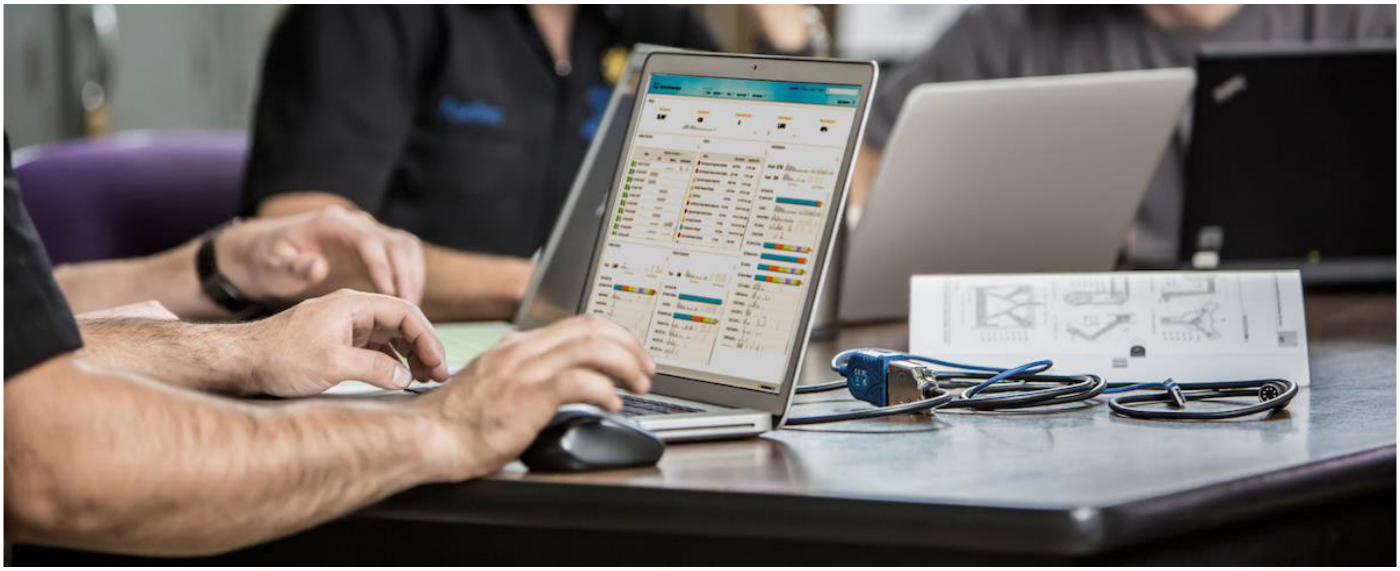


使用思科身份服务引擎 (ISE) 2.0 配置和测试与思科 pxGrid 的集成

目录

关于本文档

本文档介绍适用于思科平台交换框架 (pxGrid) 及关联 SDK 的 ISE 2.0 安装详情，并包含 pxGrid 示例脚本。这些脚本可在非 802.1X 或 802.1X 环境中运行。

pxGrid ISE 2.0 新功能：

- 动态主题 - 可在已注册/订阅的 pxGrid 客户端之间共享上下文信息。pxGrid 客户端可充当发布者或用户来发布或使用该信息。请注意，ISE 将无法使用该信息。
- 自适应网络控制 (ANC) 策略 - 提供第三方应用或思科安全解决方案来自定义缓解操作：使用 ISE 策略或 pxGrid ANC 查询脚本进行隔离、补救、调配、端口反弹或端口关闭。
- 发布 SXP 绑定 - 使用户可以接收 IP、SGT 标记、源、对等序列信息。

读者将在非 802.1X 环境中使用 Radius 模拟程序。pxGrid 会话属性（例如终端安全评估信息、终端设备）要求在 802.1X 环境中进行测试。

pxGrid ISE 2.0 功能要求在 802.1X 环境中进行测试。此外，如果计划进行 SXP 测试，网络设备将需要具有 TrustSec 兼容性。

pxGrid 操作

ISE 发布会话目录信息等信息主题，其中包括 pxGrid 客户端、思科安全解决方案或第三方生态系统合作伙伴可订阅的 ISE 上下文信息，并提供与事件相关的更有价值的信息。

以下是来自某成功的 802.1X IEEE 有线身份验证的最终用户会话示例。记录用户名、IP 地址、MAC 地址和设备类型信息，这些信息可绑定到事件。

```
Session={ip=[192.168.1.31], Audit Session Id=0A0000010000002803DBE3C1, User Name=LAB6\jeppich, AD User DNS
Domain=lab6.com, AD Host DNS Domain=null, AD User NetBIOS Name=LAB6, AD Host NETBIOS Name=null, Calling
station id=00:0C:29:79:02:A8, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint
Profile=Windows7-Workstation, NAS IP=192.168.1.2, NAS Port=GigabitEthernet1/0/12, RADIUSAVPairs=[ Acct-
Session-Id=00000053], Posture Status=NonCompliant, Posture Timestamp=Sat Aug 01 15:15:20 EDT 2015, Session
Last Update Time=Sat Aug 01 15:15:22 EDT 2015}
```

现在您得到与事件相关的此类信息，根据组织的安全策略和合规性要求，对于未遵守企业策略和使用非推荐的设备连接到组织网络的最终用户，可为安全应用提供更严格的策略。

同时，如果安全应用了解设备和用户上下文信息的类型，则可能更容易对该设备类型可能采取的补救操作应用特定的安全策略。可使用 pxGrid 自适应网络控制 (ANC) 缓解操作实现补救操作。

信息主题

ISE 发布的功能称为信息主题：

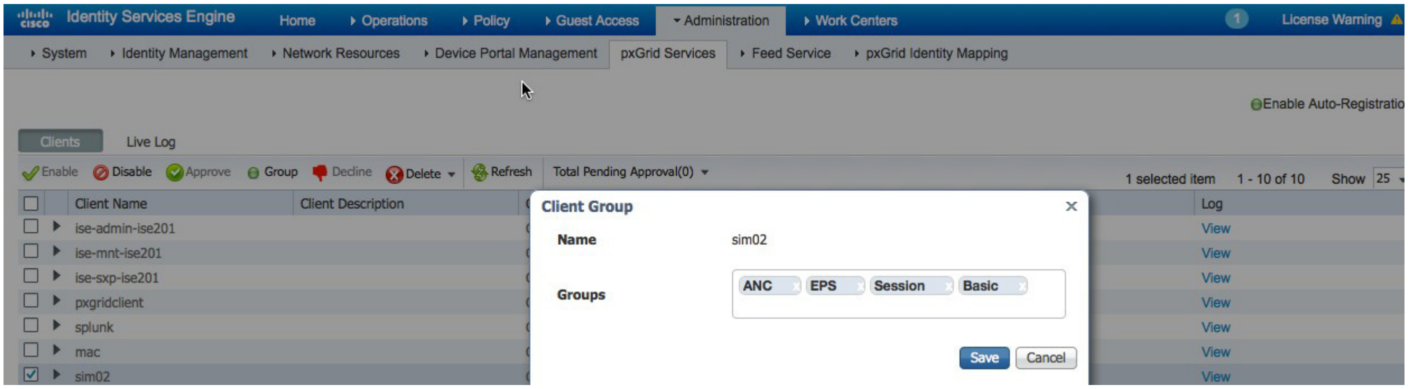
- GridControllerAdminService - 向用户提供 pxGrid 服务
- AdaptiveNetworkControl - 向用户提供增强的 pxGrid ANC 缓解功能
- 核心 - 向 pxGrid 客户端提供查询 ISE pxGrid 节点上所有已注册功能的功能
- EndpointProfileMetada - 向 pxGrid 客户端提供来自 ISE 的可用设备信息
- EndpointProtectionService - 提供来自 ISE 1.3/1.4 的兼容 EPS/ANC pxGrid 缓解操作
- TrustSecMetaData - 向 pxGrid 客户端提供公开的安全组标记 (SGT) 信息
- IdentityGroup - 向 pxGrid 客户端提供可能无法通过 802.1X 身份验证获取的身份组信息
- SessionDirectory - 向 pxGrid 客户端提供 ISE 发布的会话信息或可用的会话对象

客户端组

pxGrid 客户端将验证、连接并注册到 ISE pxGrid 节点以及注册到客户端组，以订阅这些主题或发出对这些主题的直接查询。pxGrid 客户端还可以订阅多个客户端组。

pxGrid 客户端组包括：

- 基本 - 提供 ISE pxGrid 节点连接。pxGrid 管理员必须手动将已注册的 pxGrid 客户端移动到其他客户端组，很可能是会话组，该组会提供 pxGrid 会话对象访问
- 管理员 - 为 ISE 发布的节点客户端保留
- 会话 - 提供 pxGrid 会话对象访问
- ANC - 访问 ANC 策略操作
- EPS - 与 ISE 1.3/ISE 1.4 eps_quarantine/eps_unquarantine pxGrid 脚本兼容



□	Client Name	Client Description	Log
□	ise-admin-ise201		View
□	ise-mnt-ise201		View
□	ise-sxp-ise201		View
□	pxgridclient		View
□	splunk		View
□	mac		View
☑	sim02		View

Client Group

Name: sim02

Groups: ANC, EPS, Session, Basic

测试环境

要进行 pxGrid 测试，您的实验室应该具备以下条件：

- VMware 5.5 ESX 服务器
- 至少需要 3 种不同的虚拟机：
  - ISE 2.0 pxGrid 节点
  - 适用于 Microsoft AD 的 Windows 2008 R2 CA 服务器，还将包含 DNS 和 NTP

注意：您还需要将此设置为 CA 服务器，用于测试 CA 签名的证书。

  - 使用 802.1X 请求者、Cisco AnyConnect NAM 或 RADIUS 模拟程序的 Windows PC 客户端

注意：如果没有 802.1X 环境，请使用 RADIUS 模拟程序。

- 802.1X 环境：Cisco Catalyst 3750-x、Cisco Catalyst 3560-x、Cisco Catalyst 3850，如果测试新的 ISE SXP 功能，请参阅 TrustSec 兼容性列表：http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec-matrix-archived.html，否则请确保网络访问设备与 ISE 兼容，请参阅：http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/compatibility/ise_sdt.html#pgfId-198199
- pxGrid 客户端：MAC 或 Linux 客户端、思科安全解决方案、第三方 pxGrid 合作伙伴应用
- ISE 2.0.0.306
- pxGrid sdk 1.0.2.32

思科身份服务引擎 (ISE 2.0) 虚拟机设置

本部分介绍初始 ESX 服务器虚拟机创建配置

- Linux 5 64 位操作系统
- 操作系统硬盘驱动器最小 100 GB
- 8 GB RAM
- 2 个网络接口卡（如果是 1 个网络接口卡，则其用作 SXP 侦听程序）

注意：请勿将同一个虚拟机网络接口卡用于 PC 客户端，因为如果采用 802.1X 环境，PC 客户端端口将根据 802.1X 配置来配置。

在配置 ISE 之前，确定 AD 域正常运行。ISE 设置配置将需要主机名、IP 地址、域名、DNS 和 NTP 服务器名称。

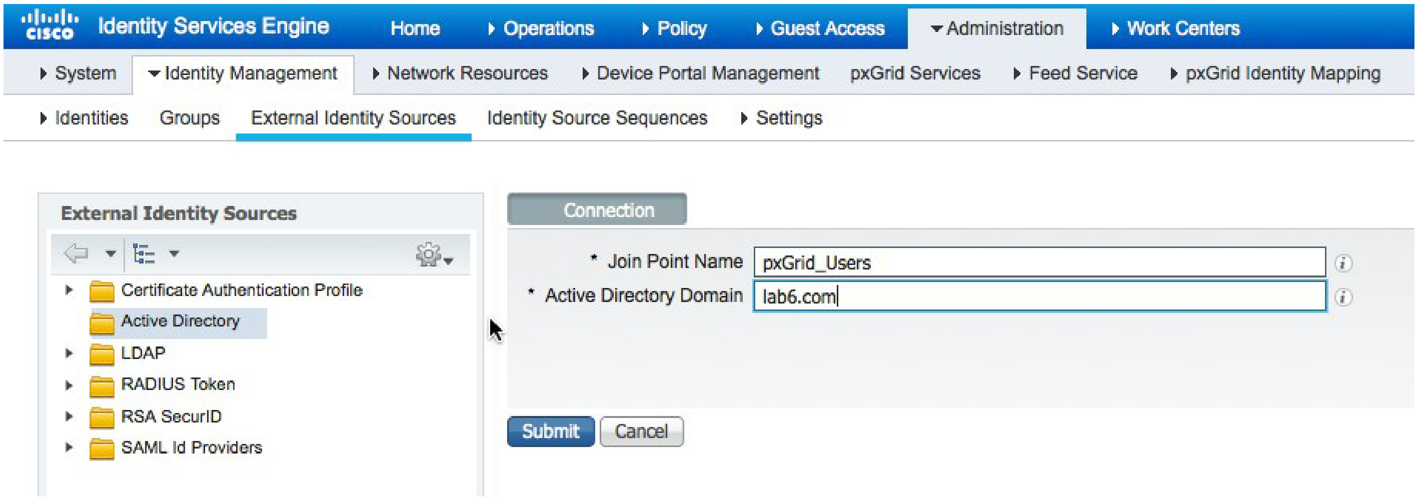
ISE、pxGrid 客户端和 PC 客户端必须能够解析 FQDN。

初始 ISE 设置

本部分介绍用于最终用户身份验证的 AD 设置。

AD 用户设置

第 1 步 配置 AD 连接
选择**管理 (Administration)->身份管理 (Identity Management)->外部身份源 (External Identity Sources)->Active Directory->添加 (Add)**
提供一个组合名称：**pxGrid_users**
Active Directory 域名：**lab6.com**

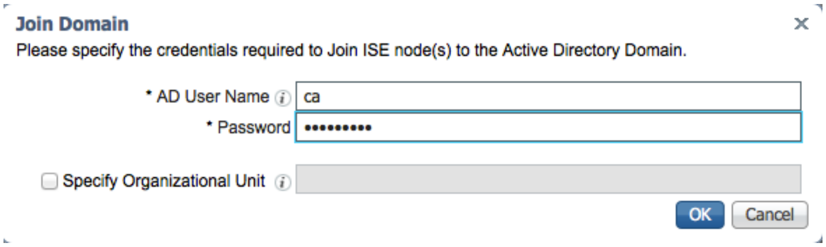


* Join Point Name: pxGrid_Users

* Active Directory Domain: lab6.com

第 2 步 选择**提交 (Submit)**，然后将所有 ISE 节点加入到 Active Directory

第 3 步 提供加入域的凭证



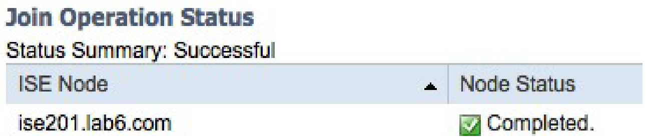
Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name: ca

* Password: •••••••••

□ Specify Organizational Unit

第 4 步 点击**确定 (OK)**，您应看到已完成的加入状态

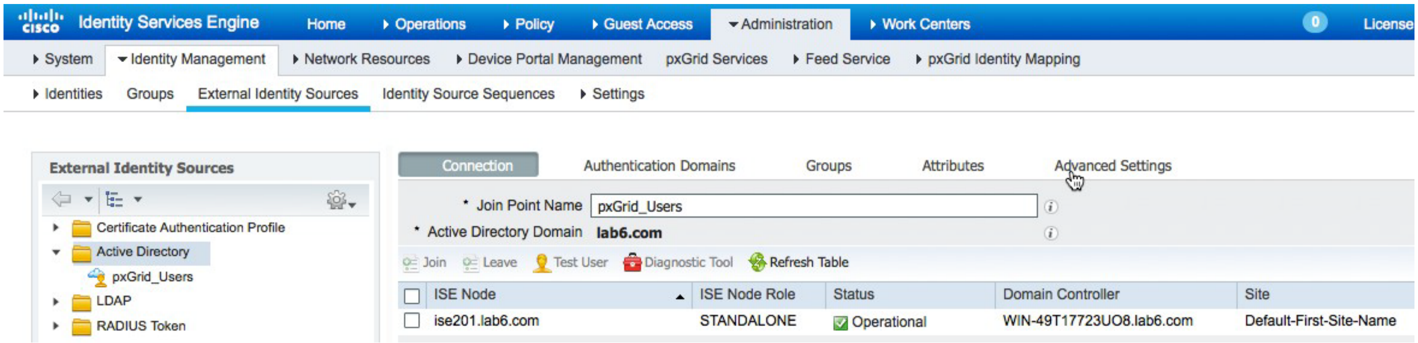


Status Summary: Successful

ISE Node	Node Status
ise201.lab6.com	✓ Completed.

注意：如果您看到故障的节点状态，请确保 ISE 和 MS AD 之间的时间是同步的，并且能够解析 FQDN

第 5 步 选择关闭 (Close)，您将看到下图所示内容：

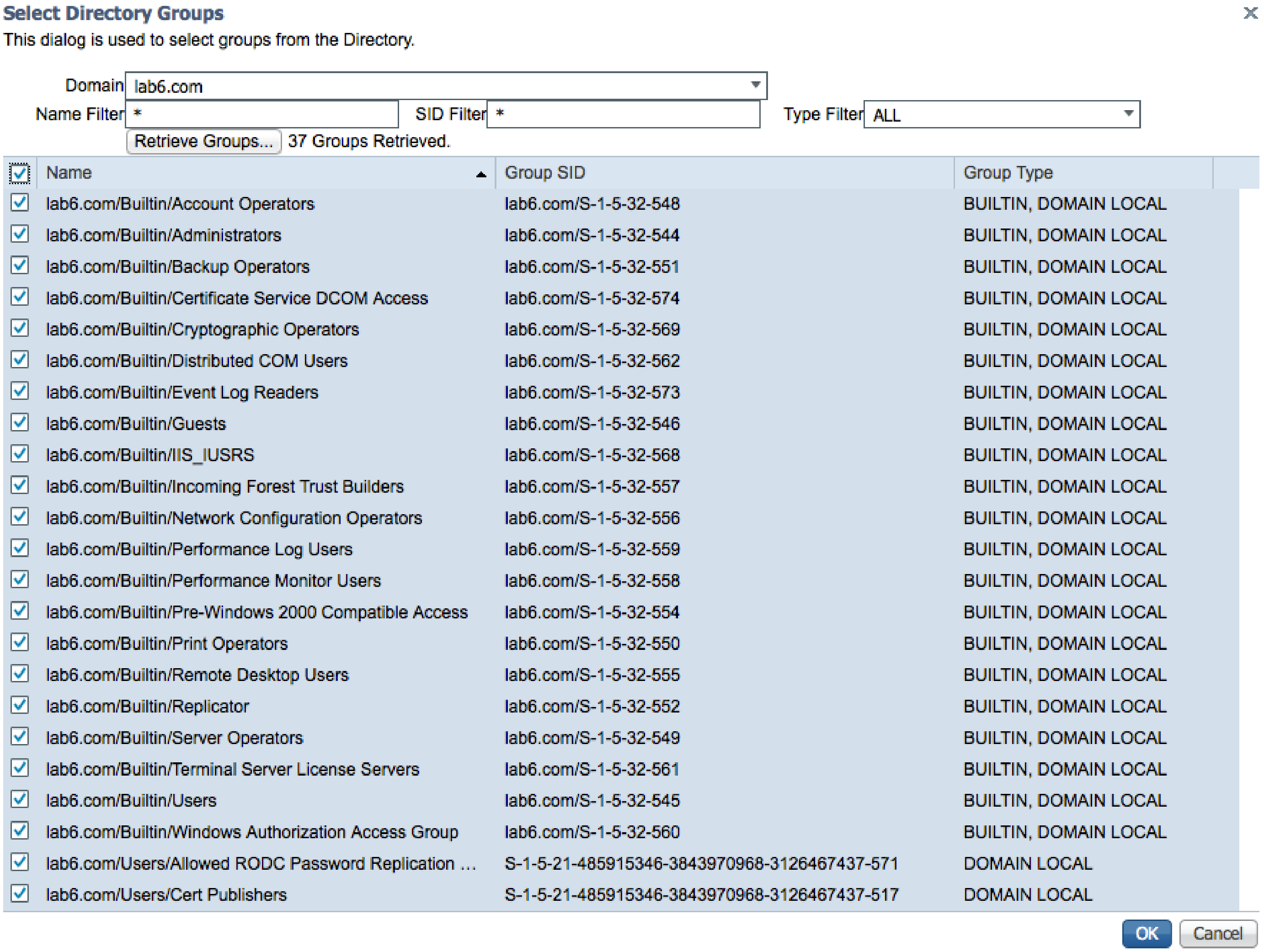


* Join Point Name: pxGrid_Users

* Active Directory Domain: lab6.com

	ISE Node	ISE Node Role	Status	Domain Controller	Site
□	ise201.lab6.com	STANDALONE	✓ Operational	WIN-49T17723UO8.lab6.com	Default-First-Site-Name

第 6 步 点击组 (Groups)->添加 (Add)->从 Active Directory 选择组 (Select Groups from Active Directory)->检索组 (Retrieve groups)->选择全部 (select all)->确定 (OK)



Select Directory Groups

This dialog is used to select groups from the Directory.

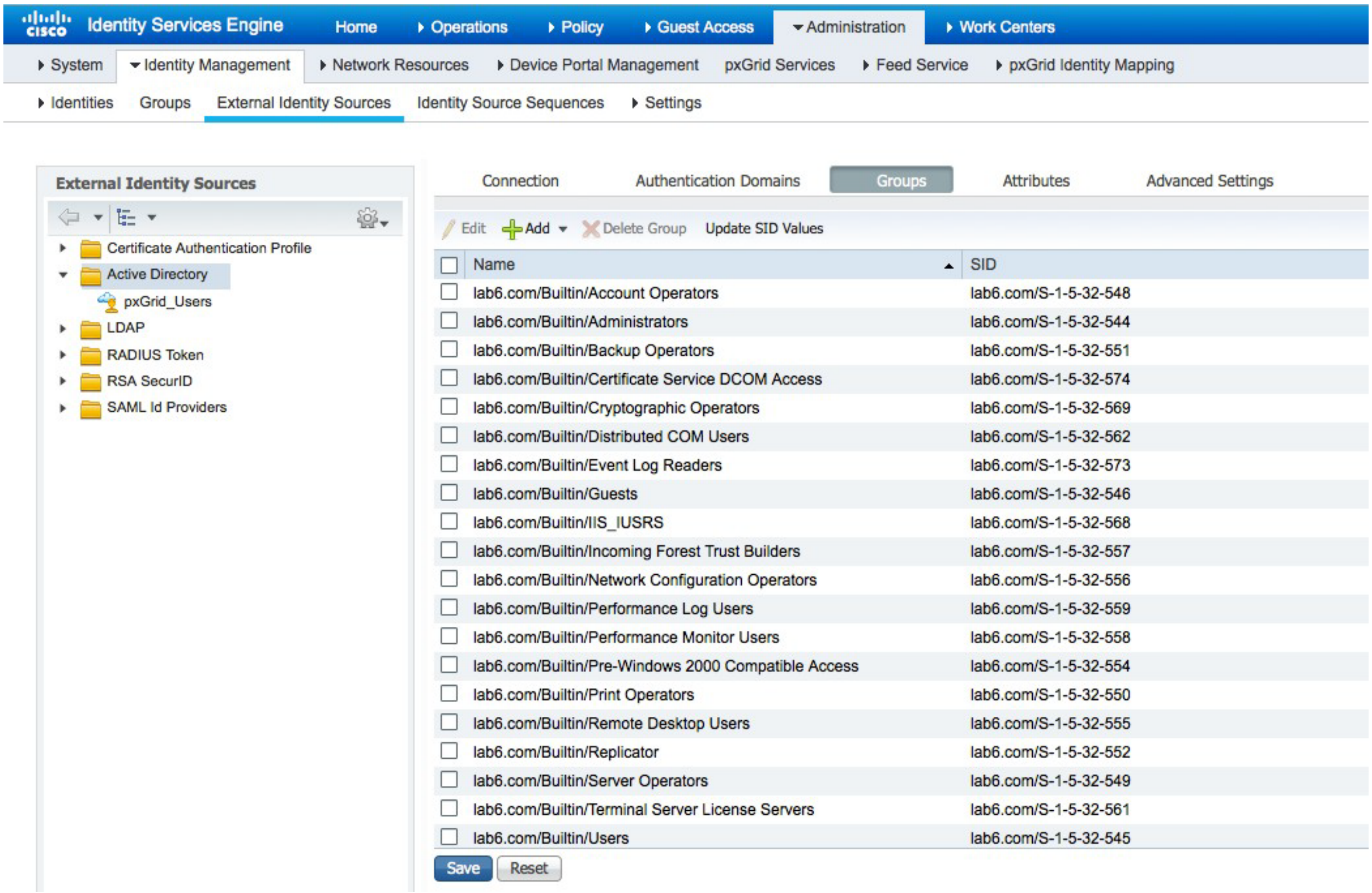
Domain: lab6.com

Name Filter: * SID Filter: * Type Filter: ALL

Retrieve Groups... 37 Groups Retrieved.

☑	Name	Group SID	Group Type
☑	lab6.com/Builtin/Account Operators	lab6.com/S-1-5-32-548	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Administrators	lab6.com/S-1-5-32-544	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Backup Operators	lab6.com/S-1-5-32-551	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Certificate Service DCOM Access	lab6.com/S-1-5-32-574	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Cryptographic Operators	lab6.com/S-1-5-32-569	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Distributed COM Users	lab6.com/S-1-5-32-562	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Event Log Readers	lab6.com/S-1-5-32-573	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Guests	lab6.com/S-1-5-32-546	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/IIS_IUSRS	lab6.com/S-1-5-32-568	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Incoming Forest Trust Builders	lab6.com/S-1-5-32-557	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Network Configuration Operators	lab6.com/S-1-5-32-556	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Performance Log Users	lab6.com/S-1-5-32-559	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Performance Monitor Users	lab6.com/S-1-5-32-558	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Pre-Windows 2000 Compatible Access	lab6.com/S-1-5-32-554	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Print Operators	lab6.com/S-1-5-32-550	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Remote Desktop Users	lab6.com/S-1-5-32-555	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Replicator	lab6.com/S-1-5-32-552	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Server Operators	lab6.com/S-1-5-32-549	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Terminal Server License Servers	lab6.com/S-1-5-32-561	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Users	lab6.com/S-1-5-32-545	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Builtin/Windows Authorization Access Group	lab6.com/S-1-5-32-560	BUILTIN, DOMAIN LOCAL
☑	lab6.com/Users/Allowed RODC Password Replication ...	S-1-5-21-485915346-3843970968-3126467437-571	DOMAIN LOCAL
☑	lab6.com/Users/Cert Publishers	S-1-5-21-485915346-3843970968-3126467437-517	DOMAIN LOCAL

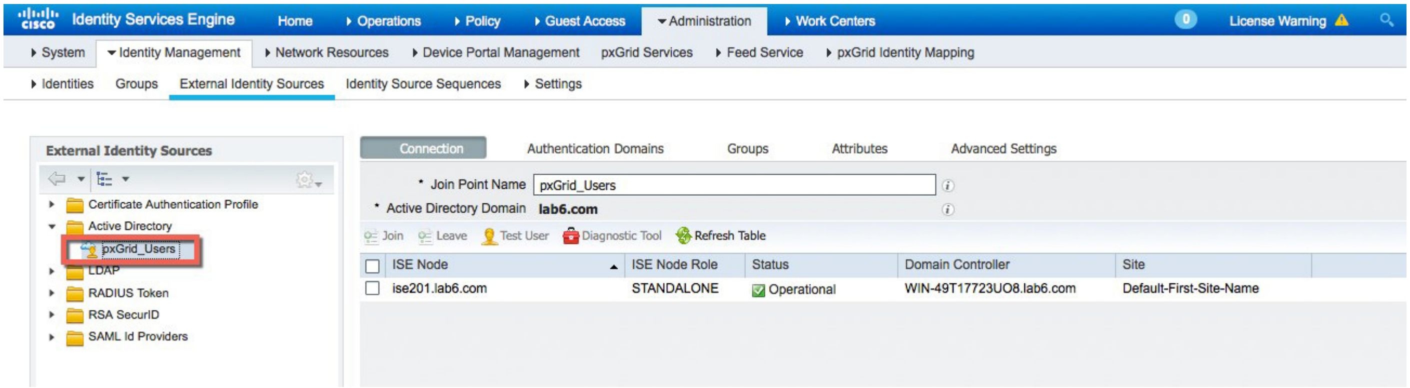
第 7 步　　点击**确定 (OK)**



□	Name	SID
□	lab6.com/Builtin/Account Operators	lab6.com/S-1-5-32-548
□	lab6.com/Builtin/Administrators	lab6.com/S-1-5-32-544
□	lab6.com/Builtin/Backup Operators	lab6.com/S-1-5-32-551
□	lab6.com/Builtin/Certificate Service DCOM Access	lab6.com/S-1-5-32-574
□	lab6.com/Builtin/Cryptographic Operators	lab6.com/S-1-5-32-569
□	lab6.com/Builtin/Distributed COM Users	lab6.com/S-1-5-32-562
□	lab6.com/Builtin/Event Log Readers	lab6.com/S-1-5-32-573
□	lab6.com/Builtin/Guests	lab6.com/S-1-5-32-546
□	lab6.com/Builtin/IIS_IUSRS	lab6.com/S-1-5-32-568
□	lab6.com/Builtin/Incoming Forest Trust Builders	lab6.com/S-1-5-32-557
□	lab6.com/Builtin/Network Configuration Operators	lab6.com/S-1-5-32-556
□	lab6.com/Builtin/Performance Log Users	lab6.com/S-1-5-32-559
□	lab6.com/Builtin/Performance Monitor Users	lab6.com/S-1-5-32-558
□	lab6.com/Builtin/Pre-Windows 2000 Compatible Access	lab6.com/S-1-5-32-554
□	lab6.com/Builtin/Print Operators	lab6.com/S-1-5-32-550
□	lab6.com/Builtin/Remote Desktop Users	lab6.com/S-1-5-32-555
□	lab6.com/Builtin/Replicator	lab6.com/S-1-5-32-552
□	lab6.com/Builtin/Server Operators	lab6.com/S-1-5-32-549
□	lab6.com/Builtin/Terminal Server License Servers	lab6.com/S-1-5-32-561
□	lab6.com/Builtin/Users	lab6.com/S-1-5-32-545

第 8 步　　点击**保存 (Save)**

第 9 步　　点击 **pxGrid_Users**，您将看到下图所示内容



* Join Point Name: pxGrid_Users

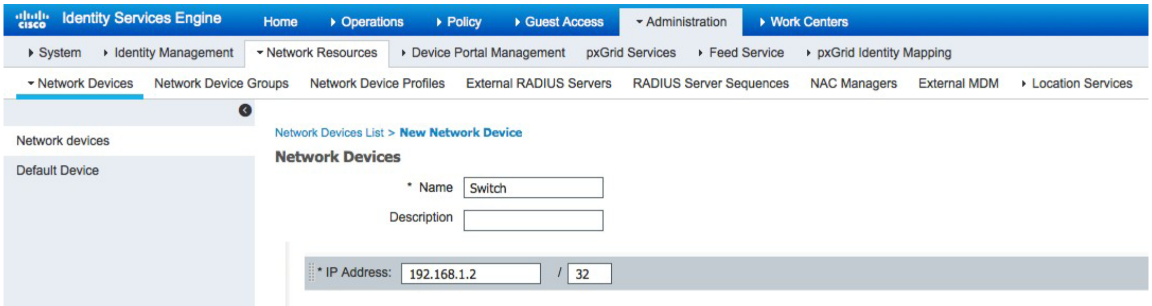
* Active Directory Domain: **lab6.com**

□	ISE Node	ISE Node Role	Status	Domain Controller	Site
□	ise201.lab6.com	STANDALONE	✓ Operational	WIN-49T17723UO8.lab6.com	Default-First-Site-Name

网络设备

添加网络设备、思科交换机和无线局域网控制器。如果您正在运行 RADIUS 模拟程序，将需要提供将运行 RADIUS 模拟程序的 PC 客户端的 IP 地址。在添加 RADIUS 模拟程序时，使用 **secret** 作为共享密钥。

第 1 步　选择**管理 (Administration)->网络资源 (Network Resources)->网络设备 (Network Devices)->添加网络设备 (Add Network Device)**
提供名称：交换机 IP
地址：192.168.1.2



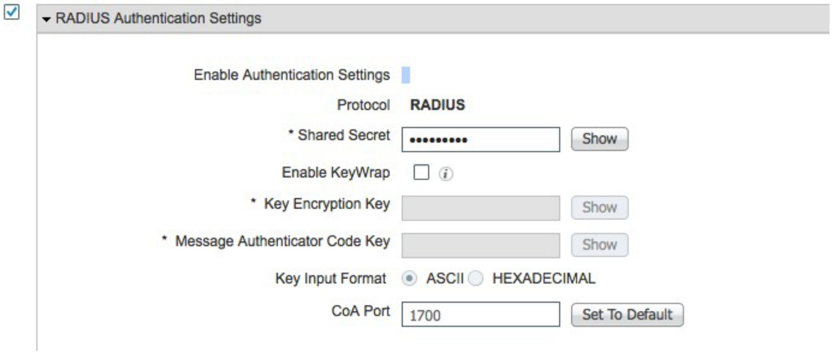
Network Devices

* Name: Switch

Description:

* IP Address: 192.168.1.2 / 32

第 2 步　启用 Radius 身份验证设置并输入共享密钥



☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: ••••••••• Show

Enable KeyWrap: □

* Key Encryption Key: Show

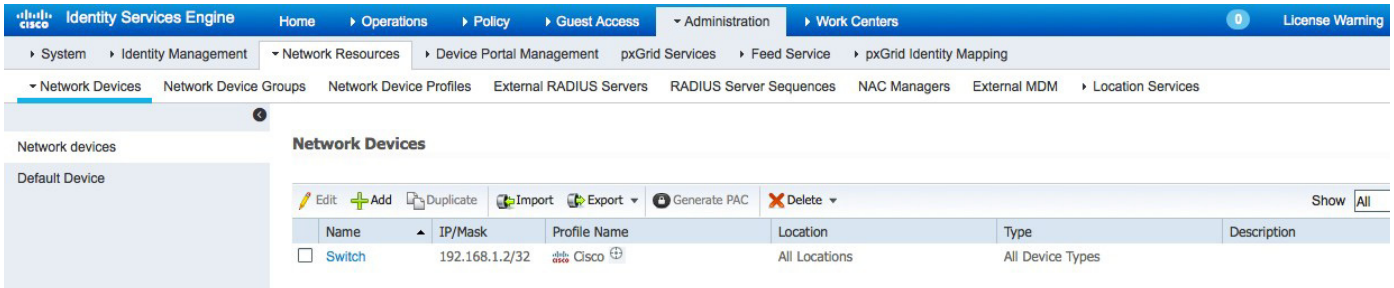
* Message Authenticator Code Key: Show

Key Input Format: ● ASCII ○ HEXADECIMAL

CoA Port: 1700 Set To Default

第 3 步　点击**提交 (Submit)**

第 4 步　您将看到下图所示内容：



Network Devices

	Name	IP/Mask	Profile Name	Location	Type	Description
□	Switch	192.168.1.2/32	Cisco	All Locations	All Device Types	

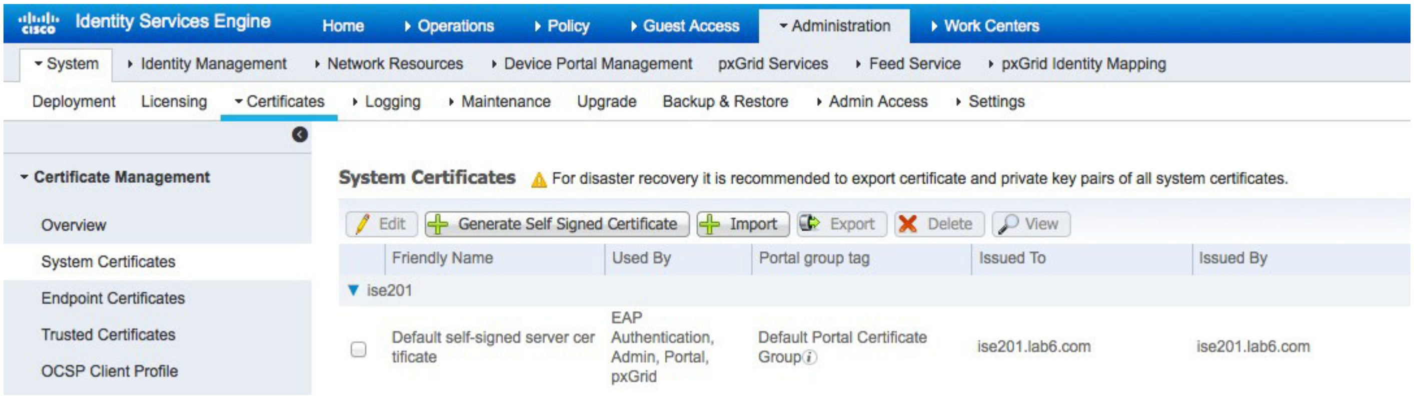
© 2015 思科系统公司

配置适用于 pxGrid 的 ISE

自签名 ISE 身份证书将用于启用 pxGrid 服务。

注意： 在 ISE 1.3 和 ISE 1.4 中，必须导出自签名 ISE 身份证书，并将其导入受信任的系统证书库中，才能启动 pxGrid 服务，而在此版本中不再是如此。

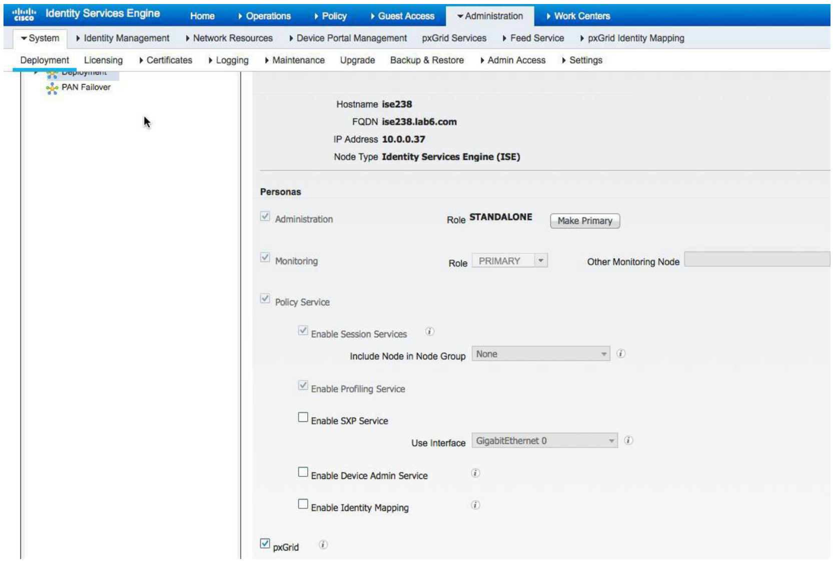
第 1 步　选择**管理 (Administration)->证书 (Certificates)->**记录默认自签名证书



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By
▼ ise201					
□	Default self-signed server certificate	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group ⓘ	ise201.lab6.com	ise201.lab6.com

第 2 步　启用 pxGrid 角色
选择**管理(Administration)->系统部署 (System Deployment)->**启用 **pxGrid 节点 (Enable pxGrid node)**



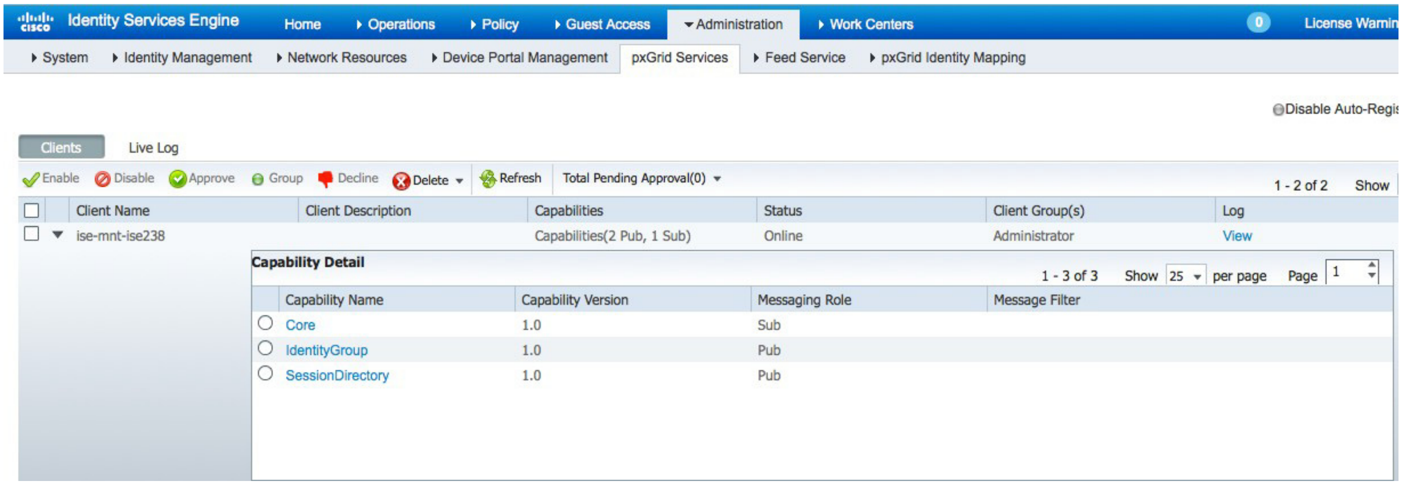
Hostname **ise238**
FQDN **ise238.lab6.com**
IP Address **10.0.0.37**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration　Role **STANDALONE**
☑ Monitoring　Role PRIMARY　Other Monitoring Node
☑ Policy Service
☑ Enable Session Services ⓘ
Include Node in Node Group None ⓘ
☑ Enable Profiling Service
□ Enable SXP Service
Use Interface GigabitEthernet 0 ⓘ
□ Enable Device Admin Service ⓘ
□ Enable Identity Mapping ⓘ
☑ pxGrid ⓘ

第 3 步　　您会在 MNT 节点中看到 ISE 发布的信息主题

注意： 这可能需要几分钟才会出现

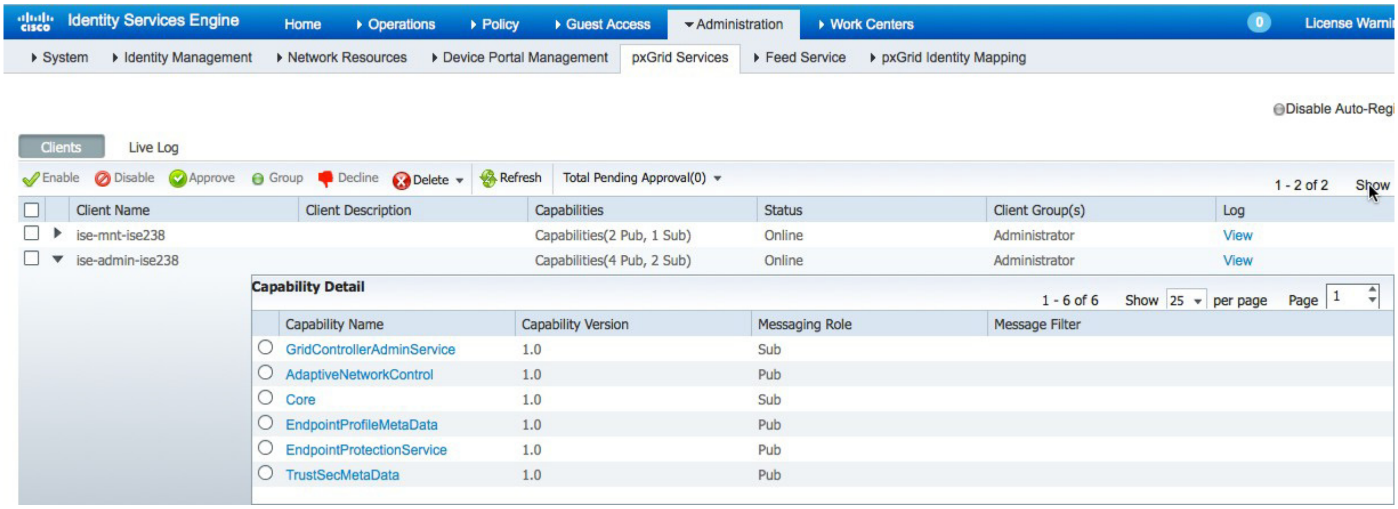


□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View

Capability Detail 1 - 3 of 3　Show 25 per page　Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	IdentityGroup	1.0	Pub	
○	SessionDirectory	1.0	Pub	

第 4 步　　您会在 Admin 节点中看到 ISE 发布的信息主题



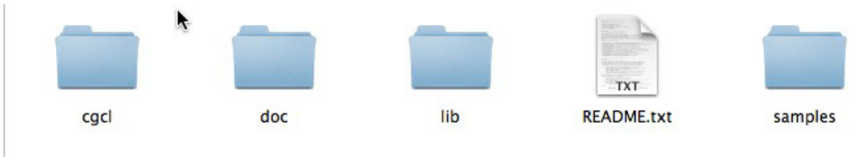
□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View

Capability Detail 1 - 6 of 6　Show 25 per page　Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	GridControllerAdminService	1.0	Sub	
○	AdaptiveNetworkControl	1.0	Pub	
○	Core	1.0	Sub	
○	EndpointProfileMetaData	1.0	Pub	
○	EndpointProtectionService	1.0	Pub	
○	TrustSecMetaData	1.0	Pub	

安装 pxGrid SDK

下载 SDK 文件，并解压文件，您将看到以下文件夹。



../samples/cert 文件夹将包含运行 pxGrid 脚本的示例证书。

../samples/bin 文件夹将包含 pxGrid“Java”脚本示例。cgcl 文件夹将包含 pxGrid“C”库。

```
ANCAction_query.sh                     identity_group_download.sh
alpha.jks                              identity_group_query.sh
alpha_root.jks                         identity_group_subscribe.sh
capability_query.sh                    multigroupclient.sh
common.sh                              propose_capability.sh
core_subscribe.sh                      securitygroup_query.sh
endpointprofile_query.sh               securitygroup_subscribe.sh
endpointprofile_subscribe.sh           session_download.sh
eps_quarantine.sh                      session_query_by_ip.sh
eps_unquarantine.sh                    session_sub_download.sh
generic_action_client.properties       session_subscribe.sh
generic_client.sh                      sxp_download.sh
generic_publisher.properties           sxp_subscribe.sh
generic_subscriber.properties
```

为运行这些脚本，需要 Oracle Java 开发工具包。

使用自签名证书进行 pxGrid 客户端测试（示例证书的备用选择）

自签名证书用于通过 ISE pxGrid 测试 pxGrid 客户端。以下是使用自签名证书进行 pxGrid 脚本测试的程序。

第 1 步　为 pxGrid 客户端生成私钥（例如 alpha.key）。

```
openssl genrsa -out alpha.key 4096

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

第 2 步　生成自签名 CSR (alpha.csr) 请求并提供质询密码。

```
openssl req -new -key alpha.key -out alpha.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 []:LAB
```

注意：在本文档各处使用相同的密码，可便于维护，并减少错误

第 3 步　生成自签名证书公钥对证书（例如 alpha.cer）。

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

第 4 步　系统将根据私钥生成 PKCS12 文件（例如 alpha.p12）。

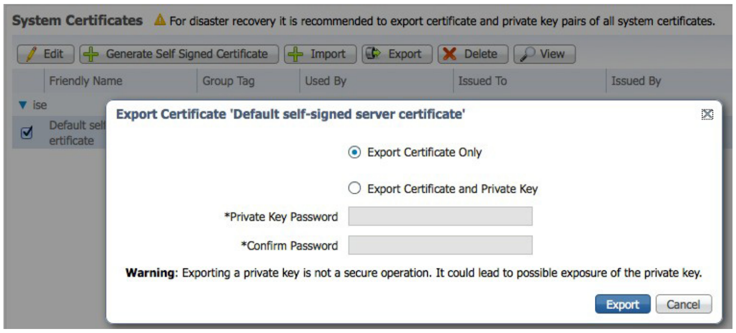
```
openssl pkcs12 -export -out alpha.p12 -inkey alpha.key -in alpha.cer

Enter Export Password: cisco123
```

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

第 5 步　alpha.p12 将导入到身份密钥库（例如 alpha.jks）中。密钥库文件名可以是扩展名为 .jks 的随机文件名。这将在 pxGrid 脚本中充当信任库文件名和关联信任库密码。

```
keytool -importkeystore -srckeystore alpha.p12 -destkeystore alpha.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
```

第 6 步　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。



For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Export Certificate 'Default self-signed server certificate'

● Export Certificate Only

○ Export Certificate and Private Key

*Private Key Password

*Confirm Password

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

第 7 步　将 .pem 文件转换为 .der 格式。

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

第 8 步　将 ISE 身份证书添加到身份密钥库。这将用于在运行 pxGrid 会话下载脚本时保护从 ISE MNT 节点进行的批量会话下载。

```
keytool -import -alias mnt1 -keystore alpha.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:[ C
  A: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
```

第 9 步　将 pxGrid 客户端证书导入到身份密钥库中。

```
keytool -import -alias pxGridclient1 -keystore alpha.jks -file alpha.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
```

__注意__：如果您收到表明证书已添加到预先存在的密钥库的消息，则可以选择"no"，这不会有任何问题。我选择了"yes"，因此我们可以验证后来是否添加了证书。

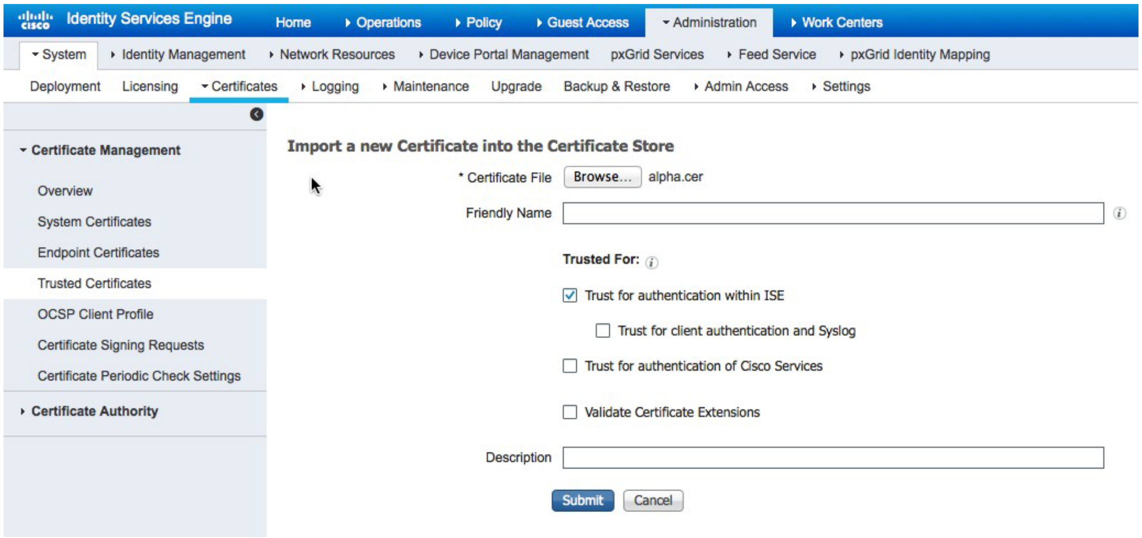
第 10 步　将 ISE 身份证书导入到信任密钥库（例如 alpha_root.jks）中。这将充当 pxGrid 脚本的信任库文件名和信任库密码。

```
keytool -import -alias root1 -keystore alpha_root.jks -file isemnt.der
Enter keystore password:
Re-enter new password:
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
```

第 11 步 将 pxGrid 客户端公共证书 (alpha.cer) 上传到 ISE 受信任证书库中。

第 12 步 选择**管理 (Administration)->证书管理 (Certificate Management)->受信任证书 (Trusted Certificates)->**将 alpha.cer 上传到 ISE pxGrid 节点。



Import a new Certificate into the Certificate Store

* Certificate File Browse... alpha.cer

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description

Submit Cancel

第 13 步 将身份密钥库 (alpha.jks) 和信任密钥库 (alpha_root.jks) 复制到 ../samples/bin/.. 文件夹中。

测试 pxGrid 客户端和 ISE pxGrid 节点

运行 multigroupclient pxGrid 脚本文件，将 pxGrid 客户端注册到 ISE pxGrid 节点。

第 1 步 将 pxGrid 客户端注册到 ISE pxGrid 节点

```
./multigroupclient.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

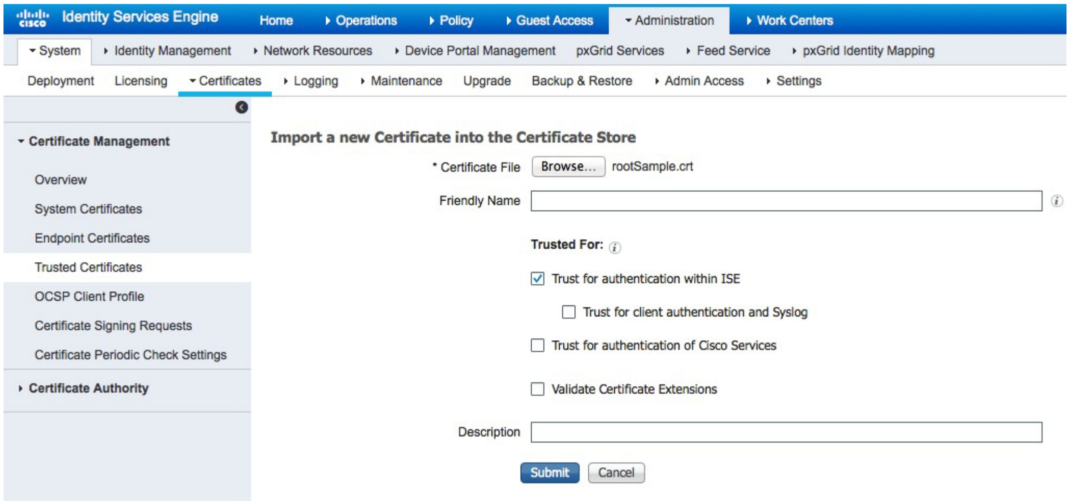
使用来自 SDK 的示例证书进行 pxGrid 测试

将 rootSample.crt 上传到 ISE pxGrid 节点，这将用作受信任证书。并上传 iseSample1.crt 和 iseSample1.key 文件，这将用作 pxGrid 客户端身份证书。请注意，私钥密码为 cisco123。

身份库 iseSample1.jks 文件和信任库 rootSample.jks 文件将从 pxGrid 脚本中调用。

注意：这仅适用于测试，不适用于 ISE 生产部署

第 1 步　将 rootSample.cert 文件上传到 ISE 系统信任库
管理 (Administration)->系统 (System)->证书管理 (Certificate Management)->受信任证书 (Trusted Certificates)->导入 rootSample.crt 文件
启用“信任 ISE 中的身份验证”(Trust for authentication within ISE)



Import a new Certificate into the Certificate Store

* Certificate File: rootSample.crt

Friendly Name:

Trusted For:

☑ Trust for authentication within ISE

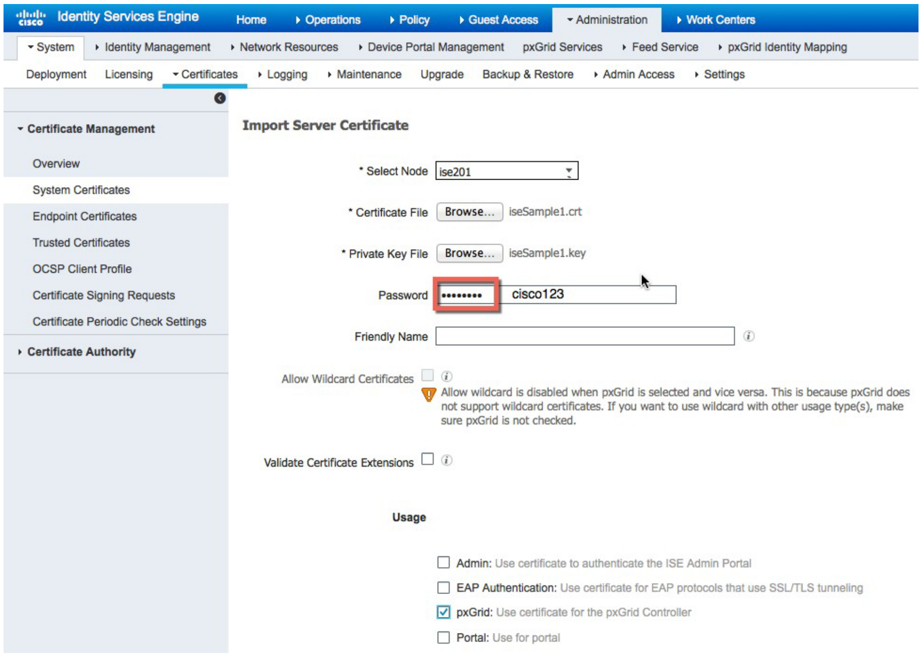
☐ Trust for client authentication and Syslog

☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description:

第 2 步　选择**提交 (Submit)**
第 3 步　将 iseSample1.crt 上传到 ISE 系统证书库中
第 4 步　选择**管理(Administration)->系统 (System)->证书管理 (Certificate Management)->系统证书 (System Certificates)->导入 iseSample1.crt** 文件
第 5 步　选择**管理 (Administration)->系统 (System)->证书管理 (Certificate Management)->系统证书 (System Certificates)->导入 iseSample1.key** 文件
第 6 步　输入密码 **cisco123**
第 7 步　启用 pxGrid 的证书使用



Import Server Certificate

* Select Node ise201

* Certificate File Browse... iseSample1.crt

* Private Key File Browse... iseSample1.key

Password •••••••• cisco123

Friendly Name

Allow Wildcard Certificates □

Allow wildcard is disabled when pxGrid is selected and vice versa. This is because pxGrid does not support wildcard certificates. If you want to use wildcard with other usage type(s), make sure pxGrid is not checked.

Validate Certificate Extensions □

Usage

□ Admin: Use certificate to authenticate the ISE Admin Portal

□ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

☑ pxGrid: Use certificate for the pxGrid Controller

□ Portal: Use for portal

第 8 步　　选择**提交 (Submit)**

测试 pxGrid 客户端和 ISE pxGrid 节点

运行 pxGrid multigroupclient 脚本，将 pxGrid 客户端注册到 ISE pxGrid 节点。

第 1 步　　将 pxGrid 客户端注册到 ISE pxGrid 节点

```
./multigroupclient.sh -a 192.168.1.23 -u SIM01 -k iseSample1.jks -p cisco123 -t rootSample.jks -q cisco123
```

RADIUS 模拟程序

RADIUS 模拟程序在没有 IEEE 802.1X 环境的组织内运行。

RADIUS 模拟程序提供 802.1X 身份验证并允许将基本属性（如 IP、MAC 和身份组信息）填充到会话目录。会话属性（例如终端配置文件，终端安全评估状态）只能使用 802.1X 获取。

注意： 在使用 RADIUS 模拟程序时，PC 上不应存在本地请求者或 AnyConnect NAM。此外，RADIUS 模拟程序具有在 RADIUS 模拟程序参数列表中定义的命令行参数。

命令行参数：-DUSERNAME、-DPASSWORD、-DCALLING_STATION_ID、- DAUDIT_SESSION_ID、-DACCT_SESSION_ID、-DFRAMED_IP_ADDRESS、-DFRAMED_IP_MASK、RadiusAccountingStart、RadiusAccountingStop、RadiusAuthentication 将用于多个最终用户身份验证测试。

注意： RADIUS 模拟程序命令区分大小写

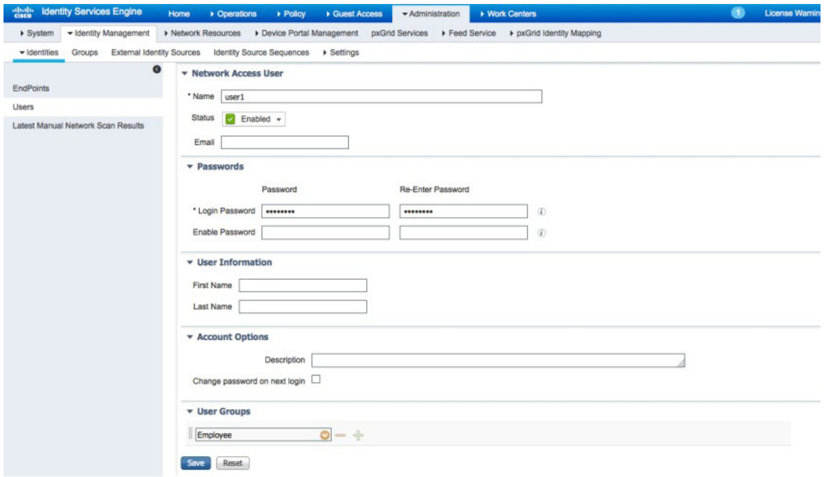
RADIUS 模拟程序需要 Java 开发工具包。RADIUS 模拟程序可在 pxGrid 客户端或客户端 PC 上运行。

如果您未在 Microsoft AD 中使用用户，可以使用 ISE 内部用户进行测试。

创建 ISE 内部用户

如果您尚未在 AD 中设置用户，我们将在此创建一些内部 ISE 用户用于测试。

第 1 步 选择**管理 (Administration)->身份管理 (Identity Management)->身份 (Identity)->用户 (Users)->添加 (Add)->用户 1 (user1)，输入密码信息添加到员工组**



Network Access User

* Name: user1

Status: ☑ Enabled

Email:

Passwords

	Password	Re-Enter Password
* Login Password	•••••••••	•••••••••
Enable Password		

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login □

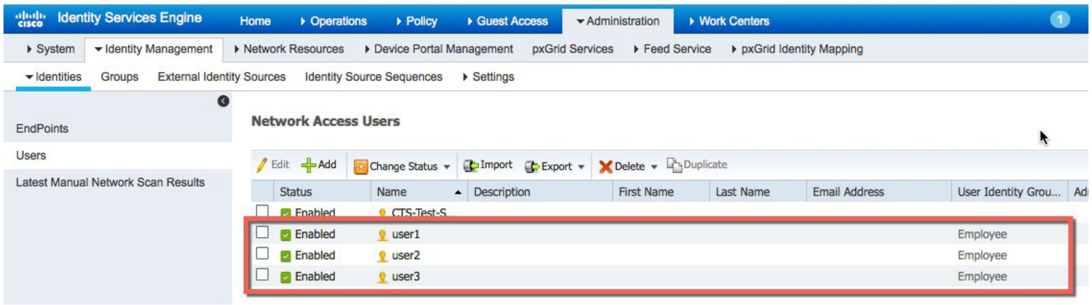
User Groups

Employee

第 2 步 选择**保存 (Save)**

第 3 步 对用户 2 和用户 3 重复同样的操作

第 4 步 您将看到下图所示内容：



Network Access Users

	Status	Name	Description	First Name	Last Name	Email Address	User Identity Grou...	Ad
□	☑ Enabled	CTS-Test-S...						
□	☑ Enabled	user1					Employee	
□	☑ Enabled	user2					Employee	
□	☑ Enabled	user3					Employee	

身份验证

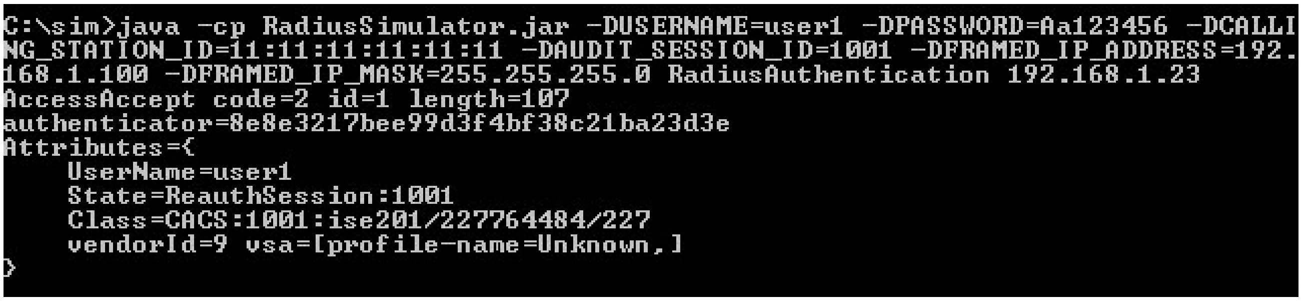
在客户端 PC 上运行 RADIUS，以模拟 802.1X 身份验证。

第 1 步　模拟用户身份验证

```
java -cp RadiusSimulator.jar -DUSERNAME=user1 -DPASSWORD=Aa123456 -DCALLING_STATION_ID=11:11:11:11:11:11 -
DAUDIT_SESSION_ID=1001 -DFRAMED_IP_ADDRESS=192.168.1.60 - DFRAMED_IP_MASK=255.255.255.0 RadiusAuthentication
192.168.1.98
```

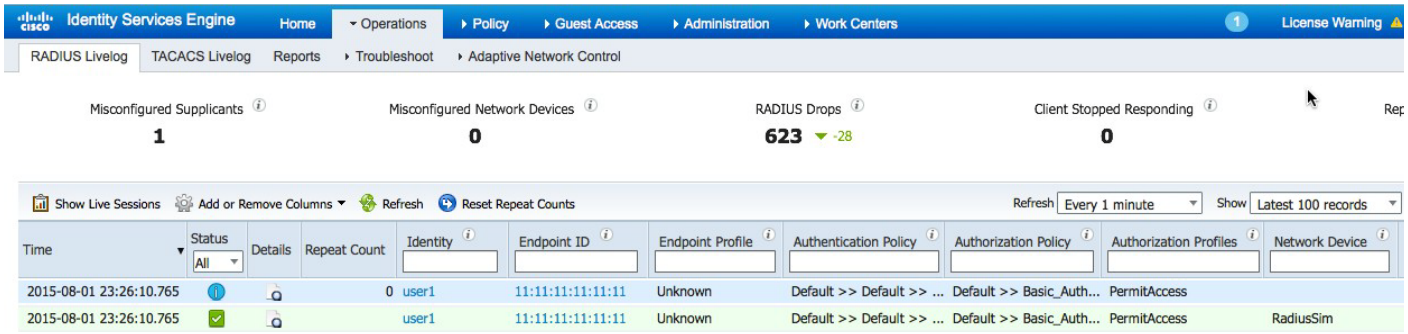
测试身份验证

第 1 步　在 ISE 的参数中键入以下身份验证



```
C:\sim>java -cp RadiusSimulator.jar -DUSERNAME=user1 -DPASSWORD=Aa123456 -DCALLI
NG_STATION_ID=11:11:11:11:11:11 -DAUDIT_SESSION_ID=1001 -DFRAMED_IP_ADDRESS=192.
168.1.100 -DFRAMED_IP_MASK=255.255.255.0 RadiusAuthentication 192.168.1.23
AccessAccept code=2 id=1 length=107
authenticator=8e8e3217bee99d3f4bf38c21ba23d3e
Attributes={
    UserName=user1
    State=ReauthSession:1001
    Class=CACS:1001:ise201/227764484/227
    vendorId=9 vsa=[profile-name=Unknown,]
}
```

第 2 步 查看 ISE 中的身份验证
选择**操作 (Operations)->RADIUS Livelog**



Misconfigured Supplicants 1 | Misconfigured Network Devices 0 | RADIUS Drops 623 -28 | Client Stopped Responding 0 | Rep

Refresh Every 1 minute | Show Latest 100 records

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device
	All									
2015-08-01 23:26:10.765	●		0	user1	11:11:11:11:11:11	Unknown	Default >> Default >> ...	Default >> Basic_Auth...	PermitAccess	
2015-08-01 23:26:10.765	✓			user1	11:11:11:11:11:11	Unknown	Default >> Default >> ...	Default >> Basic_Auth...	PermitAccess	RadiusSim

RADIUS 模拟程序参数

参数	默认设置
-DUSERNAME	
-DPASSWORD	
-DCALLING_STATION_ID	
-DAUDIT_SESSION_ID	
-DRADIUS_SECRET	密钥 (Secret)
-DNAS_IP_ADDRESS	
-DFRAMED_IP_ADDRESS	
-DFRAMED_IP_MASK	
RadiusAccountingStop	
RadiusAccountingStart	
RadiusAuthentication	

pxGrid 2.0 示例脚本

本部分概述了如何执行您的开发组织使用的设备测试，以及思科解决方案的验证测试所使用的测试案例。pxGrid 示例脚本提供了通过 pxGrid 获得的会话信息和查询的有益参考。开发人员可以修改这些脚本来提供或查询相关会话信息。

请注意，本部分提供了适用于以下情况的 2 套测试套件：1) 使用来自 pxGrid SDK 的 RADIUS 模拟程序；2) 使用配置了 802.1X 的 ISE 部署。要测试完整的 ISE 集成功能，包括能够使用用于识别终端类型（例如移动设备、打印机、笔记本电脑等）或设备安全状态（例如已安装的最新防恶意软件等）的终端分析功能，请使用本文档稍后介绍的成套 802.1X 测试。如果您的使用案例仅要求简单的 IP-to-MAC-to-User 关联，以仅将用户与您系统中的 IP 地址关联起来，您可以使用 RADIUS 模拟程序测试。

如果使用 802.1X 套件进行测试，与使用 RADIUS 模拟程序相比，它为测试超集。因此，当使用 802.1X 测试套件时，不需要也完成基于 RADIUS 模拟程序的测试套件。

以下是示例测试脚本的简短说明：

多组客户端（*替换 pxGrid 1.3/1.4 中的 register.sh*）- 连接 pxGrid 客户端并将其注册到多个客户端组

注意：Register.sh 向上兼容 ISE 2.0

功能 - 列出 pxGrid 实例所支持且 pxGrid 客户端将订阅的所有功能或发布主题

EPS_Quarantine - 执行传统端点保护服务 (EPS)/自适应网络控制（ISE 上特定 IP 地址的 ISE 13/1.4 隔离操作）

注意：注册的 pxGrid 客户端将注册到 EPS 客户端组并订阅终端保护服务功能

EPS_Unquarantine - 执行传统端点保护服务 (EPS)/自适应网络控制（ISE 上特定 MAC 地址的 ISE 13/1.4 取消隔离操作）

Identity_Group_Download - 下载与 ISE 中的活动会话关联的用户和身份组 Session_Download -

从 ISE 下载所有批量会话记录或活动会话 Session_Query_By_IP - 根据 IP 地址从 ISE 检索所有

活动会话 Session_Subscribe - 订阅会话状态变更

EndpointProfile_Query - 检索 ISE 中配置的所有终端配置文件（分析策略）

EndpointSecurityGroup_Query - 检索 ISE 中配置的所有 TrustSec 安全组 SecurtiyGroup_Subscribe - 订阅

ISE 中配置的 TrustSec 安全组中的更改

ANCaction_query - 提供自定义的 pxGrid ANC 缓解操作：隔离、补救、调配、关闭端口、端口反弹

使用 RADIUS 模拟程序测试脚本

Multigroupclient

验证

此测试用于验证第三方系统是否可以在 pxGrid 上注册到多客户端组（会话、ANC），即是否可通过身份验证和获得授权。

定义

PxGrid 客户端注册连接并将第三方应用、安全设备注册到授权的**会话**或 **ANC** 组，或在此示例中，将 Linux 主机注册到 pxGrid 控制器。其他组（如管理和基础）可用，但是，**管理**组专为 ISE 和**基础**组保留，并需要 pxGrid 管理批准，不会用于任何注册 pxGrid 示例。

所有注册的 pxGrid 客户端都可在“管理”(Administration) 下的 ISE pxGrid 服务视图中查看。

pxGrid 客户端可以是信息的发布服务器或用户，这一点将在“动态主题”中进行说明。ISE 将无法使用信息，注册的客户端之间将共享上下文信息。一旦 pxGrid 客户端成功注册到已获得授权的组，该客户端将可以获得相关会话信息或查询，如 pxGrid 示例脚本所确定的那样。

注意：在这些示例中，pxGrid 客户端将订阅 SessionDirectory、EndpointProtectionService 和 TrustSecMedata 功能。

示例

在此示例中，我们会将 Linux 主机作为会话组的 pxGrid 客户端注册到 pxGrid 控制器。Linux 主机 SIM0 是 pxGrid 客户端的用户名。我们还将在 ISE 中查看注册的 pxGrid 客户端。

第 1 步　　运行 multigroupclient 脚本

```
./multigroupclient.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果：

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session,ANC,
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
10:33:58.911 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
10:34:03.470 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
```

```
Create ANC Policy: ANC1438526035992 Result -
  com.cisco.pxgrid.model.anc.ANCResult@612fc6eb[ ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=<null>
  ancpolicies=<null>
]
Session 1.1.1.2 not found
Connection closed
10:34:04.385 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Stopped
Johns-MacBook-Pro:bin jeppich$
```

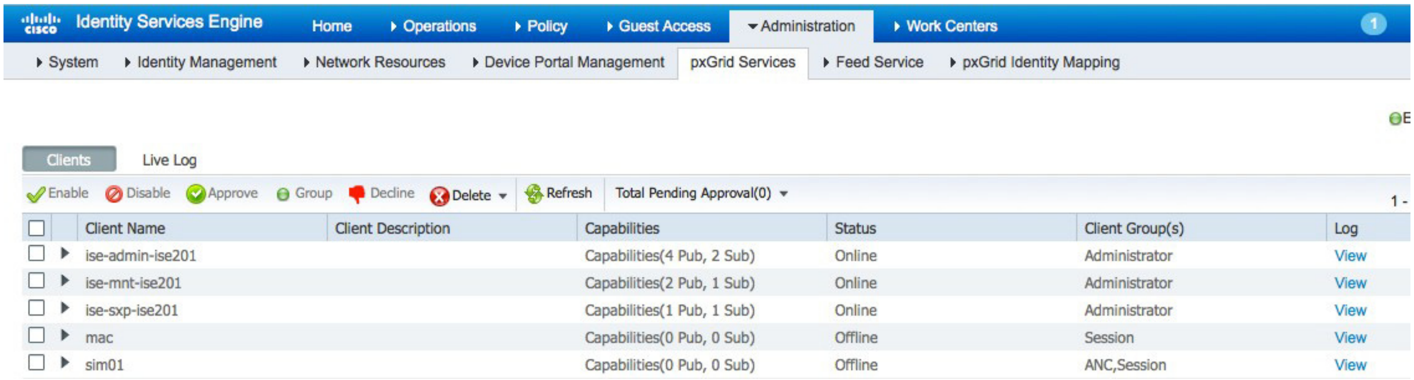
用法：

```
Usage: ./multigroupclient.sh [options]

  Main options
    -a <PXGRID_HOSTNAMES> (comma separated hostnames)
    -u <PXGRID_USERNAME>
    -g <PXGRID_GROUP>
    -d <PXGRID_DESCRIPTION>

  The followings are certificates options
    -k <PXGRID_KEYSTORE_FILENAME>
    -p <PXGRID_KEYSTORE_PASSWORD>
    -t <PXGRID_TRUSTSTORE_FILENAME>
    -q <PXGRID_TRUSTSTORE_PASSWORD>
  If not specified, it defaults to use clientSample1.jks and rootSample.jks
  Specifying values here can override the defaults

  Custom config file can fill or override parameters
    -c <config_filename>
  Config file are being sourced.Use these variables:
        PXGRID_HOSTNAMES
        PXGRID_USERNAME
        PXGRID_GROUP
        PXGRID_DESCRIPTION
        PXGRID_KEYSTORE_FILENAME
        PXGRID_KEYSTORE_PASSWORD
        PXGRID_TRUSTSTORE_FILENAME
        PXGRID_TRUSTSTORE_PASSWORD
```

结果：

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session,ANC,Session
  description=pxGrid
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
09:35:31.772 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
09:35:35.769 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Create ANC Policy: ANC1437658531354 Result -
  com.cisco.pxgrid.model.anc.ANCResult@612fc6eb[ ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=<null>
  ancpolicies=<null>
]
Session 1.1.1.2 not found
Connection closed
```

第 2 步　选择**管理 (Administration)->pxGrid 服务 (pxGrid Services)**
将 pxGrid 客户端 sim01 注册到会话客户端组。默认情况下会添加 ANC，这是 pxGrid 自适应网络控制 (ANC) 缓解操作所必需的。



□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▶	ise-admin-ise201		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▶	ise-mnt-ise201		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▶	ise-sxp-ise201		Capabilities(1 Pub, 1 Sub)	Online	Administrator	View
□	▶	mac		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	▶	sim01		Capabilities(0 Pub, 0 Sub)	Offline	ANC,Session	View

会话订阅

验证

此测试用于验证一旦第三方系统成功注册到 pxGrid 控制器，pxGrid 客户端是否会订阅 ISE 发布的会话目录以实时接收通知。

定义

一旦客户端成功注册到 pxGrid 控制器的会话和 ANC 组并获得授权，客户端便会订阅此功能并获取已通过身份验证的用户的相关会话信息。ISE MnT 节点将发布 ISE 会话目录作为 pxGrid 控制器的主题。pxGrid 客户端将订阅此功能并实时获取已通过身份验证的用户的活动会话和通知。

示例

pxGrid 客户端将订阅会话目录并实时接收用户 1、用户 2 和用户 3 身份验证的通知，并记录可用的上下文信息。

第 1 步　运行 session_subscribe 脚本

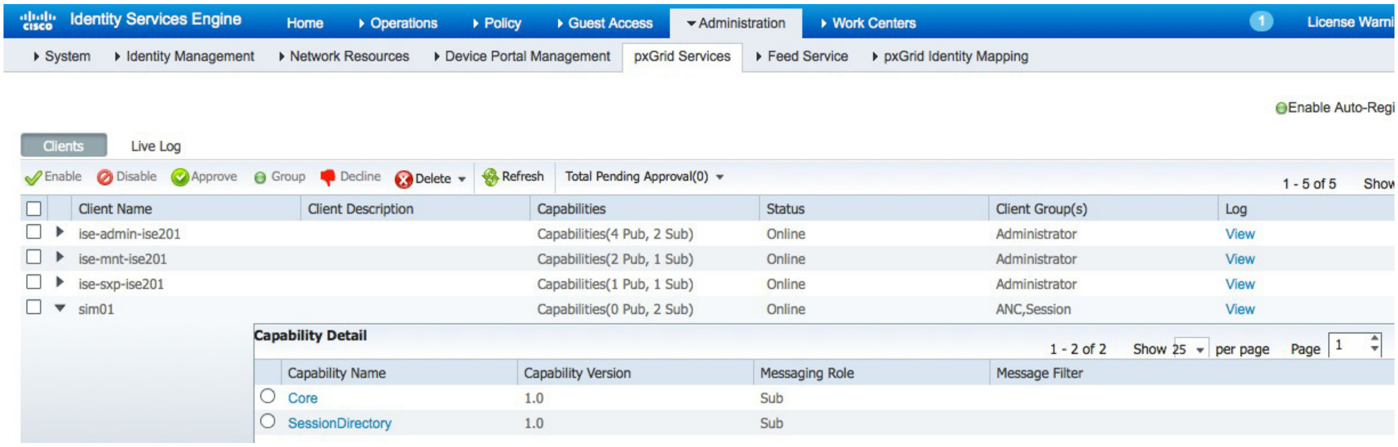
```
./session_subscribe.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
10:41:17.909 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
Filters (ex.'1.0.0.0/255.0.0.0,1234::/16,...' or <enter> for no filter): 10:41:19.311 [Thread-1] INFO
com.cisco.pxgrid.ReconnectionManager - Connected
Connected
```

第 2 步　**选择管理 (Administration)->pxGrid 服务 (pxGrid Services)**

pxGrid 客户端 SIM01 已订阅会话目录



□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▶	ise-admin-ise201		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▶	ise-mnt-ise201		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▶	ise-sxp-ise201		Capabilities(1 Pub, 1 Sub)	Online	Administrator	View
□	▼	sim01		Capabilities(0 Pub, 2 Sub)	Online	ANC,Session	View

Capability Detail

1 - 2 of 2　Show 25 per page　Page 1

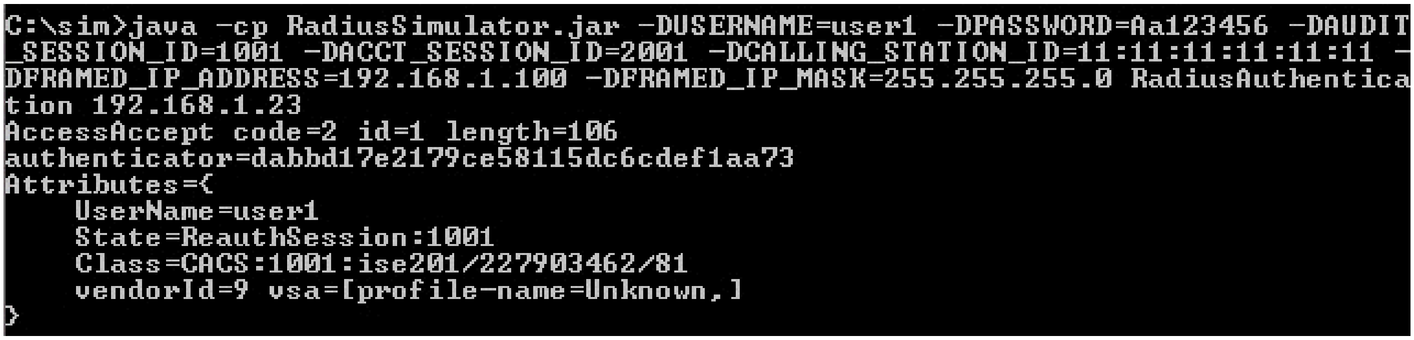
	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	SessionDirectory	1.0	Sub	

第 3 步　在客户端 PC 上运行 RADIUS 模拟程序，以模拟用户 1、用户 2 和用户 3 的 IEE 802.1X 身份验证

第 4 步　从 RadiusAuthentication 开始，为用户 1 运行 RADIUS 模拟程序

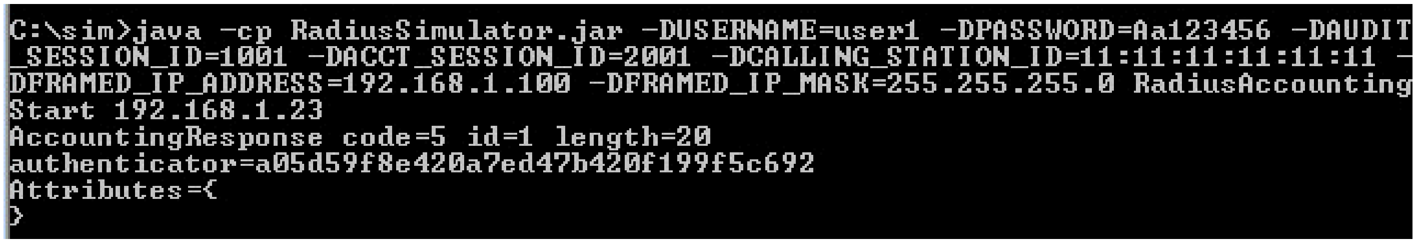
注意： 重要的一点是，每个用户的用户名、audit_session_id、acct_session_id、calling_station_id、framed_ip_address 都不同。放置顺序非常重要。

将 acct_session_id 包含在内也很重要；否则您将看到上个用户的会话。



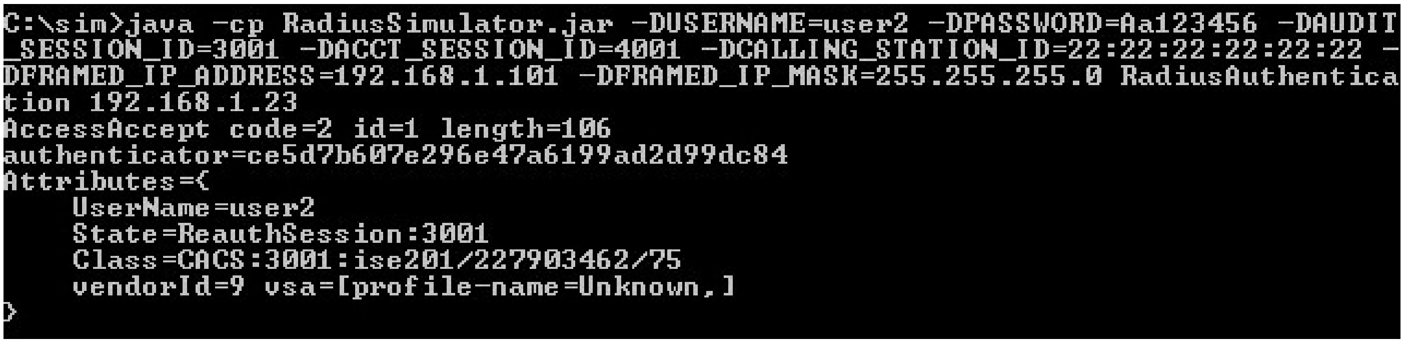
```
C:\sim>java -cp RadiusSimulator.jar -DUSERNAME=user1 -DPASSWORD=Aa123456 -DAUDIT
_SESSION_ID=1001 -DACCT_SESSION_ID=2001 -DCALLING_STATION_ID=11:11:11:11:11:11 -
DFRAMED_IP_ADDRESS=192.168.1.100 -DFRAMED_IP_MASK=255.255.255.0 RadiusAuthentica
tion 192.168.1.23
AccessAccept code=2 id=1 length=106
authenticator=dabbd17e2179ce58115dc6cdef1aa73
Attributes={
    UserName=user1
    State=ReauthSession:1001
    Class=CACS:1001:ise201/227903462/81
    vendorId=9 vsa=[profile-name=Unknown,]
}
```

第 5 步　使用 RadiusAccountingStart，为用户 1 运行 RADIUS 模拟程序



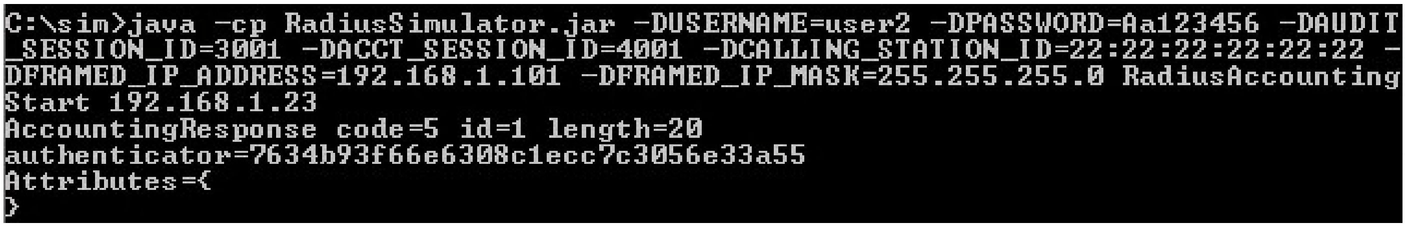
```
C:\sim>java -cp RadiusSimulator.jar -DUSERNAME=user1 -DPASSWORD=Aa123456 -DAUDIT
_SESSION_ID=1001 -DACCT_SESSION_ID=2001 -DCALLING_STATION_ID=11:11:11:11:11:11 -
DFRAMED_IP_ADDRESS=192.168.1.100 -DFRAMED_IP_MASK=255.255.255.0 RadiusAccounting
Start 192.168.1.23
AccountingResponse code=5 id=1 length=20
authenticator=a05d59f8e420a7ed47b420f199f5c692
Attributes={
}
```

第 6 步　使用 RadiusAuthentication，为用户 2 运行 RADIUS 模拟程序



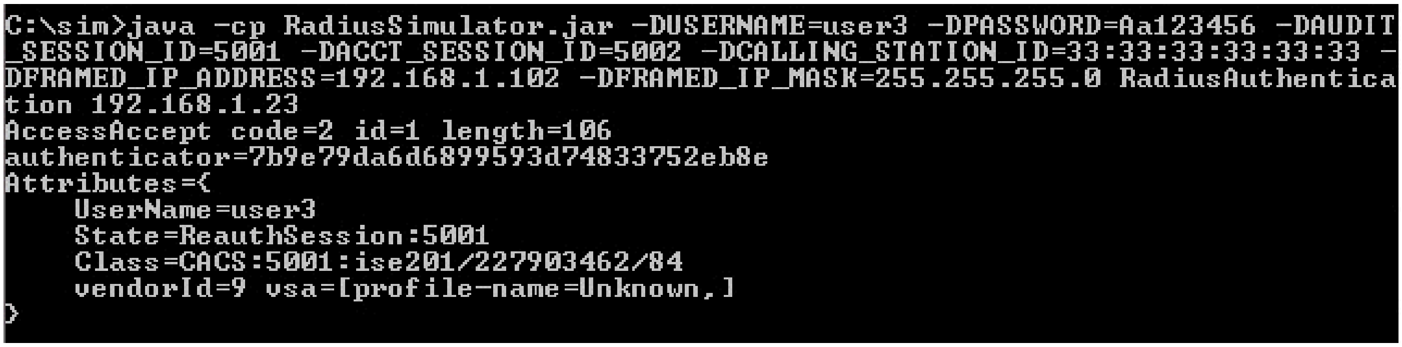
```
C:\sim>java -cp RadiusSimulator.jar -DUSERNAME=user2 -DPASSWORD=Aa123456 -DAUDIT
_SESSION_ID=3001 -DACCT_SESSION_ID=4001 -DCALLING_STATION_ID=22:22:22:22:22:22 -
DFRAMED_IP_ADDRESS=192.168.1.101 -DFRAMED_IP_MASK=255.255.255.0 RadiusAuthentica
tion 192.168.1.23
AccessAccept code=2 id=1 length=106
authenticator=ce5d7b607e296e47a6199ad2d99dc84
Attributes={
    UserName=user2
    State=ReauthSession:3001
    Class=CACS:3001:ise201/227903462/75
    vendorId=9 vsa=[profile-name=Unknown,]
}
```

第 7 步　使用 RadiusAccounting，为用户 2 运行 RADIUS 模拟程序



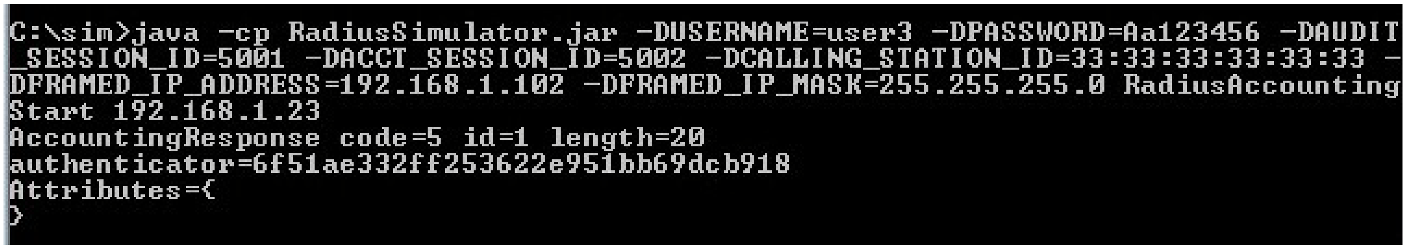
```
C:\sim>java -cp RadiusSimulator.jar -DUSERNAME=user2 -DPASSWORD=Aa123456 -DAUDIT
_SESSION_ID=3001 -DACCT_SESSION_ID=4001 -DCALLING_STATION_ID=22:22:22:22:22:22 -
DFRAMED_IP_ADDRESS=192.168.1.101 -DFRAMED_IP_MASK=255.255.255.0 RadiusAccounting
Start 192.168.1.23
AccountingResponse code=5 id=1 length=20
authenticator=7634b93f66e6308c1ecc7c3056e33a55
Attributes={
}
```

第 8 步　使用 RadiusAuthentication，为用户 3 运行 RADIUS 模拟程序



```
C:\sim>java -cp RadiusSimulator.jar -DUSERNAME=user3 -DPASSWORD=Aa123456 -DAUDIT
_SESSION_ID=5001 -DACCT_SESSION_ID=5002 -DCALLING_STATION_ID=33:33:33:33:33:33 -
DFRAMED_IP_ADDRESS=192.168.1.102 -DFRAMED_IP_MASK=255.255.255.0 RadiusAuthentica
tion 192.168.1.23
AccessAccept code=2 id=1 length=106
authenticator=7b9e79da6d6899593d74833752eb8e
Attributes={
    UserName=user3
    State=ReauthSession:5001
    Class=CACS:5001:ise201/227903462/84
    vendorId=9 vsa=[profile-name=Unknown,]
}
```

第 9 步　使用 RadiusAccountingStart，为用户 3 运行 RADIUS 模拟程序



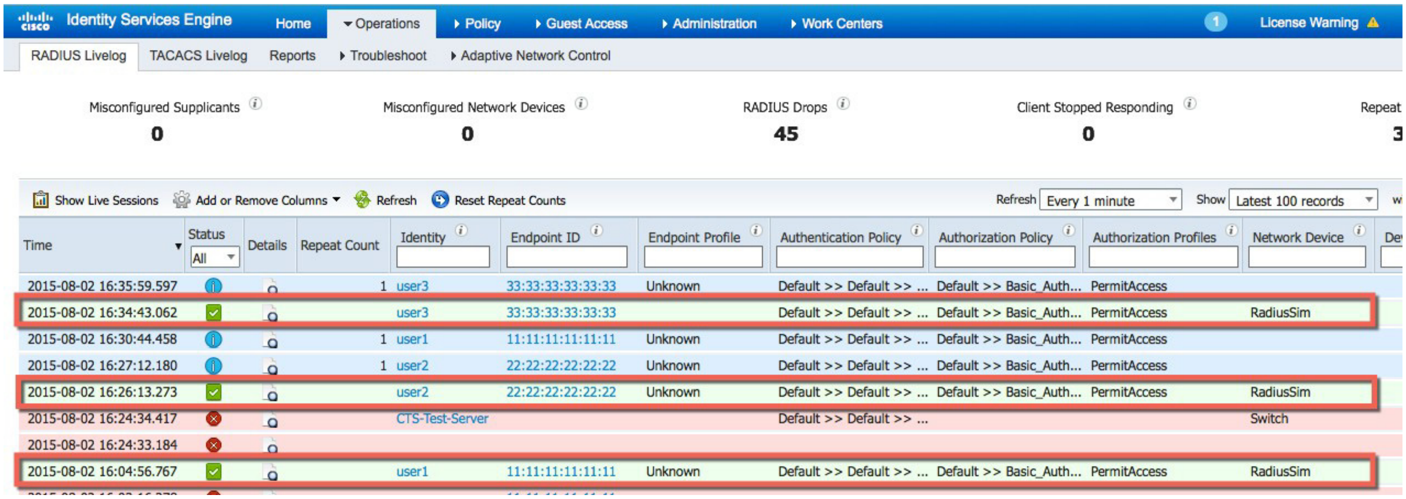
```
C:\sim>java -cp RadiusSimulator.jar -DUSERNAME=user3 -DPASSWORD=Aa123456 -DAUDIT
_SESSION_ID=5001 -DACCT_SESSION_ID=5002 -DCALLING_STATION_ID=33:33:33:33:33:33 -
DFRAMED_IP_ADDRESS=192.168.1.102 -DFRAMED_IP_MASK=255.255.255.0 RadiusAccounting
Start 192.168.1.23
AccountingResponse code=5 id=1 length=20
authenticator=6f51ae332ff253622e951bb69dcb918
Attributes={
}
```

第 10 步　注意每个用户会话可用的上下文信息在下面高亮显示。这些会话对象可在第三方应用中使用，以获得事件的更多上下文

```
./session_subscribe.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:28:19.187 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
Filters (ex.'1.0.0.0/255.0.0.0,1234::/16,...' or <enter> for no filter): 11:28:20.547 [Thread-1] INFO
com.cisco.pxgrid.ReconnectionManager - Connected

press <enter> to disconnect...session notification:
Session={ip=[192.168.1.101], Audit Session Id=3001, User Name=user2, AD User DNS Domain=null, AD Host DNS
Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station id=22:22:22:22:22:22,
Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Unknown, NAS IP=192.168.1.37,
RADIUSAVPairs=[ Acct-Session-Id=4001], Posture Status=null, Posture Timestamp=, Session Last Update Time=Sun
Aug 02 12:27:12 EDT 2015}

session notification:
Session={ip=[192.168.1.100], Audit Session Id=1001, User Name=user1, AD User DNS Domain=null, AD Host DNS
Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station id=11:11:11:11:11:11,
Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Unknown, NAS IP=192.168.1.37,
RADIUSAVPairs=[ Acct-Session-Id=2001], Posture Status=null, Posture Timestamp=, Session Last Update Time=Sun
Aug 02 12:30:44 EDT 2015}

session notification:
```

```
Session={ip=[192.168.1.102], Audit Session Id=5001, User Name=user3, AD User DNS Domain=null, AD Host DNS
Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station id=33:33:33:33:33:33,
Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Unknown, NAS IP=192.168.1.37,
RADIUSAVPairs=[ Acct-Session-Id=5002], Posture Status=null, Posture Timestamp=, Session Last Update Time=Sun
Aug 02 12:35:59 EDT 2015}
```

第 11 步 选择**操作** (Operations)->RADIUS Livelog 查看事件



Misconfigured Supplicants 0 | Misconfigured Network Devices 0 | RADIUS Drops 45 | Client Stopped Responding 0 | Repeat 3

Refresh Every 1 minute | Show Latest 100 records

Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	De
2015-08-02 16:35:59.597	ⓘ		1	user3	33:33:33:33:33:33	Unknown	Default >> Default >> ...	Default >> Basic_Auth...	PermitAccess		
2015-08-02 16:34:43.062	✓			user3	33:33:33:33:33:33		Default >> Default >> ...	Default >> Basic_Auth...	PermitAccess	RadiusSim	
2015-08-02 16:30:44.458	ⓘ		1	user1	11:11:11:11:11:11	Unknown	Default >> Default >> ...	Default >> Basic_Auth...	PermitAccess		
2015-08-02 16:27:12.180	ⓘ		1	user2	22:22:22:22:22:22	Unknown	Default >> Default >> ...	Default >> Basic_Auth...	PermitAccess		
2015-08-02 16:26:13.273	✓			user2	22:22:22:22:22:22	Unknown	Default >> Default >> ...	Default >> Basic_Auth...	PermitAccess	RadiusSim	
2015-08-02 16:24:34.417	☒			CTS-Test-Server			Default >> Default >> ...			Switch	
2015-08-02 16:24:33.184	☒										
2015-08-02 16:04:56.767	✓			user1	11:11:11:11:11:11	Unknown	Default >> Default >> ...	Default >> Basic_Auth...	PermitAccess	RadiusSim	

会话下载

验证

此测试用于验证第三方系统执行活动用户会话批量会话下载的能力。

定义

会话下载脚本从发布的 ISE 节点下载批量会话记录。

示例

pxGrid 客户端将从 ISE MnT 节点下载活动的会话。

```
./session_download.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
-------------------------------
12:23:49.800 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
Filters (ex.'1.0.0.0/255.0.0.0,1234::/16...' or <enter> for no filter): 12:23:51.043 [Thread-1] INFO
com.cisco.pxgrid.ReconnectionManager - Connected

Start time (ex.'2015-01-31 13:00:00' or <enter> for no start time):
End time (ex.'2015-01-31 13:00:00' or <enter> for no end time):
Session={ip=[192.168.1.31], Audit Session Id=0A0000010000002803DBE3C1, User Name=LAB6\jeppich, AD User DNS
Domain=lab6.com, AD Host DNS Domain=null, AD User NetBIOS Name=LAB6, AD Host NETBIOS Name=null, Calling
station id=00:0C:29:79:02:A8, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint
Profile=Windows7-Workstation, NAS IP=192.168.1.2, NAS Port=GigabitEthernet1/0/12, RADIUSAVPairs=[ Acct-
Session-Id=00000053], Posture Status=NonCompliant, Posture Timestamp=Sat Aug 01 15:15:20 EDT 2015, Session
Last Update Time=Sat Aug 01 15:15:22 EDT 2015}
Session={ip=[192.168.1.100], Audit Session Id=1001, User Name=user1, AD User DNS Domain=null, AD Host DNS
Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station id=11:11:11:11:11:11,
Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Unknown, NAS IP=192.168.1.37,
RADIUSAVPairs=[ Acct-Session-Id=2001], Posture Status=null, Posture Timestamp=, Session Last Update Time=Sun
Aug 02 12:30:44 EDT 2015}
Session={ip=[192.168.1.101], Audit Session Id=3001, User Name=user2, AD User DNS Domain=null, AD Host DNS
Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station id=22:22:22:22:22:22,
Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Unknown, NAS IP=192.168.1.37,
RADIUSAVPairs=[ Acct-Session-Id=4001], Posture Status=null, Posture Timestamp=, Session Last Update Time=Sun
Aug 02 12:27:12 EDT 2015}
Session={ip=[192.168.1.102], Audit Session Id=5001, User Name=user3, AD User DNS Domain=null, AD Host DNS
Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station id=33:33:33:33:33:33,
Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Unknown, NAS IP=192.168.1.37,
RADIUSAVPairs=[ Acct-Session-Id=5002], Posture Status=null, Posture Timestamp=, Session Last Update Time=Sun
Aug 02 12:35:59 EDT 2015}
Session count=4
Connection closed
12:23:59.504 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Stopped
Johns-MacBook-Pro:bin jeppich$
```

按 IP 进行的会话查询

验证

此测试用于验证第三方系统通过 pxGrid 执行有关特定 IP 地址的定向查询并从用户返回上下文信息的能力。

定义

按 IP 脚本进行的会话查询会按 IP 地址获取已通过身份验证的用户的会话信息。

示例

在此示例中，我们通过输入最终用户的 IP 地址来获取最终用户会话信息，即 192.168.1.100。

第 1 步　　运行 session_query_by_ip 脚本

```
./session_query_by_ip.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
12:30:45.610 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
12:30:46.935 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
IP address (or <enter> to disconnect): 192.168.1.100
Session={ip=[192.168.1.100], Audit Session Id=1001, User Name=user1, AD User DNS Domain=null, AD Host DNS
Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station id=11:11:11:11:11:11,
Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Unknown, NAS IP=192.168.1.37,
RADIUSAVPairs=[ Acct-Session-Id=2001], Posture Status=null, Posture Timestamp=, Session Last Update Time=Sun
Aug 02 12:30:44 EDT 2015}
IP address (or <enter> to disconnect):
```

EndpointProfile 订阅

验证

此测试用于验证第三方系统订阅发布的终端配置文件主题的能力。

定义

注册的 pxGrid 客户端将订阅 EndpointProfileMetaData 功能，以获取全局分析策略中的更改或修改。会话通知将包含终端配置文件 ID、名称和完全限定的名称。

示例

在此示例中，将根据用户 PC 的静态 MAC 地址创建 pxGrid EndpointProfile 示例策略。当 pxGrid 客户端订阅 EndpointprofileMetadata 功能且 ISE 分析策略有任何修改时，我们将实时在正在运行的 Linux 脚本中看到会话通知。

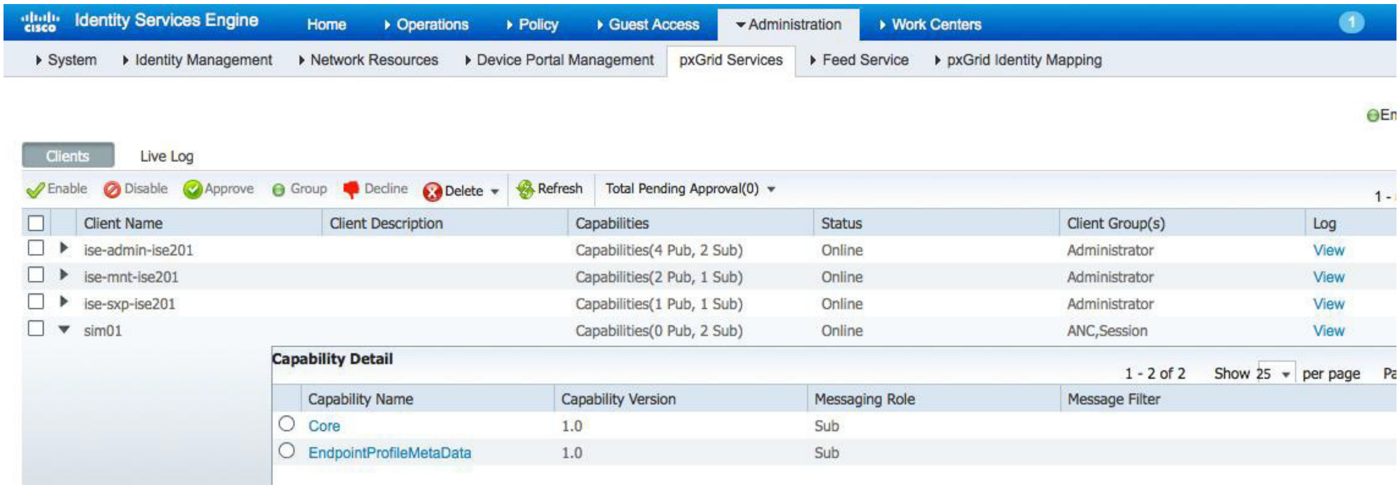
第 1 步　　运行 endpointprofile_subscribe 脚本

```
./endpointprofile_subscribe.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q
cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
12:41:22.280 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
12:41:23.552 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Press <enter> to disconnect...
```

第 2 步　选择**管理 (Administrations)->pxGrid** 服务 **(pxGrid Services)**。
pxGrid 客户端已订阅 EndpointProfileMetaData 功能



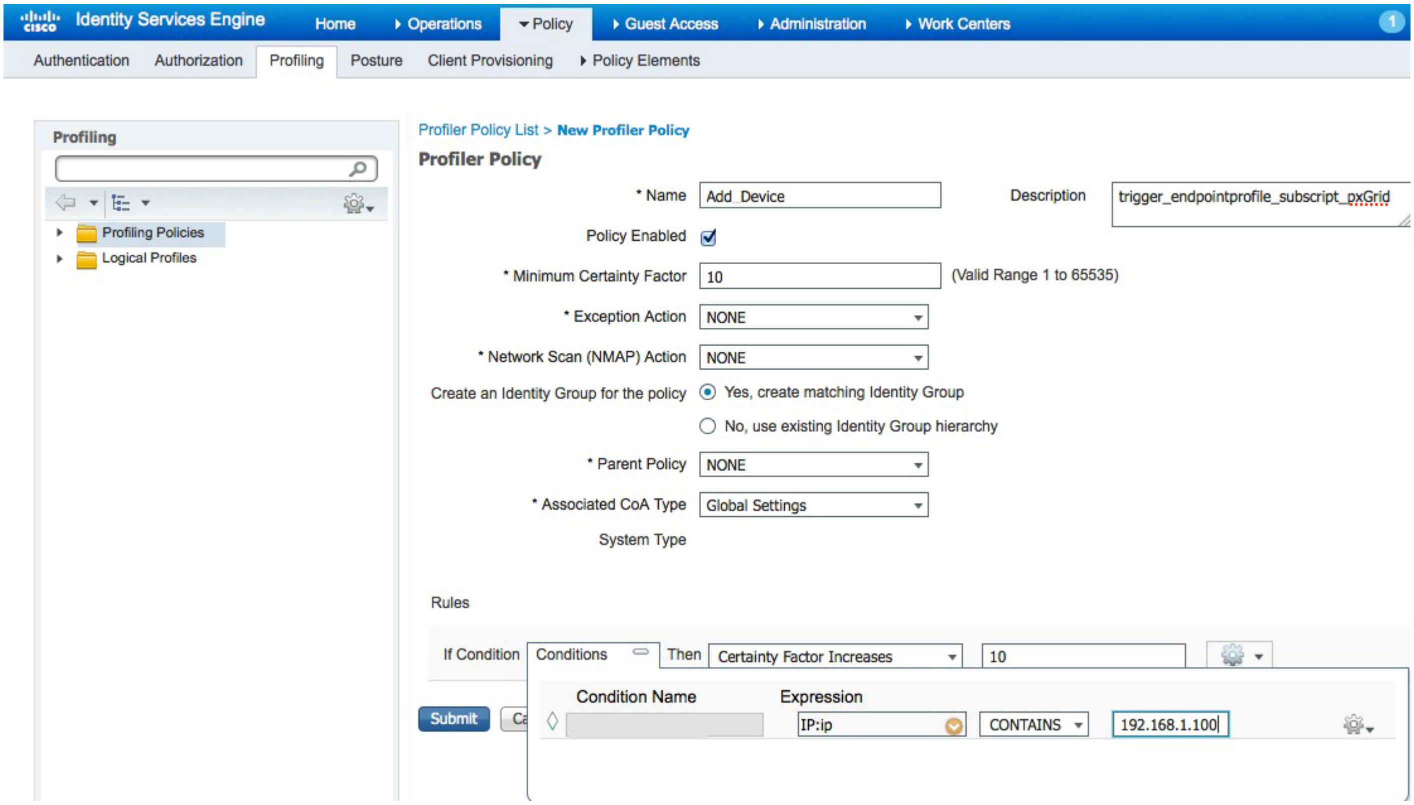
□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▶	ise-admin-ise201		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▶	ise-mnt-ise201		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▶	ise-sxp-ise201		Capabilities(1 Pub, 1 Sub)	Online	Administrator	View
□	▼	sim01		Capabilities(0 Pub, 2 Sub)	Online	ANC,Session	View

Capability Detail

1 - 2 of 2　Show 25 per page　Pa

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	EndpointProfileMetaData	1.0	Sub	

第 3 步　选择**策略 (Policy)->**分析 **(Profiling)->**添加 **(Add)**
提供策略名称和说明
在**如果条件 (If Condition)->**创建新条件 **(Create New Condition)->IP->{**提供访问网络的设备的 **IP 地址}** 下，选择**->**提交 **(Submit)**



Profiler Policy List > **New Profiler Policy**

Profiler Policy

* Name: Add_Device

Description: trigger_endpointprofile_subscript_pxGrid

Policy Enabled: ☑

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: ● Yes, create matching Identity Group ○ No, use existing Identity Group hierarchy

* Parent Policy: NONE

* Associated CoA Type: Global Settings

System Type

Rules

If Condition: Conditions Then: Certainty Factor Increases 10

Condition Name | Expression: IP:ip CONTAINS 192.168.1.100

第 4 步　您将收到一条终端配置文件订阅通知，说明您创建的分析策略已添加

```
./endpointprofile_subscribe.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q
cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
12:41:22.280 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
12:41:23.552 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Press <enter> to disconnect...EndpointProfileChangedNotification (changetype=ADD) Device profile :
id=8c8f42b0-393f-11e5-ac86-000c297fb12a, name=Add_Device, fqname=Add_Device
```

身份组下载

验证

此测试用于验证第三方系统执行用户身份信息批量下载的能力。

定义

身份组下载脚本会从会话目录下载用户组信息和用户组映射的批量会话记录。这些组包括 ISE 身份组和已分析的组。

示例

我们使用身份组下载脚本从 ISE MnT 节点发布服务器下载所有组信息。

第 1 步　运行 identity_group_download 脚本

```
./identity_group_download.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
13:01:21.977 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
13:01:23.242 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
user=host/jeppich-PC.lab6.com groups=Workstation
user=LAB6\jeppich groups=Workstation
user=user1 groups=User Identity Groups:Employee,Unknown
user=user2 groups=User Identity Groups:Employee,Unknown
user=user3 groups=User Identity Groups:Employee
User count=5
Connection closed
```

安全组查询

验证

此测试用于验证第三方系统检索 ISE 中所有安全组标记的能力。

定义

安全组查询脚本通过 TrustSecMetadata 功能主题公开 ISE 中配置的安全组标记 (SGT)。它提供一个查询方法，来根据唯一 ID、安全组标记值和说明检索 ISE 中配置的所有 SGT。

示例

在此示例中，安全组查询脚本将下载所有安全组标记上下文信息。此脚本会从 ISE 检索所有 TrustSec 安全组会话信息，这包括 TrustSec 标记名称、唯一标识符、说明和值。

对安全组标记的查询定向。

第 1 步　运行 securitygroup_query 脚本

```
./securitygroup_query.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
13:04:24.807 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
13:04:26.071 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
SecurityGroup : id=65fddc70-2a34-11e5-82cb-005056bf2f0a, name=Unknown, desc=Unknown Security Group, tag=0
SecurityGroup : id=660aadb0-2a34-11e5-82cb-005056bf2f0a, name=ANY, desc=Any Security Group, tag=65535
SecurityGroup : id=669e6230-2a34-11e5-82cb-005056bf2f0a, name=SGT_Auditor, desc=Auditor Security Group, tag=9
SecurityGroup : id=66bdd110-2a34-11e5-82cb-005056bf2f0a, name=SGT_BYOD, desc=BYOD Security Group, tag=15
SecurityGroup : id=66dd3ff0-2a34-11e5-82cb-005056bf2f0a, name=SGT_Contractor, desc=Contractor Security Group,
tag=5
SecurityGroup : id=66fcd5e0-2a34-11e5-82cb-005056bf2f0a, name=SGT_Developer, desc=Developer Security Group,
tag=8
SecurityGroup : id=671a21e0-2a34-11e5-82cb-005056bf2f0a, name=SGT_DevelopmentServers, desc=Development
Servers Security Group, tag=12
SecurityGroup : id=673c9e00-2a34-11e5-82cb-005056bf2f0a, name=SGT_Employee, desc=Employee Security Group,
tag=4
SecurityGroup : id=6759ea00-2a34-11e5-82cb-005056bf2f0a, name=SGT_Guest, desc=Guest Security Group, tag=6
SecurityGroup : id=6775d670-2a34-11e5-82cb-005056bf2f0a, name=SGT_NetworkServices, desc=Network Services
Security Group, tag=3
SecurityGroup : id=67959370-2a34-11e5-82cb-005056bf2f0a, name=SGT_PCIServers, desc=PCI Servers Security
Group, tag=14
```

```
SecurityGroup : id=67b3a2c0-2a34-11e5-82cb-005056bf2f0a, name=SGT PointOfSale, desc=PointOfSale Security
Group, tag=10
SecurityGroup : id=67d50d70-2a34-11e5-82cb-005056bf2f0a, name=SGT_ProductionServers, desc=Production Servers
Security Group, tag=11
SecurityGroup : id=67f16f10-2a34-11e5-82cb-005056bf2f0a, name=SGT_ProductionUser, desc=Production User
Security Group, tag=7
SecurityGroup : id=680df7c0-2a34-11e5-82cb-005056bf2f0a, name=SGT_Quarantine, desc=Quarantine Security Group,
tag=255
SecurityGroup : id=682a5960-2a34-11e5-82cb-005056bf2f0a, name=SGT_TestServers, desc=Test Servers Security
Group, tag=13
SecurityGroup : id=68461ec0-2a34-11e5-82cb-005056bf2f0a, name=SGT_TrustSecDevices, desc=TrustSec Devices
Security Group, tag=2
SecurityGroup : id=1bea1190-37f8-11e5-aeb1-000c297fb12a, name=3750x, desc=, tag=16
SecurityGroup : id=e855d7c0-3805-11e5-aeb1-000c297fb12a, name=ASA5505, desc=, tag=17
SecurityGroup : id=c0e5a9d0-381a-11e5-aeb1-000c297fb12a, name=Mobile_Users, desc=, tag=18
Connection closed
13:04:26.450 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Stopped
Johns-MacBook-Pro:bin jeppich$
```

安全组订阅

验证

此测试用于验证第三方系统通过 pxGrid 订阅 SecurityGroup 主题的能力。

定义

安全组订阅脚本通过 TrustsecMetaDataCapability 主题公开 ISE 中配置的安全组标记 (SGT)。如果添加/更新/删除了安全组，脚本会话通知中会显示安全组更改通知。

示例

安全组订阅脚本订阅 ISE TrustSec 策略中的更改。我们将在 ISE 中添加一个安全组标记。因为 pxGrid 客户端已订阅 TrutSecMetadataCapability 主题，我们将收到通知。

第 1 步　运行 security_subscribe 脚本

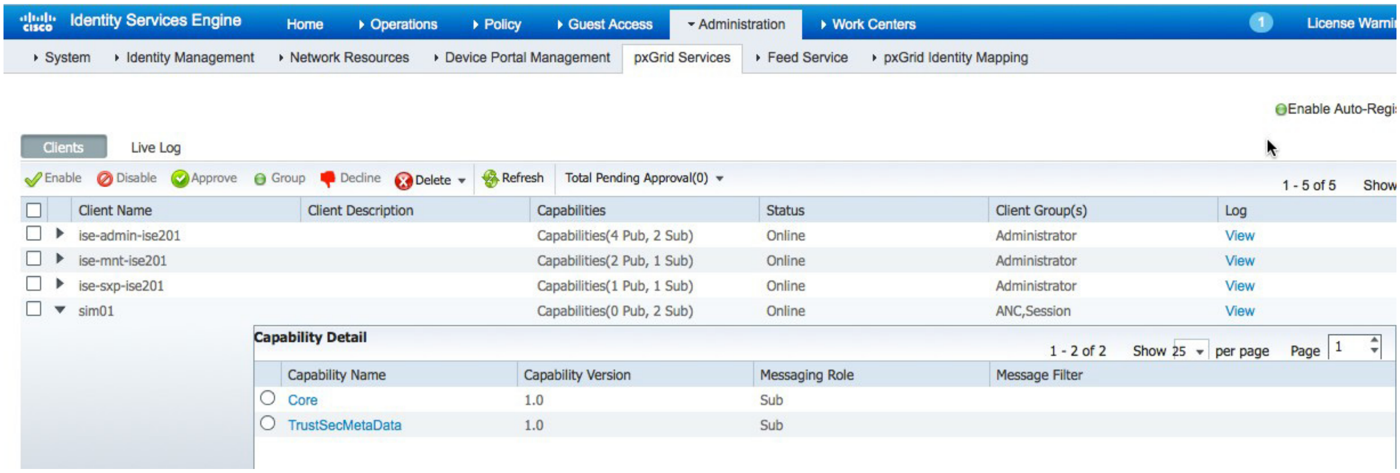
```
./securitygroup_subscribe.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
13:07:12.322 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
```

```
Connected
13:07:13.613 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Press <enter> to disconnect...
```

第 2 步 选择管理 (Administration)->pxGrid 服务 (pxGrid Service)
您会看到 smc01 已注册到 TrustsecMetadata 功能



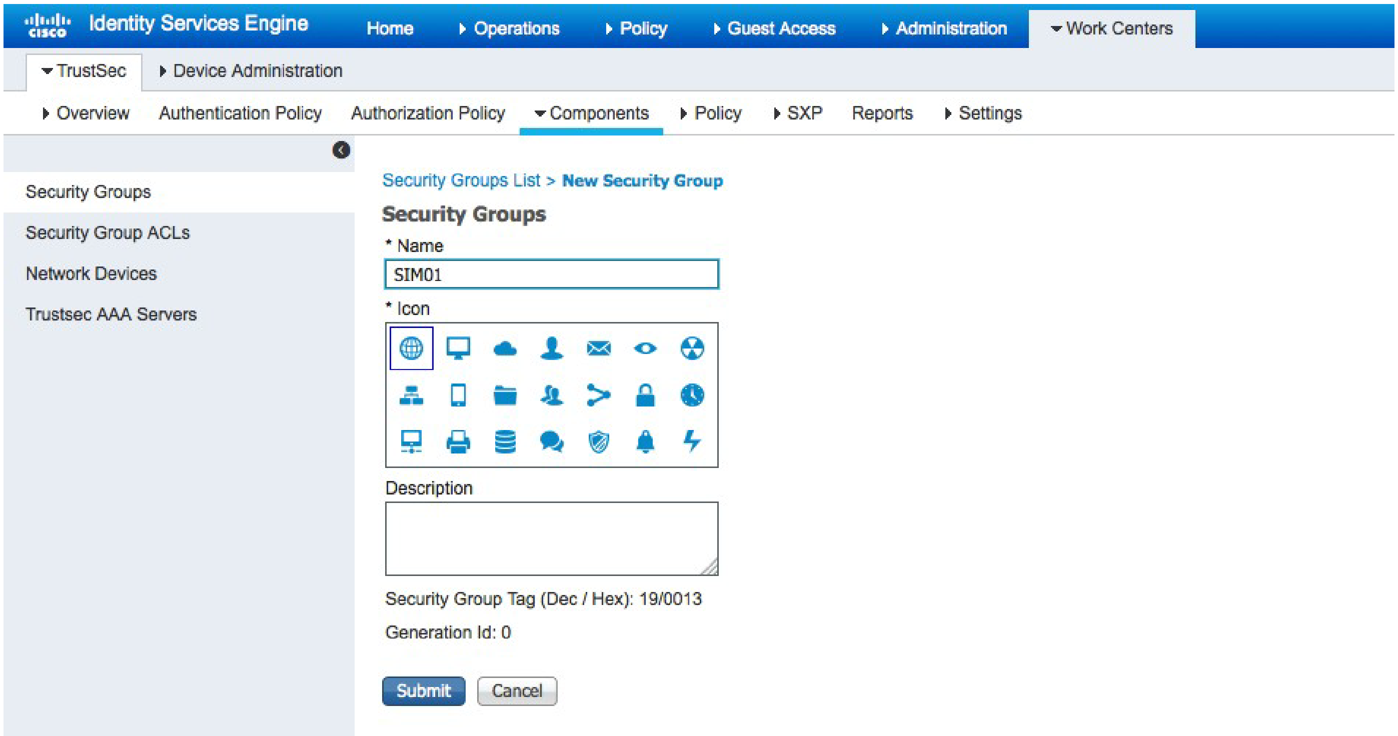
	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□ ▸	ise-admin-ise201		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□ ▸	ise-mnt-ise201		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□ ▸	ise-sxp-ise201		Capabilities(1 Pub, 1 Sub)	Online	Administrator	View
□ ▾	sim01		Capabilities(0 Pub, 2 Sub)	Online	ANC,Session	View

Capability Detail

1 - 2 of 2 Show 25 per page Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	TrustSecMetaData	1.0	Sub	

第 3 步 选择工作中心 (Work Centers)->TrustSec->组件 (Components)->安全组 (Security Groups)->新的安全组 (New Security Group)->SMC01



Security Groups List > **New Security Group**

Security Groups

* Name: SIM01

* Icon

Description

Security Group Tag (Dec / Hex): 19/0013

Generation Id: 0

第 4 步　　系统将显示安全组标记通知

```
./securitygroup_subscribe.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
13:07:12.322 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
13:07:13.613 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Connected
Press <enter> to disconnect...SecurityGroupChangeNotification (changetype=ADD) SecurityGroup : id=994e2140-
3941-11e5-ac86-000c297fb12a, name=SIM01, desc=, tag=19
```

终端配置文件查询

验证

此测试用于验证第三方系统检索 ISE 中配置的所有已启用配置文件的能力。

定义

endpointprofile_query 脚本提供一个查询方法，来检索 ISE 中配置的所有已启用的终端配置文件，并提供终端配置文件 ID、名称和完全限定的名称。如果 ISE 中添加/更新/删除了终端配置文件，用户还将收到通知。

示例

endpointprofile 查询脚本检索 ISE 中所有已启用的配置文件。

第 1 步　　运行 endpointprofile_query 脚本

```
./endpointprofile_query.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
13:14:11.358 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
13:14:12.631 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Endpoint Profile : id=8c8f42b0-393f-11e5-ac86-000c297fb12a, name=Add_Device, fqname Add_Device
Endpoint Profile : id=4d852be0-2a33-11e5-82cb-005056bf2f0a, name=Android, fqname Android
Endpoint Profile : id=4dc7b320-2a33-11e5-82cb-005056bf2f0a, name=Apple-Device, fqname Apple-Device Endpoint
Profile : id=4e190770-2a33-11e5-82cb-005056bf2f0a, name=Apple-iDevice, fqname Apple-Device:Apple-
iDevice
Endpoint Profile : id=4e452080-2a33-11e5-82cb-005056bf2f0a, name=Apple-iPad, fqname Apple-Device:Apple-iPad
Endpoint Profile : id=4e6f8be0-2a33-11e5-82cb-005056bf2f0a, name=Apple-iPhone, fqname Apple-Device:Apple-
iPhone
```

功能

验证

此测试用于验证第三方系统检索 ISE 中所有已发布功能的能力。

定义

功能脚本检索 ISE 中所有已发布的兴趣主题。

示例

功能脚本检索客户端可发布或订阅的信息主题或功能。

第 1 步 运行功能脚本

```
./capability_query.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t
```

结果

```
alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=null
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
13:16:57.359 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
13:16:58.607 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
capability=SessionDirectory, version=1.0
capability=GridControllerAdminService, version=1.0
capability=EndpointProtectionService, version=1.0
capability=IdentityGroup, version=1.0
```

```
capability=EndpointProfileMetaData, version=1.0
capability=TrustSecMetaData, version=1.0
capability=AdaptiveNetworkControl, version=1.0
capability=Core, version=1.0
Connection closed
13:16:58.659 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Stopped
Johns-MacBook-Pro:bin jeppich$
```

身份组查询

验证

此测试用于验证第三方系统从指定用户检索 ISE 身份组信息的能力。

定义

身份组查询脚本检索 ISE 身份组信息。

示例

查询用户 1、用户 2 和用户 3 以获取 ISE 身份组信息。

第 1 步　运行 identity_group_query 脚本

```
./identity_group_query.sh -a 192.168.1.23 -u SIM01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM01
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
13:18:59.446 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
13:19:00.755 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
user name (or <enter> to disconnect): user1
group=User Identity Groups:Employee,Unknown
user name (or <enter> to disconnect): user2
group=User Identity Groups:Employee,Unknown
user name (or <enter> to disconnect): user3
group=User Identity Groups:Employee
user name (or <enter> to disconnect):
```

身份组订阅

验证

此测试用于验证第三方系统订阅 ISE 发布的身份主题及接收通知的能力。

定义

订阅身份组主题允许 pxGrid 客户端接收关于 802.1X 事件的通知。

示例

在 ISE 中创建内部网络用户，并用于测试访客门户，这将触发事件。

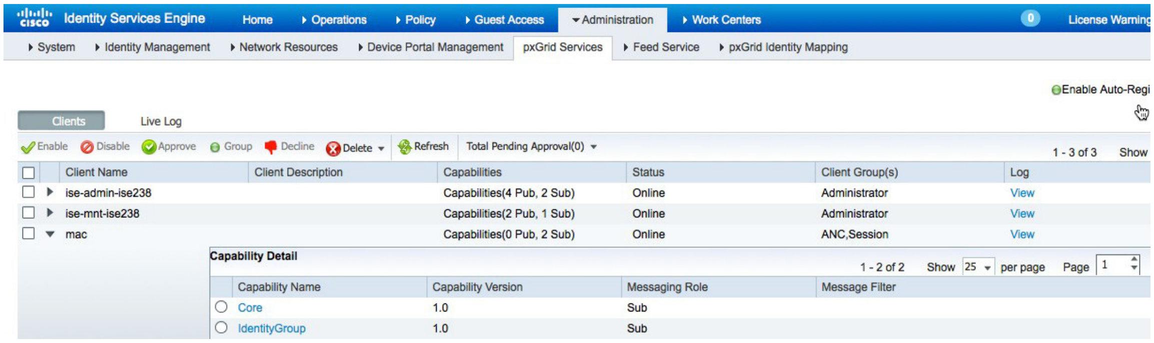
第 1 步　运行 identity_group_subscribe 脚本

```
/identity_group_subscribe.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:20:22.839 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
11:20:24.468 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Press <enter> to disconnect...
```

第 2 步　选择“管理”(Administration)->“pxGrid 服务”(pxGrid Service)，查看订阅的身份组会话



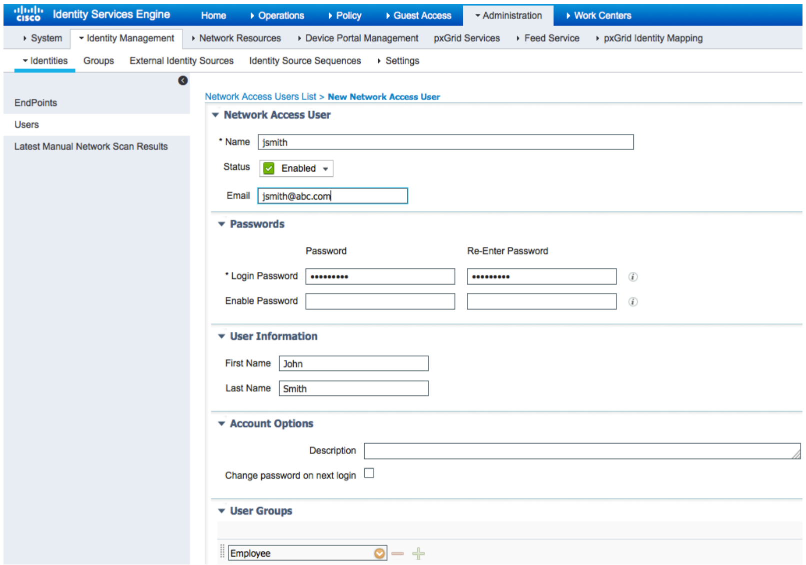
□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▶	ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▶	ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▼	mac		Capabilities(0 Pub, 2 Sub)	Online	ANC,Session	View

Capability Detail

1 - 2 of 2　Show 25 per page　Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	IdentityGroup	1.0	Sub	

第 3 步　创建用于访客门户的 ISE 身份用户，以触发员工



Network Access Users List > New Network Access User

Network Access User

* Name: jsmith

Status: ☑ Enabled

Email: jsmith@abc.com

Passwords

* Login Password — Password: •••••••••; Re-Enter Password: •••••••••

Enable Password — Password: ; Re-Enter Password:

User Information

First Name: John

Last Name: Smith

Account Options

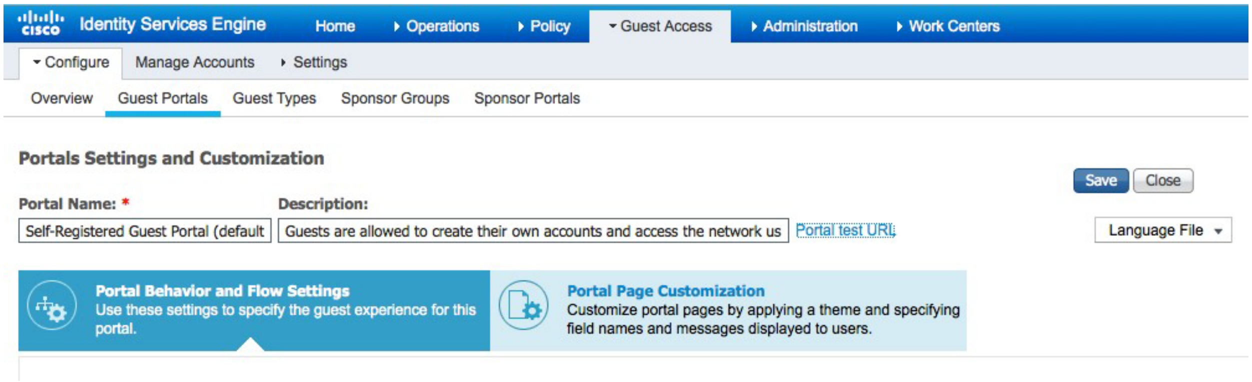
Description:

Change password on next login ☐

User Groups

Employee

第 4 步　使用默认自助服务门户测试来实时验证用户和关联的身份组，选择**访客接入 (Guest Access)->配置 (Configure)->访客门户 (Guest Portals)->门户测试 URL (Portal test URL)**



Portals Settings and Customization

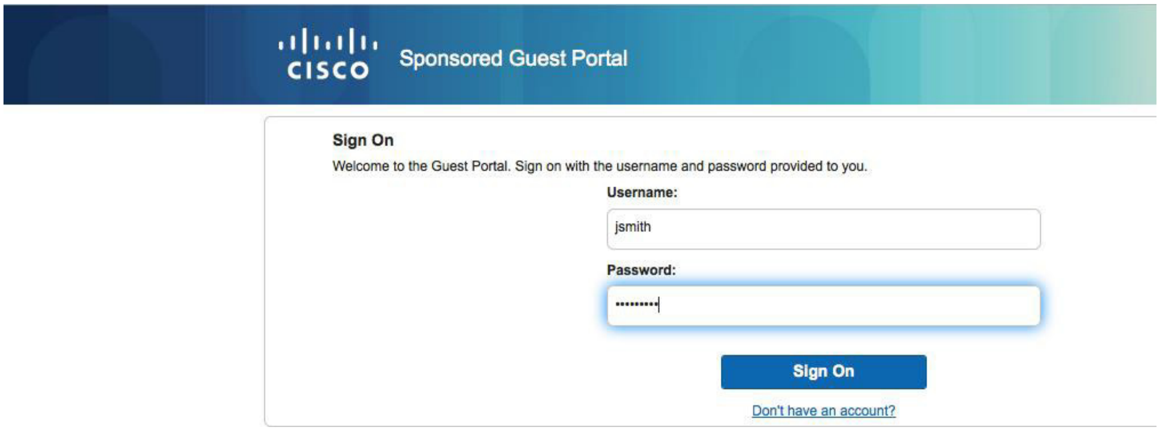
Portal Name: * Self-Registered Guest Portal (default

Description: Guests are allowed to create their own accounts and access the network us

Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.

Portal Page Customization
Customize portal pages by applying a theme and specifying field names and messages displayed to users.

第 5 步　点击**门户测试 (Portal test)** 并输入身份组用户值



Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username: jsmith

Password: •••••••••

第 6 步 点击**登录 (Sign On)**

第 7 步 系统会显示身份用户和组通知

```
./identity_group_subscribe.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

<u>结果</u>

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:20:22.839 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
11:20:24.468 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Press <enter> to disconnect...user=jsmith
group=Employee
```

EPS_Quarantine/EPS_UnQuarantine

验证

此测试用于验证第三方系统在网络上的终端执行隔离或断开网络连接操作的能力。这也将验证第三方系统按其 MAC 地址取消终端隔离的能力。

定义

pxGrid 客户端注册到已获得授权的 EPS 会话组和订阅 ISE 发布的终端保护服务功能，并隔离已通过身份验证的设备的 IP 地址和按 MAC 地址取消已通过身份验证的设备的隔离。

示例

客户端用户 1 将注册到已获得授权的 EPS 组并订阅 EndpointProtectionService 功能。eps 隔离脚本将通过 IP 地址隔离用户 1。使用 DynAuthListener 模拟授权更改 (CoA) 并执行隔离/取消隔离缓解操作。将运行 eps_quarantine 脚本来隔离终端 IP 地址。将运行 eps_unquarantine 脚本来按 MAC 地址取消终端的隔离。请注意 pxGrid 客户端已订阅终端保护服务功能。

第 1 步 运行 multigroupclient 脚本

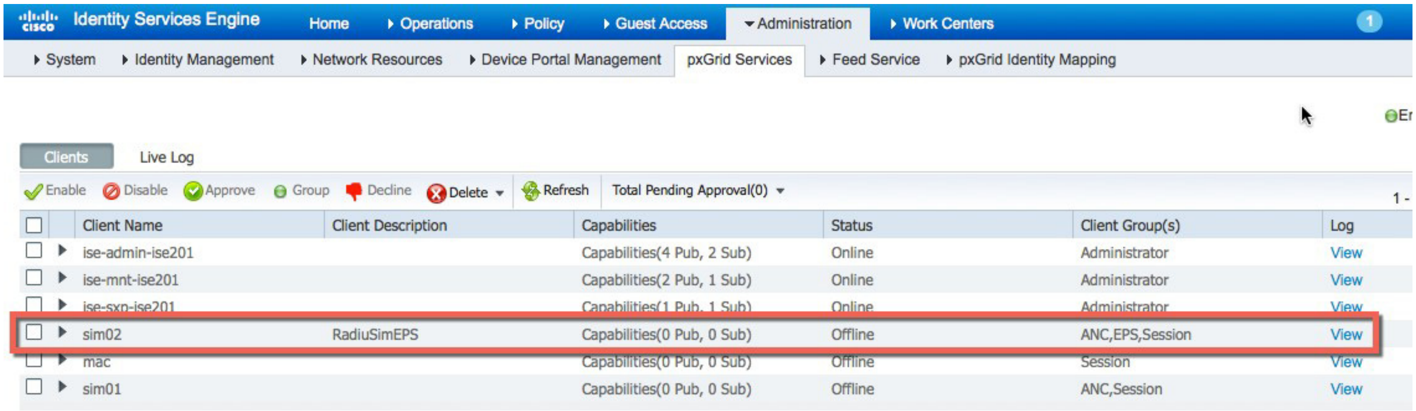
```
./multigroupclient.sh -a 192.168.1.23 -u SIM02 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123 -g EPS
-d RadiuSimEPS Tests
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM02
  group=Session,ANC,EPS
  description=RadiuSimEPS
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
13:54:57.950 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
13:54:59.800 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Connected
Create ANC Policy: ANC1438538097569 Result -
  com.cisco.pxgrid.model.anc.ANCResult@612fc6eb[ ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=<null>
  ancpolicies=<null>
]
Session 1.1.1.2 not found
Connection closed
13:55:00.434 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Stopped
Johns-MacBook-Pro:bin jeppich$
```

第 2 步 选择管理 (Administration)->pxGrid 服务 (pxGrid Services)

pxGrid 客户端会注册到 EPS 客户端组

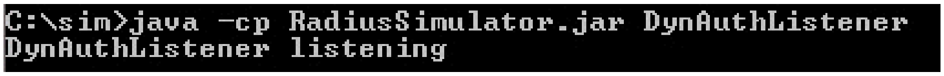


□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise201		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise201		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	ise-sxp-ise201		Capabilities(1 Pub, 1 Sub)	Online	Administrator	View
□	sim02	RadiuSimEPS	Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS,Session	View
□	mac		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	sim01		Capabilities(0 Pub, 0 Sub)	Offline	ANC,Session	View

第 3 步 在 PC 上运行 DynAuthListener

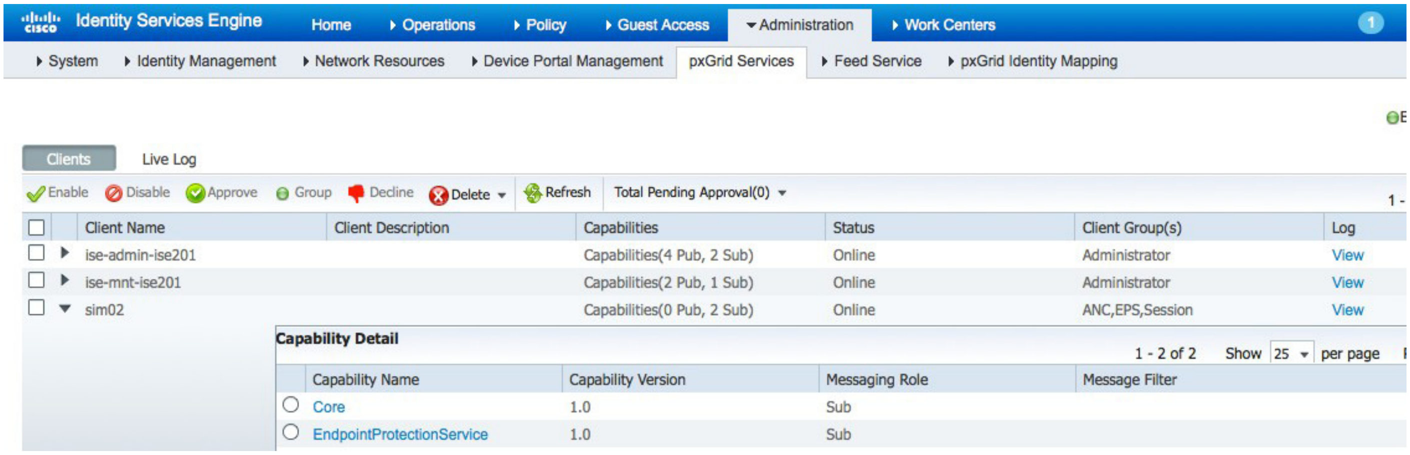
```
java -cp RadiusSimulator.jar DynAuthListener
```

您将看到下图所示内容：



```
C:\sim>java -cp RadiusSimulator.jar DynAuthListener
DynAuthListener listening
```

第 4 步　选择管理 (Administration)->pxGrid 服务 (pxGrid Services)
pxGrid 客户端已订阅终端保护服务功能



□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▶	ise-admin-ise201		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▶	ise-mnt-ise201		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▼	sim02		Capabilities(0 Pub, 2 Sub)	Online	ANC,EPS,Session	View

Capability Detail

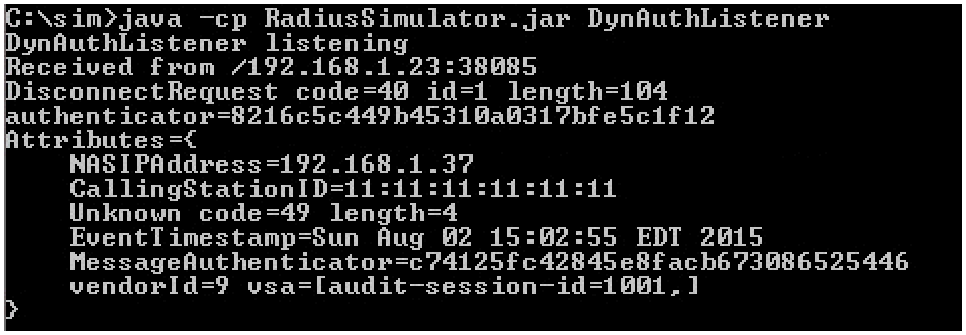
1 - 2 of 2　Show 25 per page

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	EndpointProtectionService	1.0	Sub	

第 5 步　运行 eps_quarantine 脚本

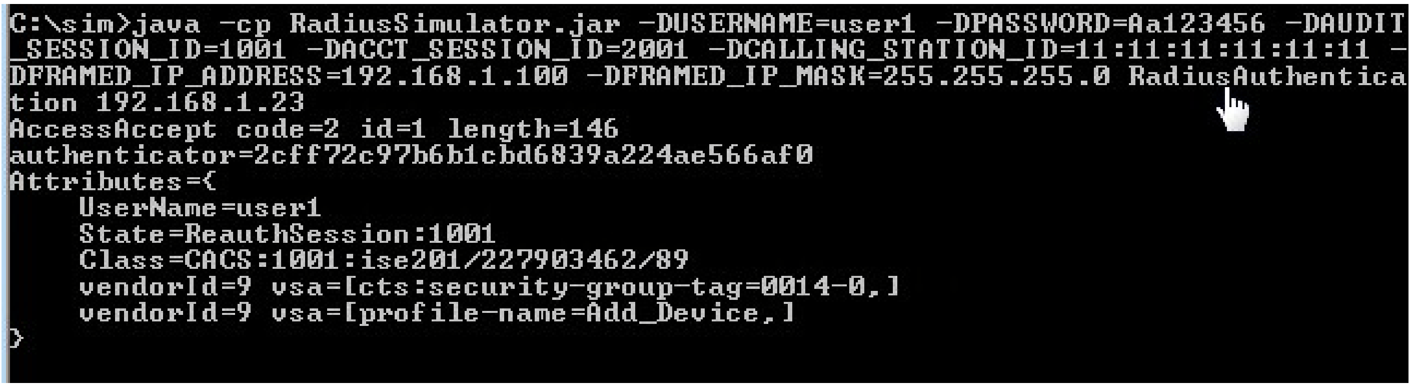
```
./eps_quarantine.sh -a 192.168.1.23 -u SIM02 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM02
  group=EPS
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
14:04:41.263 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
14:04:42.619 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
IP address (or <enter> to disconnect): 192.168.1.100
IP address (or <enter> to disconnect):
```

第 6 步　您将看到 DynAuthListener 收到隔离事件



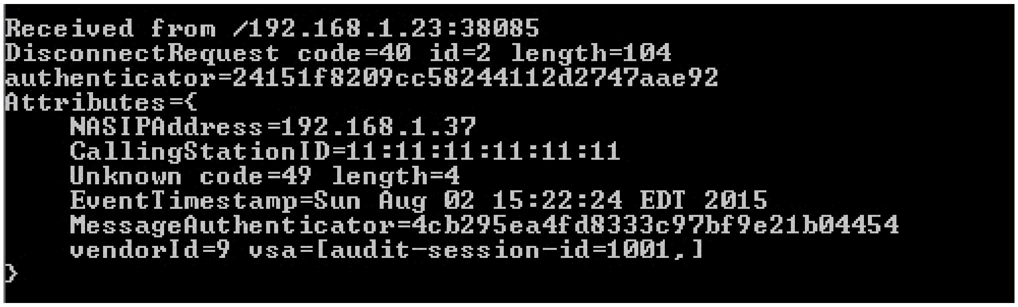
```
C:\sim>java -cp RadiusSimulator.jar DynAuthListener
DynAuthListener listening
Received from /192.168.1.23:38085
DisconnectRequest code=40 id=1 length=104
authenticator=8216c5c449b45310a0317bfe5c1f12
Attributes={
     NASIPAddress=192.168.1.37
     CallingStationID=11:11:11:11:11:11
     Unknown code=49 length=4
     EventTimestamp=Sun Aug 02 15:02:55 EDT 2015
     MessageAuthenticator=c74125fc42845e8facb673086525446
     vendorId=9 vsa=[audit-session-id=1001,]
}
```

第 7 步　在 PC 上打开另一个 cmd 窗口，并运行 RADIUS 模拟程序来对用户 1 进行身份验证



```
C:\sim>java -cp RadiusSimulator.jar -DUSERNAME=user1 -DPASSWORD=Aa123456 -DAUDIT
_SESSION_ID=1001 -DACCT_SESSION_ID=2001 -DCALLING_STATION_ID=11:11:11:11:11:11 -
DFRAMED_IP_ADDRESS=192.168.1.100 -DFRAMED_IP_MASK=255.255.255.0 RadiusAuthentica
tion 192.168.1.23
AccessAccept code=2 id=1 length=146
authenticator=2cff72c97b6b1cbd6839a224ae566af0
Attributes={
    UserName=user1
    State=ReauthSession:1001
    Class=CACS:1001:ise201/227903462/89
    vendorId=9 vsa=[cts:security-group-tag=0014-0,]
    vendorId=9 vsa=[profile-name=Add_Device,]
}
```

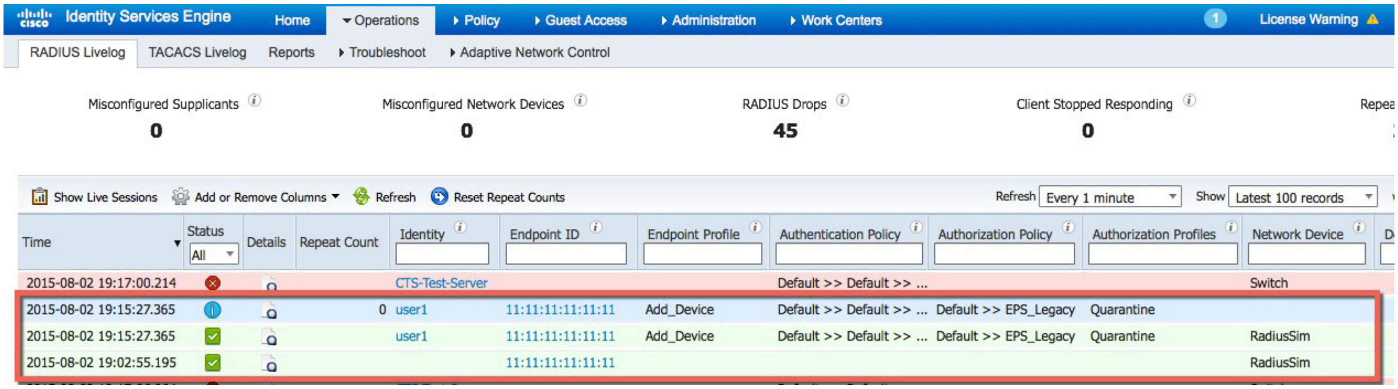
第 8 步　　您将看到 DynAuthListener 收到隔离事件



```
Received from /192.168.1.23:38085
DisconnectRequest code=40 id=2 length=104
authenticator=24151f8209cc58244112d2747aae92
Attributes={
    NASIPAddress=192.168.1.37
    CallingStationID=11:11:11:11:11:11
    Unknown code=49 length=4
    EventTimestamp=Sun Aug 02 15:22:24 EDT 2015
    MessageAuthenticator=4cb295ea4fd8333c97bf9e21b04454
    vendorId=9 vsa=[audit-session-id=1001,]
}
```

第 9 步　　选择**操作 (Operations)->RADIUS Livelog**

注意用户已被隔离



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repea
0	0	45	0	

Refresh Every 1 minute　Show Latest 100 records

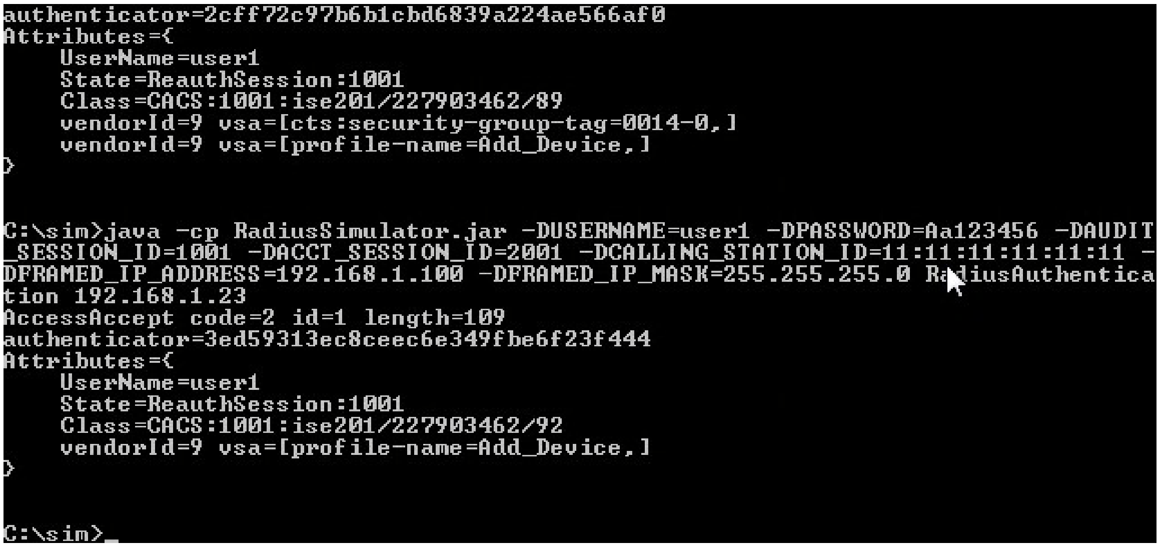
Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	D
2015-08-02 19:17:00.214	☒			CTS-Test-Server			Default >> Default >> ...			Switch	
2015-08-02 19:15:27.365	ⓘ		0	user1	11:11:11:11:11:11	Add_Device	Default >> Default >> ...	Default >> EPS_Legacy	Quarantine		
2015-08-02 19:15:27.365	☑			user1	11:11:11:11:11:11	Add_Device	Default >> Default >> ...	Default >> EPS_Legacy	Quarantine	RadiusSim	
2015-08-02 19:02:55.195	☑				11:11:11:11:11:11					RadiusSim	

第 10 步　　运行 eps_unquarantine 脚本

```
Johns-MacBook-Pro:bin jeppich$ ./eps_unquarantine.sh -a 192.168.1.23 -u SIM02 -k alpha.jks -p cisco123 -t
alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=SIM02
  group=EPS
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
14:24:07.282 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
```

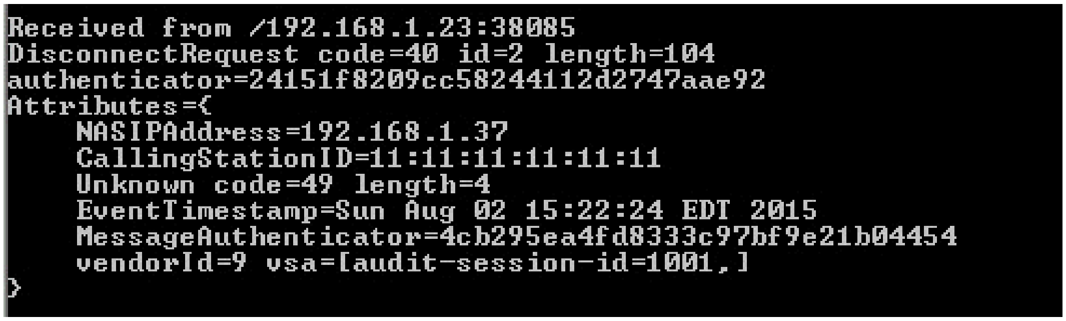
```
Connecting...
Connected
14:24:10.852 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
MAC address (or <enter> to disconnect): 11:11:11:11:11:11
MAC address (or <enter> to disconnect):
```

第 11 步　运行 RADIUS 模拟程序以对用户 1 进行身份验证



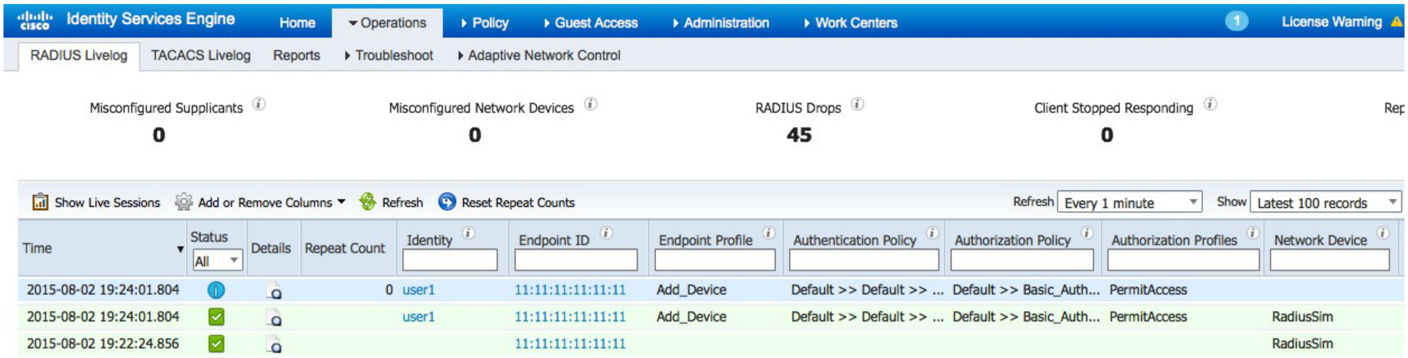
```
authenticator=2cff72c97b6b1cbd6839a224ae566af0
Attributes={
    UserName=user1
    State=ReauthSession:1001
    Class=CACS:1001:ise201/227903462/89
    vendorId=9 vsa=[cts:security-group-tag=0014-0,]
    vendorId=9 vsa=[profile-name=Add_Device,]
}

C:\sim>java -cp RadiusSimulator.jar -DUSERNAME=user1 -DPASSWORD=Aa123456 -DAUDIT
_SESSION_ID=1001 -DACCT_SESSION_ID=2001 -DCALLING_STATION_ID=11:11:11:11:11:11 -
DFRAMED_IP_ADDRESS=192.168.1.100 -DFRAMED_IP_MASK=255.255.255.0 RadiusAuthentica
tion 192.168.1.23
AccessAccept code=2 id=1 length=109
authenticator=3ed59313ec8ceec6e349fbe6f23f444
Attributes={
    UserName=user1
    State=ReauthSession:1001
    Class=CACS:1001:ise201/227903462/92
    vendorId=9 vsa=[profile-name=Add_Device,]
}

C:\sim>_
```

第 12 步　您将看到 DynAuthListener 收到隔离事件



```
Received from /192.168.1.23:38085
DisconnectRequest code=40 id=2 length=104
authenticator=24151f8209cc58244112d2747aae92
Attributes={
    NASIPAddress=192.168.1.37
    CallingStationID=11:11:11:11:11:11
    Unknown code=49 length=4
    EventTimestamp=Sun Aug 02 15:22:24 EDT 2015
    MessageAuthenticator=4cb295ea4fd8333c97bf9e21b04454
    vendorId=9 vsa=[audit-session-id=1001,]
}
```

第 13 步　选择操作 (Operations)->RADIUS Livelog



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Rep
0	0	45	0	

Refresh: Every 1 minute　Show: Latest 100 records

Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device
2015-08-02 19:24:01.804	ⓘ	🔍	0	user1	11:11:11:11:11:11	Add_Device	Default >> Default >> ...	Default >> Basic_Auth...	PermitAccess	
2015-08-02 19:24:01.804	✓	🔍		user1	11:11:11:11:11:11	Add_Device	Default >> Default >> ...	Default >> Basic_Auth...	PermitAccess	RadiusSim
2015-08-02 19:22:24.856	✓	🔍			11:11:11:11:11:11					RadiusSim

使用 802.1X 测试示例脚本

Multigroupclient

验证

此测试用于验证第三方系统是否可以在 pxGrid 上注册到多客户端组（会话、ANC），即是否可通过身份验证和获得授权。

定义

PxGrid 客户端注册连接并将第三方应用、安全设备注册到授权的**会话**或 **ANC** 组，或在此示例中，将 Linux 主机注册到 pxGrid 控制器。其他组（如管理和基础）可用，但是，**管理**组专为 ISE 和**基础**组保留，并需要 pxGrid 管理批准，不会用于任何注册 pxGrid 示例。

所有注册的 pxGrid 客户端都可在“管理” (Administration) 下的 ISE pxGrid 服务视图中查看。

pxGrid 客户端可以是信息的发布服务器或用户，这一点将在“动态主题”中进行说明。ISE 将无法使用信息，注册的客户端之间将共享上下文信息。一旦 pxGrid 客户端成功注册到已获得授权的组，该客户端将可以获得相关会话信息或查询，如 pxGrid 示例脚本所确定的那样。

示例

在此示例中，我们会将 Linux 主机作为一个会话组的 pxGrid 客户端注册到 pxGrid 控制器。Linux 主机 mac 是 pxGrid 客户端的用户名。我们还将在 ISE 中查看注册的 pxGrid 客户端。

第 1 步　运行 multigroupclient 脚本

```
./multigroupclient.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123 -g Session -
d pxGrid Client
```

用法：

```
Usage: ./multigroupclient.sh [options]

  Main options
    -a <PXGRID_HOSTNAMES> (comma separated hostnames)
    -u <PXGRID_USERNAME>
    -g <PXGRID_GROUP>
    -d <PXGRID_DESCRIPTION>

  The followings are certificates options
    -k <PXGRID_KEYSTORE_FILENAME>
    -p <PXGRID_KEYSTORE_PASSWORD>
    -t <PXGRID_TRUSTSTORE_FILENAME>
    -q <PXGRID_TRUSTSTORE_PASSWORD>
  If not specified, it defaults to use clientSample1.jks and rootSample.jks
  Specifying values here can override the defaults

  Custom config file can fill or override parameters
    -c <config_filename>
```

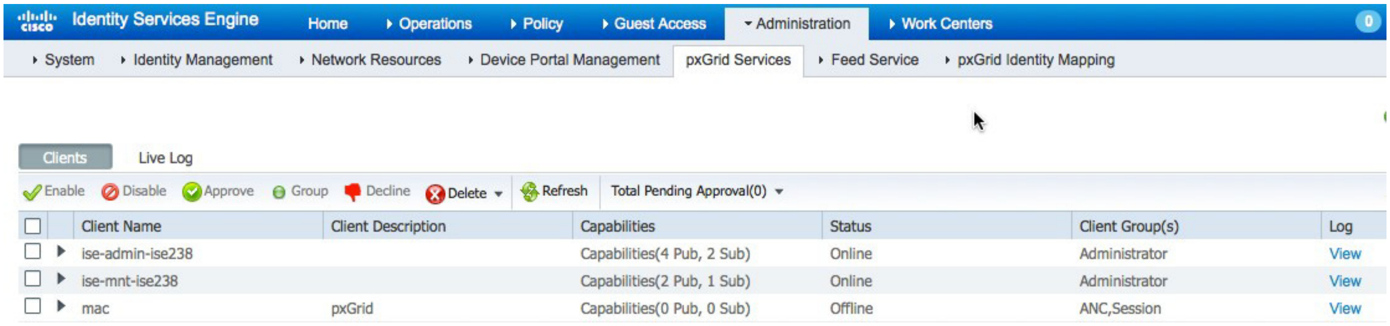
```
Config file are being sourced.Use these variables:
      PXGRID_HOSTNAMES
      PXGRID_USERNAME
      PXGRID_GROUP
      PXGRID_DESCRIPTION
      PXGRID_KEYSTORE_FILENAME
      PXGRID_KEYSTORE_PASSWORD
      PXGRID_TRUSTSTORE_FILENAME
      PXGRID_TRUSTSTORE_PASSWORD
```

结果：

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session,ANC,Session
  description=pxGrid
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
09:35:31.772 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
09:35:35.769 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Create ANC Policy: ANC1437658531354 Result -
  com.cisco.pxgrid.model.anc.ANCResult@612fc6eb[ ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=<null>
  ancpolicies=<null>
]
Session 1.1.1.2 not found
Connection closed
```

第 2 步　选择管理 (Administration)->pxGrid 服务 (pxGrid Services)

将 pxGrid 客户端 mac 注册到会话客户端组。默认情况下会添加 ANC，这是 pxGrid 自适应网络控制 (ANC) 缓解操作所必需的。



□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	mac	pxGrid	Capabilities(0 Pub, 0 Sub)	Offline	ANC,Session	View

会话订阅

验证

此测试用于验证如果可以注册的第三方系统连接到 pxGrid 客户端，该客户端是否可以订阅 pxGrid 上可用的信息主题。在这种情况下，pxGrid 客户端将订阅用户身份验证状态更新

定义

一旦客户端成功注册到 pxGrid 控制器的会话和 ANC 组并获得授权，客户端便会订阅此功能并获取已通过身份验证的用户的相关会话信息。ISE MnT 节点会将 ISE 会话目录作为一个主题发布到 pxGrid 控制器。pxGrid 客户端将订阅此功能，并实时获取已通过身份验证用户的活动会话或通知。

示例

pxGrid 客户端将订阅 SessionDirectory 功能并实时接收通知。

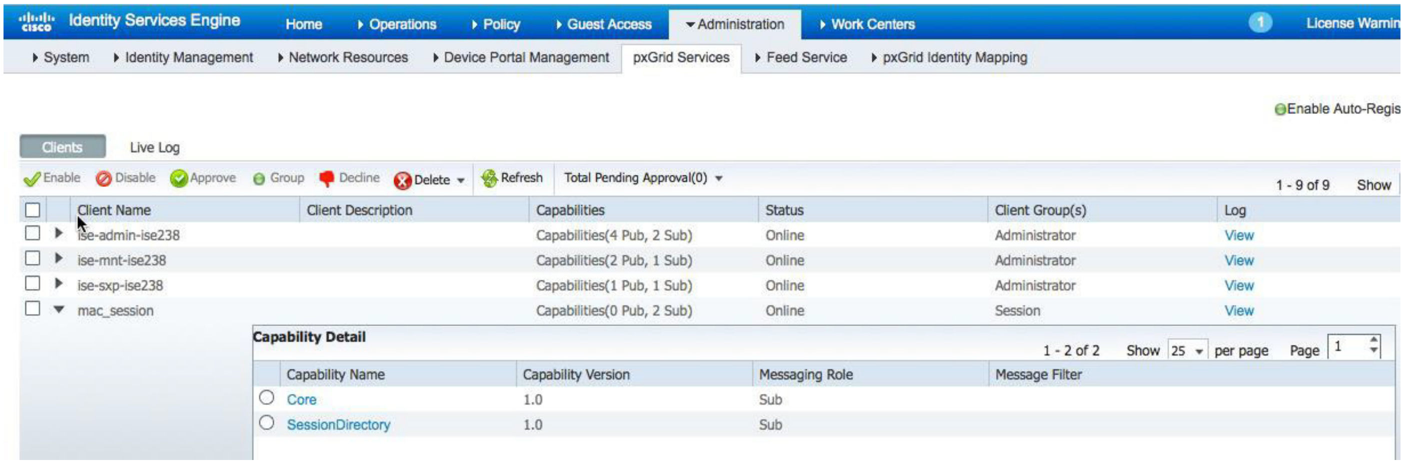
第 1 步　运行 session_subscribe 脚本

```
./session_subscribe.sh -a 10.0.0.37 -u mac_session -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac_session
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
13:00:10.800 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
Filters (ex.'1.0.0.0/255.0.0.0,1234::/16,...' or <enter> for no filter): 13:00:12.205 [Thread-1] INFO
com.cisco.pxgrid.ReconnectionManager - Connected
```

第 2 步　选择**管理 (Administration)->pxGrid 服务 (pxGrid Services)**
pxGrid 客户端已订阅 SessionDirectory 主题



□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	ise-sxp-ise238		Capabilities(1 Pub, 1 Sub)	Online	Administrator	View
□	mac_session		Capabilities(0 Pub, 2 Sub)	Online	Session	View

Capability Detail

1 - 2 of 2 Show 25 per page Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	SessionDirectory	1.0	Sub	

第 3 步 注销并登录到客户端 PC，将实时看到以下通知

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac_session
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
06:58:07.070 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
Filters (ex.'1.0.0.0/255.0.0.0,1234::/16,...' or <enter> for no filter): 06:58:08.835 [Thread-1] INFO
com.cisco.pxgrid.ReconnectionManager - Connected

press <enter> to disconnect...session notification:
Session={ip=[10.0.0.15], Audit Session Id=0A0000020000000F006EE7E0, User Name=host/jeppich-PC.lab6.com, AD
User DNS Domain=null, AD Host DNS Domain=lab6.com, AD User NetBIOS Name=null, AD Host NETBIOS Name=LAB6,
Calling station id=00:0C:29:79:02:A8, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint
Profile=Add_Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/43, RADIUSAVPairs=[ Acct-Session-
Id=00000009], Posture Status=null, Posture Timestamp=, Session Last Update Time=Tue Jul 28 07:57:25 EDT 2015}

session notification:
Session={ip=[10.0.0.15], Audit Session Id=0A0000020000000F006EE7E0, User Name=LAB6\jeppich, AD User DNS
Domain=lab6.com, AD Host DNS Domain=null, AD User NetBIOS Name=LAB6, AD Host NETBIOS Name=null, Calling
station id=00:0C:29:79:02:A8, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint
Profile=Add_Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/43, RADIUSAVPairs=[ Acct-Session-
Id=00000009], Posture Status=null, Posture Timestamp=, Session Last Update Time=Tue Jul 28 07:57:56 EDT 2015}

session notification:
Session={ip=[10.0.0.15], Audit Session Id=0A0000020000000F006EE7E0, User Name=host/jeppich-PC.lab6.com, AD
User DNS Domain=null, AD Host DNS Domain=lab6.com, AD User NetBIOS Name=null, AD Host NETBIOS Name=LAB6,
Calling station id=00:0C:29:79:02:A8, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint
Profile=Add_Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/43, RADIUSAVPairs=[ Acct-Session-
Id=00000009], Posture Status=null, Posture Timestamp=, Session Last Update Time=Tue Jul 28 07:59:17 EDT 2015}
```

会话下载

验证

此测试用于验证第三方系统执行活动用户会话批量会话下载的能力。

定义

会话下载脚本从发布的 ISE 节点下载批量会话记录。

示例

在此示例中，pxGrid 客户端将从 ISE MnT 节点下载活动会话。

第 1 步　运行会话下载脚本

```
./session_download.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
12:30:38.687 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
Filters (ex.'1.0.0.0/255.0.0.0,1234::/16...' or <enter> for no filter): 12:30:40.056 [Thread-1] INFO
com.cisco.pxgrid.ReconnectionManager - Connected

Start time (ex.'2015-01-31 13:00:00' or <enter> for no start time):
End time (ex.'2015-01-31 13:00:00' or <enter> for no end time):
Session={ip=[10.0.0.15], Audit Session Id=0A0000020000000F004BE344, User Name=jeppich, AD User DNS
Domain=lab6.com, AD Host DNS Domain=null, AD User NetBIOS Name=LAB6, AD Host NETBIOS Name=null, Calling
station id=00:0C:29:79:02:A8, Session state=AUTHENTICATED, ANCstatus=null, Security Group=null, Endpoint
Profile=Add_Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/43, RADIUSAVPairs=[ Acct-Session-
Id=00000009], Posture Status=null, Posture Timestamp=, Session Last Update Time=Thu Jul 23 13:42:25 EDT 2015}
Session={ip=[10.0.0.37], Audit Session Id=0A0000020000000E004156F4, User Name=00:0C:29:87:8D:1F, AD User DNS
Domain=null, AD Host DNS Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station
id=00:0C:29:87:8D:1F, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=VMWare-
Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/37, RADIUSAVPairs=[ Acct-Session-Id=00000005], Posture
Status=null, Posture Timestamp=, Session Last Update Time=Thu Jul 23 09:41:25 EDT 2015}
Session={ip=[10.0.0.3], Audit Session Id=0A0000020000000D00036A42, User Name=18:E7:28:2E:29:CB, AD User DNS
Domain=null, AD Host DNS Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station
id=18:E7:28:2E:29:CB, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Cisco-
Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/37, RADIUSAVPairs=[ Acct-Session-Id=00000007], Posture
Status=null, Posture Timestamp=, Session Last Update Time=Thu Jul 23 09:43:42 EDT 2015}
Session={ip=[10.0.0.15], Audit Session Id=0A0000020000000F004BE344, User Name=18:E7:28:2E:29:CC, AD User DNS
Domain=null, AD Host DNS Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station
id=18:E7:28:2E:29:CC, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Cisco-
Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/43, RADIUSAVPairs=[ Acct-Session-Id=0000000A], Posture
Status=null, Posture Timestamp=, Session Last Update Time=Thu Jul 23 13:42:25 EDT 2015}
Session={ip=[10.0.0.33], Audit Session Id=0A0000020000000C0003610A, User Name=68:05:CA:12:7C:78, AD User DNS
Domain=null, AD Host DNS Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station
id=68:05:CA:12:7C:78, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Unknown,
NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/23, RADIUSAVPairs=[ Acct-Session-Id=00000006], Posture
Status=null, Posture Timestamp=, Session Last Update Time=Thu Jul 23 09:43:42 EDT 2015}
Session count=5
Connection closed
```

按 IP 进行的会话查询

验证

此测试用于验证第三方系统通过 pxGrid 执行有关特定 IP 地址的定向查询的能力。

定义

按 IP 脚本进行的会话查询会按 IP 地址获取已通过身份验证的用户的会话信息。

示例

我们通过输入最终用户的 IP 地址获取最终用户会话信息。

第 1 步　运行 session_query_by_ip 脚本

```
./session_query_by_ip.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
12:50:33.356 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
12:50:34.961 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
IP address (or <enter> to disconnect): 10.0.0.15
Session={ip=[10.0.0.15], Audit Session Id=0A0000020000000F004BE344, User Name=18:E7:28:2E:29:CC, AD User DNS
Domain=null, AD Host DNS Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station
id=18:E7:28:2E:29:CC, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Cisco-
Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/43, RADIUSAVPairs=[ Acct-Session-Id=0000000A], Posture
Status=null, Posture Timestamp=, Session Last Update Time=Thu Jul 23 13:42:25 EDT 2015}
IP address (or <enter> to disconnect
```

EndpointProfile 订阅

验证

此测试用于验证第三方系统订阅发布的终端配置文件主题的能力。

定义

注册的 pxGrid 客户端将订阅 EndpointProfileMetaData 功能，以获取全局分析策略中的更改或修改。会话通知将包含终端配置文件 ID、名称和完全限定的名称。

示例

在此示例中，将根据用户 PC 的静态 MAC 地址创建 pxGrid EndpointProfile 示例策略。当 pxGrid 客户端订阅 EndpointprofileMetadata 功能且 ISE 分析策略有任何修改时，我们将实时在正在运行的 Linux 脚本中看到会话通知。

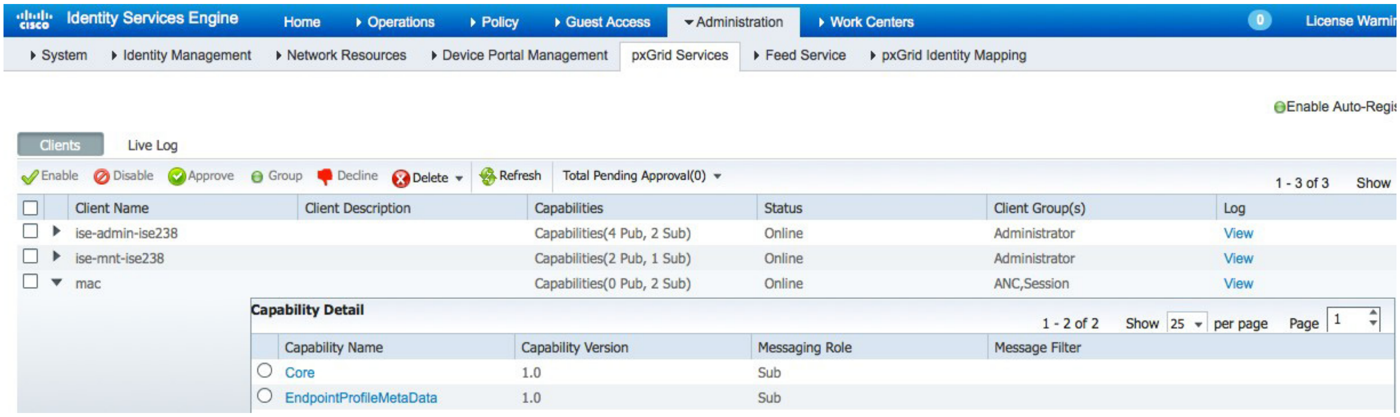
第 1 步　运行 endpointprofile_subscribe 脚本

```
./endpointprofile_subscribe.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
10:14:02.627 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
10:14:04.268 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Press <enter> to disconnect...
```

第 2 步　选择**管理 (Administration)->pxGrid 服务 (pxGrid Services)**



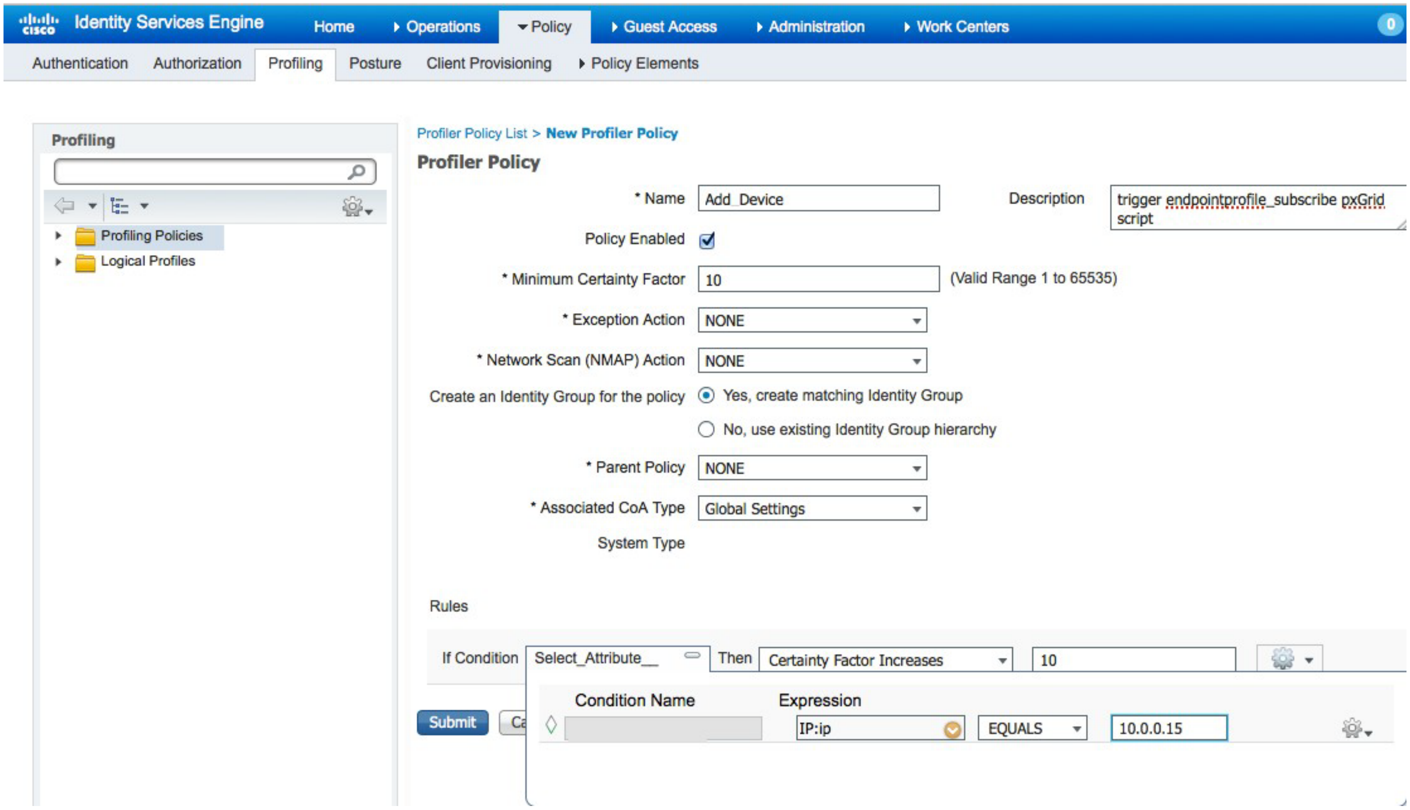
Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
mac		Capabilities(0 Pub, 2 Sub)	Online	ANC,Session	View

Capability Detail

1 - 2 of 2　Show 25 per page　Page 1

Capability Name	Capability Version	Messaging Role	Message Filter
Core	1.0	Sub	
EndpointProfileMetaData	1.0	Sub	

第 3 步　选择**策略 (Policy)->分析 (Profiling)->添加 (Add)**
提供策略名称和说明
在**如果条件 (If Condition)->创建新条件 (Create New Condition)->IP->**{提供访问网络的设备的 IP 地址} 下，选择**提交 (Submit)**



Profiler Policy

* Name: Add_Device

Description: trigger endpointprofile_subscribe pxGrid script

Policy Enabled: ☑

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: ● Yes, create matching Identity Group ○ No, use existing Identity Group hierarchy

* Parent Policy: NONE

* Associated CoA Type: Global Settings

System Type

Rules

If Condition: Select_Attribute_　Then: Certainty Factor Increases　10

Condition Name	Expression		
	IP:ip	EQUALS	10.0.0.15

第 4 步　您将收到一条终端配置文件订阅通知，说明您创建的分析策略已添加

```
./endpointprofile_subscribe.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
10:14:02.627 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
10:14:04.268 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Connected
Press <enter> to disconnect...EndpointProfileChangedNotification (changetype=ADD) Device profile :
id=a5469840-3150-11e5-9b58-000c29878d1f, name=Add_Device, fqname=Add_Device
```

身份组下载

验证

此测试用于验证第三方系统执行用户身份信息批量下载的能力。

定义

身份组下载脚本会从会话目录下载用户组信息和用户组映射的批量会话记录。这些组包括 ISE 身份组和已分析的组。

示例

在此示例中，我们使用身份组下载脚本从 ISE MnT 节点发布服务器下载所有组信息。

第 1 步　运行 identity_group_download 脚本

```
./identity_group_download.sh -a 192.168.1.23 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
20:36:26.820 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
20:36:28.397 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
user=host/jeppich-PC.lab6.com groups=Workstation
user=LAB6\jeppich groups=Workstation
user=user1 groups=User Identity Groups:Employee,Add_Device
user=user2 groups=User Identity Groups:Employee,Unknown
user=user3 groups=User Identity Groups:Employee
user=00:0C:29:79:02:A8 groups=Workstation
User count=6
Connection closed
20:36:30.882 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Stopped
```

```
Johns-MacBook-Pro:bin jeppich$
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
20:36:26.820 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
20:36:28.397 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
user=host/jeppich-PC.lab6.com groups=Workstation
user=LAB6\jeppich groups=Workstation
user=user1 groups=User Identity Groups:Employee,Add_Device
user=user2 groups=User Identity Groups:Employee,Unknown
user=user3 groups=User Identity Groups:Employee
user=00:0C:29:79:02:A8 groups=Workstation
User count=6
Connection closed
20:36:30.882 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Stopped
Johns-MacBook-Pro:bin jeppich$
```

安全组查询

验证

此测试用于验证第三方系统检索 ISE 中所有安全组标记的能力。

定义

安全组查询脚本通过 TrustSecMetadata 功能主题公开 ISE 中配置的安全组标记 (SGT)。它提供一个查询方法，来根据唯一 ID、安全组标记值和说明检索 ISE 中配置的所有 SGT。

示例

在此示例中，安全组查询脚本将下载所有安全组标记上下文信息。此脚本会从 ISE 检索所有 TrustSec 安全组会话信息。这包括 TrustSec 标记名称、唯一标识符、说明和值。

对安全组标记的查询定向。

第 1 步　运行 securitygroup_query 脚本

```
./securitygroup_query.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:53:11.474 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
11:53:12.897 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
SecurityGroup : id=65fddc70-2a34-11e5-82cb-005056bf2f0a, name=Unknown, desc=Unknown Security Group, tag=0
SecurityGroup : id=660aadb0-2a34-11e5-82cb-005056bf2f0a, name=ANY, desc=Any Security Group, tag=65535
SecurityGroup : id=669e6230-2a34-11e5-82cb-005056bf2f0a, name=SGT_Auditor, desc=Auditor Security Group, tag=9
SecurityGroup : id=66bdd110-2a34-11e5-82cb-005056bf2f0a, name=SGT_BYOD, desc=BYOD Security Group, tag=15
SecurityGroup : id=66dd3ff0-2a34-11e5-82cb-005056bf2f0a, name=SGT_Contractor, desc=Contractor Security Group,
tag=5
SecurityGroup : id=66fcd5e0-2a34-11e5-82cb-005056bf2f0a, name=SGT_Developer, desc=Developer Security Group,
tag=8
SecurityGroup : id=671a21e0-2a34-11e5-82cb-005056bf2f0a, name=SGT_DevelopmentServers, desc=Development
Servers Security Group, tag=12
SecurityGroup : id=673c9e00-2a34-11e5-82cb-005056bf2f0a, name=SGT_Employee, desc=Employee Security Group,
tag=4
SecurityGroup : id=6759ea00-2a34-11e5-82cb-005056bf2f0a, name=SGT_Guest, desc=Guest Security Group, tag=6
SecurityGroup : id=6775d670-2a34-11e5-82cb-005056bf2f0a, name=SGT_NetworkServices, desc=Network Services
Security Group, tag=3
SecurityGroup : id=67959370-2a34-11e5-82cb-005056bf2f0a, name=SGT_PCIServers, desc=PCI Servers Security
Group, tag=14
```

```
SecurityGroup : id=67b3a2c0-2a34-11e5-82cb-005056bf2f0a, name=SGT_PointOfSale, desc=PointOfSale Security
Group, tag=10
SecurityGroup : id=67d50d70-2a34-11e5-82cb-005056bf2f0a, name=SGT_ProductionServers, desc=Production Servers
Security Group, tag=11
SecurityGroup : id=67f16f10-2a34-11e5-82cb-005056bf2f0a, name=SGT_ProductionUser, desc=Production User
Security Group, tag=7
SecurityGroup : id=680df7c0-2a34-11e5-82cb-005056bf2f0a, name=SGT_Quarantine, desc=Quarantine Security Group,
tag=255
SecurityGroup : id=682a5960-2a34-11e5-82cb-005056bf2f0a, name=SGT_TestServers, desc=Test Servers Security
Group, tag=13
SecurityGroup : id=68461ec0-2a34-11e5-82cb-005056bf2f0a, name=SGT_TrustSecDevices, desc=TrustSec Devices
Security Group, tag=2
Connection closed
11:53:13:235 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager- Stopped
```

安全组订阅

验证

此测试用于验证第三方系统通过 pxGrid 订阅 SecurityGroup 主题的能力。

定义

安全组订阅脚本通过 TrustsecMetaDataCapability 主题公开 ISE 中配置的安全组标记 (SGT)。如果添加/更新/删除了安全组，脚本会话通知中会显示安全组更改通知。

示例

安全组订阅脚本订阅 ISE TrustSec 策略中的更改。在此示例中，我们将生成并创建包含 jsmith 的安全组标记信息的 .cvs 文件。此信息将用安全标签名称、值、说明来填充。此文件将上传到 ISE。文件上传后，Linux 主机上正在运行的 securitygroup_subscribe 脚本中将显示 SecurityGroupChange 通知会话通知。在 pxGrid 客户端订阅了 TrustsecMetaDataCapability 时会发生这种情况。

第 1 步　运行 securitygroup_subscribe 脚本

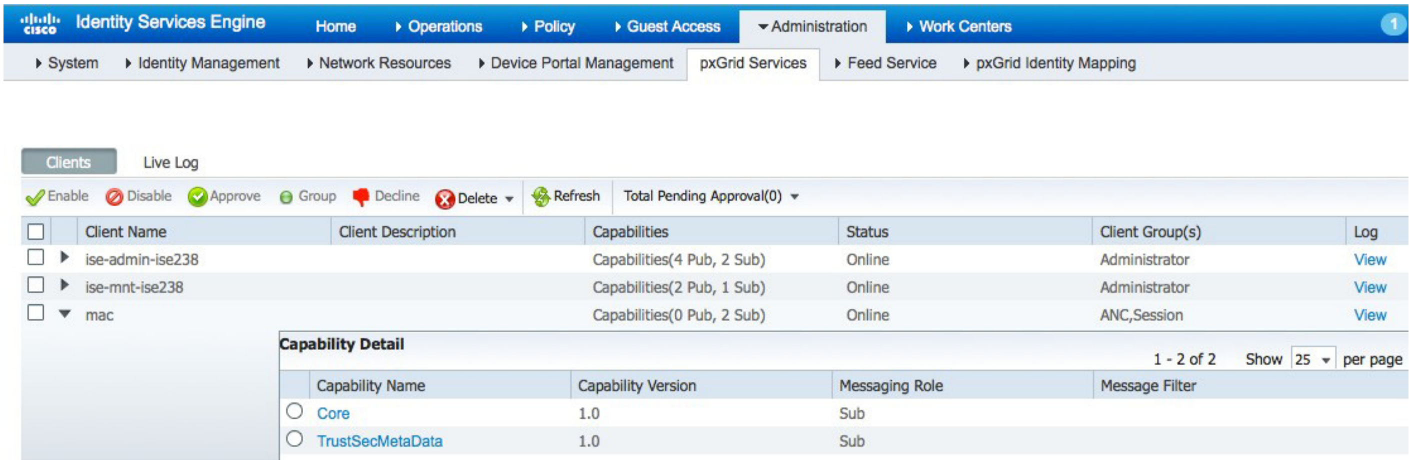
```
./securitygroup_subscribe.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
12:12:22.902 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
```

```
Connected
```

第 2 步　选择“管理”(Administration)-> “pxGrid 服务”(pxGrid services)
pxGrid 客户端已订阅 TrustSecMetadata 功能



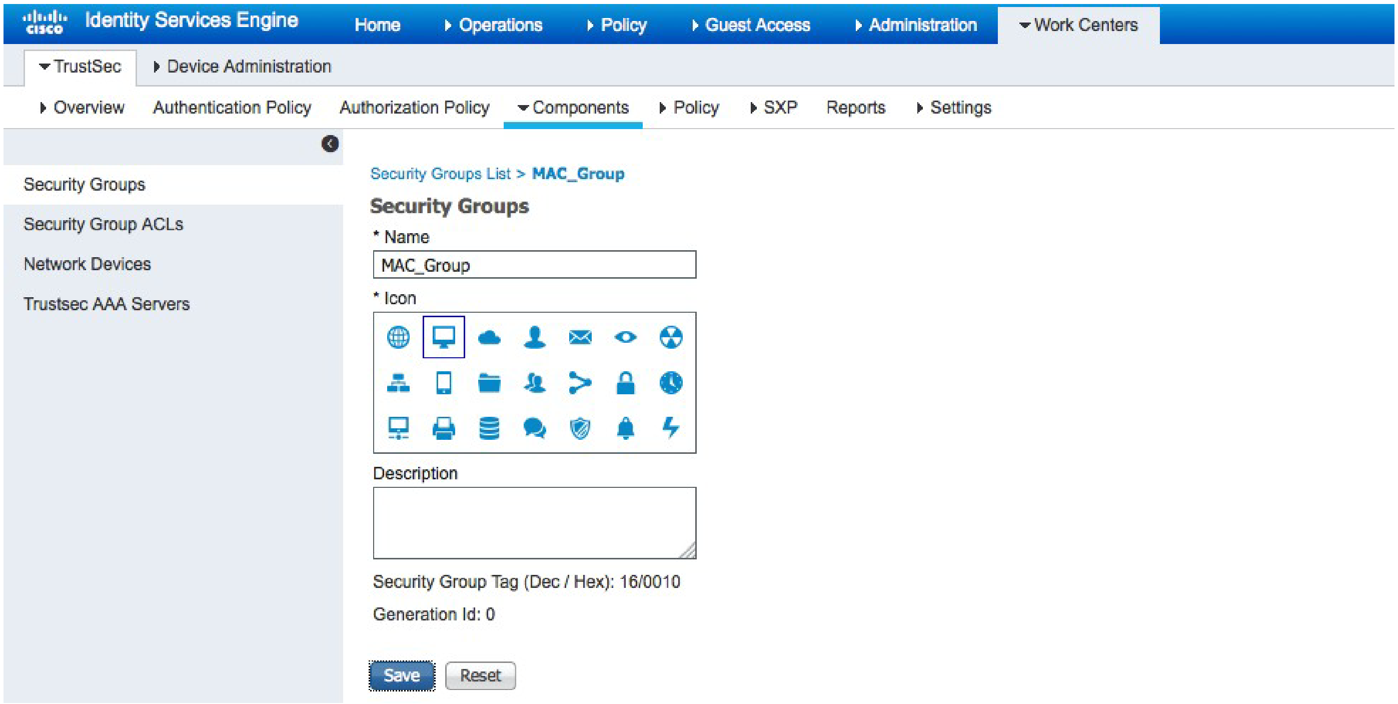
□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▶	ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▶	ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▼	mac		Capabilities(0 Pub, 2 Sub)	Online	ANC,Session	View

Capability Detail

1 - 2 of 2　Show 25 per page

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	TrustSecMetaData	1.0	Sub	

第 3 步　选择“工作中心”(Work Centers)->TrustSec-> “组件”(Components)-> “安全组列表”(Security Group List)->添加 MAC_Group



Security Groups

* Name: MAC_Group

* Icon

Description

Security Group Tag (Dec / Hex): 16/0010

Generation Id: 0

第 4 步　安全组更改通知反映如下

```
./securitygroup_subscribe.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
12:12:22.902 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
12:12:24.320 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Press <enter> to disconnect...SecurityGroupChangeNotification (changetype=MODIFY) SecurityGroup :
id=af3c6ac0-315d-11e5-9b58-000c29878d1f, name=MAC_Group, desc=, tag=16
```

终端配置文件查询

验证

此测试用于验证第三方系统检索 ISE 中配置的所有已启用配置文件的能力。

定义

endpointprofile_query 脚本提供一个查询方法，来检索 ISE 中配置的所有已启用的终端配置文件，并提供终端配置文件 ID、名称和完全限定的名称。如果 ISE 中添加/更新/删除了终端配置文件，用户还将收到通知。

示例

在此示例中，endpointprofile 脚本检索 ISE 中所有已启用的配置文件。

第 1 步　运行 endpointprofile_query 脚本

```
./endpointprofile_query.sh -a 192.168.1.23 -u pxGrid02 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=pxGrid02
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
17:57:04.103 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
```

```
17:57:05.681 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Endpoint Profile : id=8c8f42b0-393f-11e5-ac86-000c297fb12a, name=Add_Device, fqname Add_Device
Endpoint Profile : id=4d852be0-2a33-11e5-82cb-005056bf2f0a, name=Android, fqname Android
Endpoint Profile : id=4dc7b320-2a33-11e5-82cb-005056bf2f0a, name=Apple-Device, fqname Apple-Device Endpoint
Profile : id=4e190770-2a33-11e5-82cb-005056bf2f0a, name=Apple-iDevice, fqname Apple-Device:Apple-
iDevice
Endpoint Profile : id=4e452080-2a33-11e5-82cb-005056bf2f0a, name=Apple-iPad, fqname Apple-Device:Apple-iPad
```

功能

验证

此测试用于验证第三方系统检索 ISE 中所有已发布功能的能力。

定义

功能脚本检索 ISE 中所有已发布的兴趣主题。

示例

功能脚本检索客户端可以发布或订阅的信息主题或功能。

第 1 步　运行 capability_query 脚本

```
./capability_query.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=null
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
09:57:07.306 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
09:57:09.199 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Connected
capability=SessionDirectory, version=1.0
capability=GridControllerAdminService, version=1.0
capability=EndpointProtectionService, version=1.0
capability=IdentityGroup, version=1.0
capability=EndpointProfileMetaData, version=1.0
capability=TrustSecMetaData, version=1.0
capability=AdaptiveNetworkControl, version=1.0
capability=Core, version=1.0
Connection closed
09:57:09.254 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Stopped
```

身份组查询

验证

此测试用于验证第三方系统从指定用户检索 ISE 身份组信息的能力。

定义

身份组查询脚本检索 ISE 身份组信息。

示例

从最终用户检索的最终用户身份组信息。

第 1 步　运行 identity_group_query 脚本

```
./identity_group_query.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
10:58:54.937 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
10:58:56.869 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
user name (or <enter> to disconnect): jeppich
group=Profiled
```

身份组订阅

验证

此测试用于验证第三方系统订阅 ISE 发布的身份主题及接收通知的能力。

定义

订阅身份组主题允许 pxGrid 客户端接收关于 802.1X 事件的通知。

示例

在 ISE 中创建内部网络用户，并用于测试访客门户，这将触发事件。

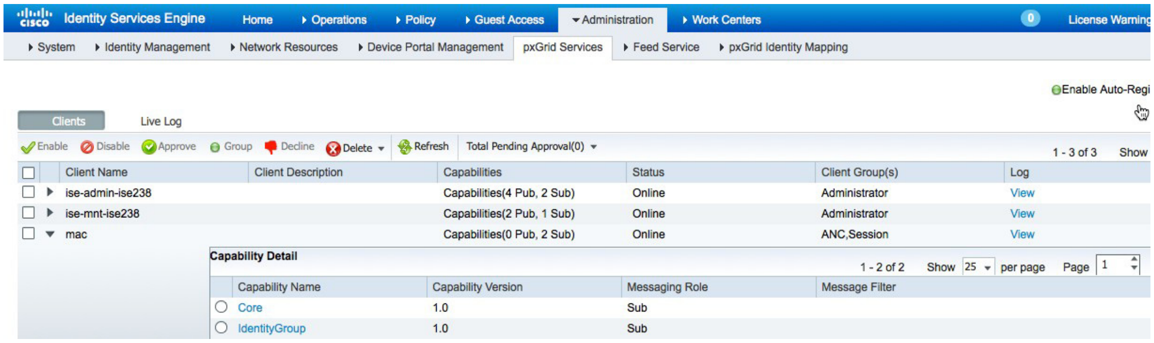
第 1 步　运行 identity_group_subscribe 脚本

```
/identity_group_subscribe.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:20:22.839 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
11:20:24.468 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Press <enter> to disconnect...
```

第 2 步　选择**管理 (Administration)->pxGrid 服务 (pxGrid Services)** 查看订阅的身份组会话



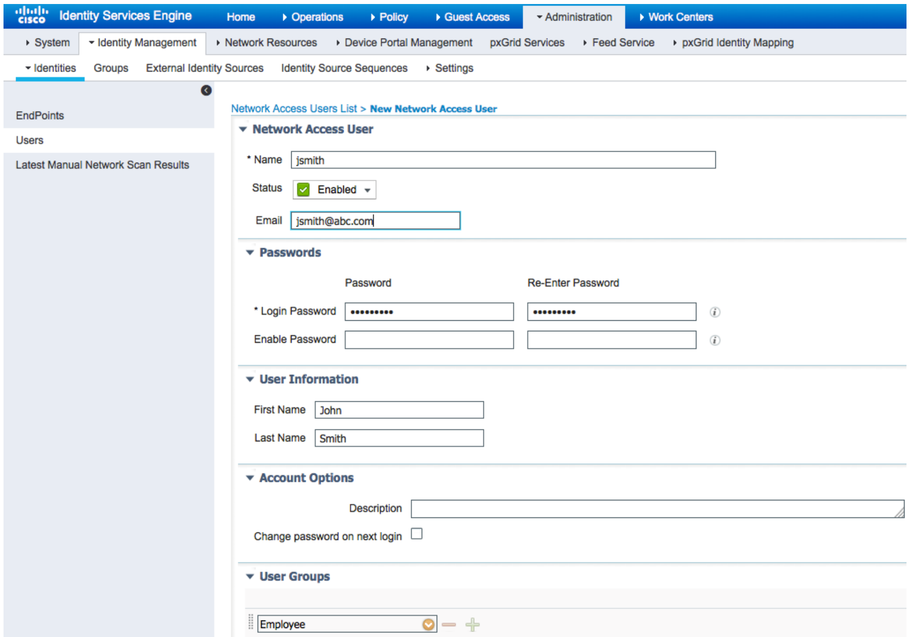
□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▸ ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▸ ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▾ mac		Capabilities(0 Pub, 2 Sub)	Online	ANC,Session	View

Capability Detail

1 - 2 of 2　Show 25 per page　Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	IdentityGroup	1.0	Sub	

第 3 步　创建用于访客门户的 ISE 身份用户，以触发员工



Network Access Users List > **New Network Access User**

Network Access User

* Name: jsmith

Status: ☑ Enabled

Email: jsmith@abc.com

Passwords

	Password	Re-Enter Password
* Login Password	•••••••••	•••••••••
Enable Password		

User Information

First Name: John

Last Name: Smith

Account Options

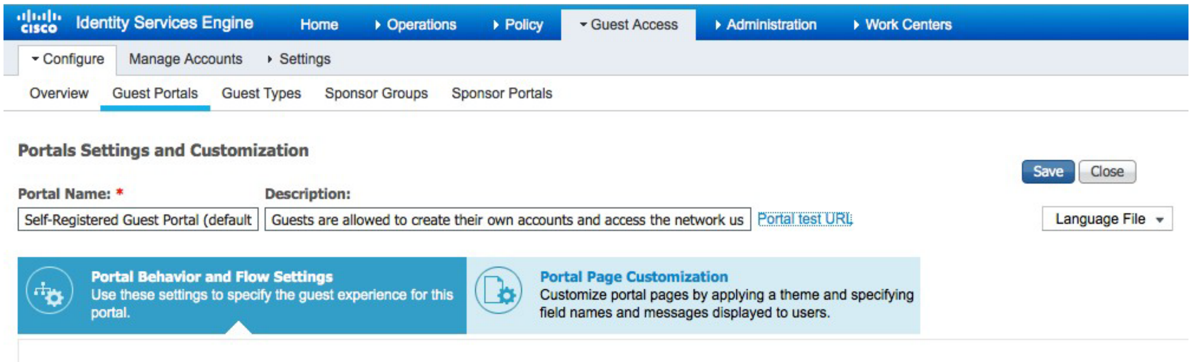
Description:

Change password on next login □

User Groups

Employee

第 4 步　使用默认自助服务门户测试来实时验证用户和关联的身份组，选择**访客接入 (Guest Access)->配置 (Configure)->访客门户 (Guest Portals)->门户测试 URL (Portal test URL)**



Portals Settings and Customization

Portal Name: * Self-Registered Guest Portal (default

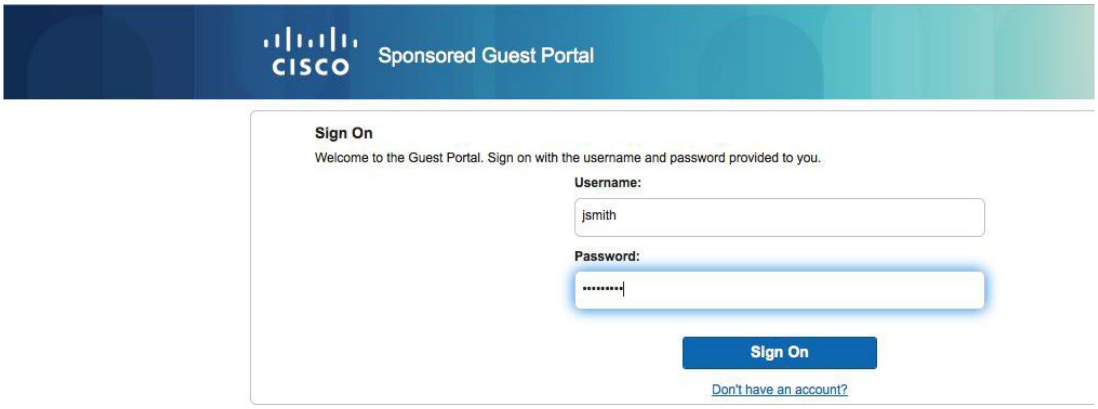
Description: Guests are allowed to create their own accounts and access the network us

Portal test URL

Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.

Portal Page Customization
Customize portal pages by applying a theme and specifying field names and messages displayed to users.

第 5 步　点击**门户测试 (Portal test)** 并输入身份组用户值



Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username: jsmith

Password: •••••••••

第 6 步　点击**登录 (Sign On)**

第 7 步　系统会显示身份用户和组通知

```
./identity_group_subscribe.sh -a 10.0.0.37 -u mac -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
```

结果

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:20:22.839 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
11:20:24.468 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Press <enter> to disconnect...user=jsmith
group=Employee
```

自适应网络控制 (ANC) 策略

自适应网络控制策略 (ANC) pxGrid 缓解策略提供第三方应用或思科安全解决方案，通过自定义操作（隔离、补救、调配、port_bounce、port_shutdown）以更具自定义性、更精细的方式执行企业安全策略。要取消终端的隔离，需发出清除命令。ANC 策略以及相关的授权条件规则 Session:ANCpolicy 在 ISE 上进行配置。您还能够通过 MAC 或 IP 地址手动在终端上执行缓解操作。

在 ISE 2.0 中，不再有 ISE 1.3 中的端点保护服务，也不再有需要在 ISE 中启用以使 ANC 缓解可操作的自适应网络控制 (ANC) 服务。此功能已默认启用。

ANCAction_query 脚本将与已通过身份验证的 802.1X 最终用户配合运行，因此读者可以自如地进行 ANC 缓解脚本调用：

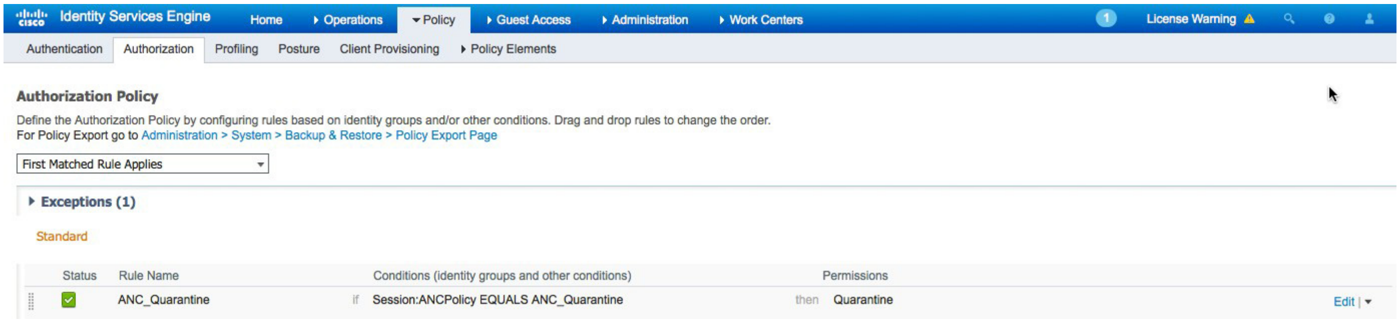
- 隔离已通过身份验证的 802.1X 终端
- 取消终端隔离（清除）
- 根据触发的 ANC 策略提供终端列表
- 订阅 ANC 功能以接收补救和调配通知

ANC 授权策略

ANC 授权策略是 ANC 策略条件规则所引发的网络操作。

第 1 步　创建 ANC 授权

第 2 步　选择**策略 (Policy)->授权 (Authorization)->在上方插入新规则，点击三角形添加**
规则名称：**ANC_Quarantine:**
创建新条件：**Session:ANCpolicy:ANC_Quarantine**
安全组：**Quarantine**



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

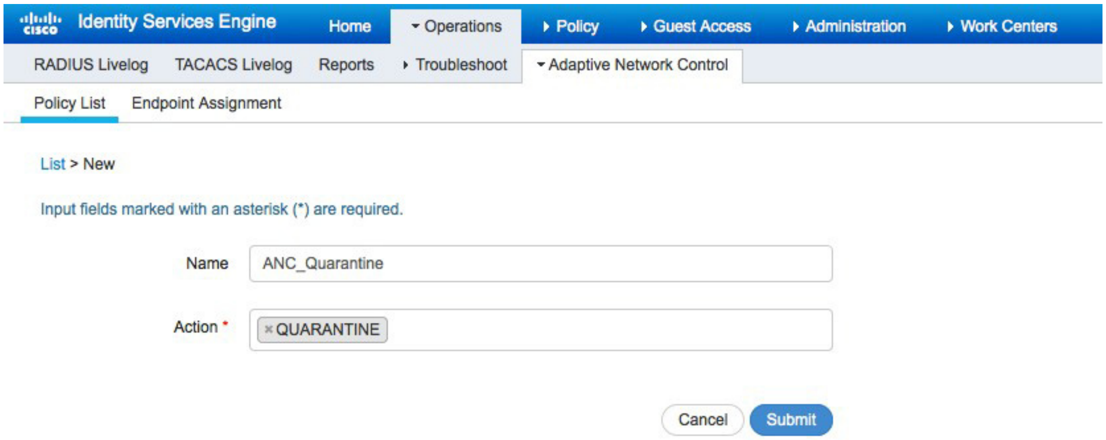
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	ANC_Quarantine	if	Session:ANCPolicy EQUALS ANC_Quarantine	then	Quarantine

第 3 步　点击**完成 (Done)->保存 (Save)**

ANC 策略：隔离

ANC 策略定义要执行的 ANC pxGrid 隔离缓解操作。

第 1 步　选择**操作 (Operations)->自适应网络控制 (Adaptive Network Control)->策略列表 (Policy List)->名称 (Name)->ANC_Ouarantine**

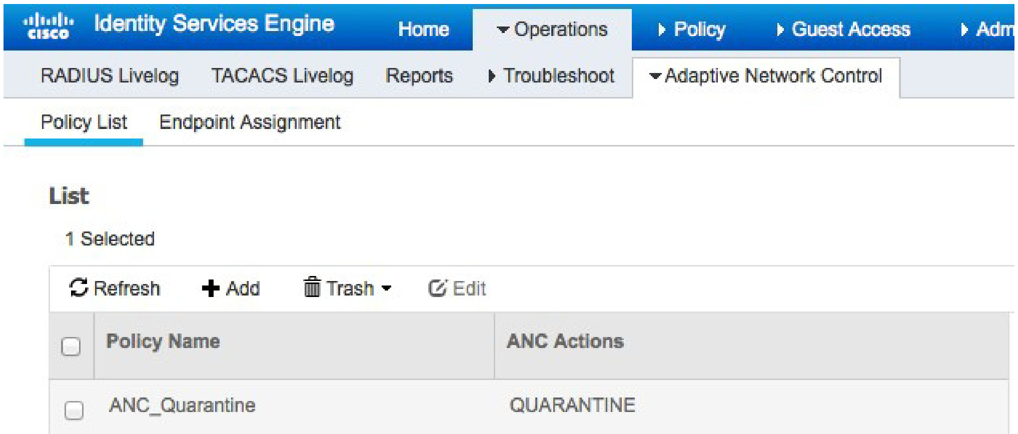


Input fields marked with an asterisk (*) are required.

Name: ANC_Quarantine

Action *: × QUARANTINE

第 2 步　选择**提交 (Submit)**
您将看到下图所示内容



List

1 Selected

□	Policy Name	ANC Actions
□	ANC_Quarantine	QUARANTINE

查看/获取/应用策略到终端的 pxGrid ANC 隔离脚本

在此示例中，将运行 ANC 查询脚本并获取 ANC_Quarantine 策略，并将此策略应用到终端。

第 1 步　运行 ANCAction_query 脚本

```
./ANCAction_query.sh -a 192.168.1.23 -u pxGridClient -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=pxGridClient
  group=ANC
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
------------------------
21:27:57.849 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
21:28:00.252 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect):
```

第 2 步　　选择 10 并输入策略名称

```
Enter number (or <enter> to disconnect): 10
Policy name (or <enter> to disconnect): ANC_Quarantine
ANCResult=com.cisco.pxgrid.model.anc.ANCResult@11758f2a[
  ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=<null>
  ancpolicies=[com.cisco.pxgrid.model.anc.ANCPolicy@74ad1f1f[
   name=ANC_Quarantine
  actions=[QUARANTINE]
]]
]
```

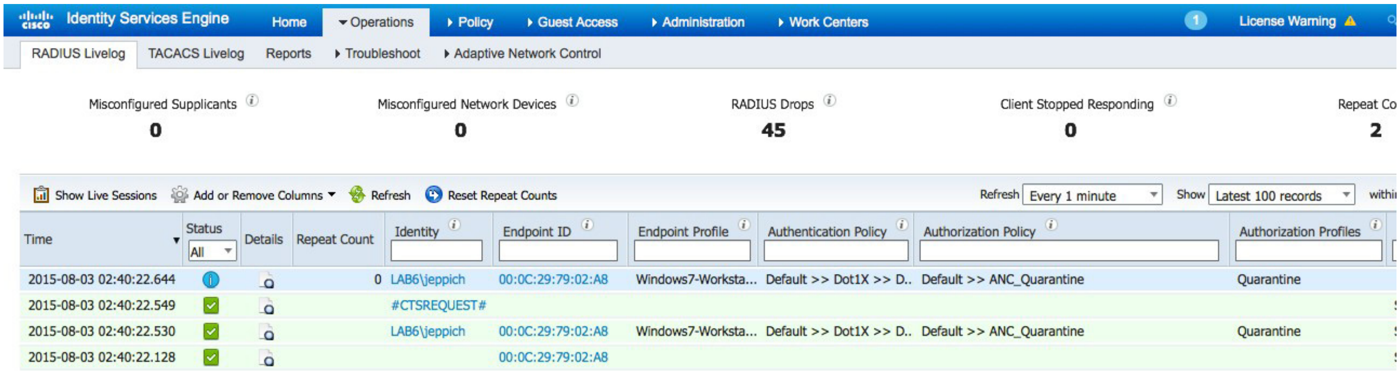
第 3 步　　选择 14 并输入策略名称

```
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect): 14
Policy name (or <enter> to disconnect): ANC_Quarantine
ANCResult=com.cisco.pxgrid.model.anc.ANCResult@66d1af89[
  ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=[com.cisco.pxgrid.model.anc.ANCEndpoint@8646db9[
   policyName=ANC_Quarantine
  macAddress=00:0C:29:79:02:A8
  ipAddress=<null>
]]
```

第 4 步 选择 3 并输入策略名称

```
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect): 
Policy name (or <enter> to disconnect): ANC Quarantine
IP address (or <enter> to disconnect): 192.168.1.38
ANCResult=com.cisco.pxgrid.model.anc.ANCResult@462d5aee[
  ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=<null>
  ancpolicies=<null>
]
```

第 5 步 选择**操作 (Operations)-> RADIUS Livelog**，注意已通过身份验证的 IP 地址已被隔离



Misconfigured Supplicants 0 | Misconfigured Network Devices 0 | RADIUS Drops 45 | Client Stopped Responding 0 | Repeat Co 2

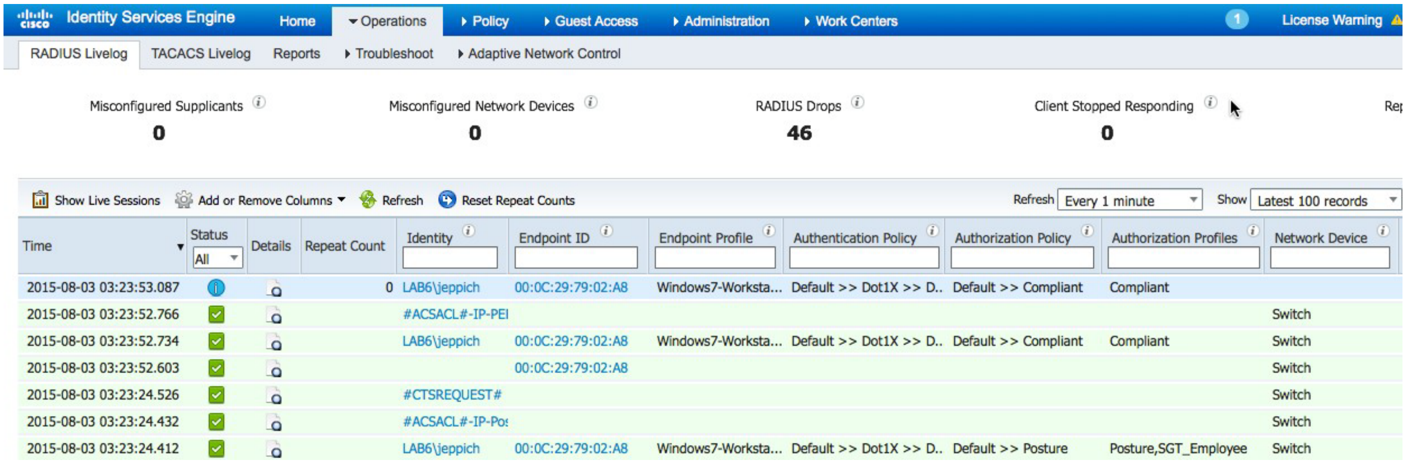
Refresh: Every 1 minute | Show: Latest 100 records | withi

Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2015-08-03 02:40:22.644	ⓘ	🔍	0	LAB6\jeppich	00:0C:29:79:02:A8	Windows7-Worksta...	Default >> Dot1X >> D..	Default >> ANC_Quarantine	Quarantine
2015-08-03 02:40:22.549	✓	🔍		#CTSREQUEST#					
2015-08-03 02:40:22.530	✓	🔍		LAB6\jeppich	00:0C:29:79:02:A8	Windows7-Worksta...	Default >> Dot1X >> D..	Default >> ANC_Quarantine	Quarantine
2015-08-03 02:40:22.128	✓	🔍			00:0C:29:79:02:A8				

第 6 步 要取消隔离（清除），选择 4 并提供 MAC 地址

```
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect): 
MAC address (or <enter> to disconnect): 00:0C:29:79:02:A8
ANCResult=com.cisco.pxgrid.model.anc.ANCResult@11758f2a[
   ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=<null>
  ancpolicies=<null>
```

第 7 步 选择**操作 (Operations)->RADIUS Livelog**
最终用户已取消隔离

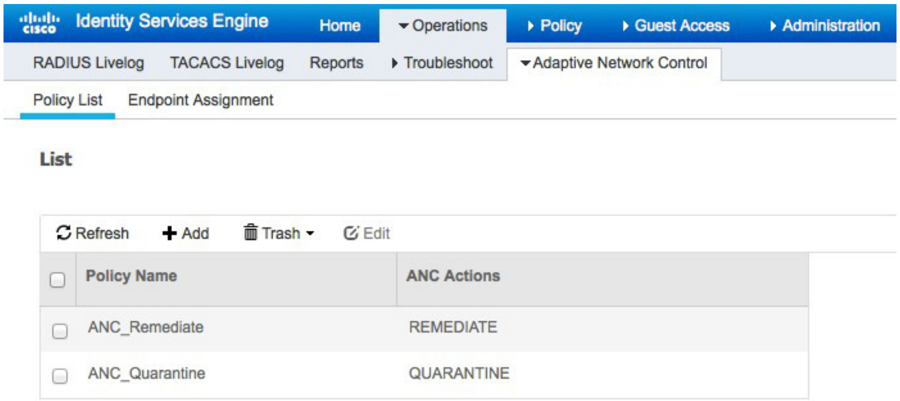


Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device
2015-08-03 03:23:53.087	ⓘ	🔍	0	LAB6\jeppich	00:0C:29:79:02:A8	Windows7-Worksta...	Default >> Dot1X >> D..	Default >> Compliant	Compliant	
2015-08-03 03:23:52.766	☑	🔍		#ACSACL#-IP-PEI						Switch
2015-08-03 03:23:52.734	☑	🔍		LAB6\jeppich	00:0C:29:79:02:A8	Windows7-Worksta...	Default >> Dot1X >> D..	Default >> Compliant	Compliant	Switch
2015-08-03 03:23:52.603	☑	🔍			00:0C:29:79:02:A8					Switch
2015-08-03 03:23:24.526	☑	🔍		#CTSREQUEST#						Switch
2015-08-03 03:23:24.432	☑	🔍		#ACSACL#-IP-Po:						Switch
2015-08-03 03:23:24.412	☑	🔍		LAB6\jeppich	00:0C:29:79:02:A8	Windows7-Worksta...	Default >> Dot1X >> D..	Default >> Posture	Posture,SGT_Employee	Switch

ANC 补救

ANC 补救缓解操作向用户提供补救操作。

第 1 步 选择**操作 (Operations)->自适应网络控制 (Adaptive Network Control) 和 ANC_Remediate，然后选择补救 (REMEDIATE) 操作**



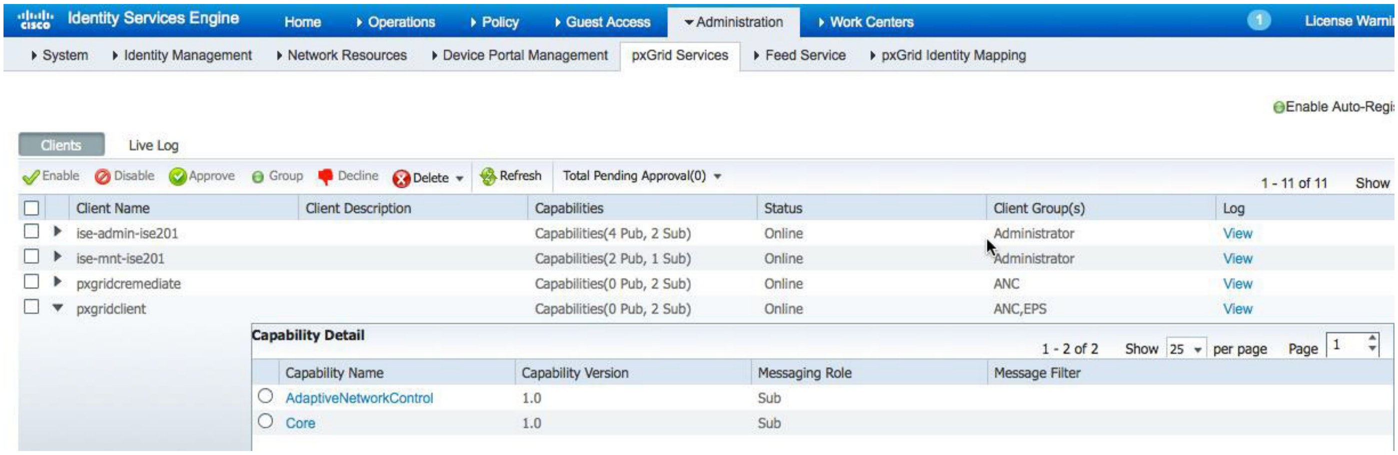
List

☐ Policy Name	ANC Actions
☐ ANC_Remediate	REMEDIATE
☐ ANC_Quarantine	QUARANTINE

第 2 步 运行 ANCQuery 脚本，选择 **6** 进行订阅

```
Johns-MacBook-Pro:bin jeppich$ ./ANCAction_query.sh -a 192.168.1.23 -u pxGridClient -k alpha.jks -p cisco123
-t alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=pxGridClient
  group=ANC
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:42:49.269 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
11:42:52.131 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect):6
Press <enter> to disconnect:
```

第 3 步 选择**管理 (Administration)->pxGrid 服务 (pxGrid Services)**， pxGrid 客户端将连接到 ANC 组



□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▶	ise-admin-ise201		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▶	ise-mnt-ise201		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▶	pxgridcremediate		Capabilities(0 Pub, 2 Sub)	Online	ANC	View
□	▼	pxgridclient		Capabilities(0 Pub, 2 Sub)	Online	ANC,EPS	View

Capability Detail

	Capability Name	Capability Version	Messaging Role	Message Filter
○	AdaptiveNetworkControl	1.0	Sub	
○	Core	1.0	Sub	

第 4 步 打开另一个外壳，然后运行以下脚本

```
./ANCAction_query.sh -a 192.168.1.23 -u pxGridCRemediate -k alpha.jks -p cisco123 -t alpha_root.jks -q
cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=pxGridCRemediate
  group=ANC
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:49:35.734 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
11:49:37.043 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect :
Policy name (or <enter> to disconnect): ANC Remediate
IP address (or <enter> to disconnect): 192.168.1.41
ANCResult=com.cisco.pxgrid.model.anc.ANCResult@11758f2a[
   ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=<null>
  ancpolicies=<null>
]
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
```

© 2015 思科系统公司

```
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect):
```

第 5 步　原始订阅脚本中应该会显示通知

```
./ANCAction_query.sh -a 192.168.1.23 -u pxGridClient -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=pxGridClient
  group=ANC
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:48:17.245 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
11:48:18.563 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect): 6
Press <enter> to disconnect:
Apply Endpoint Policy Notification:
Policy=ANC_Remediate IP Address=192.168.1.41
```

ANC 调配

ANC 调配缓解操作向用户提供补救操作。

第 1 步　运行 ANCAction 查询脚本，然后选择 **6** 进行订阅

```
Johns-MacBook-Pro:bin jeppich$ ./ANCAction_query.sh -a 192.168.1.23 -u pxGridClient -k alpha.jks -p cisco123
-t alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=pxGridClient
  group=ANC
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:42:49.269 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
11:42:52.131 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect):6
Press <enter> to disconnect:
```

第 2 步　要清除或取消隔离，将 ANC 调配策略应用到终端

```
12:03:43.784 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect): 4
IP address (or <enter> to disconnect): 192.168.1.41
ANCResult=com.cisco.pxgrid.model.anc.ANCResult@11758f2a[
  ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=<null>
  ancpolicies=<null>
]
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect  :
Policy name (or <enter> to disconnect):  ANC Provisioning
IP address (or <enter> to disconnect):  192.168.1.41
ANCResult=com.cisco.pxgrid.model.anc.ANCResult@74ad1f1f[
   ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=<null>
  ancpolicies=<null>
]
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect):
```

第 3 步　用户收到 ANC 调配策略通知

```
./ANCAction_query.sh -a 192.168.1.23 -u pxGridClient -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=pxGridClient
  group=ANC
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
12:04:19.804 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
12:04:21.292 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Connected
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect): 6
Press <enter> to disconnect:
Apply Endpoint Policy Notification:
Policy=ANC_Provisioning IP Address=192.168.1.41
```

符合 ANC 策略的终端列表

此示例涵盖已应用了 ANC 策略的终端列表。例如，您可以将 ANC 隔离策略应用到一个终端列表。

第 1 步 运行 ANC_Action 查询脚本，选择 **14**，选择策略名称 **ANC_Provisioning**。
您会看到分配了 ANC_Provisioning 策略的 MAC 地址列表。

```
./ANCAction_query.sh -a 192.168.1.23 -u pxGridClient -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=pxGridClient
  group=ANC
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
13:32:53.702 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
13:32:54.973 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect): 14
Policy name (or <enter> to disconnect): ANC_Provisioning
ANCResult=com.cisco.pxgrid.model.anc.ANCResult@11758f2a[
  ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=[com.cisco.pxgrid.model.anc.ANCEndpoint@74ad1f1f[
   policyName=ANC_Provisioning
  macAddress=00:0C:29:79:02:A8
  ipAddress=<null>
]]
  ancpolicies=<null>
]
Operation selection:
  1. ApplyEndpointPolicyByMAC
  2. ClearEndpointPolicyByMAC
  3. ApplyEndpointPolicyByIP
  4. ClearEndpointPolicyByIP
  5. GetEndpointByIP
  6. Subscribe
  7. CreatePolicy
  8. UpdatePolicy
  9. DeletePolicy
  10. GetPolicyByName
  11. GetAllPolicies
  12. GetEndPointByMAC
  13. GetAllEndpoints
  14. GetEndpointByPolicy
Enter number (or <enter> to disconnect):
```

动态主题

动态主题允许连接到 ISE pxGrid 节点的 pxGrid 客户端发布、订阅信息主题及对信息主题采取操作。动态主题包括以下内容：

- 主题设置：

  主题、查询项目和操作项目使用“propose_capabiility.sh”定义。

- 发布主题

  发布服务器使用“generic_client -c publisher.properties”定义，其中发布服务器属性为一个说明主题信息（例如，主题名称、发布服务器客户端模式及其他项目）的配置文件。

- 订阅主题

  用户使用“generic_client -c subscriber.properties”定义，其中用户属性为说明主题信息（例如，主题名称及其他项目、用户客户端模式以及查询和/或操作名称集及其他项目）的配置文件。只读查询名称集为用户提供特定访问主题信息。

  操作项目面向未订阅信息主题、但想要对主题执行查询的用户。

对于此示例，发布的主题或功能将是拍卖和拍卖服务。sdk-01-pub pxGrid 客户端将发布拍卖主题，而 sdk-01-sub pxGrid 客户端将订阅该主题，并允许查询“获取库存服务”和“获取当前投标”。另一个 pxGrid 客户端 sdk-01-act 操作也会订阅主题和接收任何通知，但是此客户端将只能“对项目投标”或者采取操作。

核心订阅

当 pxGrid 客户端订阅“核心”主题时，提供功能主题通知列表。

第 1 步　运行以下脚本：

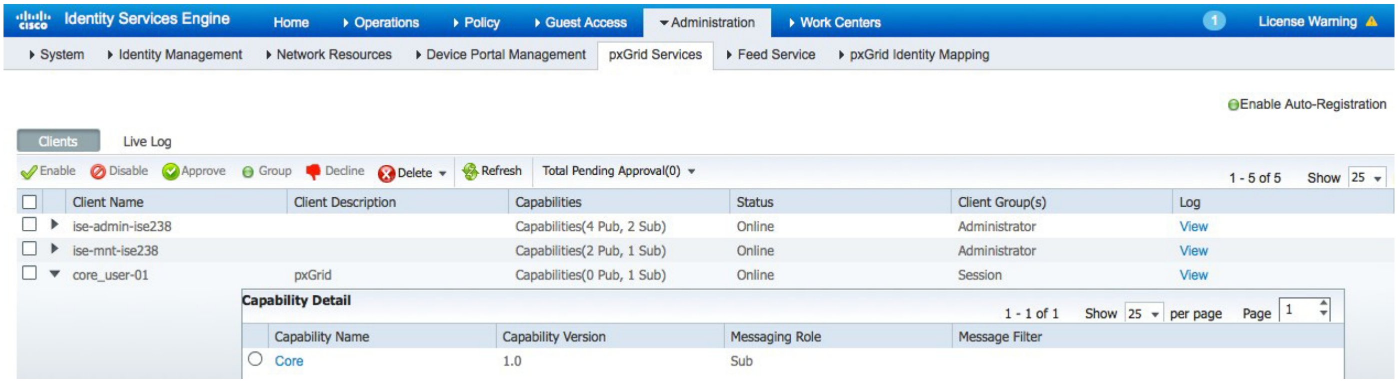
```
./core_subscribe.sh -a 10.0.0.37 -u core_user-01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123 -g
Session -d pxGrid Client
```

获取可用功能或信息主题列表。

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=core_user-01
  group=Session
  description=pxGrid
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:38:47.850 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
```

```
Connected
11:38:50.611 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
getList: status=CREATED capability=TrustSecMetaData, version=1.0
getList: status=CREATED capability=EndpointProfileMetaData, version=1.0
getList: status=CREATED capability=IdentityGroup, version=1.0
getList: status=CREATED capability=GridControllerAdminService, version=1.0
getList: status=CREATED capability=SessionDirectory, version=1.0
getList: status=CREATED capability=AdaptiveNetworkControl, version=1.0
getList: status=CREATED capability=EndpointProtectionService, version=1.0
getList: status=CREATED capability=Core, version=1.0
Capability name [, version] to query (or <enter> to quit) :
```

第 2 步　查看 pxGrid 客户端已订阅核心功能（选择**管理 [Administration]->pxGrid 服务 [pxGrid Services]**



□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	core_user-01	pxGrid	Capabilities(0 Pub, 1 Sub)	Online	Session	View

Capability Detail

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	

Propose_New 功能

向 pxGrid 节点定义新的主题信息，或可通过提供功能名称、版本、说明、平台、查询和操作项目修改现有的主题。此主题将保持待批准状态，直到 pxGrid 管理员批准。

第 1 步　运行以下脚本：

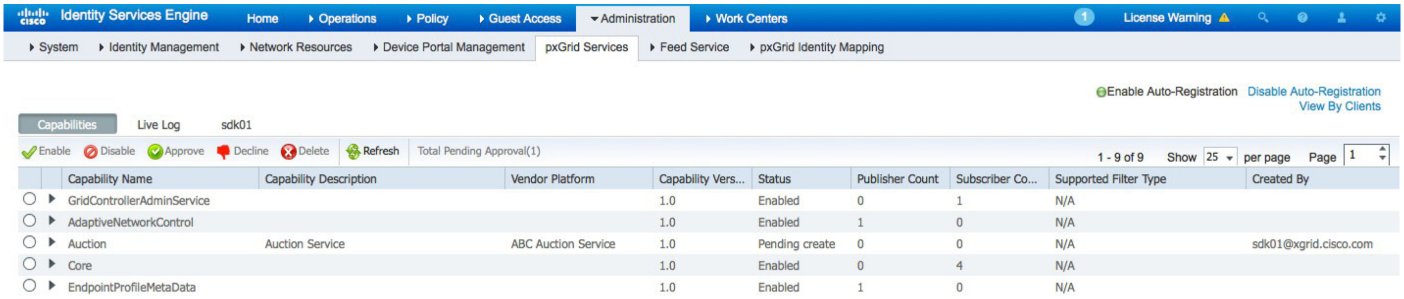
```
./propose_capability.sh -a 10.0.0.37 -u sdk01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123 -g -d
pxGrid New Publisher
```

功能信息将为必填项，系统会提示您输入该信息。

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=sdk01
  group=Basic
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
12:02:07.373 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
```

```
12:02:08.779 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Connected
New capability?(y/n): y
Enter capability name: Auction
Enter capability version: 1.0
Enter capability description: Auction Service
Enter vendor platform: ABC Auction Service
Enter query name (<enter> to continue): GetInventoryItems
Enter query name (<enter> to continue): GetCurrentBids
Enter query name (<enter> to continue):
Enter action name (<enter> to continue): BidOnItems
Enter action name (<enter> to continue):
Proposing new
capability...Press <enter> to
disconnect...Connection closed
```

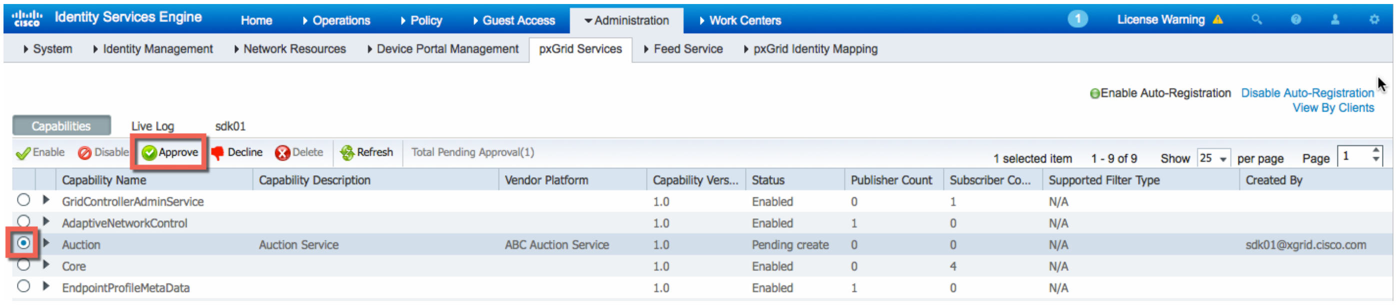
第 2 步 选择管理 (Administration)->pxGrid 服务 (pxGrid Services)->按功能查看 (View by Capabilities) 您会看到“拍卖”(Auction) 功能处于“待批准状态”



	Capability Name	Capability Description	Vendor Platform	Capability Vers...	Status	Publisher Count	Subscriber Co...	Supported Filter Type	Created By
○	GridControllerAdminService			1.0	Enabled	0	1	N/A	
○	AdaptiveNetworkControl			1.0	Enabled	1	0	N/A	
○	Auction	Auction Service	ABC Auction Service	1.0	Pending create	0	0	N/A	sdk01@xgrid.cisco.com
○	Core			1.0	Enabled	0	4	N/A	
○	EndpointProfileMetaData			1.0	Enabled	1	0	N/A	

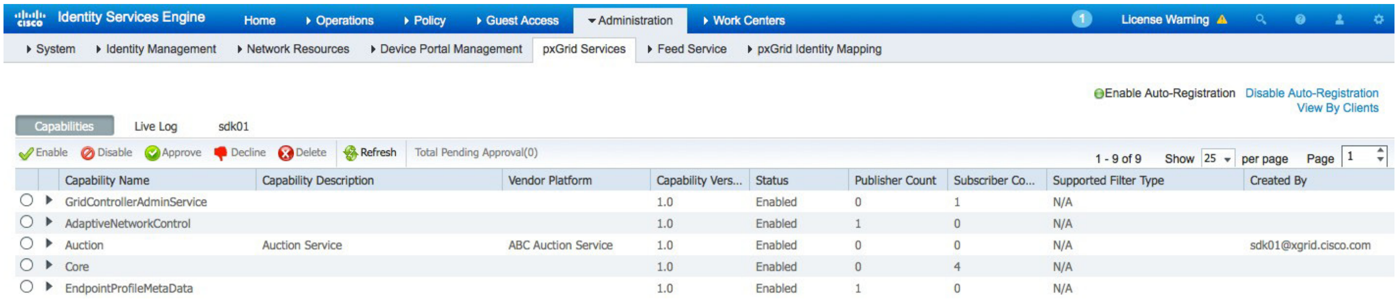
第 3 步 选择主题-> “批准” (Approve)

第 4 步 pxGrid 管理员批准主题



	Capability Name	Capability Description	Vendor Platform	Capability Vers...	Status	Publisher Count	Subscriber Co...	Supported Filter Type	Created By
○	GridControllerAdminService			1.0	Enabled	0	1	N/A	
○	AdaptiveNetworkControl			1.0	Enabled	1	0	N/A	
●	Auction	Auction Service	ABC Auction Service	1.0	Pending create	0	0	N/A	sdk01@xgrid.cisco.com
○	Core			1.0	Enabled	0	4	N/A	
○	EndpointProfileMetaData			1.0	Enabled	1	0	N/A	

第 5 步 “拍卖”主题成功创建

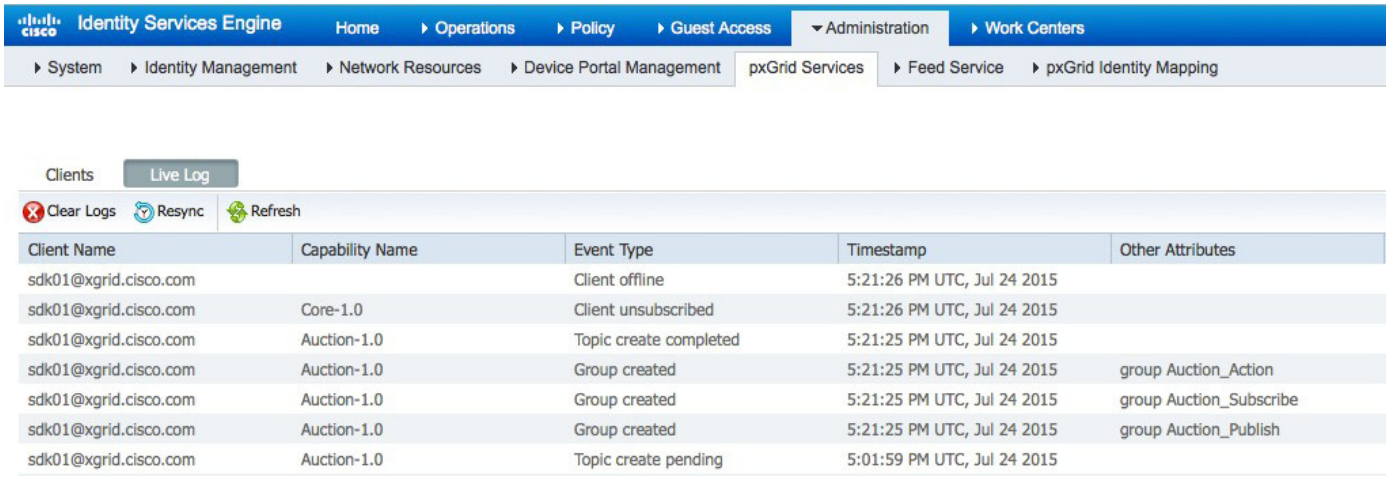


	Capability Name	Capability Description	Vendor Platform	Capability Vers...	Status	Publisher Count	Subscriber Co...	Supported Filter Type	Created By
○	GridControllerAdminService			1.0	Enabled	0	1	N/A	
○	AdaptiveNetworkControl			1.0	Enabled	1	0	N/A	
○	Auction	Auction Service	ABC Auction Service	1.0	Enabled	0	0	N/A	sdk01@xgrid.cisco.com
○	Core			1.0	Enabled	0	4	N/A	
○	EndpointProfileMetaData			1.0	Enabled	1	0	N/A	

第 6 步 如果 pxGrid 客户端如下高亮显示了“core_subscribed”， 系统将显示新主题通知

```
/core_subscribe.sh -a 10.0.0.37 -u core_user-01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123 -g
Session -d pxGrid Client
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=core_user-01
  group=Session
  description=pxGrid
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
11:48:41.155 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
11:48:42.946 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
getList: status=CREATED capability=TrustSecMetaData, version=1.0
getList: status=CREATED capability=EndpointProfileMetaData, version=1.0
getList: status=CREATED capability=IdentityGroup, version=1.0
getList: status=CREATED capability=GridControllerAdminService, version=1.0
getList: status=CREATED capability=SessionDirectory, version=1.0
getList: status=CREATED capability=AdaptiveNetworkControl, version=1.0
getList: status=CREATED capability=EndpointProtectionService, version=1.0
getList: status=CREATED capability=Core, version=1.0
Capability name [, version] to query (or <enter> to quit) : notification: status=CREATED capability=Auction,
version=1.0
```

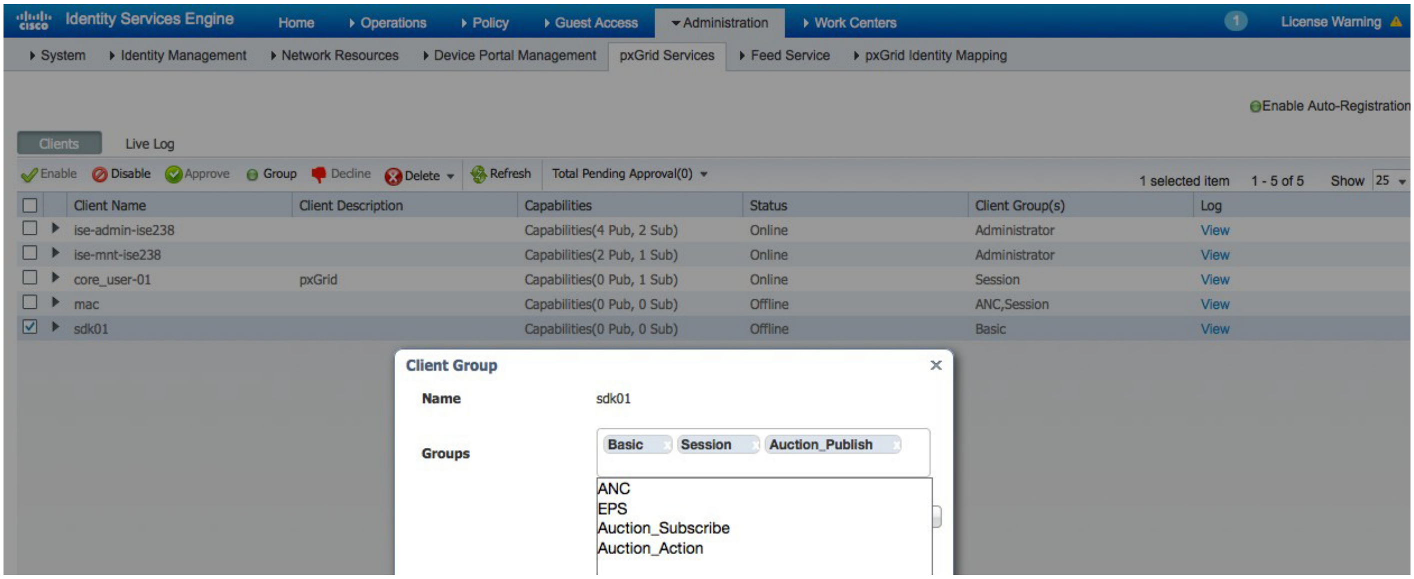
第 7 步　选择 **Live Log** 查看拍卖主题设置的记录



Client Name	Capability Name	Event Type	Timestamp	Other Attributes
sdk01@xgrid.cisco.com		Client offline	5:21:26 PM UTC, Jul 24 2015	
sdk01@xgrid.cisco.com	Core-1.0	Client unsubscribed	5:21:26 PM UTC, Jul 24 2015	
sdk01@xgrid.cisco.com	Auction-1.0	Topic create completed	5:21:25 PM UTC, Jul 24 2015	
sdk01@xgrid.cisco.com	Auction-1.0	Group created	5:21:25 PM UTC, Jul 24 2015	group Auction_Action
sdk01@xgrid.cisco.com	Auction-1.0	Group created	5:21:25 PM UTC, Jul 24 2015	group Auction_Subscribe
sdk01@xgrid.cisco.com	Auction-1.0	Group created	5:21:25 PM UTC, Jul 24 2015	group Auction_Publish
sdk01@xgrid.cisco.com	Auction-1.0	Topic create pending	5:01:59 PM UTC, Jul 24 2015	

第 8 步　选择**管理 (Administration)-> pxGrid 服务 (pxGrid Services)->sdk01->组 (Group)->基本、会话、拍卖发布 (Basic, Session, Action Publish)->保存 (Save)**

注意：管理员必须从“基本”组分配主题到其他组。“基本”组仅是一个 pxGrid 连接组。



□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	core_user-01	pxGrid	Capabilities(0 Pub, 1 Sub)	Online	Session	View
□	mac		Capabilities(0 Pub, 0 Sub)	Offline	ANC,Session	View
☑	sdk01		Capabilities(0 Pub, 0 Sub)	Offline	Basic	View

Client Group

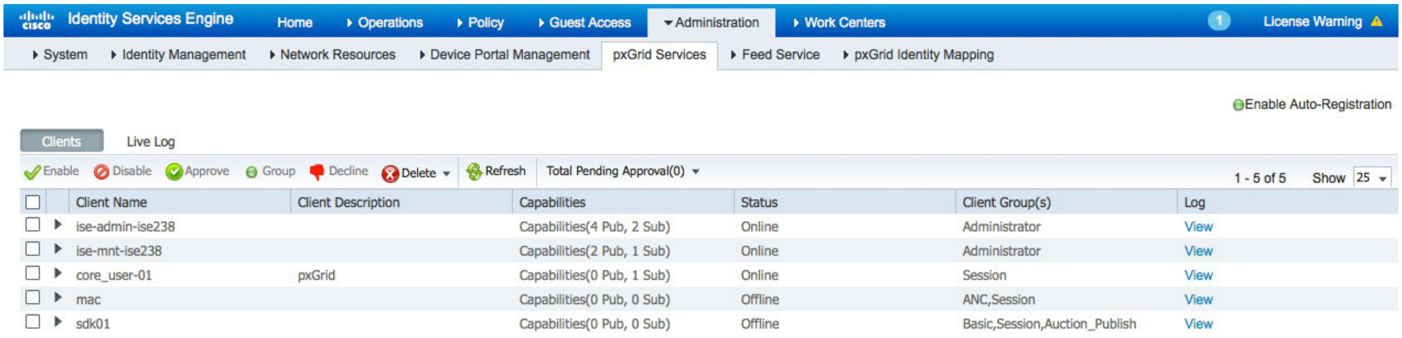
Name　sdk01

Groups　Basic　Session　Auction_Publish

ANC
EPS
Auction_Subscribe
Auction_Action

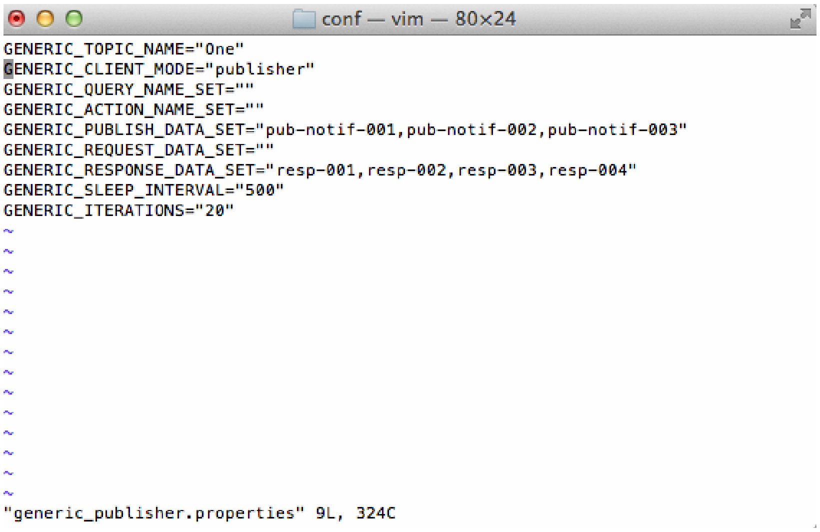
第 9 步　点击 sdk01 旁的**查看 (View)**

您会看到发布的拍卖主题。



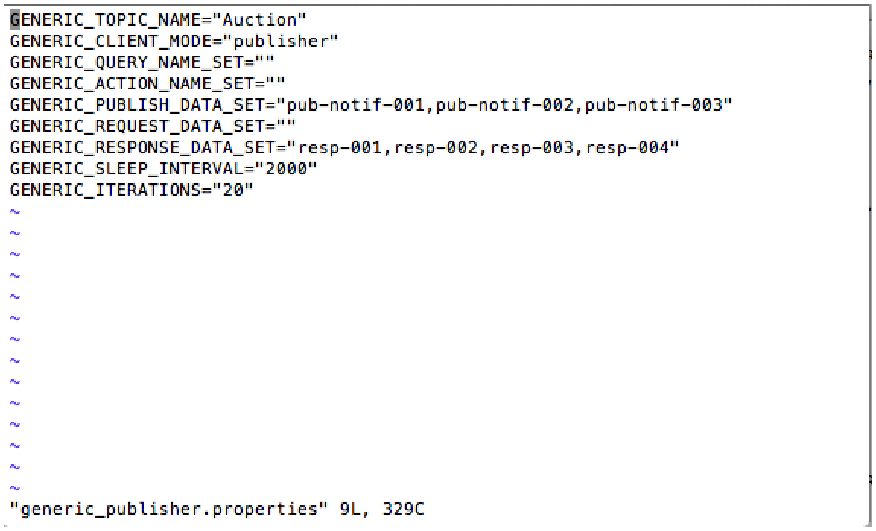
□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	core_user-01	pxGrid	Capabilities(0 Pub, 1 Sub)	Online	Session	View
□	mac		Capabilities(0 Pub, 0 Sub)	Offline	ANC,Session	View
□	sdk01		Capabilities(0 Pub, 0 Sub)	Offline	Basic,Session,Auction_Publish	View

第 10 步　我们需要确定发布事件的发布服务器。编辑 publisher.conf 文件



```
GENERIC_TOPIC_NAME="One"
GENERIC_CLIENT_MODE="publisher"
GENERIC_QUERY_NAME_SET=""
GENERIC_ACTION_NAME_SET=""
GENERIC_PUBLISH_DATA_SET="pub-notif-001,pub-notif-002,pub-notif-003"
GENERIC_REQUEST_DATA_SET=""
GENERIC_RESPONSE_DATA_SET="resp-001,resp-002,resp-003,resp-004"
GENERIC_SLEEP_INTERVAL="500"
GENERIC_ITERATIONS="20"
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"generic_publisher.properties" 9L, 324C
```

第 11 步　更改 GENERIC_TOPIC_NAME="AUCTION"，GENERIC_CLIENT_MODE= "PUBLISHER" 将发布数据集和响应数据集



```
GENERIC_TOPIC_NAME="Auction"
GENERIC_CLIENT_MODE="publisher"
GENERIC_QUERY_NAME_SET=""
GENERIC_ACTION_NAME_SET=""
GENERIC_PUBLISH_DATA_SET="pub-notif-001,pub-notif-002,pub-notif-003"
GENERIC_REQUEST_DATA_SET=""
GENERIC_RESPONSE_DATA_SET="resp-001,resp-002,resp-003,resp-004"
GENERIC_SLEEP_INTERVAL="2000"
GENERIC_ITERATIONS="20"
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"generic_publisher.properties" 9L, 329C
```

第 12 步　运行发布服务器的通用客户端脚本

```
./generic_client.sh -a 10.0.0.37 -u sdk01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123 -c
generic_publisher.properties
```

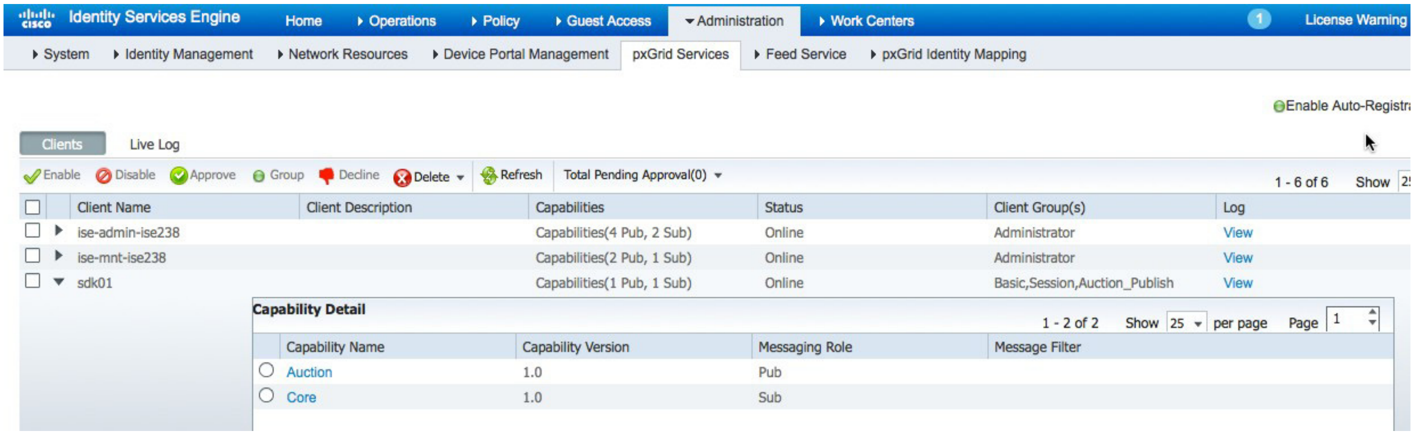
结果

```
Initialized : GenericClient:
        topicName=Auction
        clientMode=PUBLISHER
        sleepInterval=2000
        iterations=20
        queryNameSet=[]
        actionNameSet=[]
        publishDataSet=[pub-notif-001, pub-notif-002, pub-notif-003]
        requestDataSet=[]
        responseDataSet=[resp-001, resp-002, resp-003, resp-004]
```

```
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=sdk01
  group=Auction_Publish
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
14:12:59.548 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
14:13:00.921 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437847981189]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437847983193]pub-notif-002
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437847985194]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437847987195]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437847989196]pub-notif-002
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437847991197]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437847993199]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437847995200]pub-notif-002
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437847997201]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437847999202]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437848001203]pub-notif-002
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437848003207]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437848005209]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437848007210]pub-notif-002
```

```
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437848009211]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437848011213]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437848013214]pub-notif-002
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437848015216]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437848017217]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437848019218]pub-notif-002
Press <enter> to disconnect...
```

第 13 步 pxGrid 客户端 sdk01 发布拍卖主题

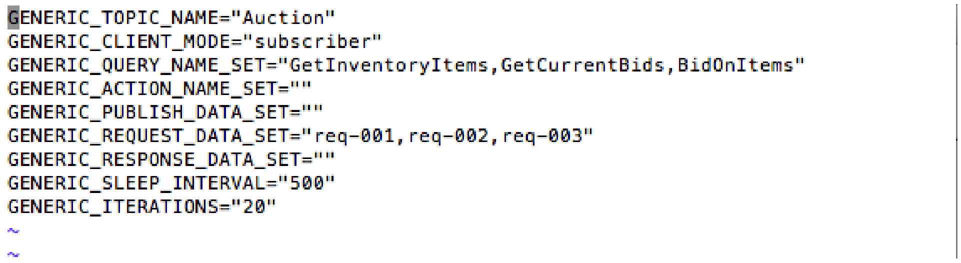


□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▸	ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▸	ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▾	sdk01		Capabilities(1 Pub, 1 Sub)	Online	Basic,Session,Auction_Publish	View

Capability Detail

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Auction	1.0	Pub	
○	Core	1.0	Sub	

第 14 步 我们需要配置用户在直接查询“GetInventoryItems”、“GetCurrentBids”上查询发布的拍卖主题



```
GENERIC_TOPIC_NAME="Auction"
GENERIC_CLIENT_MODE="subscriber"
GENERIC_QUERY_NAME_SET="GetInventoryItems,GetCurrentBids,BidOnItems"
GENERIC_ACTION_NAME_SET=""
GENERIC_PUBLISH_DATA_SET=""
GENERIC_REQUEST_DATA_SET="req-001,req-002,req-003"
GENERIC_RESPONSE_DATA_SET=""
GENERIC_SLEEP_INTERVAL="500"
GENERIC_ITERATIONS="20"
~
~
```

第 15 步 运行用户的通用用户端脚本，请注意客户可访问查询主题 GetInventoryItems、GetCurrentBid 而非 BidOnItems。BidOnItems 未定义为查询主题

```
./generic_client.sh -a 10.0.0.37 -u sdk01-sub -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123 -c
```

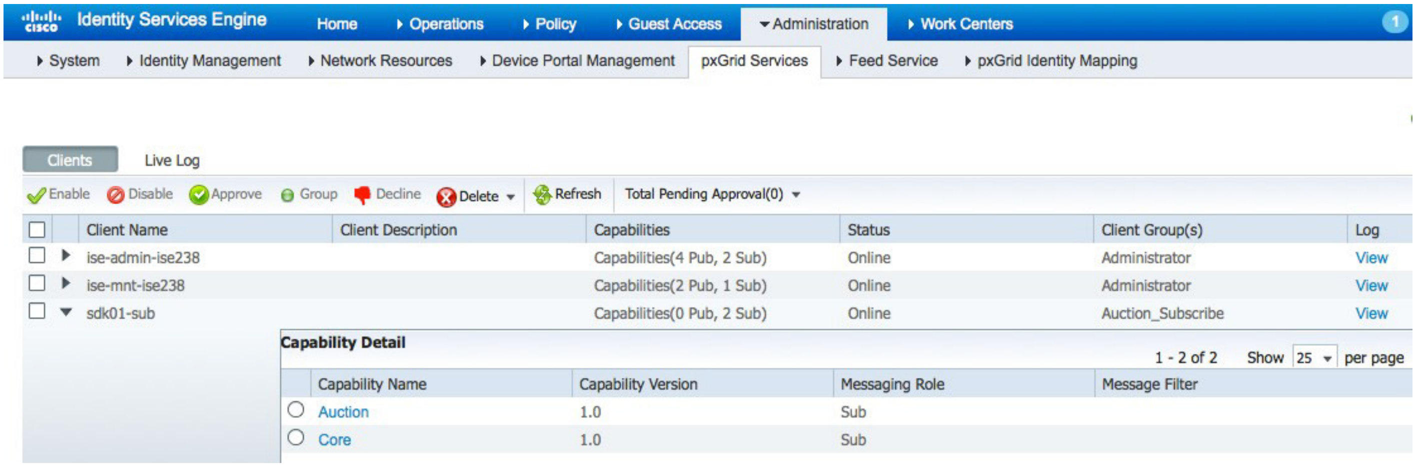
结果

```
Initialized : GenericClient:
        topicName=Auction
        clientMode=SUBSCRIBE
        R sleepInterval=500
        iterations=20
        queryNameSet=[GetInventoryItems, GetCurrentBids, BidOnItems]
        actionNameSet=[]
        publishDataSet=[]
        requestDataSet=[req-001, req-002, req-003]
        responseDataSet=[]

------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=sdk01-sub
  group=Auction_Subscribe
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
```

```
--------------------------
15:51:33.423 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
15:51:36.123 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Sending request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853896264]req-001
Received response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853896285]resp-003 - for request[QUERY[1437853896264]req-001]
Sending request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853896885]req-002
Received response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853896945]resp-004 - for request[QUERY[1437853896885]req-002]
Sending request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=BidOnItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853897457]req-003
Received response: GenericMessage:
  messageType=RESPONSE
  capabilityName=null
  operationName=null
  body:
  error=not authorized
Sending request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853898077]req-001
Received response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853898428]resp-001 - for request[QUERY[1437853898077]req-001]
```

第 16 步　选择管理 (Administration)->pxGrid 服务 (pxGrid Services)

注意 pxGrid 客户端 sdk01-sub 已订阅拍卖主题



□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▸ ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▸ ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▾ sdk01-sub		Capabilities(0 Pub, 2 Sub)	Online	Auction_Subscribe	View

Capability Detail

1 - 2 of 2　Show 25 per page

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Auction	1.0	Sub	
○	Core	1.0	Sub	

摘要

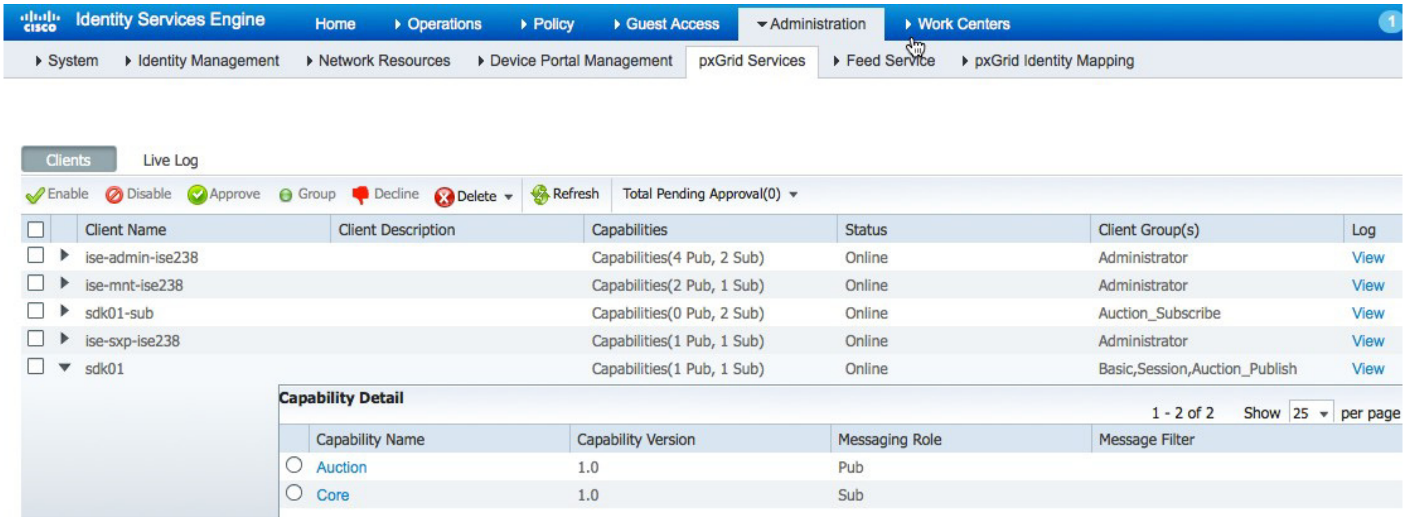
第 1 步　发布服务器 sdk01 发布拍卖主题

```
./generic_client.sh -a 10.0.0.37 -u sdk01 -k alpha.jks -p cisco123 -t alpha_root.jks -q cisco123 -c
generic_publisher.properties
Initialized : GenericClient:
        topicName=Auction
        clientMode=PUBLISHER
        sleepInterval=2000
        iterations=20
        queryNameSet=[]
        actionNameSet=[]
        publishDataSet=[pub-notif-001, pub-notif-002, pub-notif-003]
        requestDataSet=[]
        responseDataSet=[resp-001, resp-002, resp-003, resp-004]

------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=10.0.0.37
  username=sdk01
  group=Auction_Publish
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
15:47:52.196 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
15:47:53.548 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853673689]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853675695]pub-notif-002
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853677696]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853679697]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853681699]pub-notif-002
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853683700]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853685701]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853687703]pub-notif-002
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853689704]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853691705]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853693706]pub-notif-002
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853695710]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853697711]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853699712]pub-notif-002
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853701713]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853703714]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853705715]pub-notif-002
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853707717]pub-notif-003
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853709717]pub-notif-001
Publishing notification: GenericMessage:
  messageType=NOTIFICATION
  capabilityName=Auction
  operationName=sampleNotification
  body:
    content:
      contentTags=[NOTIF-TAG-201]
      contentType=PLAIN_TEXT
      value=NOTIFICATION[1437853711718]pub-notif-002
Press <enter> to disconnect...Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853868986]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853869075]resp-001 - for request[QUERY[1437853868986]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853869589]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853869616]resp-002 - for request[QUERY[1437853869589]req-002]
```

```
15:51:10.148 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853870656]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853870693]resp-003 - for request[QUERY[1437853870656]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853871201]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853871231]resp-004 - for request[QUERY[1437853871201]req-002]
15:51:11.776 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853872281]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853872418]resp-001 - for request[QUERY[1437853872281]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853872924]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853872950]resp-002 - for request[QUERY[1437853872924]req-002]
15:51:13.485 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853873991]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853874019]resp-003 - for request[QUERY[1437853873991]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853874538]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853874566]resp-004 - for request[QUERY[1437853874538]req-002]
15:51:15.106 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853875612]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853875639]resp-001 - for request[QUERY[1437853875612]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853876145]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853876175]resp-002 - for request[QUERY[1437853876145]req-002]
15:51:16.719 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853877240]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853877270]resp-003 - for request[QUERY[1437853877240]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853877776]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853877800]resp-004 - for request[QUERY[1437853877776]req-002]
15:51:18.383 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853878895]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853878925]resp-001 - for request[QUERY[1437853878895]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853879433]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853879459]resp-002 - for request[QUERY[1437853879433]req-002]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853896264]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853896285]resp-003 - for request[QUERY[1437853896264]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853896885]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853896945]resp-004 - for request[QUERY[1437853896885]req-002]
15:51:37.506 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853898077]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853898428]resp-001 - for request[QUERY[1437853898077]req-001]
```

```
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853898938]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853898977]resp-002 - for request[QUERY[1437853898938]req-002]
15:51:39.509 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853900015]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853900041]resp-003 - for request[QUERY[1437853900015]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853900547]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853900571]resp-004 - for request[QUERY[1437853900547]req-002]
15:51:41.109 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853901614]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853901641]resp-001 - for request[QUERY[1437853901614]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853902147]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853902172]resp-002 - for request[QUERY[1437853902147]req-002]
15:51:42.706 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853903210]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853903237]resp-003 - for request[QUERY[1437853903210]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853903743]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853903771]resp-004 - for request[QUERY[1437853903743]req-002]
15:51:44.412 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853904916]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853904944]resp-001 - for request[QUERY[1437853904916]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853905450]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853905479]resp-002 - for request[QUERY[1437853905450]req-002]
15:51:46.024 [Smack-Cached Executor 2 (0)] INFO c.c.p.i.GenericMessageDispatcher - Returning error -
Authorization failed for sender: sdk01-sub@xgrid.cisco.com, capability: Auction, operation: BidOnItems
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853906529]req-001
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetInventoryItems
  body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853906557]resp-003 - for request[QUERY[1437853906529]req-001]
Received request: GenericMessage:
  messageType=REQUEST
  capabilityName=Auction
  operationName=GetCurrentBids
  body:
    content:
      contentTags=[QUERY-TAG-301]
      contentType=PLAIN_TEXT
      value=QUERY[1437853907066]req-002
Returning response: GenericMessage:
  messageType=RESPONSE
  capabilityName=Auction
  operationName=GetCurrentBids body:
    content:
      contentTags=[RESP-TAG-101]
      contentType=PLAIN_TEXT
      value=RESPONSE[1437853907099]resp-004 - for request[QUERY[1437853907066]req-002]
```

第 2 步 选择**管理 (Administration)->pxGrid 服务 (pxGrid Services)**
sdk01 pxGrid 客户端注册为发布服务器



□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	▶	ise-admin-ise238		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	▶	ise-mnt-ise238		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▶	sdk01-sub		Capabilities(0 Pub, 2 Sub)	Online	Auction_Subscribe	View
□	▶	ise-sxp-ise238		Capabilities(1 Pub, 1 Sub)	Online	Administrator	View
□	▼	sdk01		Capabilities(1 Pub, 1 Sub)	Online	Basic,Session,Auction_Publish	View

Capability Detail

1 - 2 of 2 Show 25 per page

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Auction	1.0	Pub	
○	Core	1.0	Sub	

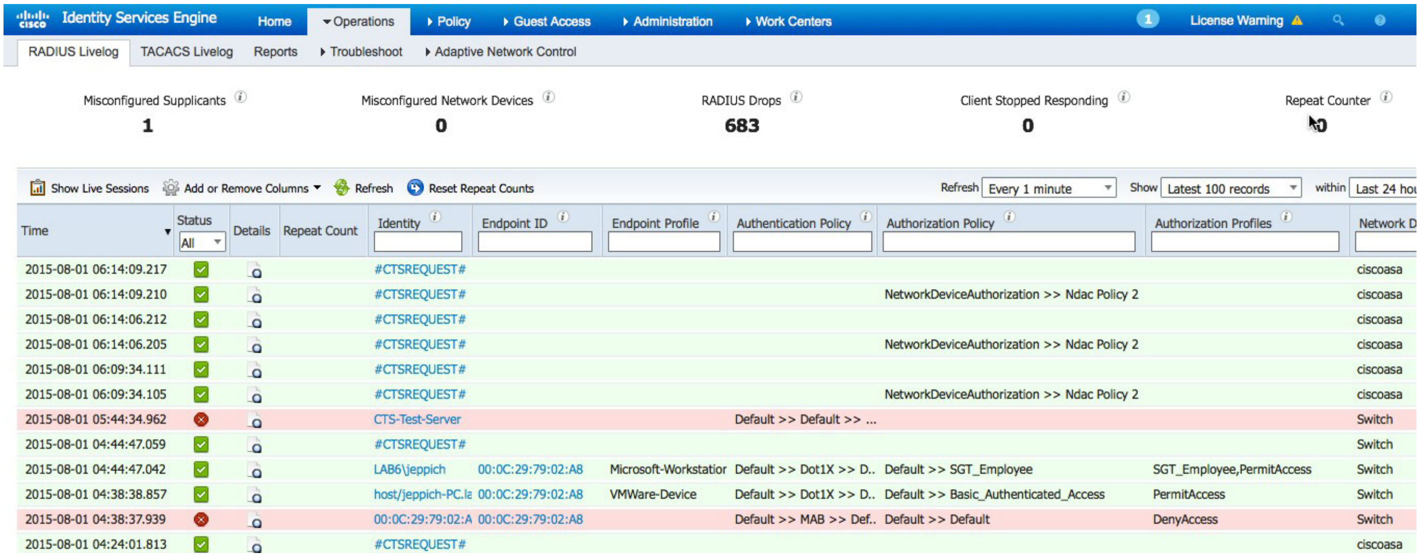
SXP 发布

ISE 2.0 提供一个 SXP 连接监听程序。pxGrid 提供 ISE 发布 SXP 连接信息（例如 IP 地址、SGT 标记、源和对等序列）的能力。

ISE 示例脚本 sxp_download 和 sxp_subscribe 脚本可用来获取此信息。

在此示例中，初始测试中使用了 Cisco Catalyst 3750x 和 ASA 5505。这些设备的 TrustSec 部署可以在参考部分找到。请注意，读者必须熟悉思科的 TrustSec 解决方案。

在配置 SXP 绑定设置之前，请确保您在启用 SXP 的设备上正确配置了 CTS。验证您在授权策略中看到的是否为合适的 #CTS 请求#。



Misconfigured Supplicants 1 | Misconfigured Network Devices 0 | RADIUS Drops 683 | Client Stopped Responding 0 | Repeat Counter 0

Refresh: Every 1 minute | Show: Latest 100 records | within: Last 24 hou

Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network D
2015-08-01 06:14:09.217	✓			#CTSREQUEST#						ciscoasa
2015-08-01 06:14:09.210	✓			#CTSREQUEST#				NetworkDeviceAuthorization >> Ndac Policy 2		ciscoasa
2015-08-01 06:14:06.212	✓			#CTSREQUEST#						ciscoasa
2015-08-01 06:14:06.205	✓			#CTSREQUEST#				NetworkDeviceAuthorization >> Ndac Policy 2		ciscoasa
2015-08-01 06:09:34.111	✓			#CTSREQUEST#						ciscoasa
2015-08-01 06:09:34.105	✓			#CTSREQUEST#				NetworkDeviceAuthorization >> Ndac Policy 2		ciscoasa
2015-08-01 05:44:34.962	☒			CTS-Test-Server			Default >> Default >> ...			Switch
2015-08-01 04:44:47.059	✓			#CTSREQUEST#						Switch
2015-08-01 04:44:47.042	✓			LAB6\jeppich	00:0C:29:79:02:A8	Microsoft-Workstatior	Default >> Dot1X >> D..	Default >> SGT_Employee	SGT_Employee,PermitAccess	Switch
2015-08-01 04:38:38.857	✓			host/jeppich-PC.la	00:0C:29:79:02:A8	VMWare-Device	Default >> Dot1X >> D..	Default >> Basic_Authenticated_Access	PermitAccess	Switch
2015-08-01 04:38:37.939	☒			00:0C:29:79:02:A	00:0C:29:79:02:A8		Default >> MAB >> Def..	Default >> Default	DenyAccess	Switch
2015-08-01 04:24:01.813	✓			#CTSREQUEST#						ciscoasa

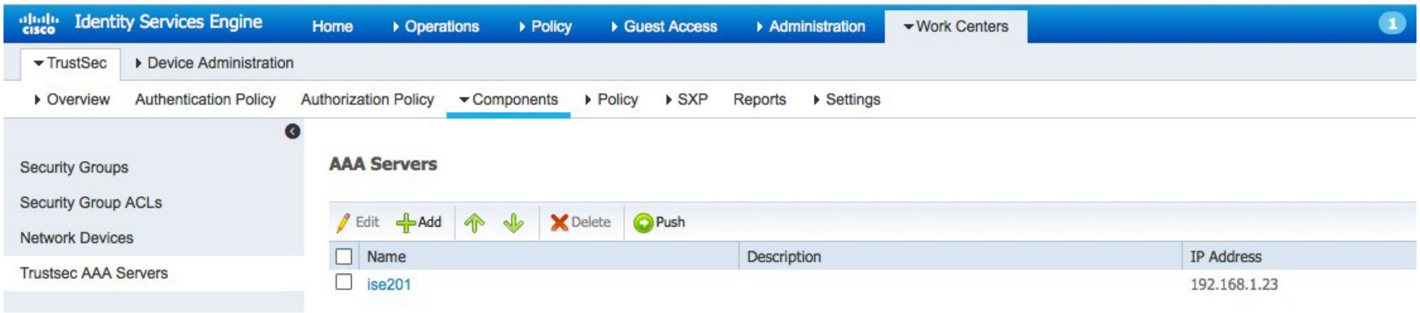
请阅读“TrustSec 概述”了解整个过程。

您还将需要在“管理”(Administration)-> “部署”(Deployment) 下启用 SXP 服务端口并选择节点。

TrustSec AAA 设备

第 1 步 选择工作中心 (Work Centers)->TrustSec->组件 (Components)->AAA 服务器 (AAA Servers)

TrustSec AAA 服务器将已面向 ISE 配置



AAA Servers

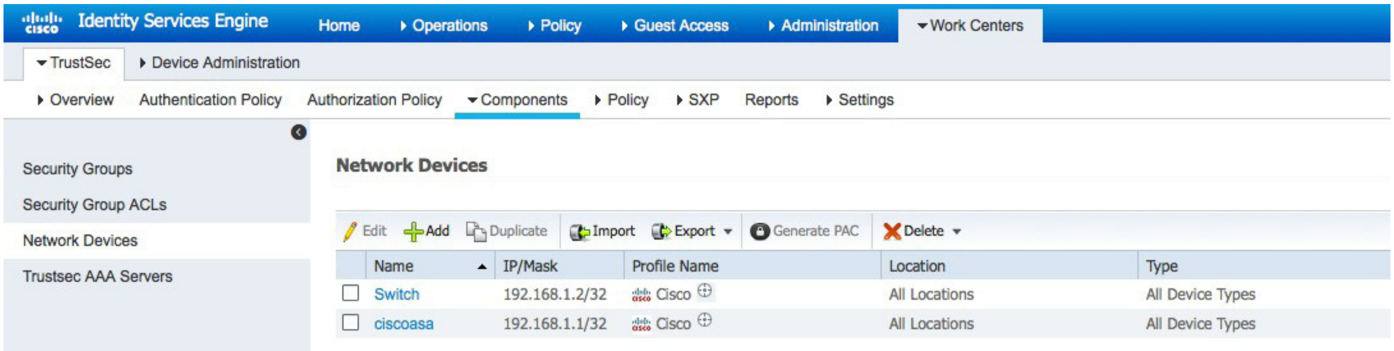
□	Name	Description	IP Address
□	ise201		192.168.1.23

配置适用于 TrustSec 的网络设备

定义适用于 TrustSec 操作的网络设备。定义了 Cisco Catalyst 3750x 交换机和 ASA 5505。

Cisco Catalyst 3750-x

第 1 步 选择工作中心 (Work Centers)->TrustSec->组件 (Components)->网络设备 (Network Devices)



Network Devices

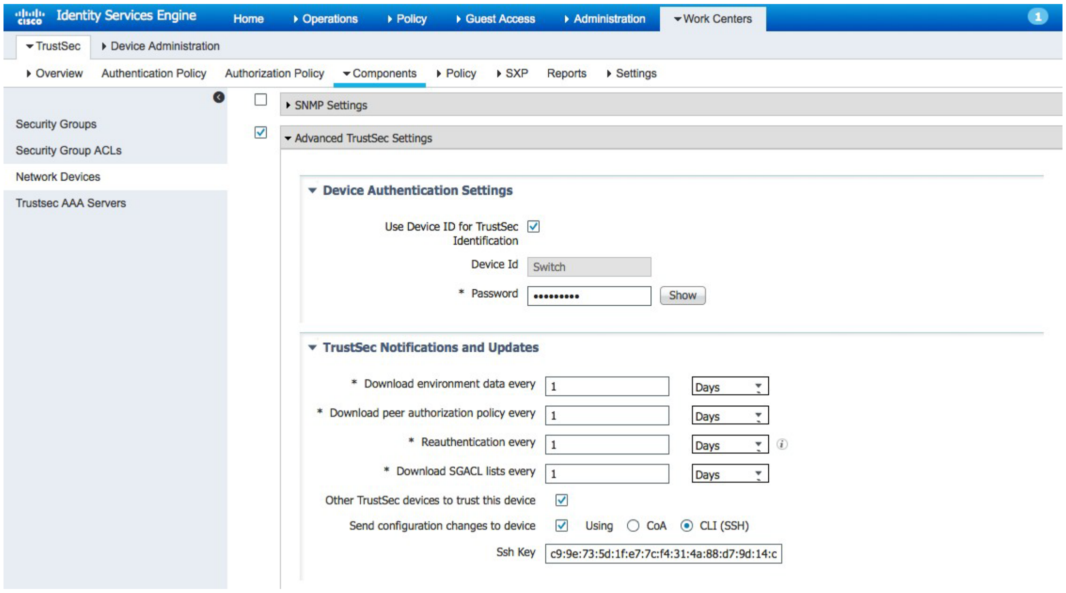
□	Name ▲	IP/Mask	Profile Name	Location	Type
□	Switch	192.168.1.2/32	Cisco ⊕	All Locations	All Device Types
□	ciscoasa	192.168.1.1/32	Cisco ⊕	All Locations	All Device Types

第 2 步　选择工作中心 (Work Centers)->TrustSec->组件 (Components)->网络设备 (Network Devices)

第 3 步　选择使用设备 ID 进行 TrustSec 识别 (Use Device ID for TrustSec Identification)

第 4 步　选择使用 (Using) CLI (SSH) 发送配置更改到设备 (Send configuration changes to device)

注意： 您需要知道 SSH 密钥。如果您不知道 SSH 密钥，您可以在已知主机文件下删除设备的 IP 地址。当您 ssh 到 IP 地址中，将看到显示的 SSH 密钥。



□ SNMP Settings

☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id: Switch

* Password: ••••••••• Show

TrustSec Notifications and Updates

* Download environment data every: 1 Days

* Download peer authorization policy every: 1 Days

* Reauthentication every: 1 Days

* Download SGACL lists every: 1 Days

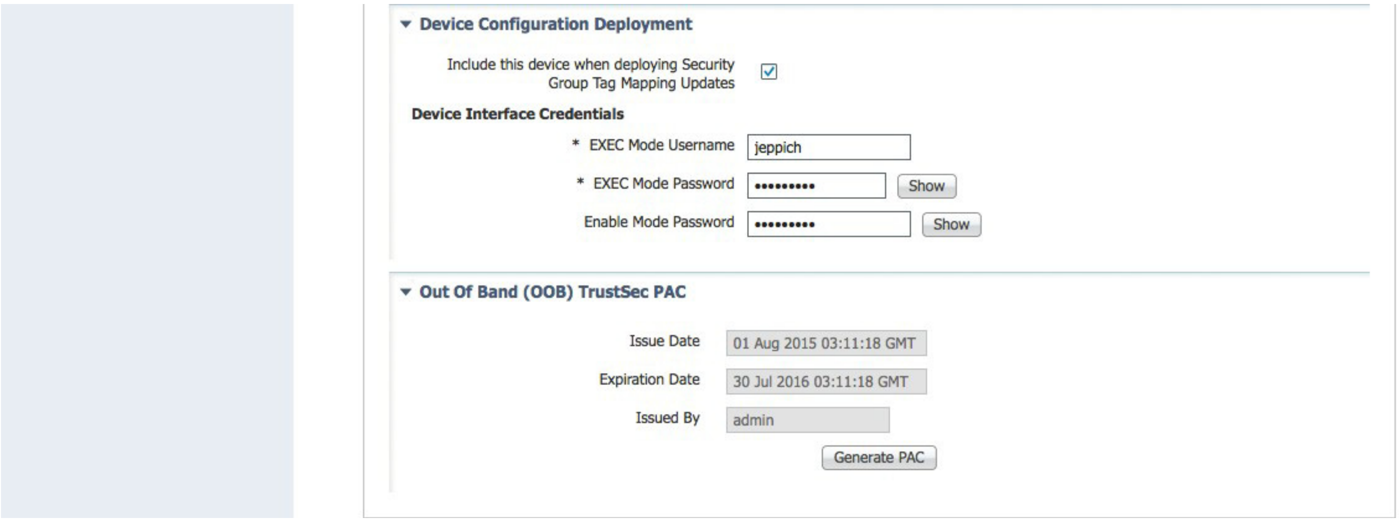
Other TrustSec devices to trust this device ☑

Send configuration changes to device ☑ Using ○ CoA ● CLI (SSH)

Ssh Key: c9:9e:73:5d:1f:e7:7c:f4:31:4a:88:d7:9d:14:c

第 5 步　在“设备配置部署”(Device Configuration Deployment) 下->启用“部署安全组标记更新时包含此设备”(Include this devices when deploying Security Group Tag Updates)

第 6 步　输入设备接口凭证信息



Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates ☑

Device Interface Credentials

* EXEC Mode Username: jeppich

* EXEC Mode Password: ••••••••• Show

Enable Mode Password: ••••••••• Show

Out Of Band (OOB) TrustSec PAC

Issue Date: 01 Aug 2015 03:11:18 GMT

Expiration Date: 30 Jul 2016 03:11:18 GMT

Issued By: admin

Generate PAC

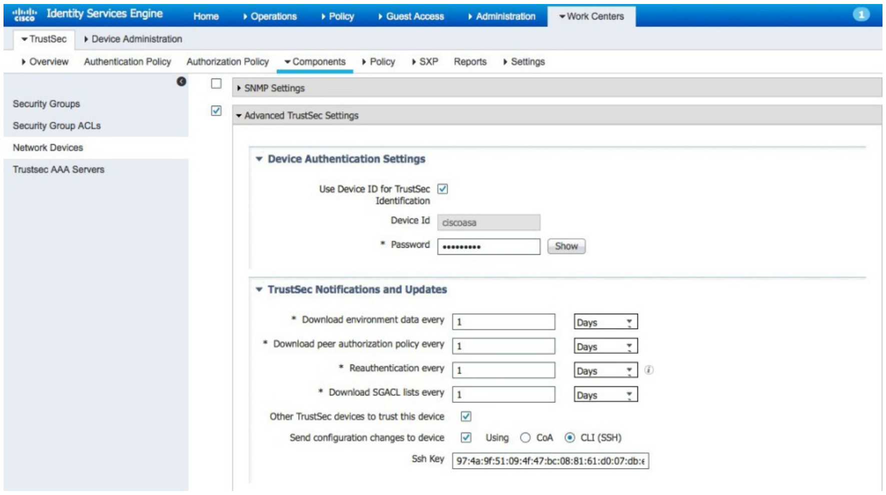
第 7 步　如需要，生成 PAC

ASA 5505

第 1 步　选择工作中心 **(Work Centers)->TrustSec->**组件 **(Components)->**网络设备 **(Network Devices)**

第 2 步　选择使用设备 **ID** 进行 **TrustSec** 识别 **(Use Device ID for TrustSec Identification)**

第 3 步　选择使用 **(Using) CLI (SSH)** 发送配置更改到设备 **(Send configuration changes to device)**



□ SNMP Settings

☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id: ciscoasa

* Password: •••••••••• Show

TrustSec Notifications and Updates

* Download environment data every: 1 Days

* Download peer authorization policy every: 1 Days

* Reauthentication every: 1 Days

* Download SGACL lists every: 1 Days

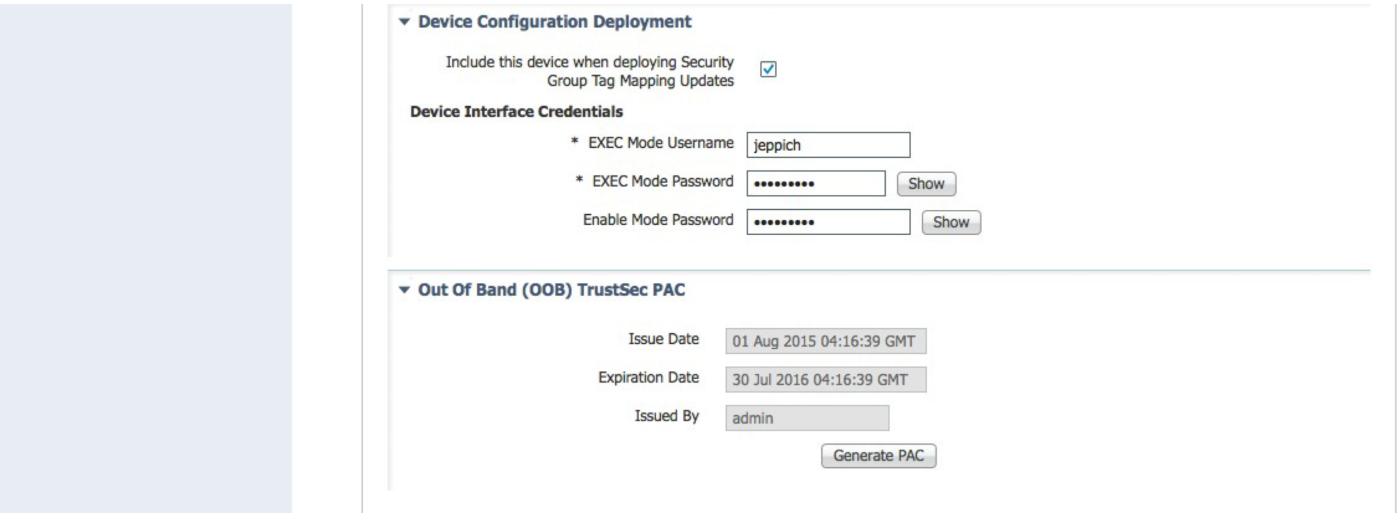
Other TrustSec devices to trust this device ☑

Send configuration changes to device ☑ Using ○ CoA ● CLI (SSH)

Ssh Key: 97:4a:9f:51:09:4f:47:bc:08:81:61:d0:07:db:ε

第 4 步　在“设备配置部署 **(Device Configuration Deployment)**”下->启用“部署安全组标记更新时包含此设备”**(Include this devices when deploying Security Group Tag Updates)**

第 5 步　输入设备接口凭证信息



Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates ☑

Device Interface Credentials

* EXEC Mode Username: jeppich

* EXEC Mode Password: ••••••••• Show

Enable Mode Password: ••••••••• Show

Out Of Band (OOB) TrustSec PAC

Issue Date: 01 Aug 2015 04:16:39 GMT

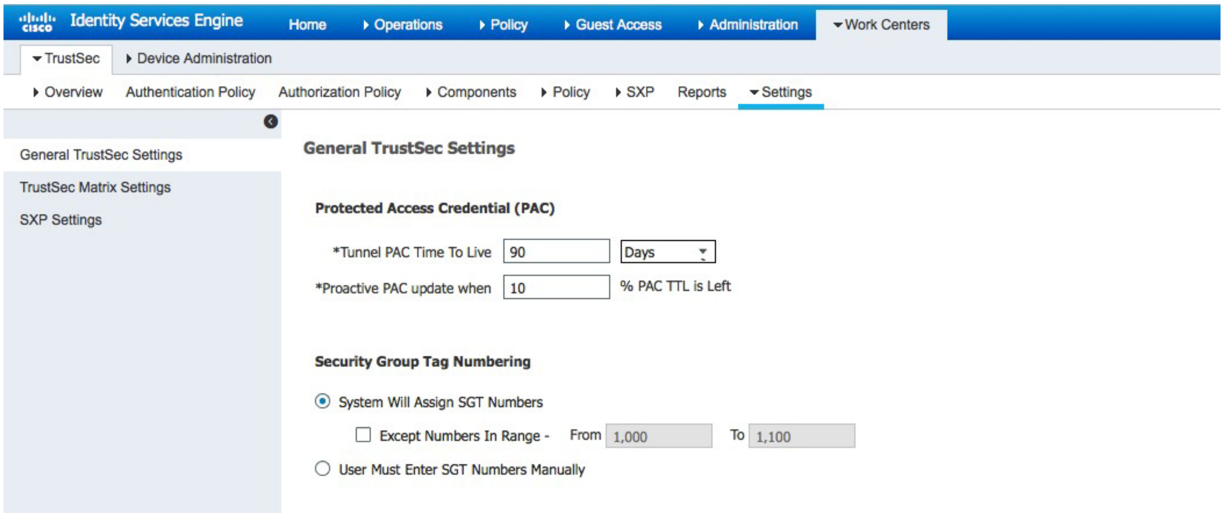
Expiration Date: 30 Jul 2016 04:16:39 GMT

Issued By: admin

配置 TrustSec 设置

此文档中使用默认设置。

第 1 步 选择工作中心 (Work Centers)->TrustSec->设置 (Settings)



General TrustSec Settings

Protected Access Credential (PAC)

*Tunnel PAC Time To Live: 90 Days

*Proactive PAC update when: 10 % PAC TTL is Left

Security Group Tag Numbering

● System Will Assign SGT Numbers

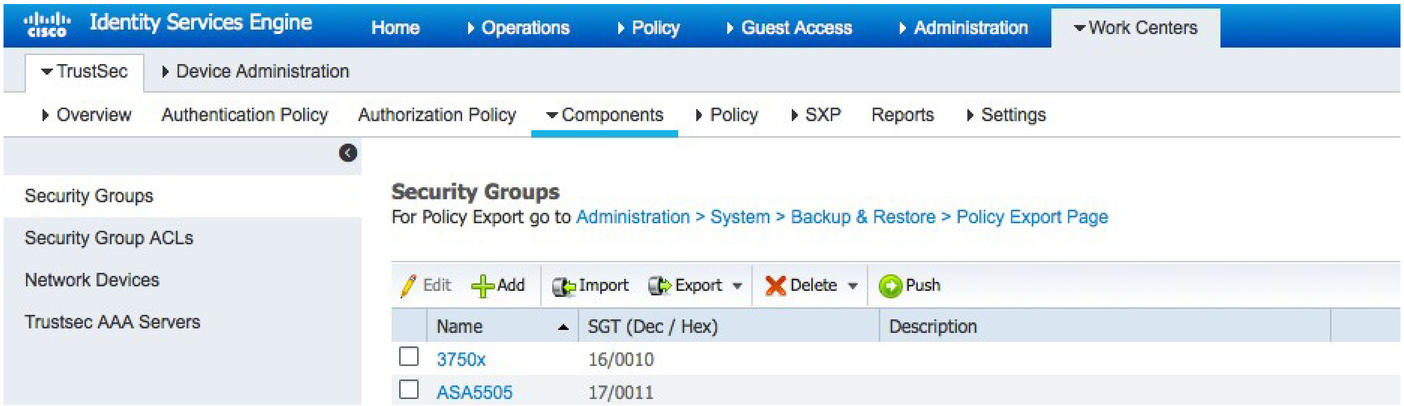
□ Except Numbers In Range - From 1,000 To 1,100

○ User Must Enter SGT Numbers Manually

配置安全组

创建了 3750x 和 ASA5505 SGT 标记。

第 1 步 选择工作中心 (Work Centers)->组件 (Components)->安全组 (Security Groups)->添加 (Add) 安全组



Security Groups

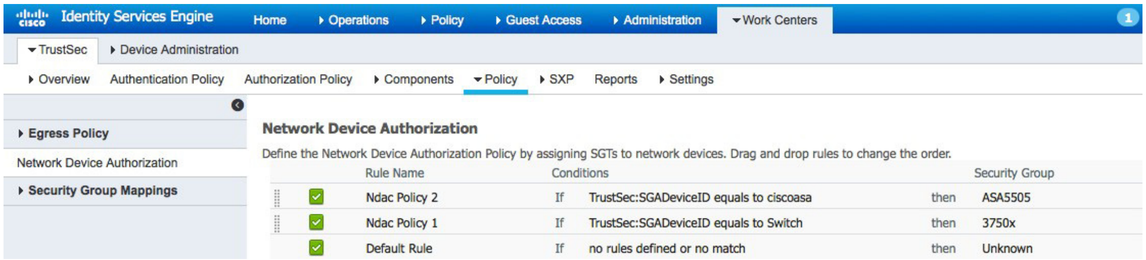
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

	Name	SGT (Dec / Hex)	Description
□	3750x	16/0010	
□	ASA5505	17/0011	

配置网络设备授权策略

为 ASA5505 和 3750x 安全组创建了两条规则

第 1 步 选择工作中心 (Work Center)->TrustSec->策略 (Policy)->添加新的网络设备规则



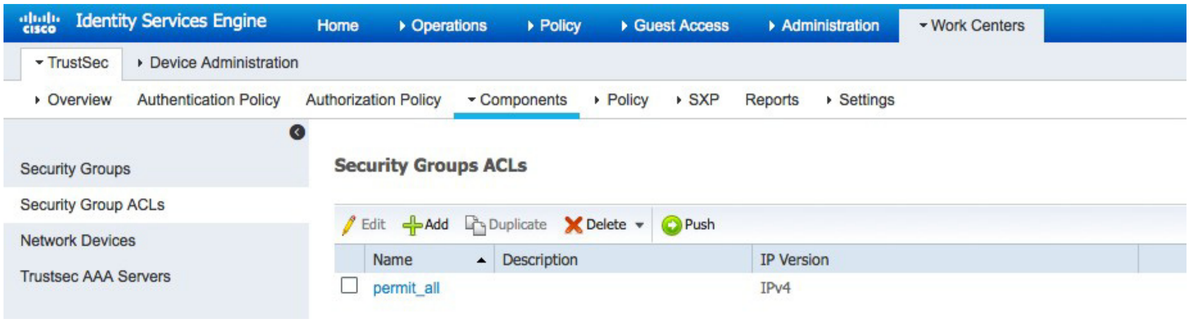
Network Device Authorization

Define the Network Device Authorization Policy by assigning SGTs to network devices. Drag and drop rules to change the order.

	Rule Name		Conditions		Security Group
☑	Ndac Policy 2	If	TrustSec:SGADeviceID equals to ciscoasa	then	ASA5505
☑	Ndac Policy 1	If	TrustSec:SGADeviceID equals to Switch	then	3750x
☑	Default Rule	If	no rules defined or no match	then	Unknown

定义 SGACL

第 1 步　选择工作中心 (Work Centers)->TrustSec->组件 (Components)->安全组 ACL (Security Group ACLs)->添加 (add)->允许全部 (permit all)



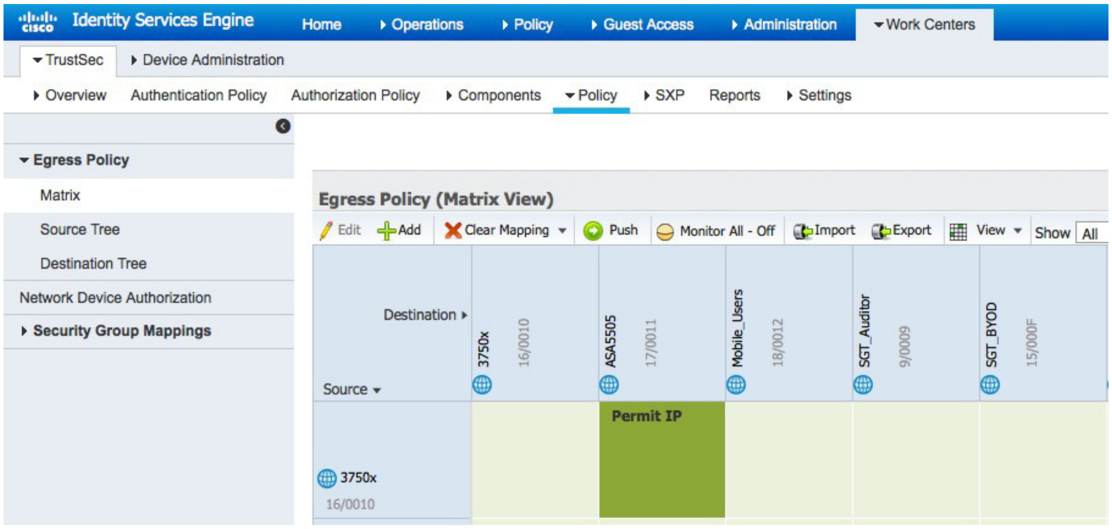
Security Groups ACLs

	Name	Description	IP Version
□	permit_all		IPv4

分配 SAGL 到矩阵

将 SAGL 分配至出口策略矩阵，以允许其他标记的网络设备的网络访问。在思科 3750x 和 ASA 5505 之间创建了一个普遍适用的允许全部 (permit all)。

第 1 步　选择工作中心 (Work Centers)->TrustSec->策略 (Policy)->出口策略矩阵 (Egress Policy Matrix)->添加 (Add)



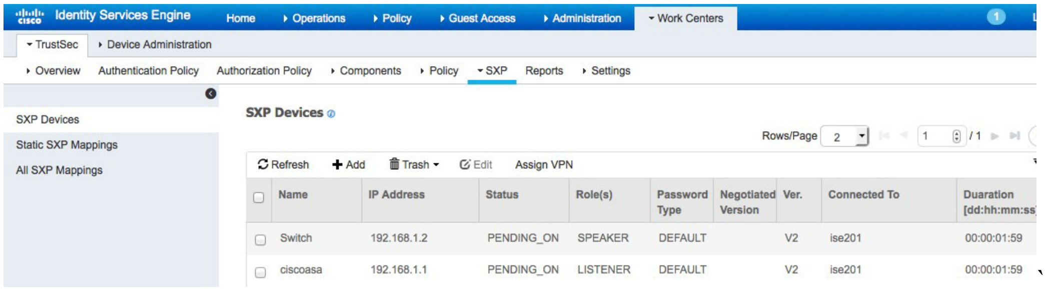
Egress Policy (Matrix View)

Source ▾ / Destination ▸	3750x 16/0010	ASA5505 17/0011	Mobile_Users 18/0012	SGT_Auditor 9/0009	SGT_BYOD 15/000F
3750x 16/0010		Permit IP			

配置 SXP 以允许将 IP 到 SGT 映射分配到非 TrustSec 设备

3750x 和 ASA5505 设备根据其 IP 地址、角色进行了定义。

第 1 步　选择工作中心 (Centers)->TrustSec->策略 (Policy)->SXP 设备 (SXP Devices)->添加 (add)



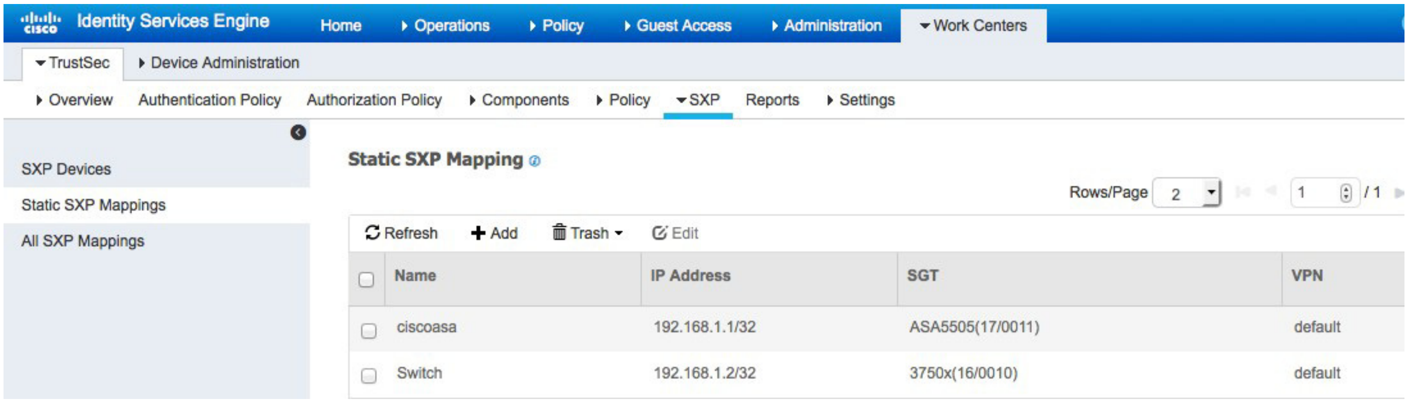
SXP Devices

Name	IP Address	Status	Role(s)	Password Type	Negotiated Version	Ver.	Connected To	Duaration [dd:hh:mm:ss
Switch	192.168.1.2	PENDING_ON	SPEAKER	DEFAULT		V2	ise201	00:00:01:59
ciscoasa	192.168.1.1	PENDING_ON	LISTENER	DEFAULT		V2	ise201	00:00:01:59

分配静态映射

创建了 3750x 和 ASA5505 映射并发布到网络。

第 1 步　选择工作中心 (Work Centers)->TrustSec->SXP->定义网络设备的静态映射



Static SXP Mapping

Name	IP Address	SGT	VPN
ciscoasa	192.168.1.1/32	ASA5505(17/0011)	default
Switch	192.168.1.2/32	3750x(16/0010)	default

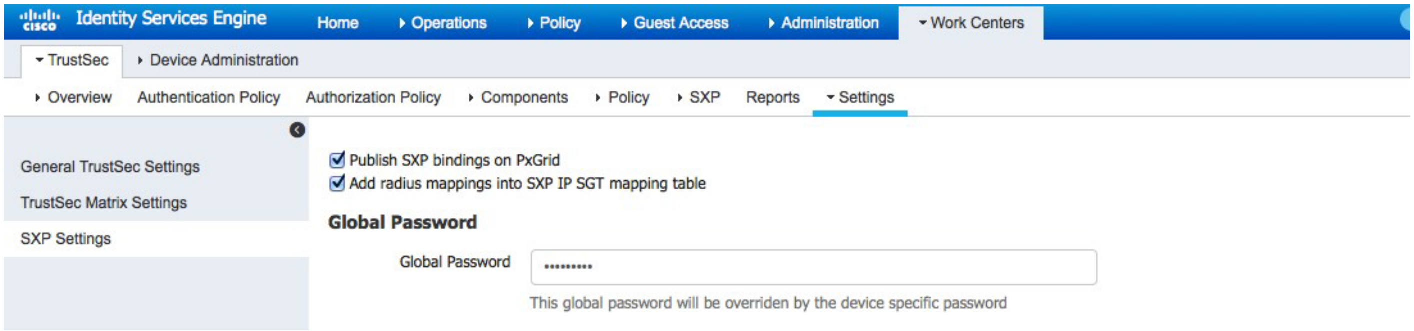
在 pxGrid 上发布 SXP 绑定

在 pxGrid 上发布 SXP 映射，以使用 SXP 脚本检索 TrustSec 会话信息。

第 1 步　选择工作中心 (Work Centers)->TrustSec->设置 (Settings)->启用“在 pxGrid 上发布 SXP 绑定” (Publish SXP bindings on pxGrid)

第 2 步　启用 (Enable)->将 radius 映射添加到 SXP IP SGT 映射表 (Add radius mappings into SXP IP SGT mapping table)

第 3 步　输入全局密码



☑ Publish SXP bindings on PxGrid
☑ Add radius mappings into SXP IP SGT mapping table

Global Password

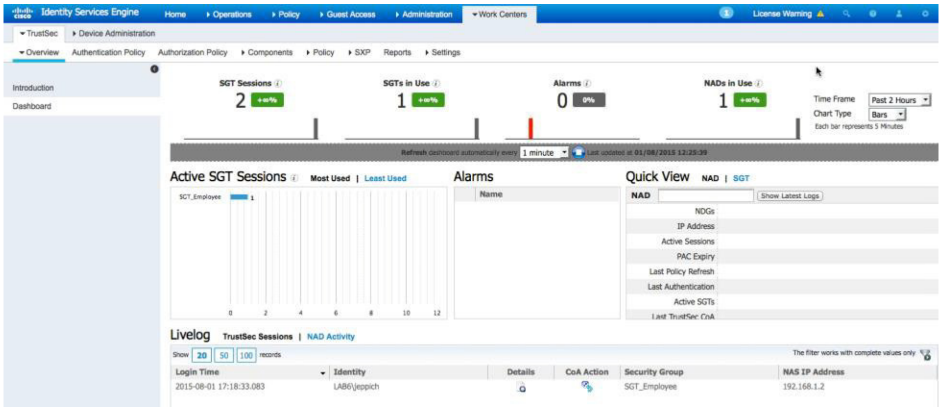
Global Password: ••••••••••

This global password will be overriden by the device specific password

TrustSec 控制面板

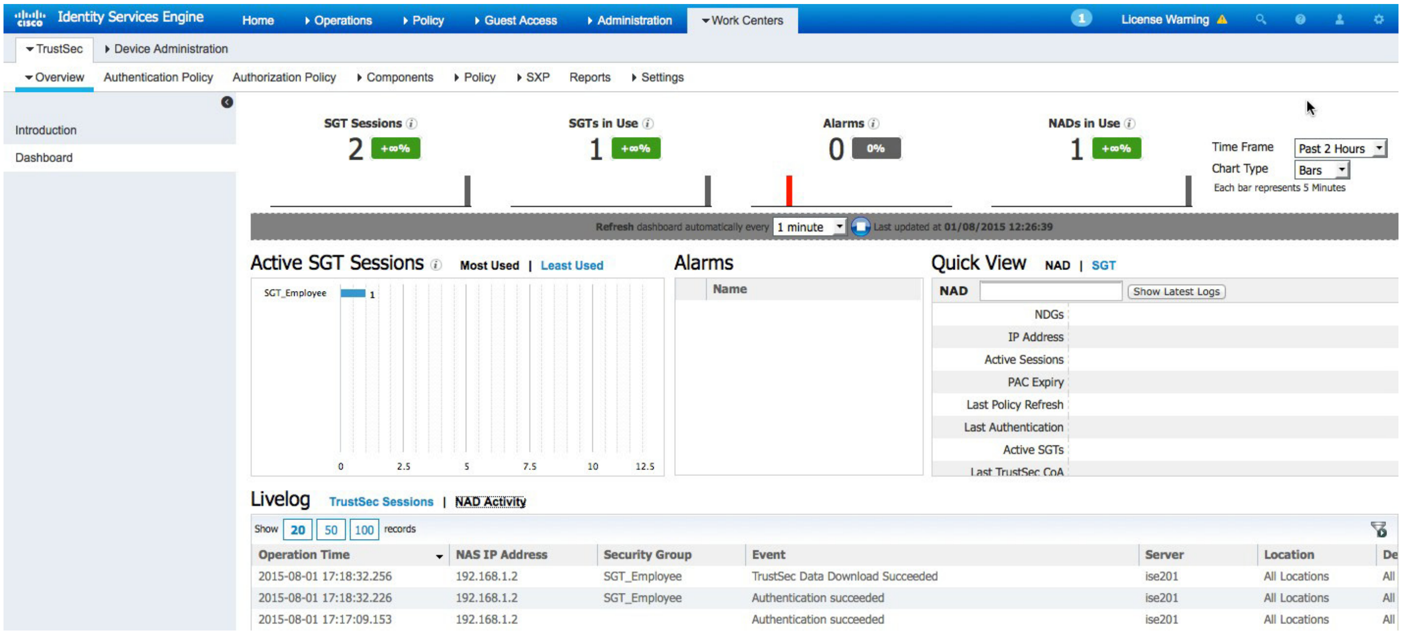
查看 TrustSec 活动，例如活动的 SGT 会话和 NAD 活动。

第 1 步　选择工作中心 (Work Centers)->TrustSec->控制面板 (Dashboard)



Login Time	Identity	Details	CoA Action	Security Group	NAS IP Address
2015-08-01 17:18:33.083	LAB6\jeppich			SGT_Employee	192.168.1.2

第 2 步　　选择 NAD 活动



Time Frame: Past 2 Hours
Chart Type: Bars
Each bar represents 5 Minutes

Refresh dashboard automatically every 1 minute　Last updated at 01/08/2015 12:26:39

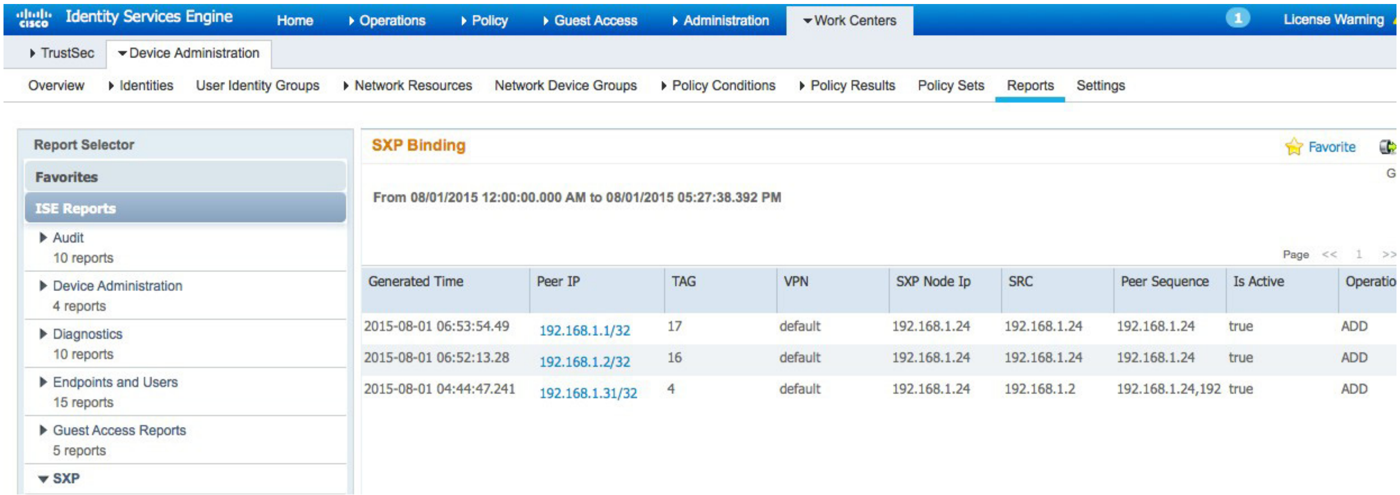
Show 20 50 100 records

Operation Time	NAS IP Address	Security Group	Event	Server	Location	De
2015-08-01 17:18:32.256	192.168.1.2	SGT_Employee	TrustSec Data Download Succeeded	ise201	All Locations	All
2015-08-01 17:18:32.226	192.168.1.2	SGT_Employee	Authentication succeeded	ise201	All Locations	All
2015-08-01 17:17:09.153	192.168.1.2		Authentication succeeded	ise201	All Locations	All

SXP 绑定报告

SXP 报告绑定和连接类型共有两种。

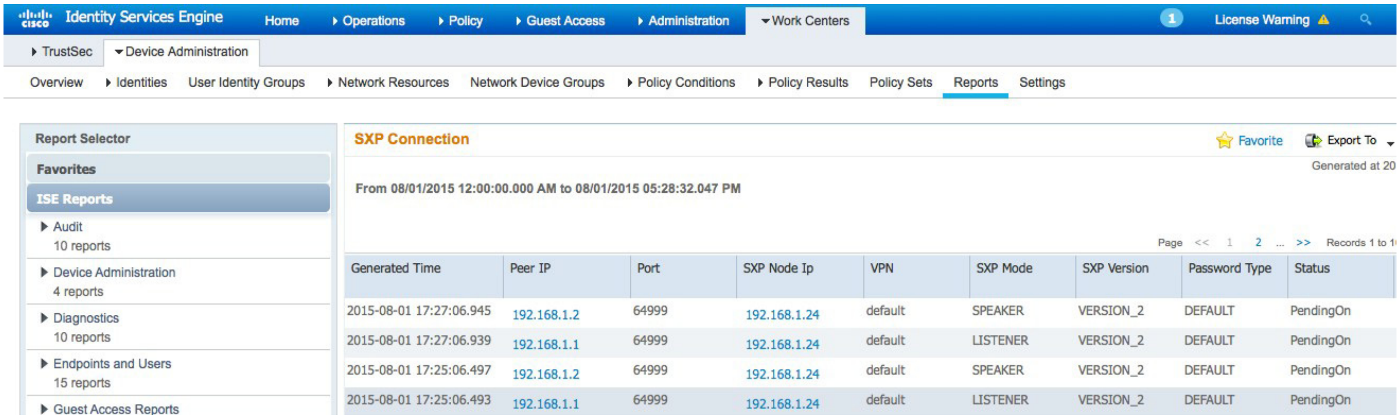
第 1 步　　选择工作中心 (Work Centers)->设备管理 (Device Administration)->报告 (Reports)->SXP->SXP 绑定 (SXP Binding)



From 08/01/2015 12:00:00.000 AM to 08/01/2015 05:27:38.392 PM

Generated Time	Peer IP	TAG	VPN	SXP Node Ip	SRC	Peer Sequence	Is Active	Operatio
2015-08-01 06:53:54.49	192.168.1.1/32	17	default	192.168.1.24	192.168.1.24	192.168.1.24	true	ADD
2015-08-01 06:52:13.28	192.168.1.2/32	16	default	192.168.1.24	192.168.1.24	192.168.1.24	true	ADD
2015-08-01 04:44:47.241	192.168.1.31/32	4	default	192.168.1.24	192.168.1.2	192.168.1.24,192	true	ADD

第 2 步　　选择工作中心 (Work Centers)->设备管理 (Device Administration)->报告 (Reports)->SXP->SXP 连接 (SXP Connection)



SXP Connection

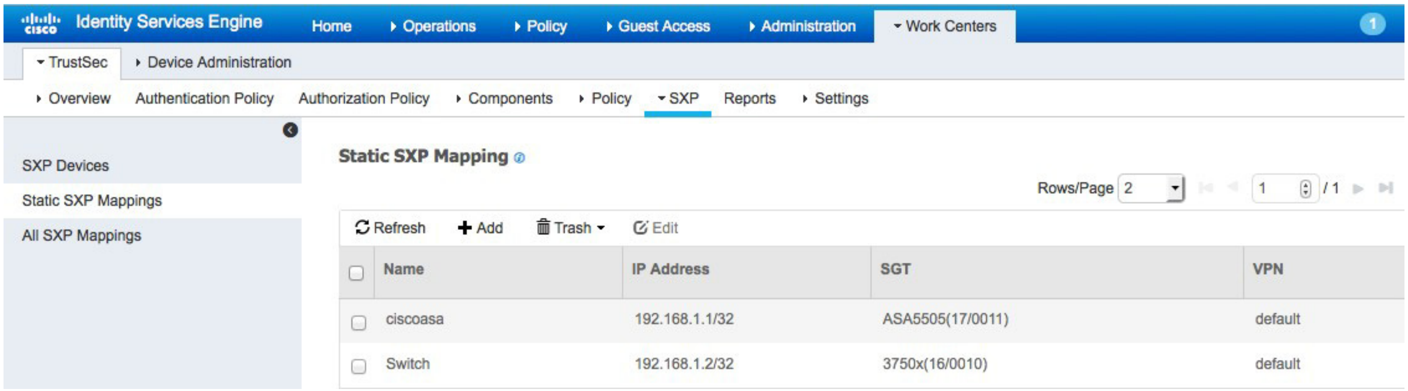
From 08/01/2015 12:00:00.000 AM to 08/01/2015 05:28:32.047 PM

Generated Time	Peer IP	Port	SXP Node Ip	VPN	SXP Mode	SXP Version	Password Type	Status
2015-08-01 17:27:06.945	192.168.1.2	64999	192.168.1.24	default	SPEAKER	VERSION_2	DEFAULT	PendingOn
2015-08-01 17:27:06.939	192.168.1.1	64999	192.168.1.24	default	LISTENER	VERSION_2	DEFAULT	PendingOn
2015-08-01 17:25:06.497	192.168.1.2	64999	192.168.1.24	default	SPEAKER	VERSION_2	DEFAULT	PendingOn
2015-08-01 17:25:06.493	192.168.1.1	64999	192.168.1.24	default	LISTENER	VERSION_2	DEFAULT	PendingOn

sxp_download 和 sxp_subscribe 脚本

下载 sxp 绑定信息。

第 1 步　选择工作中心 (Work Centers)->TrustSec->SXP->静态 SXP 映射 (Static SXP Mappings)，然后添加网络设备以触发 SXP 脚本



Static SXP Mapping

□	Name	IP Address	SGT	VPN
□	ciscoasa	192.168.1.1/32	ASA5505(17/0011)	default
□	Switch	192.168.1.2/32	3750x(16/0010)	default

第 2 步　运行 sxp_download 脚本和 sxp_subscribe 脚本

```
Johns-MacBook-Pro:bin jeppich$ ./sxp_download.sh -a 192.168.1.23 -u mac -k alpha.jks -p cisco123 -t
alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
12:42:02.433 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
12:42:03.677 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
SXPBinding={ipPrefix=192.168.1.1/32 tag=17 source=192.168.1.24 peerSequence=192.168.1.24}
SXPBinding={ipPrefix=192.168.1.2/32 tag=16 source=192.168.1.24 peerSequence=192.168.1.24}
Binding count=2
```

```
Connection closed
12:42:05.062 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Stopped
Johns-MacBook-Pro:bin jeppich$


Johns-MacBook-Pro:bin jeppich$ ./sxp_subscribe.sh -a 192.168.1.23 -u mac -k alpha.jks -p cisco123 -t
alpha_root.jks -q cisco123
------- properties -------
  version=1.0.2-30-SNAPSHOT
  hostnames=192.168.1.23
  username=mac
  group=Session
  description=null
  keystoreFilename=alpha.jks
  keystorePassword=cisco123
  truststoreFilename=alpha_root.jks
  truststorePassword=cisco123
--------------------------
12:43:00.420 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
Connected
12:43:01.646 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
press <enter> to disconnect...Binding deleted: SXPBinding={ipPrefix=192.168.1.1/32 tag=17 source=192.168.1.24
peerSequence=192.168.1.24}
Binding added: SXPBinding={ipPrefix=192.168.1.1/32 tag=17 source=192.168.1.24 peerSequence=192.168.1.24}
Binding deleted: SXPBinding={ipPrefix=192.168.1.2/32 tag=16 source=192.168.1.24 peerSequence=192.168.1.24}
Binding added: SXPBinding={ipPrefix=192.168.1.2/32 tag=16 source=192.168.1.24 peerSequence=192.168.1.24}
```

故障排除

涵盖一些基本故障排除程序。

19:37:39.475 [main] WARN o.a.cxf.phase.PhaseInterceptorChain - Interceptor for {https://ise238.lab6.com:8910/pxgrid/mnt/sd}WebClient has thrown exception, unwinding now

Ensure that pxGrid client(s) and windows 7 clients are DNS resolvable

```
19:37:39.475 [main] WARN o.a.cxf.phase.PhaseInterceptorChain - Interceptor for {https://ise238.lab6.com:8910/pxgrid/mnt/sd}WebClient has thrown exception, unwinding now

org.apache.cxf.interceptor.Fault: Could not send Message.

        at org.apache.cxf.interceptor.MessageSenderInterceptor$MessageSenderEndingInterceptor.handleMessage(MessageSenderInterceptor.java:64) ~[cxf-api-2.7.3.jar:2.7.3]
```

参考资料

TrustSec 设备配置

TrustSec 设备配置

ASA-5505 的设备配置

第 1 步　在 ASA 上配置 RADIUS

```
conf t
aaa-server ise1 protocol radius
aaa-server ise1 host 192.168.1.23 {shared secret}
```

第 1 步　创建服务器组

```
conf t
aaa-server ciscoasa protocol radius
aaa-server ciscoasa(inside) host 192.168.1.23
key Richard08
exit
cts server-group ciscoasa
```

第 2 步　从网络配置导入 OOB PAC 文件

```
conf t
cts import-pac ftp://jeppich:Richard08192.168.1.13/ciscoasa.pac password Richard08 {shared secret}
```

第 3 步　将 ASA 配置为 SPX 监听程序

```
conf t
cts sxp enable
cts sxp default password Richard08 {password should match other SXP devices}
cts sxp default source-ip 192.168.1.1 {ASA internal IP address}
cts sxp connection peer 192.168.1.2 {switch IP address} password default mode local listener
cts sxp default sxp connection peer 192.168.1.37 {bayshore} password default mode local listener
```

第 4 步　检查 ASA 是否在接收 SGT 映射，类型：

```
conf t
sh cts sxp sgt-map ipv4 detail
```

3750x 的设备配置

第 1 步　　配置 RADIUS 的交换机

```
conf t
aaa authorization network ise1 group radius
cts authorization list ise1
ip device tracking
radius-server host 192.168.23 pac key Richard08
```

第 2 步　　配置 CTS 的交换机

```
cts sxp enable
cts sxp default source-ip 192.168.1.2 {ip address of switch}
cts sxp default password Richard08 {shared secret}
cts sxp connection peer 192.168.1.1 (ip address of ASA) password default mode local
```