



# 使用 Cisco pxGrid 部署 Lancope StealthWatch



## 目录

关于本文档	
简介	4
组合使用 CA 签名证书与 SMC	5
上传 CA 根证书	5
创建 CA 签名的 SMC 证书	6
上传 CA 签名的 SMC 客户端证书	7
SMC Java 客户端	
获取主机 Java 库以信任 CA 证书	8
配置 ANC pxGrid 缓解功能	9
, 将自签名证书用于 SMC 和 ISE pxGrid 节点	
将 ISE 身份证书导入到受信任的系统证书库	
启用 pxGrid	
将 ISE 身份证书导出到 SMC 中	
为 SMC 创建自签名证书	
将自签名证书上传到 SMC	
将 SMC 自签名证书上传到 ISE 受信任的系统证书库	
启用自适应网络控制 (ANC)	
参考资料	
附录	
在 MAC 上启用 SSH	
故障排除	
SMC ANC 缓解错误消息:隔离请求未能发送到 ISE	
在 ISE pxGrid 节点中没有与 pxGrid 的连接	

## 关于本文档

本文档面向使用思科平台交换网格 (pxGrid) 部署 Lancope Stealthwatch 的思科现场工程师、技术营销工程师、 合作伙伴和客户。

Lancope Stealthwatch 6.6.1 或更高版本和思科身份服务引擎 (ISE) 1.3 或更高版本都是必需的。

本文档假定已安装 Stealthwatch 和 ISE 并将详述以下内容:

- 为用于 pxGrid 操作的证书颁发机构 (CA) 签名证书和自签名证书配置 Stealthwatch 管理控制台 (SMC)。
- Cisco(自适应网络控制)ANC pxGrid 缓解操作配置。
- 在 ISE 独立环境中使用自签名证书的 ISE pxGrid 节点和 SMC pxGrid 客户端配置的分步示例。

如果使用 CA 签名证书在生产环境中部署 pxGrid,请参阅:"在 ISE 分布式环境中配置 pxGrid": <u>http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html</u>

## 简介

Lancope 的 Stealthwatch 是一种网络安全解决方案,可实时掌握有关异常行为检测、APT、内部威胁、DDOS 和其他恶意软件的网络与用户流量的情况。Lancope 还会在事件请求对这些终端实时执行缓解操作前、中、后,收集和分析整体网络跟踪记录并对这些威胁作出响应。

思科平台交换网格 (pxGrid) 是支持生态系统合作伙伴从思科的身份服务引擎 (ISE) 获取用户和设备情景信息的 统一框架。ISE 将发布相关的信息主题,生态系统合作伙伴也会订用这些发布的主题,从而获取 ISE 会话信息 以及对终端执行自适应网络控制 (ANC) 缓解操作。ANC 以前称为 EPS "终端保护服务"。

Lancope Stealthwatch 将作为客户端注册到 ISE pxGrid 节点,还将订用终端保护服务功能并对终端执行 ANC 缓解操作。这些缓解操作包括隔离/取消隔离,以及由 ISE 执行的 IEEE 802.1X 终端身份验证。

本文档假设已安装 Stealthwatch 6.6 或更高版本,以及 ISE 1.3 或更高版本。

作为 pxGrid 客户端, Stealthwatch 需要用于 pxGrid 操作的证书颁发机构 (CA) 签名证书或自签名证书。本文档 包括两种证书的使用案例。

- 签名证书使用案例包括导入 CA 受信任的根证书,以及在由同一 CA (ISE pxGrid 节点证书由该 CA 签 名)签名的 SMC 上生成公钥/私钥对。假设已在 ISE 受信任的系统证书库中安装 CA 根证书,并且已 在 ISE 系统证书库中安装 pxGrid ISE 节点证书。
- 自签名证书分步完成完整的 ISE pxGrid 配置和自签名公钥/私钥 SMC 创建过程。ISE 以独立配置进行 部署。

两个使用案例均包括 SMC 缓解操作配置和示例。



## 组合使用 CA 签名证书与 SMC

### 上传 CA 根证书

此处导入的是受信任的 CA 根证书,此根证书也位于 ISE 受信任的系统证书库中。

**步骤1.** Admin User -> Administer Appliance -> Configuration -> Certificate Authority -> Browse, 然后上传 CA 根证书 -> Add。

ST	WATCH'	Ste	althWatch Management Console VE								
•	Admin User		Certifica	te Authority Cer	tific	ates					
ñ	Home										
se.	Configuration	۲	Number of	f Records: 2							
•	Manage Users	۲	Name 🖨	Expiration Date	¢	Issued To	¢	Issued By	¢	Delete 🔶	
=	Support Audit Log		id-1000	2011-04-04 11:51:02		Lancope		Lancope		0	
03	Operations	•	lancope	2035-01-01 05:10:10		Lancope		Lancope		0	
•	Logout										
0	Help		Delete								
		G	Calast COL	aadifaata ta add							
			Browse	root.cer							
			Name:	_							
			Add Certific	cate							

#### 步骤 2. 您将看到以下内容:

S	WATCH'	Ste	ealthWatch Management Console VE									
٠	Admin User		Certifica	te Authority	Certificates							
*	Home		N.	Number of Records: 3								
₽¢.	Configuration	Ð	Number of									
-	Manage Users	æ										
all a	Support	Ð	Name 🔶	Expiration Date 🔶	Issued To	\$	Issued By	\$	Delete	¢		
=	Audit Log		id-1000	2011-04-04 11:51:02	Lancope		Lancope					
¢,	Operations	Ð	ms_ca_root	2020-03-17 13:39:09	lab6-WIN- OCTAJ4DPT75-CA		lab6-WIN- OCTAJ4DPT75-CA					
•	Logout		lancope	2035-01-01	Lancope		Lancope					
0	Help			05:10:10								
		G										
			Delete									

### 创建 CA 签名的 SMC 证书

此处生成的是 SMC 私钥,即由 CA 机构签名的证书签名请求 (CSR)。用于 pxGrid 的 CA 模板必须同时包含对 pxGrid 操作有效的客户端身份验证和服务器身份验证的 EKU。

**步骤 1.** 在 SMC 上创建私钥。

openssl genrsa -out smc.key 4096 Generating RSA private key, 4096 bit long modulus

e is 65537 (0x10001)

步骤 2. 创建要由 CA 服务器签名的 SMC CSR 请求。

openssl req -new -key smc.key -out smc.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 []: An optional company name []:

**步骤 3.** 获取对 SMC 的根访问权限,使用 SCP 将 SMC.CSR 和 SMC.key 文件复制到安全的 PC。此 PC 用于 将 SMC.CSR 复制/粘贴到 pxGrid 自定义模板的高级用户请求中。

步骤 4. 下载 base-64 编码格式的证书。

### 上传 CA 签名的 SMC 客户端证书

此处为 pxGrid 操作上传的是 CA 签名的 SMC 客户端证书。

**步骤 1.** Admin User -> Configuration -> SSL Certificates 并将 smc.cer 和 smc.key 均上传到 SMC。

STEALTH WATCH	StealthWatch Management Console VE		
🛔 Admin User	SSL Certificate		
<ul> <li>A Home</li> <li>✓ Configuration</li> <li>▲ Manage Users</li> <li>✓ Support</li> <li>⇒ Audit Log</li> <li>Ø<sup>2</sup> Operations</li> </ul>	<ul> <li>Warning Please read and follow instruction: button:         <ul> <li>Provide a target certificate supplied by an obx.</li> <li>Provide a CA certificate chain into the seconds in the seconds of the second second</li></ul></li></ul>	s before pushing the "Upload Certificate" ifficial certification authority(CA) into the first nd box. Typically user certificate (trust target) signed by an intermediary whose certificate is a chain: user certificate, intermediary sitel is optional because in case of a a third box	
🕞 Logout		Confirmation	×
🕑 Help		The certificate was added successfully.	
	Cartificate Cartificate File(PEM-encoded):  Browse No file selected. Certificate Chain(PEM-encoded)(Optional): Browse No file selected. Private Key(Not Encrypted)(PEM-encoded): Browse No file selected. Upload Certificate		ОК



۱. ۱

## SMC Java 客户端

### 获取主机 Java 库以信任 CA 证书

注: 如果 CA 没有标准公共 CA(因为它是根),则必须将主机 Java 库配置为信任 CA 根证书,以便打开 Java 客户端。

**步骤1.** 打开已启用 Java 控制台的 SMC Java 客户端。

步骤 2. 在 Java 控制台中,查找 TrustStoreHelper 的路径。

6 INF0 [SimpleSMCClient] https://172.25.73.134/smc-client/app
8 INF0 [XMLBindings] jar:https://172.25.73.134/smc-client/app/lc-core.jar!/xml/bindings.xml
5 INF0 [XMLBindings] jar:https://172.25.73.134/smc-client/app/sw-manager-client.jar!/com/lancope/sws/smcClient/bindings.xml

5 INFO [XMLBIndings] jar:https://172.25.73.134/smc-client/app/sw-manager-client.jar!/com/lancope/sws/smcClient/bindings.xml 7 INFO [THUSISTORENEEPE] System CA Frust Store not found, of could not be opened with given possword at:/Library/internet rtug-ins/JavaAppletrug 3 INFO [TrustStoreHelper] System CA trust store loaded from:/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/security/cacerts

TNED [IRMProve/Tousset] of a second bic/open/im/Service/getBannerMessage MADN [IsunchWorkTtam] Attamntad login with secsion id failed: promotion for username and nassword

**步骤 3.** 在主机上,将 CA 根证书导入到上一步中识别的 cacerts 文件中。大多数 cacerts 文件的默认密码为 "changeit"。

keytool -keystore cacerts -importcert -alias myca -file myfile

where: myfile represents the CA root certificate (i.e. root.cer)

**步骤 4.** 启动 SMC Java 客户端。



## 配置 ANC pxGrid 缓解功能

通过 pxGrid ANC 缓解功能,SMC 可以作为 pxGrid 客户端注册到 ISE pxGrid 节点,并订用对经过 ISE 身份验 证的终端调用隔离/取消隔离缓解操作的终端保护服务功能。

- **步骤1.** 添加缓解功能。
- **步骤 2.** Tools -> Settings -> Cisco ISE Configuration 并启用 Cisco ISE Mitigation, 输入 ISE pxGrid Node 和 IP 地址。

Cisco ISE Mitigation 0	
Mitigation Nodes: 😧	
Primary PAN Node Name:	Primary PAN Node IP Address:
ise1.lab6.com	10.0.0.13
Secondary PAN Node Name (Optional):	Secondary PAN Node IP Address
ex. PAN Node 02	ex. 10.10.10.21

#### 步骤3. 连接应该会成功。

,S⊤	WATCH'				🖋 Launch SMC	
4 ه	Admin User ~		Success			
æ			The Cisco ISE cor	nnection was successful.		
*	Network					
2					Ok	
⇒				Cluster Name:		
عر	Tools			ise1.lab6.com		
	Sottingo			SMC Local Port:		
	Active Directory			3514		
				User Name:	Password:	
	Configuration			SITC		
				Deployment Nodes: 0		
				Primary Node Name:	Primary Node IP Address:	• •
				ise mado.com	10.0.0.13	
	Job Management			Add Cisco ISE Mitigation		
					Ø Dele	te 🕼 Edit



#### **步骤 4.** 您将看到 SMC 注册为 pxGrid 客户端,客户端组从 Session 更改为 EPS。 Administration -> pxGrid Services。

ahah									License Warning 🔒   ise	e1   admin	I Logout	Feedback	Q		
cisco Identity Service	s Engine		۵	Home Oper	ations 🛛 🔻	Policy   •	Guest Access	Administration	1 V					Se	etup Assistant 🔻
🐝 System 🛛 💆 Identity	Management	Network	Resources	🛃 Device F	Portal Manag	ement	🛃 pxGrid Services	Feed S	ervice 🙎 📲 pxGrid Id	lentity Mappi	ng				
Clients Live Log											Θ	Enable Auto-I	Registration	Disable Vie	Auto-Registratic w By Capabilitie
🖌 Enable 🕜 Disable 😪 Ap	prove 😝 Group	Pecline	🚷 Delete 👻	🛞 Refresh	Total Pendi	ing Approval(0	)) -			1 - 3 o	f 3 Sho	w 25 👻 pe	r page P	age 1	\$ of 1
Client Name	Clien	t Description		Capabilities	5		Status		Client Group		Log				
ise-admin-ise1				Capabilities	s(2 Pub, 1 Su	ub)	Online		Administrator		View				
ise-mnt-ise1				Capabilities	s(2 Pub, 0 Su	ub)	Online		Administrator		View				
smc				Capabilities	s(0 Pub, 0 Su	ub)	Offline		EPS		View				

#### 步骤 5. 选择要隔离的主机,然后选择 Quarantine。

STEALTH WATCH							🖋 Launch SM	ИC
<ul> <li>Admin User ∨</li> <li> <i>B</i> Dashboard     </li> </ul>	B Host R	eport for 10	0.0.0.17					
A Network	Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Da
≓ Flows	● 0	0	0	0	0	0	0	
	Host Summary View Flows Status: Host Groups: Location: Last Seen: Policies: MAC Address Quarantine	Host IP 10.0.0 Classify Inactive  Catch All RFC 1918   : 00:0c:29:7	.17 History 7:d6:85 (VMware,	/	Traffic by Peer Ho	st Group		2

#### 步骤 6. 您应该看到主机已成功隔离。

ahah			License Warning 🛕   ise1   admin   Logout	Feedback D
cisco Identity Services Engine	Home Operations	Policy V Guest Access V Administ	ration 🔽	
Authentications Reports	Endpoint Protection Service 💦 Troubleshoot			
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Re
0	0	0	0	
🔝 Show Live Sessions 🛛 🎡 Add or Remove Co	olumns 🔻 🛞 Refresh 🛛 💿 Reset Repeat Counts		Refresh Every 1 minute  T Show Late	est 20 records *
Time	Repeat Count Identity  Endpoint ID	Endpoint Profile  Authentication Policy	Authorization Policy (1) Authorization Profiles (1)	Network Device
2015-05-02 18:31:51.258 🕕 🗋	0 00:0C:29:77:D6:8 00:0C:29:77:D6:85	Win8		
2015-05-02 18:31:50.607	#ACSACL#-IP-PEI		s	w
2015-05-02 18:31:50.592 🕕 🔓	0 jskiber jskiber-10.0.0.17			
2015-05-02 18:31:50.592 🔽 🔽	jskiber@lab6.com 00:0C:29:77:D6:85	Default >> Dot1X >> D	Default >> Quarantine Quarantined s	w

**步骤 7.** 选择 Administration -> pxGrid Services -> Live Log。

ahaha 🔒							License Warning
cisco Ide	entity Servi	ces Engine	🟦 Home	Operations V	Policy V Gue	st Access 🛛 🔻 🛛 Administratio	on 💌
🔆 System	🚰 Ider	ntity Management 🛛 🔛 Networ	k Resources	Device Portal Mana	igement 🛛 🗔 px	Grid Services 🛛 🗔 Feed S	Service 🔒
Clients	Live Log	🏀 Refresh					
Client Name		Capability Name	Event Typ	e	Timestamp	Other	Attributes
smc@xgrid.cise	co.com		Client off	ne	6:40:04 PM E	ST, May 2 2015	
smc@xgrid.cise	co.com	EndpointProtectionService	Capabil Client uns	ubscribed	6:40:04 PM E	ST, May 2 2015	
smc@xgrid.cise	co.com	EndpointProtectionService	Capabil Client sub	scribed	6:40:04 PM E	ST, May 2 2015	
smc@xgrid.cise	co.com		Client onl	ne	6:40:03 PM E	ST, May 2 2015	

步骤8. 终端被视为非恶意终端后,即可对其取消隔离。



步骤 9. Operations -> Authentications,您应该看到终端已处于取消隔离状态。

ahah			License Warning 🔥   ise1   admin   Logout
cisco Identity Services Engine	Home Operations	Policy V Guest Access V Adminis	tration 🛛 🔻
Authentications	Endpoint Protection Service 💦 Troubleshoot		
Misconfigured Supplicants	Misconfigured Network Devices $(i)$	RADIUS Drops	Client Stopped Responding
0	0	0	0
🔝 Show Live Sessions 🛛 🎡 Add or Remove Co	olumns 🔻 🛞 Refresh 🛛 😳 Reset Repeat Counts		Refresh Every 1 minute  T Show
Time	Repeat Count Identity () Endpoint ID ()	Endpoint Profile () Authentication Policy ()	Authorization Policy () Authorization Profiles ()
2015-05-02 18:40:12.099 👔	0 00:0C:29:77:D6:8 00:0C:29:77:D6:85	Win8	
2015-05-02 18:40:12.090 🕕 🔓	0 jskiber jskiber-10.0.0.17		
2015-05-02 18:40:12.090	iskiber@lab6.com_00:0C:29:77:D6:85	Default >> Dot1X >> D.	Default >> 8021X Acc PermitAccess

## 将自签名证书用于 SMC 和 ISE pxGrid 节点

本节介绍如何对 Stealthwatch SMC 和 ISE pxGrid 节点使用自签名证书。自签名证书主要用于测试 PoC (概念 验证)。ISE pxGrid 节点部署在独立环境中。请注意,在 ISE 生产部署中,pxGrid 将具有其自己的角色,或存在于其自己的节点上。

### 将 ISE 身份证书导入到受信任的系统证书库

ISE 身份证书需要受信任,公共证书需要导出到 ISE 受信任的系统证书库中。

<u>注</u>:在 ISE 1.4 中可能不必执行此步骤; ISE 身份证书可能已经受信任。

**步骤 1.** Administration -> System -> Certificates -> System Certificates -> 选择 ISE 身份证书并导出。

رازیران cisco Identity Services Engine	Alama	Operations V Policy	Y Guart Arrange	License V	/arning 🚖   ise14   admin	Logout   Feedback					
	1 nome	Operations - Policy	Guest Access (	Authinistration			Setup Assistant *				
System 🎽 Identity Management	Network Resources	Device Portal Management	pxGrid Services	Feed Service	💵 pxGrid Identity Mappin	g					
Deployment Licensing Certificates	Logging Maintenance	Backup & Restore	Admin Access Sett	ings							
Certificate Management	Certificate Management System Certificates 🛆 For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.										
Overview	📝 Edit 🕂 Generate Self Si	gned Certificate	rt 💽 Export 🔀 De	elete 🔎 View							
	Friendly Name	Used By Portal	group tag Iss	ued To	Issued By	Valid From	Expiration Date				
System Certificates	▼ ise14										
Endpoint Certificates	Default self-signed server of ertificate	EAP Authentication, Defaul Admin, Portal, Group pxGrid	t Portal Certificate ise1	14.lab6.com	ise14.lab6.com	Sun, 3 May 2015	Mon, 2 May 2016 🛛 🗹				

<u>注</u>: 仅导出公共证书,您可以更改默认证书名称。在这些示例中,证书名称更改为 ise14.pem

**步骤 2.** Administration -> System -> Certificates -> Trusted Certificates -> Import -> 证书文件 -> 启用 Trust for authentication within ISE -> Submit。

սիսի	License Warning 🔥   ise14
cisco Identity Services Engine	Administration ▼ Policy ▼ Guest Access ▼ Administration ▼
🛛 🔅 System 🦉 Identity Management	🞬 Network Resources 🛛 🛃 Device Portal Management 🕞 pxGrid Services 🖓 Feed Service 💵 pxGrid Identity
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	Import a new Certificate into the Certificate Store
Overview	* Certificate File Browse ise14.pem
System Certificates	Trusted For: (i)
Endpoint Certificates	Trust for authentication within ISE
Trusted Certificates	<ul> <li>Trust for client authentication and Syslog</li> <li>Trust for authentication of Cisco Services</li> </ul>
OCSP Client Profile	Validate Certificate Extensions
Certificate Signing Requests	Description

### 启用 pxGrid

启用 pxGrid 角色,在 ISE 中应会启动 pxGrid 服务。不必要再将自签名 ISE 身份证书复制到 ISE 中。

**步骤 3.** 在 Administration -> System -> Deployment -> Save 下启用 pxGrid。

	ahah									License V	Varning 🚹   ise14   admin
¢	cisco Identit	y Services E	Engine		🟠 Home	e Operations	Policy   🔻	Guest Acces	ss 🛛 🔻	Administration   •	
1	🔆 System	🚰 Identity M	anagement	Network R	lesources	Device Portal Mana	gement	😡 pxGrid Se	rvices	Feed Service	2 pxGrid Identity Mapping
	Deployment	Licensing	Certificates	Logging	Maintenance	Backup & Res	tore A	dmin Access	Setti	ngs	
	Deployment			Deploymer	nt Nodes List > ise1	.4					
	@ •   E •		<b>₩</b> +	Edit No Gener	de ral Settings	Profiling Configuration	n				
	September 2     September	r		Person ✓ Adrr ✓ Mon ✓ Polie	Hostna FQ IP Addr Node Ty as ninistration nitoring cy Service V Enable Sessio Incl V Enable Profilir td (i)	me ise14 IDN ise14.lab6.com ess 10.0.0.58 ype Identity Servic in Services (i) lude Node in Node G ng Service	es Engine (1 Role STAND/ Role PRIMA	ISE) ALONE M ARY *	lake Prim Oth	ary er Monitoring Node	

#### **步骤 4.** 验证 pxGrid 服务是否已启用。Administration -> pxGrid Services。

<u>注</u>:这可能需要一分钟时间,请验证 pxGrid 服务是否正在初始化,在 ISE pxGrid 节点上运行"application status ise"。 如果服务仍然没有显示,请将 ISE 身份证书导出到 ISE 受信任的系统证书库中。

ultulu cisco Identity Services Engine	🟠 Home	Operations V Policy V	Guest Access 🗸 Administration	License Warning A   ise14   admin	Logout   Feedback
🐝 System 🛛 💆 Identity Management	Network Resources	Device Portal Management	🗊 pxGrid Services 🛛 🙀 Feed Se	ervice	ing
					Objective to be Described in
Clients Live Log					Disable Auto-Registration
Clients         Live Log           ✓ Enable         ⊘ Disable         ⊙ Approve         ⊕ Group	👎 Decline 🛛 🛞 Delete 👻 🍪 Ru	Refresh Total Pending Approval(0)	•	1 - 2 c	of 2 Show 25 + per page Pag
Clients     Live Log       ✓ Enable     ⊘ Disable     ⊘ Approve     ⊖ Group       □     Client Name     Clie	➡ Decline	Refresh Total Pending Approval(0) apabilities	▼ Status	1 - 2 c Client Group	of 2 Show 25 v per page Pag
Clients Live Log	Pecline      Q     Delete      Q     Rescription     Cap     Cap	Refresh Total Pending Approval(0) apabilities apabilities(3 Pub, 1 Sub)	• Status Online	1 - 2 c Client Group Administrator	Disable Auto-Registration     f 2 Show 25      per page Pag     Log     View



#### 步骤 5. 启用"Auto Registration"

սիսիս				License Warning 🛓   ise14	admin   Logout   Fi	eedback D
cisco Identity Services Engine	🏠 н	ome Operations V Policy V	Guest Access	Administration		Setup Assistant *
🐝 System 🛛 💆 Identity Management	Network Resources	🛃 Device Portal Management	pxGrid Services	S Feed Service ▲ pxGrid Ident	tity Mapping	
Clients Live Log					⊖Enab	le Auto-Registration Disable Auto-Registrati View By Capabiliti
🖌 Enable 🕜 Disable 📿 Approve 😝 Group	👎 Decline 🛛 🛞 Delete 👻	Sefresh Total Pending Approval(	0) 👻		1 - 2 of 2 Show 2	5 🔻 per page Page 1 🐥 of 1
Client Name Client	Description	Capabilities	Status	Client Group	Log	
□ ► ise-admin-ise14		Capabilities(3 Pub, 1 Sub)	Online	Administrator	View	
□ ► ise-mnt-ise14		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View	

### 将 ISE 身份证书导出到 SMC 中

**步骤 1.** 将 ISE 身份证书导入到 SMC 证书颁发机构库中。 Admin User -> Administer Appliance -> Configuration -> Certificate Authority -> 浏览并上传先前步骤 中的 ISE 身份证书 -> Add。

😭 Home							
🖋 Configuration	•		F				
💄 Manage Users	⊕ INU	mber of Record	15: 0				
🖋 Support	⊕ Nam	e 🕈	Expiration Date	¢	Issued To	Issued By	Delete 🕈
Audit Log	id-10	000	2011-04-04 11:51:02		Lancope	Lancope	
© Coperations	ise1	4_cert	2016-05-02 12:51:02		ise14.lab6.com	ise14.lab6.com	
😯 Help	ise_	14_identity_cert	2016-05-02 12:51:02		ise14.lab6.com	ise14.lab6.com	
	G ms_	ca_root	2020-03-17 13:39:09		lab6-WIN- OCTAJ4DPT75-CA	lab6-WIN- OCTAJ4DPT75-CA	
	lanc	ope	2035-01-01 05:10:10		Lancope	Lancope	
	Del	ətə					
	Pal	at CCL contificat	a ta add				
	Sel	ect SSL certificati	e to add				
	Br	owse No file	selected.				



#### 为 SMC 创建自签名证书

此处我们为 SMC(pxGrid 客户端)创建自签名证书。您需要在 SMC 上获取根访问权限。

注: 这些步骤记录在 SMC -> Help-Self-Signed Certificates 上

步骤1. 为 SMC 生成私钥,系统还将提示您输入要在后续步骤中使用的口令。

openssl genrsa -des3 -out smc1.key 2048

您将看到以下内容:

步骤 2. 生成自签名证书请求 (CSR)。

openssl req -new -key smcl.key -out smcl.csr

Note: All the field are required except for the challenge password [] and company name []

您将看到以下内容:

```
smc:~# openssl req -new -key smc1.key -out smc1.csr
Enter pass phrase for smcl.key:
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]:US
State or Province Name (full name) [Some-State]:Maryland
Locality Name (eg, city) []:Germantown
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lancope
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:smc.lab6.com
Email Address []:jdoe@lancope.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
smc:~#
```

#### 安全访问操作指南



#### **步骤 3.** 生成自签名证书。

openssl x509 -req -days 365 -in smcl.csr -signkey smcl.key -out smcl.crt

您将看到以下内容:

```
smc:~# openssl x509 -req -days 365 -in smc1.csr -signkey smc1.key -out smc1.crt
Signature ok
subject=/C=US/ST=Maryland/L=Germantown/O=Lancope/OU=Engineering/CN=smc.lab6.com/emailAddress=jdoe@lancope.com
Getting Private key
Enter pass phrase for smc1.key:
smc:~#
```

步骤4. 解密先前键入的密码。

cp smc1.key smc1.key.org openssl rsa -in smc1.key.org -out smc1.key

您将看到以下内容:

```
smc:~# cp smc1.key smc1.key.org
smc:~# openssl rsa -in smc1.key.org -out smc1.key
Enter pass phrase for smc1.key.org:
writing RSA key
smc:~#
```

步骤 5. 您应在 /root/smc 目录中具有以下内容。

smc:~# ls
smc1.crt smc1.csr smc1.key smc1.key.org
smc:~#

将以 Admin User 身份将 smc1.cert 和 smc1.key 上传到 SSL 证书下的 SMC 中。

**步骤 6.** 使用 SCP 在本地复制 smc1.crt 和 smc1.key 文件,如果在复制到本地 PC 时收到表明拒绝连接的消息,请参阅附录中的"在 MAC 上启用 SSH"以供参考。

### 将自签名证书上传到 SMC

此处我们将自签名证书的公共证书和私钥对上传到 SMC。

步骤 1. Admin User -> Configuration -> SSL Certificates 并上传 smc1.crt 和 smc1.key -> Upload Certificate。



步骤 2. 您应该看到证书已成功上传,并需要重新启动。

### 将 SMC 自签名证书上传到 ISE 受信任的系统证书库

此处我们将 SMC 自签名证书上传到 ISE 受信任的系统证书库。

**步骤1.** Administration -> System -> Certificates -> Trusted Certificates -> Import the SMC self-signed certificate。 启用"trust for authentication within ISE"并点击 Submit。

սիսի	License Warning 🛓   ise14   a
cisco Identity Services Engine	Administration ▼ Policy ▼ Guest Access ▼ Administration ▼
🔅 System 🦉 Identity Management	🔛 Network Resources 🛛 🛃 Device Portal Management 🖓 pxGrid Services 🖓 Feed Service 🕰 🖁 pxGrid Identity I
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	Import a new Certificate into the Certificate Store
Quantion	* Certificate File Browse smc1.crt
Overview	Friendly Name
System Certificates	Trusted For: ①
Endpoint Certificates	✓ Trust for authentication within ISE
	Trust for client authentication and Syslog
Trusted Certificates	Trust for authentication of Cisco Services
OCSP Client Profile	Validate Contificate Extensions
Certificate Signing Requests	Description
Certificate Authority	Submit Cancel

## 启用自适应网络控制 (ANC)

本节讨论在 ISE 1.4 上启用自适应网络控制 (ANC) 和配置授权策略。ANC 以前在 ISE 1.3 中称为终端保护服务 (EPS)。

**步骤1.** 要在 ISE 1.4 中启用 ANC,请点击 Administration -> System -> Settings -> Adaptive Network Control -> Enable->Save。

ahaha							Lice
cisco Ident	tity Services I	Engine		🟠 Home	Operations V	Policy 🔍 Guest Ac	cess 🔻 Administration 🔻
🔅 System	🚰 Identity M	lanagement	Network Re	esources 🛃	Device Portal Managen	nent 🛛 🗔 pxGrid S	Services 🛛 🖓 🖉 Servic
Deployment	Licensing	Certificates	Logging	Maintenance	Backup & Restore	Admin Access	Settings
Settings			Adaptiv	e Network Con	trol 🛈		
Client Pro	visioning						
📄 Adaptive I	Network Control						
FIPS Mod	e		Service S	tatus 🔽 Enabled	i -		
E Alarm Set	tings			_			
Posture							
Profiling			Save	Reset			
Protocols			Save	140000			

**步骤 2.** 要在 ISE 1.3 中启用 EPS,请点击 Administration -> System -> Settings -> 启用 Service Status,然后点击 Save。

ahaha									License	Warning
cisco Ident	tity Services I	Engine		🟠 Home	Operations 🔻	Policy   •	Guest A	ccess 🔻	Administration	
💀 System	Identity M	lanagement	Network R	esources 🛃	Device Portal Mana	igement	👦 pxGrid	Services	Reed Service	<u>.</u>
Deployment	Licensing	Certificates	Logging	Maintenance	Backup & Res	tore A	dmin Access	Set	tings	
Settings			Endpoi	nt Protection S	Service (i)					
E Client Pro	visioning									
Endpoint	Protection Service									
FIPS Mod	e		Service S	Status 🔽 Enable	ed 👻					
E Alarm Set	tings									
Posture										
Profiling			Save	Reset						
Protocols										
Proxy										
TrustSec S	Settings									
E SMTP Ser	ver									
📄 SMS Gate	way									
📄 System Ti	ime		-							
Policy Set	s									
ERS Settin	ngs									

**步骤 3.** Policy -> Police Elements -> Results -> Authorization -> Authorization Profiles -> Add -> Quarantine, 为 Name 输入 Quarantine -> Submit。

abab				License Warning 🛕   ise14
cisco Identity Services Engine	🟠 Home	Operations V Po	olicy 🔻 Guest Access 🖛	Administration
🚨 Authentication 🛛 👩 Authorization	Profiling 💽 Posture	😡 Client Provisionin	g 📑 TrustSec 💼	Rolicy Elements
Dictionaries Conditions Results			1	
Results	Authorization Profiles > New A Authorization Profile * Name Quara	Authorization Profile		
Authentication	Description			
Authorization	* Access Type ACCES	S_ACCEPT		
Authorization Profiles     Garage Blackhole_Wireless_Access	Service Template			
Cisco_IP_Phones     Cisco_IP_Phones     DenyAccess				



սիսի		Lice	ense Warning 🛕   ise14   admin   Logout   Feedback 🔎
cisco Identity Services Engine		olicy 🔍 Guest Access 🔍 Administration 🔍	
🕰 Authentication 🛛 👩 Authorization 🔗 Profiling	Posture 🔂 Client Provisionir	g 📄 TrustSec 🔒 Policy Elements	
Authorization Policy			h
Define the Authorization Policy by configuring rules based on identity	groups and/or other conditions. Drag and d	rop rules to change the order.	
For Policy Export go to Administration > System > Backup & Restore :	> Policy Export Page		
First Matched Rule Applies 🔹			
· Exceptions (1)			
		->	
Status kule name Con	altions (laentity groups and other condition	s) Permissions	
ANC if See	sion:EPSStatus EQUALS Quarantine	then Quarantine	

- 步骤 5. Rule Name: ANC。
- 步骤 6. New Condition Rule 添加新属性值: Session:EPStatus:Equals:Quarantine。
- 步骤 7. Permissions:Profiles:Standard:Quarantine。
- **步骤 8.** Click -> Done -> Save。

## 参考资料

其他 pxGrid 文档位于: <u>http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html</u>

- 使用 pxGrid 部署证书:使用自签名 pxGrid 客户端和自签名 ISE pxGrid 节点证书
- 使用 pxGrid 部署证书:证书颁发机构 (CA) 签名的 pxGrid 客户端和自签名 ISE pxGrid 节点证书
- 使用 pxGrid 部署证书:证书颁发机构 (CA) 签名的 pxGrid 客户端和 CA 签名的 ISE pxGrid 节点证书
- 配置并测试与 Cisco pxGrid 的集成

cisco.

## 附录

### 在 MAC 上启用 SSH

**步骤 1.** 在 MAC 上启用 SSH。

Johns-Macbook-Pro:Utilities jeppich\$ sudo launchctl load -w /System/Library/LaunchDaemons/ssh.plist Johns-Macbook-Pro:Utilities jeppich\$

步骤 2. 将文件从 SMC 复制到本地 PC。

Dddd smc:~# scp smc1.crt jeppich@10.0.0.5:/Applications/ise14\_certs/ Password: smc1.crt 100% 1330 1.3KB/s 00:00 smc:~# 1s jeppich@10.0.0.5 smc1.crt smc1.csr smc1.key smc1.key.org smc:~# scp smc1.key jeppich@10.0.0.5:/Applications/ise14\_certs/ Password: smc1.key 100% 1675 1.6KB/s 00:00 smc:~#

#### 故障排除

#### SMC ANC 缓解错误消息:隔离请求未能发送到 ISE

在 Administration -> pxGrid services 下,将 SMC 驻注册客户端分配到 ESP 组中。

#### 在 ISE pxGrid 节点中没有与 pxGrid 的连接

对于证书颁发机构 (CA) 签名证书,请确保您在 ISE 受信任的系统证书库中具有根 CA 证书,并在 ISE 系统证书库中具有 ISE pxGrid 节点证书。pxGrid 客户端证书必须同时具有客户端身份验证和服务器身份验证的 EKU。

对于 ISE 自签名证书,必须将自签名身份证书从系统证书库导出并导入到 ISE 受信任的系统证书库中。

有关详细信息,请参阅"在 ISE 分布式环境中配置 pxGrid"