Splunk 和 pxGrid 自适应网络控制 (ANC) 缓解工作流程操作

目录

关于本文档 **4**
简介 **5**
Splunk Add-on GUI 设置 **6**
EPS 工作流程操作 6
pxGrid ANC 工作流程缓解操作 7
自定义工作流程操作 **8**
ISE EPS RESTful API 和 pxGrid 工作流程操作 8
自定义 EPS RESTful API 工作流程操作 9
通过 IP 地址隔离 9
通过 MAC 地址隔离 10
通过框架 IP 地址隔离 11
通过 IP 地址取消隔离 12
通过 MAC 地址取消隔离 13
自定义 pxGrid ANC 工作流程缓解操作 14
ANC 的通过 IP 地址隔离操作 14
ANC 的通过 MAC 地址隔离操作 15
ANC 的通过 IP 地址取消隔离操作 16
ANC 的通过 MAC 地址取消隔离操作 17
为 EPS（终端保护服务）启用 ISE **18**
启用 ISE Restful API 18
为 Quarantine 创建授权策略 19
在 ISE 中配置日志记录类别 **20**
pxGrid 客户端 Java 密钥库简介 **21**
ISE pxGrid 和 Splunk pxGrid 客户端证书生成 **22**
简介 22
ISE pxGrid 角色配置 23
pxGrid 客户端证书配置 25
将 Splunk 配置为从 ISE 接收系统日志事件 **31**
Splunk pxGrid ANC 测试 **32**
pxGrid 操作 33

故障排除 **34**
无法连接到 ISE pxGrid 节点 34
检查 keystoreFilename 和密码 34
检查 Splunk pxGrid 日志文件 35
参考 **36**

关于本文档

本文档面向那些部署带有 pxGrid 和思科身份服务引擎 (ISE) 1.3 的 Splunk-for-ISE Add-on 的思科工程师、合作伙伴和客户。读者应熟悉 Splunk 和 ISE。本文档假定已安装带有 pxGrid 和 ISE 的 Splunk-for-ISE Add-on，例如 Splunk Enterprise 6.1 或 6.2。

带有 pxGrid 的 Splunk-for-ISE Add-on 当前仅在 Linux 或 MAC 平台上适用。由于对存储的 pxGrid 凭证加密的 API 支持有限，因此其在 Windows 平台上不适用。

.

简介

Splunk 是一种强大的工具，用于通过收集、存储、通知、报告和分析计算机数据来分析贵组织中的信息。借助思科平台交换网 (pxGrid)，Splunk 能够通过发出 pxGrid 自适应网络控制 (ANC) 工作流程操作，主动处理收到的网络安全系统日志事件并隔离/取消隔离终端。

Splunk-for-ISE Add-on 2.1 或更高版本采用自动化设置 GUI，通过 Splunk 工作流程操作处理 ISE EPS（终端保护服务）RESTful API 和 pxGrid ANC（自适应网络控制）缓解操作。

ISE EPS 工作流程操作适用于 ISE 1.2 和 ISE 1.3。pxGrid ANC 缓解操作适用于 ISE 1.3。

用于 pxGrid 操作的 Splunk-for-ISE Add-on 2.1 的初始版本需要其他思科文件，请咨询您的思科客户团队。

在本文档中，我们将通过使用自签名的 ISE 身份证书并为 pxGrid 客户端（即 Splunk）创建和生成自签名证书的方式，在独立环境中为 pxGrid 操作配置 ISE。

有关如何使用证书颁发机构 (CA) 签名的证书在生产环境中部署 ISE，请参阅“在 ISE 分布式环境中部署 pxGrid”。

所有 EPS 和 ANC 工作流程操作都可以按照本文档中的说明进行自定义。ISE 日志记录类别已启用，以触发发送到 Splunk 的系统日志事件。这些事件会在 Splunk 收到的 Framed_IP_Address、IpAddress、MacAddress 字段内包含实际 IP 或 MAC 地址，并在工作流程操作中进行定义。

本文档包括适用于 Splunk 的自签名 pxGrid 客户端证书生成过程，并提供了一个使用案例。在该使用案例中，Splunk 作为 pxGrid 客户端注册到 ISE pxGrid 节点并订阅终端保护功能主题，从而对终端执行隔离缓解操作（可在 ISE 中看到结果）。请注意，ISE 将在独立环境中部署。

本文档还涵盖基于已启用的 ISE 记录类别的工作流程自定义过程，之后是故障排除和参考部分。

.

Splunk Add-on GUI 设置

Splunk Add-on GUI 设置提供一种用于配置 ISE EPS RESTful API 和 ISE pxGrid ANC 缓解工作流程操作的自动化方法。您可以选择启用其中一个工作流程操作，或启用所有工作流程操作。

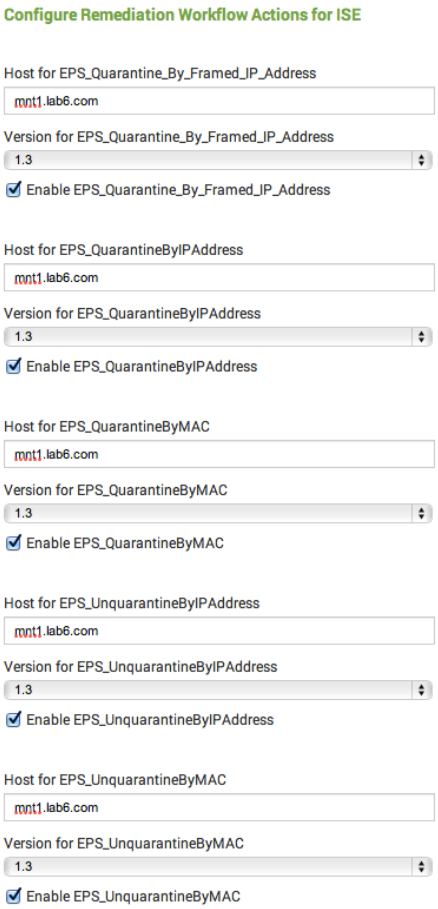
EPS 工作流程操作

步骤 1 启用 ISE EPS RESTful API 工作流程操作
Splunk -> Apps -> Splunk Add-on for Cisco ISE -> Setup

工作流程操作的“host”值在独立部署中表示 ISE 的 IP 地址或 FQDN。

注：ISE 的主机 IP 地址或 FQDN 在 ISE 分布式部署中应是 ISE MnT 节点。

您可以从下拉菜单选择 ISE 所需的 ISE 版本（ISE 1.2 或 ISE 1.3），并设置工作流程操作的启用状态。这些工作流程操作可在 Settings -> Fields -> Workflow actions 下自定义。

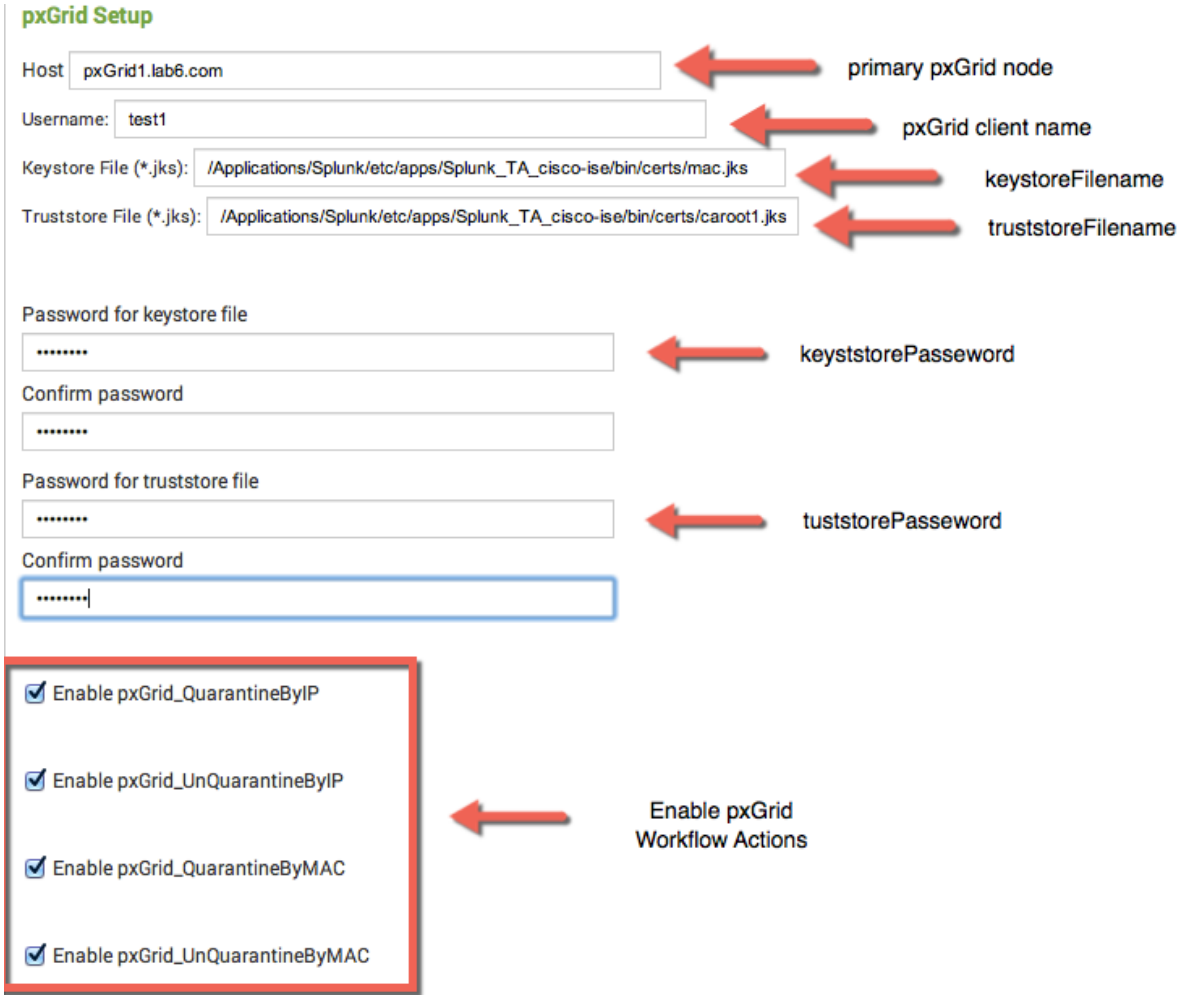


pxGrid ANC 工作流程缓解操作

步骤 1 启用 pxGrid 连接和 pxGrid ANC 缓解工作流程操作
Splunk -> Apps -> Splunk Add-on for Cisco ISE -> Setup

以下是 ISE pxGrid 操作的连接参数的概括说明：

- **Host**：定义 pxGrid 主节点的 IP 地址或 FQDN。
- **Username**：定义 pxGrid 注册客户端名称
- **Keystore File**：根据身份客户端证书定义 keystoreFilename (JKS)
- **Truststore File**：根据 CA 根证书和/或自签名的 ISE 证书定义 keystoreFilename (JKS)
- **Password for the keystore file**：定义 keystoreFilename 的密码
- **Password for the truststore file**：定义 truststoreFilename 的密码
- **pxGrid Workflow Actions**：可用的 pxGrid 缓解操作



自定义工作流程操作

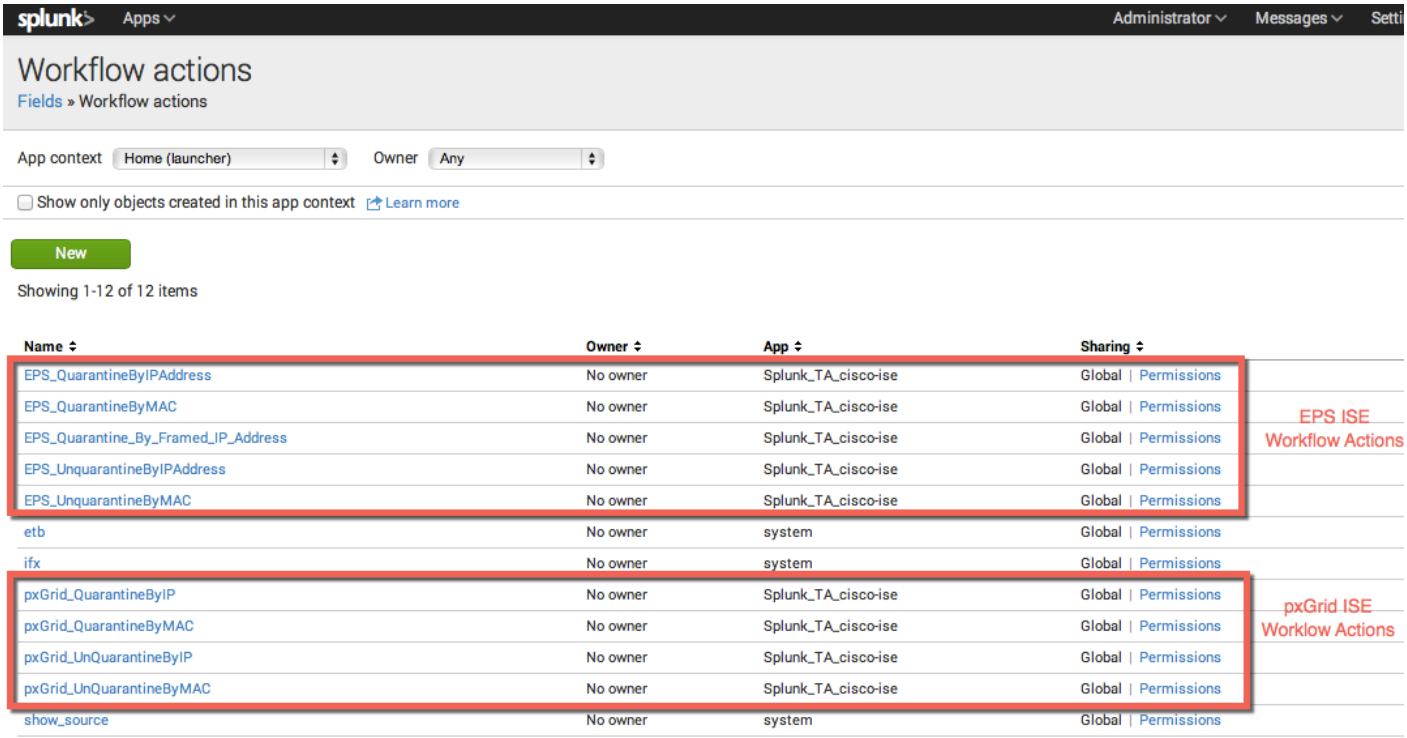
ISE EPS RESTful 工作流程操作和 pxGrid ANC 缓解工作流程操作可以自定义为根据系统日志事件收到的 Splunk 变量或字段使用不同的实际 IP 或 MAC 地址。在本文档中，ISE 日志记录类别将在发送到 Splunk 的这些系统日志事件中的 Framed_IP_Address、IpAddress、MacAddress 字段内包含实际 IP 或实际 MAC 地址。

可以使用其他实际 IP 或 MAC 地址，但是，终端必须具有处于活动状态并已进行身份验证的 IEEE 802.X 会话。

ISE EPS RESTful API 和 pxGrid 工作流程操作

以下屏幕展示了两种类别的工作流程操作

步骤 1 查看 Splunk EPS 和 pxGrid 工作流程操作
Settings -> Field -> Workflow actions

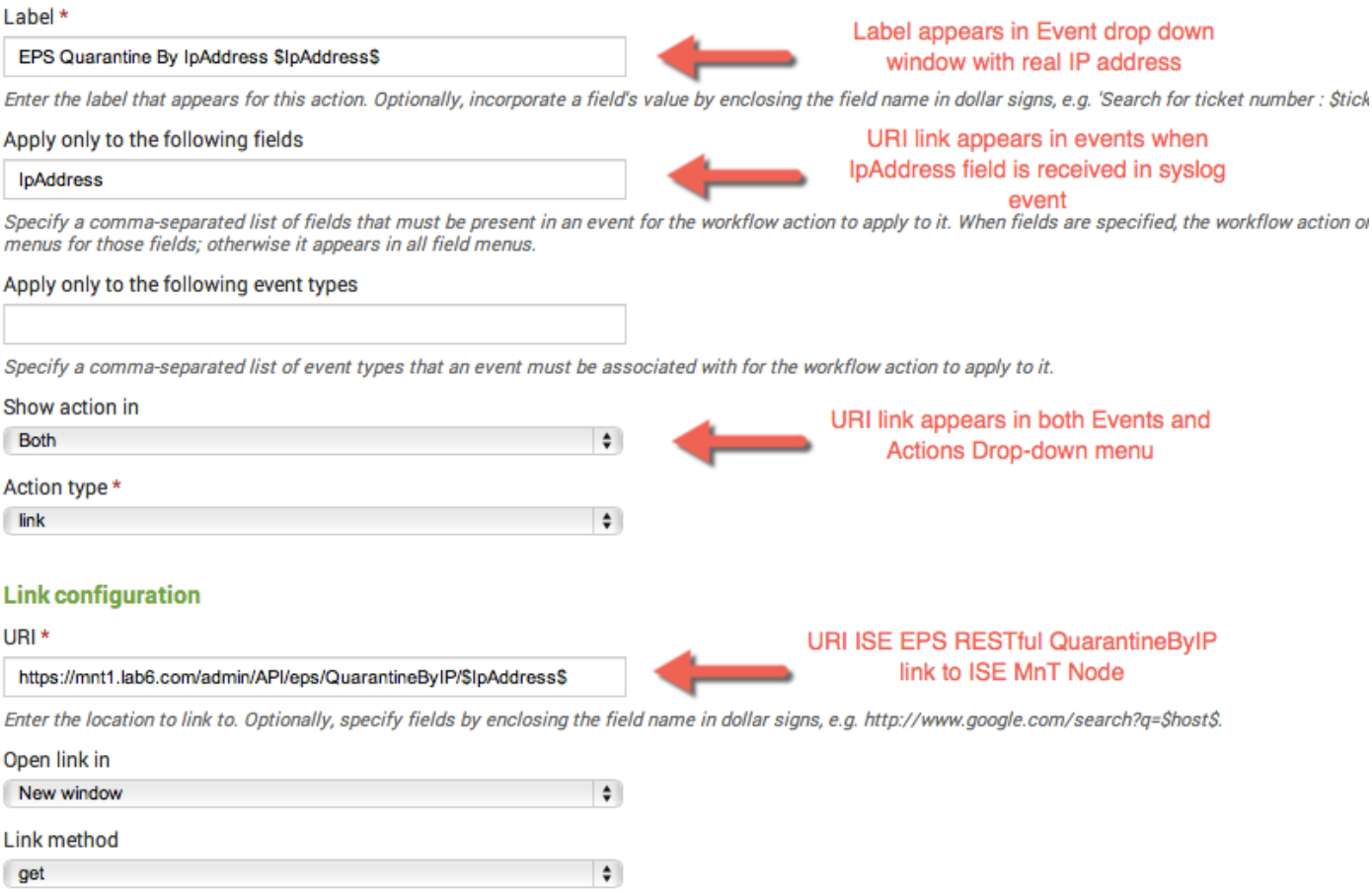


自定义 EPS RESTful API 工作流程操作

通过 IP 地址隔离

EPS 的“通过 IP 地址隔离”操作使用从以下启用 ISE 的日志记录类别收到的系统日志事件的 IpAddress 字段中或 $IpAddress$ Splunk 变量中包含的实际 IP 地址。

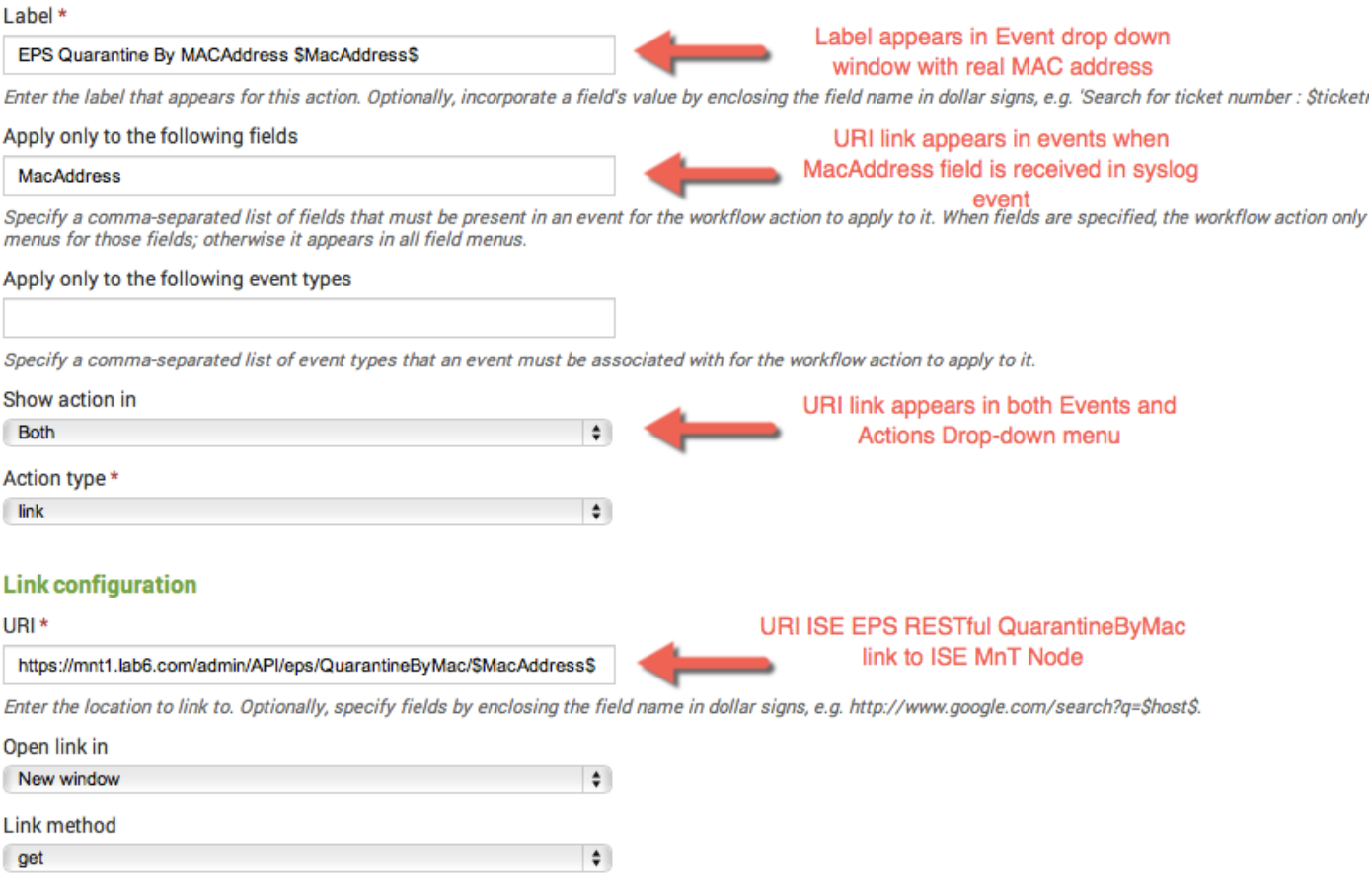
- 状态和客户端调配审核
- 通过身份验证
- 失败尝试
- 访客



通过 MAC 地址隔离

EPS 的“通过 MAC 地址隔离”操作使用从以下启用 ISE 的日志记录类别收到的系统日志事件的 MacAddress 字段中或 $MacAddress$ 变量中包含的实际 MAC 地址。

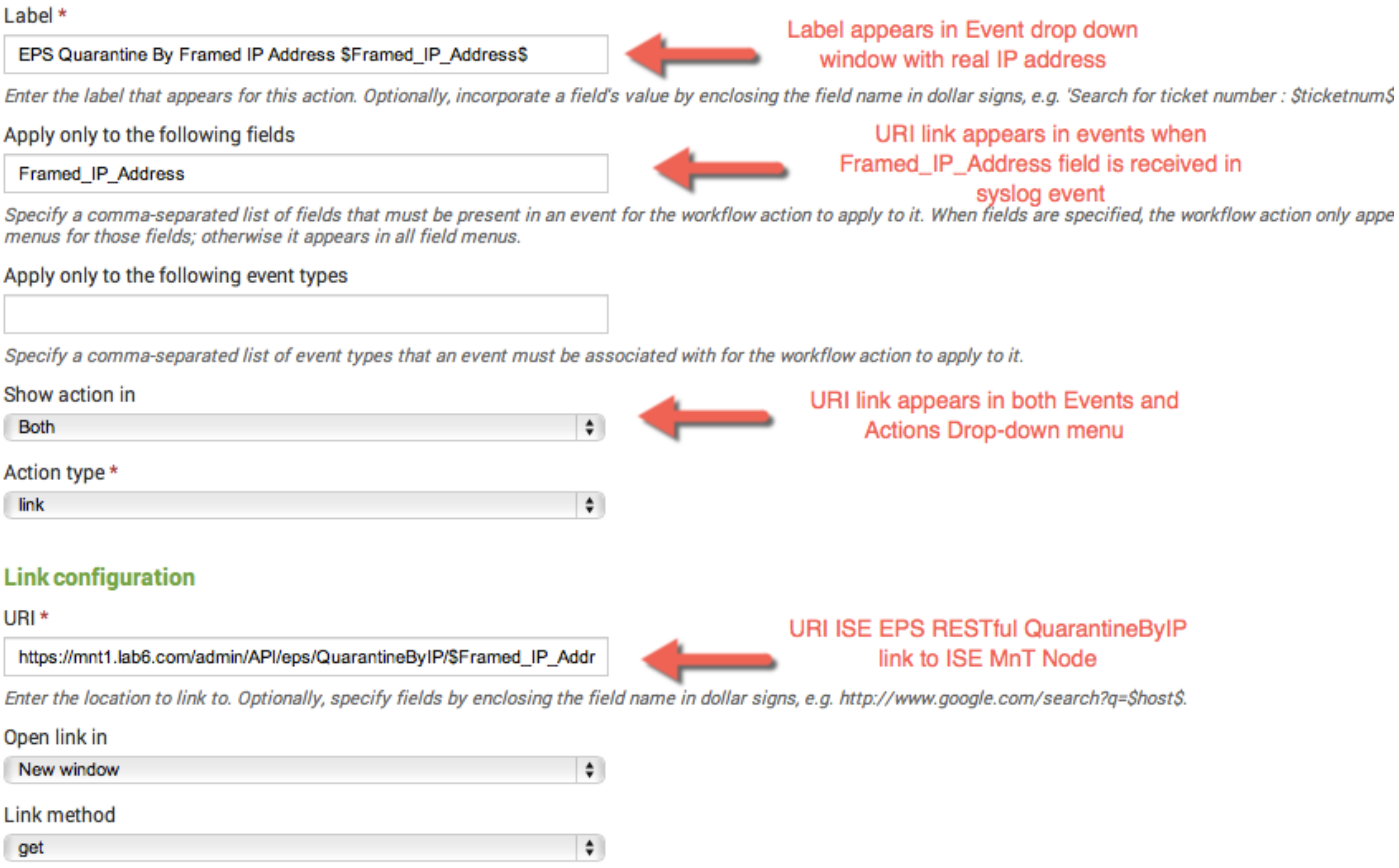
- 状态和客户端调配审核
- 通过身份验证
- 管理和业务审核
- 失败尝试
- 访客
- 分析器



通过框架 IP 地址隔离

EPS 的“通过框架 IP 地址隔离”操作使用从以下启用 ISE 的日志记录类别收到的系统日志事件的 Framed_IP_Address 字段中或 $Framed_IP_Address$ 变量中包含的实际 IP 地址。

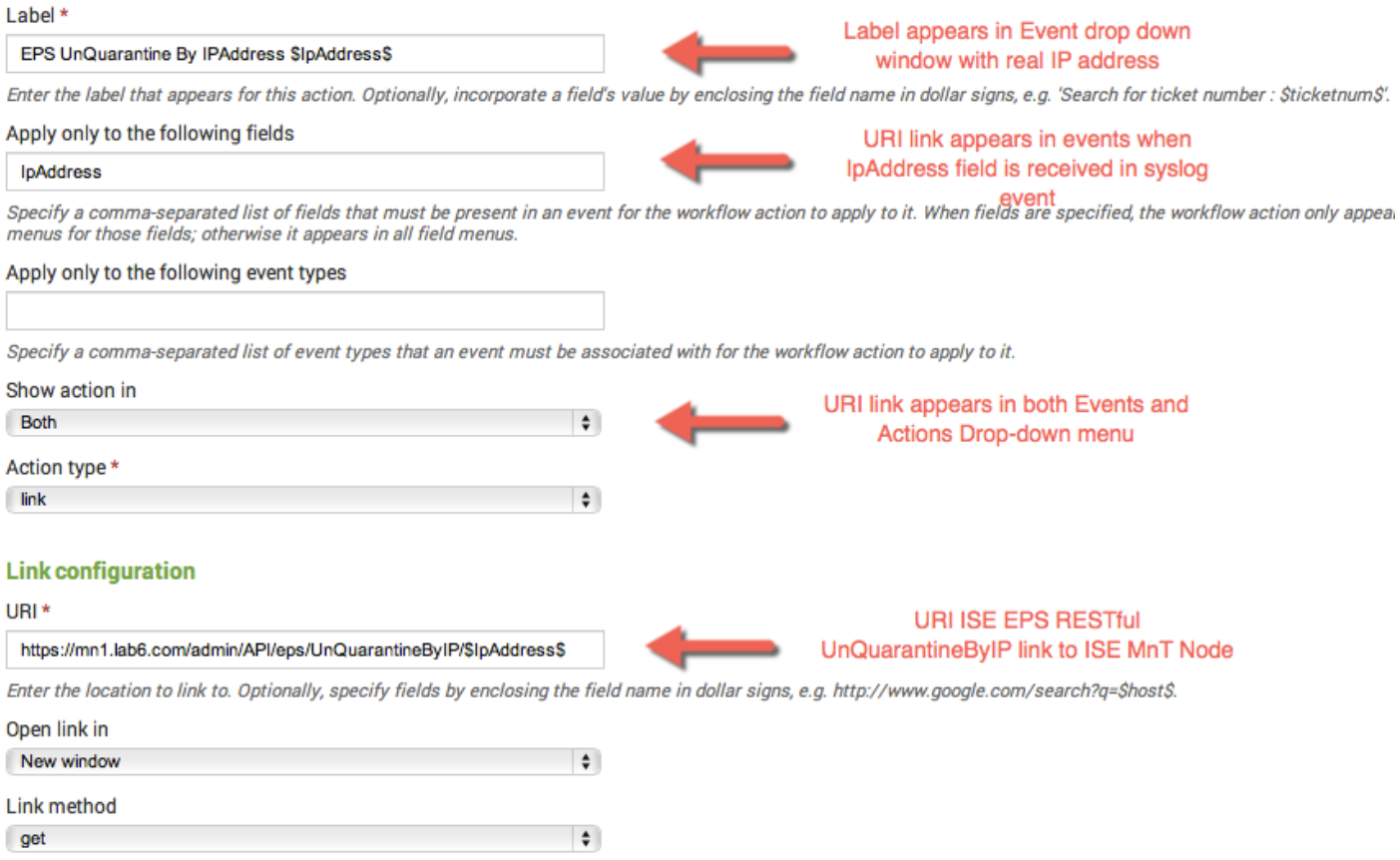
- 通过身份验证
- 失败尝试
- RADIUS 记帐
- RADIUS 诊断
- 分析器



通过 IP 地址取消隔离

EPS 的“通过 IP 地址取消隔离”操作使用从以下启用 ISE 的日志记录类别收到的系统日志事件的 IpAddress 字段中或 $IpAddress$ 变量中包含的实际 IP 地址。

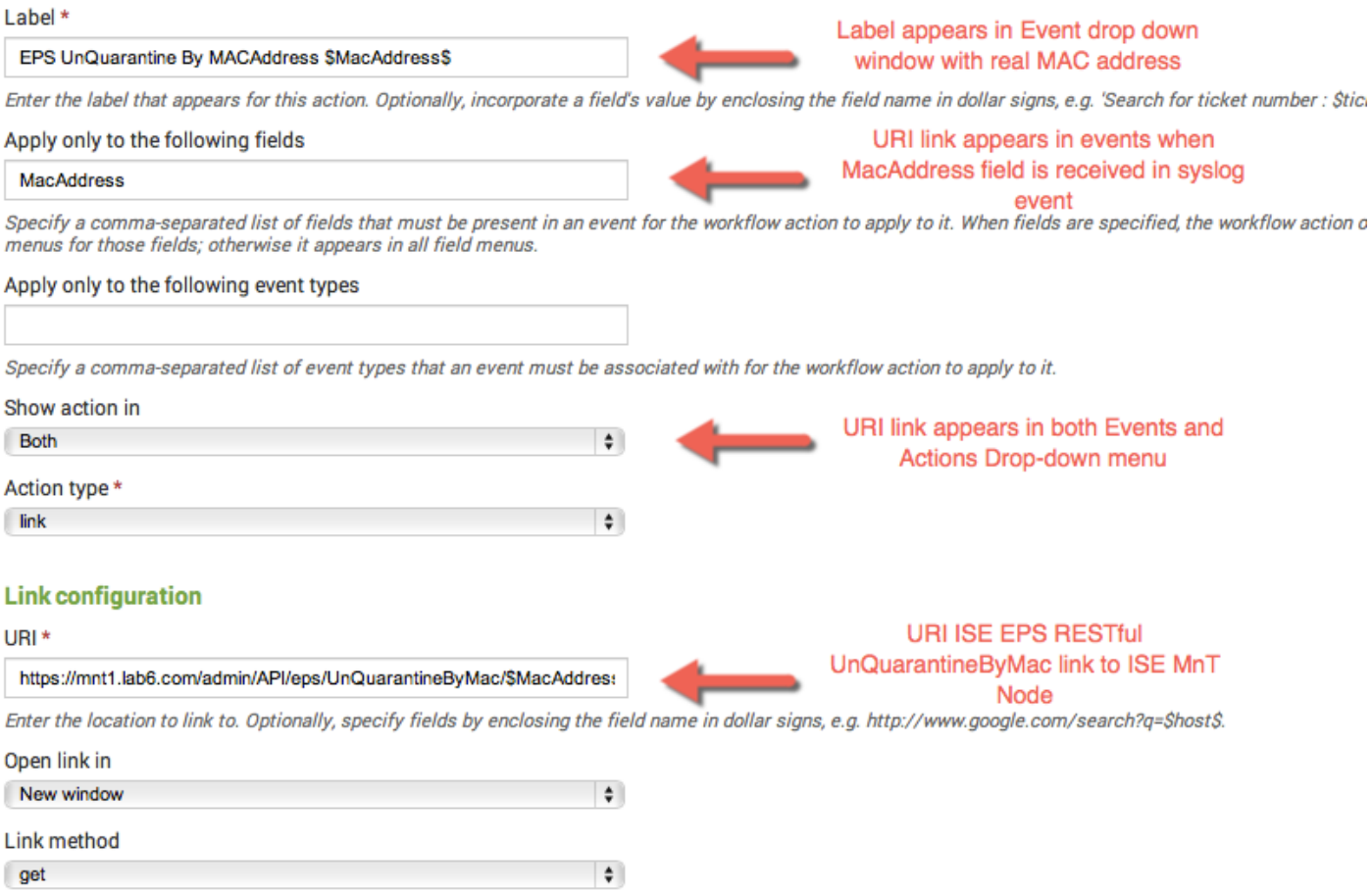
- 状态和客户端调配审核
- 通过身份验证
- 失败尝试
- 访客



通过 MAC 地址取消隔离

EPS 的“通过 MAC 地址取消隔离”操作使用从以下启用 ISE 的日志记录类别收到的系统日志事件的 MacAddress 字段中或 $MacAddress$ 变量中包含的实际 MAC 地址。

- 状态和客户端调配审核
- 通过身份验证
- 管理和业务审核
- 失败尝试
- 访客
- 分析器

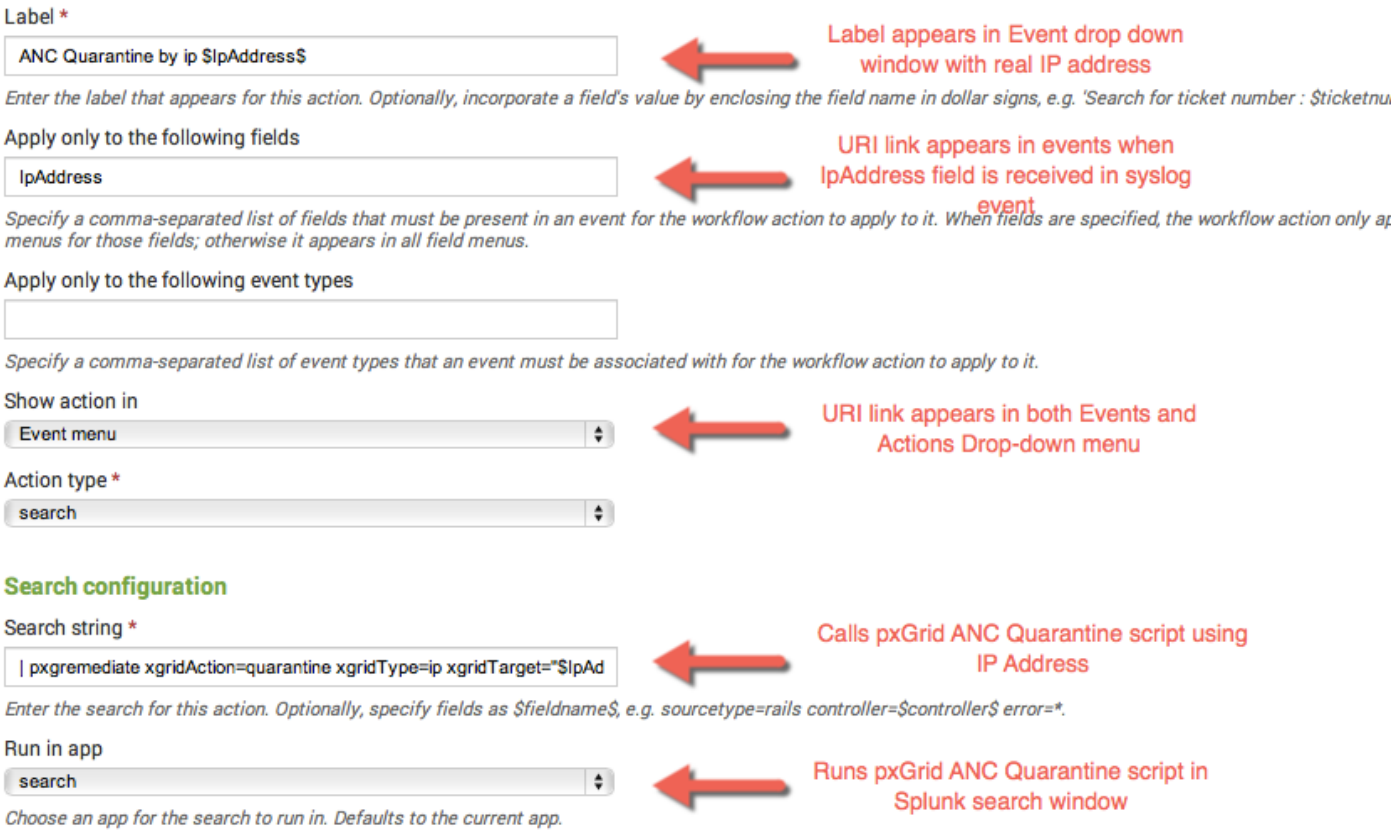


自定义 pxGrid ANC 工作流程缓解操作

ANC 的通过 IP 地址隔离操作

ANC 的“通过 IP 地址隔离”操作使用从以下启用 ISE 的日志记录类别收到的系统日志事件的 IpAddress 字段中或 $IpAddress$ 变量中包含的实际 IP 地址调用 pxGrid 脚本。

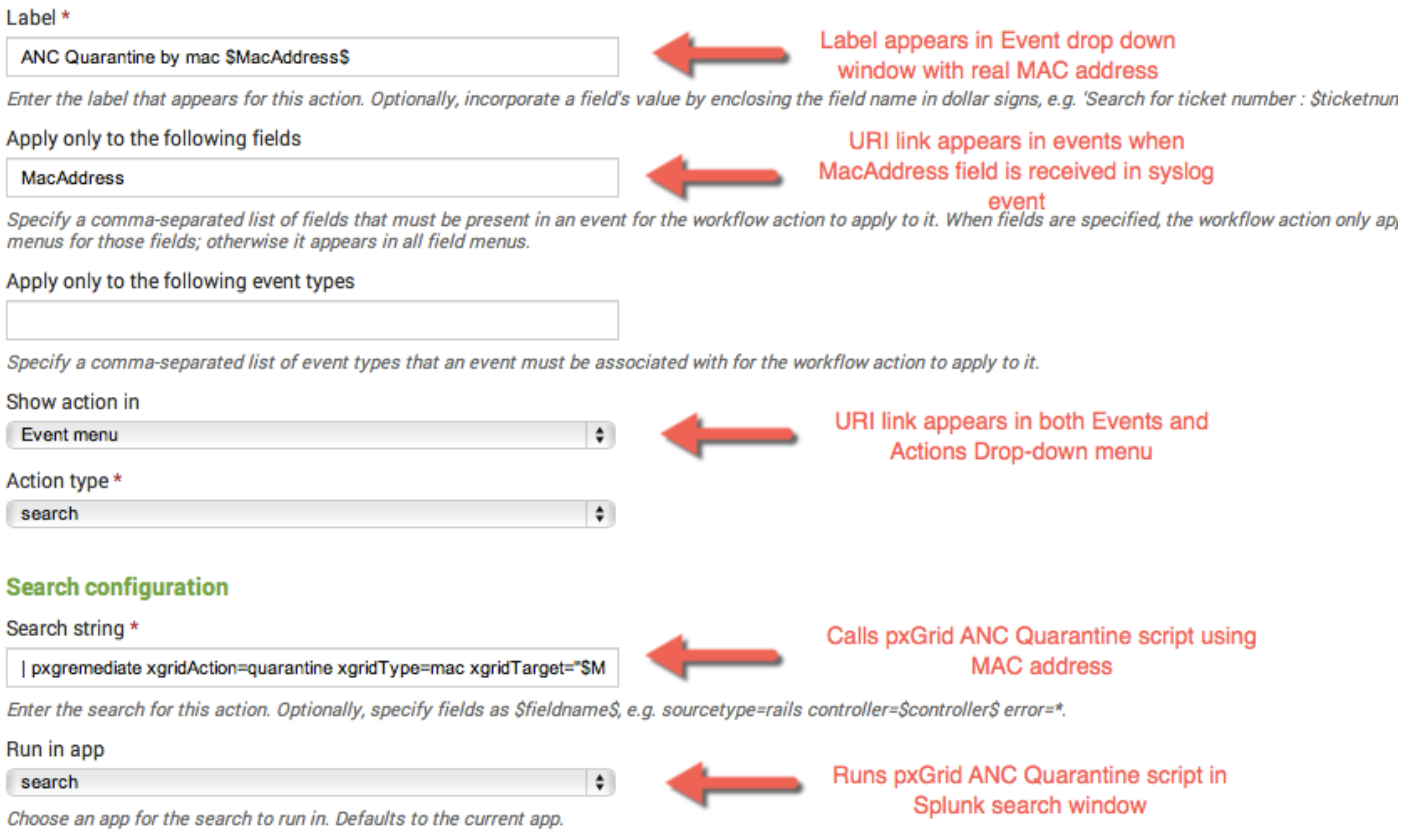
- 状态和客户端调配审核
- 通过身份验证
- 失败尝试
- 访客



ANC 的通过 MAC 地址隔离操作

ANC 的“通过 MAC 地址隔离”操作使用从以下启用 ISE 的日志记录类别收到的系统日志事件的 MacAddress 字段中或 $MacAddress$ 变量中包含的实际 MAC 地址调用 pxGrid 脚本。

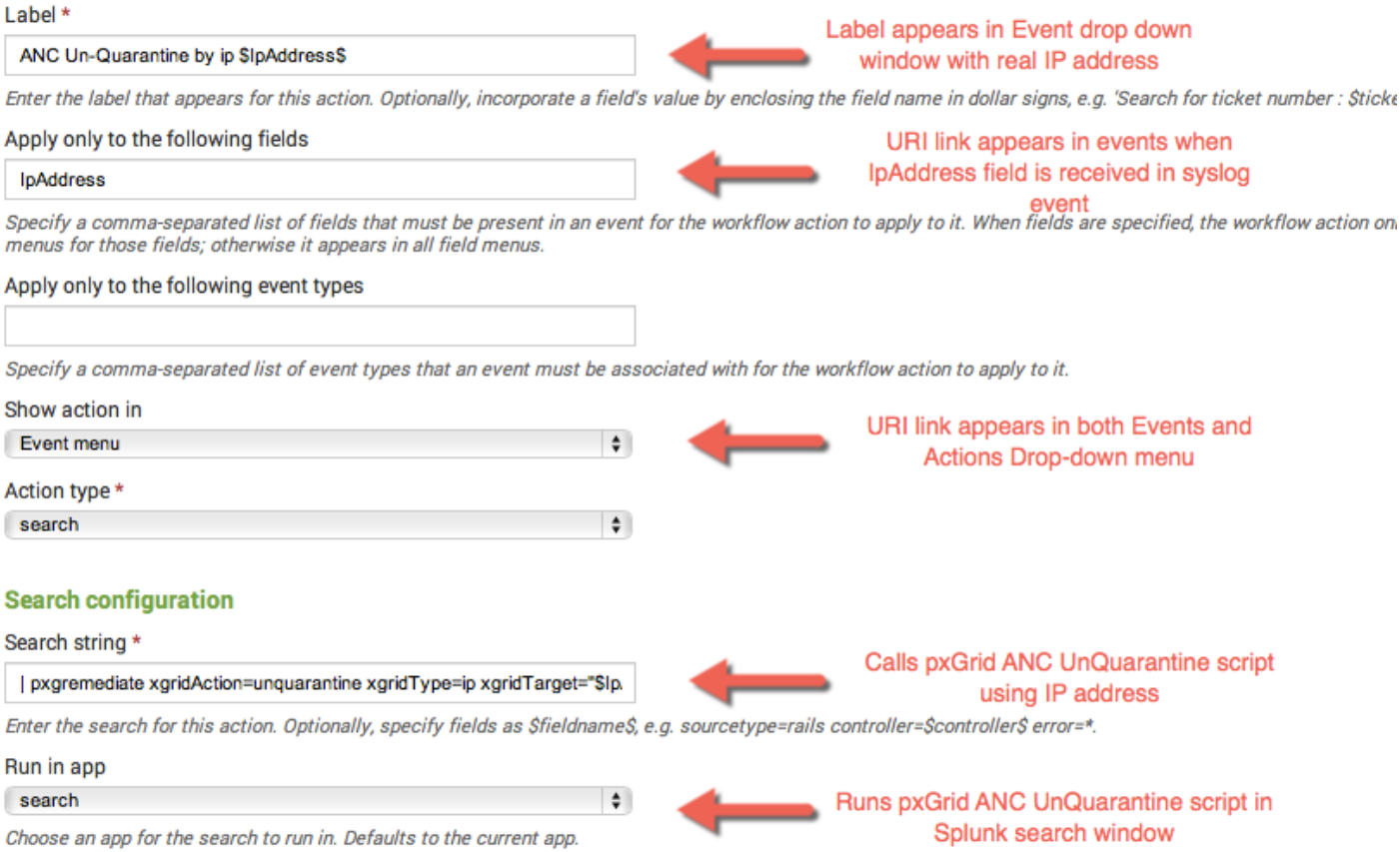
- 状态和客户端调配审核
- 通过身份验证
- 管理和业务审核
- 失败尝试
- 访客
- 分析器



ANC 的通过 IP 地址取消隔离操作

ANC 的“通过 IP 地址取消隔离”操作使用从以下启用 ISE 的日志记录类别收到的系统日志事件的 IpAddress 字段中或 $IpAddress$ 变量中包含的实际 IP 地址调用 pxGrid 脚本。

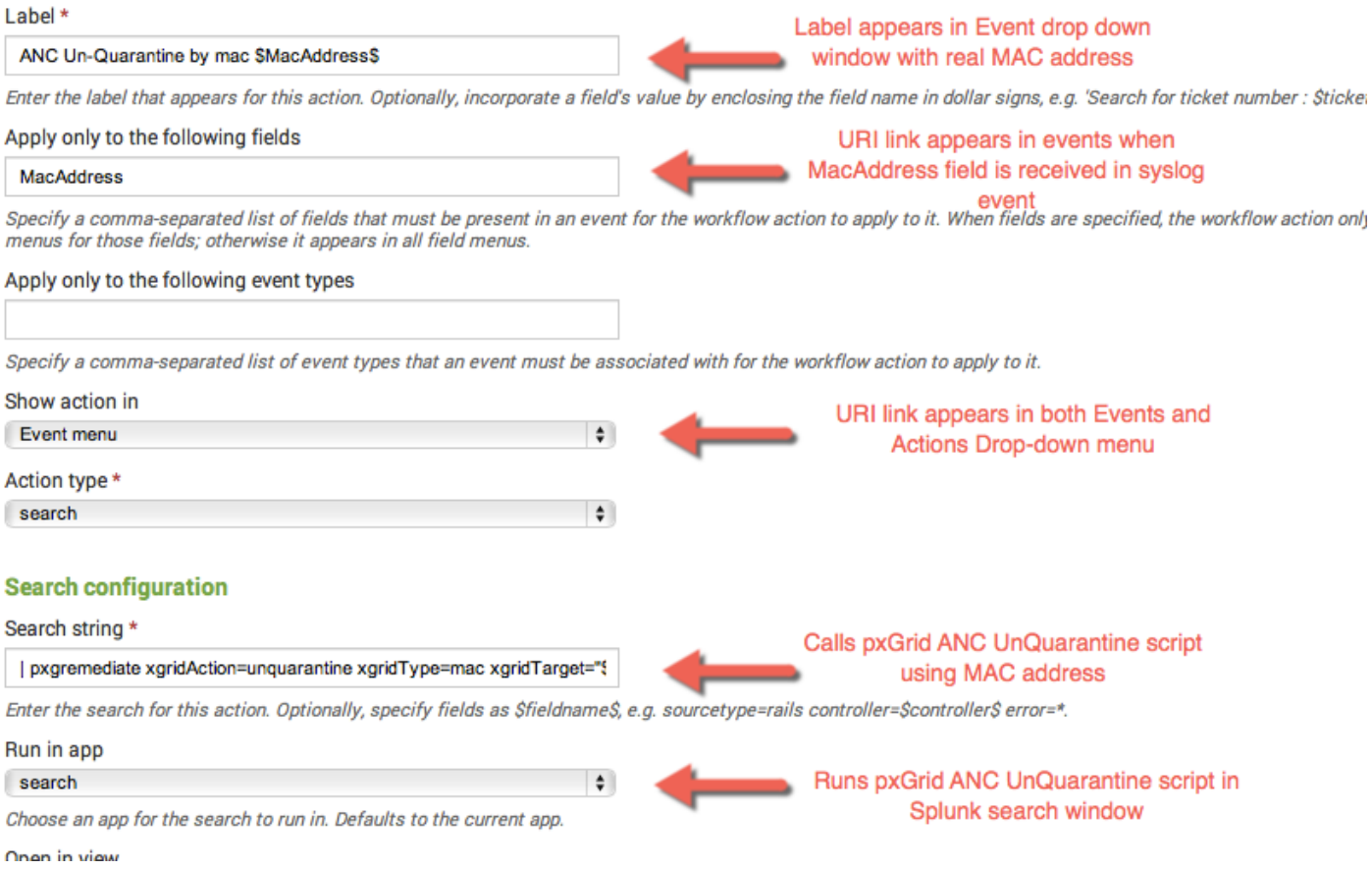
- 状态和客户端调配审核
- 通过身份验证
- 失败尝试
- 访客



ANC 的通过 MAC 地址取消隔离操作

ANC 的“通过 MAC 地址取消隔离”操作使用从以下启用 ISE 的日志记录类别收到的系统日志事件的 MacAddress 字段中或 $MacAddress$ 变量中包含的实际 MAC 地址调用 pxGrid 脚本。

- 状态和客户端调配审核
- 通过身份验证
- 管理和业务审核
- 失败尝试
- 访客
- 分析器



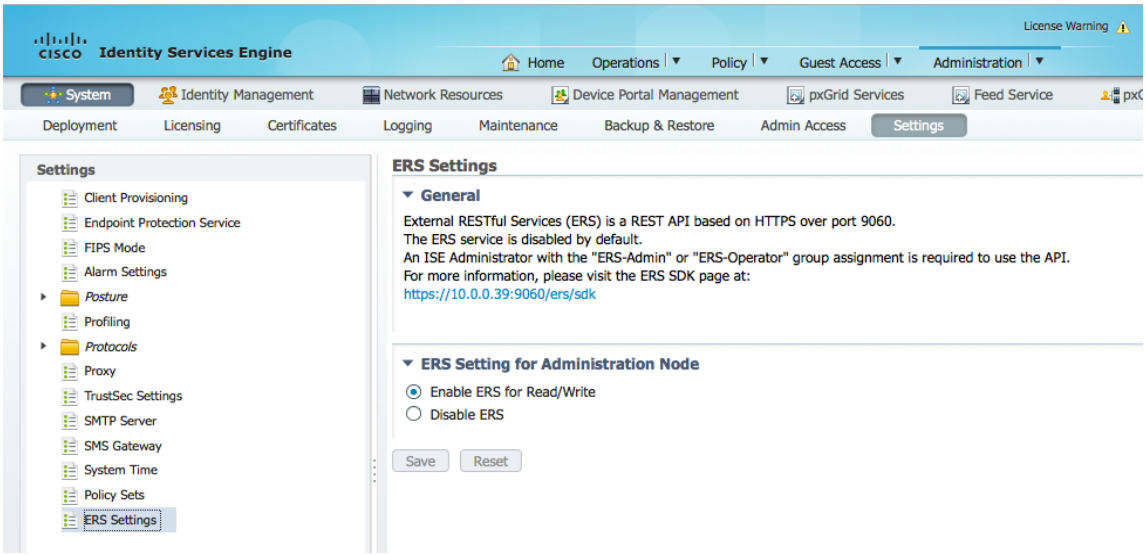
为 EPS（终端保护服务）启用 ISE

ISE 将配置为使 RESTful API 和终端保护服务能够正常工作。此外，还将创建用于隔离终端的授权配置文件。

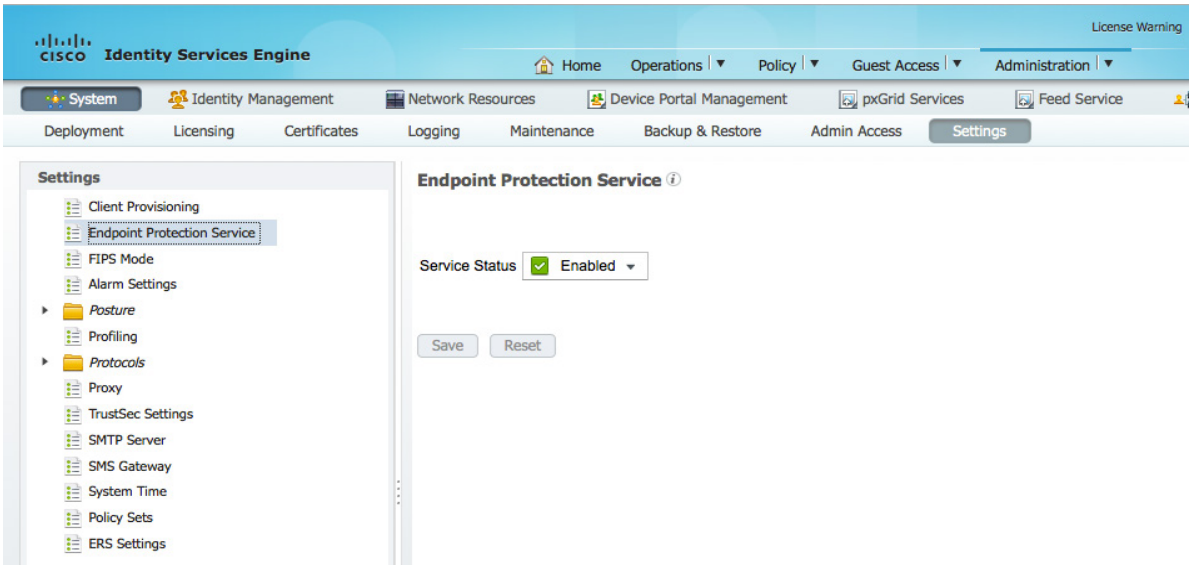
启用 ISE Restful API

步骤 1 启用 ERS 设置
Administration -> System -> Settings -> ERS Settings，然后点击 Save

注：在分布式 ISE 环境中，您还希望为所有其他节点“启用”ERS 设置



步骤 2 启用终端保护服务
Administration -> System -> Settings -> 启用 Service Status，然后点击 Save



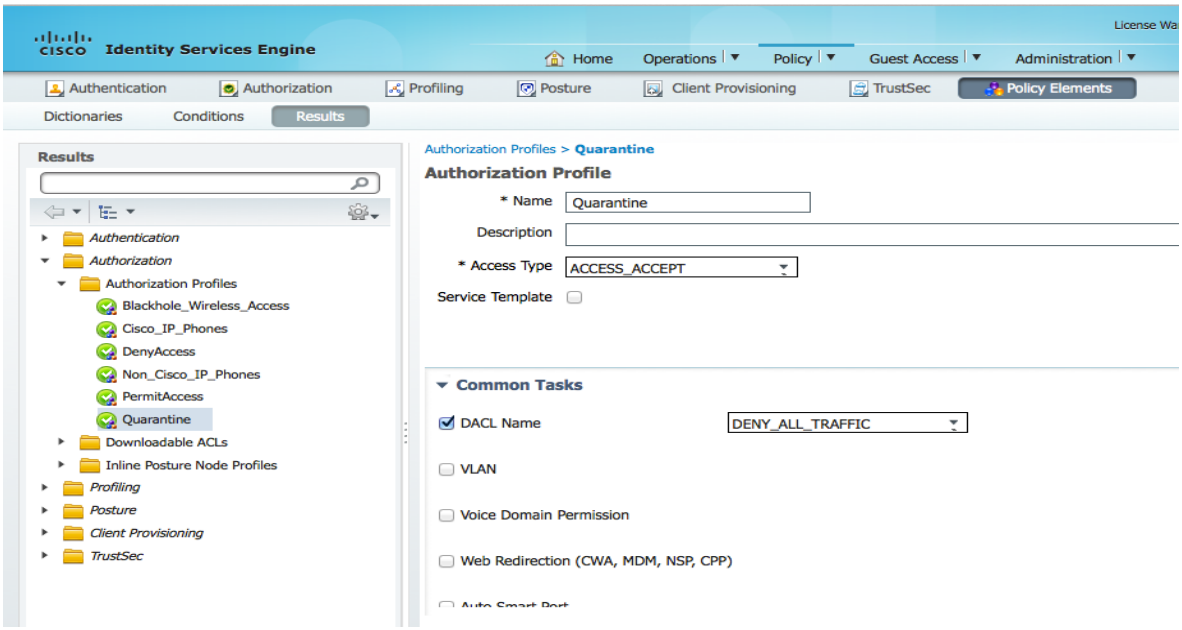
为 Quarantine 创建授权策略

在此过程中，我们将创建用于隔离终端的 EPS Quarantine 授权配置文件和授权策略。

步骤 3 创建 Quarantine 授权配置文件

Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles -> 添加 Quarantine 配置文件，然后点击 Submit

注：您可以选择 DENY 或 ALLOW 来拒绝或允许所有用于测试的流量。授权策略配置文件结果在 ISE 操作身份验证视图中仍是“Quarantine”

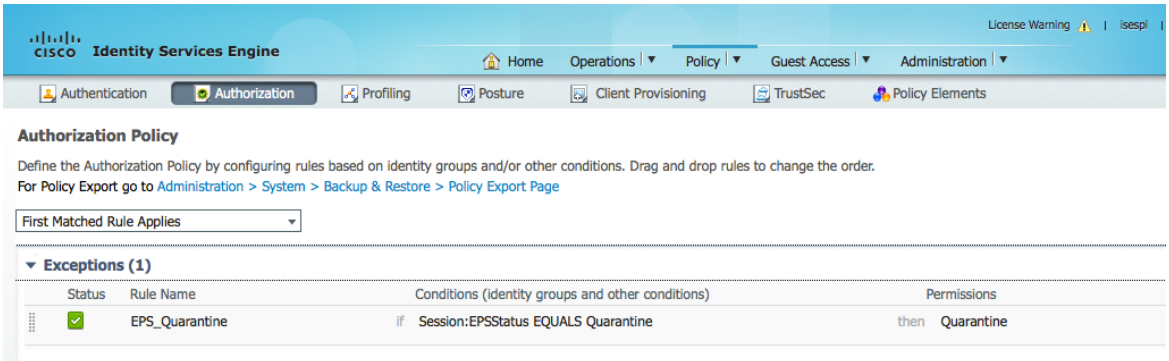


步骤 4 创建 EPS Quarantine 授权策略

Policy -> Authorization -> Exceptions 并使用以下内容创建新规则：

- 在 Rule Name 中提供名称：EPS_Quarantine
- 创建新的 Condition：Session:Equals:Quarantine
- Permissions：标准配置文件中的 Quarantine

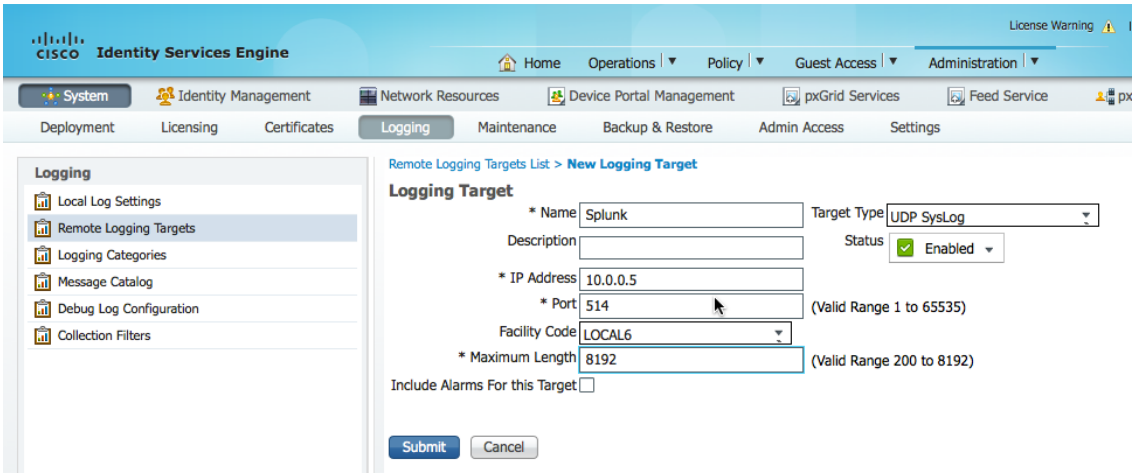
点击 -> Done -> Save



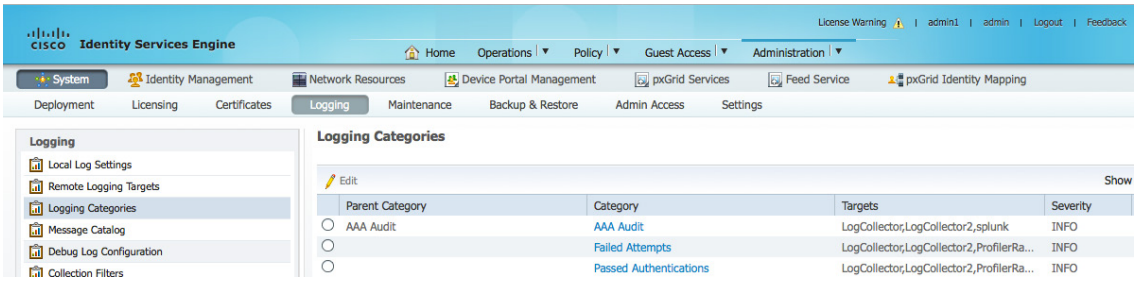
在 ISE 中配置日志记录类别

在此过程中，我们将配置 ISE 的日志记录类别

步骤 1 Administration -> System -> Logging -> Remote Logging Targets -> 添加并输入远程 Splunk 服务器设置，然后点击 Submit



步骤 2 添加远程日志记录类别
Administration -> System -> Logging -> Logging Categories -> 通过编辑选择类别并选择 Splunk 作为日志记录目标，然后保存



pxGrid 客户端 Java 密钥库简介

Java 密钥库包含诸如 CA 根证书、主机身份或 pxGrid 客户端证书、自签名证书等证书的公钥/私钥对。Java 密钥库本身为 PKCS #12 格式 (JKS)。

证书本身为 PEM 或 CER 格式，并会转换为 DER 并导入到 Java 密钥库中。

keystoreFilename 包含 JKS 格式的 pxGrid 客户端身份证书。

truststoreFilename 可以包含 JKS 格式的 CA 根证书、MnT 节点证书，以及自签名 ISE 身份证书。

注：在本例中，我们将仅对 truststoreFilename 使用 ISE 身份证书

keystorePassword 在转换为 DER 并导入到 keystoreFilename 中时包含 pxGrid 客户端身份证书的密码

truststorePassword 在转换为 DER 并导入到 truststoreFilename 中时包含 CA 根证书、MnT 节点证书和自签名 ISE 身份证书的密码。

keystoreFilename、keystorePassword、truststoreFilename、truststorePassword 在 pxGrid 脚本中用于 SASL 身份验证和连接到 pxGrid 角色。

如果采用 Splunk，则会从 pxGrid.jar 文件调用 pxGrid 脚本（例如 pxgremediate python 脚本），该文件在 Splunk 搜索栏中调用 pxGrid ANC 工作流程缓解操作。

ISE pxGrid 和 Splunk pxGrid 客户端证书生成

此部分展示了在概念验证 (POC) 环境中使用 ISE 1.3 设置 pxGrid 所需的步骤。在此过程中，我们将创建并生成适用于 Splunk 的自签名证书，并且使用自签名 ISE 身份证书执行 pxGrid 操作。ISE 是在独立环境中进行配置。

请注意，在 ISE 生产环境中，证书颁发机构 (CA) 签名的证书将用于签署 pxGrid 客户端证书和 ISE 证书，有关详细信息，请参阅：https://cisco.box.com/s/o6jt09pkvo9sew4novnnvbqyfvx63h9b。

简介

您在 Linux 或 MAC 服务器上应具有 openssl 或 keytool。如果缺少任何一项，请查阅 Linux 操作系统，了解如何安装这些文件。

作为要求，请为 Linux 操作系统下载 Oracle Java Development Kit：

http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html

要安装 Oracle Java Development Kit，必须卸载存在于系统上的旧版本 Java。

注：如果您是使用 MAC 进行测试，请参阅：https://www.java.com/en/download/help/mac_uninstall_java.xml 来卸载 Java

如果您使用的是 Centos 6.5，请参阅附录“**在 Centos 6.5 上删除 Java 并安装 JDK 8.0**”

请确保路径中包含“keytool”：

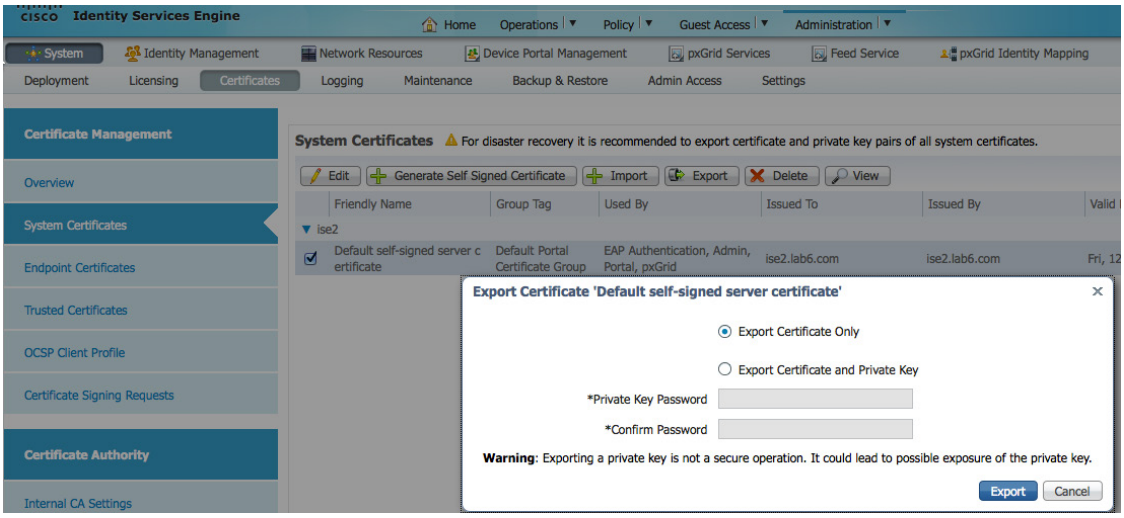
注：您必须对 Centos 64 执行上述操作

```
Append the"../jdk1.7._51/bin"to PATH

export
PATH=/usr/lib64/qt3.3/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/jeppich/bin:/usr
/java/jdk1.7.0_51/bin
```

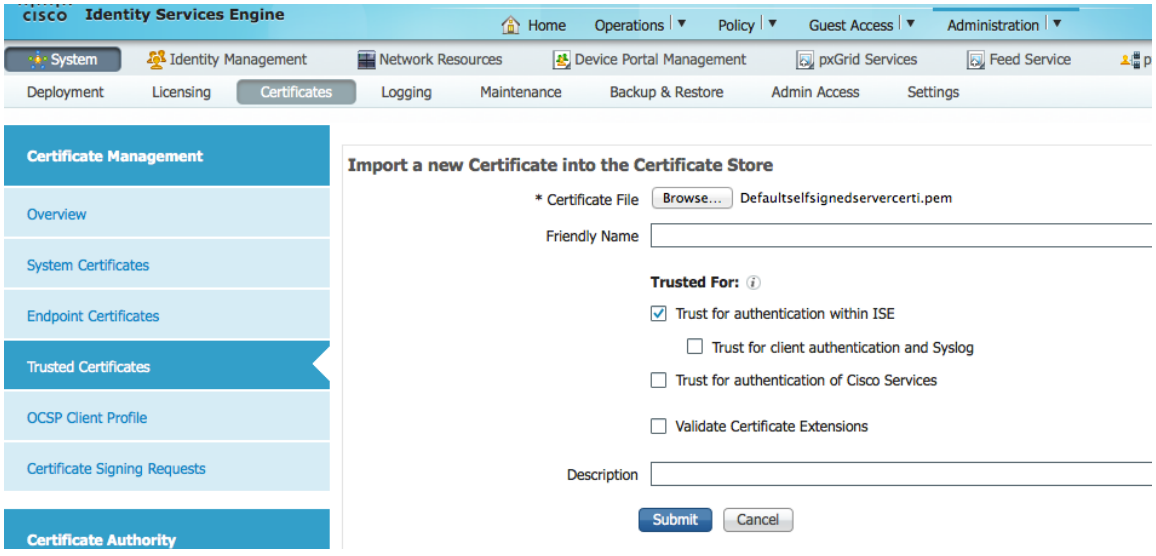
ISE pxGrid 角色配置

自签名的 ISE 身份证书将从系统证书库导出并导入到 ISE 受信任的证书库中。ISE 身份证书导入到受信任的证书库中之后，系统将会启用 ISE 节点上的 pxGrid 角色。pxGrid ISE 节点将成为主节点。

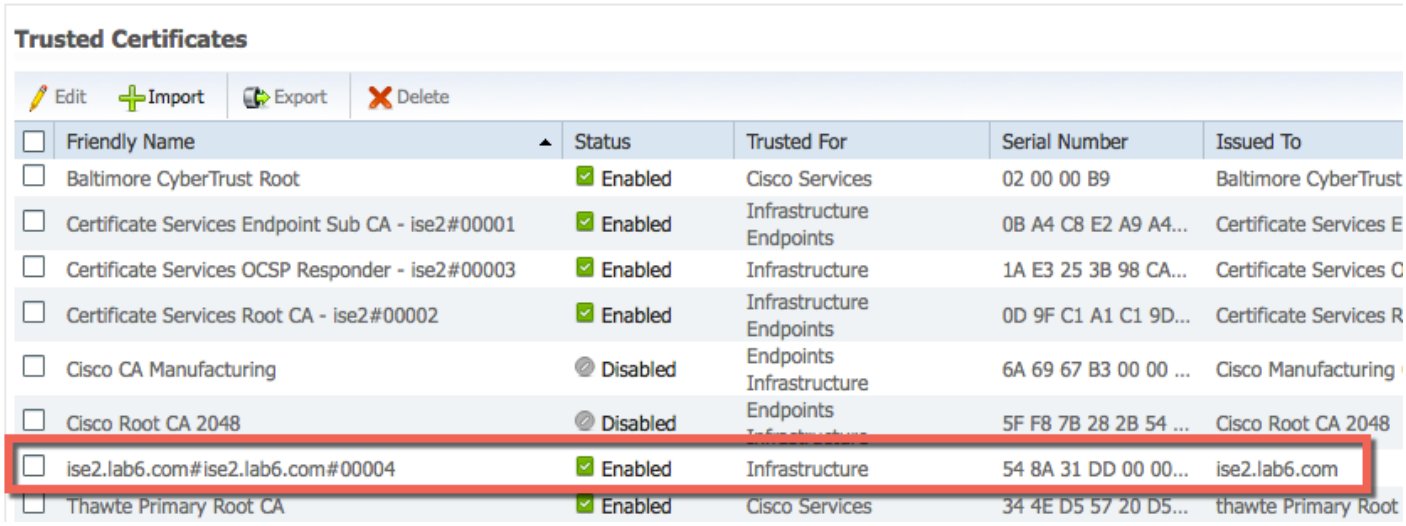
步骤 1 导出自签名的 ISE 身份证书并另存为 .pem 文件。
Administration -> System -> Certificates -> 选择 ISE 身份证书 -> Export（仅限公钥）



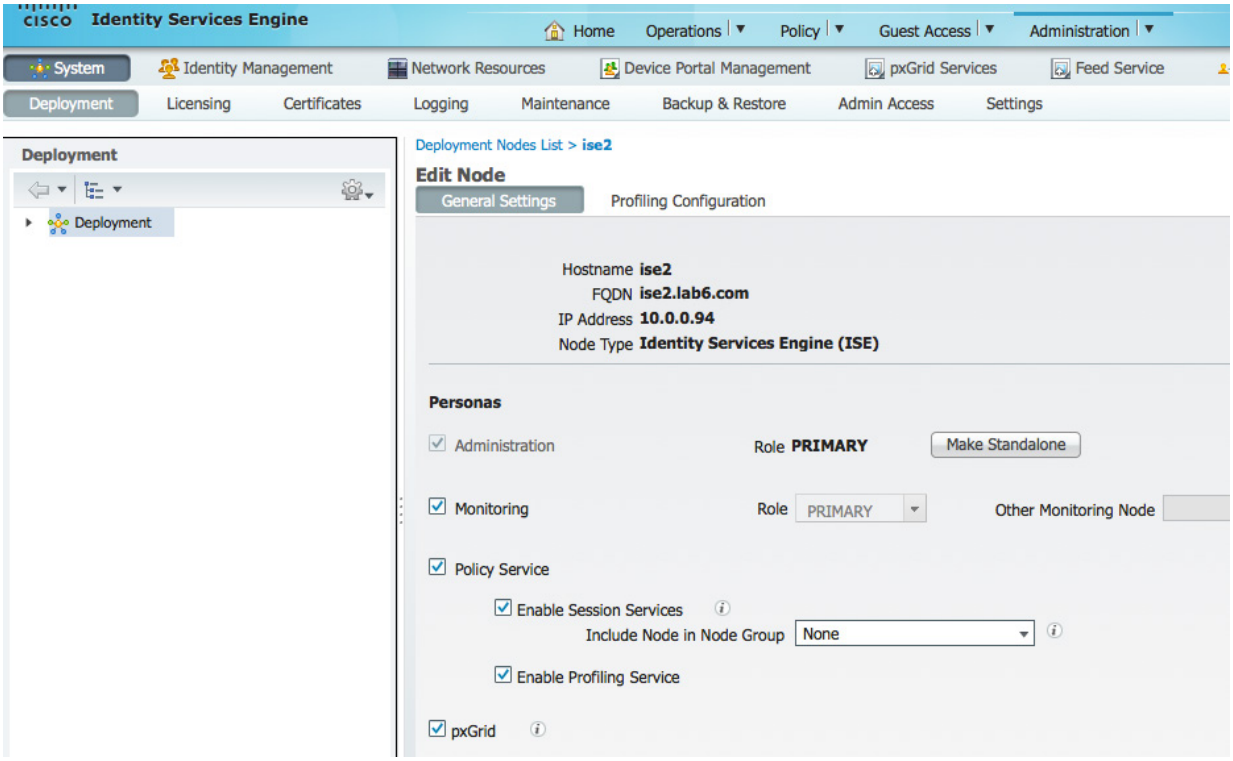
步骤 2 将已保存的 ISE .pem 文件导入到 ISE 受信任的证书库中
Administration -> System -> Certificates -> Trusted Certificates -> 浏览并上传文件 -> Submit
启用“trust for authentication within ISE”



您将在受信任的证书库中看到已导入的 ISE 身份证书

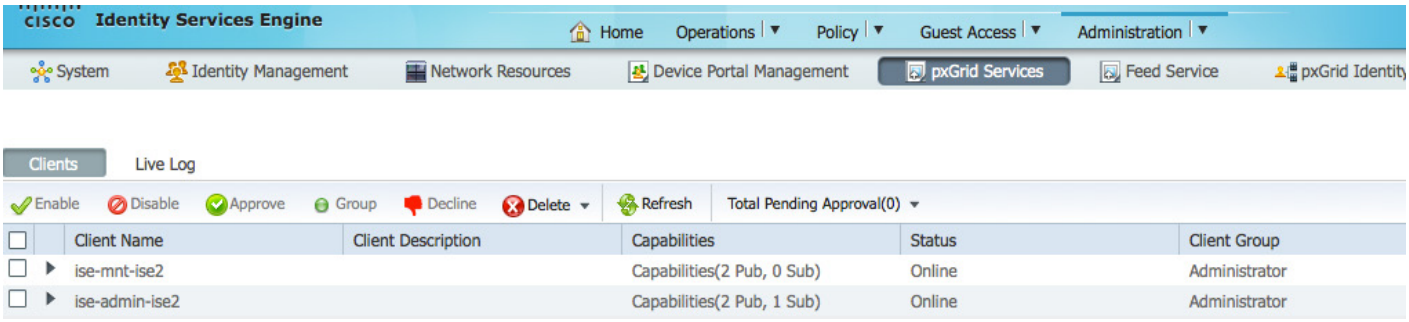


步骤 3 在 ISE 中启用 pxGrid 角色。
Administration -> System -> Deployment-> 启用 pxGrid -> 将 Role 更改为 Primary -> Save



注：无需将 Role 更改为 Primary

步骤 4 验证发布的服务是否已启动。
Administration -> pxGrid Services



注：在 ISE 发布节点出现之前，可能会有延迟。在启用 pxGrid 角色之前，必须先安装证书。

pxGrid 客户端证书配置

系统将在 pxGrid 客户端（即 Splunk）上创建并生成自签名的证书。

下面介绍了此过程：

- 为 pxGrid 客户端生成私钥（例如 mac.key）
- 根据私钥生成 CSR（证书签名请求）（例如 mac.csr）。需要稍后将用于密钥库管理的质询密钥
- 系统将根据 Linux 主机上的私钥自行生成证书 (mac.cer)
- 系统将根据公钥/私钥对和根证书创建 PKCS#12 文件 (mac.p12)。这将用于创建 keystoreFilename (JKS) 和 truststoreFilename (JKS) 的密钥库
- 系统将创建 keystoreFilename (JKS)（例如 mac.jks）
- 系统将创建 truststoreFilename (JKS)（例如 caroot1.jks）
- 从 ISE 主节点 (isemnt.pem) 导入自签名的 ISE 身份证书

注：在生产环境中，此证书将从 ISE MnT 节点导入。这还用于批量会话下载，但不在 Splunk 实施中使用。此文件还进行了重命名，以更易于处理。

- 将 ISE 身份证书 PEM 文件 (isemnt.pem) 转换为 DER 格式 (isemnt.der) 并添加到 keytoreFileName 密钥库（例如 mac.jks）
- 将 pxGrid 客户端证书（例如 mac.cer）导入到 keystoreFilename (JKS) 中（例如 mac.jks）
- 将 ISE 身份证书（例如 isemnt.der）导入到 truststoreFilename (JKS) 中（例如 caroot1.jks）
- 将 keystoreFilename (mac.jks) 和 truststoreFilename (caroot1.jks) 文件均复制到 SPLUNK 目录（例如 /Applications/splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs 文件夹）中

步骤 1 为 pxGrid 客户端生成私钥（例如 mac.key）

```
openssl genrsa -out mac.key 4096

Generating RSA private key, 4096 bit long modulus
..................++
..............................++
e is 65537 (0x10001)
```

步骤 2 生成自签名的 CSR (mac.csr) 请求并提供质询密码（例如 cisco123）

注：质询密码将成为 keystoreFilename 密码

```
openssl req -new -key mac.key -out mac.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:cisco123
An optional company name []:
```

注：在本文档各处使用相同的密码可便于维护，并减少错误

步骤 3 生成自签名的证书公钥/私钥对证书（例如 mac.cer）

```
openssl req -x509 -days 365 -key mac.key -in mac.csr -out mac.cer
```

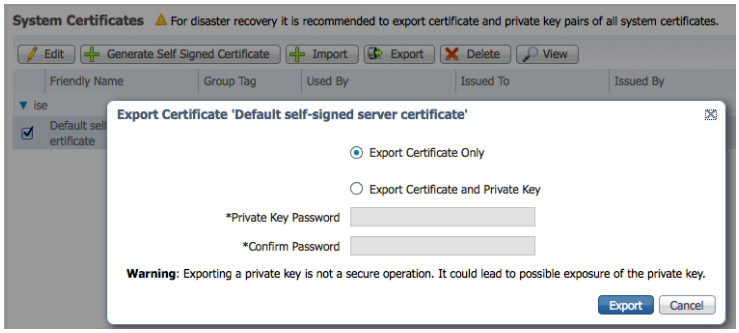
步骤 4 系统将根据私钥创建 PKCS12 文件（例如 mac.p12）。

```
openssl pkcs12 -export -out mac.p12 -inkey mac.key -in mac.cer

Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
```

步骤 5 mac.p12 将导入到身份密钥库（例如 mac.jks）中。这可以是扩展名为 .jks 的随机文件名。这将在 pxGrid 脚本中充当 keystoreFilename 和关联的 keystorePassword。

```
keytool -importkeystore -srckeystore mac.p12 -destkeystore mac.jks -srcstoretype PKCS12

Enter destination keystore password: cisco123
Re-enter new password: cisco123
Enter source keystore password: cisco123
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
```

步骤 6 仅将公共 ISE 身份证书导出到 pxGrid 客户端中，请注意导出文件将采用 .pem 格式。可以重命名扩展名为 .pem 的文件以使其更易于读取，在本例中该文件重命名为 isemnt.pem。



步骤 7 将 .pem 文件转换为 .der 格式。

```
openssl x509 -outform der -in isemnt.pem -out isemnt.der
```

步骤 8 将 ISE 身份证书添加到 keystoreFilename。

```
keytool -import -alias mnt1 -keystore mac.jks -file isemnt.der

Enter keystore password: cisco123
Owner: CN=ise.lab6.com
Issuer: CN=ise.lab6.com
Serial number: 548502f500000000ec27e53c1dd64f46
Valid from: Sun Dec 07 17:46:29 PST 2014 until: Mon Dec 07 17:46:29 PST 2015
Certificate fingerprints:
         MD5: 04:7D:67:04:EC:D2:F5:BC:DC:79:4D:0A:FF:62:09:FD
         SHA1: 5A:7B:02:E4:07:A1:D2:0B:7D:A5:AE:83:27:3B:E7:33:33:30:1E:32
         SHA256:
C4:21:6C:6F:5B:06:F3:2C:D7:26:35:CB:BE:2B:1B:FF:0E:EE:09:91:F6:B6:54:0C:6F:63:CB:43:1F:77:F2:37
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
```

```
  serverAuth
  clientAuth
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_Encipherment
  Key_Agreement
  Key_CertSign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL server
]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: C4 F3 1A 9E 7B 1B 14 4F   51 9E A4 88 33 07 7A AC  .......OQ...3.z.
0010: 75 37 36 D4                                        u76.
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
Johns-MacBook-Pro:bin jeppich$
```

步骤 9　将 pxGrid 客户端证书导入到 keystoreFilename 中。

```
keytool -import -alias pxGridclient -keystore mac.jks -file mac.cer

Enter keystore password:
Certificate already exists in keystore under alias <1>
Do you still want to add it? [no]: n
Certificate was not added to keystore
```

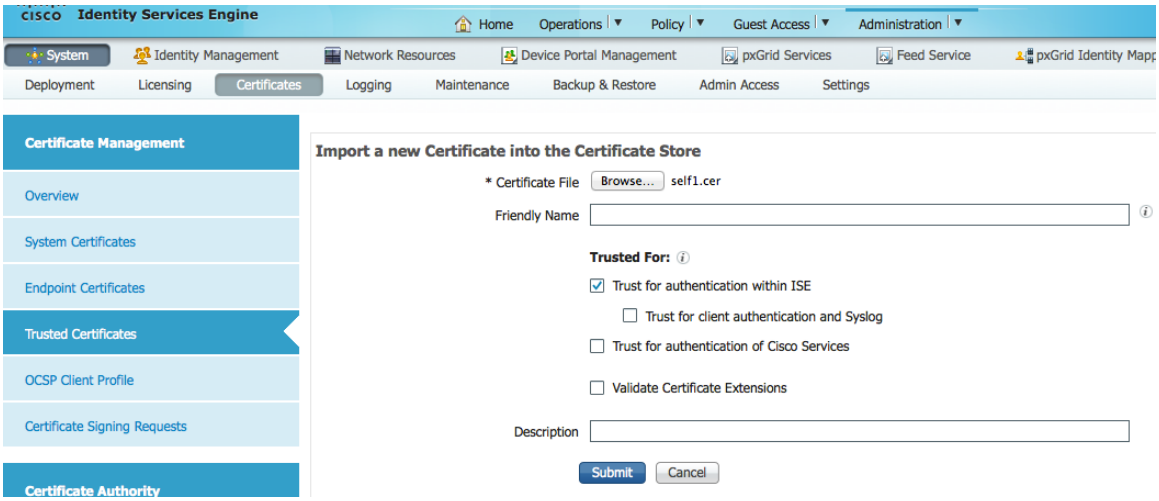
注：如果收到以下消息，表示证书已添加到已有的密钥库，选择“no”也没有问题。我选择了“yes”，以便我们可以在稍后添加证书后进行验证。

步骤 10　将 ISE 身份证书导入到 truststoreFilename（例如 caroot1.jks），后者在 pxGrid 脚本中充当 truststoreFilename 和 truststorePassword。

```
keytool -import -alias root -keystore caroot1.jks -file isemnt.der
Enter keystore password:  cisco123
Re-enter new password:  cisco123
Owner: CN=ise.lab6.com
Issuer: CN=ise.lab6.com
Serial number: 548502f500000000ec27e53c1dd64f46
Valid from: Sun Dec 07 17:46:29 PST 2014 until: Mon Dec 07 17:46:29 PST 2015
Certificate fingerprints:
         MD5:  04:7D:67:04:EC:D2:F5:BC:DC:79:4D:0A:FF:62:09:FD
         SHA1: 5A:7B:02:E4:07:A1:D2:0B:7D:A5:AE:83:27:3B:E7:33:33:30:1E:32
```

```
        SHA256:
C4:21:6C:6F:5B:06:F3:2C:D7:26:35:CB:BE:2B:1B:FF:0E:EE:09:91:F6:B6:54:0C:6F:63:CB:43:1F:77:F2:37
        Signature algorithm name: SHA1withRSA
        Version: 3

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_Encipherment
  Key_Agreement
  Key_CertSign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL server
]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: C4 F3 1A 9E 7B 1B 14 4F   51 9E A4 88 33 07 7A AC  .......OQ...3.z.
0010: 75 37 36 D4                                        u76.
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

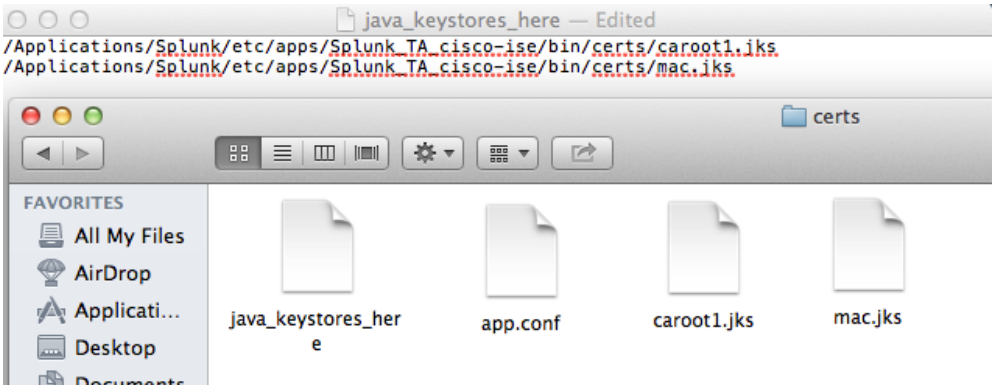
步骤 11 将 pxGrid 客户端公共证书 (mac.cer) 上传到 ISE 受信任的证书库中。
Administration -> System Certificates -> Trusted Certificates -> 从 pxGrid 客户端上传 mac.cer



步骤 12 将身份 keystoreFilename (mac.jks) 和 truststoreFilename (caroot1.jks) 复制到 /Applications/splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs 文件夹中

注：路径与 Splunk 的安装位置有关

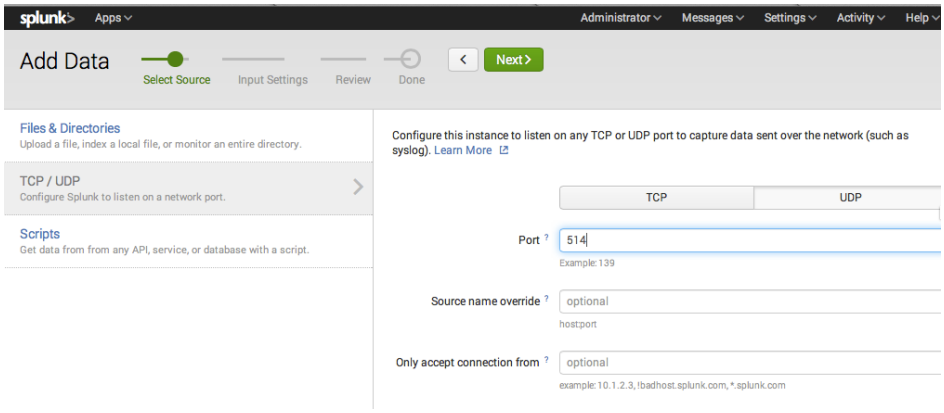
步骤 13 编辑 java_keystores_here 文件并包含 truststoreFilename 和 keystoreFilename 的路径



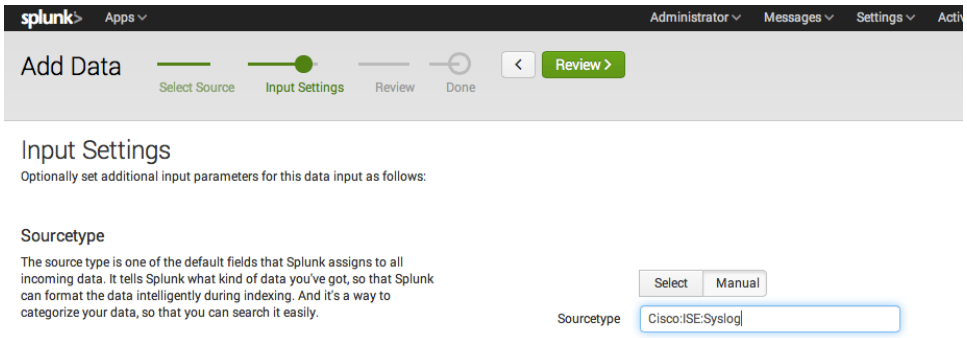
将 Splunk 配置为从 ISE 接收系统日志事件

下面详细介绍 Splunk 用于接收事件的初始配置，其中使用了 Splunk Enterprise 6.2。如果您使用的是 Splunk Enterprise 6.1，请设置为手动接收。

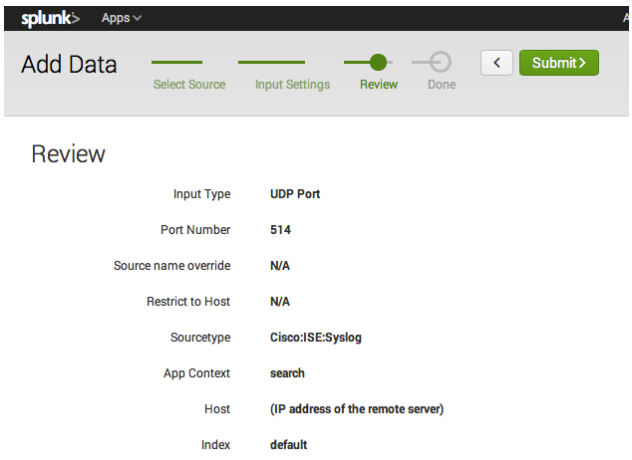
步骤 1 Splunk -> Settings -> Data Inputs -> UDP -> New 并选择可用端口，然后点击 Next



步骤 2 选择“Manual”，然后输入：Cisco:ISE:Syslog



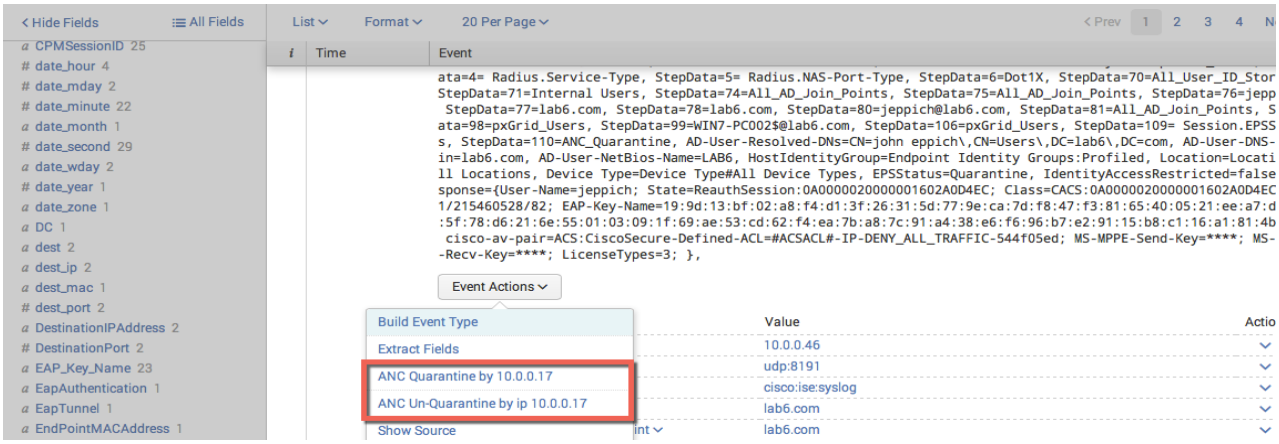
步骤 3 选择 -> Review -> Submit -> Done



Splunk pxGrid ANC 测试

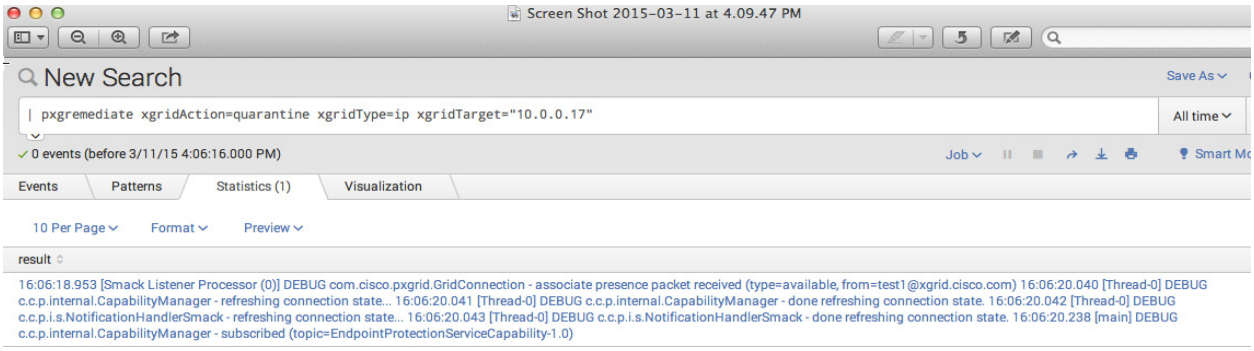
在本例中，我们将启用 ISE 的“通过身份验证”ISE 远程日志记录类别，并将这些系统日志事件发送到 Splunk。我们将修改 pxGrid_Quarantine 和 pxGrid_UnQuarantine 工作流程操作，以包含 $Framed_IP_Address$ 变量。

当 IEEE 802.1X 身份验证成功时，将在 Splunk 中触发系统日志事件。然后，我们将在 Splunk 中搜索事件，并且从 Event 下拉窗口中发出 ANC pxgrid_Quarantine by IP 操作请求。

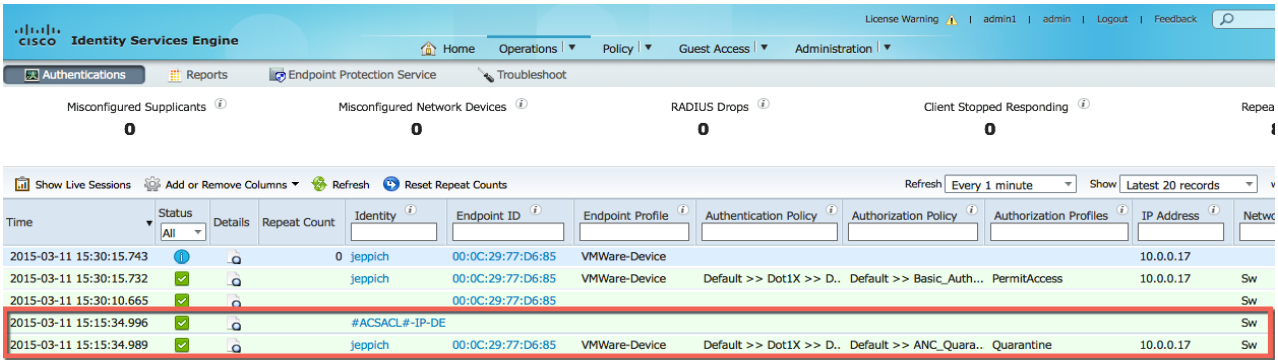


选择“ANC Un-Quarantine by IP”工作流程操作

您应该看到以下内容：

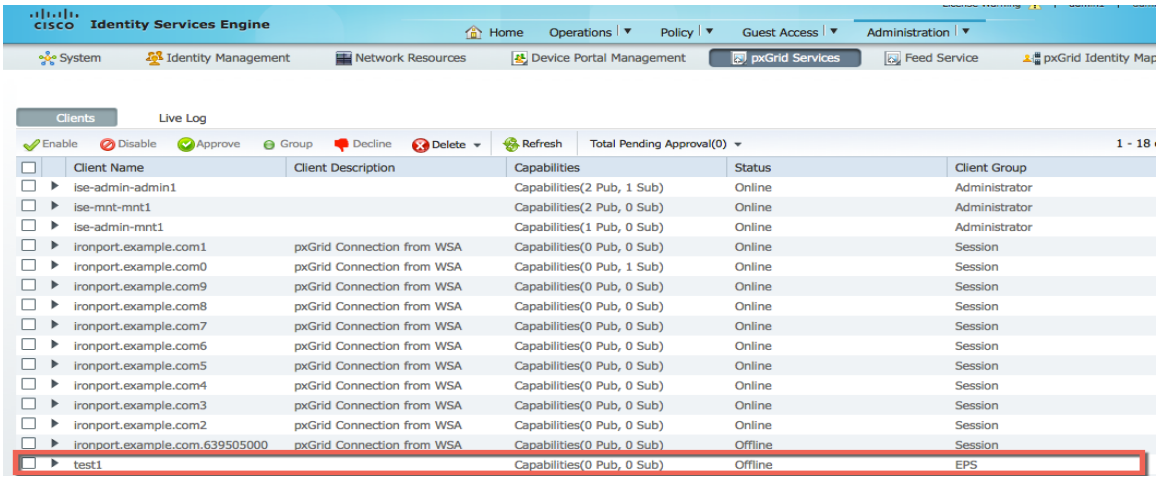


如果您在 ISE 中查阅 Operations -> Events，则应该看到终端已隔离

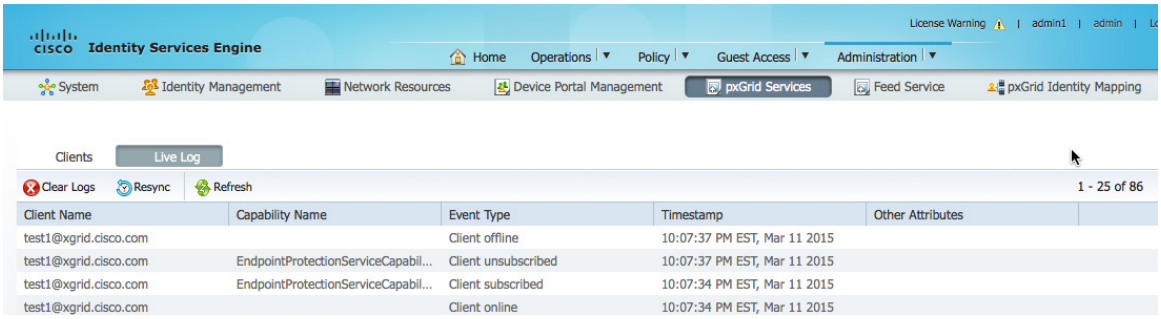


pxGrid 操作

启动 pxGrid 工作流程后，您应该看到 Splunk 按照 Splunk pxGrid 设置中的“username”的指示注册为 pxGrid 客户端



pxGrid 客户端还将订用终端保护功能，以调用隔离缓解操作



故障排除

无法连接到 ISE pxGrid 节点

确保 Splunk 服务器的 FQDN 可通过 ISE 解析 DNS

检查 keystoreFilename 和密码

- 确保您具有正确的 keystoreFilename 和 truststoreFilename 路径
- 在 Linux 命令行上运行 Splunk 搜索字符串以帮助诊断问题

  如果您看到以下内容：

```
java -jar /Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/lib/pxGrid_Search.jar pxGrid1.lab6.com test1
/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/mac.jks cisco123
/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/caroot1.jks cisco123 10.0.0.17 quarantine_ip
17:46:53.596 [Smack Listener Processor (0)] DEBUG com.cisco.pxgrid.GridConnection - associate presence packet
received (type=available, from=test1@xgrid.cisco.com)
17:46:55.266 [Thread-0] DEBUG c.c.p.internal.CapabilityManager - refreshing connection state...
17:46:55.273 [Thread-0] DEBUG c.c.p.internal.CapabilityManager - done refreshing connection state.
17:46:55.290 [Thread-0] DEBUG c.c.p.i.s.NotificationHandlerSmack - refreshing connection state...
17:46:55.291 [Thread-0] DEBUG c.c.p.i.s.NotificationHandlerSmack - done refreshing connection state.
17:46:55.502 [main] DEBUG c.c.p.internal.CapabilityManager - subscribed
(topic=EndpointProtectionServiceCapability-1.0)
```

  这意味着 pxGrid 隔离操作已成功

检查 Splunk pxGrid 日志文件

日志文件可以位于“/Applications/splunk/var/log/splunk/pxgridremediate.log”或 Splunk 的安装路径中。

下面的详细信息表明已通过 Splunk pxGrid_unQuarantine_by_IP 工作流程操作成功对终端取消隔离

```
2015-03-11 23:20:51,662 [016929] INFO     root:  Logger Initialized
2015-03-11 23:20:52,084 [016929] INFO     root:
item=pxGrid1.lab6.com|test1|/Applications/Splunk/etc/apps/Splunk_TA_cisco-
ise/bin/certs/mac.jks|/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/caroot1.jks|
2015-03-11 23:20:52,084 [016929] INFO     root:  xgridHostname=pxGrid1.lab6.com
2015-03-11 23:20:52,084 [016929] INFO     root:  xgridUsername=test1
2015-03-11 23:20:52,084 [016929] INFO     root:
keystoreFilename=/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/mac.jks
2015-03-11 23:20:52,084 [016929] INFO     root:
truststoreFilename=/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/caroot1.jks
2015-03-11 23:20:52,411 [016929] INFO     root:  keystorePassword=<password />
2015-03-11 23:20:52,411 [016929] INFO     root:  truststorePassword=<password />
2015-03-11 23:20:52,411 [016929] INFO     root:  xgridAction=unquarantine
2015-03-11 23:20:52,411 [016929] INFO     root:  xgridType=ip
2015-03-11 23:20:52,411 [016929] INFO     root:  xgridTarget=10.0.0.17
2015-03-11 23:20:52,411 [016929] INFO     root:  LAUNCHING: java -jar
/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/lib/pxGrid_Search.jar pxGrid1.lab6.com test1
/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/mac.jks cisco123
/Applications/Splunk/etc/apps/Splunk_TA_cisco-ise/bin/certs/caroot1.jks cisco123 10.0.0.17 unquarantine_ip
2015-03-11 23:21:08,792 [016929] INFO     root:  result from java cmd: 23:20:53.968 [Smack Listener Processor
(0)] DEBUG com.cisco.pxgrid.GridConnection - associate presence packet received (type=available,
from=test1@xgrid.cisco.com)23:21:00.132 [Thread-0] DEBUG c.c.p.internal.CapabilityManager - refreshing
connection state...
23:21:00.133 [Thread-0] DEBUG c.c.p.internal.CapabilityManager - done refreshing connection state.
23:21:00.134 [Thread-0] DEBUG c.c.p.i.s.NotificationHandlerSmack - refreshing connection state...
23:21:00.135 [Thread-0] DEBUG c.c.p.i.s.NotificationHandlerSmack - done refreshing connection state.
23:21:00.390 [main] DEBUG c.c.p.internal.CapabilityManager - subscribed
(topic=EndpointProtectionServiceCapability-1.0)
```

参考

有关 pxGrid 的更多详细信息，请参阅：
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-84-Configure_and_Test_Integration_with_Cisco_pxGrid.pdf

有关 Cisco ISE pxGrid 部署指南，请参阅：
https://cisco.box.com/s/o6jt09pkvo9sew4novnnvbqyfvx63h9b

Splunk 中引用的 ISE EPS RESTful 工作流程操作：
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-85-Integrating_and_Monitoring_Cisco_ISE_User-Device_Context_in_Splunk.pdf