



## 维护和监控

---

- [自适应网络控制](#)，第 2 页
- [在思科 ISE 中启用自适应网络控制](#)，第 3 页
- [配置网络访问设置](#)，第 3 页
- [ANC 隔离和取消隔离流程](#)，第 4 页
- [ANC NAS 端口关闭流程](#)，第 5 页
- [终端清除设置](#)，第 5 页
- [隔离的终端在策略更改后不会重新进行身份验证](#)，第 6 页
- [当未找到 IP 地址或 MAC 地址时 ANC 操作失败](#)，第 7 页
- [通过外部身份验证的管理员无法执行 ANC 操作](#)，第 7 页
- [备份数据类型](#)，第 7 页
- [备份和恢复存储库](#)，第 8 页
- [按需备份和计划备份](#)，第 12 页
- [思科 ISE 恢复操作](#)，第 18 页
- [导出身份验证和授权策略配置](#)，第 24 页
- [计划策略导出设置](#)，第 24 页
- [在分布式环境中同步主节点和辅助节点](#)，第 25 页
- [恢复独立和分布式部署中断开的节点](#)，第 25 页
- [思科 ISE 日志记录机制](#)，第 29 页
- [思科 ISE 系统日志](#)，第 30 页
- [配置远程系统日志收集位置](#)，第 30 页
- [思科 ISE 消息代码](#)，第 32 页
- [思科 ISE 消息目录](#)，第 32 页
- [终端调试日志收集器](#)，第 33 页
- [集合过滤器](#)，第 33 页
- [思科 ISE 报告](#)，第 35 页
- [报告过滤器](#)，第 35 页
- [创建快速过滤器条件](#)，第 36 页
- [创建高级过滤条件](#)，第 36 页
- [运行并查看报告](#)，第 36 页

- 报告导航，第 37 页
- 导出报告，第 37 页
- 安排和保存思科 ISE 报告，第 38 页
- 思科 ISE 活动 RADIUS 会话，第 39 页
- 可用报告，第 41 页
- RADIUS 实时日志，第 59 页
- RADIUS 实时会话 (Live Sessions)，第 62 页
- TACACS 实时日志，第 65 页
- 导出摘要，第 67 页

## 自适应网络控制

自适应网络控制 (ANC) 是一项在管理节点上运行的服务。此服务可监控和控制终端的网络访问。ANC 由 ISE 管理员在管理 GUI 上调用，也可以通过 pxGrid 从第三方系统调用。ANC 支持有线和无线部署，并且需要 Plus 许可证。

您可以使用 ANC 更改授权状态，无需修改系统的总体授权策略。ANC 允许您在隔离终端时设置授权状态。结果会建立授权策略，这些授权策略定义为检查 ANCPolicy 以限制或拒绝网络访问。您可以取消隔离终端，使其获得完整的网络访问权限。您也可以关闭网络连接系统 (NAS) 上的端口，断开终端与网络之间的连接。

一次可以隔离的用户数量没有限制。此外，隔离期长度没有时间限制。

您可以执行以下操作，以便通过 ANC 监控和控制网络访问：

- 隔离 - 允许您使用例外策略（授权策略）限制或拒绝终端接入网络。必须创建例外策略，以根据 ANCPolicy 分配不同的授权配置文件（权限）。设置为隔离状态，本质上是将其默认 VLAN 迁移到指定的隔离 VLAN。您必须提前定义隔离 VLAN，在同一 NAS 上作为终端获得支持。
- 取消隔离 - 允许您解除隔离状态，让终端获得完整的网络访问权限。这是通过使终端返回原 VLAN 实现的。
- 关闭 - 允许您禁用 NAS 上的端口，断开终端与网络之间的连接。当终端连接的 NAS 上的端口关闭后，应重新手动重置 NAS 上的端口。这可以让终端连接到网络（不适用于无线部署）。

隔离和取消隔离操作可以从活动终端的会话目录报告触发。



注释

如果取消隔离已隔离的会话，新取消隔离的会话的发起方法将取决于交换机配置指定的身份验证方法。



注释

从 Cisco ISE 1.4 开始，ANC 取代了端点保护服务 (EPS)。ANC 提供额外的分类和性能改进。虽然在策略中使用 ERS 属性有时仍然适用于某些 ANC 操作，但应使用 ANC 属性。

# 在思科 ISE 中启用自适应网络控制

默认情况下禁用 ANC。只有在启用 pxGrid 时才会启用 ANC，并且它将保持启用状态，直到在管理员门户中手动禁用该服务。

## 配置网络访问设置

ANC 可以让您重置终端的网络访问状态，以便对端口进行隔离、取消隔离或关闭端口。这些定义了网络中终端的授权程度。

您可以使用终端 IP 地址或 MAC 地址隔离或取消隔离终端抑或关闭终端所连接的网络访问服务器 (NAS) 端口。您可以在同一终端上多次执行隔离和取消隔离操作，但不能同时执行这两种操作。如果在网络上发现恶意终端，可以使用 ANC 关闭 NAS 端口，从而禁止终端访问。

将 ANC 策略分配至终端：

### 开始之前

- 启用 ANC。
- 为 ANC 创建授权配置文件和例外类型授权策略。

---

**步骤 1** 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 **操作 (Operations) > 自适应网络控制 (Adaptive Network Control) > 策略列表 (Policy List)**。

**步骤 2** 点击添加 (Add)。

**步骤 3** 输入一个 ANC 策略名称并指定 ANC 操作。可提供以下选项：

- 隔离
- Shut\_Down
- Port\_Bounce

您可以选择一个或多个操作，但是您无法将 Shut\_Down 和 Port\_Bounce 与其他 ANC 操作结合。

**步骤 4** 选择策略 (Policy) > 策略集 (Policy Sets)，然后展开策略集。

**步骤 5** 使用 ANCPolicy 属性将 ANC 策略与相应的授权策略相关联。

**步骤 6** 选择操作 (Operations) > 自适应网络控制 (Adaptive Network Control) > 终端分配。

**步骤 7** 点击添加 (Add)。

**步骤 8** 输入终端的 IP 地址或 MAC 地址，并从策略分配 (Policy Assignment) 下拉列表选择策略。

**步骤 9** 点击提交 (Submit)。

---

## 通过 ANC 创建网络访问的授权配置文件

您必须创建一个应该与 ANC 配合使用的授权配置文件。您可以在标准授权配置文件列表中查看该授权配置文件。终端可在网络中进行身份验证和授权，但是限于接入网络。

**步骤 1** 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 **策略 (Policy) > 策略元素 (Policy Elements) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles)**。

**步骤 2** 点击添加 (Add)。

**步骤 3** 为授权配置文件输入唯一名称和说明，并将访问类型 (Access Type) 更新为 **ACCESS\_ACCEPT**。

**步骤 4** 选中 **DACL Name** 复选框，然后从下拉列表中选择 **DENY\_ALL\_TRAFFIC**。

**步骤 5** 点击提交 (Submit)。

例外授权策略用于授权有限访问，满足特殊条件或权限或直接要求。对于 ANC 授权，需要创建隔离例外策略，该策略先于所有标准授权策略进行处理。您需要使用以下条件创建例外规则：

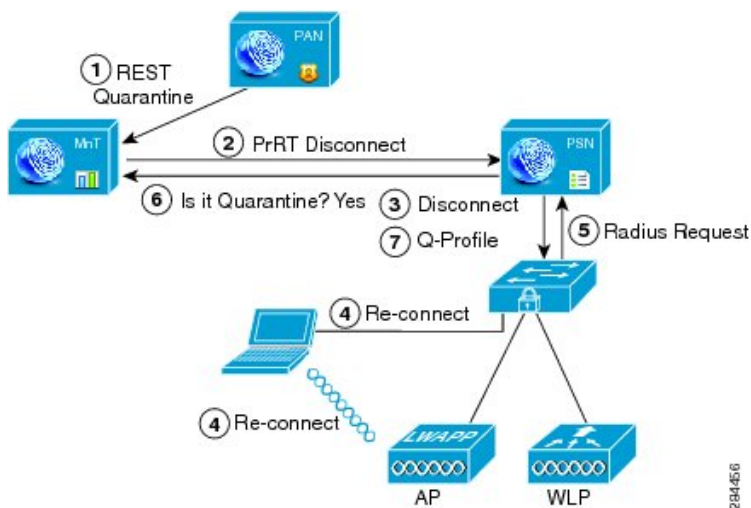
**Session:ANCPolicy EQUALS 隔离。**

## ANC 隔离和取消隔离流程

可以使用 ANC 隔离所选终端，以限制其对网络的访问。您可以隔离终端并建立根据状态分配不同授权配置文件的例外授权策略。授权配置文件用作您在授权策略中定义的允许访问指定网络服务的权限的容器。当授权完成时，系统会为网络访问请求授予权限。如果之后对终端进行了验证，则可以对终端取消隔离以允许其对网络进行完全访问。

此图显示了隔离流程，它假定已配置授权规则并已建立 ANC 会话。

图 1: ANC 隔离流程



284456

1. 客户端设备通过无线设备 (WLC) 登录到网络，并且系统会从管理节点 (PAP) 向监控节点 (MnT) 发出隔离 REST API 调用。
2. 然后，监控节点会通过策略服务 Cisco ISE 节点 (PDP) 来调用 PrRT，从而引发授权证书 (CoA)。
3. 客户端设备的连接会断开。
4. 然后，客户端设备会重新进行身份验证并重新连接。
5. 对客户端设备的 RADIUS 请求会发回到监控节点。
6. 在进行检查时，系统将隔离客户端设备。
7. 系统将应用 Q-Profile 授权策略并验证客户端设备。
8. 系统会对客户端设备取消隔离，并向其提供对网络的完全访问权限。

## ANC NAS 端口关闭流程

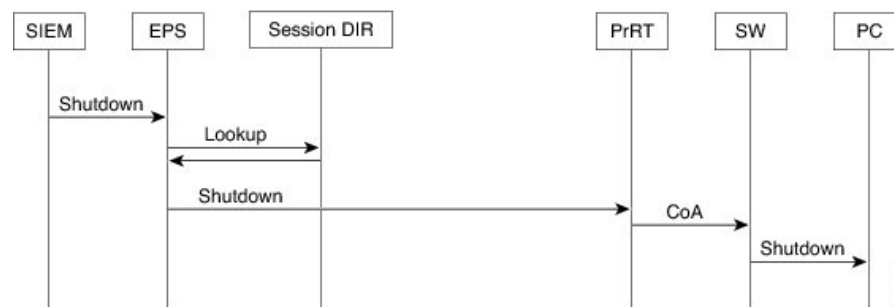
您可以使用终端 IP 地址或 MAC 地址关闭终端所连接的 NAS 端口。

通过此关闭功能您可以根据 MAC 地址的指定 IP 地址关闭 NAS 端口。您必须手动恢复该端口，才能将此终端重新接入网络，这仅对通过有线媒介连接的终端有效。

并非所有设备都支持此关闭功能。不过，大多数交换机应该都支持关闭命令。您可以使用 `getResult()` 命令验证关闭是否执行成功。

下图说明 ANC 关闭流程。对于客户端设备，关闭操作是在客户端设备用于访问网络的 NAS 上执行的。

图 2: ANC 关闭流程



## 终端清除设置

可以根据身份组和其他条件，通过配置规则来定义终端清除策略。在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 管理 (Administration) > 身份管理 (Identity Management) > 设置 (Settings) > 终端清除 (Endpoint Purge)。您可以选择不清除特定终端以及根据选择的分析条件清除终端。

您可以安排终端清除作业计划。默认情况下，此终端清除计划处于启用状态。默认情况下，Cisco ISE 会删除超出 30 天的终端和已注册设备。系统根据主 PAN 中配置的时区于每日凌晨 1 点（午夜）执行清除作业。

终端清除作业每 3 分钟删除 5000 多个终端。

以下是您可以用于清除终端的一些条件以及示例：

- **InactivityDays** - 距离终端上最后一次分析活动或更新的天数
  - 此条件用于清除随时间推移累积的陈旧设备，通常是临时访客或个人设备或废弃的设备。在您的部署中，这些终端容易形成干扰，因为它们在网络上不再活动或近期不再可能出现。如果它们偶然再进行连接，系统将在必要的情况下对其进行发现、分析、注册等。
  - 当存在来自端点的更新时，只要启用分析功能，**InactivityDays** 便会重置为 0。
- **ElapsedDays** - 创建对象之后经过的天数。
  - 此条件适用于获得特定时间段内未经身份验证或有条件的访问权限的终端，例如访客或承包商终端，或利用 **webauth** 进行网络访问的员工。在所允许的连接期限到期之后，他们必须重新进行完全身份验证和注册。
- **PurgeDate** - 要清除终端的日期。
  - 此选项用于在不考虑创建或开始时间的情况下，获得特定时间的访问权限的特殊事件或组。此选项允许同时清除所有终端。例如，贸易展览、会议或每周都有新成员的每周培训课程，在这种情况下，访问权限是根据特定周或月份授予的，而不是绝对的天、周、月。

## 隔离的终端在策略更改后不会重新进行身份验证

### 问题

策略或其他身份更改后，身份验证失败，并且系统不会重新进行身份验证。身份验证失败或有问题的终端仍然无法连接网络。根据分配给用户角色的终端安全策略，未能通过安全评估的客户端计算机上经常会出现此问题。

### 可能的原因

客户端计算机上身份验证计时器的设置不正确，或者交换机上身份验证时间间隔的设置不正确。

### 解决方案

要解决此问题，有几种可能的办法：

1. 在 Cisco ISE 中查看指定 NAD 或交换机的会话状态摘要 (**Session Status Summary**) 报告，确保该界面已配置适当的身份验证间隔。

2. 在 NAD/交换机上输入 “show running configuration” 命令，确保接口已配置适当的 “authentication timer restart” 设置。（例如，“authentication timer restart 15” 和 “authentication timer reauthenticate 15”。）
3. 输入 “interface shutdown” 和 “no shutdown” 退回 NAD/交换机上的端口，并在 Cisco ISE 的潜在配置更改后，强制重新进行身份验证。



注释 由于 CoA 需要 MAC 地址或会话 ID，因此我们建议您不要退回网络设备 SNMP 报告中显示的端口。

## 当未找到 IP 地址或 MAC 地址时 ANC 操作失败

当终端的活动会话不包含关于 IP 地址的信息时，在该终端上执行的 ANC 操作会失败。对于该终端的 MAC 地址和会话 ID，也存在这种情况。



注释 如果要通过 ANC 更改终端的授权状态时，则必须提供该终端的 IP 地址或 MAC 地址。如果在终端的活动会话中无法找到 IP 地址或 MAC 地址，则会看到以下错误消息：

```
未找到此 MAC 地址、IP 地址或会话 ID 的活动会话 (No active session found for this MAC address, IP Address or Session ID)
```

。

## 通过外部身份验证的管理员无法执行 ANC 操作

如果通过外部身份验证的管理员尝试从实时会话发出 CoA 隔离，Cisco ISE 会返回以下错误消息：

```
CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated. (Cause:User not found internally. Possible use of unsupported externally authenticated user
```

如果通过外部身份验证的管理员使用终端的 IP 地址或 MAC 地址执行 ANC 操作（从操作 (Operations)），则 Cisco ISE 会显示以下错误消息：

```
Server failure: User not found internally. Possible use of unsupported externally authenticated user
```

## 备份数据类型

Cisco ISE 允许您从主 PAN 和从监控节点备份数据。可以从 CLI 或用户界面完成备份。

Cisco ISE 允许您备份以下类型的数据：

- 配置数据 - 包含应用特定和Cisco ADE 操作系统配置数据。备份可以使用 GUI 或 CLI 通过主 PAN 完成。
- 运行数据 - 包含监控和故障排除数据。备份可以通过主 PAN GUI 或使用监控节点的 CLI 来完成。

当Cisco ISE 在 VMware 上运行时，不支持用 VMware 快照备份 ISE 数据。



**注释** VMware 快照用于保存 VM 在给定时间点的状态，因此Cisco ISE 不支持使用 VMware 快照备份 ISE 数据。在多节点Cisco ISE 部署中，所有节点中的数据都与当前数据库信息保持同步。恢复快照可能会导致数据库复制和同步问题。建议您使用Cisco ISE 中包含的备份功能来存档和恢复数据。

使用 VMware 快照或任何第三方备份服务备份Cisco ISE 数据可能会导致Cisco ISE 服务中断。当 VMware 或任何其他第三方备份服务（如 CommVault SAN 级别备份）启动备份时，它会暂停文件系统以保持崩溃一致性，这可能会导致Cisco ISE 功能冻结。您需要重启才能恢复Cisco ISE 部署上的服务。

可以使用更低版本的Cisco ISE 的备份文件执行恢复操作并且可以在更高版本上执行恢复操作。例如，如果您拥有来自Cisco ISE 版本 1.3 或 1.4 的 ISE 节点的备份，您可以在Cisco ISE 版本 2.1 上恢复该备份。

Cisco ISE 版本 2.7 支持从版本 2.2 及更高版本获取的备份恢复。

## 备份和恢复存储库

Cisco ISE 允许您通过管理员门户创建和删除存储库。您可以创建以下类型的存储库：

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS



**注释** 存储库位于每台设备本地位置。

建议对于所有类型的部署（小型、中型和大型），创建最低 100 GB 大小的存储库。



下表显示了Cisco ISE 操作与外部存储库类型之间的可支持性信息：

表 1: 外部存储库的可支持性表格

存储库类型	配置备份	配置恢复	升级	操作备份	运行恢复	支持捆绑包	从用户界面验证	从用户界面导出报告	从用户界面导出策略
<b>FTP</b>	√	√	√	√	√	√	√	√	√
<b>SFTP</b>	√	√	√	√	√	√	√	√	√
<b>TFTP</b>	√	√	√	√	√	√	X	√	√
<b>HTTP</b>	X	X	√	X	X	X	X	X	X
<b>HTTPS</b>	X	X	√	X	X	X	X	X	X
<b>NFS</b>	√	√	√	√	√	√	√	√	√

## 创建存储库

可以使用 CLI 和 GUI 创建存储库。由于以下原因，我们建议您使用 GUI：

- 通过 CLI 创建的存储库保存在本地且不会被复制到其他部署节点。这些存储库不会列于 GUI 的存储库页面。
- 在主 PAN 创建的存储库会被复制到其他部署节点。

在 GUI 中，密钥仅在主 PAN 上生成，因此在升级期间，需要新的主管理节点的 GUI 中再次生成密钥，并将其导出到 SFTP 服务器。如果从部署中删除节点，需要在非管理节点的 GUI 中生成密钥，并将其导出到 SFTP 服务器。

可以在 Cisco ISE 中凭借 RSA 公共密钥身份验证配置 SFTP 存储库。您可以选择使用安全密钥的 RSA 公共密钥身份验证来加密数据库和日志，而不必使用管理员创建的密码。对于通过 RSA 公共密钥创建的 SFTP 存储库，在 GUI 中创建的存储库不会在 CLI 中复制，在 CLI 中创建的存储库也不会 GUI 中复制。要在 CLI 和 GUI 中配置相同存储库，请在 CLI 和 GUI 中生成 RSA 公共密钥，并将密钥输出到 SFTP 服务器。

### 开始之前

- 必须具有超级管理员或系统管理员权限才能执行以下任务。
- 如果要使用 RSA 公共密钥身份验证创建 SFTP 存储库，请执行以下步骤：
  - 在 SFTP 存储库中启用 RSA 公共密钥身份验证。
  - 从 Cisco ISE CLI 使用 **crypto host\_key add** 命令输入 SFTP 服务器的主机密钥。主机密钥字符串应当与您在存储库配置页面的路径 (**Path**) 字段中输入的主机名匹配。

- 生成密钥对，并从 GUI 将公共密钥导出到您的本地系统。在 Cisco ISE CLI 中，使用 **crypto key generate rsa passphrase test123** 命令生成密钥对，其中 **passphrase** 必须超过四个字母，然后将密钥导出到任何存储库（本地磁盘或任何其他配置的存储库）。
- 将导出的 RSA 公共密钥复制到启用 PKI 的 SFTP 服务器并将其添加到 “authorized\_keys” 文件。

**步骤 1** 依次选择 **管理 (Administration)** > **系统 (System)** > **维护 (Maintenance)** > **存储库 (Repository)**。

**步骤 2** 在思科 ISE GUI 中，点击 **菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **维护 (Maintenance)** > **存储库 (Repository)**。

**步骤 3** 点击 **添加 (Add)** 以添加新存储库。

**步骤 4** 根据需要输入值以设置新存储库。请参阅 [存储库设置](#)，第 10 页 以了解字段说明：

**步骤 5** 点击 **提交 (Submit)** 以创建存储库。

**步骤 6** 通过点击左侧 **操作 (Operations)** 导航窗格中的 **存储库 (Repository)** 来验证是否成功创建存储库，或点击 **存储库 (Repository)** 窗口顶部的 **存储库列表 (Repository List)** 链接以转至存储库列表页面。

### 下一步做什么

- 确保已创建的存储库有效。可以从 **存储库列表 (Repository listing)** 窗口执行此操作。选择对应存储库并点击 **验证 (Validate)**。或者，您可以从 Cisco ISE 命令行界面执行以下命令：

```
show repository repository_name
```

其中 *repository\_name* 是已创建的存储库的名称。



**注 释** 如果在创建存储库时提供的路径不存在，则会遇到以下错误：

```
%Invalid Directory
```

- 运行按需备份或安排备份。

## 存储库设置

下表介绍了 **存储库列表 (Repository List)** 页面上的字段，可以使用此页面创建存储备份文件的存储库。要查看此处窗口，请点击 **菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **维护 (Maintenance)** > **存储库 (Repository)**。

表 2: 存储库设置

字段	使用指南
存储库 (Repository)	输入存储库的名称。允许使用字母数字字符，最大长度为 80 个字符。
协议 (Protocol)	从可用协议中选择一个您想要使用的协议。
服务器名称 (Server Name)	<p>(对于 TFTP、HTTP、HTTPS、FTP、SFTP 和 NFS 为必填字段) 输入您想要在其上创建存储库的服务器的主机名或 IP 地址 (IPv4 或 IPv6)。</p> <p><b>注释</b> 如果要添加使用 IPv6 地址的存储库，请确保 ISE eth0 接口配置了 IPv6 地址。</p>
路径 (Path)	<p>输入存储库的路径。此路径必须有效而且在您创建数据库时必须存在。</p> <p>此值可以用双前斜杠 (//) 或单前斜杠 (/) 开头，表示服务器的根目录。但是，对于 FTP 协议，单前斜杠 (/) 表示 FTP 的本地设备主目录，而不是根目录。</p>
启用 PKI 身份验证 (Enable PKI authentication)	(可选；仅适用于 SFTP 存储库) 如果要在 SFTP 存储库中启用 RSA 公钥身份验证，请选中此复选框。
用户名 (User Name)	(对于 FTP、SFTP 为必填字段) 输入对指定服务器拥有写入权限的用户名。只允许使用字母数字字符。
密码 (Password)	(对于 FTP、SFTP 为必填字段) 输入用于访问指定服务器的密码。密码可以包含以下字符： 0-9、a-z、A-Z、-、.、 、@、#、\$、%、^、&、*、(、)、+、和 =。

## 相关主题

[备份和恢复存储库](#)，第 8 页

[创建存储库](#)，第 9 页

## 在 SFTP 存储库中启用 RSA 公共密钥身份验证

在 SFTP 服务器中，每个节点必须具有两个 RSA 公共密钥，一个用于 CLI，一个用于 GUI。要在 SFTP 存储库中启用 RSA 公共密钥身份验证，请执行以下步骤：

**步骤 1** 用有权限编辑 `/etc/ssh/sshd_config` 的帐户登录 SFTP 服务器。

注释 `sshd_config` 文件的位置可能根据操作系统安装而有所不同。

步骤 2 输入 `vi /etc/ssh/sshd_config` 命令。

系统列出 `sshd_config` 文件的内容。

步骤 3 从以下行中删除“#”符号以启用 RSA 公共密钥身份验证：

- `RSAAuthentication` 是
- `PubkeyAuthentication` 是

注释 如果公共身份验证密钥为“否”(No)，则将其更改为“是”(Yes)。

- `AuthorizedKeysFile` `~/.ssh/authorized_keys`

---

## 按需备份和计划备份

您可以配置主 PAN 和主监控节点的按需备份。当您希望立即备份数据时，系统会执行按需备份。

您可以安排一次性、每日、每周或每月运行系统级备份。由于备份操作持续时间较长，您可以将备份操作安排在空闲时间执行。您可以从管理门户安排备份。



---

注释 如果使用的是内部 CA，应使用 CLI 导出证书和密钥。在管理门户中使用的备份不会备份 CA 链。

有关详细信息，请参阅《思科身份服务引擎管理员指南》的“基本设置”一章中的“导出思科 ISE CA 证书和密钥”部分。

---

相关主题

[维护设置](#)

## 执行按需备份

可以执行按需备份以立即备份配置或监控（操作）数据。恢复操作可将 Cisco ISE 恢复到获取备份时的配置状态。

**重要事项**

当执行备份和恢复时，恢复功能会使用源系统中的证书列表覆盖目标系统上的受信任证书列表。需要注意的是，备份和恢复功能不包括与内部证书颁发机构(CA)证书关联的私钥，这一点至关重要。

如果要执行备份并从一个系统恢复到另一个系统，则必须选择以下选项之一以避免错误：

**• 选项 1:**

通过 CLI 从源 ISE 节点导出 CA 证书并将其导入到目标系统。

**优点：**从源系统向终端颁发的所有证书将继续受信任。由目标系统颁发的所有新证书将由同一密钥签名。

**缺点：**在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

**• 选项 2:**

在恢复过程之后，为内部 CA 生成所有新证书。

**优点：**推荐采用此选项，这是一种较为安全的方法，其中将使用原始源证书或原始目标证书。由原始源系统颁发的证书将继续受信任。

**缺点：**在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

**开始之前**

- 在执行按需备份之前，应对Cisco ISE 中的备份数据类型有基本的了解。
- 确保已创建存储备份文件的存储库。
- 不要使用本地存储库进行备份。您无法在远程监控节点的本地存储库中备份监控数据。
- 确保在获取备份之前执行所有证书相关的更改。
- 要执行以下任务，您必须是超级管理员或系统管理员。

**注  
释**

对于备份和恢复操作，系统不支持以下存储库类型：CD-ROM、HTTP、HTTPS 或 TFTP。这是因为，这些存储库类型为只读或者协议不支持文件列表。要恢复备份，请选择存储库，然后点击恢复 (**Restore**)。

**步骤 1** 选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup and Restore)**。

**步骤 2** 在思科 ISE GUI 中，点击菜单 (**Menu**) 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup and Restore)**。

**步骤 3** 选择备份类型：“配置” (Configuration) 或 “运行” (Operational)。

**步骤 4** 点击立即备份 (**Backup Now**)。

**步骤 5** 根据需要输入值以执行备份。

**步骤 6** 点击 **备份 (Backup)**。

**步骤 7** 验证备份是否成功完成。

Cisco ISE 在备份文件名中附加时间戳并将文件存储在指定存储库中。除了时间戳外，Cisco ISE 会为配置备份添加 CFG 标签，为运行备份添加 OPS 标签。确保备份文件位于指定的存储库中。

在分布式部署中，不要在备份运行时更改节点角色或升级节点。如果并发运行备份，则更改节点角色不会关闭所有进程，并可能导致数据不一致。在进行任何节点角色更改之前，请等待备份完成。

备份正在运行时，请勿升级节点。如果并发运行备份，这将关闭所有进程并可能导致数据不一致。在进行任何节点更改之前，请等待备份完成。

**注释** 备份正在运行时，可能会看到 CPU 使用率高并收到平均负载高的警报。备份完成时，CPU 使用率将恢复正常。

#### 相关主题

[思科 ISE 恢复操作](#)，第 18 页

[导出身份验证和授权策略配置](#)，第 24 页

## 按需备份设置

下表介绍**按需备份 (On-Demand Backup)** 窗口上的字段，您可以随时使用此窗口获取备份。要查看此处窗口，请点击菜单 (Menu) 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup & Restore)**。

表 3: 按需备份设置

字段名称	使用指南
类型	选择以下其中一个选项： <ul style="list-style-type: none"> <li>• <b>配置数据备份 (Configuration Data Backup):</b> 包含应用特定配置数据和 Cisco ADE 操作系统配置数据</li> <li>• <b>运行数据备份 (Operational Data Backup):</b> 包含监控和故障排除数据</li> </ul>
备份名称 (Backup Name)	输入备份文件的名称。
存储库名称 (Repository Name)	应该保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
加密密钥 (Encryption Key)	此密钥用于加密和解密备份文件。

### 相关主题

- [备份数据类型](#)，第 7 页
- [按需备份和计划备份](#)，第 12 页
- [备份历史记录](#)，第 17 页
- [备份失败](#)，第 17 页
- [思科 ISE 恢复操作](#)，第 18 页
- [导出身份验证和授权策略配置](#)，第 24 页
- [在分布式环境中同步主节点和辅助节点](#)，第 25 页
- [执行按需备份](#)，第 12 页

## 计划备份

可以执行按需备份以立即备份配置或监控（操作）数据。恢复操作可将Cisco ISE 恢复到获取备份时的配置状态。



### 重要事项

当执行备份和恢复时，恢复功能会使用源系统中的证书列表覆盖目标系统上的受信任证书列表。需要注意的是，备份和恢复功能不包括与内部证书颁发机构 (CA) 证书关联的私钥，这一点至关重要。

如果要执行备份并从一个系统恢复到另一个系统，则必须选择以下选项之一以避免错误：

#### • 选项 1:

通过 CLI 从源 ISE 节点导出 CA 证书并将其导入到目标系统。

**优点：**从源系统向终端颁发的所有证书将继续受信任。由目标系统颁发的所有新证书将由同一密钥签名。

**缺点：**在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

#### • 选项 2:

在恢复过程之后，为内部 CA 生成所有新证书。

**优点：**推荐采用此选项，这是一种较为安全的方法，其中将使用原始源证书或原始目标证书。由原始源系统颁发的证书将继续受信任。

**缺点：**在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

### 开始之前

- 在安排备份之前，应对Cisco ISE 中的备份数据类型有基本的了解。
- 确保已配置存储库。
- 不要使用本地存储库进行备份。您无法在远程监控节点的本地存储库中备份监控数据。
- 要执行以下任务，您必须是超级管理员或系统管理员。

- 如果已从Cisco ISE 1.1 或更低版本升级到Cisco ISE 1.2，应当重新配置已计划的备份。请参见《思科身份服务引擎升级指南》版本 1.2 “已知升级问题”一节。



**注释** 对于备份和恢复操作，系统不支持以下存储库类型：CD-ROM、HTTP、HTTPS 或 TFTP。这是因为，这些存储库类型为只读或者协议不支持文件列表。

## 计划备份设置

下表介绍“定期备份”(Scheduled Backup)窗口上的字段，您可以使用此窗口恢复完整备份或增量备份。要查看此处窗口，请点击菜单(Menu)图标(☰)，然后选择管理(Administration) > 系统(System) > 备份和恢复(Backup and Restore)。

表 4: 计划备份设置

字段名称	使用指南
类型 (Type)	选择以下其中一个选项： <ul style="list-style-type: none"> <li>• <b>配置数据备份 (Configuration Data Backup):</b> 包含应用特定配置数据和Cisco ADE 操作系统配置数据</li> <li>• <b>运行数据备份 (Operational Data Backup):</b> 包含监控和故障排除数据</li> </ul>
名称 (Name)	输入备份文件的名称。您可以输入您所选的描述性名称。Cisco ISE 会将时间戳附加到备份文件名之后并将其存储在存储库中。即使您配置了一系列备份，也要有唯一的备份文件名。在“定期备份”(Scheduled Backup)列表窗口上，备份文件名前面将附加“backup_occur”，表示文件是一次 <b>kron</b> 作业。
说明	输入对备份的说明。
存储库名称 (Repository Name)	选择保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
加密密钥 (Encryption Key)	输入用于加密和解密备份文件的密钥。
计划选项	选择计划备份的频率并相应地填写其他选项。

### 相关主题

[备份数据类型](#)，第 7 页



[按需备份和计划备份](#)，第 12 页  
[备份历史记录](#)，第 17 页  
[备份失败](#)，第 17 页  
[思科 ISE 恢复操作](#)，第 18 页  
[导出身份验证和授权策略配置](#)，第 24 页  
[在分布式环境中同步主节点和辅助节点](#)，第 25 页  
[使用 CLI 备份](#)，第 17 页  
[计划备份](#)，第 15 页

## 使用 CLI 备份

虽然可以从 CLI 和 GUI 安排备份，但是建议使用 GUI。不过，只能从 CLI 对辅助监控节点执行操作备份。

## 备份历史记录

备份历史记录提供关于定时备份和按需备份的基本信息。它会列出备份名称、备份文件大小、存储备份的库以及指明获得备份的时间的时间戳。此信息在操作审核报告以及历史记录表的 **Backup and Restore** 页面上列出。

对于故障备份，Cisco ISE 将触发警报。备份历史记录页面提供故障原因。操作审核报告也引用故障原因。如果故障原因缺失或不清楚，您可以从 Cisco ISE CLI 运行 **backup-logs** 命令，查看 ADE.log 了解更多信息。

在备份操作运行的过程中，您可以使用 **show backup status** CLI 命令查看备份操作的进度。

备份历史记录与 Cisco ADE 操作系统配置数据一起存储。甚至在应用升级后历史记录依然存在，只有当您重置 PAN 映像时才能将历史记录删除。

## 备份失败

如果备份失败，请检查以下事宜：

- 检查是否存在任何 NTP 同步或服务失败问题。如果 Cisco ISE 上的 NTP 服务无效，Cisco ISE 将发出 NTP 服务失败警报。当 Cisco ISE 无法与所有配置的 NTP 服务器同步时，Cisco ISE 会发出 NTP 同步失败警报。如果 NTP 服务停止或有任何同步问题，Cisco ISE 备份可能会失败。检查“警报” (Alarms) Dashlet 并修复 NTP 同步或服务问题，然后再重试备份操作。
- 确保没有同时运行任何其他备份。
- 检查已配置存储库的可用磁盘空间。
  - 如果监控数据占用的空间超过所分配的监控数据库大小的 75%，则监控（操作）备份会失败。例如，如果向监控节点分配的空间为 600 GB，而监控数据占用超过 450 GB 的存储空间，则监控备份会失败。

- 如果数据库磁盘使用量超过 90%，系统会执行清除操作，使数据库的大小小于或等于所分配空间的 75%。
- 验证是否正在进行清除。进行清除时，备份和恢复操作不起作用。
- 验证存储库的配置是否正确。

## 思科 ISE 恢复操作

可以在主管理节点或独立管理节点上恢复配置数据。在主 PAN 上恢复数据后，必须手动将辅助节点与主 PAN 同步。

恢复运营数据的过程根据部署类型而异。



**注释** Cisco ISE 中新的备份/恢复用户界面利用备份文件名中的元数据。因此，在备份完成后，不应手动修改备份文件名。如果手动修改备份文件名，则 Cisco ISE 备份/恢复用户界面将无法识别备份文件。如果必须修改备份文件名，应使用 Cisco ISE CLI 恢复备份。

## 数据恢复指南

下面提供了恢复 Cisco ISE 备份数据时应遵守的指南。

- 利用 Cisco ISE，您可以从 ISE 节点 (A) 获取备份并将其存储到另一个 ISE 节点 (B) 上，这两个节点有相同的主机名（但 IP 地址不同）。但是，当您在节点 B 上恢复备份后，不会更改节点 B 的主机名，因为这样做可能会导致证书和门户组标记出现问题。
- 如果在一个时区内从主 PAN 获取备份，并尝试在另一时区中的另一个 Cisco ISE 节点上恢复该备份，恢复过程可能失败。如果备份文件中的时间戳晚于恢复备份所在的 Cisco ISE 节点上的系统时间，则会发生此故障。如果在获得备份之后一天恢复备份，那么备份文件中的时间戳则为过去时间，恢复过程将成功。
- 当主 PAN 上恢复的备份所使用的主机名不同于获得备份的主机名时，此主 PAN 将成为独立节点。部署已损坏，辅节点将无法运行。您必须使独立节点成为主节点，重置辅节点上的配置，并在主节点上重新注册这些辅节点。要重置 Cisco ISE 节点上的配置，请从 Cisco ISE CLI 输入以下命令：
  - **application reset-config ise**
- 建议您在初始 Cisco ISE 安装和设置之后，不要更改系统时区。
- 如果更改了部署中的一个或多个节点上的证书配置，则必须获得另一个备份才能从独立 Cisco ISE 节点或主 PAN 恢复数据。否则，如果您尝试使用旧备份恢复数据，节点之间的通信可能失败。
- 在主 PAN 上恢复配置备份后，可以导入先前导出的 Cisco ISE CA 证书和密钥。



**注 释** 如果没有导出思科 ISE CA 证书和密钥，则在主 PAN 上恢复配置备份后，在主 PAN 和策略服务节点 (PSN) 上生成根 CA 和从属 CA。

- 如果尝试恢复白金级数据库而没有使用正确的 FQDN（白金级数据库的 FQDN），则需要重新生成 CA 证书。（要查看此处窗口，请点击菜单 (Menu) 图标 (≡)，然后选择 **管理 (Administration) > 证书 (Certificates) > 证书签名请求 (Certificate Signing Requests) > 更换 ISE 根 CA 证书链 (Replace ISE Root CA certificate chain)**）。不过，如果使用正确的 FQDN 恢复白金级数据库，请注意 CA 证书将自动重新注册。
- 需要一个数据存储库，供 Cisco ISE 保存备份文件。您必须创建一个存储库，然后才能运行按需备份或定期备份。
- 如果有一个独立管理节点发生故障，则必须运行配置备份进行恢复。如果主 PAN 发生故障，则可以使用分布式设置，将辅助管理节点升级为主管理节点。实现之后，可以在主 PAN 上恢复数据。



**注 释** 思科 ISE 还提供 **backup-logs** CLI 命令，可用来收集日志和配置文件以用于故障排除。

## 从 CLI 恢复配置或监控（操作）备份

要通过 Cisco ISE CLI 恢复配置数据，请在 EXEC 模式下使用 **restore** 命令。使用以下命令从配置或操作备份恢复数据：

**restore filename repository repository-name encryption-key hash|plain encryption-key name include-adeos**

语法说明

<b>restore</b>	键入此命令，从配置或操作备份恢复数据。
<i>filename</i>	驻留在存储库的备份文件的名称。最多支持 120 个字母数字字符。  <b>注 释</b> 必须在文件名后面添加 .tar.gpg 扩展名（例如，myfile.tar.gpg）。
<b>repository</b>	指定包含备份的存储库。
<i>repository-name</i>	您想要从其恢复备份的存储库的名称。
<b>encryption-key</b>	（可选）指定用户定义的加密密钥以恢复备份。

<b>hash</b>	恢复备份的散列加密密钥。指定跟随的加密（散列）加密密钥。最多支持 40 个字符。
<b>plain</b>	用于恢复备份的明文加密密钥。指定跟随的未加密明文加密密钥。最多支持 15 个字符。
<i>encryption-key name</i>	输入加密密钥。
<b>include-adeos</b>	（可选，仅适用于配置备份）如果您想要从配置备份恢复 ADE-OS 配置，请输入此命令运算符参数。当您恢复配置备份，如果不包含此参数，Cisco ISE 仅恢复 Cisco ISE 应用配置数据。

### 默认值

无默认行为或值。

### 命令模式

EXEC

### 使用指南

在 Cisco ISE 中使用 `restore` 命令时，Cisco ISE 服务器会自动重新启动。

恢复数据时，加密密钥为可选。要在您未提供加密密钥的情况下，支持恢复更早的备份，您可以使用 `restore` 命令，无需加密密钥。

### 示例

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key
plain Lab12345 恢复操作可能需要重新启动应用服务。(Restore may require a restart of application
services.) Continue? (是/否) [是]? 是 正启动恢复。(yes/no) [yes] ? yes Initiating restore.)
请稍候... ISE 应用恢复正在进行。(ISE application restore is in progress.) This process could
take several minutes. Please wait... Stopping ISE Application Server... Stopping ISE
Monitoring & Troubleshooting Log Processor... 正停止 ISE 监控并排查日志收集器...(Stopping ISE
Monitoring & Troubleshooting Log Collector...) 正停止 ISE 监控并排查警报进程...(Stopping ISE
Monitoring & Troubleshooting Alert Process...) 正停止 ISE 监控并排查会话数据库...(Stopping ISE
Monitoring & Troubleshooting Session Database...) Stopping ISE Database processes... 正启动
ISE 数据库进程...(Starting ISE Database processes...) 正启动 ISE 监控和排查会话数据库...(Starting
ISE Monitoring & Troubleshooting Session Database...) 正启动 ISE 应用服务器...(Starting ISE
Application Server...) 正启动 ISE 监控并排查警报进程...(Starting ISE Monitoring & Troubleshooting
Alert Process...) 正启动 ISE 监控并排查日志收集器...(Starting ISE Monitoring & Troubleshooting
Log Collector...) 正启动 ISE 监控并排查日志处理器...(Starting ISE Monitoring & Troubleshooting
Log Processor...) Note: ISE Processes are initializing. 使用“show application status ise” CLI
可确认所有进程全部处于运行状态。ise/admin#
```

### 相关命令

	说明
<b>backup</b>	执行备份（Cisco ISE 和 Cisco ADE OS），并将备份放在存储库中。
<b>backup-logs</b>	备份系统日志。
<b>repository</b>	输入备份配置的存储库子模式。
<b>show repository</b>	显示位于特定存储库上的可用备份文件。
<b>show backup history</b>	显示系统的备份历史记录。
<b>show backup status</b>	显示备份操作的状态。
<b>show restore status</b>	显示恢复操作的状态。

如果任何辅助节点的应用恢复后同步状态和复制状态为 不同步 (*Out of Sync*)，则必须将此辅助节点的证书重新导入主 PAN，执行手动同步。

## 从 GUI 恢复配置备份

可以从管理门户恢复配置备份。GUI 只列出从当前版本提取的备份。要恢复此版本之前的备份，请从 CLI 使用恢复命令。

### 开始之前

确保主 PAN 自动故障转移配置（如果已在部署中启用）已关闭。当恢复备份配置时，应用服务器进程会重新启动。这些服务重新启动时可能会出现延迟。由于服务重新启动时出现这种延迟，可能会触发辅助 PAN 的自动故障转移。

在配置备份期间，如果您的部署是双节点部署，请确保满足以下条件：

- 如果用于恢复的源节点和目标节点与用于配置备份的相应节点相同，目标节点可以是独立节点或主节点。
- 如果用于恢复的源节点和目标节点与用于配置备份的相应节点不同，目标节点必须是独立节点。



**注释** 可以仅在主 PAN 上恢复配置数据库备份和重新生成根 CA。不过，无法恢复注册 PAN 上的配置数据库备份。

**步骤 1** 选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup and Restore)**。

**步骤 2** 在思科 ISE GUI 中，点击 **菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup and Restore)**。

**步骤 3** 从配置备份列表中选择备份名称，然后点击 **Restore**。

**步骤 4** 输入在备份过程中使用的加密密钥。

**步骤 5** 点击恢复 (**Restore**)。

---

### 下一步做什么

如果使用Cisco ISE CA 服务，必须：

1. 重新生成整个Cisco ISE CA 根链。
2. 从主 PAN 获取Cisco ISE CA 证书和密钥的备份，然后在辅助 PAN 上恢复备份。这样确保了辅助 PAN 可以在主 PAN 故障时用作外部 PKI 的根 CA 或从属 CA，您可将辅助 PAN 升级为主 PAN。

## 恢复监控数据库

恢复监控数据库的流程因部署类型不同而异。以下各节介绍如何在独立和分布式部署中恢复监控数据库。

必须使用 CLI 从Cisco ISE 的先前版本恢复按需监控数据库备份。不支持跨Cisco ISE 版本恢复定期备份。



---

**注释** 如果尝试将数据恢复到调取数据所在节点以外的节点，必须将日志记录目标设置配置为指向新节点。这可以确保监控系统日志发送到正确节点。

---

### 在独立环境中恢复监控（运行）备份

GUI 只列出从当前版本提取的备份。要恢复从早期版本获取的备份，请从 CLI 使用恢复命令。

#### 开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

---

**步骤 1** 选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup and Restore)**。

**步骤 2** 在思科 ISE GUI 中，点击菜单 (**Menu**) 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup and Restore)**。

**步骤 3** 从操作备份列表中选择备份的名称，然后点击恢复 (**Restore**)。

**步骤 4** 输入在备份过程中使用的加密密钥。

**步骤 5** 点击恢复。

---

## 通过管理和监控角色恢复监控备份

您可以使用管理和监控角色在分布式环境中恢复监控备份。

### 开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

---

**步骤 1** 如果使用的是主 PAN 和辅助 PAN，请同步 PAN。

同步 PAN 时，必须选择一个 PAN 并将其升级为活动的主 PAN。

**步骤 2** 在注销监控节点之前，应将监控角色分配给部署中的其他节点。

每个部署必须至少有一个正常运行的监控节点。

**步骤 3** 注销监控节点以进行备份。

**步骤 4** 将监控备份恢复到最近注销的节点。

**步骤 5** 向当前管理节点注册新恢复的节点。

**步骤 6** 将新恢复和注册的节点升级为主用监控节点。

---

## 通过监控角色恢复监控备份

只能通过监控角色恢复分布式环境中的监控备份。

### 开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

---

**步骤 1** 准备取消注册要恢复的节点。这是通过将监控角色分配给部署中的另一个节点来完成的。

部署必须至少有一个正常运行的监控节点。

**步骤 2** 取消注册要恢复的节点。

**注释** 请等待，直到取消注册完成后，再继续执行恢复操作。该节点必须处于独立状态，然后您才能继续执行恢复操作。

**步骤 3** 将监控备份恢复到最近取消注册的节点。

**步骤 4** 向当前管理节点注册新恢复的节点。

**步骤 5** 将新恢复和注册的节点升级为 PAN。

---

## 恢复历史记录

可以从操作审核报告 (Operations Audit Report) 中获取所有恢复操作、日志事件和状态的相关信息。



**注释** 但是，操作审核报告 (Operations Audit Report) 窗口不提供与之前的恢复操作对应的起始时间信息。

要获得故障排除信息，必须从Cisco ISE CLI 运行 **backup-logs** 命令并查看 ADE.log 文件。

在恢复操作进行过程中，所有Cisco ISE 服务都会停止。您可以使用 **show restore status** CLI 命令查看恢复操作的进度。

## 导出身份验证和授权策略配置

您可以将身份验证和授权策略配置导出为 XML 文件，您可以离线阅读此文件以识别任何配置错误并用于故障排除。此 XML 文件包括身份验证和授权策略规则、简单和复合策略条件、自主访问控制列表 (dACL) 和授权配置文件。您可以选择以邮件方式发送 XML 文件或将其保存在本地系统中。

**步骤 1** 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup & Restore)**。

**步骤 2** 点击策略导出 (Policy Export)。

**步骤 3** 根据需要输入值。

**步骤 4** 点击导出 (Export)。

使用文本编辑器，例如 WordPad，查看 XML 文件的内容。

## 计划策略导出设置

下表对计划策略导出 (Schedule Policy Export) 窗口中的字段进行了说明。要查看此处窗口，请点击菜单 (Menu) 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup and Restore) > 策略导出 (Policy Export)**。

表 5: 计划策略导出设置

字段名称	使用指南
加密 (Encryption)	
加密密钥 (Encryption Key)	输入用于加密和解密导出数据的密钥。仅当您选择使用加密密钥导出 (Export with Encryption Key) 选项时，才会启用此字段。



字段名称	使用指南
<b>目标 (Destination)</b>	
<b>下载文件到本地计算机 (Download file to local computer)</b>	可以让您将策略导出文件下载到本地系统。
<b>通过邮件将文件发送到 (Email file to)</b>	您可输入多个邮件地址，用逗号分隔。
<b>存储库 (Repository)</b>	选择要将策略数据导出到的存储库。无法在此处输入存储库名称。只能从下拉列表选择一个可用存储库。确保在计划策略导出之前创建存储库。
<b>立即导出 (Export Now)</b>	点击此选项可将数据导出到本地计算机或作为电子邮件附件发送。您无法导出到存储库；只能计划存储库导出。
<b>时间表 (Schedule)</b>	
<b>计划选项</b>	选择导出计划的频率，并相应地输入其他详细信息。

## 在分布式环境中同步主节点和辅助节点

在分布式环境中，在 PAN 上恢复备份文件之后，主节点和辅助节点中的 Cisco ISE 数据库有时不会自动同步。如果发生这种情况，可以手动强制从 PAN 完全复制到辅助 ISE 节点。只能强制从 PAN 同步到辅助节点。在同步操作过程中，无法进行任何配置更改。通过 Cisco ISE，只能在同步完成后导航至其他 Cisco ISE 管理员门户页面和进行配置更改。

### 开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

**步骤 1** 选择 **管理 (Administration) > 系统 (System) > 部署 (Deployment)**。

**步骤 2** 在思科 ISE GUI 中，点击 **菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup & Restore)**。

**步骤 3** 选中处于不同步复制状态的辅助 ISE 节点旁边的复选框。

**步骤 4** 点击 **同步 (Syncup)**，等到节点与 PAN 同步。必须等到此流程完成，然后才能再次访问 Cisco ISE 管理员门户。

## 恢复独立和分布式部署中断开的节点

此部分提供可用于恢复独立和分布式部署中断开的节点的故障排除信息。以下某些用例使用备份和恢复功能，而其他用例则使用复制功能恢复已丢失的数据。

## 使用现有 IP 地址和主机名恢复分布式部署中断开的节点

### 场景

在分布式部署中，一场自然灾害导致丢失了所有节点。在恢复之后，您想要使用现有 IP 地址和主机名。

例如，您有两个节点：N1（主策略管理节点，即主 PAN）和 N2（辅助策略管理节点，即辅助 PAN）。可提供在时间 T1 执行的 N1 节点的备份。后来，由于自然灾害，N1 和 N2 节点都出现了故障。

### 假定条件

部署中的所有 Cisco ISE 节点都已被破坏。已使用相同的主机名和 IP 地址对新硬件进行映像。

### 解决步骤

1. 您必须更换 N1 和 N2 节点。N1 和 N2 节点现在具有独立配置。
2. 用 N1 和 N2 节点的 UDI 获取许可证并将其安装在 N1 节点上。
3. 然后，您必须在更换的 N1 节点上恢复备份。恢复脚本将尝试在 N2 上同步数据，但是，N2 现已成为独立节点，所以同步失败。N1 上的数据将重置至时间 T1。
4. 您必须登录 N1 Admin 门户以删除和重新注册 N2 节点。N1 和 N2 节点都将使数据重置至时间 T1。

## 在分布式部署中使用新 IP 地址和主机名恢复丢失的节点

### 场景

在分布式部署中，一场自然灾害导致丢失了所有节点。新硬件在新位置进行了重新镜像并且需要新的 IP 地址和主机名。

例如，您有两个 ISE 节点：N1（主策略管理节点，即主 PAN）和 N2（辅助策略服务节点）。系统可提供在时间 T1 执行的 N1 节点备份。后来，由于自然灾害，N1 和 N2 节点都出现了故障。Cisco ISE 节点在新位置被替换，新主机名为 N1A（主 PAN）和 N2A（辅助策略服务节点）。此处 N1A 和 N2A 都是独立节点。

### 假定条件

部署中的所有 Cisco ISE 节点都已被破坏。新硬件已使用不同的主机名和 IP 地址在另一位置进行镜像。

### 解决步骤

1. 获取 N1 备份并在 N1A 上恢复此备份。恢复脚本将识别主机名更改和域名更改，并且将根据当前主机名在部署配置中更新主机名和域名。
2. 您必须生成新的自签证书。

3. 您必须登录到 N1A 上的 Cisco ISE 管理员门户。在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 管理 (Administration) > 系统 (System) > 部署 (Deployment)，然后执行以下操作：

删除旧 N2 节点。

将新 N2A 节点注册为辅助节点。系统会将 N1A 节点的数据复制到 N2A 节点。

## 使用现有 IP 地址和主机名恢复独立部署中的节点

### 场景

独立管理节点出现故障。

例如，您有一个独立管理节点 N1。已在时间 T1 执行 N1 数据库的备份。N1 节点由于物理故障宕机，必须重置映像此节点或需要使用新的硬件。必须以相同的 IP 地址和主机名恢复 N1 节点。

### 假定条件

此部署是独立部署，而且新硬件或重置映像的硬件具有相同的 IP 地址和主机名。

### 解决步骤

N1 节点在重置映像或您采用具有相同 IP 地址和主机名的新 Cisco ISE 节点后开始运行时，您必须从旧 N1 节点恢复备份。您无需执行任何角色变更。

## 使用新 IP 地址和主机名恢复独立部署中的节点

### 场景

独立管理节点出现故障。

例如，您有一个独立管理节点 N1。系统可以提供在时间 T1 执行的 N1 数据库备份。N1 节点由于物理故障而宕机，此节点更换为另一位置具有不同 IP 地址和主机名的新硬件。

### 假定条件

这是独立部署，并且所更换的硬件具有不同的 IP 地址和主机名。

### 解决步骤

1. 使用新硬件更换 N1 节点。此节点将处于独立状态，主机名为 N1B。
2. 您可以在 N1B 节点恢复备份。不需要更改角色。

## 配置回滚

### 问题

有时候，您可能会不小心更改配置，然后您发现所做的更改不正确。例如，您可能会错误地删除几个 NAD 或修改一些 RADIUS 属性，然后在数小时后才发现问题。在这种情况下，可以通过恢复您在进行更改之前所做的备份，恢复原来的配置。

### 可能的原因

有两个节点：N1（主策略管理节点，即主 PAN）和 N2（辅助策略管理节点，即辅助 PAN），并且可提供 N1 节点的备份。您在 N1 节点上做了一些错误的配置更改并且想要撤消更改。

### 解决方案

获取在执行错误的配置更改之前所执行的 N1 节点备份。在 N1 节点上恢复此备份。恢复脚本会将数据从 N1 同步至 N2。

## 在分布式部署出现故障的情况下恢复主节点

### 场景

在多节点部署中，PAN 出现故障。

例如，您有两个 Cisco ISE 节点：N1 (PAN) 和 N2（辅助管理节点）。由于硬件问题，N1 出现了故障。

### 假定条件

仅分布式部署中的主节点出现故障。

### 解决步骤

1. 登录 N2 管理员门户。在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 部署 (Deployment)**，并将 N2 配置为主节点。

使用新硬件更换 N1 节点，重新镜像此节点并使之处于独立状态。

2. 从 N2 管理员门户，将新的 N1 节点注册为辅助节点。

现在，N2 节点就成为您的主要节点，而 N1 节点则成为您的辅助节点。

如果您希望重新将 N1 节点设置为主要节点，请登录 N1 Admin 门户并将其设置为主要节点。N2 就自动成为辅助服务器。不会有数据丢失。

## 在分布式部署出现故障的情况下恢复辅助节点

### 场景

在多节点部署中，一个辅助节点出现故障。无需恢复。

例如，具有多个节点：N1（主 PAN）、N2（辅助 PAN）、N3（辅助策略服务节点）、N4（辅助策略服务节点）。其中一个辅助节点 N3 出现故障。

### 解决步骤

1. 将新的 N3A 节点重新映像到默认独立状态。
2. 登录到 N1 管理门户并删除 N3 节点。
3. 重新注册 N3A 节点。

数据将从 N1 复制到 N3A。无需恢复。

## 思科 ISE 日志记录机制

Cisco ISE 提供用于审核、故障管理和故障排除的日志记录机制。日志记录机制可以帮助您识别所部署的服务中的故障情况并有效地对相应问题进行故障排除。它还以一致的方式从监控和故障排除主要节点提供日志记录输出。

您可以将 Cisco ISE 配置为使用虚拟环回地址在本地系统中收集日志。要从外部收集日志，您可以配置外部系统日志服务器，这些服务器称为目标。日志分为多个预定义的类别。您可以根据各个类别的目标、严重性级别等编辑各个类别，以自定义日志记录输出。

作为最佳实践，请勿将网络设备配置为 Cisco ISE 监控和故障排除 (MnT) 节点，因为这会导致一些网络访问设备 (NAD) 系统日志丢失，并使 MnT 服务器过载，进而导致加载问题。如果 NAD 系统日志配置为直接发送至 MnT，会话管理功能可能会中断。NAD 系统日志可定向到外部系统日志服务器以进行故障排除，但不应定向到 MnT。

当 ISE 消息服务在节点上失败时，将不再触发“进程已关闭” (Process Down) 警报。当 ISE 消息服务在节点上失败时，所有系统日志和“进程已关闭” (Process Down) 警报将丢失，直至消息服务在此节点上恢复。

在此情况下，管理员必须查找**队列链接错误 (Queue Link Error)** 警报，此警报将列在 Cisco ISE 主页 (**Home**) 窗口的**警报 (Alarms)** Dashlet 上。点击此警报，随即将打开包含**建议操作 (Suggested Actions)** 部分的新窗口。请遵循这些说明解决问题。



### 注释

如果将监控节点配置为网络设备的系统日志服务器，请确保日志记录源使用以下格式发送正确的网络访问服务器 (NAS) IP 地址：

```
<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>
```

否则，这可能会影响依赖 NAS IP 地址的功能。

## 配置系统日志清除设置

使用此流程可设置本地日志存储期，并可在一定时间后删除本地日志。

**步骤 1** 选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **本地日志设置 (Local Log Settings)**。

**步骤 2** 在思科 ISE GUI 中，点击菜单 (**Menu**) 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **本地日志设置 (Local Log Settings)**。

**步骤 3** 在 **Local Log Storage Period** 字段中，输入要将日志条目保留在配置源中的最大天数。

如果 localStore 文件夹达到 97 GB，则可能会早于配置的本地日志存储期 (**Local Log Storage Period**) 而删除日志。

**步骤 4** 点击 **Delete Logs Now** 可在存储期到期前的任何时间删除现有日志文件。

**步骤 5** 点击保存 (**Save**)。

## 思科 ISE 系统日志

在 Cisco ISE 中，日志记录目标的位置会收集系统日志。目标是指收集和存储日志的服务器的 IP 地址。您可以在本地生成和存储日志，也可以使用 FTP 工具将日志传输至外部服务器。Cisco ISE 具有以下默认目标，在本地系统的环回地址中会动态配置这些目标：

- LogCollector - 日志收集器的系统日志默认目标。
- ProfilerRadiusProbe - 分析器 RADIUS 探测功能的默认系统日志目标。

默认情况下，在执行全新 Cisco ISE 安装或升级期间会禁用 AAA 诊断子类别和系统诊断子类别日志记录目标，以减少磁盘空间。您可以为这些子类别手动配置日志记录目标，但这些子类别的本地日志记录始终处于启用状态。

您可以使用在 Cisco ISE 安装结束时在本地配置的默认日志记录目标，也可以创建外部目录来存储日志。



注释

如果在分布式部署中配置了系统日志服务器，系统日志消息会直接从进行身份验证的 PSN 发送到系统日志服务器，而不是从 MnT 节点发送。

相关主题

[思科 ISE 消息代码](#)，第 32 页

## 配置远程系统日志收集位置

您可以使用 Web 界面创建向其发送系统日志消息的远程系统日志服务器目标。日志消息根据系统日志协议标准被发送至远程系统日志服务器目标（请参阅 RFC-3164）。系统日志协议为非安全 UDP。

当发生某一事件时，系统会生成消息。事件可能是显示状态的事件，例如当存在某个程序时显示的消息，或报警。诸如内核、电子邮件和用户级别等多个设施会生成不同类型的事件消息。事件消息与严重性级别相关，它允许管理员过滤消息并将其进行优先级排序。数字代码被分配给该设备和严重性级别。系统日志服务器为事件消息收集器并从这些设施收集事件消息。管理员可以基于其严重性级别选择将消息转发至哪个事件消息收集器。

UDP 系统日志（日志收集器）是默认远程日志记录目标。当禁用此日志记录目标时，它不会再充当日志收集器，并且系统会将其从日志记录类别 (**Logging Categories**) 窗口中删除。当启用此日志记录目标时，它会成为日志记录类别 (**Logging Categories**) 窗口中的日志收集器。



**注释** 对默认远程日志记录目标 **SecureSyslogCollector** 的任何更改都会导致思科 ISE 监控和故障排除日志处理器服务重新启动。

**步骤 1** 在思科 ISE GUI 中，点击菜单 (**Menu**) 图标 (≡)，然后选择 **管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 远程日志记录目标 (Remote Logging Targets)**。

**步骤 2** 点击添加 (**Add**)。

**步骤 3** 输入必要的详细信息。

**步骤 4** 点击保存 (**Save**)。

**步骤 5** 转至 Remote Logging Targets 页面，然后验证新的目标是否创建。

然后，可以将日志记录目标映射到下面的每个日志记录类别。PSN 节点根据这些节点上启用的服务将相关日志发送到远程日志记录目标。

- AAA 审核
- AAA 诊断
- 记账
- 外部 MDM
- 被动 ID
- 终端安全评估和客户端调配审核
- 终端安全评估和客户端调配诊断
- Profiler

部署中的所有节点会将以下类别的日志发送到日志记录目标：

- 管理和操作审核
- 系统诊断
- 系统统计项

## 思科 ISE 消息代码

日志记录类别是用于说明功能、流程或用例的消息代码的捆绑包。在Cisco ISE 中，每条日志根据日志消息内容与日志记录类别所捆绑的消息代码相关联。日志记录类别帮助说明其包含的消息的内容。

日志记录类别可升级日志记录配置。每个类别具有可以根据应用要求进行设置的名称、目标和严重性级别。

Cisco ISE 为可以向其分配日志目标的 Posture、Profiler、Guest、AAA（身份验证、授权和记帐）等服务提供预定义日志记录类别。

对于日志记录类别通过的**身份验证 (Passed Authentications)**，默认情况下禁用允许本地日志记录的选项。启用此类别的本地日志记录将导致操作空间利用率高，并填写 `prrt-server.log` 与 `iseLocalStore.log`。


如果您选择为通过的**身份验证 (Passed Authentications)** 启用本地日志记录，请转至 **管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)**，从类别部分中点击通过的**身份验证 (Passed Authentications)**，然后选中本地日志记录 (**Local Logging**) 复选框。

### 相关主题


[设置消息代码的严重性级别](#)，第 32 页

## 设置消息代码的严重性级别

您可以设置日志严重性级别，选择存储所选类别的日志的日志记录目标。

- 
- 步骤 1** 在思科 ISE GUI 中，点击菜单 (**Menu**) 图标 ()，然后选择 **管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)**。
  - 步骤 2** 点击想要编辑的类别旁边的单选按钮，点击**编辑 (Edit)**。
  - 步骤 3** 修改必填字段值。
  - 步骤 4** 点击**保存 (Save)**。
  - 步骤 5** 转至“日志记录类别” (Logging Categories) 页面，验证对特定类别所做的配置更改。
- 

## 思科 ISE 消息目录

您可以使用“消息目录” (Message Catalog) 页面查看所有可能的日志消息和说明。在思科 ISE GUI 中，点击菜单 (**Menu**) 图标 ()，然后选择 **管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 消息目录 (Message Catalog)**。

系统将显示“日志消息目录” (Log Message Catalog) 页面，您可以在此查看所有显示在日志文件中可能的日志消息。依次选择**导出 (Export)** 以 CSV 文件的形式导出所有系统日志消息。



您还可以参阅[思科 ISE 系统日志](#)文档，了解Cisco ISE 发送的系统日志消息的综合列表、它们的含义以及它们如何记录在本地和远程目标中。

## 终端调试日志收集器

要排除特定终端的问题，可以根据其 IP 地址或 MAC 地址为该特定终端下载调试日志。该特定终端专用部署中的各个节点的日志收集在一个文件中，从而帮助您快速、有效地排除问题。一次只能对一个终端运行此故障排除工具。日志文件列于 GUI 中。您可以为部署中的一个节点或所有节点的终端下载日志。

### 下载特定终端的调试日志

要解决与网络中的特定终端相关的问题，可以从管理员门户使用调试终端工具。或者，可以从 **Authentications** 页面运行此工具。从 **Authentications** 页面右键单击 **Endpoint ID**，然后单击 **Endpoint Debug**。此工具在一个文件中提供关于特定终端的所有服务的所有调试信息。

#### 开始之前

需要准备收集其调试日志的终端的 IP 地址或 MAC 地址。

---

**步骤 1** 在思科 ISE GUI 中，点击菜单 (**Menu**) 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **端点调试 (Endpoint Debug)**。

**步骤 2** 点击 **MAC Address** 或 **IP** 单选按钮，输入终端的 MAC 或 IP 地址。

**步骤 3** 如果想要在指定的时间之后停止日志收集，请选中 **Automatic disable after *n* Minutes** 复选框。如果选中此复选框，必须输入 1 和 60 分钟之间的时间值。

显示以下消息：“Endpoint Debug degrades the deployment performance. Would you like to continue?”

**步骤 4** 点击 **Continue** 收集日志。

**步骤 5** 当想要手动停止日志收集时，请点击 **Stop**。

---

#### 相关主题

[终端调试日志收集器](#)，第 33 页

## 集合过滤器

您可以配置集合过滤器来禁止将系统日志消息发送到监控节点和外部服务器。可以根据不同属性类型在策略服务节点级别执行禁止。您可以使用特定属性类型和对应的值定义多个过滤器。

在将系统日志消息发送到监控节点或外部服务器之前，Cisco ISE 会将这些值与要发送的系统日志消息中的字段进行比较。如果找到任何匹配项，则不会发送对应的消息。

## 配置集合过滤器

您可以根据各种属性类型配置一系列集合过滤器。建议将过滤器数限制在20个以内。您可以添加、编辑或删除集合过滤器。

**步骤 1** 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 集合过滤器 (Collection Filters)**。

**步骤 2** 点击添加 (Add)。

**步骤 3** 从以下列表选择 **Filter Type**:

- User Name
- MAC Address
- Policy Set Name
- NAS IP Address
- Device IP Address

**步骤 4** 为您已选的过滤器类型选择对应的 **Value**。

**步骤 5** 从下拉列表中选择 **Result**。结果可能是 All、Passed 或 Failed。

**步骤 6** 点击提交 (Submit)。

### 相关主题

[集合过滤器](#)，第 33 页

[事件抑制绕行过滤器](#)，第 34 页

## 事件抑制绕行过滤器

Cisco ISE 允许您设置过滤器，以禁止向监控节点和使用收集过滤器的其他外部服务器发送某些系统日志消息。有时，您需要访问这些禁止发送的日志消息。Cisco ISE 现在为您提供根据特定属性（例如用户名）在可配置的时间内绕过事件抑制的选项。默认值为 50 分钟，但您可以将持续时间配置为 5 分钟至 480 分钟（8 小时）。配置事件抑制绕行后，该功能会立即生效。如果您设置的持续时间结束，则绕行抑制过滤器将过期。

您可以在 Cisco ISE 用户界面的 **Collection Filters** 页面中配置抑制绕行过滤器。使用此功能，您现在可以查看某个特定身份（用户）的所有日志并实时解决该身份遇到的问题。

您可以启用或禁用过滤器。如果您在绕行事件过滤器中配置的持续时间结束，则过滤器会自动禁用，直至您再次启用该过滤器。

Cisco ISE 在更改配置审核报告中捕获这些配置更改。此报告提供了事件抑制或绕行抑制配置人员的相关信息，以及抑制事件或绕行抑制的持续时间。

# 思科 ISE 报告

Cisco 身份服务引擎 (ISE) 报告用于监控和故障排除功能分析趋势、和，监控系统性能和网络活动从中心位置。

Cisco ISE 从整个网络收集日志和配置数据。然后，将数据聚合到报告，供您查看和分析。Cisco ISE 提供一套标准的预定义报告，您可以直接使用，也可以自定义以满足自己的需求。

Cisco ISE 报告经过预配置，划分为不同的逻辑类别，包含有关身份验证、会话流量、设备管理、配置和管理以及故障排除的信息。

## 相关主题

[运行并查看报告](#)，第 36 页

[导出报告](#)，第 37 页

[可用报告](#)，第 41 页

# 报告过滤器

有两种报告类型：single-section 和 multi-section。Single-section 报告包含单一网格（RADIUS 身份验证报告），multi-section 报告包含多个网格（身份验证摘要报告），并以图表和表格的形式代表数据。单段报告中的过滤器下拉菜单包含快速过滤器 (Quick Filter) 和自定义过滤器 (Custom Filter)。在 multi-section 报告中，仅可以指定高级过滤器。

多段报告可能包含需要您输入的一个或多个必填自定义过滤器。例如，当点击“运行状况摘要” (Health Summary) 报告（操作 (Operations) > 报告 (Reports) > 诊断 (Diagnostics) 页面）时，会显示两个必填自定义过滤器：服务器 (Server) 和时间范围 (Time Range)。您必须为这两个过滤器指定操作符命令、服务器名称和所需值，然后点击开始 (Go) 生成报告。您可以点击加号 (+) 添加新的高级过滤器。您仅可将 multi-section 导出为 PDF 格式。您不能计划在特定时间或时间间隔运行和重新运行 Cisco ISE multi-section 报告。



## 注释

当点击报告时，默认生成当前日期的数据。但是，除时间范围外，某些多段报告需要用户强制输入。

默认情况下，快速过滤器显示为 single-section 报告的第一行。字段可能是一个包含可选择搜索条件的下拉列表，也可以是一个文本框。

高级过滤器包含一个外部标准，其中含有一个或多个内部标准。外部标准用于指定搜索是否应满足所有或任何指定的内部标准。内部标准包含一个或多个条件，用于指定类别（终端 ID、身份组）、方法（操作符命令，例如包含、不包含）和该条件的时间范围。

使用快速过滤器 (Quick Filter) 时，可以从记录于 (Logged At) 下拉列表中选择日期或时间，以生成过去 30 天或以内记录的数据集的报告。如果要为 30 天前的日期或时间生成报告，请使用高级过滤器 (Advanced Filter)，在下拉列表中自定义 (Custom) 选项的从 (From) 字段和到 (To) 字段中设置所需的时间范围。

## 创建快速过滤器条件

本节介绍如何创建快速过滤器条件。您只能为单段报告创建快速过滤器条件。

- 
- 步骤 1** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations) > 报告 (Reports)** 并点击所需的报告。
- 步骤 2** 从**设置 (Settings)** 下拉列表中选择所需字段。
- 步骤 3** 在必填字段中，您可以从下拉列表中选择或者键入特定字符以过滤数据。搜索使用 **Contains** 运算符命令。例如，要过滤以“K”开头的文本，请输入 K，或者要过滤任意位置包含“geo”的文本，请输入 geo。您还可以使用星号 (\*)，例如，以 \*abc 开头并以 \*def 结尾的正则表达式。
- 快速过滤器使用以下条件：包含、开头为、结尾为、开头为或结尾为，以及使用 **OR** 运算符的多个值。
- 步骤 4** 按 **Enter** 键。
- 

## 创建高级过滤条件

本节介绍如何创建高级过滤条件。您可以为单段和多段报告创建高级过滤器。单段报告中的过滤器下拉菜单包含**快速过滤器 (Quick Filter)** 和**自定义过滤器 (Custom Filter)**。在多段报告中，仅可以指定高级过滤器。

- 
- 步骤 1** 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations) > 报告 (Reports)** 并点击所需的报告。
- 步骤 2** 在**过滤器 (Filters)** 部分，从**匹配 (Match)** 下拉列表中选择一项。
- 选择**所有 (All)** 以匹配所有指定的条件。
  - 选择**任意 (Any)** 以匹配任意一个指定的条件。
- 步骤 3** 从**时间范围 (Time Range)** 下拉列表中选择所需类别。
- 步骤 4** 从**运算符命令 (Operator Commands)** 下拉列表中，选择所需的命令。例如，可以过滤以特定字符开头的文本（使用“开头为”）或任意位置存在特定字符的文本（使用“包含”）。或者，您可以选择**记录时间 (Logged Time)** 和对应的**自定义 (Custom)** 选项并在日历中指定开始和结束的日期和时间以过滤数据。
- 步骤 5** 从**时间范围 (Time Range)** 下拉列表中选择所需选项。
- 步骤 6** 点击 **Go**（前往）。
- 

您可以保存已过滤的报告并从**过滤器 (Filters)** 下拉列表中检索该报告以供将来参考。

## 运行并查看报告

本节描述如何使用报告视图运行、查看并导航报告。默认情况下，当您点击报告时，可生成最近七天的数据。每个报告每页显示 500 行数据。您可以指定报告中所显示数据的时间增量。

**步骤 1** 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 操作 (Operations) > 报告 (Reports) > ISE 报告 (ISE Reports)。

还可以导航至每个工作中心下的报告 (Reports) 链接，以查看特定于此工作中心的报告集。

**步骤 2** 点击 " 可用报告页上的类别的报告。

**步骤 3** 选择一个或多个过滤器以运行报告。每个报告都具有不同的可用过滤器，某些过滤器为必选而某些则为可选。

**步骤 4** 为过滤器输入适当的值。

**步骤 5** 点击 Go (前往)。

#### 相关主题

[导出报告](#)，第 37 页

[可用报告](#)，第 41 页

## 报告导航

您可以从报告输出中获得详细信息。例如，如果您为五个月的一个时间段生成了报告，其图表将按月列出报告的汇总数据。

您可以从表格中点击特定值以查看与此特定字段相关的其他报告。例如，身份验证摘要报告将显示用户或用户组的失败计数。当您点击失败计数时，系统就会打开该特定失败计数的身份验证摘要报告。

## 导出报告

仅可以导出以下报告的 PDF 文件格式：

- 身份验证摘要
- 运行状况摘要
- RBACL 丢弃摘要



注  
释

RBACL 丢弃的数据包流仅适用于 Cisco Catalyst 6500 系列交换机。

- 访客赞助商摘要
- 终端配置文件修改
- 网络设备会话状态

**步骤 1** 如“运行和查看报告” (Running and Viewing Reports) 一节所述运行报告。

**步骤 2** 点击报告摘要页面右上角的导出到 (**Export To**)。

**步骤 3** 选择以下选项之一：

- 存储库 (CSV)：将报告以 CSV 文件格式导出到存储库
- 本地 (CSV)：将报告以 CSV 文件格式导出到本地磁盘
- 本地 (PDF)：将报告以 PDF 文件格式导出到本地磁盘

**注释** 当选择本地 CSV 或 PDF 选项时，仅会导出前 500 条记录。您可以使用存储库 CSV 选项导出所有记录。

## 安排和保存思科 ISE 报告

可以自定义报告并将更改另存为新报告，或在报告摘要页面右上角的我的报告 (**My Reports**) 中恢复默认报告设置。

还可以自定义和安排 Cisco ISE 报告，以在特定时间或时间间隔运行和重新运行。对于生成的报告，还可以发送和接收电子邮件通知。

以每小时 (**Hourly**) 频率安排报告时，可以让报告运行多天，但时间段不能跨越两天。

例如，在安排从 2019 年 5 月 4 日到 2019 年 5 月 8 日的每小时报告时，可以将时间间隔设置为每天上午 6:00 至晚上 11:00，但不能设置为某日下午 6:00 到次日上午 11:00。Cisco ISE 会显示错误消息，说明在后一种情况下的时间范围无效。



**注释** 如果外部管理员（例如 Active Directory 管理员）在未填写电子邮件 ID 字段的情况下创建计划报告，则不会发送任何电子邮件通知。

无法安排以下报告：

- 身份验证摘要
- 运行状况摘要
- RBACL 丢弃摘要
- 访客赞助商摘要
- 终端配置文件更改
- 网络设备会话状态



注释 只能从 PAN 保存或安排（自定义）思科 ISE 报告。



注释 如果主 MnT 关闭，则辅助 MnT 将执行计划的报告作业。计划的报告作业在主 MnT 和辅助 MnT 上运行。在辅助 MnT 上，在运行导出作业之前，它会尝试对主 MnT 执行 ping 操作。如果 ping 操作失败，则它将仅运行导出作业，否则将跳过导出作业。

**步骤 1** 如“运行和查看报告”一节所述运行报告。

**步骤 2** 点击报告摘要页面右上角的**我的报告 (My Reports)**。

**步骤 3** 在对话框中输入所需的详细信息。

**步骤 4** 点击**另存为新报告 (Save as New)**。

当返回到保存的报告时，所有过滤器选项在默认情况下都处于选中状态。取消选中不想要使用的过滤器。

还可以从**我的报告 (My Reports)** 类别中删除已保存的报告。

## 思科 ISE 活动 RADIUS 会话

Cisco ISE 为实时会话提供动态的授权更改 (CoA) 功能，通过此功能，可以动态地控制活动 RADIUS 会话。可以将重新验证或断开请求发送到网络接入设备 (NAD) 以执行以下任务：

- 排除与身份验证相关的问题 - 可以使用 **Session reauthentication** 选项继续尝试重新验证。但是，不能使用此选项来限制访问。要限制访问，请使用 **shutdown** 选项。
- 阻止有问题主机 - 可以将 **Session termination** 与 **port shutdown** 选项一起使用，以阻止在网络上发送大量流量的被感染主机。但是，RADIUS 协议当前不支持重新启用已关闭端口的的方法。
- 强制终端重新获取 IP 地址 - 可以将 **Session termination** 与 **port bounce** 选项一起使用，以便没有请求方或客户端的终端在 VLAN 更改之后生成 DHCP 请求。
- 将更新的授权策略推送到终端 - 可以使用 **Session reauthentication** 选项执行更新的策略配置，例如，根据管理员的决定更改现有会话的授权策略。例如，如果启用终端安全评估验证，当终端初次获得访问权限时，通常会被隔离。已知终端的身份和终端安全评估之后，可将 **Session reauthentication** 命令发送到终端，以便该终端根据其终端安全评估获取实际授权策略。

为了让设备读懂 CoA 命令，应适当地配置选项，这一点非常重要。

为了使 CoA 正常工作，必须为每台需要动态授权更改的设备配置共享密钥。Cisco ISE 使用共享密钥配置向设备请求访问权限并向其发出 CoA 命令。



**注释** 在此思科 ISE 版本中，可以显示的经过身份验证的最大活动终端会话数限制为 100,000。

#### 相关主题

[更改 RADIUS 会话的授权](#)，第 40 页

## 更改 RADIUS 会话的授权

您网络中的某些网络接入设备可能不会在重新加载后发送 Accounting Stop 或 Accounting Off 数据包。因此，您可能在 Session Directory 报告中找到两个会话，其中一个已过期。

要动态地更改活动 RADIUS 会话的授权或断开活动 RADIUS 会话的连接，请务必选择最近的会话。

**步骤 1** 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 **操作 (Operations) > RADIUS 实时日志 (RADIUS Livelog)**。

**步骤 2** 将视图切换到 **Show Live Session**。

**步骤 3** 点击要发出 CoA 的 RADIUS 会话的 CoA 链接，然后选择以下其中一个选项：

- **SAnet Session Query** - 使用此选项查询有关支持 SAnet 的设备的信息。
- **Session reauthentication** - 重新对会话进行身份验证。如果您为在支持 COA 的 ASA 设备上建立的会话选择此选项，则此操作将会调用 Session Policy Push CoA。
- **Session reauthentication with last** - 为此会话使用最后一个成功身份验证方法。
- **Session reauthentication with rerun** - 从头开始运行配置的身份验证方法。

**注释** 思科 IOS 软件中当前不支持使用上一个方法进行会话重新身份验证 (**Session reauthentication with last**) 和通过重新运行进行会话重新身份验证 (**Session reauthentication with rerun**) 选项。

- **Session termination** - 仅终止会话。交换机会在不同的会话中重新对客户端进行身份验证。
- **Session termination with port bounce** - 终止会话并重新启动报告。
- **Session termination with port shutdown** - 终止会话并关闭报告。

**步骤 4** 点击 **运行 (Run)** 使用选定的 reauthenticate 或 terminate 选项发出 CoA。

如果您的 CoA 失败，可能是由于以下其中一个原因引起：

- 设备不支持 CoA。
- 身份或授权策略已发生更改。
- 共享密钥不匹配。



## 可用报告

下表按照报告类别分组列出系统预配置的报告。此外还提供对报告功能和日志记录类别的说明。

要为日志记录类别生成系统日志，请将其日志严重性级别 (**Log Severity Level**) 设置为信息 (**Info**):

- 在思科 ISE GUI 中，点击菜单 (**Menu**) 图标 (≡)，然后选择 **管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)**。
- 点击必须为其生成系统日志的日志记录类别。
- 在日志严重性级别 (**Log Severity Level**) 字段中，从下拉菜单中选择信息 (**Info**)。
- 点击 **保存 (Save)**。



注释

在 Cisco ISE 版本 2.6 及更高版本中，使用 IPv6 地址的用户将在审核报告中记录以下事件：登录/注销、密码更改和操作更改。在管理员登录、用户更改密码审核和操作审核报告中，您现在可以按 IPv4 和 IPv6 记录过滤日志。

报告名称	说明	日志记录类别
<b>审计</b>		
自适应网络控制审计	自适应网络控制审计报告以 RADIUS 计费为基础。它可以显示每个终端所有网络会话的历史报告数据。	在思科 ISE GUI 中，点击菜单 ( <b>Menu</b> ) 图标 (≡)，然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> ，然后选择“已通过的身份验证” (Passed Authentications) 和“RADIUS 记账” (RADIUS Accounting)。
Administrator Logins	管理员登录报告提供关于所有基于 GUI 的管理员登录事件以及成功的 CLI 登录事件的信息。	在思科 ISE GUI 中，点击菜单 ( <b>Menu</b> ) 图标 (≡)，然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> ，然后选择“管理和操作审核” (Administrative and Operational audit)。

报告名称	说明	日志记录类别
更改配置审核	更改配置审核报告提供关于指定时间内配置更改的详细信息。如果需要对某个功能进行故障排除，此报告可以帮助您确定是不是最近的配置更改导致了问题。	
数据清除审核	<p>数据清除审核报告记录何时清除了日志记录数据。</p> <p>此报告会反映两个数据清除来源。</p> <p>每天凌晨 4 点，Cisco ISE 会检查是否有任何日志记录文件符合您在“管理” (Administration) &gt; “维护” (Maintenance) &gt; “数据清除” (Data Purging) 页面设置的条件。如有，Cisco ISE 会删除这些文件并将其记录于此报告中。此外，Cisco ISE 继续为日志文件保留最多 80% 的已用存储空间。Cisco ISE 每小时都会检查此百分比并删除最早的数据，直到再次达到此 80% 的阈值。这些信息也会记录于此报告中。</p> <p>如果磁盘空间利用率高，系统会在达到 80% 阈值时显示一条警报消息，说明 ISE 监控节点即将超过最大分配量 (ISE Monitor node(s) is about to exceed the maximum amount allocated is displayed at the 80 percent threshold)。随后，系统会在达到 90% 阈值显示一条警报消息，说明 ISE 监控节点已超过最大分配量 (ISE Monitor node(s) has exceeded the maximum amount allocated)。</p>	

报告名称	说明	日志记录类别
终端清除活动	用户可以通过终端清除活动报告查看终端清除活动的历史记录。此报告要求启用“分析器”(Profiler)日志记录类别。该类别在默认情况下已启用。	在思科 ISE GUI 中, 点击菜单 (Menu) 图标 (☰), 然后选择 管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories), 然后选择“分析器”(Profiler)。
内部管理员摘要	您可以通过内部管理员摘要报告验证管理员用户的注册情况。您还可以从此报告访问管理员登录和更改配置审核报告, 从而可以查看每个管理员的此类详细信息。	-
操作审核	操作审核报告提供关于任何操作变更的详细信息, 例如运行备份、注册 Cisco ISE 节点或重新启动应用。	在思科 ISE GUI 中, 点击菜单 (Menu) 图标 (☰), 然后选择 管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories), 然后选择“管理和操作审核”(Administrative and Operational audit)。
pxGrid Administrator Audit	pxGrid 管理员审核报告提供关于 pxGrid 管理操作的详细信息, 例如在主 PAN 上注册客户端、注销客户端、批准客户端、创建主题、删除主题、添加发布者-订用者, 以及删除发布者-订用者。 每条记录都会注明在节点上执行相应操作的管理员名称。 您可以根据管理员和消息条件过滤 pxGrid 管理员审核报告。	-
Secure Communications Audit	安全通信审核报告提供关于 Cisco ISE 管理员 CLI 中的安全性相关事件的审核详细信息, 该管理员 CLI 包括: 身份验证失败、可能的入侵尝试、SSH 登录、失效密码、SSH 注销和无效用户帐户等。	-

报告名称	说明	日志记录类别
用户更改密码审核	用户更改密码审核报告显示关于员工密码更改的验证信息。	管理和操作审核
Trustsec 审核	Trustsec 审核日志包含： <ul style="list-style-type: none"> <li>• 管理（创建、重命名、更新和删除）Trustsec 组件。</li> <li>• 将 SGACL 和 SGT 部署到启用 Trustsec 的 NAD</li> <li>• Trustsec 会话。</li> </ul> <p>如果Cisco ISE 与Cisco DNA 中心集成，并且 SD 访问由Cisco DNA 中心管理，则此日志为空。</p>	-
设备管理		
身份验证摘要	TACACS 身份验证摘要报告会详细说明最常见的身份验证以及身份验证失败的原因。	—
TACACS 计费	TACACS 计费报告为设备会话提供计费的详细信息。它显示用户和设备的生成和日志记录时间的相关信息。	在思科 ISE GUI 中，点击菜单 <b>(Menu)</b> 图标 (☰)，然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> ，然后选择“TACACS 记账” (TACACS Accounting)。
不同失败原因的前 N 个身份验证	“不同失败原因的前 N 个身份验证” (Top N Authentication by Failure Reason) 报告根据所选参数显示特定期间内不同失败原因的身份验证总数。	—
不同网络设备的前 N 个身份验证	“不同网络设备的前 N 个身份验证” (Top N Authentication by Network Device) 报告根据所选参数按网络设备名称显示特定期间内已通过和已失败的身份验证数量。	—

报告名称	说明	日志记录类别
不同用户的前 N 个身份验证	“不同用户的前 N 个身份验证” (Top N Authentication by User) 报告根据所选参数按用户名显示特定期间内已通过和失败的身份验证数量。	—
<b>诊断</b>		
AAA 诊断	<p>AAA 诊断报告提供Cisco ISE 和用户之间所有网络会话的详细信息。如果用户无法访问网络，您可查看此报告以确定其动态并明确问题是仅限于特定用户还是普遍存在。</p> <p><b>注释</b> 有时，如果正在进行用户身份验证，ISE 会以静默方式丢弃终端的计费停止 (Accounting Stop) 请求。但是，一旦用户身份验证完成，ISE 将开始确认所有计费请求。</p>	在思科 ISE GUI 中，点击菜单 (Menu) 图标 (≡)，然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> ，然后选择这些日志记录类别：“政策诊断” (Policy Diagnostics)、 “身份存储区诊断” (Identity Stores Diagnostics)、 “身份验证流程诊断” (Authentication Flow Diagnostics) 和 “RADIUS 诊断” (RADIUS Diagnostics)。
AD 连接器操作	<p>AD Connector Operations 报告提供关于 AD 连接器执行的操作的日志，例如Cisco ISE 服务器密码更新、Kerberos 票证管理、DNS 查询、DC 发现、LDAP 和 RPC 连接管理等。</p> <p>如果遇到某些 AD 故障，您可以在此报告中查看详细信息以确定可能的原因。</p>	在思科 ISE GUI 中，点击菜单 (Menu) 图标 (≡)，然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> ，然后选择 “AD 连接器” (AD Connector)。
Endpoint Profile Changes	终端顶级授权 (MAC 地址) 报告显示Cisco ISE 已授权每个终端 MAC 地址访问网络的次数。	已通过身份验证、失败尝试

报告名称	说明	日志记录类别
运行状况摘要	<p>运行状况摘要报告提供与控制面板类似的详细信息。但是，控制面板仅显示前 24 小时的数据，而您可以使用此报告查看更久之前的历史数据。</p> <p>您可以评估这些数据，以查看数据中的一致模式。例如，您可能预计当大多数员工都开始工作时，CPU 使用率较高。如果您发现这些趋势存在不一致性，您可以确定潜在的问题。</p> <p>CPU 使用率表列出不同 Cisco ISE 功能的 CPU 使用率百分比。此表中提供 <b>show cpu usage</b> CLI 命令的输出，您可以将这些值与部署中的问题相关联，从而识别可能的原因。</p>	—
ISE 计数器	<p>ISE 计数器报告列出各种属性的阈值。这些不同的属性值按照不同的时间间隔收集，而数据以表格格式呈现；一个间隔为 5 分钟，另一个间隔大于 5 分钟。</p> <p>您可以评估这些数据以查看趋势，如果发现高于阈值的值，则可以将此信息与部署中的问题相关联，以确定可能的原因。</p> <p>默认情况下，Cisco ISE 会收集这些属性值。您可以在 Cisco ISE CLI 中使用 <b>application configure ise</b> 命令禁用此数据收集操作。选择选项 14 可启用或禁用计数器属性收集。</p>	—
关键性能指标	<p>关键性能指标报告提供有关连接到部署的终端数量以及每个 PSN 每小时处理的 RADIUS 请求数量的统计信息。此报告列出服务器上的平均负载、每个请求的平均延迟和每秒的平均事务数。</p>	-

报告名称	说明	日志记录类别
配置有误的 NAS	<p>配置有误的 NAS 报告提供关于记帐频率不正确（通常指频繁地发送记帐信息）的 NAD 的信息。如果您已采取纠正措施并修复配置错误的 NAD，此报告会显示修复确认信息。</p> <p><b>注释</b> 应启用 RADIUS 抑制才能运行此报告。</p>	-
配置有误的请求方	<p>配置有误的请求方报告提供配置错误的请求方的列表以及对具体请求方执行的失败尝试的统计信息。如果您已采取纠正措施并修复配置错误的请求方，此报告会显示修复确认信息。</p> <p><b>注释</b> 应启用 RADIUS 抑制才能运行此报告。</p>	-
网络设备会话状态	<p>您可以通过网络设备会话状态摘要报告显示交换机配置，而无需直接登录交换机。</p> <p>Cisco ISE 使用 SNMP 查询功能获取这些详细信息，而且要求用 SNMP v1/v2c 配置您的网络设备。</p> <p>如果用户遇到网络问题，此报告可帮助您识别问题是否与交换机配置相关，而与 Cisco ISE 无关。</p>	-
OCSP 监控	<p>OCSP 监控报告指明在线证书状态协议 (OCSP) 服务的状态。它可以确定 Cisco ISE 能否成功连接证书服务器并提供证书状态审核，还提供对 Cisco ISE 执行的所有 OCSP 证书验证操作的汇总。此外，它可从 OCSP 服务器检索关于正常和已吊销主要证书与辅助证书的信息。Cisco ISE 缓存响应并利用响应生成后续 OCSP 监控报告。如果缓存已清除，它将从 OCSP 服务器检索信息。</p>	<p>在思科 ISE GUI 中，点击菜单 <b>(Menu)</b> 图标 (≡)，然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b>，然后选择“系统诊断” (System Diagnostics)。</p>

报告名称	说明	日志记录类别
RADIUS 错误	您可以通过 RADIUS 错误报告检查已丢失的 RADIUS 请求（从未知网络访问设备丢弃的身份验证/记账请求）、EAP 连接超时和未知 NAD。  注释 您只能查看过去 5 天的报告。	在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)，然后选择“失败尝试” (Failed Attempts)。
系统诊断	系统诊断报告提供关于 Cisco ISE 节点的状态的详细信息。如果 Cisco ISE 节点无法注册，您可查看此报告以对问题进行故障排除。  此报告要求首先启用几个诊断日志记录类别。收集这些日志可能会对 Cisco ISE 性能产生负面影响。因此，默认情况下未启用这些类别。如果您启用这些类别，应使其启用持续时间刚好满足收集数据的要求即可。否则，30 分钟后系统会自动禁用这些类别。	在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories) 然后选择以下日志记录类别：“内部操作诊断” (Internal Operations Diagnostics)、 “分布式管理” (Distributed Management)、 “管理员身份验证” (Administrator Authentication) 和 “授权” (Authorization)。
<b>Endpoints and Users</b>		
身份验证摘要	身份验证摘要报告以 RADIUS 身份验证为基础。您可以通过此报告确定最常见的身份验证以及任何身份验证失败的原因。例如，如果一个 Cisco ISE 服务器处理的身份验证明显多于其他服务器，您可能需要重新将用户分配给其他 Cisco ISE 服务器，以实现更好的负载均衡。  注释 由于身份验证摘要报告或控制面板要收集和显示与失败或成功的身份验证对应的最新数据，所以报告的内容会延迟几分钟才显示。	-
无代理终端安全评估	列出运行无代理终端安全评估的所有终端。	



报告名称	说明	日志记录类别
客户端调配	<p>客户端调配报告显示应用于特定终端的客户端调配代理。您可以使用此报告验证应用于每个终端的策略以确定是否正确调配了终端。</p> <p><b>注释</b> 如果终端不与 ISE 连接（未建立会话）或对会话使用网络地址转换 (NAT) 地址，则终端的 MAC 地址不会显示在“终端 ID” (Endpoint ID) 列中。</p>	在思科 ISE GUI 中，点击菜单 (Menu) 图标 (≡)，然后选择 管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)，然后选择“终端安全评估和客户端调配审核” (Posture and Client Provisioning Audit) 以及“终端安全评估和客户端调配诊断” (Posture and Client Provisioning Diagnostics)。
当前活动会话	<p>您可以通过当前活动会话报告导出包含关于指定时间内哪些用户正在访问网络的详细信息的报告。</p> <p>如果用户无法访问网络，您可以查看会话是否经过了身份验证或是否中断，或会话是否存在其他问题。</p>	-
终端脚本调配摘要	<p><b>终端脚本调配摘要 (Endpoint Scripts Provisioning Summary)</b> 窗口显示过去 30 天内通过终端脚本向导运行的作业的详细信息。</p> <p>有关终端脚本向导和此报告内容的详细信息，请参阅<a href="#">适用于 Windows 和 Macintosh 终端的终端脚本向导</a>。</p>	—
外部移动设备管理	<p>外部移动设备管理报告提供关于 Cisco ISE 与外部移动设备管理 (MDM) 服务器之间的集成的详细信息。</p> <p>您可以使用此报告查看哪些终端经过了 MDM 服务器调配，而无需直接登录 MDM 服务器。此报告还显示注册和 MDM 合规状态等信息。</p>	在思科 ISE GUI 中，点击菜单 (Menu) 图标 (≡)，然后选择 管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)，然后选择“MDM”。

报告名称	说明	日志记录类别
被动 ID	<p>您可以通过被动 ID (Passive ID) 报告监控与域控制器的 WMI 连接的状态并收集与之相关的统计信息（例如接收的通知数量、每秒钟用户登录/注销的次数等）。</p> <p><b>注释</b> 通过此方法进行身份验证的会话在报告中没有身份验证详细信息。</p>	在思科 ISE GUI 中，点击菜单 <b>(Menu)</b> 图标 (☰)，然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> ，然后选择“身份映射” (Identity Mapping)。
手动证书调配	手动证书调配报告列出所有通过证书调配门户手动调配的证书。	-
按条件进行终端安全评估	通过按条件进行终端安全评估报告，您可以查看 ISE 中配置的基于终端安全评估策略条件的记录，从而对最新安全设置和应用在客户端计算机上的可用性进行验证。	-
按终端进行终端安全评估	<p>“不同终端的终端安全评估”报告提供终端的详细信息，如时间、状态和 PRA 操作。您可以点击<b>详细信息 (Details)</b> 以查看终端的更多信息。</p> <p><b>注释</b> “不同终端的终端安全评估”报告不提供终端应用和硬件属性的终端安全评估策略详细信息。您只能在“情景可视性” (Context Visibility) 页面中查看这些信息。</p>	-

报告名称	说明	日志记录类别
已分析终端总结	<p>已分析终端总结报告提供关于正在访问网络的终端的分析详细信息。</p> <p><b>注释</b> 对于不注册会话时间的终端（例如思科 IP 电话），“终端会话时间” (Endpoint session time) 字段中会显示“不适用” (Not Applicable)。</p>	在思科 ISE GUI 中，点击菜单 <b>(Menu)</b> 图标 (☰)，然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> ，然后选择“分析器” (Profiler)。
RADIUS 计费	<p>RADIUS 计费报告指出用户访问网络持续的时间。如果用户失去了网络连接，您可以使用此报告确定是不是 Cisco ISE 导致的网络连接问题。</p> <p><b>注释</b> 如果 RADIUS 记账临时更新包含有关给定会话的 IPv4 或 IPv6 地址更改的信息，则 RADIUS 记账报告中会包含 Radius 记账临时更新。</p>	
RADIUS 身份验证	您可以通过 RADIUS 身份验证报告查看身份验证失败和成功的历史记录。如果用户无法访问网络，您可以在此报告中查看详细信息以确定可能的原因。	在思科 ISE GUI 中，点击菜单 <b>(Menu)</b> 图标 (☰)，然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> ，然后选择以下日志记录类别：“已通过身份验证” (Passed Authentications) 和“失败尝试” (Failed Attempts)。
注册终端	注册终端报告显示员工注册的所有个人设备。	-
拒绝的终端	“拒绝的终端” (Rejected Endpoints) 报告列出了员工注册的所有被拒绝或放行的个人设备。	—

报告名称	说明	日志记录类别
请求方调配	请求方调配报告提供关于调配至员工个人设备的请求方的详细信息。	终端安全评估和客户端调配审核
按终端查看顶级授权	终端顶级授权 (MAC 地址) 报告显示 Cisco ISE 已授权每个终端 MAC 地址访问网络的次数。	已通过身份验证、失败尝试
按用户查看顶级授权	按用户查看顶级授权报告显示 Cisco ISE 已授权每个用户访问网络的次数。	已通过身份验证、失败尝试
不同访问服务的前 N 个身份验证	“不同访问服务的前 N 个身份验证” (Top N Authentication by Access Service) 报告根据所选参数按特定时间段的访问服务类型显示已通过和失败的身份验证数量。	—
不同失败原因的前 N 个身份验证	“不同失败原因的前 N 个身份验证” (Top N Authentication by Failure Reason) 报告根据所选参数显示特定期间内不同失败原因的身份验证总数。	—
不同网络设备的前 N 个身份验证	“不同网络设备的前 N 个身份验证” (Top N Authentication by Network Device) 报告根据所选参数按网络设备名称显示特定期间内已通过和已失败的身份验证数量。	—
不同用户的前 N 个身份验证	“不同用户的前 N 个身份验证” (Top N Authentication by User) 报告根据所选参数按用户名显示特定期间内已通过和失败的身份验证数量。	—
<b>Guest</b>		

报告名称	说明	日志记录类别
AUP Acceptance Status	AUP Acceptance Status 报告提供从所有 Guest 门户接受的 AUP 的详细信息。	在思科 ISE GUI 中, 点击菜单 <b>(Menu)</b> 图标 (≡), 然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> , 然后选择 “访客” (Guest)。
访客计费	访客计费报告是 RADIUS 计费报告的一部分。此报告中显示分配至激活访客或访客身份组的所有用户。	-
主访客报告	<p>主访客报告综合各个访客接入报告的数据, 并且允许您从不同报告来源导出数据。主访客报告还提供关于访客用户正在访问的网站的信息。您可以使用此报告进行安全审核, 以证明访客用户何时访问了网络以及他们在网络上执行了什么活动。</p> <p>您还必须在用于访客流量的网络访问设备 (NAD) 上启用 HTTP 检查。这些信息由 NAD 发送回 Cisco ISE。</p> <p>要检查客户端何时达到最大并行会话限制数, 从管理员门户选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> 并执行以下操作:</p> <ol style="list-style-type: none"> <li>1. 将 “身份验证流量诊断” (Authentication Flow Diagnostics) 日志类别的日志级别从警告提高到信息。</li> <li>2. 从 AAA 诊断 “日志记录类别” 下, 将 LogCollector 目标从可用的更改为已选的。</li> </ol>	在思科 ISE GUI 中, 点击菜单 <b>(Menu)</b> 图标 (≡), 然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> , 然后选择 “已通过的身份验证” (Passed Authentications)。

报告名称	说明	日志记录类别
我的设备登录和审核	我的设备登录和审核报告提供关于用户通过设备在“我的设备门户” (My Devices Portal) 中执行的登录活动和操作的详细信息。	在思科 ISE GUI 中，点击菜单 <b>(Menu)</b> 图标 (☰)，然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> ，然后选择“我的设备” (My Devices)。
Sponsor Login and Audit	<p>Sponsor Login and Audit 报告提供关于访客用户的登录、添加、删除、启用、暂停和更新操作以及发起人在发起人门户上的登录活动的详细信息。</p> <p>如果批量添加访客用户，则“访客用户” (Guest Users) 列下会显示这些用户。此列默认处于隐藏状态。在导出时，这些批量用户也会显示于导出的文件上。</p>	在思科 ISE GUI 中，点击菜单 <b>(Menu)</b> 图标 (☰)，然后选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> ，然后选择“访客” (Guest)。
<b>SXP</b>		
SXP 绑定	SXP 绑定报告提供与通过 SXP 连接进行交换的 IP-SGT 绑定有关的信息。	-
SXP 连接	您可以使用此报告来监控 SXP 连接的状态并收集与之相关的信息，例如对等 IP、SXP 节点 IP、VPN 名称、SXP 模式等。	—
<b>TrustSec</b>		

报告名称	说明	日志记录类别
RBACL 丢包摘要	<p>RBACL 丢包摘要报告专用于 TrustSec 功能，只有在具备 Cisco ISE 高级许可证的情况下才可用。</p> <p>此报告还要求您将网络设备配置为向 Cisco ISE 发送关于丢包事件的 NetFlow 事件。</p> <p>如果用户违反特定策略或访问权限，系统会丢弃数据包并在此报告中指明。</p> <p><b>注释</b> RBACL 丢弃的数据包流仅适用于 Cisco Catalyst 6500 系列交换机。</p>	-
按用户前 N 个 RBACL 丢包	<p>按用户前 N 个 RBACL 丢包报告专用于 TrustSec 功能，只有在具备 Cisco ISE 高级许可证的情况下才可用。</p> <p>此报告还要求您将网络设备配置为向 Cisco ISE 发送关于丢包事件的 NetFlow 事件。</p> <p>此报告显示特定用户违反策略的情况（依据数据包丢弃情况）。</p> <p><b>注释</b> RBACL 丢弃的数据包流仅适用于 Cisco Catalyst 6500 系列交换机。</p>	—
TrustSec ACI	<p>此报告列出与 EEPG、终端和 APIC 子网配置同步的 SGT 和 SXP 映射。只有当 TrustSec APIC 集成功能启用时，这些细节才会显示。</p>	-

报告名称	说明	日志记录类别
TrustSec 部署验证		-



报告名称	说明	日志记录类别
	<p>您可以使用此报告验证是否在所有网络设备上部署了最新的 TrustSec 策略，或者在 Cisco ISE 中配置的策略与网络设备之间是否存在任何差异。</p> <p>点击<b>详细信息 (Details)</b> 图标以查看验证过程的结果。您可以查看以下详细信息：</p> <ul style="list-style-type: none"> <li>• 验证过程开始和完成的时间</li> <li>• 是否在网络设备上成功部署了最新的 TrustSec 策略。您还可以查看部署了最新 TrustSec 策略的网络设备的名称和 IP 地址。</li> <li>• 在 Cisco ISE 中配置的策略与网络设备之间是否存在任何差异。它显示每个策略差异的设备名称、IP 地址和相应的错误消息。</li> </ul> <p>您可以在<b>警报 (Alarms) Dashlet</b>（在工作中心 (<b>Work Centers</b>) &gt; <b>TrustSec &gt; 控制板 (Dashboard)</b> 和主页 (<b>Home</b>) &gt; <b>摘要 (Summary)</b> 下）中查看 TrustSec 部署验证警报。</p> <p><b>注释</b></p> <ul style="list-style-type: none"> <li>• 报告所需的时间取决于部署中的网络设备和 TrustSec 组数量。</li> <li>• “TrustSec 部署验证” (TrustSec Deployment Verification) 报告中的错误消息长度当前限制为 480 个字符。超过 480 个字符的错误消息将被截断，并且报告中仅显示前 480 个字符。</li> </ul>	

报告名称	说明	日志记录类别
Trustsec 策略下载	此报告列出网络设备发出的策略 (SGT/SGACL) 下载请求和 ISE 发出的详细信息。如果启用工作流模式，对于生产或暂存表，可对请求进行过滤。	要查看此报告，必须执行以下操作： <ol style="list-style-type: none"> <li>1. 在思科 ISE GUI 中，点击菜单 (Menu) 图标 (≡)，然后选择 管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)。</li> <li>2. 选择 AAA 诊断 (AAA Diagnostics) &gt; RADIUS 诊断 (RADIUS Diagnostics)。</li> <li>3. 将 RADIUS 诊断的日志严重性级别设置为“调试” (DEBUG)。</li> </ol>
<b>以威胁防护为中心的 NAC 服务</b>		
适配器状态	适配器状态报告显示威胁和漏洞适配器的状态。	-
COA 事件	当收到某个终端的漏洞事件时，Cisco ISE 对该终端触发 CoA。CoA 事件报告显示这些 CoA 事件的状态。同时显示这些终端的新旧授权规则和配置文件详细信息。	-
威胁事件	“威胁事件” (Threat Events) 报告提供 Cisco ISE 从已配置的各种适配器接收的所有威胁事件的列表。	-
漏洞评估	漏洞评估报告为您的终端提供正在进行的评估的信息。您可以查看此报告以确认评估是否以配置策略为基础正在进行。	-

# RADIUS 实时日志

下表介绍“实时日志”(Live logs)窗口中的字段，其中显示最近的 RADIUS 身份验证。在思科 ISE GUI 中，点击菜单(Menu)图标(☰)，然后选择操作(Operations) > RADIUS > 实时日志(Live Logs)。只能在主 PAN 中查看 RADIUS 实时日志。

表 6: RADIUS 实时日志

字段名称	说明描述
时间 (Time)	显示监控和故障排除收集代理接收日志的时间。此列为必选项，无法取消选择。
状态 (Status)	显示身份验证是否成功。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。
详细信息 (Details)	<p>点击“详细信息”(Details)列下的图标可在新浏览器窗口中打开身份验证详细报告(Authentication Detail Report)。此报告提供有关身份验证和相关属性以及身份验证流程的信息。在身份验证详细信息(Authentication Details)框中，响应时间(Response Time)是Cisco ISE 处理身份验证流程所需的总时间。例如，如果身份验证包含三个往返消息，初始消息花费 300 毫秒，下一条消息花费 150 毫秒，最后一条消息花费 100 毫秒，则响应时间(Response Time)为 <math>300 + 150 + 100 = 550</math> 毫秒。</p> <p><b>注释</b> 您无法查看活动时间超过 48 小时的终端的详细信息。当点击活动时间超过 48 小时的终端的详细信息(Details)图标时，可能会看到一个包含以下消息的页面：此记录无可用数据。(No Data available for this record.) 数据可能已清除或此会话记录的身份验证发生在一周之前。(Either the data is purged or authentication for this session record happened a week ago.) 或者，如果这是“PassiveID”或“PassiveID 可视性”(PassiveID Visibility)会话，则不会有 ISE 身份验证详细信息，只有会话。(Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.)</p>

字段名称	说明描述
重复次数 (Repeat Count)	显示过去 24 小时内身份验证请求的重复次数，它们在身份、网络设备和授权方面没有任何变化。
身份 (Identity)	<p>显示与身份验证关联的已登录用户名。</p> <p>如果用户名不存在于任何 ID 存储区中，则显示为 INVALID。如果身份验证由于任何其他原因而失败，则显示为 USERNAME。</p> <p>注释 这仅适用于用户。这不适用于 MAC 地址。</p> <p>为了帮助进行调试，可以强制 Cisco ISE 显示无效的用户名。为此，请选中位于以下路径下方的披露无效用户名 (Disclose Invalid Usernames) 复选框：管理 (Administration) &gt; 系统 (System) &gt; 设置 (Settings) &gt; 安全设置 (Security Settings)。您还可以将披露无效用户名 (Disclose Invalid Usernames) 选项配置为超时，这样就不必手动将其关闭。</p>
终端 ID (Endpoint ID)	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
终端配置文件 (Endpoint Profile)	显示所分析的终端的类型，例如分析为 iPhone、Android、MacBook、Xbox 等。
身份验证策略 (Authentication Policy)	显示为特定身份验证选择的策略的名称。
授权策略 (Authorization Policy)	显示为特定授权选择的策略的名称。
授权配置文件 (Authorization Profiles)	显示用于身份验证的授权配置文件。
IP 地址 (IP Address)	显示终端设备的 IP 地址。
网络设备 (Network Device)	显示网络访问设备的 IP 地址。
设备端口 (Device Port)	显示终端连接的端口号。
身份组 (Identity Group)	显示分配给生成了日志的用户或终端的身份组。
终端安全评估状态 (Posture Status)	显示安全评估验证的状态和身份验证的详细信息。
服务器 (Server)	指示生成日志的策略服务。
MDM 服务器名称 (MDM Server Name)	显示 MDM 服务器的名称。

字段名称	说明描述
事件 (Event)	显示事件状态。
故障原因 (Failure Reason)	如果身份验证失败，显示失败的详细原因。
身份验证方法 (Auth Method)	显示 RADIUS 协议（例如 Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)、IEEE 802.1x 或 dot1X 等）使用的身份验证方法。
身份验证协议 (Authentication Protocol)	显示所使用的身份验证协议，例如受保护的可扩展身份验证协议 (PEAP) 和可扩展身份验证协议 (EAP) 等等。
安全组 (Security Group)	显示由身份验证日志标识的组。
会话 ID (Session ID)	显示会话 ID。



注释

在 **RADIUS 实时日志 (RADIUS Live Logs)** 和 **TACACS+ 实时日志 (TACACS+ Live Logs)** 窗口中，系统会为每个策略授权规则的第一个属性显示一个“已查询 PIP” (Queried PIP) 条目。如果授权规则中的所有属性都与已为之前的规则查询的字典相关，则不会显示其他“已查询 PIP” (Queried PIP) 条目。

您可以在 **RADIUS 实时日志 (Live Logs)** 窗口中执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。
- 对列值排序。



注释

所有用户自定义将存储为用户首选项。

## 身份验证延迟

身份验证延迟是 RADIUS 身份验证程序自身份验证程序启动后的平均响应时间。在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择控制板 > 系统摘要 (System Summary) Dashlet。查看 Cisco ISE 身份验证延迟。

可以从下拉列表中选择以下身份验证延迟时间：

- **60 分钟 (60 mins)**: 此选项对于在前 60 分钟内启动的身份验证提供身份验证延迟。
- **12 小时 (12 hrs)**: 此选项对于在前 24 小时内启动的身份验证程序提供身份验证延迟。

显示的响应时间以毫秒 (ms) 为单位。要查看身份验证延迟的详细报告，请点击**实时日志 (Live Logs)** 窗口中的最新日志。要查看此处窗口，请点击**菜单 (Menu)** 图标 (≡)，然后选择 **操作 (Operations) > RADIUS**。

## RADIUS实时会话 (Live Sessions)

下表说明了 RADIUS 实时会话 (Live Sessions) 窗口中的字段，此窗口显示实时身份验证。要查看此处窗口，请点击**菜单 (Menu)** 图标 (≡)，然后选择您仅可在主 PAN 上查看 RADIUS 实时会话。

表 7: RADIUS 实时会话

字段名称	说明
启动时间 (Initiated)	显示启动会话时的时间戳。
已更新 (Updated)	显示会话上次由于更改而更新时的时间戳。
帐户会话时间 (Account Session Time)	显示用户会话的时间跨度 (秒)。
会话状态 (Session Status)	显示终端设备的当前状态。
操作 (Action)	点击 <b>操作 (Actions)</b> 图标可对活动 RADIUS 会话重新进行身份验证或断开活动 RADIUS 会话连接。
重复次数 (Repeat Count)	显示用户或终端重新进行身份验证的次数。
终端 ID	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
身份 (Identity)	显示终端设备的用户名。
IP 地址 (IP Address)	显示终端设备的 IP 地址。
审核会话 ID (Audit Session ID)	显示唯一会话标识符。
帐户会话 ID (Account Session ID)	显示网络设备提供的唯一 ID。
终端配置文件	显示设备的终端配置文件。
终端安全评估状态 (Posture Status)	显示安全评估验证的状态和身份验证的详细信息。
安全组 (Security Group)	显示由身份验证日志标识的组。

字段名称	说明
服务器 (Server)	指示已从中生成日志的策略服务节点。
身份验证方法 (Auth Method)	显示RADIUS协议使用的身份验证方法，例如密码身份验证协议 (PAP)、质询握手身份验证协议 (CHAP)、IEE 802.1x 或 dot1x 等等。
身份验证协议 (Authentication Protocol)	显示所使用的身份验证协议，例如受保护的可扩展身份验证协议 (PEAP) 和可扩展身份验证协议 (EAP) 等等。
身份验证策略 (Authentication Policy)	显示为特定身份验证选择的策略的名称。
授权策略 (Authorization Policy)	显示为特定授权选择的策略的名称。
授权配置文件 (Authorization Profiles)	显示用于身份验证的授权配置文件。
NAS IP 地址 (NAS IP Address)	显示网络设备的 IP 地址。
设备端口 (Device Port)	显示网络设备的连接端口。
PRA 操作 (PRA Action)	显示客户端在网络上成功通过合规性验证后，在客户端上采取的定期重评估操作。
ANC 状态 (ANC Status)	设备的自适应网络控制状态，如“隔离” (Quarantine)、“取消隔离” (Unquarantine) 或“关闭” (Shutdown)。
WLC 漫游 (WLC Roam)	<p>显示用于跟踪已在漫游期间从一个 WLC 传递到另一个 WLC 的终端的布尔值 (Y/N)。它的值为 <code>cisco-av-pair=nas-update=Y</code> 或 <code>N</code>。</p> <p>注释 Cisco ISE 依靠 WLC 中的 <code>nas-update=true</code> 属性识别会话是否处于漫游状态。当原始 WLC 在 <code>nas-update=true</code> 时发送记账停止属性时，不会在 ISE 中删除会话，以避免重新进行身份验证。如果漫游失败，ISE 将在会话处于非活动状态五天后清除该会话。</p>
接收的数据包 (Packets In)	显示接收的数据包数量。
发送的数据包 (Packets Out)	显示发送的数据包数量。
接收的字节 (Bytes In)	显示接收的字节数。
发送的字节 (Bytes Out)	显示发送的字节数。

字段名称	说明
会话源 (Session Source)	指示它是 RADIUS 会话还是被动 ID 会话。
用户域名 (User Domain Name)	显示用户的注册 DNS 名称。
主机域名 (Host Domain Name)	显示主机的注册 DNS 名称。
用户 NetBIOS 名称 (User NetBIOS Name)	显示用户的 NetBIOS 名称。
主机 NetBIOS 名称 (Host NetBIOS Name)	显示主机的 NetBIOS 名称。
许可证类型 (License Type)	显示使用的许可证类型。
许可证详细信息 (License Details)	显示许可证详细信息。
提供程序 (Provider)	<p>终端活动获悉自不同的系统日志源。这些系统日志源称为提供程序。</p> <ul style="list-style-type: none"> <li>• Windows Management Instrumentation (WMI) - WMI 是一种 Windows 服务，用于提供通用接口和对象模型来访问有关操作系统、设备、应用和服务的管理信息。</li> <li>• 代理：代表客户端或另一个程序在客户端上运行的程序。</li> <li>• 系统日志：客户端发送事件消息的日志记录服务器。</li> <li>• REST：客户端通过终端服务器进行身份验证。对于此系统日志源，将会显示“TS代理 ID”、“源端口开始时间”、“源端口结束时间”和“源第一个端口”值。</li> <li>• SPAN：使用 SPAN 探测器发现的网络信息。</li> <li>• DHCP：DHCP 事件。</li> <li>• 终端</li> </ul> <p><b>注释</b> 从终端会话获悉来自不同提供程序的两个事件后，提供程序在实时会话页面中显示为逗号分隔值。</p>
MAC 地址 (MAC Address)	显示客户端的 MAC 地址。
终端检查时间	显示终端探测器上次检查终端的时间。



字段名称	说明
终端检查结果	显示终端探测的结果。可能的值包括： <ul style="list-style-type: none"> <li>• 无法接通</li> <li>• 用户退出</li> <li>• 活动用户</li> </ul>
起始源端口 (Source Port Start)	(仅为 REST 提供程序显示值) 显示端口范围中的第一个端口号。
结束源端口	(仅为 REST 提供程序显示值) 显示端口范围中的最后一个端口号。
源第一个端口 (Source First Port)	(仅为 REST 提供程序显示值) 显示由终端服务器代理分配的第一个端口。  终端服务器指允许多个终端在无需调制解调器或网络接口的情况下连接到其上的服务器或网络设备，可实现多个终端到 LAN 网络的连接。多个终端可能会有相同的 IP 地址，因此难以识别特定用户的 IP 地址。所以，为了识别特定用户，需在服务器上安装终端服务器代理，为每个用户分配一个端口范围。这有助于创建 IP 地址-端口用户映射。
TS 代理 ID (TS Agent ID)	(仅为 REST 提供程序显示值) 显示安装在终端上的终端服务器代理的唯一标识。
AD 用户解析的身份 (AD User Resolved Identities)	(仅为 AD 用户显示值) 显示匹配的潜在账户。
AD 用户解析的 DN (AD User Resolved DNs)	(仅为 AD 用户显示值) 显示 AD 用户的可分辨名称，例如 CN=chris,CN=Users,DC=R1,DC=com

#### 相关主题

[更改 RADIUS 会话的授权](#)，第 40 页

[思科 ISE 活动 RADIUS 会话](#)，第 39 页

## TACACS 实时日志

下表列出“TACACS+ 实时日志”(TACACS Live Logs) 页面的字段，此页面显示 TACACS+ AAA 详细信息。在思科 ISE GUI 中，点击菜单 (Menu) 图标 (≡)，然后选择操作 (Operations) > TACACS > 实时日志 (Live Logs)。您只能在主 PAN 中查看 TACACS 实时日志。

表 8: TACACS 实时日志

字段名称	使用指南
生成时间 (Generated Time)	根据特定事件触发时间显示系统日志生成时间。
日志记录时间 (Logged Time)	显示监控节点处理和存储系统日志的时间。此列为必选项，无法取消选择。
状态 (Status)	显示身份验证是否成功。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。
详细信息 (Details)	在点击放大镜图标时显示报告，使您能够深入查看有关所选身份验证方案的更多详细信息。此列为必选项，无法取消选择。
会话密钥 (Session Key)	显示由 ISE 返回到网络设备的会话密钥（在 EAP 成功或 EAP 失败消息中查找）。
用户名 (Username)	显示设备管理员的用户名。此列为必选项，无法取消选择。
类型 (Type)	包括两种类型 - 身份验证和授权。显示身份验证已通过和/或失败的用户名。此列为必选项，无法取消选择。
身份验证策略 (Authentication Policy)	显示为特定身份验证选择的策略的名称。
授权策略 (Authorization Policy)	显示为特定授权选择的策略的名称。
ISE 节点 (ISE Node)	显示处理访问请求的 ISE 节点的名称。
网络设备名称 (Network Device Name)	显示网络设备的名称。
网络设备 IP (Network Device IP)	显示访问请求已处理的网络设备的 IP 地址。
网络设备组 (Network Device Groups)	显示网络设备所属相应网络设备组的名称。
设备类型 (Device Type)	显示用于处理来自不同网络设备的访问请求的设备类型。
位置 (Location)	显示用于处理来自网络设备的访问请求的基于位置的策略。
设备端口 (Device Port)	显示发出访问请求的设备端口号。
故障原因 (Failure Reason)	显示拒绝网络设备发出的访问请求的原因。
远程地址 (Remote Address)	显示唯一标识终端站的 IP 地址、MAC 地址，或任何其他字符串。

字段名称	使用指南
匹配的命令集 (Matched Command Set)	如果 MatchedCommandSet 属性值存在，则显示该值，或如果 MatchedCommandSet 属性值为空或属性本身不存在于系统日志，则显示一个空值。
外壳配置文件 (Shell Profile)	显示已授予设备管理员用于在网络设备执行命令的权限。

您可以在 TACACS 实时日志页面执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。
- 对列值排序。



注释 所有用户自定义将存储为用户首选项。

#### 相关主题

[TACACS+ 设备管理](#)  
[配置全局 TACACS+ 设置](#)

## 导出摘要

您可以查看过去 7 天内所有用户导出的报告的详细信息以及状态。导出摘要包括手动报告和已计划的报告。导出摘要页面每 2 分钟自动刷新一次。点击刷新图标可手动刷新导出摘要页面。

超级管理员可以取消正在进行或处于排队状态的导出进程。其他用户只能取消他们发起的导出进程。

默认情况下，在给定的时间点只能运行 3 次报告手动导出，其余触发的报告手动导出将排队。计划导出的报告没有此类限制。



注释 当思科 ISE 服务器重新启动时，所有处于排队状态的报告都将重新安排，处于正在进行或正在取消状态的报告将标记为失败。



注释 如果主 MnT 节点关闭，则已计划的报告导出作业将在辅助 MnT 节点上运行。

下表列出“导出摘要”(Export Summary)页面中的字段。在思科 ISE GUI 中，点击菜单 (Menu) 图标 (☰)，然后选择 操作 (Operations) > 报告 (Reports) > 导出摘要 (Export Summary)。

表 9: 导出摘要

字段名称	说明
报告已导出	显示报告的名称。
导出依据	显示发起导出进程的用户的角色。
已计划	显示报告导出是否为计划性导出。
触发于	显示在系统中触发导出进程的时间。
存储库	显示将存储导出数据的存储库的名称。
过滤器参数	显示导出报告时选择的过滤器参数。
状态	<p>显示导出的报告的状态。它可以是下列类型之一：</p> <ul style="list-style-type: none"> <li>• 已排队</li> <li>• 正在进行</li> <li>• 已完成</li> <li>• 正在取消</li> <li>• 已取消</li> <li>• 失败</li> <li>• 已跳过</li> </ul> <p><b>注释</b> 失败状态指示失败的原因。已跳过状态指示当主 MnT 节点关闭时，跳过了计划的报告导出。</p>

您可以在“导出摘要”(Export Summary)页面中执行以下操作：

- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。