使用Rapid7配置ISE 2.2以威脅為中心的NAC(TC-NAC)

目錄

簡介

本文檔介紹如何使用Identity Service Engine(ISE)2.2上的Rapid7配置以威脅為中心的NAC並對其進行故障排除。威脅中心網路訪問控制(TC-NAC)功能使您能夠根據從威脅和漏洞介面卡接收的威脅和漏洞屬性建立授權策略。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- 思科身分識別服務引擎
- Nexpose漏洞掃描器

採用元件

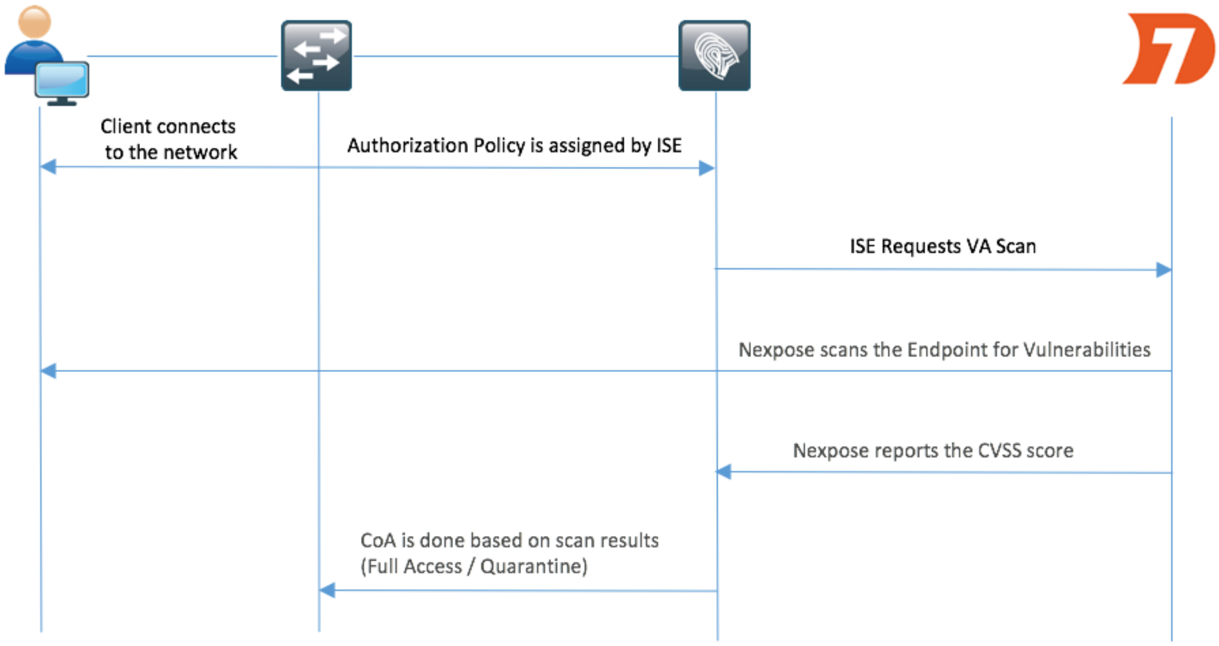
本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎版本2.2
- Cisco Catalyst 2960S交換器15.2(2a)E1
- Rapid7 Nexpose漏洞掃描器企業版
- Windows 7 Service Pack 1
- Windows Server 2012 R2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

高級流程圖


Client connects
to the network
Authorization Policy is assigned by ISE
ISE Requests VA Scan
Nexpose scans the Endpoint for Vulnerabilities
Nexpose reports the CVSS score
CoA is done based on scan results
(Full Access / Quarantine)

以下是流程：

1. 客戶端連線到網路，提供有限的訪問並分配啟用了**Assess Vulnerabilities**覈取方塊的配置檔案。
2. PSN節點向MNT節點傳送系統日誌消息，確認發生了身份驗證，並且VA掃描是授權策略的結果。
3. MNT節點使用以下資料向TC-NAC節點（使用管理WebApp）提交SCAN:
   -MAC 地址

-IP 位址
— 掃描間隔
— 定期掃描已啟用
— 始發PSN

4. Nexpose TC-NAC（封裝在Docker容器中）與Nexpose Scanner通訊以觸發掃描（如果需要）。

5. Nexpose Scanner掃描ISE請求的端點。

6. Nexpose Scanner將掃描結果傳送到ISE。

7. 掃描結果將傳送回TC-NAC:
-MAC 地址
— 所有CVSS分數
— 所有漏洞（標題、CVEID）

8. TC-NAC使用步驟7中的所有資料更新PAN。

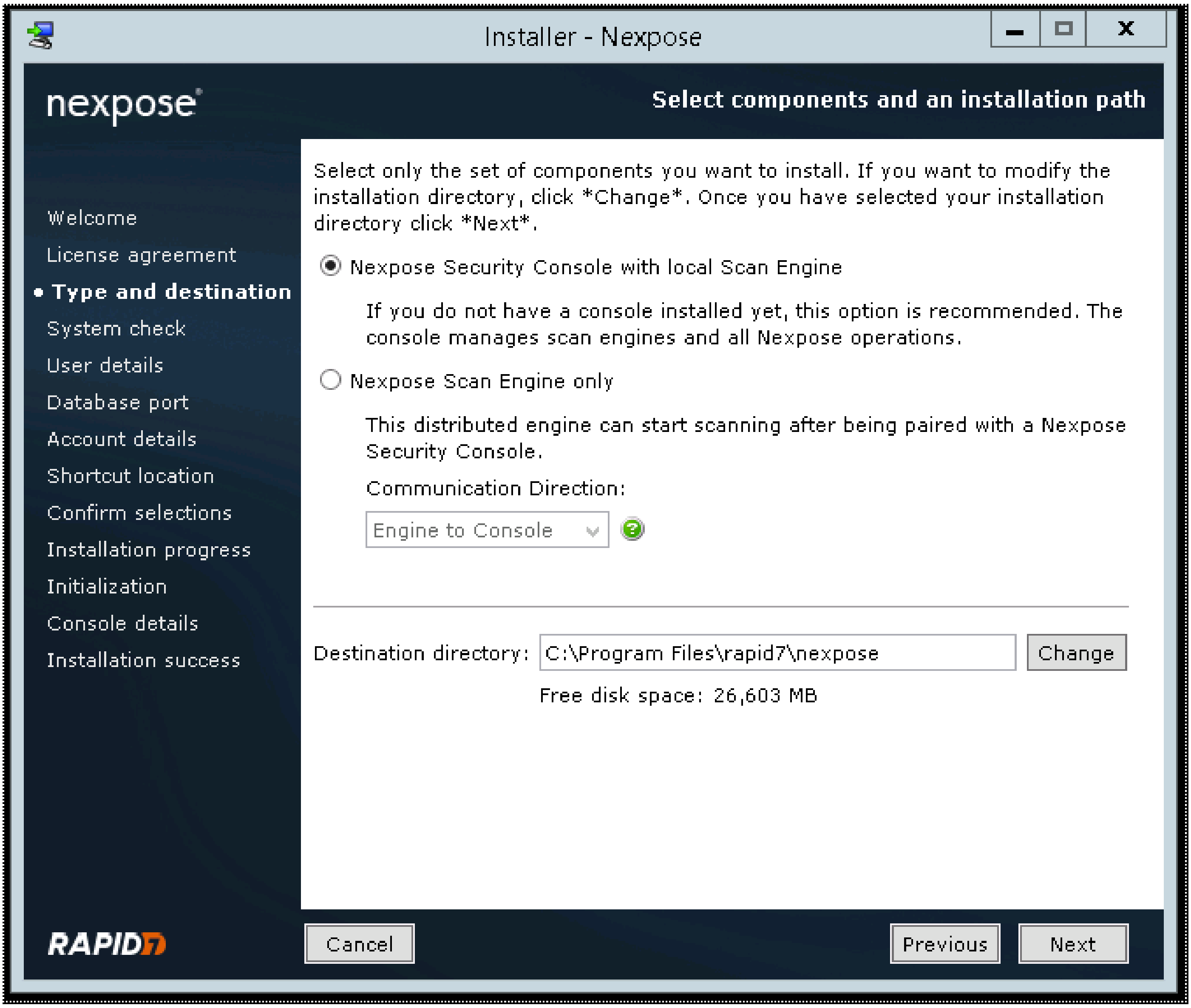
9. 如果需要，將根據配置的授權策略觸發CoA。

部署和配置下一掃描程式

注意：本文檔中的附件配置用於實驗目的，請諮詢Rapid7工程師以瞭解設計注意事項

步驟1.部署Nexpose Scanner。

Nexpose掃描器可以從OVA檔案部署，安裝在Linux和Windows作業系統之上。在本文檔中，安裝在Windows Server 2012 R2上完成。從Rapid7網站下載映像並開始安裝。配置**Type and destination**時，請選擇**Nexpose Security Console with local Scan Engine**



Select components and an installation path

Select only the set of components you want to install. If you want to modify the installation directory, click *Change*. Once you have selected your installation directory click *Next*.

● Nexpose Security Console with local Scan Engine

If you do not have a console installed yet, this option is recommended. The console manages scan engines and all Nexpose operations.

○ Nexpose Scan Engine only

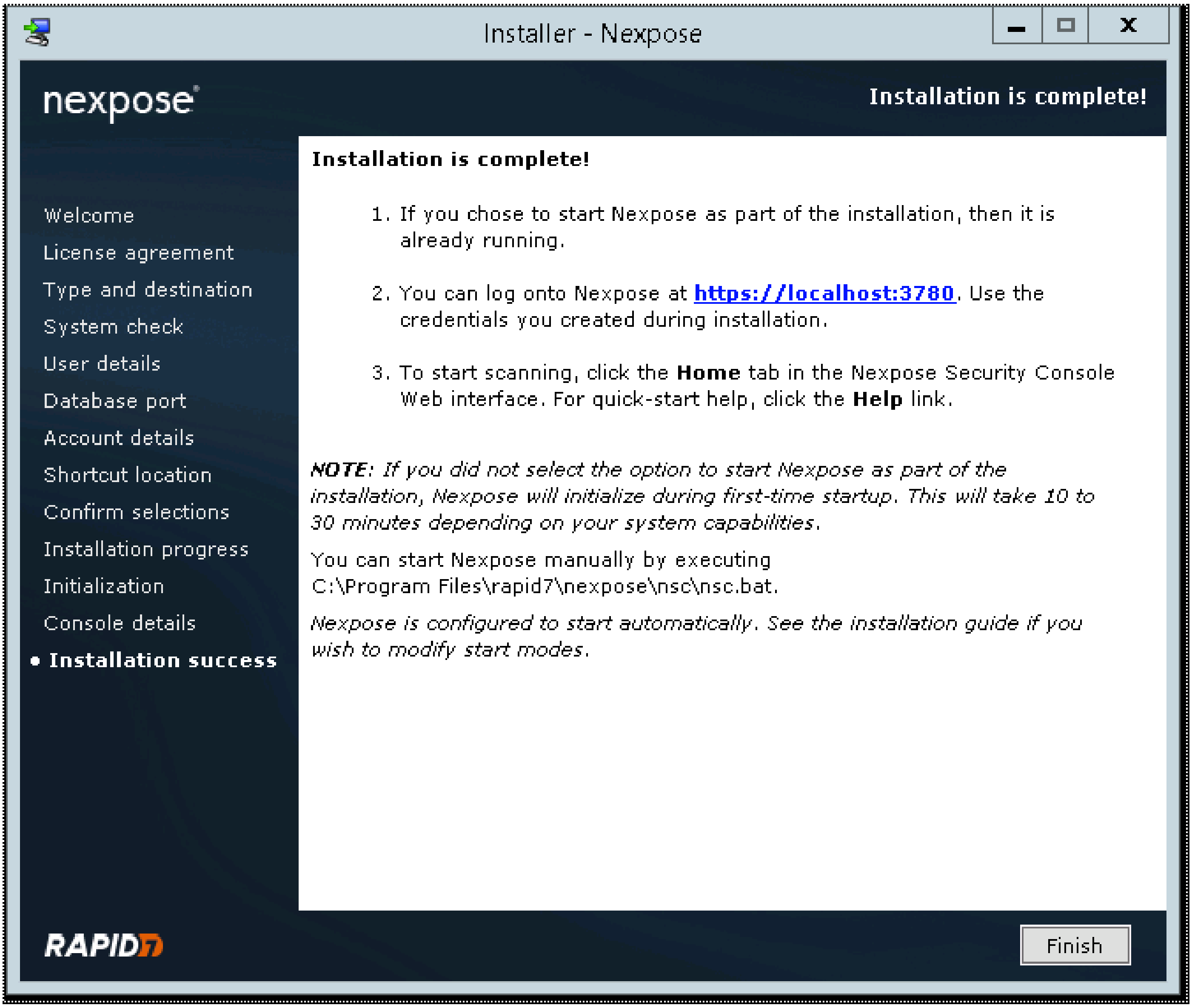
This distributed engine can start scanning after being paired with a Nexpose Security Console.

Communication Direction: Engine to Console

Destination directory: C:\Program Files\rapid7\nexpose

Free disk space: 26,603 MB

安裝完成後，伺服器將重新啟動。啟動後，Nexpose掃描器應可通過3780埠訪問，如下圖所示：



Installation is complete!

Installation is complete!

1. If you chose to start Nexpose as part of the installation, then it is already running.

2. You can log onto Nexpose at https://localhost:3780. Use the credentials you created during installation.

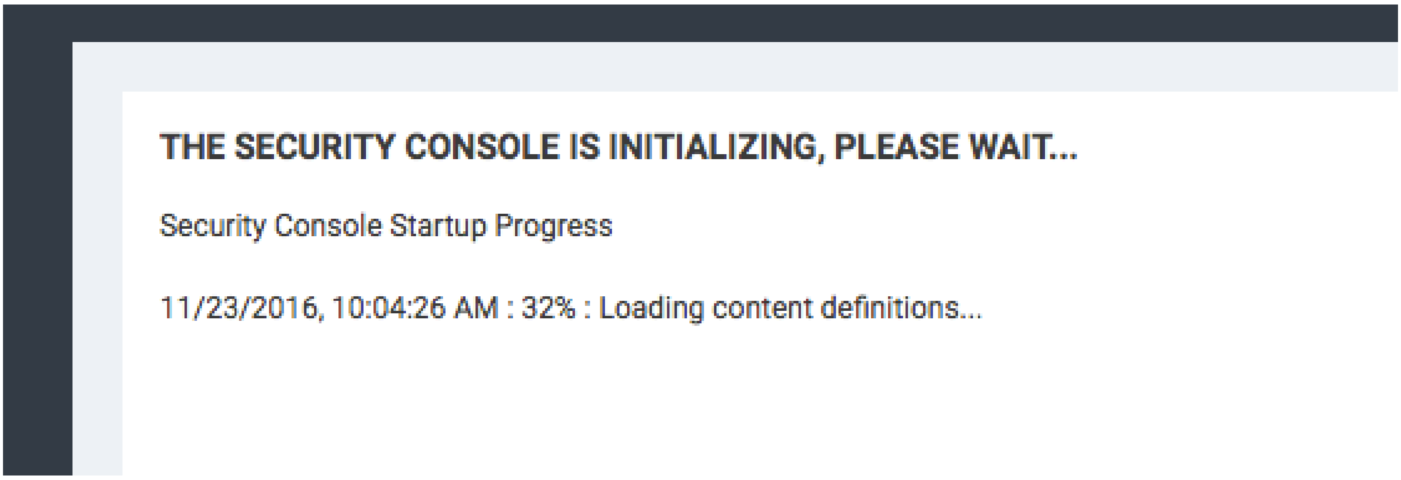
3. To start scanning, click the **Home** tab in the Nexpose Security Console Web interface. For quick-start help, click the **Help** link.

NOTE: If you did not select the option to start Nexpose as part of the installation, Nexpose will initialize during first-time startup. This will take 10 to 30 minutes depending on your system capabilities.

You can start Nexpose manually by executing C:\Program Files\rapid7\nexpose\nsc\nsc.bat.

Nexpose is configured to start automatically. See the installation guide if you wish to modify start modes.

如圖所示，scanner將經歷安全控制檯啟動過程：



THE SECURITY CONSOLE IS INITIALIZING, PLEASE WAIT...

Security Console Startup Progress

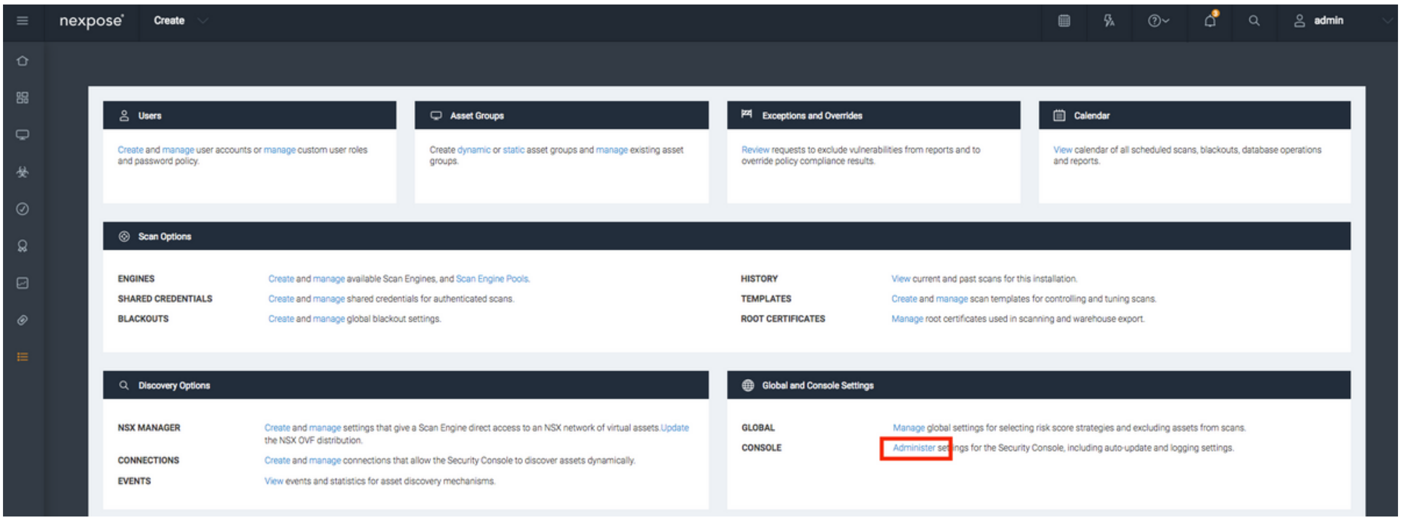
11/23/2016, 10:04:26 AM : 32% : Loading content definitions...

之後，要訪問GUI，應提供許可證金鑰。請注意，需要Enterprise Edition of Nexpose Scanner，如果安裝了Community Edition，則不會觸發掃描。

步驟2.配置Nexpose Scanner。

第一步是在Nexpose掃描器上安裝證書。本文檔中的證書由與ISE（實驗室CA）管理證書相同的

CA頒發。 導航到**Administration > Global and Console Settings**。在**Console**下選擇**管理**，如下圖所示。



Users

Create and manage user accounts or manage custom user roles and password policy.

Asset Groups

Create dynamic or static asset groups and manage existing asset groups.

Exceptions and Overrides

Review requests to exclude vulnerabilities from reports and to override policy compliance results.

Calendar

View calendar of all scheduled scans, blackouts, database operations and reports.

Scan Options

ENGINES	Create and manage available Scan Engines, and Scan Engine Pools.
SHARED CREDENTIALS	Create and manage shared credentials for authenticated scans.
BLACKOUTS	Create and manage global blackout settings.
HISTORY	View current and past scans for this installation.
TEMPLATES	Create and manage scan templates for controlling and tuning scans.
ROOT CERTIFICATES	Manage root certificates used in scanning and warehouse export.

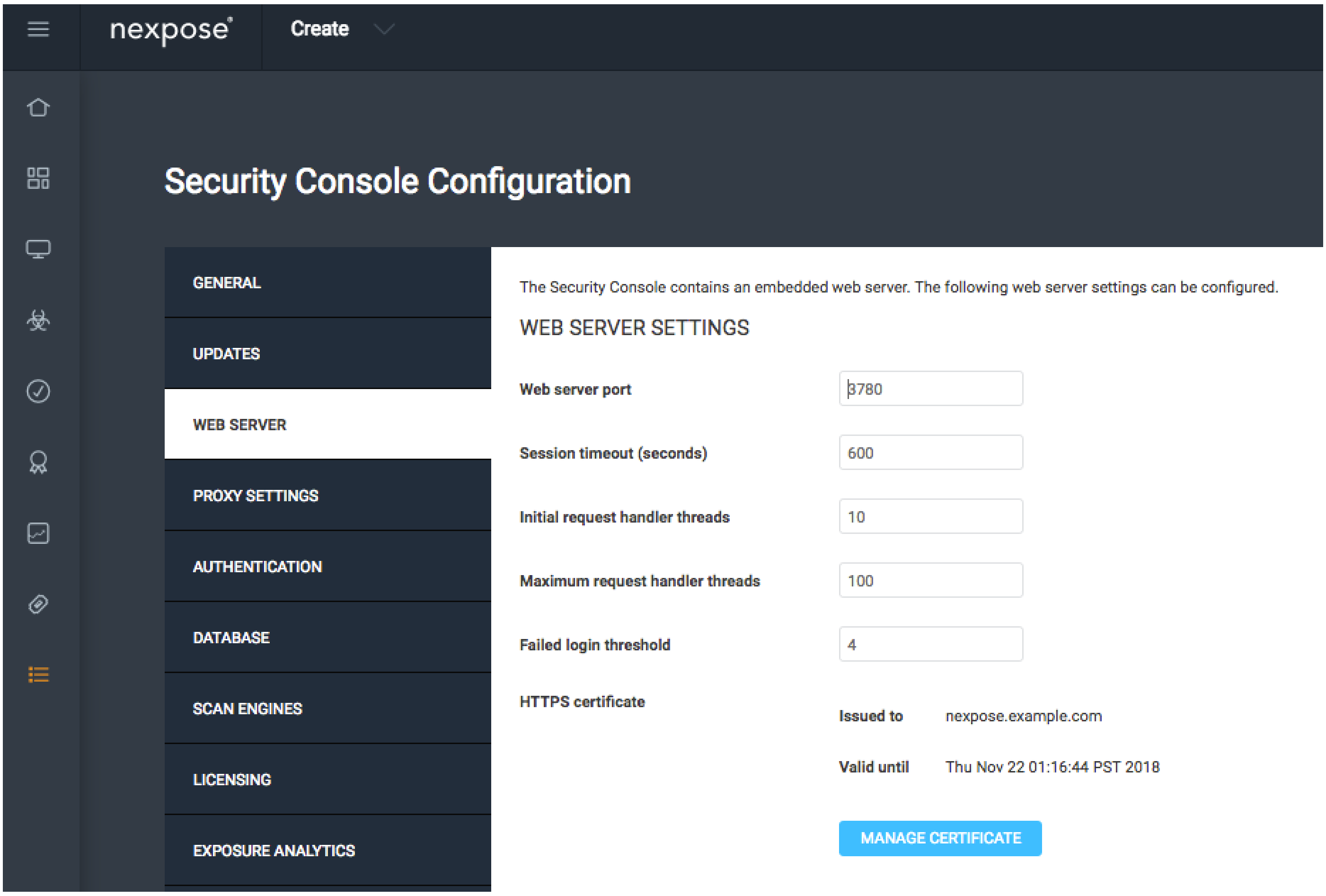
Discovery Options

NSX MANAGER	Create and manage settings that give a Scan Engine direct access to an NSX network of virtual assets.Update the NSX OVF distribution.
CONNECTIONS	Create and manage connections that allow the Security Console to discover assets dynamically.
EVENTS	View events and statistics for asset discovery mechanisms.

Global and Console Settings

GLOBAL	Manage global settings for selecting risk score strategies and excluding assets from scans.
CONSOLE	Administer settings for the Security Console, including auto-update and logging settings.

按一下「**Manage Certificate**」，如下圖所示：



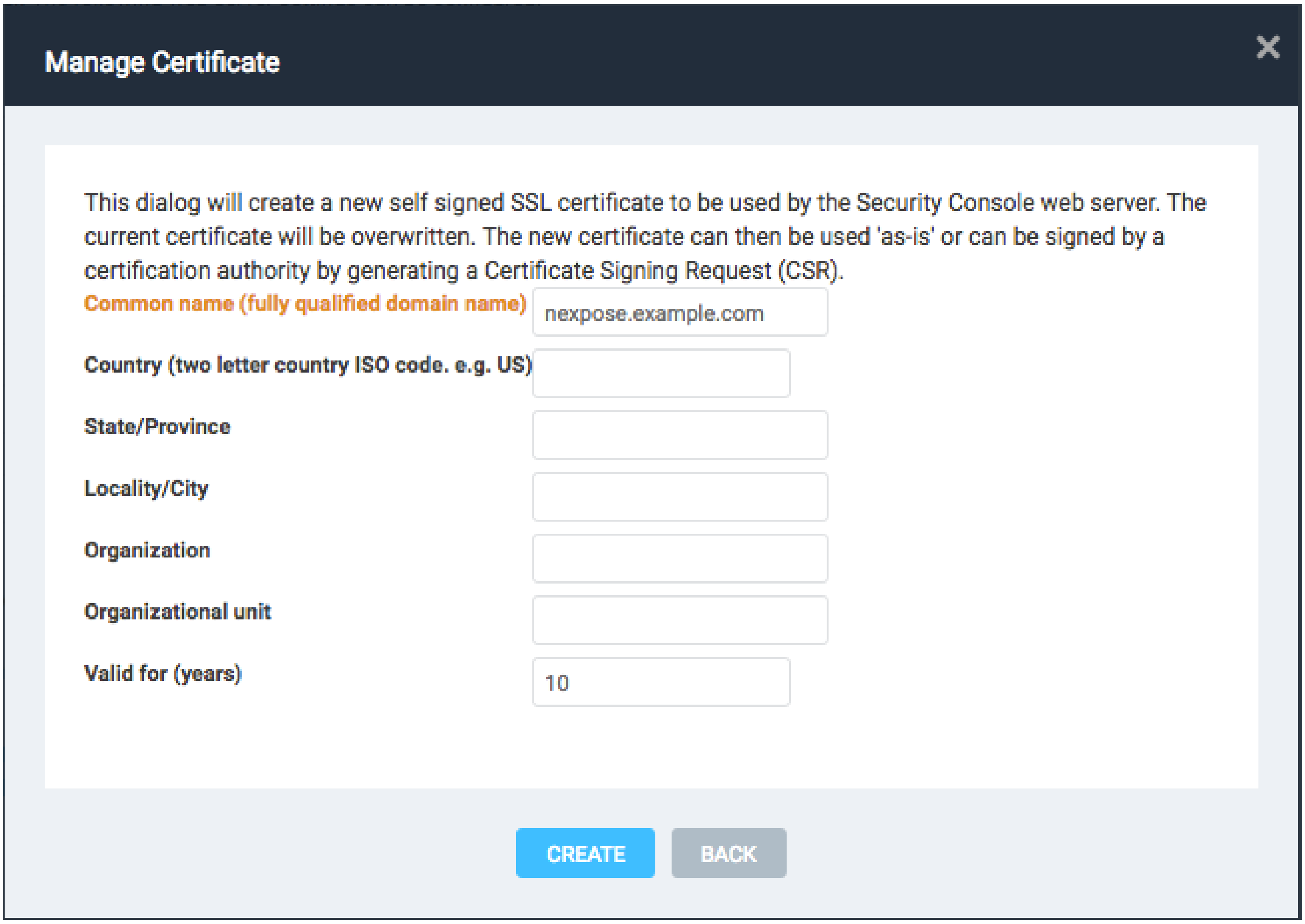
Security Console Configuration

The Security Console contains an embedded web server. The following web server settings can be configured.

WEB SERVER SETTINGS

Web server port	3780
Session timeout (seconds)	600
Initial request handler threads	10
Maximum request handler threads	100
Failed login threshold	4
HTTPS certificate	Issued to nexpose.example.com Valid until Thu Nov 22 01:16:44 PST 2018

如圖所示，在**建立新證書**中按一下。輸入**Common Name**以及您希望在Nexpose Scanner的身份證書中包含的任何其他資料。確保ISE能夠使用DNS解析附屬掃描器FQDN。



Manage Certificate

This dialog will create a new self signed SSL certificate to be used by the Security Console web server. The current certificate will be overwritten. The new certificate can then be used 'as-is' or can be signed by a certification authority by generating a Certificate Signing Request (CSR).

Common name (fully qualified domain name) nexpose.example.com

Country (two letter country ISO code. e.g. US)

State/Province

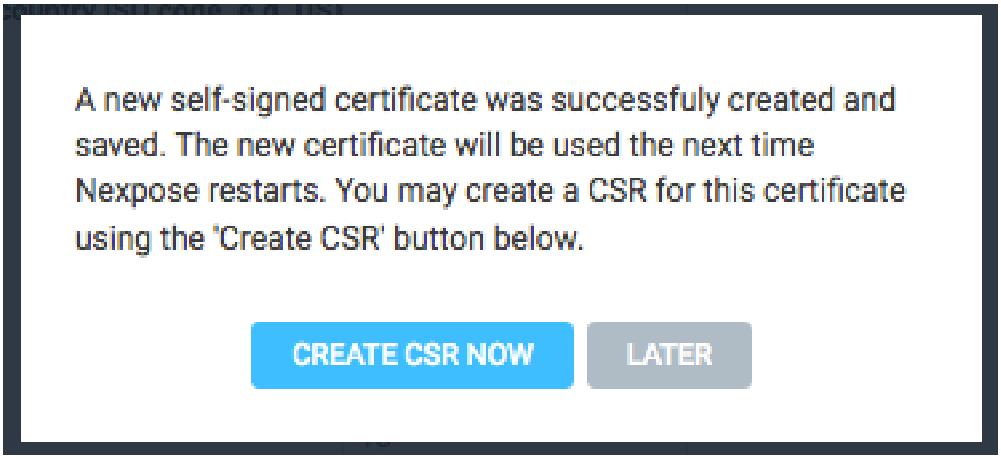
Locality/City

Organization

Organizational unit

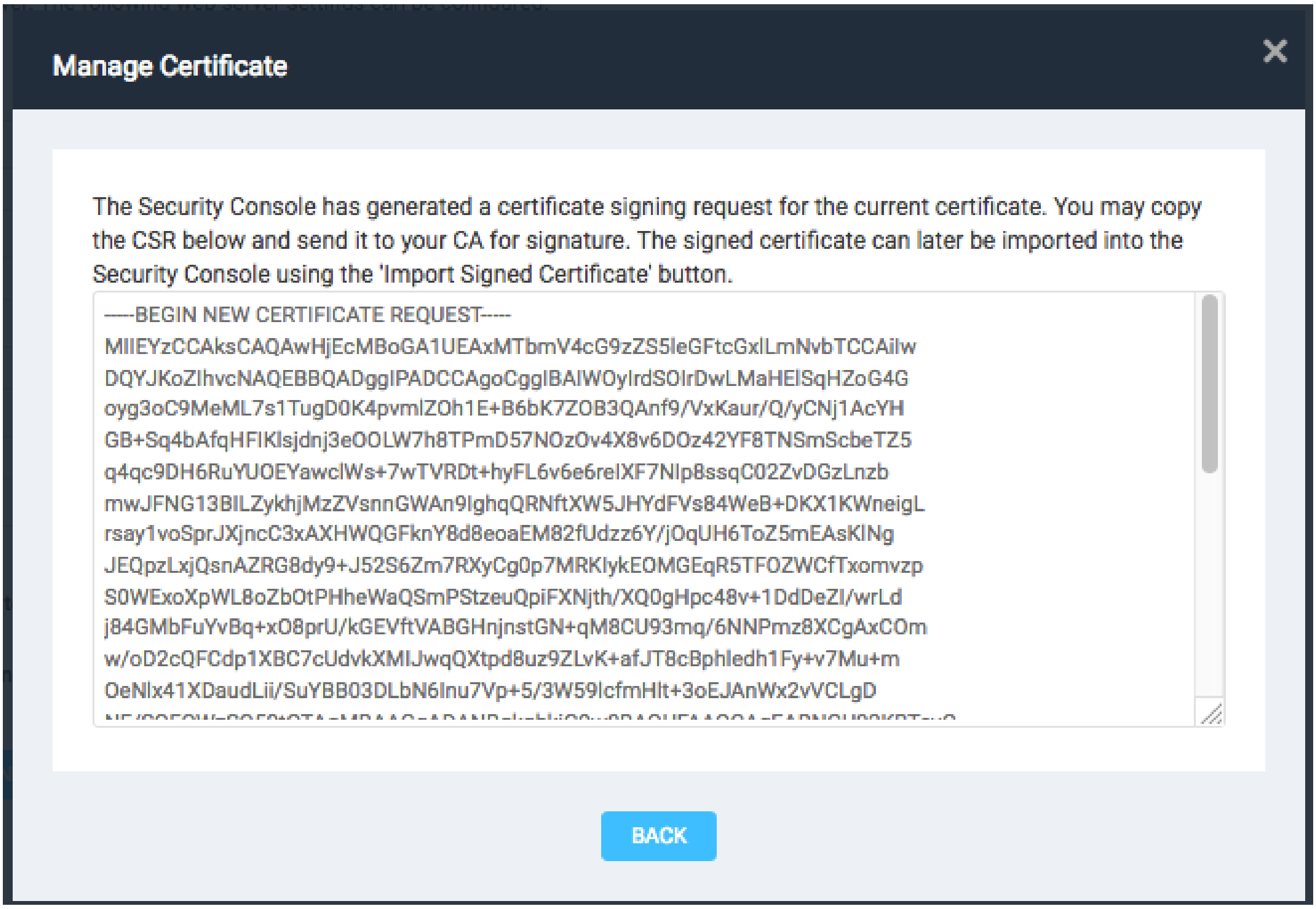
Valid for (years) 10

將憑證簽署請求(CSR)匯出到終端。



A new self-signed certificate was successfuly created and saved. The new certificate will be used the next time Nexpose restarts. You may create a CSR for this certificate using the 'Create CSR' button below.

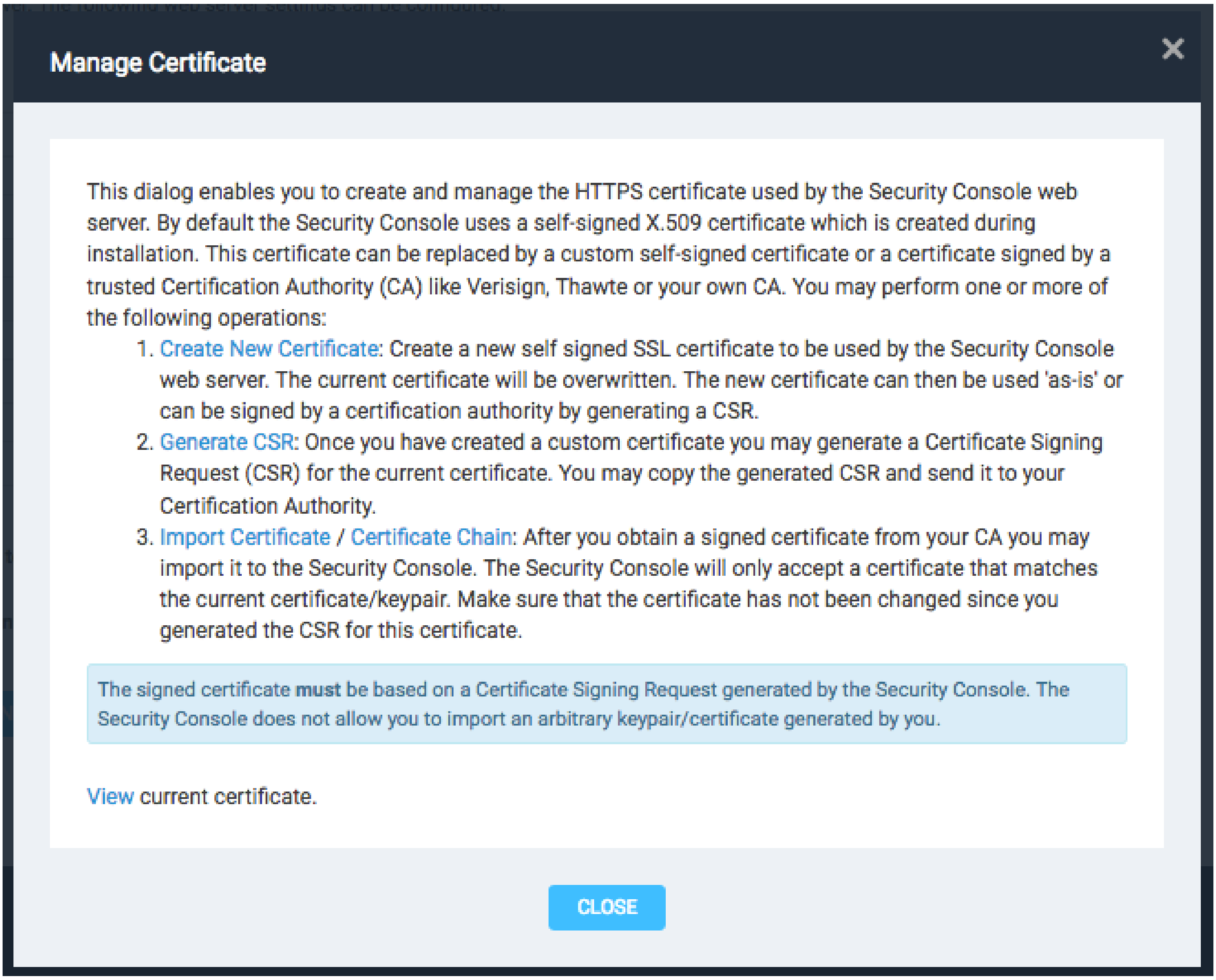
此時，您需要與憑證授權單位(CA)簽署CSR。



The Security Console has generated a certificate signing request for the current certificate. You may copy the CSR below and send it to your CA for signature. The signed certificate can later be imported into the Security Console using the 'Import Signed Certificate' button.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEYzCCAksCAQAwHjEcMBoGA1UEAxMTbmV4cG9zZS5leGFtcGxlLmNvbTCCAilw
DQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAIWOylrdSOIrDwLMaHElSqHZoG4G
oyg3oC9MeML7s1TugD0K4pvmlZOh1E+B6bK7ZOB3QAnf9/VxKaur/Q/yCNj1AcYH
GB+Sq4bAfqHFIKlsjdnj3eOOLW7h8TPmD57NOzOv4X8v6DOz42YF8TNSmScbeTZ5
q4qc9DH6RuYUOEYawclWs+7wTVRDt+hyFL6v6e6relXF7NIp8ssqC02ZvDGzLnzb
mwJFNG13BILZykhjMzZVsnnGWAn9IghqQRNftXW5JHYdFVs84WeB+DKX1KWneigL
rsay1voSprJXjncC3xAXHWQGFknY8d8eoaEM82fUdzz6Y/jOqUH6ToZ5mEAsKINg
JEQpzLxjQsnAZRG8dy9+J52S6Zm7RXyCg0p7MRKlykEOMGEqR5TFOZWCfTxomvzp
S0WExoXpWL8oZbOtPHheWaQSmPStzeuQpiFXNjth/XQ0gHpc48v+1DdDeZI/wrLd
j84GMbFuYvBq+xO8prU/kGEVftVABGHnjnstGN+qM8CU93mq/6NNPmz8XCgAxCOm
w/oD2cQFCdp1XBC7cUdvkXMIJwqQXtpd8uz9ZLvK+afJT8cBphledh1Fy+v7Mu+m
OeNlx41XDaudLii/SuYBB03DLbN6Inu7Vp+5/3W59lcfmHlt+3oEJAnWx2vVCLgD
```

按一下**Import Certificate**，匯入CA頒發的證書。



Manage Certificate

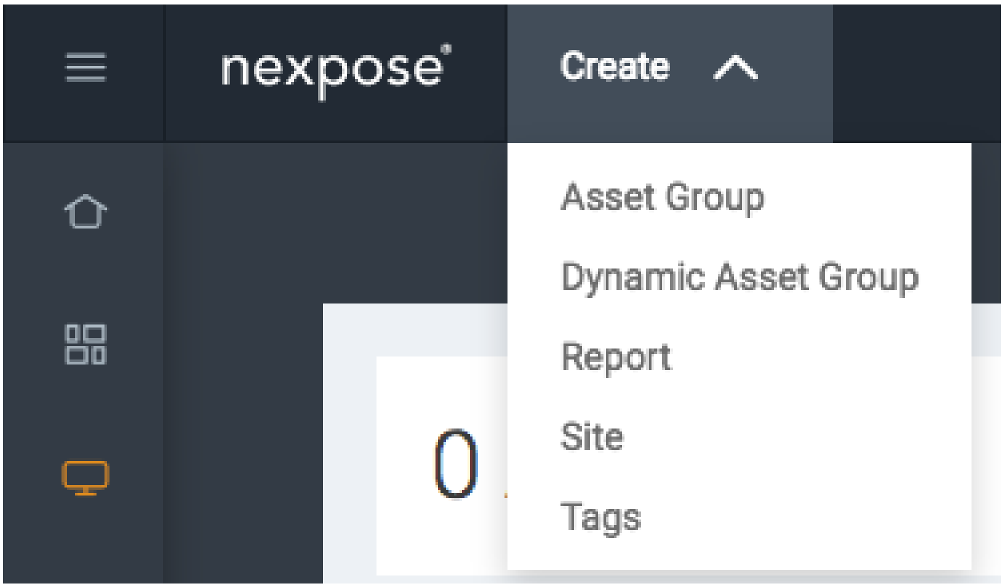
This dialog enables you to create and manage the HTTPS certificate used by the Security Console web server. By default the Security Console uses a self-signed X.509 certificate which is created during installation. This certificate can be replaced by a custom self-signed certificate or a certificate signed by a trusted Certification Authority (CA) like Verisign, Thawte or your own CA. You may perform one or more of the following operations:

1. Create New Certificate: Create a new self signed SSL certificate to be used by the Security Console web server. The current certificate will be overwritten. The new certificate can then be used 'as-is' or can be signed by a certification authority by generating a CSR.
2. Generate CSR: Once you have created a custom certificate you may generate a Certificate Signing Request (CSR) for the current certificate. You may copy the generated CSR and send it to your Certification Authority.
3. Import Certificate / Certificate Chain: After you obtain a signed certificate from your CA you may import it to the Security Console. The Security Console will only accept a certificate that matches the current certificate/keypair. Make sure that the certificate has not been changed since you generated the CSR for this certificate.

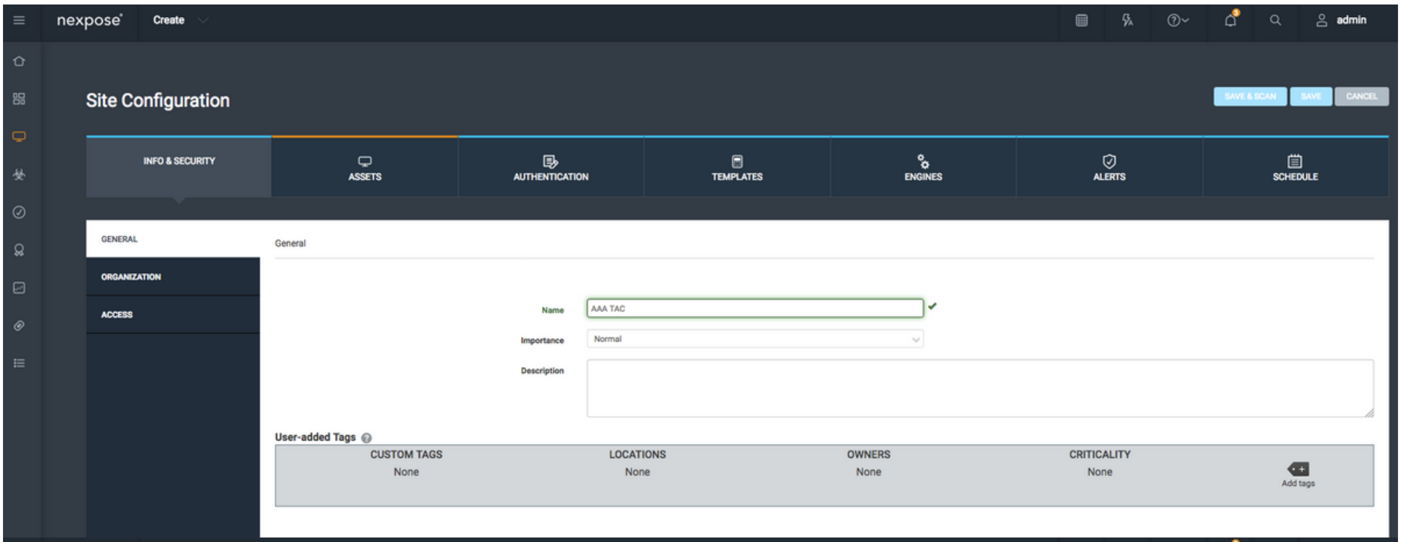
The signed certificate **must** be based on a Certificate Signing Request generated by the Security Console. The Security Console does not allow you to import an arbitrary keypair/certificate generated by you.

View current certificate.

配置站點。站點包含您應該能夠掃描的資產，並且用於將ISE與附屬掃描器整合的帳戶應具有管理站點和建立報告的許可權。導覽至**Create > Site**，如下圖所示。



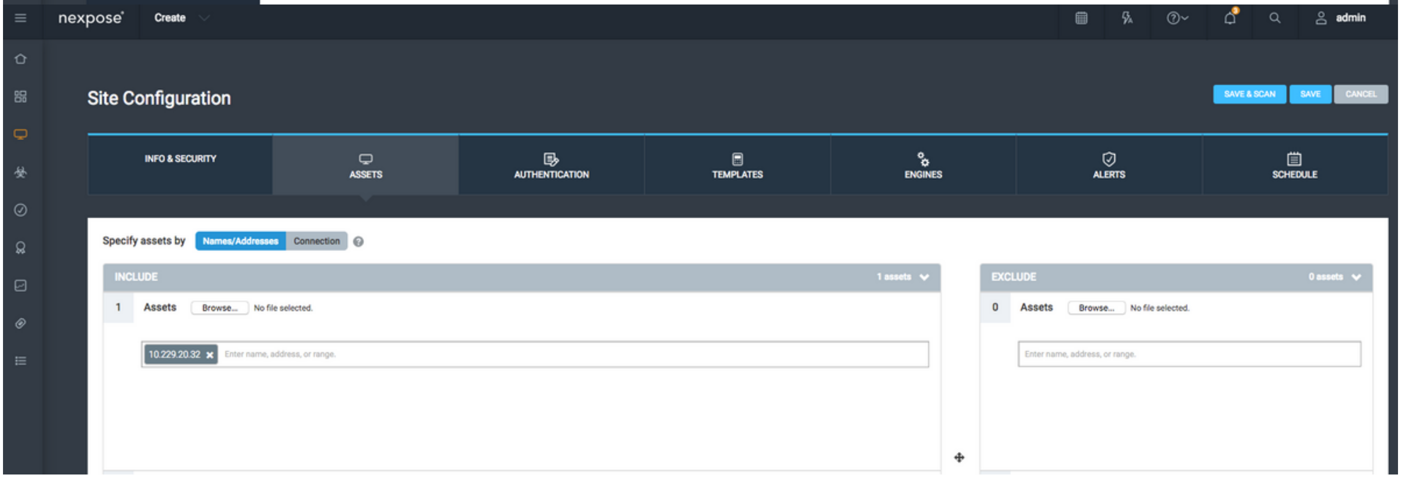
如圖所示，在「**Info & Security**」索引標籤上輸入**Name**。**Assets**頁籤應包含有效資產的IP地址，即符合漏洞掃描條件的端點。



Name: AAA TAC
Importance: Normal
Description:

User-added Tags

CUSTOM TAGS	LOCATIONS	OWNERS	CRITICALITY
None	None	None	None

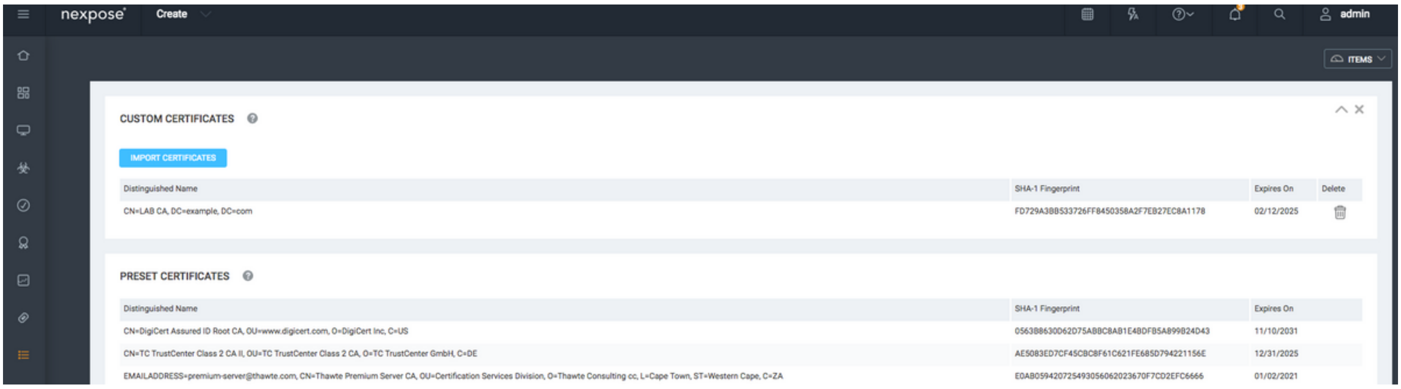


Specify assets by: Names/Addresses

INCLUDE — 1 assets
1 Assets — No file selected.
10.229.20.32

EXCLUDE — 0 assets
0 Assets — No file selected.

將簽署ISE證書的CA證書匯入到受信任的儲存中。導航到**管理>根證書>管理>匯入證書**。



CUSTOM CERTIFICATES

Distinguished Name	SHA-1 Fingerprint	Expires On	Delete
CN=LAB CA, DC=example, DC=com	FD729A3BB533726FF8450358A2F7EB27EC8A1178	02/12/2025	🗑

PRESET CERTIFICATES

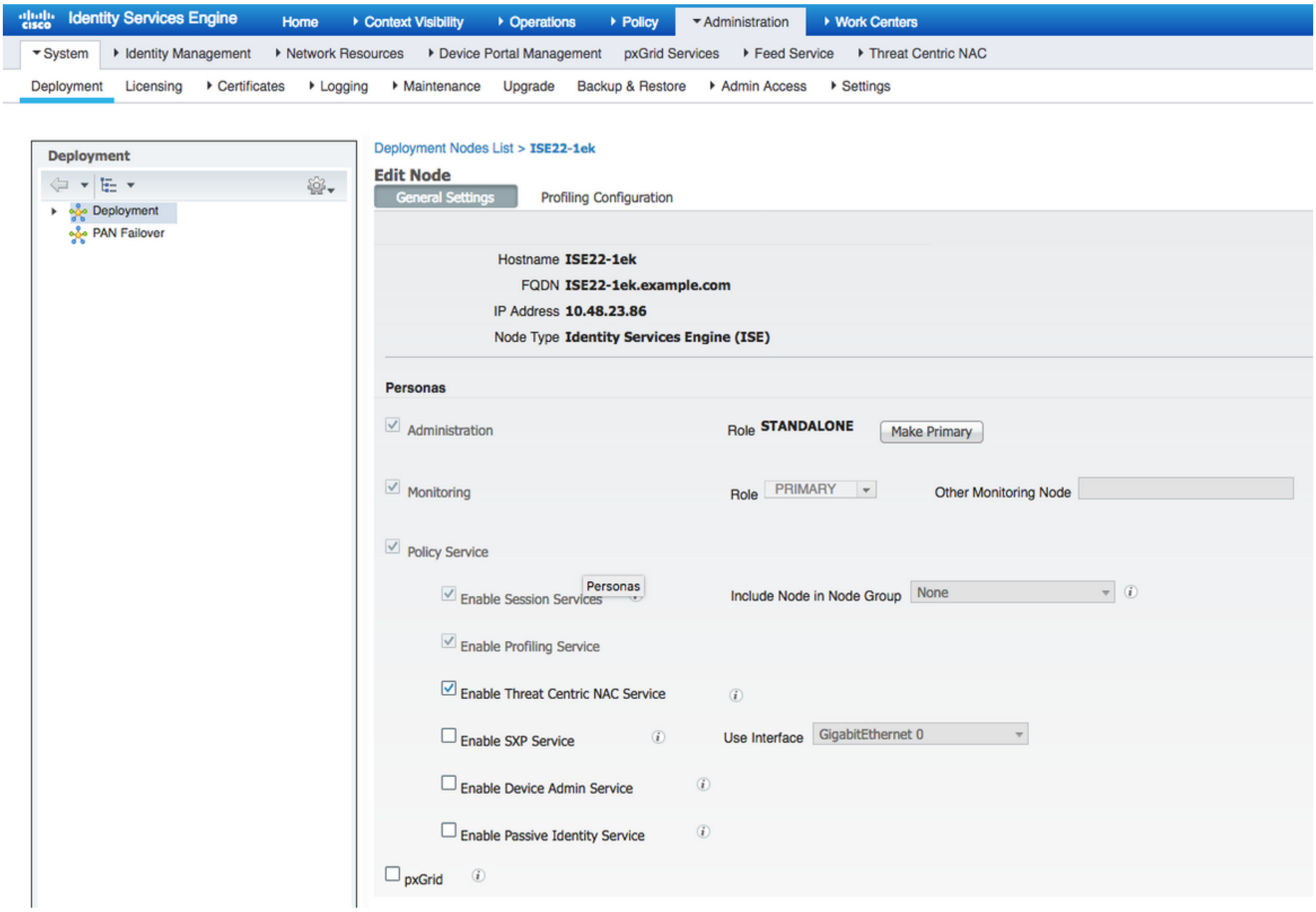
Distinguished Name	SHA-1 Fingerprint	Expires On
CN=DigiCert Assured ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43	11/10/2031
CN=TC TrustCenter Class 2 CA II, OU=TC TrustCenter Class 2 CA, O=TC TrustCenter GmbH, C=DE	AE5083ED7CF45CBC8F61C621FE685D794221156E	12/31/2025
EMAILADDRESS=premium-server@thawte.com, CN=Thawte Premium Server CA, OU=Certification Services Division, O=Thawte Consulting cc, L=Cape Town, ST=Western Cape, C=ZA	E0AB059420725493056062023670F7CD2EFC6666	01/02/2021

配置ISE

步驟1.啟用TC-NAC服務。

在ISE節點上啟用TC-NAC服務。請注意以下事項：

- 以威脅為中心的NAC服務需要Apex許可證。
- 對於以威脅為中心的NAC服務，您需要單獨的策略服務節點(PSN)。
- 只能在部署中的一個節點上啟用以威脅為中心的NAC服務。
- 對於漏洞評估服務，每個供應商只能新增一個介面卡例項。



Edit Node

Hostname ISE22-1ek
FQDN ISE22-1ek.example.com
IP Address 10.48.23.86
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 Threat Centric NAC Service

□ Enable SXP Service — Use Interface GigabitEthernet 0

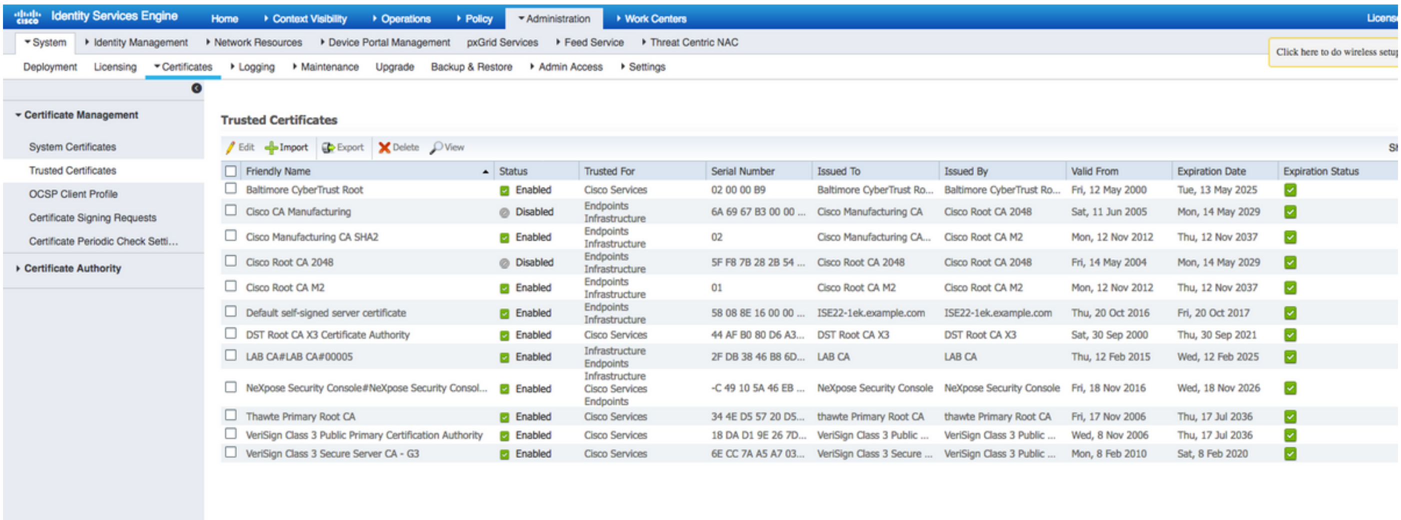
□ Enable Device Admin Service

□ Enable Passive Identity Service

□ pxGrid

步驟2.匯入附屬掃描器證書。

將Nexpose Scanner CA證書匯入思科ISE中的受信任證書庫(**Administration > Certificates > Certificate Management > Trusted Certificates > Import**)。 確保在思科ISE受信任證書儲存中匯入（或存在）相應的根證書和中間證書

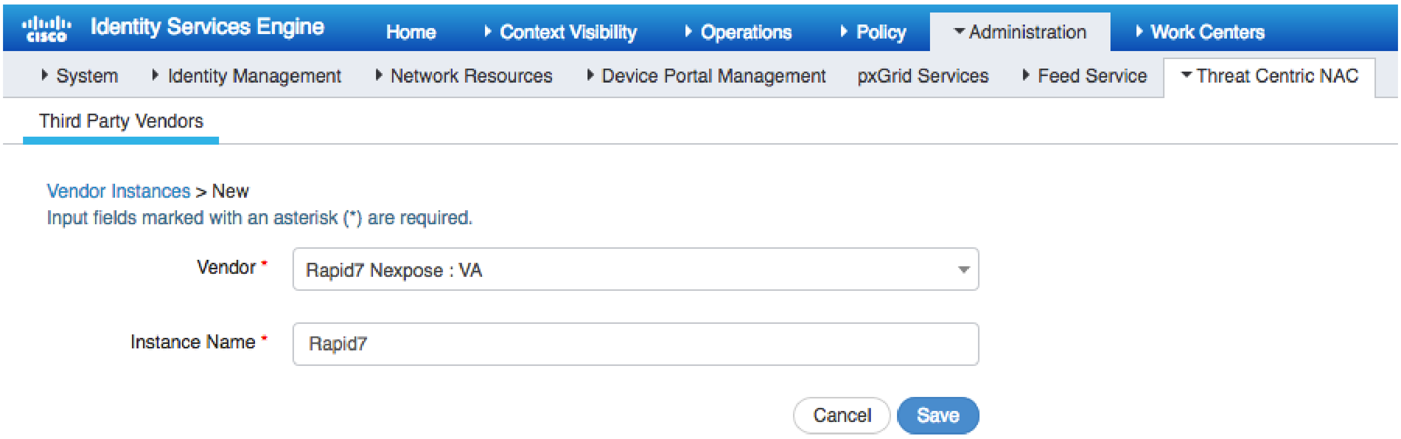


Trusted Certificates

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Tue, 13 May 2025	✓
Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00 ...	Cisco Manufacturing CA	Cisco Root CA 2048	Sat, 11 Jun 2005	Mon, 14 May 2029	✓
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	✓
Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54 ...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029	✓
Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	✓
Default self-signed server certificate	Enabled	Endpoints Infrastructure	58 08 8E 16 00 00 ...	ISE22-1ek.example.com	ISE22-1ek.example.com	Thu, 20 Oct 2016	Fri, 20 Oct 2017	✓
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A3...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2021	✓
LAB CA#LAB CA#00005	Enabled	Infrastructure Endpoints	2F DB 38 46 B8 6D...	LAB CA	LAB CA	Thu, 12 Feb 2015	Wed, 12 Feb 2025	✓
NeXpose Security Console#NeXpose Security Consol...	Enabled	Infrastructure Cisco Services Endpoints	-C 49 10 5A 46 EB ...	NeXpose Security Console	NeXpose Security Console	Fri, 18 Nov 2016	Wed, 18 Nov 2026	✓
Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5...	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov 2006	Thu, 17 Jul 2036	✓
VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D...	VeriSign Class 3 Public ...	VeriSign Class 3 Public ...	Wed, 8 Nov 2006	Thu, 17 Jul 2036	✓
VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03...	VeriSign Class 3 Secure ...	VeriSign Class 3 Public ...	Mon, 8 Feb 2010	Sat, 8 Feb 2020	✓

步驟3.配置Nexpresence Scanner TC-NAC例項。

在**Administration > Threat Centric NAC > Third Party Vendors**處新增Rapid7例項。

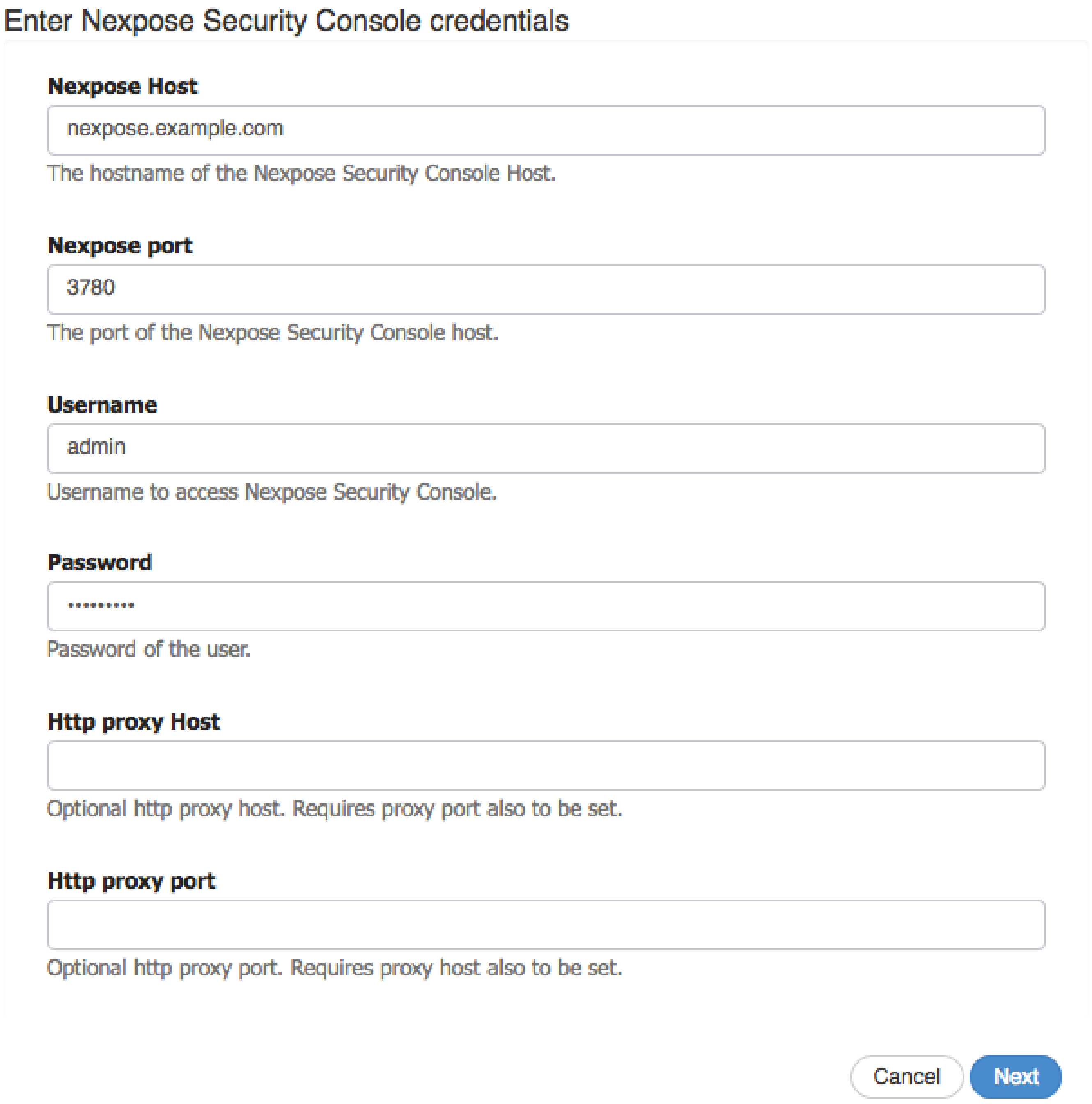


Vendor Instances > New

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

Vendor *	Rapid7 Nexpose : VA
Instance Name *	Rapid7

新增例項後，例項將轉至**Ready to Configure**狀態。按一下此連結。配置**Nexpose Host**(Scanner)和**Port**，預設情況下為3780。指定**Username**和**Password**，以便訪問正確的站點。



Enter Nexpose Security Console credentials

Nexpose Host

nexpose.example.com

The hostname of the Nexpose Security Console Host.

Nexpose port

3780

The port of the Nexpose Security Console host.

Username

admin

Username to access Nexpose Security Console.

Password

•••••••••

Password of the user.

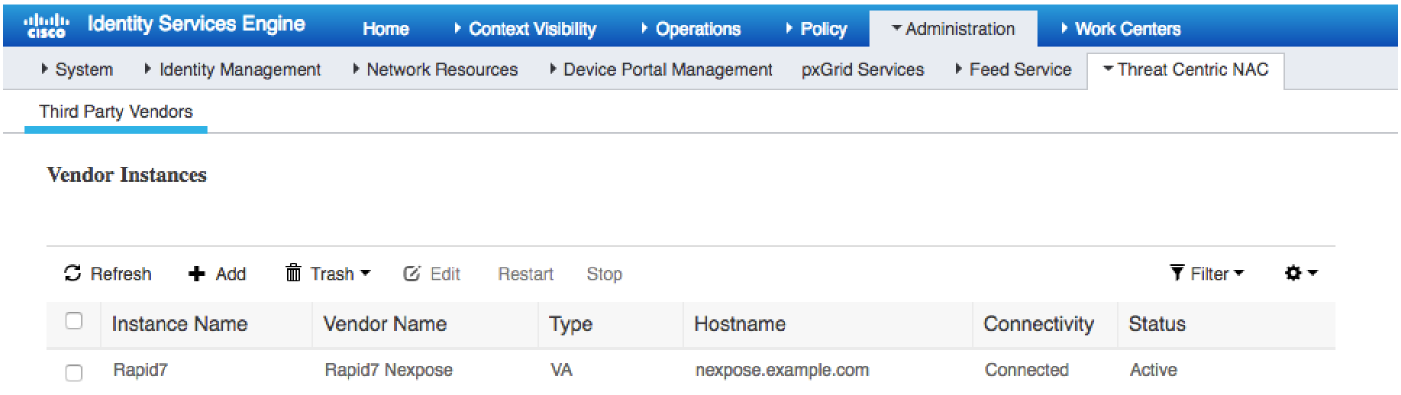
Http proxy Host

Optional http proxy host. Requires proxy port also to be set.

Http proxy port

Optional http proxy port. Requires proxy host also to be set.

高級設定在ISE 2.2管理指南中有詳細記錄，可以在本文檔的參考部分找到連結。按一下**Next**和**Finish**。Nexpose例項轉換為**Active**狀態並開始下載知識庫。



□	Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
□	Rapid7	Rapid7 Nexpose	VA	nexpose.example.com	Connected	Active

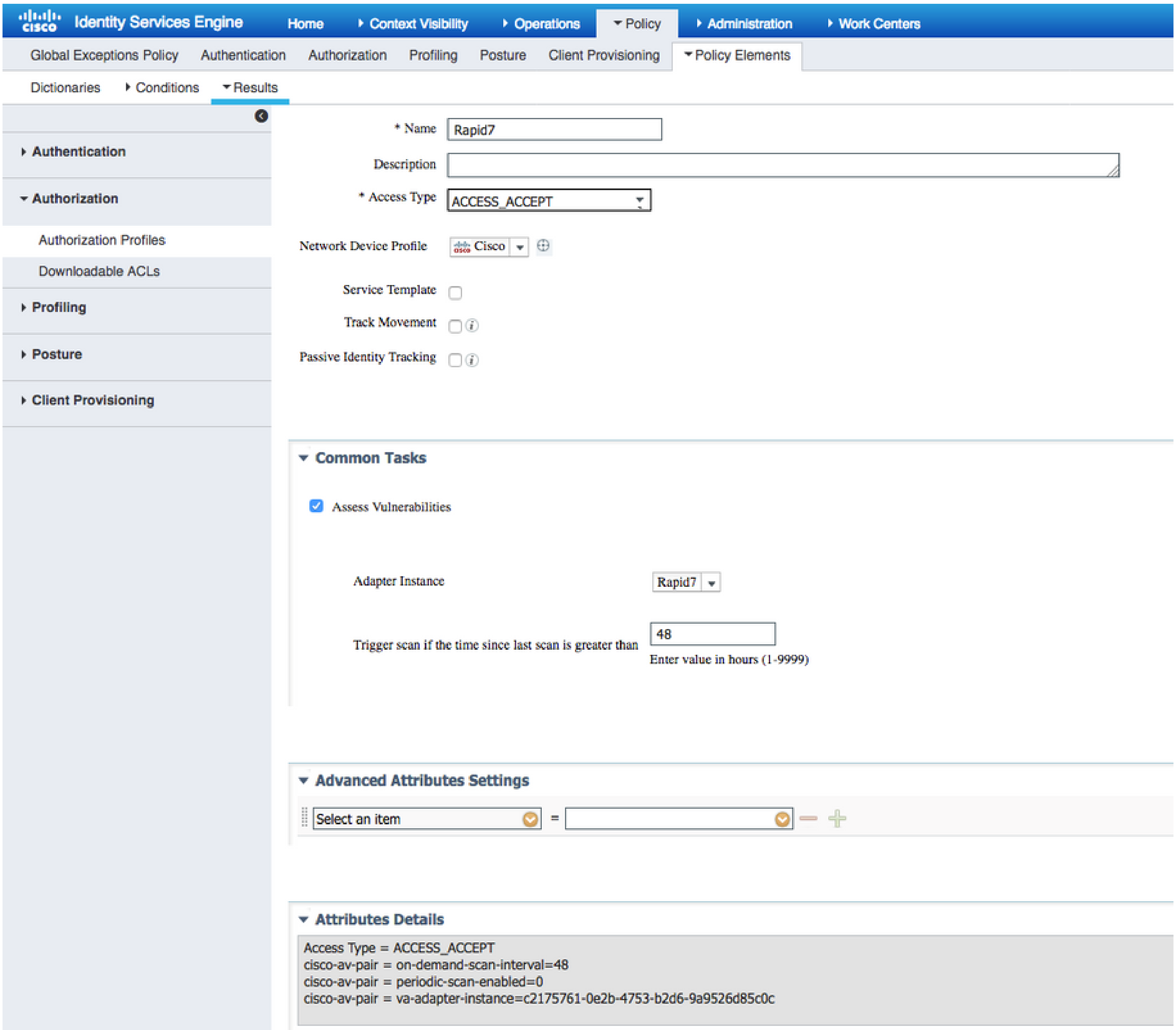
步驟4.配置授權配置檔案以觸發VA掃描。

導航到**Policy > Policy Elements > Results > Authorization > Authorization Profiles**。新增新配置檔案。在**Common Tasks**下，選中**Vulnerability Assessment**覈取方塊。應根據網路設計選擇按需掃描間隔。

授權配置檔案包含這些av對：

```
cisco-av-pair = on-demand-scan-interval=48
cisco-av-pair = periodic-scan-enabled=0
cisco-av-pair = va-adapter-instance=c2175761-0e2b-4753-b2d6-9a9526d85c0c
```

它們被傳送到訪問接受資料包中的網路裝置，儘管它們的真正目的是告訴監控(MNT)節點應該觸發掃描。MNT指示TC-NAC節點與附件掃描程式通訊。



* Name: Rapid7

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

☑ Assess Vulnerabilities

Adapter Instance: Rapid7

Trigger scan if the time since last scan is greater than: 48

Enter value in hours (1-9999)

Advanced Attributes Settings

Select an item =

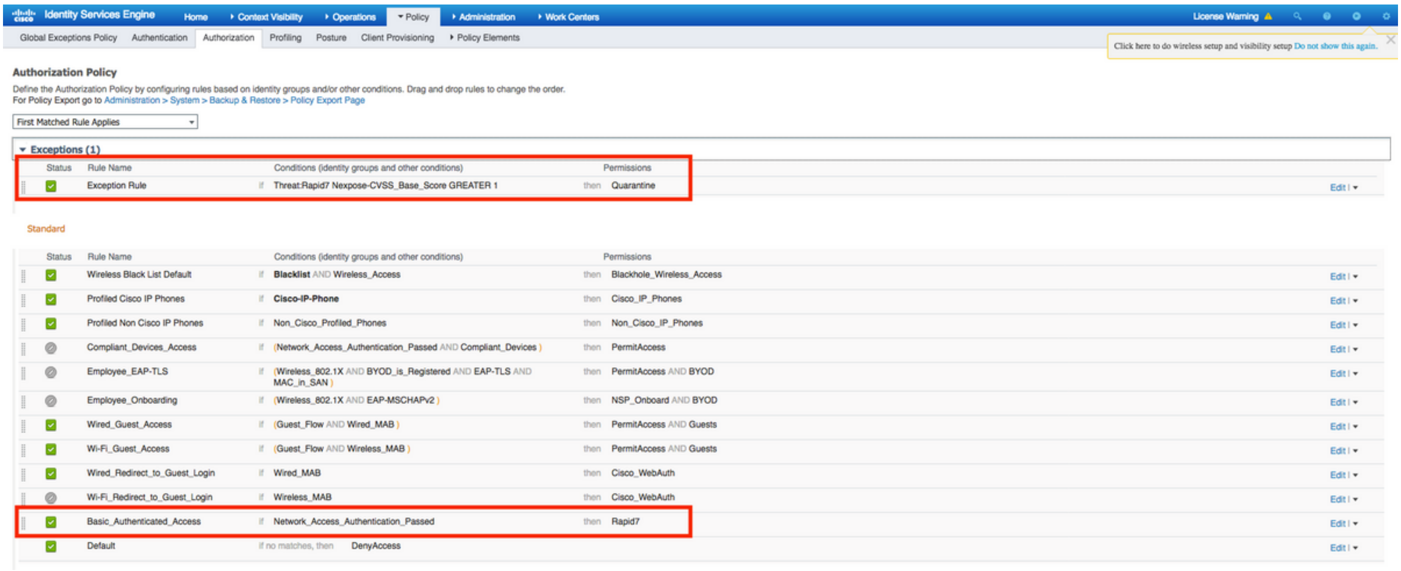
Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = on-demand-scan-interval=48
cisco-av-pair = periodic-scan-enabled=0
cisco-av-pair = va-adapter-instance=c2175761-0e2b-4753-b2d6-9a9526d85c0c
```

步驟5.配置授權策略。

- 配置授權策略以使用步驟4中配置的新授權配置檔案。導航到Policy > Authorization > Authorization Policy，找到Basic_Authenticated_Access規則，然後按一下Edit。將許可權從PermitAccess更改為新建立的Standard Rapid7。這將導致對所有使用者的漏洞掃描。在Save中按一下。

- 為隔離的電腦建立授權策略。導航到Policy > Authorization > Authorization Policy > Exceptions並建立**例外規則**。現在，導航到**條件>建立新條件（高級選項）>選擇屬性**，向下滾動並選擇**威脅**。展開Threat屬性並選擇Nexpose-CVSS_Base_Score。將運算子更改為**大於**，然後根據您的安全策略輸入一個值。**隔離**授權配置檔案應授予對易受攻擊的電腦的有限訪問許可權。



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

Exceptions (1)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Exception Rule	if	Threat:Rapid7 Nexpose-CVSS_Base_Score GREATER 1	then	Quarantine	Edit | ▾

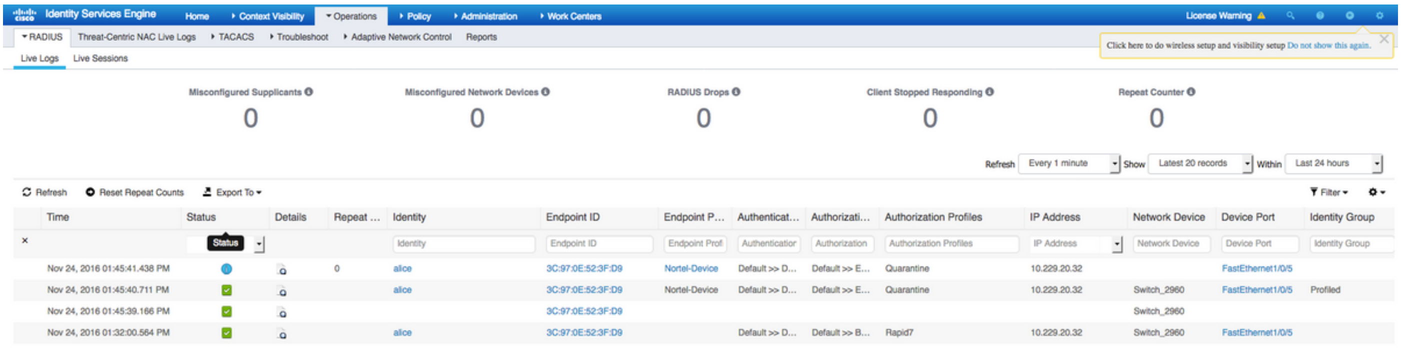
Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Wireless Black List Default	if	Blacklist AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones	Edit | ▾
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit | ▾
⊘	Compliant_Devices_Access	if	(Network_Access_Authentication_Passed AND Compliant_Devices)	then	PermitAccess	Edit | ▾
⊘	Employee_EAP-TLS	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then	PermitAccess AND BYOD	Edit | ▾
⊘	Employee_Onboarding	if	(Wireless_802.1X AND EAP-MSCHAPv2)	then	NSP_Onboard AND BYOD	Edit | ▾
✓	Wired_Guest_Access	if	(Guest_Flow AND Wired_MAB)	then	PermitAccess AND Guests	Edit | ▾
✓	Wi-Fi_Guest_Access	if	(Guest_Flow AND Wireless_MAB)	then	PermitAccess AND Guests	Edit | ▾
✓	Wired_Redirect_to_Guest_Login	if	Wired_MAB	then	Cisco_WebAuth	Edit | ▾
⊘	Wi-Fi_Redirect_to_Guest_Login	if	Wireless_MAB	then	Cisco_WebAuth	Edit | ▾
✓	Basic_Authenticated_Access	if	Network_Access_Authentication_Passed	then	Rapid7	Edit | ▾
✓	Default	if no matches, then	DenyAccess			Edit | ▾

驗證

身分識別服務引擎

第一個連線觸發VA掃描。掃描完成後，如果匹配了CoA Reauthentication，將觸發CoA Reauthentication應用新策略。

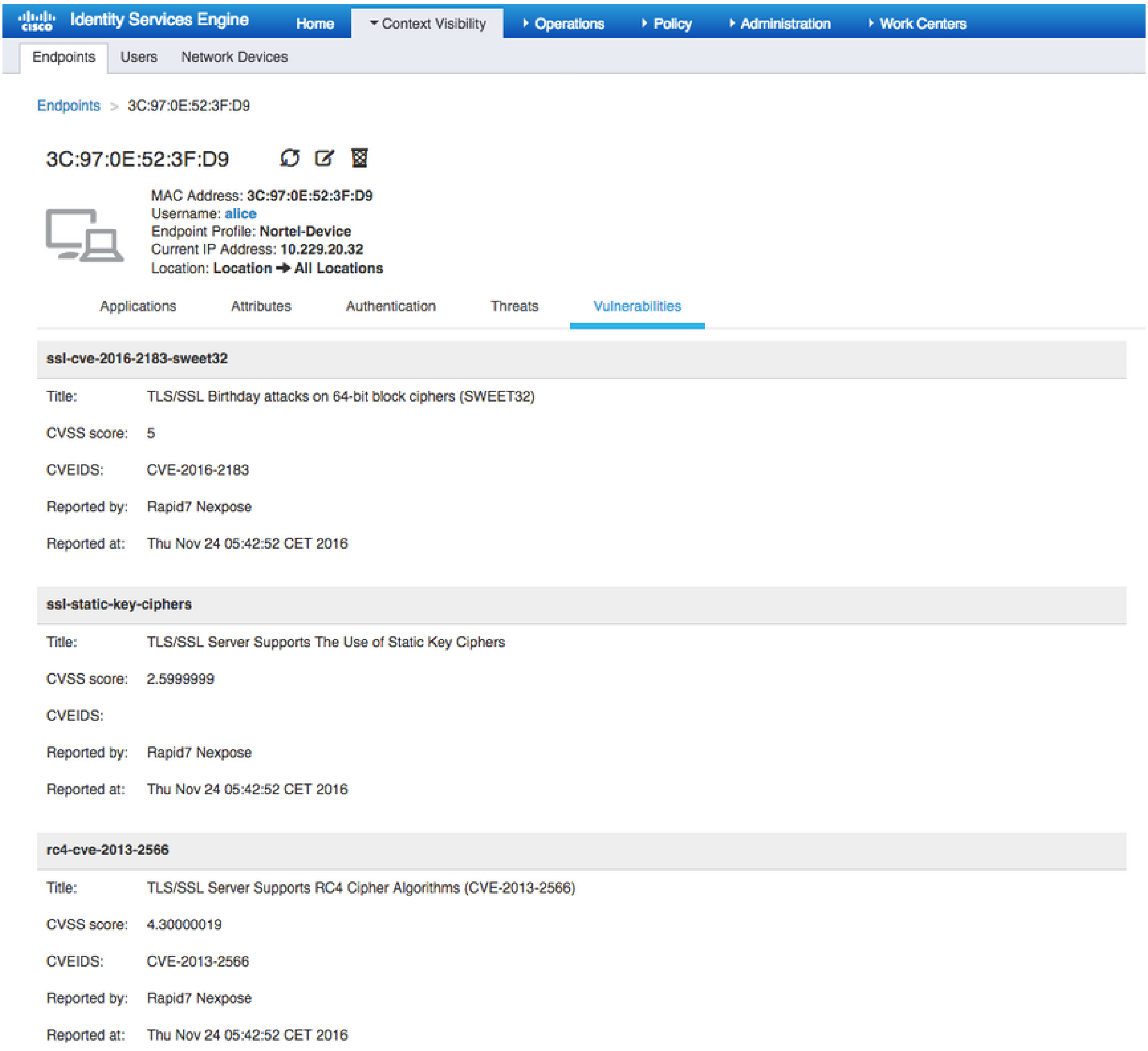


Misconfigured Supplicants 0 | Misconfigured Network Devices 0 | RADIUS Drops 0 | Client Stopped Responding 0 | Repeat Counter 0

Refresh Every 1 minute | Show Latest 20 records | Within Last 24 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Profiles	IP Address	Network Device	Device Port	Identity Group
Nov 24, 2016 01:45:41.438 PM	●	🔍	0	alice	3C:97:0E:52:3F:D9	Nortel-Device	Default >> D...	Default >> E...	Quarantine	10.229.20.32		FastEthernet1/0/5	
Nov 24, 2016 01:45:40.711 PM	✓	🔍		alice	3C:97:0E:52:3F:D9	Nortel-Device	Default >> D...	Default >> E...	Quarantine	10.229.20.32	Switch_2960	FastEthernet1/0/5	Profiled
Nov 24, 2016 01:45:39.166 PM	✓	🔍			3C:97:0E:52:3F:D9						Switch_2960		
Nov 24, 2016 01:32:00.564 PM	✓	🔍		alice	3C:97:0E:52:3F:D9		Default >> D...	Default >> B...	Rapid7	10.229.20.32	Switch_2960	FastEthernet1/0/5	

若要驗證檢測到哪些漏洞，請導覽至**Context Visibility > Endpoints**。使用Nexpose Scanner為其提供的分數檢查每個終端的漏洞。



3C:97:0E:52:3F:D9

MAC Address: **3C:97:0E:52:3F:D9**
Username: **alice**
Endpoint Profile: **Nortel-Device**
Current IP Address: **10.229.20.32**
Location: **Location → All Locations**

ssl-cve-2016-2183-sweet32

Title:	TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)
CVSS score:	5
CVEIDS:	CVE-2016-2183
Reported by:	Rapid7 Nexpose
Reported at:	Thu Nov 24 05:42:52 CET 2016

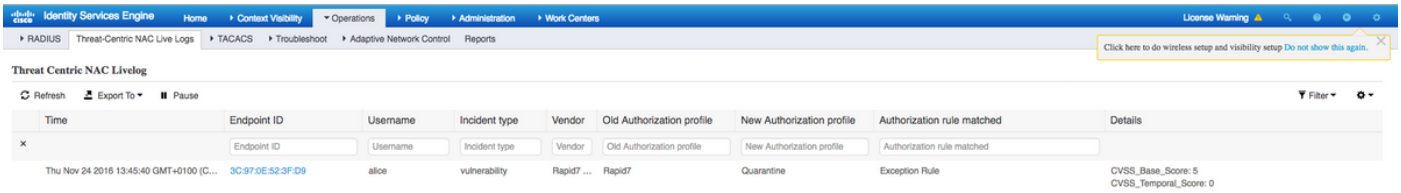
ssl-static-key-ciphers

Title:	TLS/SSL Server Supports The Use of Static Key Ciphers
CVSS score:	2.5999999
CVEIDS:	
Reported by:	Rapid7 Nexpose
Reported at:	Thu Nov 24 05:42:52 CET 2016

rc4-cve-2013-2566

Title:	TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)
CVSS score:	4.30000019
CVEIDS:	CVE-2013-2566
Reported by:	Rapid7 Nexpose
Reported at:	Thu Nov 24 05:42:52 CET 2016

在Operations > TC-NAC Live Logs中，您可以檢視應用的授權策略以及CVSS_Base_Score的詳細資訊。



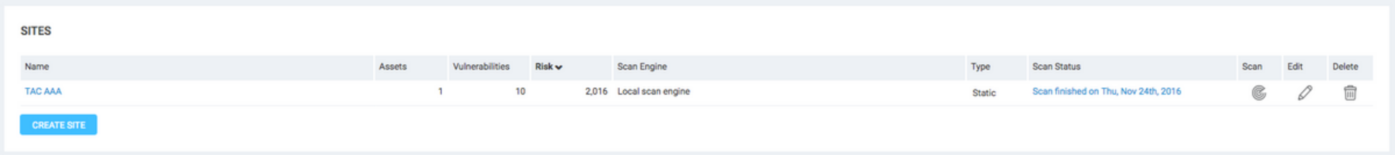
Click here to do wireless setup and visibility setup Do not show this again.

Threat Centric NAC Livelog

Time	Endpoint ID	Username	Incident type	Vendor	Old Authorization profile	New Authorization profile	Authorization rule matched	Details
Thu Nov 24 2016 13:45:40 GMT+0100 (C...	3C:97:0E:52:3F:D9	alice	vulnerability	Rapid7 ...	Rapid7	Quarantine	Exception Rule	CVSS_Base_Score: 5 CVSS_Temporal_Score: 0

附件掃描器

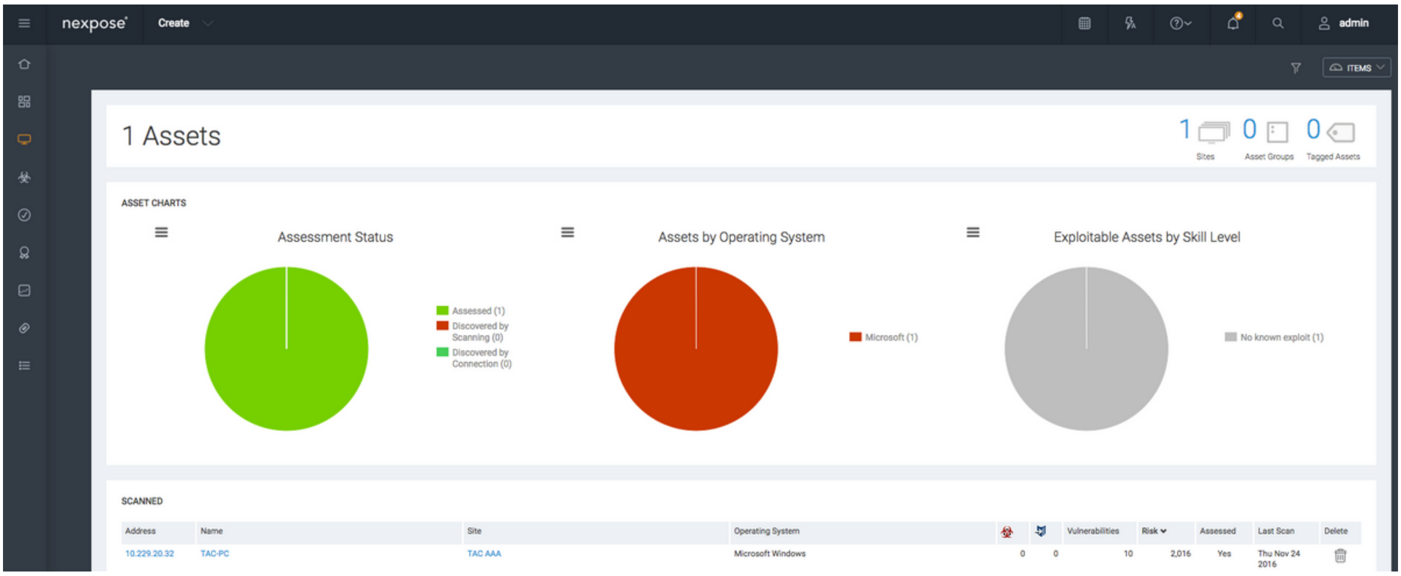
當TC-NAC附件掃描觸發VA掃描轉變為**In-Progress**狀態，並且掃描器開始探測端點時，如果您在端點上運行wireshark捕獲，此時您會看到端點與掃描器之間的資料包交換。掃描程式完成後，結果可在**首頁**下找到。



SITES

Name	Assets	Vulnerabilities	Risk	Scan Engine	Type	Scan Status	Scan	Edit	Delete
TAC AAA	1	10	2,016	Local scan engine	Static	Scan finished on Thu, Nov 24th, 2016			

在**Assets**頁面下，您可以看到有新的終端可用於掃描結果，已標識作業系統，並且檢測到10個漏洞。

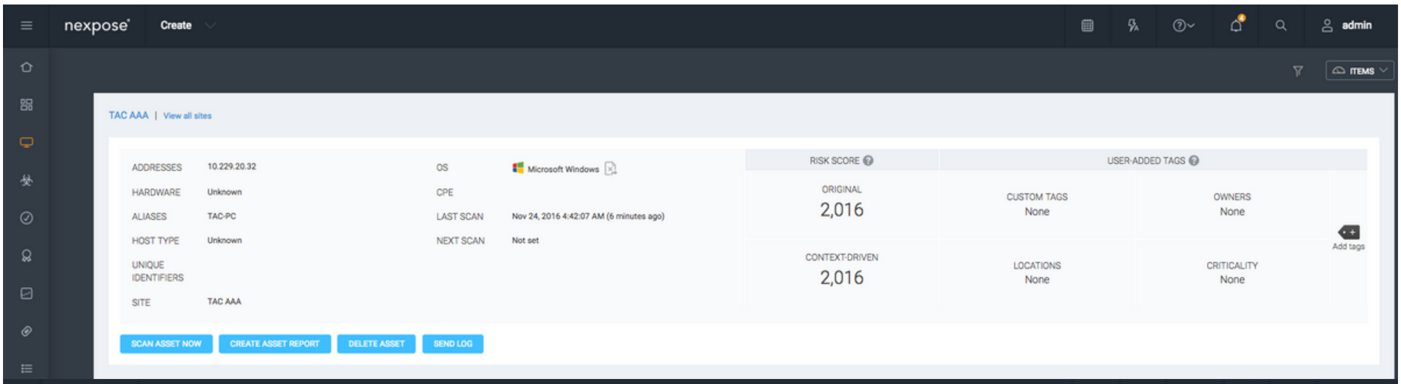


1 Assets

SCANNED

Address	Name	Site	Operating System			Vulnerabilities	Risk	Assessed	Last Scan	Delete
10.229.20.32	TAC-PC	TAC AAA	Microsoft Windows	0	0	10	2,016	Yes	Thu Nov 24 2016	

當您按一下終端的IP地址時，Nexpose Scanner將帶您進入新的選單，您可以在其中看到包括主機名、Risc評分和漏洞詳細清單在內的詳細資訊



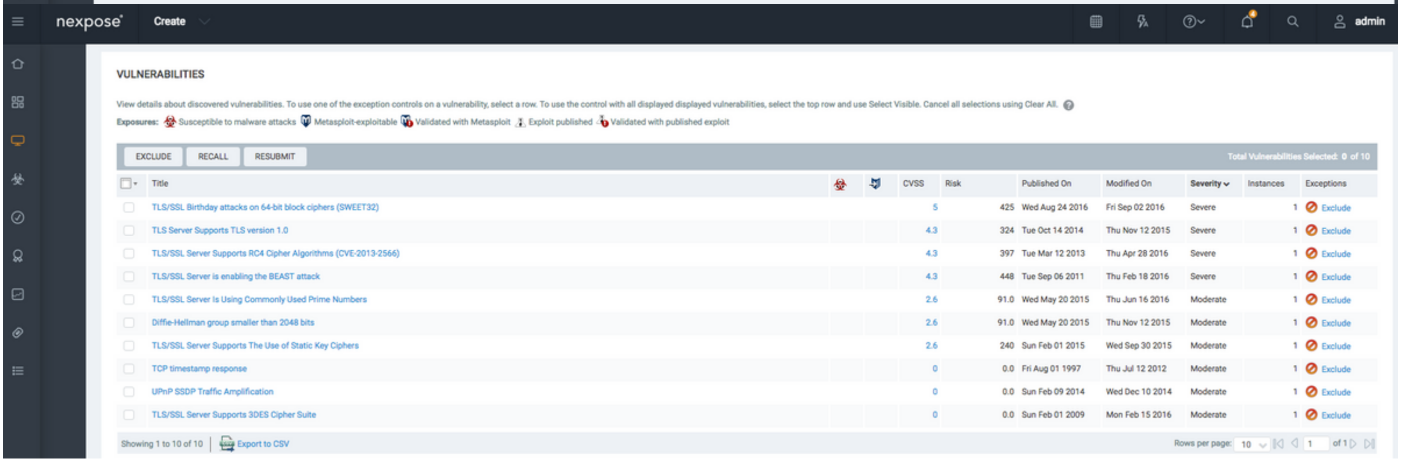
TAC AAA | View all sites

ADDRESSES 10.229.20.32
HARDWARE Unknown
ALIASES TAC-PC
HOST TYPE Unknown
UNIQUE IDENTIFIERS
SITE TAC AAA

OS Microsoft Windows
CPE
LAST SCAN Nov 24, 2016 4:42:07 AM (6 minutes ago)
NEXT SCAN Not set

RISK SCORE
ORIGINAL 2,016
CONTEXT-DRIVEN 2,016

USER-ADDED TAGS
CUSTOM TAGS None
OWNERS None
LOCATIONS None
CRITICALITY None



VULNERABILITIES

View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed displayed vulnerabilities, select the top row and use Select Visible. Cancel all selections using Clear All.

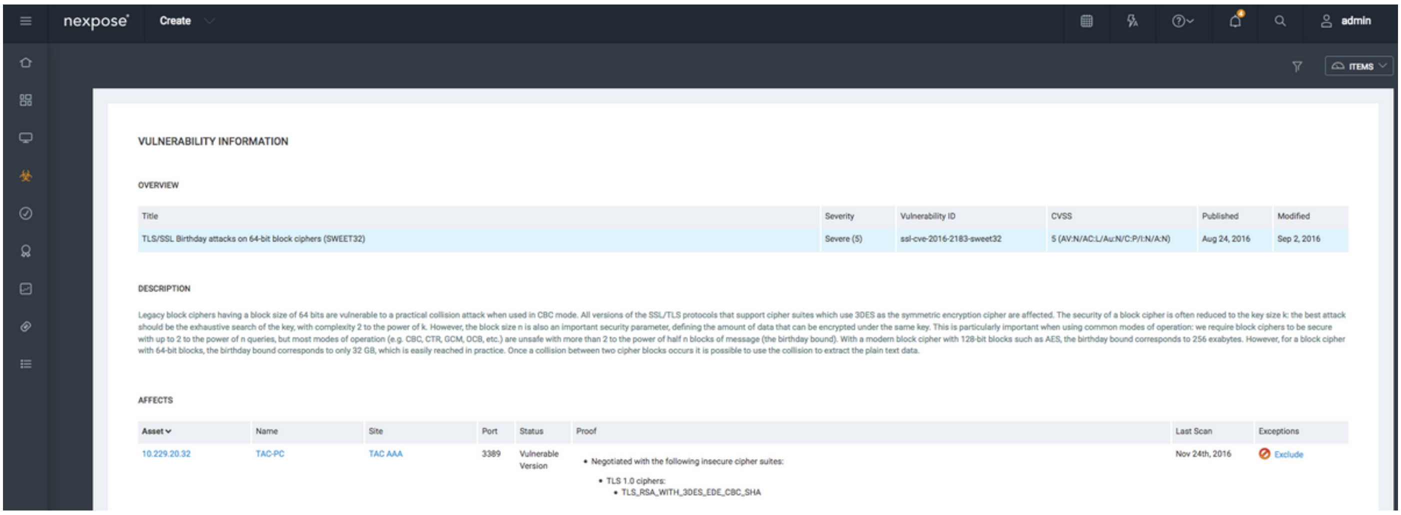
Exposures: Susceptible to malware attacks Metasploit-exploitable Validated with Metasploit Exploit published Validated with published exploit

Total Vulnerabilities Selected: 0 of 10

Title			CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)			5	425	Wed Aug 24 2016	Fri Sep 02 2016	Severe	1	Exclude
TLS Server Supports TLS version 1.0			4.3	324	Tue Oct 14 2014	Thu Nov 12 2015	Severe	1	Exclude
TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566)			4.3	397	Tue Mar 12 2013	Thu Apr 28 2016	Severe	1	Exclude
TLS/SSL Server is enabling the BEAST attack			4.3	448	Tue Sep 06 2011	Thu Feb 18 2016	Severe	1	Exclude
TLS/SSL Server Is Using Commonly Used Prime Numbers			2.6	91.0	Wed May 20 2015	Thu Jun 16 2016	Moderate	1	Exclude
Diffie-Hellman group smaller than 2048 bits			2.6	91.0	Wed May 20 2015	Thu Nov 12 2015	Moderate	1	Exclude
TLS/SSL Server Supports The Use of Static Key Ciphers			2.6	240	Sun Feb 01 2015	Wed Sep 30 2015	Moderate	1	Exclude
TCP timestamp response			0	0.0	Fri Aug 01 1997	Thu Jul 12 2012	Moderate	1	Exclude
UPnP SSDP Traffic Amplification			0	0.0	Sun Feb 09 2014	Wed Dec 10 2014	Moderate	1	Exclude
TLS/SSL Server Supports 3DES Cipher Suite			0	0.0	Sun Feb 01 2009	Mon Feb 15 2016	Moderate	1	Exclude

Showing 1 to 10 of 10 | Export to CSV

按一下**Vulnerability**本身時，圖中顯示完整的說明。



VULNERABILITY INFORMATION

OVERVIEW

Title	Severity	Vulnerability ID	CVSS	Published	Modified
TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)	Severe (5)	ssl-cve-2016-2183-sweet32	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	Aug 24, 2016	Sep 2, 2016

DESCRIPTION

Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of the SSL/TLS protocols that support cipher suites which use 3DES as the symmetric encryption cipher are affected. The security of a block cipher is often reduced to the key size k: the best attack should be the exhaustive search of the key, with complexity 2 to the power of k. However, the block size n is also an important security parameter, defining the amount of data that can be encrypted under the same key. This is particularly important when using common modes of operation: we require block ciphers to be secure with up to 2 to the power of n queries, but most modes of operation (e.g. CBC, CTR, GCM, OCB, etc.) are unsafe with more than 2 to the power of half n blocks of message (the birthday bound). With a modern block cipher with 128-bit blocks such as AES, the birthday bound corresponds to 256 exabytes. However, for a block cipher with 64-bit blocks, the birthday bound corresponds to only 32 GB, which is easily reached in practice. Once a collision between two cipher blocks occurs it is possible to use the collision to extract the plain text data.

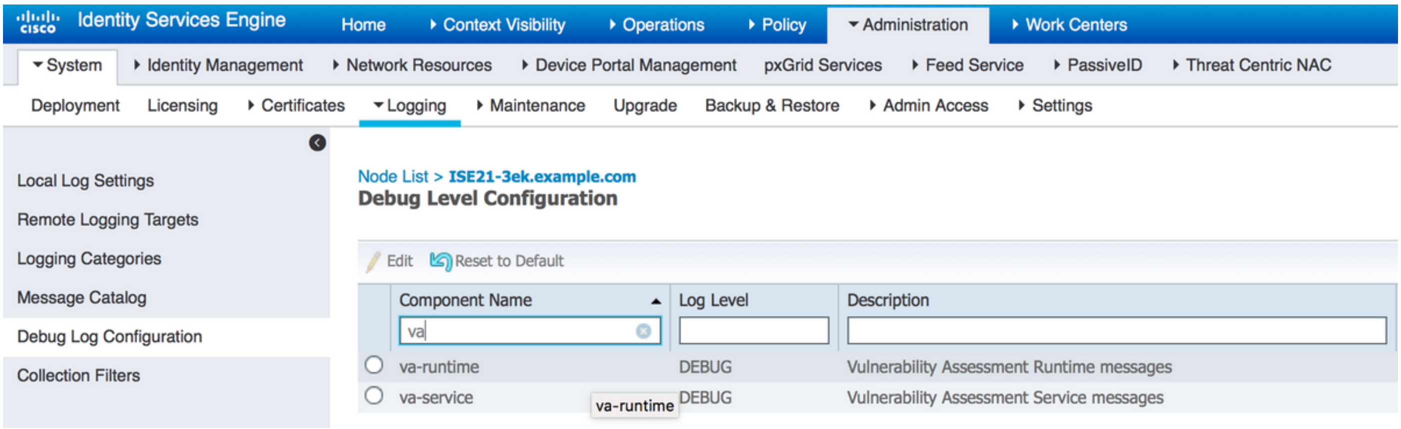
AFFECTS

Asset	Name	Site	Port	Status	Proof	Last Scan	Exceptions
10.229.20.32	TAC-PC	TAC AAA	3389	Vulnerable Version	• Negotiated with the following insecure cipher suites: • TLS 1.0 ciphers: • TLS_RSA_WITH_3DES_EDE_CBC_SHA	Nov 24th, 2016	Exclude

疑難排解

ISE上的調試

要在ISE上啟用調試，請導航到**管理>系統>記錄>調試日誌配置**，選擇TC-NAC節點，並將**日誌級別** va-runtime和**va-service**元件更改為**DEBUG**。



Node List > ISE21-3ek.example.com
Debug Level Configuration

	Component Name	Log Level	Description
	va		
○	va-runtime	DEBUG	Vulnerability Assessment Runtime messages
○	va-service	DEBUG	Vulnerability Assessment Service messages

要檢查的日誌 — varuntime.log。您可以直接從ISE CLI對其進行跟蹤：

```
ISE21-3ek/admin# show logging application varuntime.log tail
```

TC-NAC Docker收到對特定端點執行掃描的指令。

```
2016-11-24 13:32:04,436 DEBUG [Thread-94][] va.runtime.admin.mnt.EndpointFileReader -:::::- VA:
Read va runtime.
[{"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","ondemandScanInt
erval":"48","isPeriodicScanEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"c217
5761-0e2b-4753-b2d6-9a9526d85c0c","psnHostName":"ISE22-1ek","heartBeatTime":0,"lastScanTime":0},
{"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","isPeriodicScanEn
abled":false,"heartBeatTime":0,"lastScanTime":0}]
2016-11-24 13:32:04,437 DEBUG [Thread-94][] va.runtime.admin.vaservice.VaServiceRemotingHandler
-:::::- VA: received data from Mnt:
{"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","ondemandScanInte
rval":"48","isPeriodicScanEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"c2175
761-0e2b-4753-b2d6-9a9526d85c0c","psnHostName":"ISE22-1ek","heartBeatTime":0,"lastScanTime":0}
2016-11-24 13:32:04,439 DEBUG [Thread-94][] va.runtime.admin.vaservice.VaServiceRemotingHandler
```

```
-:::::- VA: received data from Mnt:
{"operationType":1,"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","isPeriodicScanEn
abled":false,"heartBeatTime":0,"lastScanTime":0}
```

收到結果後，它會將所有漏洞資料儲存在上下文目錄中。

```
2016-11-24 13:45:28,378 DEBUG [Thread-94][] va.runtime.admin.vaservice.VaServiceRemotingHandler
-:::::- VA: received data from Mnt:
{"operationType":2,"isPeriodicScanEnabled":false,"heartBeatTime":1479991526437,"lastScanTime":0}
2016-11-24 13:45:33,642 DEBUG [pool-115-thread-19][]
va.runtime.admin.vaservice.VaServiceMessageListener -:::::- Got message from VaService:
[{"macAddress":"3C:97:0E:52:3F:D9","ipAddress":"10.229.20.32","lastScanTime":1479962572758,"vuln
erabilities":["{\"vulnerabilityId\":\"ssl-cve-2016-2183-sweet32\",\"cveIds\":\"CVE-2016-
2183\",\"cvssBaseScore\":\"5\",\"vulnerabilityTitle\":\"TLS/SSL Birthday attacks on 64-bit block
ciphers (SWEET32)\",\"vulnerabilityVendor\":\"Rapid7 Nexpose\"}","{\"vulnerabilityId\":\"ssl-
static-key-
ciphers\",\"cveIds\":\"\",\"cvssBaseScore\":\"2.5999999\",\"vulnerabilityTitle\":\"TLS/SSL
Server Supports The Use of Static Key Ciphers\",\"vulnerabilityVendor\":\"Rapid7
Nexpose\"}","{\"vulnerabilityId\":\"rc4-cve-2013-2566\",\"cveIds\":\"CVE-2013-
2566\",\"cvssBaseScore\":\"4.30000019\",\"vulnerabilityTitle\":\"TLS/SSL Server Supports RC4
Cipher Algorithms (CVE-2013-2566)\",\"vulnerabilityVendor\":\"Rapid7
Nexpose\"}","{\"vulnerabilityId\":\"tls-dh-prime-under-2048-
bits\",\"cveIds\":\"\",\"cvssBaseScore\":\"2.5999999\",\"vulnerabilityTitle\":\"Diffie-Hellman
group smaller than 2048 bits\",\"vulnerabilityVendor\":\"Rapid7
Nexpose\"}","{\"vulnerabilityId\":\"tls-dh-
primes\",\"cveIds\":\"\",\"cvssBaseScore\":\"2.5999999\",\"vulnerabilityTitle\":\"TLS/SSL Server
Is Using Commonly Used Prime Numbers\",\"vulnerabilityVendor\":\"Rapid7
Nexpose\"}","{\"vulnerabilityId\":\"ssl-cve-2011-3389-beast\",\"cveIds\":\"CVE-2011-
3389\",\"cvssBaseScore\":\"4.30000019\",\"vulnerabilityTitle\":\"TLS/SSL Server is enabling the
BEAST attack\",\"vulnerabilityVendor\":\"Rapid7 Nexpose\"}","{\"vulnerabilityId\":\"tlsv1_0-
enabled\",\"cveIds\":\"\",\"cvssBaseScore\":\"4.30000019\",\"vulnerabilityTitle\":\"TLS Server
Supports TLS version 1.0\",\"vulnerabilityVendor\":\"Rapid7 Nexpose\"}"]}]
2016-11-24 13:45:33,643 DEBUG [pool-115-thread-19][]
va.runtime.admin.vaservice.VaServiceMessageListener -:::::- VA: Save to context db,
lastscantime: 1479962572758, mac: 3C:97:0E:52:3F:D9
2016-11-24 13:45:33,675 DEBUG [pool-115-thread-19][]
va.runtime.admin.vaservice.VaPanRemotingHandler -:::::- VA: Saved to elastic search:
{3C:97:0E:52:3F:D9=[{"vulnerabilityId":"ssl-cve-2016-2183-sweet32","cveIds":"CVE-2016-
2183","cvssBaseScore":"5","vulnerabilityTitle":"TLS/SSL Birthday attacks on 64-bit block ciphers
(SWEET32)","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"ssl-static-key-
ciphers","cveIds":"","cvssBaseScore":"2.5999999","vulnerabilityTitle":"TLS/SSL Server Supports
The Use of Static Key Ciphers","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"rc4-
cve-2013-2566","cveIds":"CVE-2013-
2566","cvssBaseScore":"4.30000019","vulnerabilityTitle":"TLS/SSL Server Supports RC4 Cipher
Algorithms (CVE-2013-2566)","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"tls-dh-
prime-under-2048-bits","cveIds":"","cvssBaseScore":"2.5999999","vulnerabilityTitle":"Diffie-
Hellman group smaller than 2048 bits","vulnerabilityVendor":"Rapid7 Nexpose"},
{"vulnerabilityId":"tls-dh-
primes","cveIds":"","cvssBaseScore":"2.5999999","vulnerabilityTitle":"TLS/SSL Server Is Using
Commonly Used Prime Numbers","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"ssl-
cve-2011-3389-beast","cveIds":"CVE-2011-
3389","cvssBaseScore":"4.30000019","vulnerabilityTitle":"TLS/SSL Server is enabling the BEAST
attack","vulnerabilityVendor":"Rapid7 Nexpose"}, {"vulnerabilityId":"tlsv1_0-
enabled","cveIds":"","cvssBaseScore":"4.30000019","vulnerabilityTitle":"TLS Server Supports TLS
version 1.0","vulnerabilityVendor":"Rapid7 Nexpose"}]}
```

要檢查的日誌 — vaservice.log。您可以直接從ISE CLI對其進行跟蹤：

```
ISE21-3ek/admin# show logging application vaservice.log tail
```

漏洞評估請求已提交至介面卡。

```
2016-11-24 12:32:05,783 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -
:::::- VA SendSyslog systemMsg :
[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA request submitted to
adapter","TC-NAC.Details","VA request submitted to adapter for processing","TC-
NAC.MACAddress","3C:97:0E:52:3F:D9","TC-NAC.IpAddress","10.229.20.32","TC-
NAC.AdapterInstanceUuid","c2175761-0e2b-4753-b2d6-9a9526d85c0c","TC-NAC.VendorName","Rapid7
Nexpose","TC-NAC.AdapterInstanceName","Rapid7"]}]
2016-11-24 12:32:05,810 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -
:::::- VA SendSyslog systemMsg res: {"status":"SUCCESS","statusMessages":["SUCCESS"]}
```

AdapterMessageListener每隔5分鐘檢查一次掃描的狀態，直到掃描完成。

```
2016-11-24 12:36:28,143 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::- Message from adapter :
{"AdapterInstanceName":"Rapid7","AdapterInstanceUid":"7a2415e7-980d-4c0c-b5ed-
fe4e9fadadbd","VendorName":"Rapid7 Nexpose","OperationMessageText":"Number of endpoints queued
for checking scan results: 0, Number of endpoints queued for scan: 0, Number of endpoints for
which the scan is in progress: 1"}
2016-11-24 12:36:28,880 DEBUG [endpointPollerScheduler-5][] cpm.va.service.util.VaServiceUtil -
:::::- VA SendSyslog systemMsg :
[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","Adapter Statistics","TC-
NAC.Details","Number of endpoints queued for checking scan results: 0, Number of endpoints
queued for scan: 0, Number of endpoints for which the scan is in progress: 1","TC-
NAC.AdapterInstanceUuid","7a2415e7-980d-4c0c-b5ed-fe4e9fadadbd","TC-NAC.VendorName","Rapid7
Nexpose","TC-NAC.AdapterInstanceName","Rapid7"]}]
```

介面卡獲得CVE以及CVSS分數。

```
2016-11-24 12:45:33,132 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::- Message from adapter :
{"returnedMacAddress":"","requestedMacAddress":"3C:97:0E:52:3F:D9","scanStatus":"ASSESSMENT_SUCC
ESS","lastScanTimeLong":1479962572758,"ipAddress":"10.229.20.32","vulnerabilities":[{"vulnerabil
ityId":"tlsv1_0-enabled","cveIds":"","cvssBaseScore":"4.30000019","vulnerabilityTitle":"TLS
Server Supports TLS version 1.0","vulnerabilityVendor":"Rapid7
Nexpose"},{"vulnerabilityId":"rc4-cve-2013-2566","cveIds":"CVE-2013-
2566","cvssBaseScore":"4.30000019","vulnerabilityTitle":"TLS/SSL Server Supports RC4 Cipher
Algorithms (CVE-2013-2566)","vulnerabilityVendor":"Rapid7 Nexpose"},{"vulnerabilityId":"ssl-cve-
2016-2183-sweet32","cveIds":"CVE-2016-2183","cvssBaseScore":"5","vulnerabilityTitle":"TLS/SSL
Birthday attacks on 64-bit block ciphers (SWEET32)","vulnerabilityVendor":"Rapid7
Nexpose"},{"vulnerabilityId":"ssl-static-key-
ciphers","cveIds":"","cvssBaseScore":"2.5999999","vulnerabilityTitle":"TLS/SSL Server Supports
The Use of Static Key Ciphers","vulnerabilityVendor":"Rapid7 Nexpose"},{"vulnerabilityId":"tls-
dh-primes","cveIds":"","cvssBaseScore":"2.5999999","vulnerabilityTitle":"TLS/SSL Server Is Using
Commonly Used Prime Numbers","vulnerabilityVendor":"Rapid7 Nexpose"},{"vulnerabilityId":"tls-dh-
prime-under-2048-bits","cveIds":"","cvssBaseScore":"2.5999999","vulnerabilityTitle":"Diffie-
Hellman group smaller than 2048 bits","vulnerabilityVendor":"Rapid7
Nexpose"},{"vulnerabilityId":"ssl-cve-2011-3389-beast","cveIds":"CVE-2011-
3389","cvssBaseScore":"4.30000019","vulnerabilityTitle":"TLS/SSL Server is enabling the BEAST
attack","vulnerabilityVendor":"Rapid7 Nexpose"}]}
2016-11-24 12:45:33,137 INFO [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::- Endpoint Details sent to IRF is
{"3C:97:0E:52:3F:D9":[{"vulnerability":{"CVSS_Base_Score":5.0,"CVSS_Temporal_Score":0.0},"time-
stamp":1479962572758,"title":"Vulnerability","vendor":"Rapid7 Nexpose"}]}
2016-11-24 12:45:33,221 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -
:::::- VA SendSyslog systemMsg :
[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA successfully
completed","TC-NAC.Details","VA completed; number of vulnerabilities found: 7","TC-
NAC.MACAddress","3C:97:0E:52:3F:D9","TC-NAC.IpAddress","10.229.20.32","TC-
NAC.AdapterInstanceUuid","c2175761-0e2b-4753-b2d6-9a9526d85c0c","TC-NAC.VendorName","Rapid7
Nexpose","TC-NAC.AdapterInstanceName","Rapid7"]}]
2016-11-24 12:45:33,299 DEBUG [endpointPollerScheduler-7][] cpm.va.service.util.VaServiceUtil -
:::::- VA SendSyslog systemMsg res: {"status":"SUCCESS","statusMessages":["SUCCESS"]}
```

相關資訊

- 技術支援與文件 - Cisco Systems
- ISE 2.2版本說明
- ISE 2.2硬體安裝指南
- ISE 2.2升級指南
- ISE 2.2引擎管理員指南