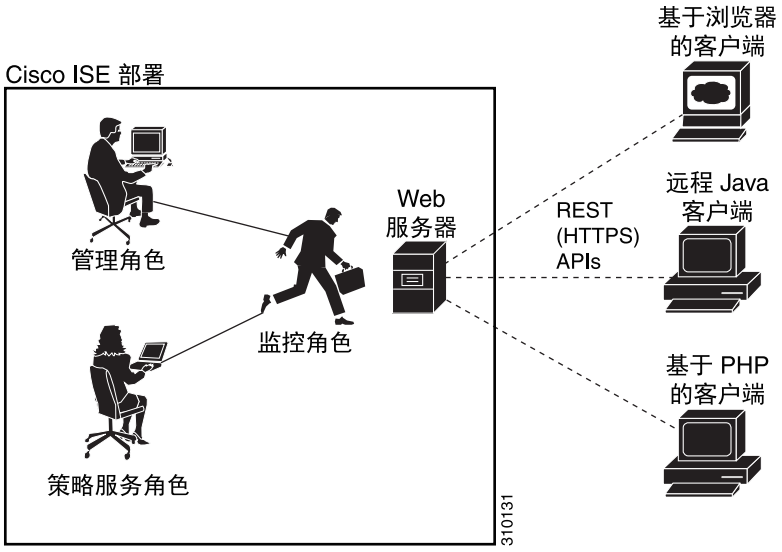
监控 REST API 简介

通过在您的网络，以监控节点监控的 REST API 允许您收集会话和节点特定信息。当您访问所需的节点并完成操作需要收集信息时，会话定义为持续时间在之间。

监控 REST API 呼叫在网络允许您隔离，监控和累计在单个终端上存储的重要实时，基于会话的信息。您可以通过监控节点的此信息。

实时，您收集可帮助了解 Cisco ISE 操作并帮助诊断情况或问题的基于会话的信息。它还可用于故障排除可影响监控操作的错误状态或活动或行为。如图 1-1 所示，监控的 REST API 呼叫用于访问监控节点和检索在 Cisco ISE 配置终端已存储的重要基于会话的信息。

图 1-1　　监控在分布式部署的 REST API 呼叫



要使用监控 REST API 执行操作，用户必须被分配至以下管理员组之一，而且必须通过存储在思科 ISE 内部数据库中的凭证进行身份验证（内部管理员用户）：

- 超级管理员
- 系统管理员
- MnT 管理员

系统支持以下监控 REST API 类别：

- 会话管理
- 故障排除
- 授权更改 (CoA)

您可以使用这些 API 收集有关被监控角色监控的终端的信息。对于本指南其他，“监控节点”将用于描述 Cisco ISE 节点的监控作用。

所有尝试使用这些类别收集有关 Cisco ISE 设备的策略服务角色的信息产生错误。有关思科 ISE 节点和角色的详细信息，请参阅 *《思科身份服务引擎管理员指南》*。

验证监控节点

准备工作

才能成功传输之前 API 在监控节点，您不需要验证要监控的节点是有效的。

备注　使用有效的凭证，希望能够使用公共监控的 REST API，您必须首先是否与 Cisco ISE。

步骤 1　在思科 ISE 登录窗口中输入有效的登录凭证（用户名和密码），然后点击**登录**。

Cisco ISE 仪表板和用户界面显示。

步骤 2　选择 **Authorization > System > Deployment**。

系统将显示 Deployment Nodes 页面，其中列出所部署的所有已配置的节点。

步骤 3　在部署节点的列呼叫的角色，验证您要监控的目标节点的角色列为监控节点。

支持的 API 呼叫

下表介绍 API 呼叫不同类型并提供 API 呼叫格式的示例

- 表 1-1，第 1-2 页 - 定义用于会话管理的 API 调用。
- 表 1-2，第 1-5 页 - 定义用于故障排除的 API 调用。
- 表 1-3，第 1-6 页 - 定义 CoA API 调用。

如果您要使用通用编程接口是否与 Cisco ISE 支持的显示器的 REST API，您需要先创建桥接 Cisco ISE 和特定工具您使用的基于 REST 的客户端。然后使用此 REST 客户端是否与 Cisco ISE 监控 REST API，安排和提交 API 请求到监控节点，然后 unmarshal API 响应和转发到指定的工具。

表 1-1　Cisco ISE Session Management API 呼叫

API 呼叫类别	说明和示例
会话计数器	
ActiveCount	列出了“活动会话的数量”。 https://<ISEhost>/admin/API/mnt/Session/ActiveCount **备注**　要查看活动会话数，您必须在 HTTP 身份验证报头中添加身份验证凭证。

表 1-1　Cisco ISE Session Management API 呼叫（续）

API 呼叫类别	说明和示例
PostureCount	列出 Postured 终端的数量。 https://<ISEhost>/admin/API/mnt/Session/PostureCount **备注**　状态处于控制中帮助该状态的服务（或状态）所有终端连接到 Cisco ISE 网络。Cisco ISE 为检查设备的状态合规性使用 NAC 代理。
ProfilerCount	列出了活动的分析器服务会话数量。 https://<ISEhost>/admin/API/mnt/Session/ProfilerCount **备注**　分析器是在确定，找到和定位为所有相连的终端功能在 Cisco ISE 网络的服务。
会话列表 **备注**　会话列表包括 MAC 地址、网络接入设备 (NAD) IP 地址，用户名和会话 ID 信息与会话相关联。	
ActiveList	列出所有活动会话。 https://<ISEhost>/admin/API/mnt/Session/ActiveList **备注**　在此 Cisco ISE 版本中，可以显示且经过身份验证的最大活动终端会话数为 250000。
AuthList	列出所有当前活动的已验证的会话。 https://<ISEhost>/admin/API/mnt/Session/AuthList/<parameteroptions> 您可以指定将返回不同值的以下参数选项卡 • 空/空列出所有激活已验证会话。 • 空/Endtime 列出所有激活已验证会话在指定的结束时间之后。 • 开始/空列出所有活动在指定的开始时间之前的已验证的会话。 • 开始/Endtime 列出所有活动在指定的开始时间和结束时间之间的已验证的会话。 输入日期和时间的开始时间和结束时间使用以下格式 YYYY - MM - DD hh : mm 格式 mm : ss.s 其中： • YYYY 四年数字 • MM 两个数字个月（01=January，等等） • DD 两 Num 天（ 01 - 31） • HH 两位小时（ 00 - 23）（客户经理和 p.m、不允许） • 毫米两位分钟（ 00 - 59） • 接下来 hh : mm : ss 两位（ 00 - 59） • 表示十进制一转眼工夫的 s - one 或更多数字 **备注**　每个 Cisco ISE 节点配置时区。建议使用的时区为 UTC。 用于采样从与空/空选项的 AuthList API 调用返回的数据，第 2-9 页显示所有四个参数选项的示例，请参阅。

表 1-1　Cisco ISE Session Management API 呼叫（续）

API 呼叫类别	说明和示例
会话属性 **备注**　这是包含指定的搜索属性的最新的会话的基于时间戳的搜索。	
MAC 地址	搜索数据库包含指定的 MAC 地址的最新的会话。 https://<ISEhost>/admin/API/mnt/Session/MACAddress/<macaddress> **备注**　XX:XX:XX:XX:XX:XX 是 MAC 地址格式不区分大小写（例如，答案 0a:0B:0c:0D:0e:0F）。 **备注**　MAC 地址作为唯一的唯一密钥对找到您要监控的正确的会话。使用 ActiveList API 呼叫列出所有活动会话和其 MAC 地址，您可以根据自己的 MAC 地址搜索。
UserName	搜索数据库包含指定的用户名的最新的会话。 https://<ISEhost>/admin/API/mnt/Session/UserName/<username> **备注**　用户名必须符合用于网络用户名相同的 Cisco ISE 密码策略。监控 REST API 的唯一无效字符为反斜线（\）字符。有关详细信息，请参阅“用户密码策略”在*思科身份服务引擎用户指南，版本1.1*。
IPAddress（IP 地址）	搜索数据库中包含指定 NAS IP 地址（IPv4 或 IPv6 地址）的最新会话。 https://<ISEhost>/admin/API/mnt/Session/IPAddress/<nasipaddress> **备注**　xxx.xxx.xxx.xxx 是 NAS IP 地址格式（例如，10.10.10.10） 或 https://<ISEhost>/admin/API/mnt/Session/IPAddress/<nasipv6address> **备注**　xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx 是 NAS IPv6 地址格式（例如，2001:cdba:0:0:0:0:3247:9651）
Audit Session ID	搜索数据库包含指定的审计会话 ID 的最新的会话。 https://<ISEhost>/admin/API/mnt/Session/Active/SessionID/<audit - session - id>/0 **备注**　使用 ActiveList API 呼叫列出所有活动会话及其审计会话 ID，您可以根据您的会话 ID 搜索。或者，您可以获得实时会话页面的审计会话 ID 在管理员门户。

有关 Cisco ISE API 呼叫的特定详细信息请求会话管理，请参阅第 2 章“会话管理查询 API”。

表 1-2　排除 API 呼叫 - 故障排除的 Cisco ISE

API 调用	说明和示例
版本	列出节点版本和类型。 https://<ISEhost>/admin/API/mnt/Version 节点类型可以是下列值（ 0 - 3）中的任何一个。 0 - STAND_ALONE_MNT_NODE 1 - ACTIVE_MNT_NODE 2 - STAND_BY_MNT_NODE 3 - NOT_AN_MNT_NODE **备注** STAND_ALONE_MNT_NODE 意味着它是在任何已分配的配置无法正常运行的监控节点。 ACTIVE_MNT_NODE 意味着它是一个主要的关系的主节点在分布式部署。 STAND_BY_MNT_NODE 意味着它是一个主要的第二个的辅助节点在分布式部署。 NOT_AN_MNT_NODE 意味着它不是监控节点。有关*支持的 ESS 节点和人员的*详细信息，请参阅思科身份服务引擎用户指南，版本1.1。
FailureReasons	列出故障的原因。 https://<ISEhost>/admin/API/mnt/FailureReasons 每个故障原因显示错误代码（failureReason ID），简短说明（代码），故障原因（原因）和一个可能的响应（分辨率），如以下示例所示： <failureReason id= "100009" > <code> 100009 WEBAUTH_FAIL <cause> 可以或可能不指示违规。 <resolution> 根据您组织的策略请查看并解决此问题。 **备注** FailureReasons API 呼叫仅一次将调用收集从监控节点的信息。您应存储所有返回的故障原因拖动到文件系统或数据库。这些 API 调用返回的目录供参考使用。如果您在身份验证过程中遇到任何问题，您应当比较故障原因代码列表故障原因在验证响应提供的您在您的文件系统或数据库存储了。 有关 Cisco ISE 故障原因的完整列表，请参阅附录 A“Cisco ISE 故障原因报告”。
AuthStatus	列出所有会话的身份验证状态。 https://<ISEhost>/admin/API/mnt/AuthStatus/MACAddress/<macaddress>/<numberofseconds>/<numberofrecordspermacaddress>/All **备注** 秒参数 <numberofseconds> 是用户可配置的，范围为 0 秒至 432000 秒（5 天）。

表 1-2　排除 API 呼叫 - 故障排除的 Cisco ISE（续）

API 调用	说明和示例
获得 ISN 客户状态	
AcctStatus	列出所有会话的客户状态在给定时间段内。 https://<ISEhost>/admin/API/mnt/AcctStatusTT/MACAddress/<macaddress>/<numberof seconds> **备注**　秒参数<numberofseconds>与该范围是用户可配置的，是从 0 - 432000 秒（5 天）。

有关 Cisco ISE API 呼叫的特定详细信息请求进行故障排除，请参阅第 2 章“会话管理查询 API”。

表 1-3　权限 API 呼叫 Cisco ISE 更改

API 调用	说明和示例
Reauth	发送一个默认端口命令和类型。 https://<ISEhost>/admin/API/mnt/CoA/Reauth/<serverhostname>/<macaddress>/<reauthtype>/<nasipaddress>/<destinationipaddress> 其中 <*ISEhost*> 表示 ESS 主机的 IP 地址，<*serverhostname*> 表示 ESS 服务器的名称，<*nasipaddress*> 表示 NAS 的确定的 IP 地址，而且，<*destinationipaddress*> 表示目标的 IP 地址。 Reauth 类型可以是下列值（ 0 - 2）中的任何一个。 0 - REAUTH_TYPE_DEFAULT 1 - REAUTH_TYPE_LAST 2 - REAUTH_TYPE_RERUN **备注**　如果您不知道 NAS IP 地址，您可以输入所需的值向上传送到该点，并 API 在其搜索查询将使用这些值。但是，您必须知道 MAC 地址执行此 API 调用，但是，您可以从 NAS IP 地址开始将其它参数为空。如果提供了 NAS IP 地址还提供目标 IP 地址是必要的。 此 API 呼叫在一台显示器上 ESS 节点只能执行，提交请求远程执行 CoA。管理 ESS 节点不是包含或所需的执行这些 CoA API 呼叫。

表 1-3　　权限 API 呼叫 Cisco ISE 更改（续）

API 调用	说明和示例
会话断开连接	
Disconnect	发送一个会话断开命令和端口选项类型。 https://<ISEhost>/admin/API/mnt/CoA/Disconnect/<serverhostname>/<macaddress>/<disconnecttype>/<nasipaddress>/<destinationipaddress> 端口选项类型可以是下列值（ 0 - 2）中的任何一个。 0 - DYNAMIC_AUTHZ_PORT_DEFAULT 1 - DYNAMIC_AUTHZ_PORT_BOUNCE 2 - DYNAMIC_AUTHZ_PORT_SHUTDOWN **备注**　如果您不知道 NAS IP 地址，请输入所需的值向上传送到该点，并 API 在其搜索查询将使用这些值。但是，您必须知道 MAC 地址执行此 API 调用，但是，您可以将其他参数为空。

有关权限 API 呼叫的详情 Cisco ISE 更改，请参阅第 4 章“权限 REST API 更改”。

HTTP 将 API 呼叫

类似于 AuthStatus API 呼叫表 1-2，可让客户端检索客户状态 API 呼叫的 HTTP Put 版本。监控的 REST API 支持 Put HTTP 和 HTTP GET 呼叫，与提供 HTTP GET 呼叫的此指南的示例。Put HTTP 处理要求参数输入的呼叫的需求。以下架构文件示例是一个需要客户状态：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="acctRequest" type="mnTRESTAcctRequest"/>
<xs:complexType name="mnTRESTAcctRequest">
    <xs:complexContent>
      <xs:extension base="mnTRESTRequest">
        <xs:sequence>
          <xs:element name="duration" type="xs:string" minOccurs="0"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="mnTRESTRequest" abstract="true">
    <xs:sequence>
      <xs:element name="valueList">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="value" type="xs:string" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="searchCriteria" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

会话管理查询 API

本章介绍检索重要会话相关的信息提供方法从监控您的 Cisco ISE 部署的思科内部 ESS 节点的会话管理 API 呼叫。

会话计数器 API 呼叫

以下会话计数器 API 呼叫可让您快速收集当前计数有关目标监控您的 Cisco ISE 配置的 Cisco 的会话相关的信息 ESS 节点：

- 活动会话（ActiveCount）- 活动会话已验证在网络中的一个。
- 状况评估的会话（PostureCount）- 状况评估的状态断言，当状态结束时（兼容/不合规）。状态是可选的，例如，IP 电话/打印机不会转到状况评估的状态。状况评估的状态是一个短期的临时状态，因为在状况评估后，它将移至开头的状态，在设置时认为的开始时间。
- 已分析的会话（ProfilerCount）

如果终端陷在任何一个阶段，这些不同状态被视为故障排除。

活动会话计数器

您可以使用 ActiveCount API 呼叫检索的计数所有当前活动的会话。

备注 要查看活动会话数，您必须在 HTTP 身份验证报头中添加身份验证凭证。

ActiveCount API 输出方案

此示例架构文件是 ActiveCount API 呼叫的输出请求检索活动会话的计数 ESS 节点的目标监控作用的：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="sessionCount" type="activeCount"/>
  <xs:complexType name="activeCount">
    <xs:sequence>
      <xs:element name="count" type="xs:int"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

调用 ActiveCount API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与 ActiveCount API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/ <specific - api - call>）：

```
https://acme123/admin/API/mnt/Session/ActiveCount
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定表示该目标监视器 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从 ActiveCount API 调用返回的数据

以下示例说明返回的数据（活动会话数），当您将在目标监视器 ESS 节点时的 Cisco 的一 ActiveCount API 呼叫：

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.
-
<sessionCount>
<count>5</count>
</sessionCount>
```

计数器状态的会话

您可以使用 PostureCount API 呼叫检索当前计数所有当前活动的会话状态。

PostureCount API 输出方案

此示例架构文件是 PostureCount API 呼叫的输出请求检索当前有效的会话状态的计数目标的监控 ESS 节点的 Cisco：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="sessionCount" type="postureCount"/>

  <xs:complexType name="postureCount">
    <xs:sequence>
```

```
      <xs:element name="count" type="xs:int"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

调用 PostureCount API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与PostureCount API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/Session/ <specific - api - call>）：

```
https://acme123/admin/API/mnt/Session/PostureCount
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定表示该目标监视器 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从 PostureCount API 调用返回的数据

以下示例说明返回的数据（当前有效的状态会话数），当您将在目标监视器 ESS 节点时的 Cisco 的一 PostureCount API 呼叫：

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<sessionCount>
<count>3</count>
</sessionCount>
```

计数器分析器的会话

您可以使用 ProfilerCount API 呼叫检索的计数所有当前活动的分析器会话。

ProfilerCount API 输出方案

此示例架构文件是 ProfilerCount API 呼叫的输出请求检索当前有效的分析器会话的计数目标的监控 ESS 节点的 Cisco：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="sessionCount" type="profilerCount"/>

  <xs:complexType name="profilerCount">
    <xs:sequence>
      <xs:element name="count" type="xs:int"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

调用 ProfilerCount API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与 ProfilerCount API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/Session/ <specific - api - call>）：

```
https://acme123/admin/API/mnt/Session/ProfilerCount
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从 ProfilerCount API 调用返回的数据

以下示例说明返回的数据（有效的分析器会话数），当您将在目标监视器 ESS 节点时的 Cisco 的一 ProfilerCount API 呼叫：

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<sessionCount>
<count>1</count>
</sessionCount>
```

简单的会话列表 API 呼叫

以下简单的会话列表 API 呼叫可让您快速收集会话相关的信息（例如 MAC 地址、网络接入设备 (NAD) IP 地址，账号和会话 ID 与目标的监控您的 Cisco ISE 配置的 Cisco 一当前活动会话相关 ESS 节点：

- 活动会话列表（ActiveList）
- 已验证会话列表（AuthList）

活动会话列表

您可以使用 ActiveList API 呼叫列出所有当前活动的会话。

备注　激活最大数量验证可以显示是限制为 100,000 的终端会话。

ActiveList API 输出方案

此示例架构文件是 ActiveList API 呼叫的输出请求检索当前活动会话（和会话相关的信息的）列表有关该目标监视器 ESS 节点的 Cisco：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:element name="activeSessionList" type="simpleActiveSessionList"/>

<xs:complexType name="simpleActiveSessionList">
    <xs:sequence>
      <xs:element name="activeSession" type="simpleActiveSession" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="noOfActiveSession" type="xs:int" use="required"/>
  </xs:complexType>

  <xs:complexType name="simpleActiveSession">
    <xs:sequence>
      <xs:element name="user_name" type="xs:string" minOccurs="0"/>
      <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="server" type="xs:string" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>

<xs:element name="nas_ipv6_address" type="xs:string"/>
  <xs:complexType name="framed_ipv6_address_list">
    <xs:sequence minOccurs="0" maxOccurs="8"><xs:element name="ipv6_address"
type="xs:string" />
    </xs:sequence>
  </xs:complexType>
<xs:element name="framed_ipv6_address" type="framed_ipv6_address_list" minOccurs="1"
maxOccurs="1"/>
</xs:schema>
```

调用 ActiveList API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与 ActiveList API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/Session/ <specific - api - call>）：

```
https://acme123/admin/API/mnt/Session/ActiveList
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从 ActiveList API 调用返回的数据

当您将在目标监视器 ESS 节点时，思科的一 ActiveList API 调用以下示例说明从活动会话列表返回的会话相关的数据

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<activeSessionList noOfActiveSession="5">
-
<activeSession>
<calling_station_id>00:0C:29:FA:EF:0A</calling_station_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<calling_station_id>70:5A:B6:68:F7:CC</calling_station_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>tom_wolfe</user_name>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<nas_ipv6_address>2001:cdba::3257:9652</nas_ipv6_address>
<acct_session_id>00000032</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
```

```
<user_name>graham_hancock</user_name>
<calling_station_id>00:50:56:8E:28:BD</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<nas_ipv6_address>2001:cdba::3257:9652</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3257:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3257:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:9652</ipv6_address>
</framed_ipv6_address>
<acct_session_id>0000002C</acct_session_id>
<audit_session_id>0ACB6BA10000002A165FD0C8</audit_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>ipepvpnuser</user_name>
<calling_station_id>172.23.130.89</calling_station_id>
<nas_ip_address>10.203.107.45</nas_ip_address>
<nas_ipv6_address>2001:cdba::357:965</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3157:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3247:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:962</ipv6_address>
</framed_ipv6_address>
<acct_session_id>A2000070</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
</activeSessionList>
```

已验证会话列表

您可以使用 AuthList API 呼叫检索所有当前活动的已验证的会话列表。

备注　激活最大数量验证可以显示是限制为 100,000 的终端会话。

AuthList API 输出方案

此示例架构文件是 AuthList API 呼叫的输出请求检索所有当前活动的已验证的会话列表在指定的时间段内（或使用“空/空”参数的未指定时间）在该目标监视器 ESS 节点的 Cisco：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="activeSessionList" type="simpleActiveSessionList"/>

<xs:complexType name="simpleActiveSessionList">
    <xs:sequence>
      <xs:element name="activeSession" type="simpleActiveSession" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="noOfActiveSession" type="xs:int" use="required"/>
  </xs:complexType>

  <xs:complexType name="simpleActiveSession">
    <xs:sequence>
      <xs:element name="user_name" type="xs:string" minOccurs="0"/>
      <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
```

```
      <xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="server" type="xs:string" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="nas_ipv6_address" type="xs:string"/>
  <xs:complexType name="framed_ipv6_address_list">
    <xs:sequence minOccurs="0" maxOccurs="8"><xs:element name="ipv6_address"
type="xs:string" />
    </xs:sequence>
  </xs:complexType>
  <xs:element name="framed_ipv6_address" type="framed_ipv6_address_list" minOccurs="1"
maxOccurs="1"/>

</xs:schema>
```

调用 AuthList API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与 AuthList API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/Session/ <specific - api - call>）：

备注　第一下列两个示例使用已定义的开始时间和空参数，显示当前的活动会话列表在指定的启动时间后验证。第二个示例使用显示所有当前活动的已验证的会话列表为空/参数。参阅采样从与空/空选项的 AuthList API 调用返回的数据，第 2-9 页，显示四个参数设置类型示例此 API 呼叫的。

```
https://acme123/admin/API/mnt/Session/AuthList/2010-12-14 15:33:15/null

https://acme123/admin/API/mnt/Session/AuthList/null/null
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从与空/空选项的 AuthList API 调用返回的数据

以下示例说明使用空/空选项时，返回当前活动的已验证的会话的列表，在调用 AuthList API 呼叫：

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<activeSessionList noOfActiveSession="3">
-
<activeSession>
<user_name>ipepwlcuser</user_name>
<calling_station_id>00:26:82:7B:D2:51</calling_station_id>
<nas_ip_address>10.203.107.10</nas_ip_address>
<nas_ipv6_address>2001:cdba::3257:9652</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3257:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3257:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:9652</ipv6_address>
</framed_ipv6_address>
<audit_session_id>0acb6b0c000000174D07F487</audit_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>tom_wolfe</user_name>
<calling_station_id>00:50:56:8E:28:BD</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<nas_ipv6_address>2001:cdba::357:965</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3157:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3247:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:962</ipv6_address>
</framed_ipv6_address>
<acct_session_id>00000035</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>graham_hancock</user_name>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<nas_ipv6_address>2001:cdba::357:965</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3157:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3247:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:962</ipv6_address>
</framed_ipv6_address>
<acct_session_id>00000033</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
</activeSessionList>
```

从与 endtime/空选项的 AuthList API 调用返回的示例数据

以下示例说明使用 endtime/空选项时，返回当前活动的已验证的会话的列表，在调用 AuthList API 呼叫：

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
```

```
<activeSessionList noOfActiveSession="3">
-
<activeSession>
<user_name>ipepwlcuser</user_name>
<calling_station_id>00:26:82:7B:D2:51</calling_station_id>
<nas_ip_address>10.203.107.10</nas_ip_address>
<nas_ipv6_address>2001:cdba::3257:9652</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3257:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3257:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:9652</ipv6_address>
</framed_ipv6_address>
<audit_session_id>0acb6b0c0000001F4D08085A</audit_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>hunter_thompson</user_name>
<calling_station_id>00:50:56:8E:28:BD</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<nas_ipv6_address>2001:cdba::357:965</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3157:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3247:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:962</ipv6_address>
</framed_ipv6_address>
<acct_session_id>00000035</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>bob_ludlum</user_name>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<nas_ipv6_address>2001:cdba::357:965</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3157:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3247:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:962</ipv6_address>
</framed_ipv6_address>
<acct_session_id>00000033</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
</activeSessionList>
```

从与空/starttime 选项的 AuthList API 调用返回的示例数据

以下示例说明使用空/starttime 选项时，返回当前活动的已验证的会话的列表，在调用 AuthList API 呼叫：

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<activeSessionList noOfActiveSession="3">
-
<activeSession>
<user_name>ipepwlcuser</user_name>
<calling_station_id>00:26:82:7B:D2:51</calling_station_id>
<nas_ip_address>10.203.107.10</nas_ip_address>
<nas_ipv6_address>2001:cdba::3257:9652</nas_ipv6_address>
<framed_ipv6_address>
```

```
<ipv6_address>200:cdba:0000:0000:0000:0000:3257:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3257:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:9652</ipv6_address>
</framed_ipv6_address>
<audit_session_id>0acb6b0c0000001F4D08085A</audit_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>bob_ludlum</user_name>
<calling_station_id>00:50:56:8E:28:BD</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<nas_ipv6_address>2001:cdba::357:965</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3157:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3247:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:962</ipv6_address>
</framed_ipv6_address>
<acct_session_id>00000035</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>tom_wolfe</user_name>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<nas_ipv6_address>2001:cdba::357:965</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3157:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3247:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:962</ipv6_address>
</framed_ipv6_address>
<acct_session_id>00000033</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
</activeSessionList>
```

从与 statttime/endtime 选项的 AuthList API 调用返回的示例数据

以下示例说明使用开始/endtime 选项时，返回当前活动的已验证的会话的列表，在调用 AuthList API 呼叫：

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.
-
<activeSessionList noOfActiveSession="3">
-
<activeSession>
<user_name>ipepwlcuser</user_name>
<calling_station_id>00:26:82:7B:D2:51</calling_station_id>
<nas_ip_address>10.203.107.10</nas_ip_address>
<audit_session_id>0acb6b0c0000001F4D08085A</audit_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>graham_hancock</user_name>
<calling_station_id>00:50:56:8E:28:BD</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>00000035</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
```

```
-
<activeSession>
<user_name>hunter_thompson</user_name>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>00000033</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
</activeSessionList>
```

详细会话属性 API 呼叫

以下详细会话属性 API 呼叫可让您快速搜索最新的会话密钥信息，例如下列

- MAC 地址会话搜索（MAC 地址）
- 账号会话搜索（用户名）
- NAS IP 地址会话搜索（IP 地址与监控 ESS 节点）的目标相关联
- 终端 IP 地址会话搜索 (EndPointIPAddress)
- 跟踪会话 ID 搜索（跟踪会话 ID）

MAC 地址会话搜索

您可以使用 MAC 地址 API 呼叫从当前，活动会话检索指定的 MAC 地址。此 API 呼叫列表从节点数据库表中获取的各种会话相关的信息。

MAC 地址 API 输出方案

此示例架构文件是 MAC 地址 API 呼叫的输出请求检索指定的 MAC 地址从当前活动会话数

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="sessionParameters" type="restsdStatus"/>

  <xs:complexType name="restsdStatus">
    <xs:sequence>
      <xs:element name="passed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="failed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="user_name" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="failure_reason" type="xs:string" minOccurs="0"/>
      <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_group" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_name" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_server" type="xs:string" minOccurs="0"/>
      <xs:element name="authen_protocol" type="xs:string" minOccurs="0"/>
      <xs:element name="framed_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_groups" type="xs:string" minOccurs="0"/>
      <xs:element name="access_service" type="xs:string" minOccurs="0"/>
      <xs:element name="auth_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="authentication_method" type="xs:string" minOccurs="0"/>
      <xs:element name="execution_steps" type="xs:string" minOccurs="0"/>
      <xs:element name="radius_response" type="xs:string" minOccurs="0"/>
      <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
```

```
<xs:element name="nas_identifier" type="xs:string" minOccurs="0"/>
<xs:element name="nas_port_id" type="xs:string" minOccurs="0"/>
<xs:element name="nac_policy_compliance" type="xs:string" minOccurs="0"/>
<xs:element name="auth_id" type="xs:long" minOccurs="0"/>
<xs:element name="auth_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="message_code" type="xs:string" minOccurs="0"/>
<xs:element name="acs_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="service_selection_policy" type="xs:string" minOccurs="0"/>
<xs:element name="authorization_policy" type="xs:string" minOccurs="0"/>
<xs:element name="identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="response" type="xs:string" minOccurs="0"/>
<xs:element name="service_type" type="xs:string" minOccurs="0"/>
<xs:element name="cts_security_group" type="xs:string" minOccurs="0"/>
<xs:element name="use_case" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_av_pair" type="xs:string" minOccurs="0"/>
<xs:element name="ad_domain" type="xs:string" minOccurs="0"/>
<xs:element name="acs_username" type="xs:string" minOccurs="0"/>
<xs:element name="radius_username" type="xs:string" minOccurs="0"/>
<xs:element name="nac_role" type="xs:string" minOccurs="0"/>
<xs:element name="nac_username" type="xs:string" minOccurs="0"/>
<xs:element name="nac_posture_token" type="xs:string" minOccurs="0"/>
<xs:element name="nac_radius_is_user_auth" type="xs:string" minOccurs="0"/>
<xs:element name="selected_posture_server" type="xs:string" minOccurs="0"/>
<xs:element name="selected_identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="authentication_identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="azn_exp_pol_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="ext_pol_server_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="grp_mapping_pol_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="identity_policy_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="nas_port_type" type="xs:string" minOccurs="0"/>
<xs:element name="query_identity_stores" type="xs:string" minOccurs="0"/>
<xs:element name="selected_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="sel_exp_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="selected_query_identity_stores" type="xs:string" minOccurs="0"/>
<xs:element name="eap_tunnel" type="xs:string" minOccurs="0"/>
<xs:element name="tunnel_details" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_ssg_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="other_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="response_time" type="xs:long" minOccurs="0"/>
<xs:element name="nad_failure" type="xs:anyType" minOccurs="0"/>
<xs:element name="destination_ip_address" type="xs:string" minOccurs="0"/>
<xs:element name="acct_id" type="xs:long" minOccurs="0"/>
<xs:element name="acct_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_status_type" type="xs:string" minOccurs="0"/>
<xs:element name="acct_session_time" type="xs:long" minOccurs="0"/>
<xs:element name="acct_input_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_output_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_input_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_output_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_class" type="xs:string" minOccurs="0"/>
<xs:element name="acct_terminate_cause" type="xs:string" minOccurs="0"/>
<xs:element name="acct_multi_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_authentic" type="xs:string" minOccurs="0"/>
<xs:element name="termination_action" type="xs:string" minOccurs="0"/>
<xs:element name="session_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="idle_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="acct_interim_interval" type="xs:string" minOccurs="0"/>
<xs:element name="acct_delay_time" type="xs:string" minOccurs="0"/>
<xs:element name="event_timestamp" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_connection" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_packet_lost" type="xs:string" minOccurs="0"/>
```

```
      <xs:element name="security_group" type="xs:string" minOccurs="0"/>
      <xs:element name="cisco_h323_setup_time" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="cisco_h323_connect_time" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="cisco_h323_disconnect_time" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="framed_protocol" type="xs:string" minOccurs="0"/>
      <xs:element name="started" type="xs:anyType" minOccurs="0"/>
      <xs:element name="stopped" type="xs:anyType" minOccurs="0"/>
      <xs:element name="ckpt_id" type="xs:long" minOccurs="0"/>
      <xs:element name="type" type="xs:long" minOccurs="0"/>
      <xs:element name="nad_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="vlan" type="xs:string" minOccurs="0"/>
      <xs:element name="dacl" type="xs:string" minOccurs="0"/>
      <xs:element name="authentication_type" type="xs:string" minOccurs="0"/>
      <xs:element name="interface_name" type="xs:string" minOccurs="0"/>
      <xs:element name="reason" type="xs:string" minOccurs="0"/>
      <xs:element name="endpoint_policy" type="xs:string" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="nas_ipv6_address" type="xs:string"/>
  <xs:complexType name="framed_ipv6_address_list">
    <xs:sequence minOccurs="0" maxOccurs="8"><xs:element name="ipv6_address"
type="xs:string" />
    </xs:sequence>
  </xs:complexType>
  <xs:element name="framed_ipv6_address" type="framed_ipv6_address_list" minOccurs="1"
maxOccurs="1"/>
</xs:schema>
```

调用 MAC 地址 API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点字段输入 MAC 地址 API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/ <specific - api - call>/<macaddress>）：

```
https://acme123/admin/API/mnt/Session/MACAddress/0A:0B:0C:0D:0E:0F
```

备注　确保使用 XX，您指定 MAC 地址：XX : XX : XX : XX : XX 格式。

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从 MAC 地址 API 调用返回的数据

以下示例说明在触发 MACAddress API 调用时从活动会话列表返回的与会话相关的数据：

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<sessionParameters>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>hunter_thompson</user_name>
<nas_ip_address>10.203.107.161</nas_ip_address>
<nas_ipv6_address>2001:cdba::357:965</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3157:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3247:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:962</ipv6_address>
</framed_ipv6_address>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_port>50115</nas_port>
<identity_group>Profiled</identity_group>
<network_device_name>Core-Switch</network_device_name>
<acs_server>HAREESH-R6-1-PDP2</acs_server>
<authen_protocol>Lookup</authen_protocol>
-
<network_device_groups>
Device Type#All Device Types,Location#All Locations
</network_device_groups>
<access_service>RADIUS</access_service>
<auth_acs_timestamp>2010-12-15T02:11:12.359Z</auth_acs_timestamp>
<authentication_method>mab</authentication_method>
-
<execution_steps>
11001,11017,11027,15008,15048,15004,15041,15004,15013,24209,24211,22037,15036,15048,15048,
15004,15016,11022,11002
</execution_steps>
<audit_session_id>0ACB6BA1000000351BBFBF8B</audit_session_id>
<nas_port_id>GigabitEthernet1/0/15</nas_port_id>
<nac_policy_compliance>Pending</nac_policy_compliance>
<auth_id>1291240762077361</auth_id>
<auth_acsview_timestamp>2010-12-15T02:11:12.360Z</auth_acsview_timestamp>
<message_code>5200</message_code>
<acs_session_id>HAREESH-R6-1-PDP2/81148292/681</acs_session_id>
<service_selection_policy>MAB</service_selection_policy>
<identity_store>Internal Hosts</identity_store>
-
<response>
{UserName=00-14-BF-5A-0C-03; User-Name=00-14-BF-5A-0C-03;
State=ReauthSession:0ACB6BA1000000351BBFBF8B;
Class=CACS:0ACB6BA1000000351BBFBF8B:HAREESH-R6-1-PDP2/81148292/681;
Termination-Action=RADIUS-Request; cisco-av-pair=url-redirect-acl=ACL-WEBAUTH-REDIRECT;
cisco-av-pair=url-redirect=https://HAREESH-R6-1-PDP2.cisco.com:8443/guestportal/gateway?se
ssionId=0ACB6BA1000000351BBFBF8B&action=cwa;
cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL-DENY-4ced8390; }
</response>
<service_type>Call Check</service_type>
<use_case>Host Lookup</use_case>
<cisco_av_pair>audit-session-id=0ACB6BA1000000351BBFBF8B</cisco_av_pair>
```

```
<acs_username>00:14:BF:5A:0C:03</acs_username>
<radius_username>00:14:BF:5A:0C:03</radius_username>
<selected_identity_store>Internal Hosts</selected_identity_store>
<authentication_identity_store>Internal Hosts</authentication_identity_store>
<identity_policy_matched_rule>Default</identity_policy_matched_rule>
<nas_port_type>Ethernet</nas_port_type>
<selected_azn_profiles>CWA</selected_azn_profiles>
-
<other_attributes>
ConfigVersionId=44,DestinationIPAddress=10.203.107.162,DestinationPort=1812,Protocol=Radiu
s,Framed-MTU=1500,EAP-Key-Name=,CPMSessionID=0ACB6BA1000000351BBFBF8B,CPMSessionID=0ACB6BA
1000000351BBFBF8B,EndPointMACAddress=00-14-BF-5A-0C-03,HostIdentityGroup=Endpoint Identity
Groups:Profiled,Device Type=Device Type#All Device Types,Location=Location#All
Locations,Model Name=Unknown,Software Version=Unknown,Device IP
Address=10.203.107.161,Called-Station-ID=04:FE:7F:7F:C0:8F
</other_attributes>
<response_time>77</response_time>
<acct_id>1291240762077386</acct_id>
<acct_acs_timestamp>2010-12-15T02:12:30.779Z</acct_acs_timestamp>
<acct_acsview_timestamp>2010-12-15T02:12:30.780Z</acct_acsview_timestamp>
<acct_session_id>00000038</acct_session_id>
<acct_status_type>Interim-Update</acct_status_type>
<acct_session_time>78</acct_session_time>
<acct_input_octets>13742</acct_input_octets>
<acct_output_octets>6277</acct_output_octets>
<acct_input_packets>108</acct_input_packets>
<acct_output_packets>66</acct_output_packets>
-
<acct_class>
CACS:0ACB6BA1000000351BBFBF8B:HAREESH-R6-1-PDP2/81148292/681
</acct_class>
<acct_delay_time>0</acct_delay_time>
<started xsi:type="xs:boolean">false</started>
<stopped xsi:type="xs:boolean">false</stopped>
</sessionParameters>
```

账号会话搜索

您可以使用用户名 API 呼叫从当前，活动会话检索指定的账号。此 API 将列出从节点数据库表中获取的各种会话相关的信息。

用户名 API 输出方案

此示例架构文件是用户名 API 呼叫的输出请求检索指定的账号从当前活动会话数

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="sessionParameters" type="restsdStatus"/>

  <xs:complexType name="restsdStatus">
    <xs:sequence>
      <xs:element name="passed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="failed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="user_name" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="failure_reason" type="xs:string" minOccurs="0"/>
      <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_group" type="xs:string" minOccurs="0"/>
```

```
<xs:element name="network_device_name" type="xs:string" minOccurs="0"/>
<xs:element name="acs_server" type="xs:string" minOccurs="0"/>
<xs:element name="authen_protocol" type="xs:string" minOccurs="0"/>
<xs:element name="framed_ip_address" type="xs:string" minOccurs="0"/>
<xs:element name="network_device_groups" type="xs:string" minOccurs="0"/>
<xs:element name="access_service" type="xs:string" minOccurs="0"/>
<xs:element name="auth_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="authentication_method" type="xs:string" minOccurs="0"/>
<xs:element name="execution_steps" type="xs:string" minOccurs="0"/>
<xs:element name="radius_response" type="xs:string" minOccurs="0"/>
<xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="nas_identifier" type="xs:string" minOccurs="0"/>
<xs:element name="nas_port_id" type="xs:string" minOccurs="0"/>
<xs:element name="nac_policy_compliance" type="xs:string" minOccurs="0"/>
<xs:element name="auth_id" type="xs:long" minOccurs="0"/>
<xs:element name="auth_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="message_code" type="xs:string" minOccurs="0"/>
<xs:element name="acs_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="service_selection_policy" type="xs:string" minOccurs="0"/>
<xs:element name="authorization_policy" type="xs:string" minOccurs="0"/>
<xs:element name="identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="response" type="xs:string" minOccurs="0"/>
<xs:element name="service_type" type="xs:string" minOccurs="0"/>
<xs:element name="cts_security_group" type="xs:string" minOccurs="0"/>
<xs:element name="use_case" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_av_pair" type="xs:string" minOccurs="0"/>
<xs:element name="ad_domain" type="xs:string" minOccurs="0"/>
<xs:element name="acs_username" type="xs:string" minOccurs="0"/>
<xs:element name="radius_username" type="xs:string" minOccurs="0"/>
<xs:element name="nac_role" type="xs:string" minOccurs="0"/>
<xs:element name="nac_username" type="xs:string" minOccurs="0"/>
<xs:element name="nac_posture_token" type="xs:string" minOccurs="0"/>
<xs:element name="nac_radius_is_user_auth" type="xs:string" minOccurs="0"/>
<xs:element name="selected_posture_server" type="xs:string" minOccurs="0"/>
<xs:element name="selected_identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="authentication_identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="azn_exp_pol_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="ext_pol_server_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="grp_mapping_pol_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="identity_policy_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="nas_port_type" type="xs:string" minOccurs="0"/>
<xs:element name="query_identity_stores" type="xs:string" minOccurs="0"/>
<xs:element name="selected_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="sel_exp_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="selected_query_identity_stores" type="xs:string" minOccurs="0"/>
<xs:element name="eap_tunnel" type="xs:string" minOccurs="0"/>
<xs:element name="tunnel_details" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_ssg_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="other_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="response_time" type="xs:long" minOccurs="0"/>
<xs:element name="nad_failure" type="xs:anyType" minOccurs="0"/>
<xs:element name="destination_ip_address" type="xs:string" minOccurs="0"/>
<xs:element name="acct_id" type="xs:long" minOccurs="0"/>
<xs:element name="acct_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_status_type" type="xs:string" minOccurs="0"/>
<xs:element name="acct_session_time" type="xs:long" minOccurs="0"/>
<xs:element name="acct_input_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_output_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_input_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_output_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_class" type="xs:string" minOccurs="0"/>
```

```
      <xs:element name="acct_terminate_cause" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_multi_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_authentic" type="xs:string" minOccurs="0"/>
      <xs:element name="termination_action" type="xs:string" minOccurs="0"/>
      <xs:element name="session_timeout" type="xs:string" minOccurs="0"/>
      <xs:element name="idle_timeout" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_interim_interval" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_delay_time" type="xs:string" minOccurs="0"/>
      <xs:element name="event_timestamp" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_tunnel_connection" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_tunnel_packet_lost" type="xs:string" minOccurs="0"/>
      <xs:element name="security_group" type="xs:string" minOccurs="0"/>
      <xs:element name="cisco_h323_setup_time" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="cisco_h323_connect_time" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="cisco_h323_disconnect_time" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="framed_protocol" type="xs:string" minOccurs="0"/>
      <xs:element name="started" type="xs:anyType" minOccurs="0"/>
      <xs:element name="stopped" type="xs:anyType" minOccurs="0"/>
      <xs:element name="ckpt_id" type="xs:long" minOccurs="0"/>
      <xs:element name="type" type="xs:long" minOccurs="0"/>
      <xs:element name="nad_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="vlan" type="xs:string" minOccurs="0"/>
      <xs:element name="dacl" type="xs:string" minOccurs="0"/>
      <xs:element name="authentication_type" type="xs:string" minOccurs="0"/>
      <xs:element name="interface_name" type="xs:string" minOccurs="0"/>
      <xs:element name="reason" type="xs:string" minOccurs="0"/>
      <xs:element name="endpoint_policy" type="xs:string" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="nas_ipv6_address" type="xs:string"/>
  <xs:complexType name="framed_ipv6_address_list">
    <xs:sequence minOccurs="0" maxOccurs="8"><xs:element name="ipv6_address"
type="xs:string" />
    </xs:sequence>
  </xs:complexType>
  <xs:element name="framed_ipv6_address" type="framed_ipv6_address_list" minOccurs="1"
maxOccurs="1"/>
</xs:schema>
```

调用用户名 API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点字段输入用户名 API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/ <specific - api - call>/<username>）：

```
https://acme123/admin/API/mnt/Session/UserName/graham_hancock
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从用户名 API 调用返回的数据

当您将用户名 API 呼叫时，以下示例说明从活动会话列表返回的会话相关的数据

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<sessionParameters>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>graham_hancock</user_name>
<nas_ip_address>10.203.107.161</nas_ip_address>
<nas_ipv6_address>2001:cdba::357:965</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3157:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3247:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:962</ipv6_address>
</framed_ipv6_address>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_port>50115</nas_port>
<identity_group>Profiled</identity_group>
<network_device_name>Core-Switch</network_device_name>
<acs_server>HAREESH-R6-1-PDP2</acs_server>
<authen_protocol>Lookup</authen_protocol>
-
<network_device_groups>
Device Type#All Device Types,Location#All Locations
</network_device_groups>
<access_service>RADIUS</access_service>
<auth_acs_timestamp>2010-12-15T02:11:12.359Z</auth_acs_timestamp>
<authentication_method>mab</authentication_method>
-
<execution_steps>
11001,11017,11027,15008,15048,15004,15041,15004,15013,24209,24211,22037,15036,15048,15048,
15004,15016,11022,11002
</execution_steps>
<audit_session_id>0ACB6BA1000000351BBFBF8B</audit_session_id>
<nas_port_id>GigabitEthernet1/0/15</nas_port_id>
<nac_policy_compliance>Pending</nac_policy_compliance>
<auth_id>1291240762077361</auth_id>
<auth_acsview_timestamp>2010-12-15T02:11:12.360Z</auth_acsview_timestamp>
<message_code>5200</message_code>
<acs_session_id>HAREESH-R6-1-PDP2/81148292/681</acs_session_id>
<service_selection_policy>MAB</service_selection_policy>
<identity_store>Internal Hosts</identity_store>
-
<response>
```

```
{UserName=graham_hancock; User-Name=graham_hancock;
State=ReauthSession:0ACB6BA1000000351BBFBF8B;
Class=CACS:0ACB6BA1000000351BBFBF8B:HAREESH-R6-1-PDP2/81148292/681;
Termination-Action=RADIUS-Request; cisco-av-pair=url-redirect-acl=ACL-WEBAUTH-REDIRECT;
cisco-av-pair=url-redirect=https://HAREESH-R6-1-PDP2.cisco.com:8443/guestportal/gateway?se
ssionId=0ACB6BA1000000351BBFBF8B&action=cwa;
cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL-DENY-4ced8390; }
</response>
<service_type>Call Check</service_type>
<use_case>Host Lookup</use_case>
<cisco_av_pair>audit-session-id=0ACB6BA1000000351BBFBF8B</cisco_av_pair>
<acs_username>graham_hancock</acs_username>
<radius_username>00:14:BF:5A:0C:03</radius_username>
<selected_identity_store>Internal Hosts</selected_identity_store>
<authentication_identity_store>Internal Hosts</authentication_identity_store>
<identity_policy_matched_rule>Default</identity_policy_matched_rule>
<nas_port_type>Ethernet</nas_port_type>
<selected_azn_profiles>CWA</selected_azn_profiles>
-
<other_attributes>
ConfigVersionId=44,DestinationIPAddress=10.203.107.162,DestinationPort=1812,Protocol=Radiu
s,Framed-MTU=1500,EAP-Key-Name=,CPMSessionID=0ACB6BA1000000351BBFBF8B,CPMSessionID=0ACB6BA
1000000351BBFBF8B,EndPointMACAddress=00-14-BF-5A-0C-03,HostIdentityGroup=Endpoint Identity
Groups:Profiled,Device Type=Device Type#All Device Types,Location=Location#All
Locations,Model Name=Unknown,Software Version=Unknown,Device IP
Address=10.203.107.161,Called-Station-ID=04:FE:7F:7F:C0:8F
</other_attributes>
<response_time>77</response_time>
<acct_id>1291240762077386</acct_id>
<acct_acs_timestamp>2010-12-15T02:12:30.779Z</acct_acs_timestamp>
<acct_acsview_timestamp>2010-12-15T02:12:30.780Z</acct_acsview_timestamp>
<acct_session_id>00000038</acct_session_id>
<acct_status_type>Interim-Update</acct_status_type>
<acct_session_time>78</acct_session_time>
<acct_input_octets>13742</acct_input_octets>
<acct_output_octets>6277</acct_output_octets>
<acct_input_packets>108</acct_input_packets>
<acct_output_packets>66</acct_output_packets>
-
<acct_class>
CACS:0ACB6BA1000000351BBFBF8B:HAREESH-R6-1-PDP2/81148292/681
</acct_class>
<acct_delay_time>0</acct_delay_time>
<started xsi:type="xs:boolean">false</started>
<stopped xsi:type="xs:boolean">false</stopped>
</sessionParameters>
```

NAS IP 地址会话搜索

您可以使用 IPAddress API 调用从当前会话中检索指定 NAS IP 地址（IPv4 或 IPv6 地址）的数据。此 API 将列出从节点数据库表中获取的各种会话相关的信息。

IP 地址 API 输出方案

此样本架构文件是用于从当前活动会话中检索指定 NAS IP 地址（IPv4 或 IPv6 地址）的 IPAddress API 调用的输出：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">
```

```
<xs:element name="sessionParameters" type="restsdStatus"/>

<xs:complexType name="restsdStatus">
  <xs:sequence>
    <xs:element name="passed" type="xs:anyType" minOccurs="0"/>
    <xs:element name="failed" type="xs:anyType" minOccurs="0"/>
    <xs:element name="user_name" type="xs:string" minOccurs="0"/>
    <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
    <xs:element name="failure_reason" type="xs:string" minOccurs="0"/>
    <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
    <xs:element name="nas_port" type="xs:string" minOccurs="0"/>
    <xs:element name="identity_group" type="xs:string" minOccurs="0"/>
    <xs:element name="network_device_name" type="xs:string" minOccurs="0"/>
    <xs:element name="acs_server" type="xs:string" minOccurs="0"/>
    <xs:element name="authen_protocol" type="xs:string" minOccurs="0"/>
    <xs:element name="framed_ip_address" type="xs:string" minOccurs="0"/>
    <xs:element name="network_device_groups" type="xs:string" minOccurs="0"/>
    <xs:element name="access_service" type="xs:string" minOccurs="0"/>
    <xs:element name="auth_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
    <xs:element name="authentication_method" type="xs:string" minOccurs="0"/>
    <xs:element name="execution_steps" type="xs:string" minOccurs="0"/>
    <xs:element name="radius_response" type="xs:string" minOccurs="0"/>
    <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
    <xs:element name="nas_identifier" type="xs:string" minOccurs="0"/>
    <xs:element name="nas_port_id" type="xs:string" minOccurs="0"/>
    <xs:element name="nac_policy_compliance" type="xs:string" minOccurs="0"/>
    <xs:element name="auth_id" type="xs:long" minOccurs="0"/>
    <xs:element name="auth_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
    <xs:element name="message_code" type="xs:string" minOccurs="0"/>
    <xs:element name="acs_session_id" type="xs:string" minOccurs="0"/>
    <xs:element name="service_selection_policy" type="xs:string" minOccurs="0"/>
    <xs:element name="authorization_policy" type="xs:string" minOccurs="0"/>
    <xs:element name="identity_store" type="xs:string" minOccurs="0"/>
    <xs:element name="response" type="xs:string" minOccurs="0"/>
    <xs:element name="service_type" type="xs:string" minOccurs="0"/>
    <xs:element name="cts_security_group" type="xs:string" minOccurs="0"/>
    <xs:element name="use_case" type="xs:string" minOccurs="0"/>
    <xs:element name="cisco_av_pair" type="xs:string" minOccurs="0"/>
    <xs:element name="ad_domain" type="xs:string" minOccurs="0"/>
    <xs:element name="acs_username" type="xs:string" minOccurs="0"/>
    <xs:element name="radius_username" type="xs:string" minOccurs="0"/>
    <xs:element name="nac_role" type="xs:string" minOccurs="0"/>
    <xs:element name="nac_username" type="xs:string" minOccurs="0"/>
    <xs:element name="nac_posture_token" type="xs:string" minOccurs="0"/>
    <xs:element name="nac_radius_is_user_auth" type="xs:string" minOccurs="0"/>
    <xs:element name="selected_posture_server" type="xs:string" minOccurs="0"/>
    <xs:element name="selected_identity_store" type="xs:string" minOccurs="0"/>
    <xs:element name="authentication_identity_store" type="xs:string" minOccurs="0"/>
    <xs:element name="azn_exp_pol_matched_rule" type="xs:string" minOccurs="0"/>
    <xs:element name="ext_pol_server_matched_rule" type="xs:string" minOccurs="0"/>
    <xs:element name="grp_mapping_pol_matched_rule" type="xs:string" minOccurs="0"/>
    <xs:element name="identity_policy_matched_rule" type="xs:string" minOccurs="0"/>
    <xs:element name="nas_port_type" type="xs:string" minOccurs="0"/>
    <xs:element name="query_identity_stores" type="xs:string" minOccurs="0"/>
    <xs:element name="selected_azn_profiles" type="xs:string" minOccurs="0"/>
    <xs:element name="sel_exp_azn_profiles" type="xs:string" minOccurs="0"/>
    <xs:element name="selected_query_identity_stores" type="xs:string" minOccurs="0"/>
    <xs:element name="eap_tunnel" type="xs:string" minOccurs="0"/>
    <xs:element name="tunnel_details" type="xs:string" minOccurs="0"/>
    <xs:element name="cisco_h323_attributes" type="xs:string" minOccurs="0"/>
    <xs:element name="cisco_ssg_attributes" type="xs:string" minOccurs="0"/>
    <xs:element name="other_attributes" type="xs:string" minOccurs="0"/>
    <xs:element name="response_time" type="xs:long" minOccurs="0"/>
    <xs:element name="nad_failure" type="xs:anyType" minOccurs="0"/>
```

```
      <xs:element name="destination_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_id" type="xs:long" minOccurs="0"/>
      <xs:element name="acct_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="acct_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_status_type" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_session_time" type="xs:long" minOccurs="0"/>
      <xs:element name="acct_input_octets" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_output_octets" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_input_packets" type="xs:long" minOccurs="0"/>
      <xs:element name="acct_output_packets" type="xs:long" minOccurs="0"/>
      <xs:element name="acct_class" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_terminate_cause" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_multi_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_authentic" type="xs:string" minOccurs="0"/>
      <xs:element name="termination_action" type="xs:string" minOccurs="0"/>
      <xs:element name="session_timeout" type="xs:string" minOccurs="0"/>
      <xs:element name="idle_timeout" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_interim_interval" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_delay_time" type="xs:string" minOccurs="0"/>
      <xs:element name="event_timestamp" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_tunnel_connection" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_tunnel_packet_lost" type="xs:string" minOccurs="0"/>
      <xs:element name="security_group" type="xs:string" minOccurs="0"/>
      <xs:element name="cisco_h323_setup_time" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="cisco_h323_connect_time" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="cisco_h323_disconnect_time" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="framed_protocol" type="xs:string" minOccurs="0"/>
      <xs:element name="started" type="xs:anyType" minOccurs="0"/>
      <xs:element name="stopped" type="xs:anyType" minOccurs="0"/>
      <xs:element name="ckpt_id" type="xs:long" minOccurs="0"/>
      <xs:element name="type" type="xs:long" minOccurs="0"/>
      <xs:element name="nad_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="vlan" type="xs:string" minOccurs="0"/>
      <xs:element name="dacl" type="xs:string" minOccurs="0"/>
      <xs:element name="authentication_type" type="xs:string" minOccurs="0"/>
      <xs:element name="interface_name" type="xs:string" minOccurs="0"/>
      <xs:element name="reason" type="xs:string" minOccurs="0"/>
      <xs:element name="endpoint_policy" type="xs:string" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="nas_ipv6_address" type="xs:string"/>
  <xs:complexType name="framed_ipv6_address_list">
    <xs:sequence minOccurs="0" maxOccurs="8"><xs:element name="ipv6_address"
type="xs:string" />
    </xs:sequence>
  </xs:complexType>
  <xs:element name="framed_ipv6_address" type="framed_ipv6_address_list" minOccurs="1"
maxOccurs="1"/>
</xs:schema>
```

调用 NAS IP 地址 API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点字段输入 IP 地址 API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/ <specific - api - call>/<nasipaddress>）：

```
https://acme123/admin/API/mnt/Session/IPAddress/10.10.10.10
```

备注　确保分别使用 xxx.xxx.xxx.xxx 格式或压缩格式指定 IPv4 地址/IPv6 地址（NAS IP 地址）。

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从 IP 地址 API 调用返回的数据

当您将 IP 地址 API 呼叫时，以下示例说明从活动会话列表返回的会话相关的数据

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.
-
<sessionParameters>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>ipepvpnuser</user_name>
<nas_ip_address>10.10.10.10</nas_ip_address>
<nas_ipv6_address>2001:cdba::357:965</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>200:cdba:0000:0000:0000:0000:3157:9652</ipv6_address>
<ipv6_address> 2001:cdba:0:0:0:0:3247:9651</ipv6_address>
<ipv6_address>2001:cdba::3257:962</ipv6_address>
</framed_ipv6_address>
<calling_station_id>172.23.130.90</calling_station_id>
<nas_port>1015</nas_port>
<identity_group>iPEP-VPN-Group</identity_group>
<network_device_name>iPEP-HA-Routed</network_device_name>
<acs_server>HAREESH-R6-1-PDP2</acs_server>
<authen_protocol>PAP_ASCII</authen_protocol>
-
<network_device_groups>
Device Type#All Device Types,Location#All Locations
</network_device_groups>
<access_service>RADIUS</access_service>
<auth_acs_timestamp>2010-12-15T19:57:29.885Z</auth_acs_timestamp>
<authentication_method>PAP_ASCII</authentication_method>
-
<execution_steps>
11001,11017,15008,15048,15048,15004,15041,15004,15013,24210,24212,22037,15036,15048,15048,
15004,15016,11002
```

```
</execution_steps>
<audit_session_id>0acb6be4000000044D091DA9</audit_session_id>
<nac_policy_compliance>NotApplicable</nac_policy_compliance>
<auth_id>1291240762083580</auth_id>
<auth_acsview_timestamp>2010-12-15T19:57:29.887Z</auth_acsview_timestamp>
<message_code>5200</message_code>
<acs_session_id>HAREESH-R6-1-PDP2/81148292/693</acs_session_id>
<service_selection_policy>iPEP-VPN</service_selection_policy>
<identity_store>Internal Users</identity_store>
-
<response>
{User-Name=ipepvpnuser; State=ReauthSession:0acb6be4000000044D091DA9;
Class=CACS:0acb6be4000000044D091DA9:HAREESH-R6-1-PDP2/81148292/693;
Termination-Action=RADIUS-Request; }
</response>
<service_type>Framed</service_type>
-
<cisco_av_pair>
audit-session-id=0acb6be4000000044D091DA9,ipep-proxy=true
</cisco_av_pair>
<acs_username>ipepvpnuser</acs_username>
<radius_username>ipepvpnuser</radius_username>
<selected_identity_store>Internal Users</selected_identity_store>
<authentication_identity_store>Internal Users</authentication_identity_store>
<identity_policy_matched_rule>Default</identity_policy_matched_rule>
<nas_port_type>Virtual</nas_port_type>
<selected_azn_profiles>iPEP-Unknown-Auth-Profile</selected_azn_profiles>
<tunnel_details>Tunnel-Client-Endpoint=(tag=0) 172.23.130.90</tunnel_details>
-
<other_attributes>
ConfigVersionId=44,DestinationIPAddress=10.203.107.162,DestinationPort=1812,Protocol=Radiu
s,Framed-Protocol=PPP,Proxy-State=Cisco Secure
ACS9e733142-070a-11e0-c000-000000000000-2906094480-3222,CPMSessionID=0acb6be4000000044D091
DA9,CPMSessionID=0acb6be4000000044D091DA9,Device Type=Device Type#All Device
Types,Location=Location#All Locations,Model Name=Unknown,Software Version=Unknown,Device
IP Address=10.203.107.228,Called-Station-ID=172.23.130.94
</other_attributes>
<response_time>20</response_time>
<acct_id>1291240762083582</acct_id>
<acct_acs_timestamp>2010-12-15T19:57:30.281Z</acct_acs_timestamp>
<acct_acsview_timestamp>2010-12-15T19:57:30.283Z</acct_acsview_timestamp>
<acct_session_id>F1800007</acct_session_id>
<acct_status_type>Start</acct_status_type>
-
<acct_class>
CACS:0acb6be4000000044D091DA9:HAREESH-R6-1-PDP2/81148292/693
</acct_class>
<acct_delay_time>0</acct_delay_time>
<framed_protocol>PPP</framed_protocol>
<started xsi:type="xs:boolean">true</started>
<stopped xsi:type="xs:boolean">false</stopped>
</sessionParameters>
```

终端 IP 地址会话搜索

您可以使用 EndPointIPAddress API 调用检索某个当前活动会话的会话目录信息。此会话可提供以下内容：一个方案文件输出样本；一个程序，用于在节点数据库中搜索包含 EndPointIPAddress API 调用指定的 IP 地址的最新活动会话；以及在发起此 API 调用后返回的终端相关数据的样本。此 API 调用会列出从节点数据库表中获取的各种会话目录信息。

EndPointIPAddress API 输出方案

此方案文件样本是 EndPointIPAddress API 调用的输出，此 API 调用可从来自目标思科监控 ISE 节点上当前活动会话的会话目录信息中检索特定终端：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="sessionParameters" type="restsdStatus"/>
<xs:complexType name="restsdStatus">
<xs:sequence>
<xs:element name="passed" type="xs:anyType" minOccurs="0"/>
<xs:element name="failed" type="xs:anyType" minOccurs="0"/>
<xs:element name="user_name" type="xs:string" minOccurs="0"/>
<xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
<xs:element name="failure_reason" type="xs:string" minOccurs="0"/>
<xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
<xs:element name="nas_port" type="xs:string" minOccurs="0"/>
<xs:element name="identity_group" type="xs:string" minOccurs="0"/>
<xs:element name="network_device_name" type="xs:string" minOccurs="0"/>
<xs:element name="acs_server" type="xs:string" minOccurs="0"/>
<xs:element name="authen_protocol" type="xs:string" minOccurs="0"/>
<xs:element name="framed_ip_address" type="xs:string" minOccurs="0"/>
<xs:element name="network_device_groups" type="xs:string" minOccurs="0"/>
<xs:element name="access_service" type="xs:string" minOccurs="0"/>
<xs:element name="auth_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="authentication_method" type="xs:string" minOccurs="0"/>
<xs:element name="execution_steps" type="xs:string" minOccurs="0"/>
<xs:element name="radius_response" type="xs:string" minOccurs="0"/>
<xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="nas_identifier" type="xs:string" minOccurs="0"/>
<xs:element name="nas_port_id" type="xs:string" minOccurs="0"/>
<xs:element name="nac_policy_compliance" type="xs:string" minOccurs="0"/>
<xs:element name="auth_id" type="xs:long" minOccurs="0"/>
<xs:element name="auth_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="message_code" type="xs:string" minOccurs="0"/>
<xs:element name="acs_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="service_selection_policy" type="xs:string" minOccurs="0"/>
<xs:element name="authorization_policy" type="xs:string" minOccurs="0"/>
<xs:element name="identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="response" type="xs:string" minOccurs="0"/>
<xs:element name="service_type" type="xs:string" minOccurs="0"/>
<xs:element name="cts_security_group" type="xs:string" minOccurs="0"/>
<xs:element name="use_case" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_av_pair" type="xs:string" minOccurs="0"/>
<xs:element name="ad_domain" type="xs:string" minOccurs="0"/>
<xs:element name="acs_username" type="xs:string" minOccurs="0"/>
<xs:element name="radius_username" type="xs:string" minOccurs="0"/>
<xs:element name="nac_role" type="xs:string" minOccurs="0"/>
<xs:element name="nac_username" type="xs:string" minOccurs="0"/>
<xs:element name="nac_posture_token" type="xs:string" minOccurs="0"/>
<xs:element name="nac_radius_is_user_auth" type="xs:string" minOccurs="0"/>
<xs:element name="selected_posture_server" type="xs:string" minOccurs="0"/>
<xs:element name="selected_identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="authentication_identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="azn_exp_pol_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="ext_pol_server_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="grp_mapping_pol_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="identity_policy_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="nas_port_type" type="xs:string" minOccurs="0"/>
<xs:element name="query_identity_stores" type="xs:string" minOccurs="0"/>
<xs:element name="selected_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="sel_exp_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="selected_query_identity_stores" type="xs:string" minOccurs="0"/>
```

```
<xs:element name="eap_tunnel" type="xs:string" minOccurs="0"/>
<xs:element name="tunnel_details" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_ssg_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="other_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="response_time" type="xs:long" minOccurs="0"/>
<xs:element name="nad_failure" type="xs:anyType" minOccurs="0"/>
<xs:element name="destination_ip_address" type="xs:string" minOccurs="0"/>
<xs:element name="acct_id" type="xs:long" minOccurs="0"/>
<xs:element name="acct_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_status_type" type="xs:string" minOccurs="0"/>
<xs:element name="acct_session_time" type="xs:long" minOccurs="0"/>
<xs:element name="acct_input_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_output_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_input_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_output_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_class" type="xs:string" minOccurs="0"/>
<xs:element name="acct_terminate_cause" type="xs:string" minOccurs="0"/>
<xs:element name="acct_multi_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_authentic" type="xs:string" minOccurs="0"/>
<xs:element name="termination_action" type="xs:string" minOccurs="0"/>
<xs:element name="session_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="idle_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="acct_interim_interval" type="xs:string" minOccurs="0"/>
<xs:element name="acct_delay_time" type="xs:string" minOccurs="0"/>
<xs:element name="event_timestamp" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_connection" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_packet_lost" type="xs:string" minOccurs="0"/>
<xs:element name="security_group" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_setup_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="cisco_h323_connect_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="cisco_h323_disconnect_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="framed_protocol" type="xs:string" minOccurs="0"/>
<xs:element name="started" type="xs:anyType" minOccurs="0"/>
<xs:element name="stopped" type="xs:anyType" minOccurs="0"/>
<xs:element name="ckpt_id" type="xs:long" minOccurs="0"/>
<xs:element name="type" type="xs:long" minOccurs="0"/>
<xs:element name="nad_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="vlan" type="xs:string" minOccurs="0"/>
<xs:element name="dacl" type="xs:string" minOccurs="0"/>
<xs:element name="authentication_type" type="xs:string" minOccurs="0"/>
<xs:element name="interface_name" type="xs:string" minOccurs="0"/>
<xs:element name="reason" type="xs:string" minOccurs="0"/>
<xs:element name="endpoint_policy" type="xs:string" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
</xs:schema>
```

使用 EndPointIPAddress API 调用

备注　请确保您已确认您要发起 API 调用的终端节点是有效的思科监控 ISE 节点。

要发起 EndPointIPAddress API 调用，请完成以下步骤：

步骤 1　登录目标思科监控 ISE 节点。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 2　在目标节点的 URL 地址字段中输入 EndPointIPAddress API 调用，并将“/admin/”部分替换为 API 调用命令 (/ise/mnt/api/Session/EndPointIPAddress/<endpoint_ip>)：

```
https://acme123/ise/mnt/api/Session/EndPointIPAddress/A.B.C.D
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 3　按 **Enter** 发出 API 呼叫。

从 EndPointIPAddress API 调用返回的数据样本

以下示例显示了在目标思科监控 ISE 节点上使用 EndPointIPAddress API 调用后，从活动会话列表返回的会话相关数据：

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<sessionParameters>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>00:0C:29:95:A5:C1</user_name>
<nas_ip_address>10.77.152.139</nas_ip_address>
<calling_station_id>00:0C:29:95:A5:C1</calling_station_id>
<nas_port>50109</nas_port>
<identity_group>RegisteredDevices</identity_group>
<network_device_name>switch</network_device_name>
<acs_server>ise248</acs_server>
<authen_protocol>Lookup</authen_protocol>
<framed_ip_address>10.20.40.10</framed_ip_address>
-
<network_device_groups>
Device Type#All Device Types,Location#All Locations
</network_device_groups>
<access_service>RADIUS</access_service>
<auth_acs_timestamp>2012-03-13T17:02:22.169+05:30</auth_acs_timestamp>
<authentication_method>mab</authentication_method>
-
<execution_steps>
11001,11017,11027,15008,15048,15048,15004,15041,15006,15013,24209,24211,22037,15036,15048,
15004,15016,11022,11002
</execution_steps>
<audit_session_id>0A4D988B000000E337B8D983</audit_session_id>
<nas_port_id>GigabitEthernet1/0/9</nas_port_id>
<nac_policy_compliance>Pending</nac_policy_compliance>
<auth_id>1331101769985927</auth_id>
<auth_acsview_timestamp>2012-03-13T17:02:22.171+05:30</auth_acsview_timestamp>
<message_code>5200</message_code>
```

```
<acs_session_id>ise248/120476308/97</acs_session_id>
<service_selection_policy>MAB</service_selection_policy>
<authorization_policy>wired_redirect</authorization_policy>
<identity_store>Internal Endpoints</identity_store>
-
<response>
{UserName=00:0C:29:95:A5:C1; User-Name=00-0C-29-95-A5-C1;
State=ReauthSession:0A4D988B000000E337B8D983;
Class=CACS:0A4D988B000000E337B8D983:ise248/120476308/97;
Termination-Action=RADIUS-Request; Tunnel-Type=(tag=1) VLAN; Tunnel-Medium-Type=(tag=1)
802; Tunnel-Private-Group-ID=(tag=1) 30;
cisco-av-pair=url-redirect-acl=ACL-WEBAUTH-REDIRECT;
cisco-av-pair=url-redirect=https://ise248.cisco.com:8443/guestportal/gateway?sessionId=0A4
D988B000000E337B8D983&action=cwa;
cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-cwa_wired-4f570619;
cisco-av-pair=profile-name=WindowsXP-Workstation; }
</response>
<service_type>Call Check</service_type>
<use_case>Host Lookup</use_case>
<cisco_av_pair>audit-session-id=0A4D988B000000E337B8D983</cisco_av_pair>
<acs_username>00:0C:29:95:A5:C1</acs_username>
<radius_username>00:0C:29:95:A5:C1</radius_username>
<selected_identity_store>Internal Endpoints</selected_identity_store>
<authentication_identity_store>Internal Endpoints</authentication_identity_store>
<identity_policy_matched_rule>Default</identity_policy_matched_rule>
<nas_port_type>Ethernet</nas_port_type>
<selected_azn_profiles>wired_cwa_redirect</selected_azn_profiles>
<response_time>17</response_time>
<destination_ip_address>10.77.152.248</destination_ip_address>
-
<other_attributes>
ConfigVersionId=15,DestinationPort=1812,Protocol=Radius,Framed-MTU=1500,EAP-Key-Name=,cisc
o-nas-port=GigabitEthernet1/0/9,CPMSessionID=0A4D988B000000E337B8D983,EndPointMACAddress=0
0-0C-29-95-A5-C1,EndPointMatchedProfile=WindowsXP-Workstation,HostIdentityGroup=Endpoint
Identity Groups:RegisteredDevices,Device Type=Device Type#All Device
Types,Location=Location#All Locations,Device IP
Address=10.77.152.139,Called-Station-ID=EC:C8:82:55:2E:09
</other_attributes>
<acct_id>1331101769985928</acct_id>
<acct_acs_timestamp>2012-03-13T17:02:22.365+05:30</acct_acs_timestamp>
<acct_acsview_timestamp>2012-03-13T17:02:22.366+05:30</acct_acsview_timestamp>
<acct_session_id>000000FC</acct_session_id>
<acct_status_type>Interim-Update</acct_status_type>
<acct_session_time>16411</acct_session_time>
<acct_input_octets>3053882</acct_input_octets>
<acct_output_octets>2633472</acct_output_octets>
<acct_input_packets>20166</acct_input_packets>
<acct_output_packets>20297</acct_output_packets>
<acct_class>CACS:0A4D988B000000E337B8D983:ise248/120476308/97</acct_class>
<acct_delay_time>0</acct_delay_time>
<started xsi:type="xs:boolean">false</started>
<stopped xsi:type="xs:boolean">false</stopped>
<vlan>30</vlan>
<dacl>#ACSACL#-IP-cwa_wired-4f570619</dacl>
<endpoint_policy>WindowsXP-Workstation</endpoint_policy>
</sessionParameters>
```

跟踪会话 ID 搜索

您可以使用会话 ID API 呼叫从当前，活动会话检索指定的跟踪会话。此 API 呼叫列表从节点数据库表中获取的各种会话相关的信息。

跟踪会话 ID API 输出方案

此示例架构文件是跟踪会话 ID API 呼叫的输出请求检索指定的审计会话 ID 从当前活动会话数

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="sessionParameters" type="restsdStatus"/>

  <xs:complexType name="restsdStatus">
    <xs:sequence>
      <xs:element name="passed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="failed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="user_name" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="failure_reason" type="xs:string" minOccurs="0"/>
      <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_group" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_name" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_server" type="xs:string" minOccurs="0"/>
      <xs:element name="authen_protocol" type="xs:string" minOccurs="0"/>
      <xs:element name="framed_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_groups" type="xs:string" minOccurs="0"/>
      <xs:element name="access_service" type="xs:string" minOccurs="0"/>
      <xs:element name="auth_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="authentication_method" type="xs:string" minOccurs="0"/>
      <xs:element name="execution_steps" type="xs:string" minOccurs="0"/>
      <xs:element name="radius_response" type="xs:string" minOccurs="0"/>
      <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_identifier" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_policy_compliance" type="xs:string" minOccurs="0"/>
      <xs:element name="auth_id" type="xs:long" minOccurs="0"/>
      <xs:element name="auth_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="message_code" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="service_selection_policy" type="xs:string" minOccurs="0"/>
      <xs:element name="authorization_policy" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_store" type="xs:string" minOccurs="0"/>
      <xs:element name="response" type="xs:string" minOccurs="0"/>
      <xs:element name="service_type" type="xs:string" minOccurs="0"/>
      <xs:element name="cts_security_group" type="xs:string" minOccurs="0"/>
      <xs:element name="use_case" type="xs:string" minOccurs="0"/>
      <xs:element name="cisco_av_pair" type="xs:string" minOccurs="0"/>
      <xs:element name="ad_domain" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_username" type="xs:string" minOccurs="0"/>
      <xs:element name="radius_username" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_role" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_username" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_posture_token" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_radius_is_user_auth" type="xs:string" minOccurs="0"/>
      <xs:element name="selected_posture_server" type="xs:string" minOccurs="0"/>
      <xs:element name="selected_identity_store" type="xs:string" minOccurs="0"/>
      <xs:element name="authentication_identity_store" type="xs:string" minOccurs="0"/>
      <xs:element name="azn_exp_pol_matched_rule" type="xs:string" minOccurs="0"/>
```

```
        <xs:element name="ext_pol_server_matched_rule" type="xs:string" minOccurs="0"/>
        <xs:element name="grp_mapping_pol_matched_rule" type="xs:string" minOccurs="0"/>
        <xs:element name="identity_policy_matched_rule" type="xs:string" minOccurs="0"/>
        <xs:element name="nas_port_type" type="xs:string" minOccurs="0"/>
        <xs:element name="query_identity_stores" type="xs:string" minOccurs="0"/>
        <xs:element name="selected_azn_profiles" type="xs:string" minOccurs="0"/>
        <xs:element name="sel_exp_azn_profiles" type="xs:string" minOccurs="0"/>
        <xs:element name="selected_query_identity_stores" type="xs:string" minOccurs="0"/>
        <xs:element name="eap_tunnel" type="xs:string" minOccurs="0"/>
        <xs:element name="tunnel_details" type="xs:string" minOccurs="0"/>
        <xs:element name="cisco_h323_attributes" type="xs:string" minOccurs="0"/>
        <xs:element name="cisco_ssg_attributes" type="xs:string" minOccurs="0"/>
        <xs:element name="other_attributes" type="xs:string" minOccurs="0"/>
        <xs:element name="response_time" type="xs:long" minOccurs="0"/>
        <xs:element name="nad_failure" type="xs:anyType" minOccurs="0"/>
        <xs:element name="destination_ip_address" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_id" type="xs:long" minOccurs="0"/>
        <xs:element name="acct_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
        <xs:element name="acct_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
        <xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_status_type" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_session_time" type="xs:long" minOccurs="0"/>
        <xs:element name="acct_input_octets" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_output_octets" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_input_packets" type="xs:long" minOccurs="0"/>
        <xs:element name="acct_output_packets" type="xs:long" minOccurs="0"/>
        <xs:element name="acct_class" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_terminate_cause" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_multi_session_id" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_authentic" type="xs:string" minOccurs="0"/>
        <xs:element name="termination_action" type="xs:string" minOccurs="0"/>
        <xs:element name="session_timeout" type="xs:string" minOccurs="0"/>
        <xs:element name="idle_timeout" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_interim_interval" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_delay_time" type="xs:string" minOccurs="0"/>
        <xs:element name="event_timestamp" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_tunnel_connection" type="xs:string" minOccurs="0"/>
        <xs:element name="acct_tunnel_packet_lost" type="xs:string" minOccurs="0"/>
        <xs:element name="security_group" type="xs:string" minOccurs="0"/>
        <xs:element name="cisco_h323_setup_time" type="xs:dateTime" minOccurs="0"/>
        <xs:element name="cisco_h323_connect_time" type="xs:dateTime" minOccurs="0"/>
        <xs:element name="cisco_h323_disconnect_time" type="xs:dateTime" minOccurs="0"/>
        <xs:element name="framed_protocol" type="xs:string" minOccurs="0"/>
        <xs:element name="started" type="xs:anyType" minOccurs="0"/>
        <xs:element name="stopped" type="xs:anyType" minOccurs="0"/>
        <xs:element name="ckpt_id" type="xs:long" minOccurs="0"/>
        <xs:element name="type" type="xs:long" minOccurs="0"/>
        <xs:element name="nad_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
        <xs:element name="vlan" type="xs:string" minOccurs="0"/>
        <xs:element name="dacl" type="xs:string" minOccurs="0"/>
        <xs:element name="authentication_type" type="xs:string" minOccurs="0"/>
        <xs:element name="interface_name" type="xs:string" minOccurs="0"/>
        <xs:element name="reason" type="xs:string" minOccurs="0"/>
        <xs:element name="endpoint_policy" type="xs:string" minOccurs="0"/>
      </xs:sequence>
    </xs:complexType>

    <xs:element name="nas_ipv6_address" type="xs:string"/>
    <xs:complexType name="framed_ipv6_address_list">
      <xs:sequence minOccurs="0" maxOccurs="8"><xs:element name="ipv6_address"
  type="xs:string" />
      </xs:sequence>
    </xs:complexType>
```

```
  <xs:element name="framed_ipv6_address" type="framed_ipv6_address_list" minOccurs="1"
maxOccurs="1"/>

</xs:schema>
```

调用跟踪会话 ID API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与审计会话 ID API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/Session/Active/SessionID/ <*审计会话 ID* >/0）：

```
https://acme123/admin/API/mnt/Session/Active/SessionID/0A000A770000006B609A13A9/0
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从审计会话 ID API 调用返回的数据

在调用跟踪会话 ID API 呼叫时，以下示例说明从活动会话列表返回的会话相关的数据

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.
-<activeSessionList noOfActiveSession="1">
    -<activeSession>
        <calling_station_id>00:50:56:10:13:02</calling_station_id>
        <session_state_bit>0</session_state_bit>
        <session_source>0</session_source>
        <acct_session_time>0</acct_session_time>
        <nas_ip_address>10.0.10.119</nas_ip_address>
        <nas_ipv6_address>2001:cdba::3257:9652</nas_ipv6_address>
        <framed_ipv6_address>
        <ipv6_address>200:cdba:0000:0000:0000:0000:3257:9652</ipv6_address>
        <ipv6_address> 2001:cdba:0:0:0:0:3257:9651</ipv6_address>
        <ipv6_address>2001:cdba::3257:9652</ipv6_address>
        </framed_ipv6_address>
        <nas_port_id>GigabitEthernet1/0/15</nas_port_id>
        <auth_method>dot1x</auth_method>
        <auth_protocol>PEAP (EAP-MSCHAPv2)</auth_protocol>
        <posture_status>Compliant</posture_status>
        <endpoint_policy>Undetermined</endpoint_policy>
        <server>acme123</server>
        <paks_in>0</paks_in>
```

```
        <paks_out>0</paks_out>
        <bytes_in>0</bytes_in>
        <bytes_out>0</bytes_out>
    </activeSession>
</activeSessionList>
```

过时的会话

某些设备，例如无线局域网控制器 (WLC)，可以允许过时会话徘徊。在这种情况下，您可以使用 HTTP **删除** API 呼叫手动删除非活动会话。为此，请使用 **curl**，用于传输数据的免费 3 方命令行工具与 URL（HTTP，HTTPS）语法。

ISE 不再跟踪这些会话。这是为了缓解问题，当 ISE 长时间失去网络连接，并沿着 Forensic 从 WLC/NAD 的记账停止。您可以清除使用此 API 的 ISE 的此类过时的信息。

备注　GNU Wget，检索的免费程序文件使用 HTTP，并且 HTTPS，不支持 HTTP **删除** API 呼叫。

删除已过期的会话

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

备注　API 呼叫区分大小写，并且必须小心输入。可变的 <mntnode> 代表监控 ESS 节点的 Cisco。

步骤 4　手动删除 MAC 地址的过期的会话，请发出在命令行中以下 API 呼叫：

```
curl -X DELETE https://<mntnode>/admin/API/mnt/Session/Delete/MACAddress/<madaddress>
```

步骤 5　手动删除会话 ID 的过期的会话，请发出在命令行中以下 API 呼叫：

```
curl -X DELETE https://<mntnode>/admin/API/mnt/Session/Delete/SessionID/<sid#>
```

步骤 6　手动删除监控节点的所有会话，请发出在命令行中以下 API 呼叫：

```
curl -X DELETE https://<mntnode>/admin/API/mnt/Session/Delete/All
```

相关主题

- 验证监控节点，第 1-2 页

用于故障排除的查询 API

本章提供示例并描述如何使用单独的 Cisco Prime 网络控制系统 (NCS) REST API 呼叫。

Cisco Prime NCS API 呼叫

Cisco Prime NCS API 呼叫获取有关该目标监视器 ESS 包括节点版本和类型、故障原因、身份验证状态和客户状态的节点会话的思科重要故障排除信息的框架。

使用查询 API 呼叫的故障排除 Cisco ISE

Cisco Prime 排除 API 呼叫的NCS 发送状态请求到目标监控您的 Cisco ISE 配置的 Cisco ESS 节点并检索以下诊断相关的信息。

- 节点版本和类型（使用版本 API 呼叫，）
- 故障原因（使用 FailureReasons API 呼叫，）
- 身份验证状态（使用 AuthStatus API 呼叫，）
- 客户状态（使用 AcctStatus API 呼叫，）

节点版本和类型 API 呼叫

您可以使用版本 API 呼叫测试其它编程接口 (PI) 服务和每个节点凭证。本节提供请求 Cisco ISE 软件和节点类型的版本提供架构文件输出示例、方法通过调用此 API 呼叫和返回节点版本和类型的示例发出后，在此 API 调用。

节点类型可以是以下任意值：

- STANDALONE_MNT_NODE = 0
- ACTIVE_MNT_NODE= 1
- BACKUP_MNT_NODE = 2
- NOT_AN_MNT_NODE = 3

版本 API 输出方案

此示例架构文件是版本 API 呼叫的输出在发送后到目标监控 ESS 节点的 Cisco：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="product" type="product"/>

  <xs:complexType name="product">
    <xs:sequence>
      <xs:element name="version" type="xs:string" minOccurs="0"/>
  <xs:element name="type_of_node" type="xs:int"/>
    </xs:sequence>
    <xs:attribute name="name" type="xs:string"/>
  </xs:complexType>
</xs:schema>
```

调用版本 API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

如果您的登录不成功，单击登录时**出现问题？**链接在登录页并按照第 2 步中的说明。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与版本 API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/ <specific - api - call>）：

```
https://acme123/admin/API/mnt/Version
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从版本 API 调用返回的数据

当您将在目标监视器 ESS 节点时，思科的版本 API 调用以下示例说明返回的数据。此 API 调用返回目标节点的以下两个值。

- 节点版本（本示例显示 1.0.3.032）。
- ESS 监控节点的 Cisco 的类型（本示例显示了“1”，这意味着监控 ESS 节点）的虚拟化思科。

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<product name="Cisco Identity Services Engine">
<version>1.0.3.032</version>
<type_of_node>1</type_of_node>
</product>
```

故障原因 API 呼叫

您可以使用 FailureReasons API 调用返回故障原因列表在身份验证状态检查返回的完成目标节点。本节提供架构文件输出示例，请求的 Cisco 记录的所有故障原因列表方法监控 ESS 节点通过调用此 API 调用，并发出在此 API 呼叫后返回的故障原因的示例。返回的每个故障原因包括显示的以下元素。表 3-1

备注 有关使用 Cisco ISE 故障原因编辑器的详细信息访问故障原因的完整列表，请参阅 Cisco ISE 故障原因报告，第 A-1 页。

表 3-1　　思科身份服务引擎的产品文档

故障原因元素	示例
故障原因 ID	<failureReason id="11011">
代码	<11011 RADIUS listener failed>
原因	<Could not open one or more of the ports used to receive RADIUS requests>
分辨率	<Ensure that the ports 1812, 1813, 1645 and 1646 are not being used by another process on the system>

备注 使用 Cisco ISE 用户界面（单击**监控 > 报告 > 目录 > 故障原因**），**您还可以检查故障原因**报告，将显示故障原因报告。

FailureReasons API 输出方案

此示例架构文件是 FailureReasons API 呼叫的输出在发送请求后到目标监视器 ESS 节点的 Cisco：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="failureReasonList" type="failureReasonList"/>

  <xs:complexType name="failureReasonList">
    <xs:sequence>
      <xs:element name="failureReason" type="failureReason" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="failureReason">
    <xs:sequence>
```

```
      <xs:element name="code" type="xs:string" minOccurs="0"/>
      <xs:element name="cause" type="xs:string" minOccurs="0"/>
      <xs:element name="resolution" type="xs:string" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="id" type="xs:string"/>
  </xs:complexType>
</xs:schema>
```

调用 FailureReasons API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

如果您的登录不成功，单击登录时**出现问题？**链接在登录页并按照第 2 步中的说明。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与 FailureReasons API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/ <specific - api - call>）：

```
https://acme123/admin/API/mnt/FailureReasons
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从 FailureReasons API 调用返回的数据

当您将在目标监视器 ESS 节点时，思科的一 FailureReasons API 调用以下示例说明返回的数据。此 API 调用返回故障列表从目标节点证明，并且每个故障原因由故障 ID、失败代码、原因和分辨率定义的（如果知道）。

备注　以下 FailureReasons API 呼叫示例仅显示可以返回数据的小型示例。

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<failureReasonList>
-
<failureReason id="100001">
-
<code>
100001 AUTHMGR-5-FAIL Authorization failed for client
```

```
</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
-
<failureReason id="100002">
-
<code>
100002 AUTHMGR-5-SECURITY_VIOLATION Security violation on the interface
</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
-
<failureReason id="100003">
-
<code>
100003 AUTHMGR-5-UNAUTHORIZED Interface unauthorized
</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
-
<failureReason id="100004">
-
<code>
100004 DOT1X-5-FAIL Authentication failed for client
</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
-
<failureReason id="100005">
<code>100005 MAB-5-FAIL Authentication failed for client</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
-
<failureReason id="100006">
-
<code>
100006 RADIUS-4-RADIUS_DEAD RADIUS server is not responding
</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
```

```
-
<failureReason id="100007">
-
<code>
100007 EPM-6-POLICY_APP_FAILURE Interface ACL not configured
</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
```

相关主题

- 验证监控节点，第 1-2 页
- 附录 A“Cisco ISE 故障原因报告”

身份验证状态 API 呼叫

您可以使用 AuthStatus API 呼叫检查会话的身份验证状态目标节点的。查询与此 API 呼叫关联的返回的指定的 MAC 地址至少需要一个 MAC 地址被搜索到一个匹配项，与新记录的一个用户可配置限制。

本节提供架构文件输出示例，发送方式请求搜索会话在目标监控模式的身份验证状态通过调用此 API 调用，并发出在此 API 呼叫后返回的数据的示例。

AuthStatus API 呼叫让您配置以下搜索相关的参数。

- 持续时间 - 定义尝试搜索和检索与指定 MAC 地址相关的身份验证状态记录所花费的时间（秒数）。有效的用户可配置值范围为 1 秒至 864000 秒（10 天）。如果您输入 0 秒的值，此字段指定 10 天的默认持续时间。
- 记录 - 定义每个 MAC 地址所要搜索的会话记录的数量。用户可配置的有效值范围是 1 至 500 条记录。如果输入 0，则指定 200 记录默认设置。

  备注　如果您为持续时间和记录参数指定该值 0，此 API 调用返回只需要最新的身份验证会话记录将指定的 MAC 地址。

  这是 URL 的通用表单示例与持续时间和记录属性的：

  https://10.10.10.10/admin/API/mnt/AuthStatus/MACAddress/01:23:45:67:89:98/900000/2/All

- 属性 - 定义在使用 AuthStatus API 调用搜索身份验证状态时返回的身份验证状态表中包含的属性数量。有效值包括 0（默认），所有或 user_name+acs_timestamp（参阅 AuthStatus 方案示例，AcctStatus API 输出方案，第 3-12 页）。
  - 如果您输入“0”，定义的属性返回。表 3-2 这些在输出方案的 RESTAuthStatus 部分列出。
  - 如果您输入“所有”，属性全套返回。这些在输出方案的 fullRESTAuthStatus 部分列出。
  - 如果您在 user_name+acs_timestamp 的方案输入列出的值，那些属性返回。user_name 和 acs_timestamp 属性在输出方案的 RESTAuthStatus 部分列出。

表 3-2　身份验证状态表属性

属性	说明
name=“通过”或 name=“失败”	身份验证状态结果： • 已通过 • 失败
name=”user_name”	用户名
name=”nas_ip_address”	网络访问设备的 IP 地址/主机名
name=”nas_ipv6_address”	网络访问设备的 IPv6 地址/主机名
name=” failure_reason”	会话身份验证失败的原因
name=” calling_station_id”	源 IP 地址
name=” nas_port”	网络访问服务器端口
name=” identity_group”	包含相关用户和主机的逻辑组
name=” network_device_name”	网络设备的名称
name=” acs_server”	思科 ISE 设备的名称
name=” eap_authentication”	身份验证请求所使用的扩展身份验证协议 (EAP) 方法
name=” framed_ip_address”	为特定用户配置的地址
name=”framed_ipv6_address”	为特定用户配置的地址
network_device_groups”	包含相关网络设备的逻辑组
name=” access_service”	已应用的访问服务
name=” acs_timestamp”	与思科 ISE 身份验证请求关联的时间戳
name=”authentication_method”	标识身份验证中使用的方法
name=”execution_steps”	处理请求时记录的各个诊断消息的消息代码列表
name=”radius_response”	RADIUS 响应类型（例如 VLAN 或 ACL）
name=”audit_session_id”	身份验证会话的 ID
name=”nas_identifier”	与特定资源关联的网络访问服务器 (NAS)
name=”nas_port_id”	所使用的 NAS 端口的 ID
name=”nac_policy_compliance”	反映安全状态（合规或不合规）
name=”selected_azn_profiles”	标识身份验证中使用的配置文件
name=”service_type”	表示帧的用户
name=”eap_tunnel”	EAP 身份验证所使用的隧道或外部方法
name=”message_code”	审计消息，用于标识请求处理结果
name=”destination_ip_address”	标识目的 IP 地址

AuthStatus API 输出方案

此示例架构文件是 AuthStatus API 呼叫的输出在发送后到目的地的监控 ESS 节点的 Cisco 指定的会话数：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="authStatusOutputList" type="fullRESTAuthStatusOutputList"/>

  <xs:complexType name="fullRESTAuthStatusOutputList">
    <xs:sequence>
      <xs:element name="authStatusList" type="fullRESTAuthStatusList" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="fullRESTAuthStatusList">
    <xs:sequence>
      <xs:element name="authStatusElements" type="fullRESTAuthStatus" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="key" type="xs:string"/>
  </xs:complexType>

  <xs:complexType name="fullRESTAuthStatus">
    <xs:complexContent>
      <xs:extension base="restAuthStatus">
        <xs:sequence>
          <xs:element name="id" type="xs:long" minOccurs="0"/>
          <xs:element name="acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
          <xs:element name="acs_session_id" type="xs:string" minOccurs="0"/>
          <xs:element name="service_selection_policy" type="xs:string" minOccurs="0"/>
          <xs:element name="authorization_policy" type="xs:string" minOccurs="0"/>
          <xs:element name="identity_store" type="xs:string" minOccurs="0"/>
          <xs:element name="response" type="xs:string" minOccurs="0"/>
          <xs:element name="cts_security_group" type="xs:string" minOccurs="0"/>
          <xs:element name="use_case" type="xs:string" minOccurs="0"/>
          <xs:element name="cisco_av_pair" type="xs:string" minOccurs="0"/>
          <xs:element name="ad_domain" type="xs:string" minOccurs="0"/>
          <xs:element name="acs_username" type="xs:string" minOccurs="0"/>
          <xs:element name="radius_username" type="xs:string" minOccurs="0"/>
          <xs:element name="nac_role" type="xs:string" minOccurs="0"/>
          <xs:element name="nac_username" type="xs:string" minOccurs="0"/>
          <xs:element name="nac_posture_token" type="xs:string" minOccurs="0"/>
          <xs:element name="nac_radius_is_user_auth" type="xs:string" minOccurs="0"/>
          <xs:element name="selected_posture_server" type="xs:string" minOccurs="0"/>
          <xs:element name="selected_identity_store" type="xs:string" minOccurs="0"/>
          <xs:element name="authentication_identity_store" type="xs:string"

minOccurs="0"/>
          <xs:element name="azn_exp_pol_matched_rule" type="xs:string" minOccurs="0"/>
          <xs:element name="ext_pol_server_matched_rule" type="xs:string" minOccurs="0"/>
          <xs:element name="grp_mapping_pol_matched_rule" type="xs:string" minOccurs="0"/>
          <xs:element name="identity_policy_matched_rule" type="xs:string" minOccurs="0"/>
          <xs:element name="nas_port_type" type="xs:string" minOccurs="0"/>
          <xs:element name="query_identity_stores" type="xs:string" minOccurs="0"/>
          <xs:element name="sel_exp_azn_profiles" type="xs:string" minOccurs="0"/>
          <xs:element name="selected_query_identity_stores" type="xs:string"
minOccurs="0"/>
          <xs:element name="tunnel_details" type="xs:string" minOccurs="0"/>
          <xs:element name="cisco_h323_attributes" type="xs:string" minOccurs="0"/>
          <xs:element name="cisco_ssg_attributes" type="xs:string" minOccurs="0"/>
```

```
            <xs:element name="other_attributes" type="xs:string" minOccurs="0"/>
            <xs:element name="response_time" type="xs:long" minOccurs="0"/>
            <xs:element name="nad_failure" type="xs:anyType" minOccurs="0"/>
          </xs:sequence>
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="restAuthStatus">
      <xs:sequence>
        <xs:element name="passed" type="xs:anyType" minOccurs="0"/>
        <xs:element name="failed" type="xs:anyType" minOccurs="0"/>
        <xs:element name="user_name" type="xs:string" minOccurs="0"/>
        <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
        <xs:element name="failure_reason" type="xs:string" minOccurs="0"/>
        <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
        <xs:element name="nas_port" type="xs:string" minOccurs="0"/>
        <xs:element name="identity_group" type="xs:string" minOccurs="0"/>
        <xs:element name="network_device_name" type="xs:string" minOccurs="0"/>
        <xs:element name="acs_server" type="xs:string" minOccurs="0"/>
        <xs:element name="eap_authentication" type="xs:string" minOccurs="0"/>
        <xs:element name="framed_ip_address" type="xs:string" minOccurs="0"/>
        <xs:element name="network_device_groups" type="xs:string" minOccurs="0"/>
        <xs:element name="access_service" type="xs:string" minOccurs="0"/>
        <xs:element name="acs_timestamp" type="xs:dateTime" minOccurs="0"/>
        <xs:element name="authentication_method" type="xs:string" minOccurs="0"/>
        <xs:element name="execution_steps" type="xs:string" minOccurs="0"/>
        <xs:element name="radius_response" type="xs:string" minOccurs="0"/>
        <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
        <xs:element name="nas_identifier" type="xs:string" minOccurs="0"/>
        <xs:element name="nas_port_id" type="xs:string" minOccurs="0"/>
        <xs:element name="nac_policy_compliance" type="xs:string" minOccurs="0"/>
        <xs:element name="selected_azn_profiles" type="xs:string" minOccurs="0"/>
        <xs:element name="service_type" type="xs:string" minOccurs="0"/>
        <xs:element name="eap_tunnel" type="xs:string" minOccurs="0"/>
        <xs:element name="message_code" type="xs:string" minOccurs="0"/>
        <xs:element name="destination_ip_address" type="xs:string" minOccurs="0"/>
      </xs:sequence>
    </xs:complexType>

    <xs:element name="nas_ipv6_address" type="xs:string"/>
    <xs:complexType name="framed_ipv6_address_list">
      <xs:sequence minOccurs="0" maxOccurs="8"><xs:element name="ipv6_address"
type="xs:string" />
      </xs:sequence>
    </xs:complexType>
    <xs:element name="framed_ipv6_address" type="framed_ipv6_address_list" minOccurs="1"
maxOccurs="1"/>
</xs:schema>
```

调用 AuthStatus API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

如果您的登录不成功，单击登录时**出现问题？**链接在登录页并按照第 2 步中的说明。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与 AuthStatus API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/ <specific - api - call>/MACAddress/ <macaddress>/<seconds>/<numberofrecordspermacaddress>/All）：

```
https://acme123/admin/API/mnt/AuthStatus/MACAddress/00:50:56:10:13:02/120/100/All
```

备注　REST API 呼叫区分大小写。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从 AuthStatus API 调用返回的数据

当您将在目标监视器 ESS 节点时，思科的一 AuthStatus API 调用以下示例说明返回的数据：

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<authStatusOutputList>
-
<authStatusList key="00:0C:29:46:F3:B8"><authStatusElements>
-
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>suser77</user_name>
<nas_ip_address>10.77.152.209</nas_ip_address>
<nas_ipv6_address>2001:cdba::3257:9652</nas_ipv6_address>
<calling_station_id>00:0C:29:46:F3:B8</calling_station_id>
<identity_group>User Identity Groups:Guest</identity_group>
<acs_server>guest-240</acs_server>
<acs_timestamp>2012-10-05T10:50:56.515Z</acs_timestamp>
<execution_steps>5231</execution_steps>
<message_code>5231</message_code>
<id>1349422277270561</id>
<acsview_timestamp>2012-10-05T10:50:56.517Z</acsview_timestamp>
<identity_store>Internal Users</identity_store>
<response_time>146</response_time>
<other_attributes>ConfigVersionId=81,EndPointMACAddress=00-0C-29-46-F3-B8,PortalName=Defau
ltGuestPortal,
CPMSessionID=0A4D98D1000001F26F0C04D9,CiscoAVPair=</other_attributes>
</authStatusElements>
-
<authStatusElements>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>00:0C:29:46:F3:B8</user_name>
<nas_ip_address>10.77.152.209</nas_ip_address>
<nas_ipv6_address>2001:cdba::3257:9652</nas_ipv6_address>
<framed_ipv6_address>
<ipv6_address>2001:cdba:0000:0000:0000:0000:3257:9652</ipv6_address>
```

```
<ipv6_address> 2001:cdba:0:0:0:0:3257:9652</ipv6_address>
<ipv6_address>2001:cdba::3257:9652</ipv6_address>
</framed_ipv6_address>
<calling_station_id>00:0C:29:46:F3:B8</calling_station_id>
<identity_group>Guest_IDG</identity_group>
<network_device_name>switch</network_device_name>
<acs_server>guest-240</acs_server>
<authentication_method>mab</authentication_method>
<authentication_protocol>Lookup</authentication_protocol>
<acs_timestamp>2012-10-05T10:49:47.915Z</acs_timestamp>
<execution_steps>11001,11017,11027,15049,15008,15048,15048,15004,15041,15006,15013,24209,2
421
1,22037,15036,15048,15004,15016,11022,11002</execution_steps>
<response>{UserName
=00:0C:29:46:F3:B8; User-Name=00-0C-29-46-F3-B8;
State=ReauthSession:0A4D98D1000001F26F0C04D9;
Class=CACS:0A4D98D1000001F26F0C04D9:guest-240/138796808/76;
Termination-Action=RADIUS-Request; Tunnel-Type=(tag=1) VLAN;
Tunnel-Medium-Type=(tag=1) 802; Tunnel-Private-Group-ID=(tag=1) 2;
cisco-av-pair=url-redirect-acl=ACL-WEBAUTH-REDIRECT;
cisco-av-pair=url-redirect=https://guest-240.cisco.com:8443/guestportal/gateway?
sessionId=0A4D98D1000001F26F0C04D9&action=cwa;
cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-pre-posture-506e980a;
cisco-av-pair=profile-name=WindowsXP-Workstation;}</response
><audit_session_id>0A4D98D1000001F26F0C04D9</audit_session_id><nas_po
rt_id>GigabitEthernet1/0/17</nas_port_id><posture_status>Pending</posture_status>
<selected_azn_profiles>CWA_Redirect</selected_azn_profiles>
<service_type>Call Check</service_type>
<message_code>5200</message_code>
<nac_policy_compliance>Pending</nac_policy_compliance>
<id>1349422277270556</id>
<acsview_timestamp>2012-10-05T10:49:47.915Z</acsview_timestamp>
<identity_store>Internal Endpoints</identity_store>
<response_time>13</response_time>
<other_attributes>ConfigVersionId=81,DestinationPort=1812,Protocol=Radius,AuthorizationPol
icyMatchedRule=CWA_Redirect,
NAS-Port=50117,Framed-MTU=1500,NAS-Port-Type=Ethernet,EAP-Key-N
ame=,cisco-nas-port=GigabitEthernet1/0/17,AcsSessionID=guest-240/138796808/76,Us
eCase=Host Lookup,SelectedAuthenticationIdentityStores=Internal
Endpoints,ServiceSelectionMatchedRule=MAB,IdentityPolicyMatchedRule=Default,CPMS
essionID=0A4D98D1000001F26F0C04D9,EndPointMACAddress=00-0C-29-46-F3-B8,EndPointM
atchedProfile=WindowsXP-Workstation,ISEPolicySetName=Default,HostIdentityGroup=E
ndpoint Identity Groups:Guest_IDG,Device Type=Device Type#All Device
Types,Location=Location#All Locations,Device IP
Address=10.77.152.209,Called-Station-ID=00:24:F7:73:9A:91,CiscoAVPair=audit-sess
ion-id=0A4D98D1000001F26F0C04D9</other_attributes>
-
</authStatusElements>
-
</authStatusList>
-
</authStatusOutputList>
```

客户状态 API 呼叫

您可以使用 AcctStatus API 呼叫检索有关目的节点的最新的设备和会话帐户信息。本节提供架构文件输出示例，发送的一个需要方法最新的设备和会话信息通过调用此 API 调用，并发出在此 API 呼叫后返回的数据的示例。AcctStatus API 呼叫让您配置一个与时间相关的参数。

- 持续时间 - 定义尝试搜索和检索与指定 MAC 地址相关的最后账户设备记录所花费的时间（秒数）。有效的用户可配置值范围为 1 秒至 432000 秒（5 天）。例如，
  - 如果您输入 2400 秒（40 分钟）的值，这意味着您想要是可用在过去 40 分钟内指定的 MAC 地址的最新客户设备记录。
  - 如果您输入 0 秒的值，这为 15 分钟（900 秒）的默认持续时间。这意味着您希望在此时段可用的指定的 MAC 地址的最新客户设备记录。

AcctList API 呼叫提供以下客户状态数据字段，当 API 输出（请参阅表 3-3）：

表 3-3　　客户状态数据字段

数据字段	说明
MAC 地址	客户端的 MAC 地址
跟踪会话 ID	身份验证会话 ID
传入的数据包数	已收到的数据包总数
传出的数据包数	已发送的数据包总数
收到的字节数	已收到的总字节数
外发的字节数	已发送的总字节数
会话超时	当前会话的持续时间

AcctStatus API 输出方案

此示例架构文件是 AcctStatus API 呼叫的输出在发送后到目的地的监控 ESS 节点的 Cisco 指定的会话数：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="acctStatusOutputList" type="restAcctStatusOutputList"/>

  <xs:complexType name="restAcctStatusOutputList">
    <xs:sequence>
      <xs:element name="acctStatusList" type="restAcctStatusList" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="restAcctStatusList">
    <xs:sequence>
      <xs:element name="acctStatusElements" type="restAcctStatus" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="macAddress" type="xs:string"/>
    <xs:attribute name="username" type="xs:string"/>
  </xs:complexType>

  <xs:complexType name="restAcctStatus">
    <xs:sequence>
```

```
        <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
        <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
        <xs:element name="paks_in" type="xs:long" minOccurs="0"/>
        <xs:element name="paks_out" type="xs:long" minOccurs="0"/>
        <xs:element name="bytes_in" type="xs:long" minOccurs="0"/>
        <xs:element name="bytes_out" type="xs:long" minOccurs="0"/>
        <xs:element name="session_time" type="xs:long" minOccurs="0"/>
        <xs:element name="username" type="xs:string" minOccurs="0"/>
    <xs:element name="server" type="xs:string" minOccurs="0"/>
      </xs:sequence>
    </xs:complexType>
</xs:schema>
```

调用 AcctStatus API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

如果您的登录不成功，单击登录时**出现问题？**链接在登录页并按照第 2 步中的说明。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与 AcctStatus API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/ <specific - api - call>/MACAddress/<macaddress>/ <durationofcurrenttime>）：

```
https://acme123/admin/API/mnt/AcctStatus/MACAddress/00:26:82:7B:D2:51/1200
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从 AcctStatus API 调用返回的数据

当您将在目标监视器 ESS 节点时，思科的一 AcctStatus API 调用以下示例说明返回的数据：

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<acctStatusOutputList>
-
<acctStatusList macAddress="00:25:9C:A3:7D:48">
-
<acctStatusElements>
<calling_station_id>00:25:9C:A3:7D:48</calling_station_id>
<audit_session_id>0acb6b0b0000000B4D0C0DBD</audit_session_id>
```

```
<paks_in>0</paks_in>
<paks_out>0</paks_out>
<bytes_in>0</bytes_in>
<bytes_out>0</bytes_out>
<session_time>240243</session_time>
<server>HAREESH-R6-1-PDP1</server>
</acctStatusElements>
</acctStatusList>
</acctStatusOutputList>
```

权限 REST API 更改

本章提供示例并描述如何使用授权思科身份服务引擎此版本支持的 (CoA) REST API 调用以下单独更改。

简介

CoA API 呼叫用于发送会话身份验证和会话断开命令提供了到监控您的 Cisco ISE 配置的指定的 Cisco ESS 节点。

CoA Session Management API 呼叫

CoA 会话管理 API 呼叫允许您发送重新进行身份验证和断开命令到目标的监控您的 Cisco ISE 配置的 Cisco 指定的会话 ESS 节点：

- 默认端口（Reauth）
- 会话断开（断开）

默认端口 API 呼叫

默认端口 API 呼叫构成以下类型的

- REAUTH_TYPE_DEFAULT = 0
- REAUTH_TYPE_LAST = 1
- REAUTH_TYPE_RERUN = 2

Reauth API 输出方案

此示例架构文件是 Reauth API 呼叫的输出在发送后到目的地的监控 ESS 节点的 Cisco 指定的会话数。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="remoteCoA" type="coAResult"/>
<xs:complexType name="coAResult">
    <xs:sequence>
      <xs:element name="results" type="xs:boolean" minOccurs="0"/>
    </xs:sequence>
```

```
    <xs:attribute name="requestType" type="xs:string"/>
  </xs:complexType>
</xs:schema>
```

调用 Reauth API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与 Reauth API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/CoA/ <specific - api - call>/<macaddress>/ <reauthtype>：

```
https://acme123/admin/API/mnt/CoA/Reauth/server12/00:26:82:7B:D2:51/1
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样从 Reauth API 调用返回的数据

当您将在目标监视器 ESS 节点时，思科的一 Reauth API 调用以下示例说明返回的数据。两种可能的结果可以从调用此命令返回：

- true 表明命令已成功执行。
- 错误表示命令并未执行（由于各种情况）。

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<remoteCoA requestType="reauth">
<results>true</results>
</remoteCoA>
```

会话断开 API 呼叫

会话断开 API 呼叫构成以下断开端口选项类型：

- DYNAMIC_AUTHZ_PORT_DEFAULT = 0
- DYNAMIC_AUTHZ_PORT_BOUNCE = 1
- DYNAMIC_AUTHZ_PORT_SHUTDOWN = 2

断开 API 输出方案

此示例架构文件是断开 API 呼叫的输出在发送后到目的地的监控 ESS 节点的 Cisco 指定的会话数

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="remoteCoA" type="coAResult"/>

  <xs:complexType name="coAResult">
    <xs:sequence>
      <xs:element name="results" type="xs:boolean" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="requestType" type="xs:string"/>
  </xs:complexType>
</xs:schema>
```

调用断开 API 呼叫

步骤 1　在浏览器的地址栏内输入 Cisco ISE URL（例如，*https://<ISE 主机名或 IP 地址>/admin/*）。

步骤 2　输入在 Cisco ISE 初始设置过程中指定和配置的用户名及密码（区分大小写）。

步骤 3　点击 **Login** 或按 **Enter**。

例如，当您最初记录到监控与主机名的 Cisco ESS 节点 - acme123 时，将显示此节点的以下 URL 地址：

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

步骤 4　在 URL 地址目标节点领域参与断开 API 呼叫通过替换“/admin/”组件使用的 API 呼叫组件（/admin/API/mnt/CoA/ <Disconnect>/<serverhostname>/<macaddress>/<portoptiontype>/<nasipaddress>/<destinationipaddress>：

```
https://acme123/admin/API/mnt/CoA/Disconnect/server12/00:26:82:7B:D2:51/2/10.10.10.10/192.168.1.1
```

备注　因为这些呼叫区分大小写，您必须在 URL 地址目标节点领域仔细输入每个 API 调用。使用“安装”在 API 呼叫约定代表监控 ESS 节点的 Cisco。

步骤 5　按 **Enter** 发出 API 呼叫。

相关主题

- 验证监控节点，第 1-2 页

采样断开与 API 调用返回的数据

当您将在目标监视器 ESS 节点时，思科的断开 API 调用以下示例说明返回的数据。两种可能的结果可通过调用此命令返回：

- true 表明命令已成功执行。
- 错误表示命令并未执行（由于各种情况）。

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<remoteCoA requestType="reauth">
<results>true</results>
</remoteCoA>
```

第 2 部分

Cisco ISE 外部 RESTful 服务 API

ERS API 简介

使用外部 RESTful 服务 API 调用的前提条件

您必须满足以下必备条件，才能发起外部 RESTful 服务 API 调用：

- 您必须已通过 GUI 启用外部 RESTful 服务。
- 您必须具有外部 RESTful 服务管理员权限。

您可以使用 REST 客户端（如 JAVA）、curl linux 命令、python 或任何其他客户端来调用外部 RESTful 服务 API 调用。

外部宁静的服务 SDK

您可以使用外部宁静的服务 SDK 开始迁移工具支持工具。您可以使用如下 URL 获取外部 RESTful 服务 SDK：`https://<ISE-ADMIN-NODE>:9060/ers/sdk`。

只有外部 RESTful 服务管理员用户可以获取外部 RESTful 服务 SDK。SDK 包括以下组件

- 快速参考 API文档
- 所有可用 API 操作的完整列表
- 架构文件可下载
- 在 Java 的示例应用程序可以下载
- curl 脚本格式的使用案例
- Python 脚本格式的使用案例
- 使用 Chrome Postman 的说明

SDK 中提供以下 API：

- 证书模板 API
- 清除威胁和漏洞 API
- 出口表单元格 API
- 终端 API
- 终端证书 API
- 终端身份组 API
- 访客位置 API
- 访客 SMTP 通知配置 API

- 访客 SSID API
- 访客类型 API
- 访客用户 API
- 热点门户 API
- IP 到 SGT 映射 API
- IP 到 SGT 映射组 API
- ISE 服务信息 API
- 身份组 API
- 身份序列 API
- 内部用户 API
- 我的设备门户 API
- 本地请求方配置文件 API
- 网络设备 API
- 网络设备组 API
- 节点详细信息 API
- 采用 RADIUS 服务的 PSN 节点详细信息 API
- 门户 API
- 门户主题 API
- 分析器配置文件 API
- SMS 服务器 API
- SXP 链接 API
- SXP 本地绑定 API
- SXP VPN API
- 安全组 API
- 安全组 ACL (SGACL) API
- 自注册门户 API
- 发起方组 API
- 发起方组成员 API
- 发起方门户 API
- 发起的访客门户 API

外部宁静的服务 API 身份验证和授权

外部宁静的服务 API 根据 HTTPS 协议和其他方式和使用端口 9060。

外部宁静的服务 API 支持基本身份验证。身份验证凭证加密并是请求报头的一部分。

ESS 管理员分配种类到用户执行操作使用外部宁静的服务 API。

要使用外部 RESTful 服务 API（访客 API 除外）执行操作，用户必须被分配至以下管理员组之一，而且必须通过存储在思科 ISE 内部数据库中的凭证进行身份验证（内部管理员用户）：

- 外部 RESTful 服务管理员 - 对所有 ERS API（GET、POST、DELETE、PUT）的完整访问权限。此用户可以创建、读取、更新和删除 ERS API 请求。
- 外部 RESTful 服务操作人员 - 只读权限（只能使用 GET 请求）。

使用外部宁静的服务 API，如果您没有所需的权限和仍不尝试执行操作，您将收到错误响应。

Cisco ISE 故障原因报告

本附录提供可用于访问 Cisco ISE 故障原因报告的过程。Cisco ISE 故障原因报告允许您查看故障原因列表。

简介

Cisco ISE 故障原因报告是在提供有关所有的信息故障原因可能遇到的 Cisco ISE 用户界面的选项。您可以使用此检查返回作为输出将故障原因映射呼叫，当使用故障排除 API 时的 Cisco ISE 查询的。

Cisco ISE 故障原因报告让您访问的故障原因的完整列表适用于监控 ISE 节点运行的 Cisco ISE 软件定义的。以下程序允许您查看或编辑定义的故障原因列表。您必须登录到该目标 ISE 监控节点的 Cisco ISE 用户界面查看和访问故障原因。有关登录的详细信息，请参阅验证监控节点，第 1-2 页。

查看故障原因

步骤 1 选择**操作 > 报告 > 身份验证摘要**报告。

步骤 2 在 Navigation 窗格中，展开**监控**并选择**故障原因编辑器**。

步骤 3 从提供的过滤器列表选择故障原因。

步骤 4 提供您要查找的故障原因。

步骤 5 点击 Run。

故障原因列表在右侧面板中显示。

步骤 6 单击任何故障原因获得详细数据报表在新窗口中。