

# Qualys로 ISE 2.1 Threat-Centric NAC(TC-NAC) 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[상위 레벨 플로우 다이어그램](#)

[Qualys 클라우드 및 스캐너 구성](#)

[1단계. Qualys 스캐너 구축](#)

[2단계. Qualys 스캐너 구성](#)

[ISE 구성](#)

[1단계. ISE와의 통합을 위한 Qualys 클라우드 설정 조정](#)

[2단계. TC-NAC 서비스 활성화](#)

[3단계. ISE VA 프레임워크에 대한 Qualys 어댑터 연결 구성](#)

[4단계. VA 스캔을 트리거하도록 권한 부여 프로파일 구성](#)

[5단계. 권한 부여 정책 구성](#)

[다음을 확인합니다.](#)

[Identity Services Engine](#)

[Qualys 클라우드](#)

[문제 해결](#)

[ISE의 디버깅](#)

[일반적인 문제](#)

[참조](#)

## 소개

이 문서에서는 Threat-Centric NAC를 ISE(Identity Services Engine) 2.1에서 Qualys로 구성하는 방법에 대해 설명합니다. TC-NAC(Threat Centric Network Access Control) 기능을 사용하면 위협 및 취약성 어댑터에서 수신한 위협 및 취약성 특성을 기반으로 권한 부여 정책을 생성할 수 있습니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- Cisco Identity Service Engine
- Qualys ScanGuard

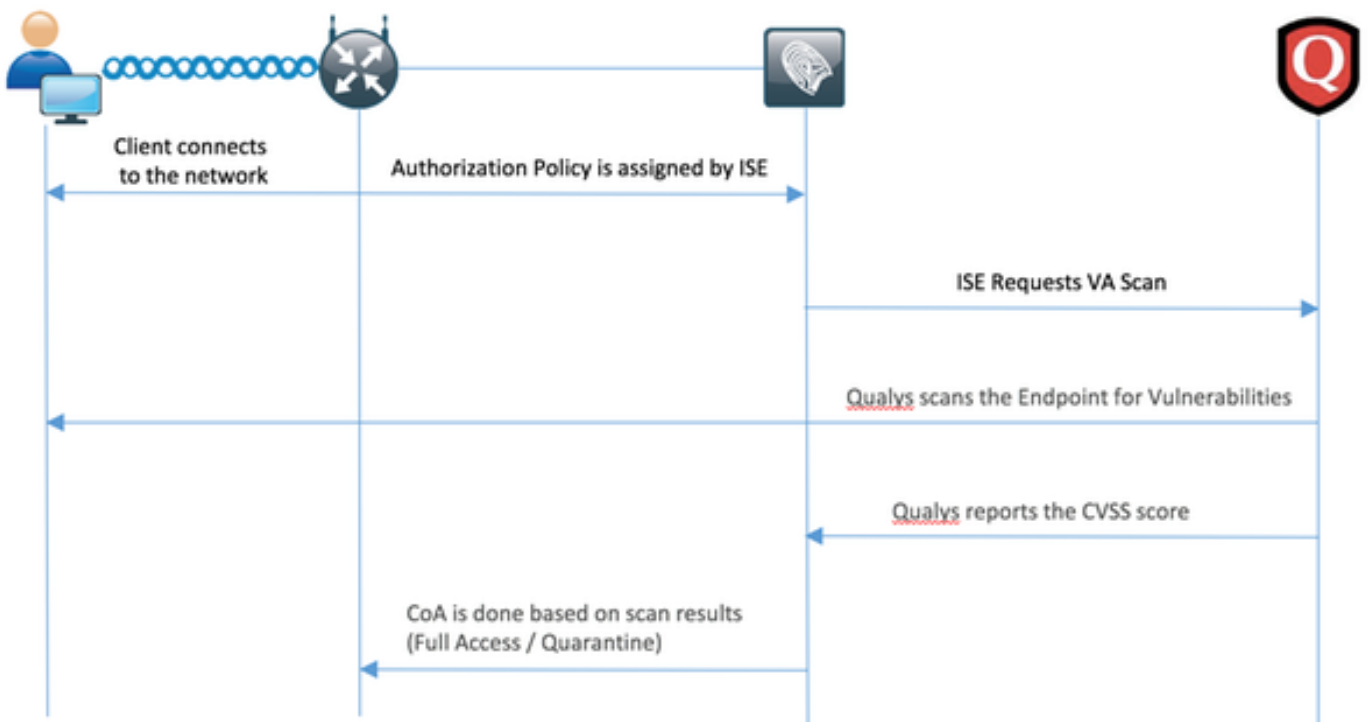
## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Service Engine 버전 2.1
- WLC(Wireless LAN Controller) 8.0.121.0
- Qualys Guard Scanner 8.3.36-1, 서명 2.3.364-2
- Windows 7 서비스 팩 1

## 구성

### 상위 레벨 플로우 다이어그램



다음은 플로우입니다.

1. 클라이언트가 네트워크에 연결되고, 제한된 액세스가 부여되며, Assessment Vulnerabilities(취약성 평가) 확인란이 활성화된 프로파일이 할당됩니다.
2. PSN 노드가 Syslog 메시지를 MNT 노드로 전송하여 인증이 수행되었고 VA 스캔은 권한 부여 정책의 결과임
3. MNT 노드는 다음 데이터를 사용하여 TC-NAC 노드(Admin WebApp 사용)에 SCAN을 제출합니다.
  - MAC 주소
  - IP 주소
  - 스캔 간격
  - 정기 검사 사용
  - 원래 PSN
4. Qualys TC-NAC(Docker 컨테이너에서 캡슐화)는 Qualys Cloud(REST API를 통해)와 통신하여 필요한 경우 스캔을 트리거합니다.

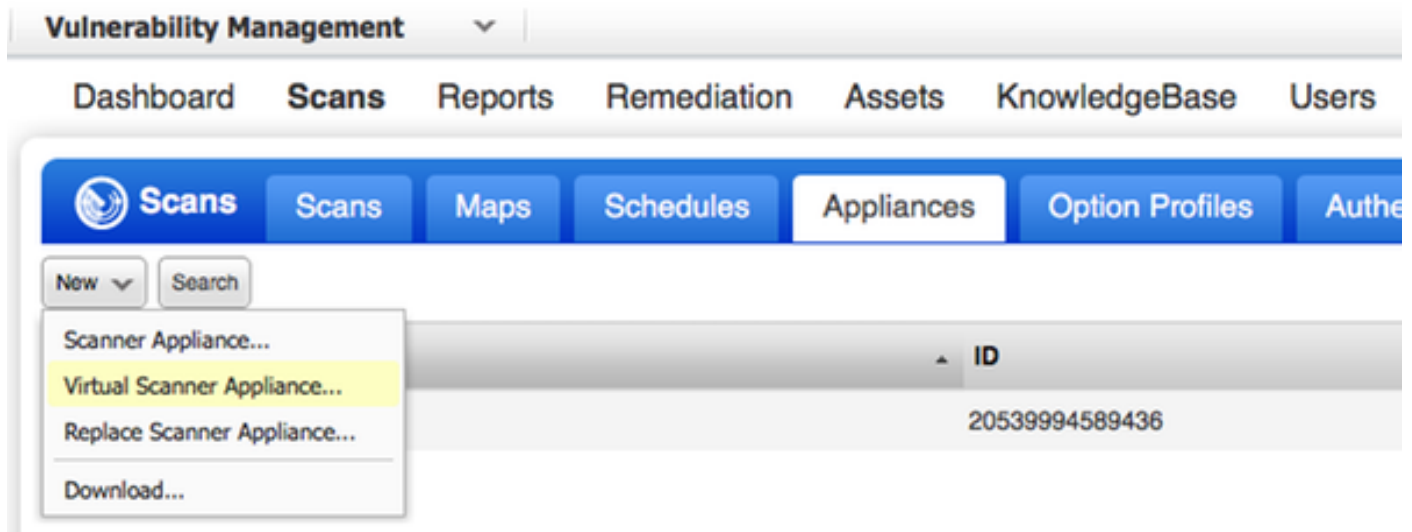
5. Qualys Cloud는 엔드포인트를 스캔하도록 Qualys Scanner에 지시합니다.
6. Qualys Scanner는 스캔 결과를 Qualys Cloud로 전송합니다.
7. 스캔 결과는 TC-NAC로 다시 전송됩니다.
  - MAC 주소
  - 모든 CVSS 점수
  - 모든 취약성(QID, 제목, CVEID)
8. TC-NAC는 7단계의 모든 데이터로 PAN을 업데이트합니다.
9. CoA는 필요한 경우 구성된 권한 부여 정책에 따라 트리거됩니다.

## Qualys 클라우드 및 스캐너 구성

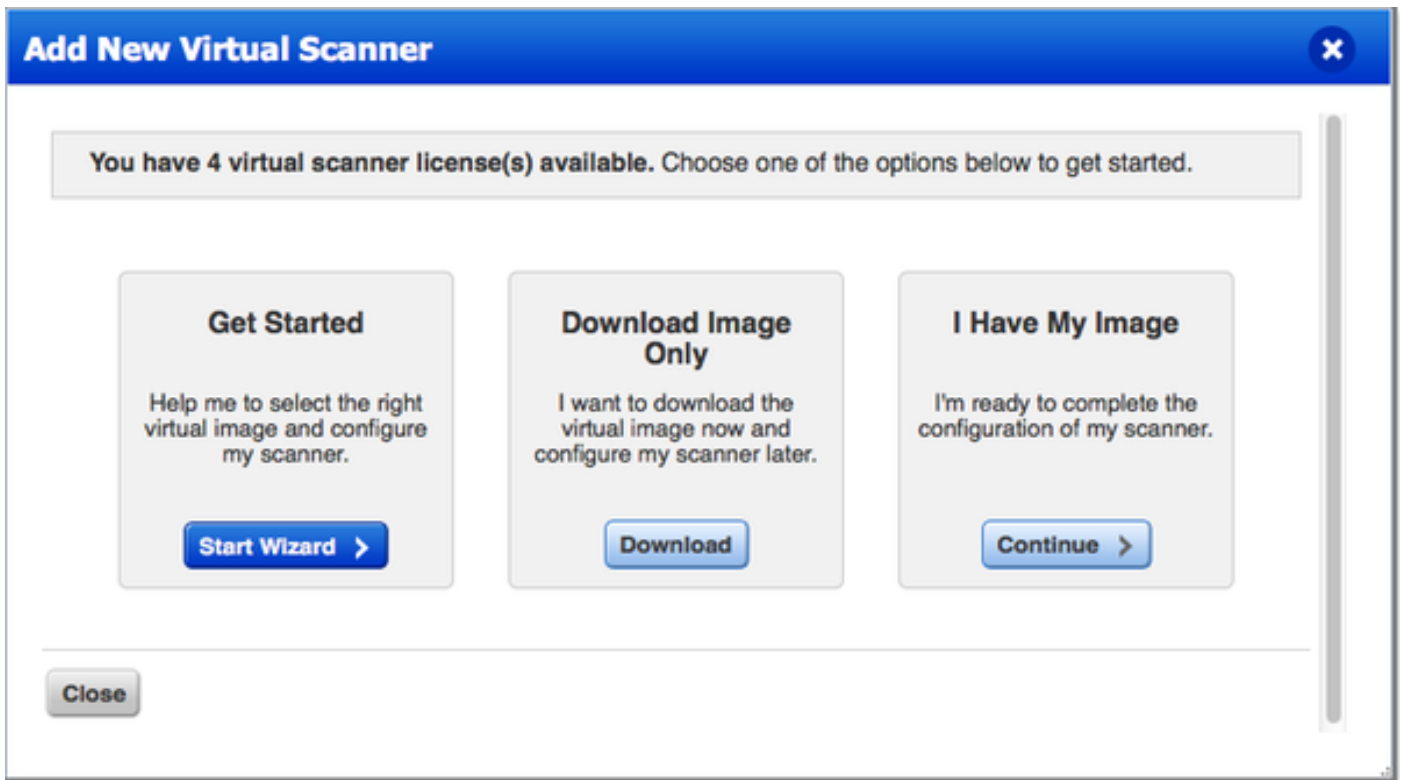
**주의:**이 문서의 Qualys 컨피그레이션은 랩 용도로 작성되었습니다. 설계 고려 사항은 Qualys 엔지니어에게 문의하십시오.

### 1단계. Qualys 스캐너 구축

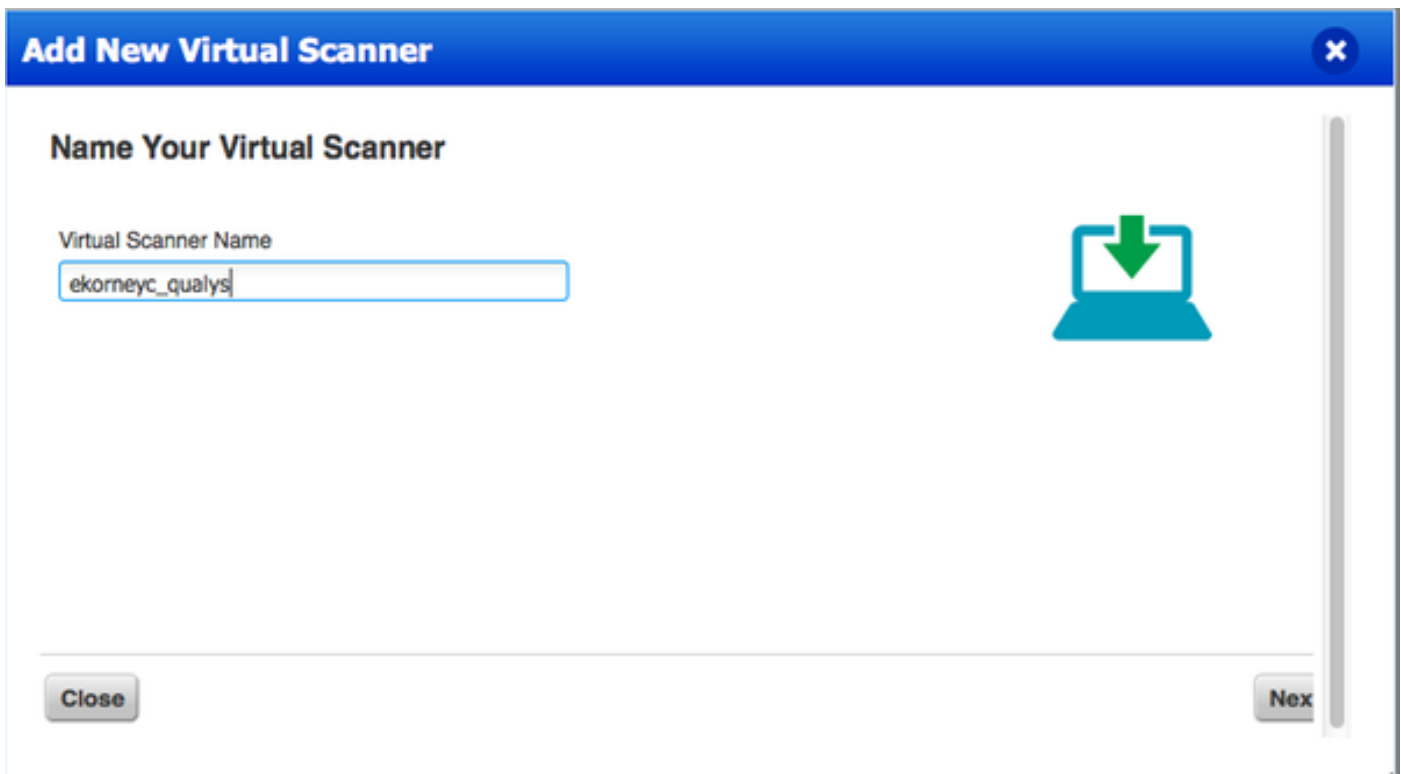
Qualys 스캐너는 OVA 파일에서 구축할 수 있습니다. Qualys 클라우드에 로그인하고 Scans(스캔) > Appliances(어플라이언스)로 이동한 다음 New(새로 만들기) > Virtual Scanner Appliance(가상 스캐너 어플라이언스)를 선택합니다.



Download Image Only(이미지만 다운로드)를 선택하고 적절한 배포를 선택합니다.



활성화 코드를 가져오려면 Scans(스캔) > Appliances(어플라이언스)로 이동하여 New(새로 만들기) > Virtual Scanner Appliance(가상 스캐너 어플라이언스)를 선택하고 I Have My Image(내 이미지 있음)를 선택할 수 있습니다.



스캐너 이름을 입력하면 나중에 사용할 인증 코드가 제공됩니다.

## 2단계. Qualys 스캐너 구성

원하는 가상화 플랫폼에 OVA를 구축합니다. 완료되면 다음 설정을 구성합니다.

- 네트워크(LAN) 설정
- WAN 인터페이스 설정(2개의 인터페이스를 사용하는 경우)
- 프록시 설정(프록시를 사용하는 경우)
- 이 스캐너 사용자 지정



### QualysGuard® Scanner Console

Name: ekorneyc\_qualys, LAN IP: 10.62.145.82

Set up network (LAN) >

Change WAN interface >

Disable WAN interface >

Enable proxy >

Reset network config >

System shutdown >

System reboot >

Version info: 3.11.16.5.11.0

Exit this menu? (Y/N)

#### TIP:

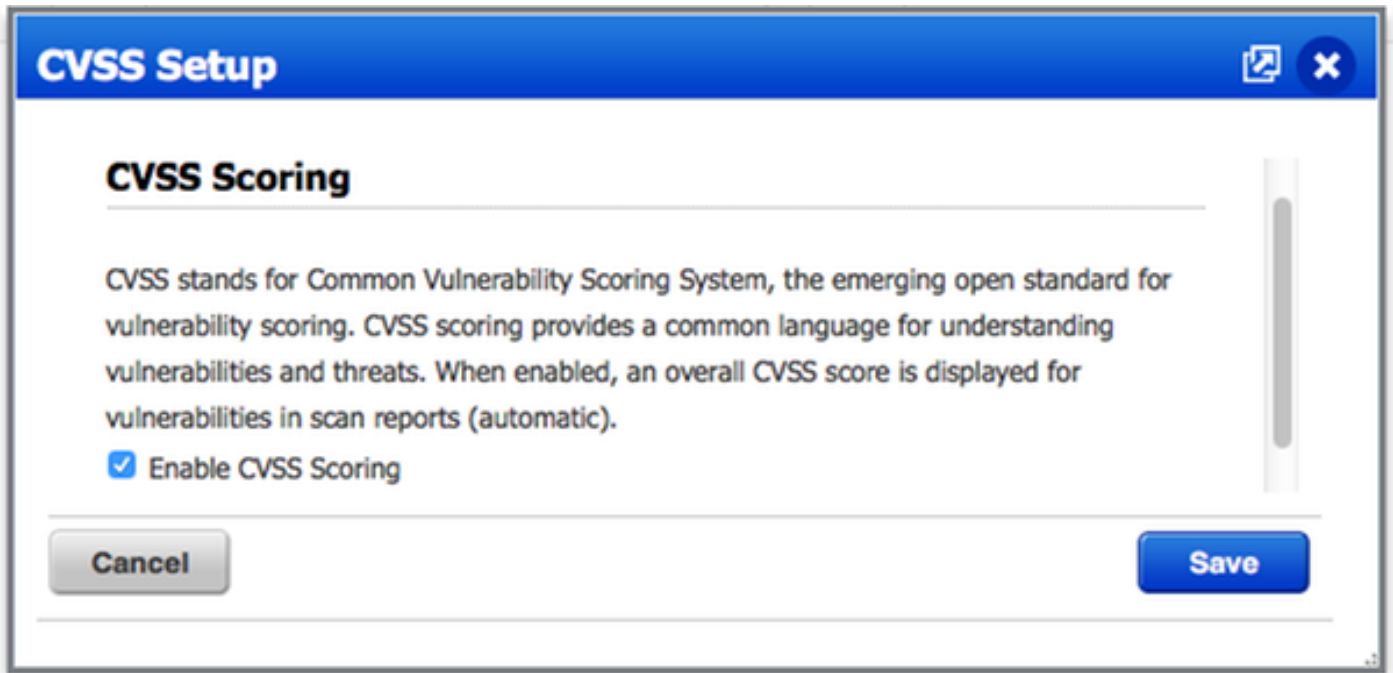
This is the main (top-level) menu of the Virtual Scanner Console.

Press the UP and DOWN arrow keys to navigate the menu.

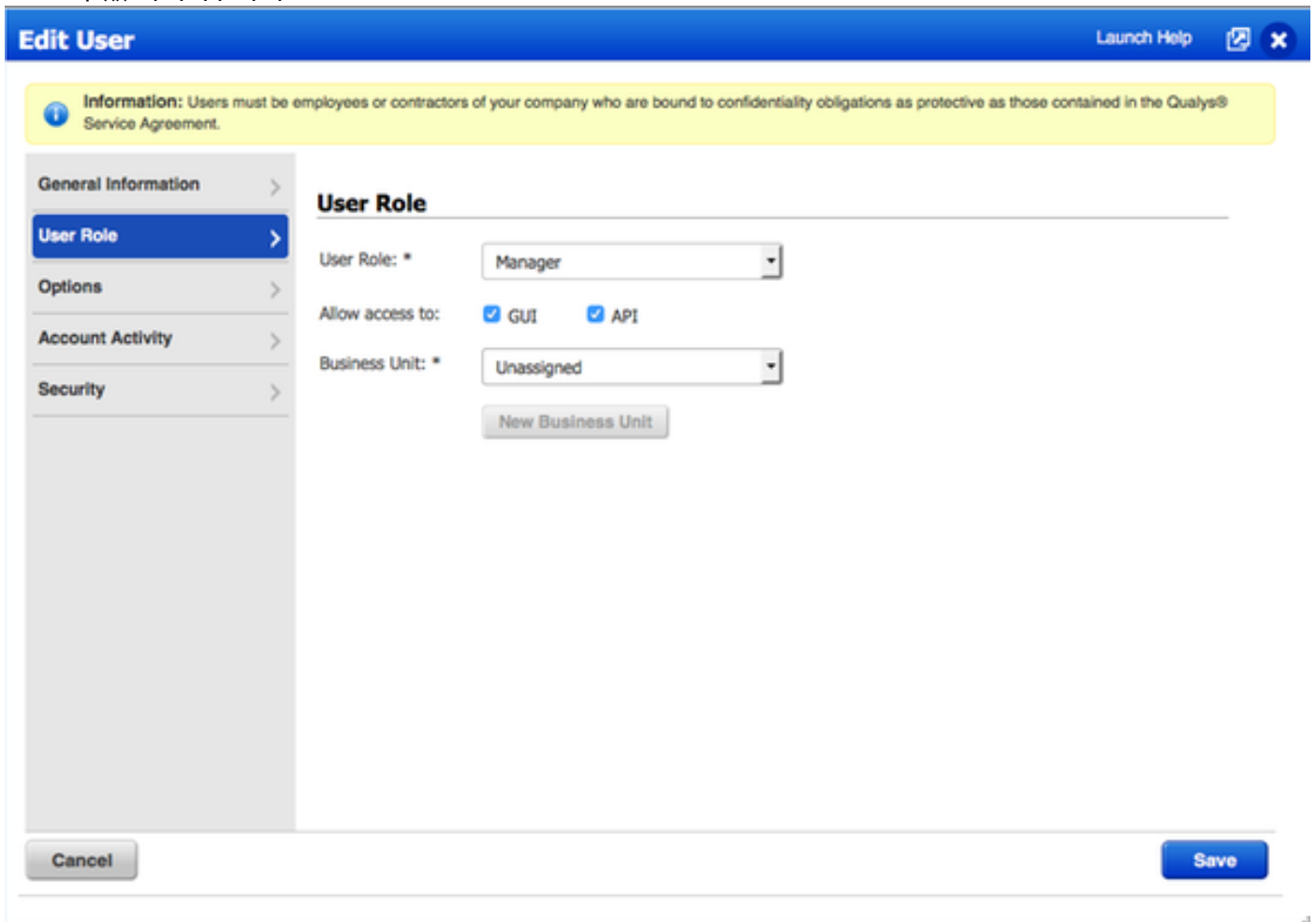
Press the RIGHT arrow or ENTER key to choose a menu item.

이후 스캐너가 Qualys에 연결되고 최신 소프트웨어와 서명을 다운로드합니다.





- 어댑터 구성에 사용된 사용자 자격 증명에 관리자 권한이 있는지 확인합니다. 왼쪽 상단 모서리에서 사용자를 선택하고 **User Profile**(사용자 프로필)을 클릭합니다. **사용자 역할**에 관리자 권한이 있어야 합니다.



- 취약성 평가가 필요한 엔드포인트의 IP 주소/서브넷이 Qualys at Vulnerability Management > Assets > Host Assets > New > IP Tracked Hosts에 추가되었는지 확인합니다.

Help for proper formatting.' Below this is a text input field labeled 'IPs: \*' containing the IP range '10.62.148.1-10.62.148.128'. Underneath the input field is a checkbox labeled 'Add to Policy Compliance Module'. Below the checkbox is an example text '(ex: 192.168.0.200,192.168.0.87-192.168.0.92)'. At the bottom of the main area, it says 'Validate IPs through [Whois](#)'. At the bottom of the window, there are two buttons: 'Cancel' on the left and 'Add' on the right."/>

## 2단계. TC-NAC 서비스 활성화

Administration(관리) > Deployment(구축) > Edit Node(노드 수정)에서 TC-NAC Services(TC-NAC 서비스)를 활성화합니다. 확인 **Threat Centric NAC 서비스 활성화** 확인란을 선택합니다.

**참고:**구축당 TC-NAC 노드는 하나만 있을 수 있습니다.



## Edit Node

General Settings

Profiling Configuration

Hostname **ISE21-3ek**  
 FQDN **ISE21-3ek.example.com**  
 IP Address **10.62.145.25**  
 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

## 3단계. ISE VA 프레임워크에 대한 Qualys 어댑터 연결 구성

Administration(관리) > Threat Centric NAC > Third Party Vendors(서드파티 벤더) > Add(추가)로 이동합니다. Save(저장)를 클릭합니다.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Third Party Vendors

Vendor Instances > New  
 Input fields marked with an asterisk (\*) are required.

Vendor \* Qualys : VA

Instance Name \* QUALYS\_VA

Qualys Instance(Qualys 인스턴스)가 **Ready to configure state**(상태 구성 준비)로 전환되면 Status(상태)에서 **Ready to configure**(구성 준비) 옵션을 클릭합니다.

Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
QUALYS_VA	Qualys	VA		Disconnected	Ready to configure

REST API 호스트는 계정이 있는 Qualys Cloud에 사용하는 호스트여야 합니다. 이 예에서 - qualysguard.qg2.apps.qualys.com

어카운트는 관리자 권한이 있는 어카운트여야 합니다. **Next(다음)**를 클릭합니다.

Vendor Instances > QUALYS\_VA

### Enter Qualys Configuration Details

Enable CVSS Scoring in Qualys (Reports->Setup->CVSS Scoring->Enable CVSS Scoring) and add the IP address of your endpoints in Qualys (Assets > Host Assets)

**REST API Host**  
  
 The hostname of the Qualys platform where your account is located.

**REST API Port**  
  
 The port used by the REST API host.

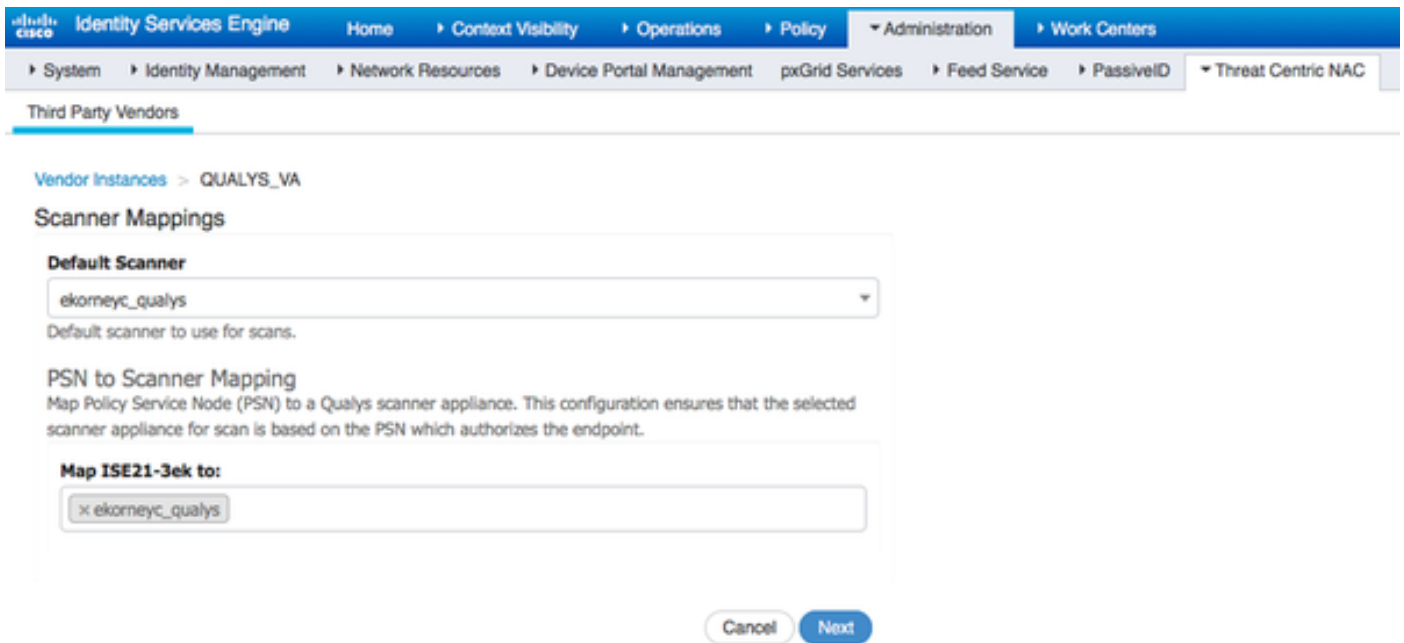
**Username**  
  
 User account with Manager privileges to the Qualys platform.

**Password**  
  
 Password of the user.

**HTTP Proxy Host**  
  
 Optional HTTP Proxy Host. Requires proxy port also to be set.

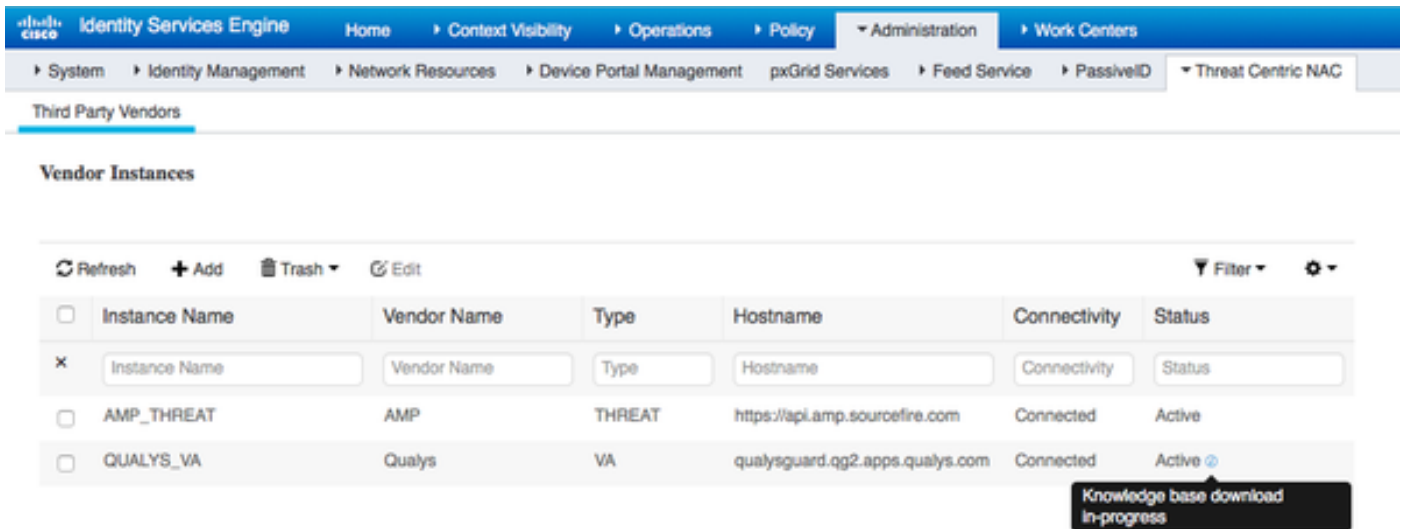
**HTTP Proxy Port**  
  
 Optional HTTP Proxy Port. Requires proxy host also to be set.

ISE는 Qualys Cloud에 연결된 스캐너에 대한 정보를 다운로드합니다. 이 페이지에서 PSN과 스캐너 매핑을 구성할 수 있습니다. 선택한 스캐너가 엔드포인트를 승인하는 PSN을 기반으로 선택되었는지 확인합니다.



고급 설정은 ISE 2.1 관리 가이드에 잘 설명되어 있습니다. 링크는 이 문서의 참조 섹션에서 찾을 수 있습니다. Next(다음)와 Finish(마침)를 클릭합니다. Qualys Instance가 Active 상태 및 지식 기반 다운로드로 전환됩니다.

**참고:**구축당 Qualys 인스턴스는 하나만 있을 수 있습니다.



#### 4단계. VA 스캔을 트리거하도록 권한 부여 프로파일 구성

Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동합니다. 새 프로필을 추가합니다. Common Tasks(공통 작업) 아래에서 Vulnerability Assessment(취약성 평가) 확인란을 선택합니다. 네트워크 설계에 따라 온디맨드 스캔 간격을 선택해야 합니다.

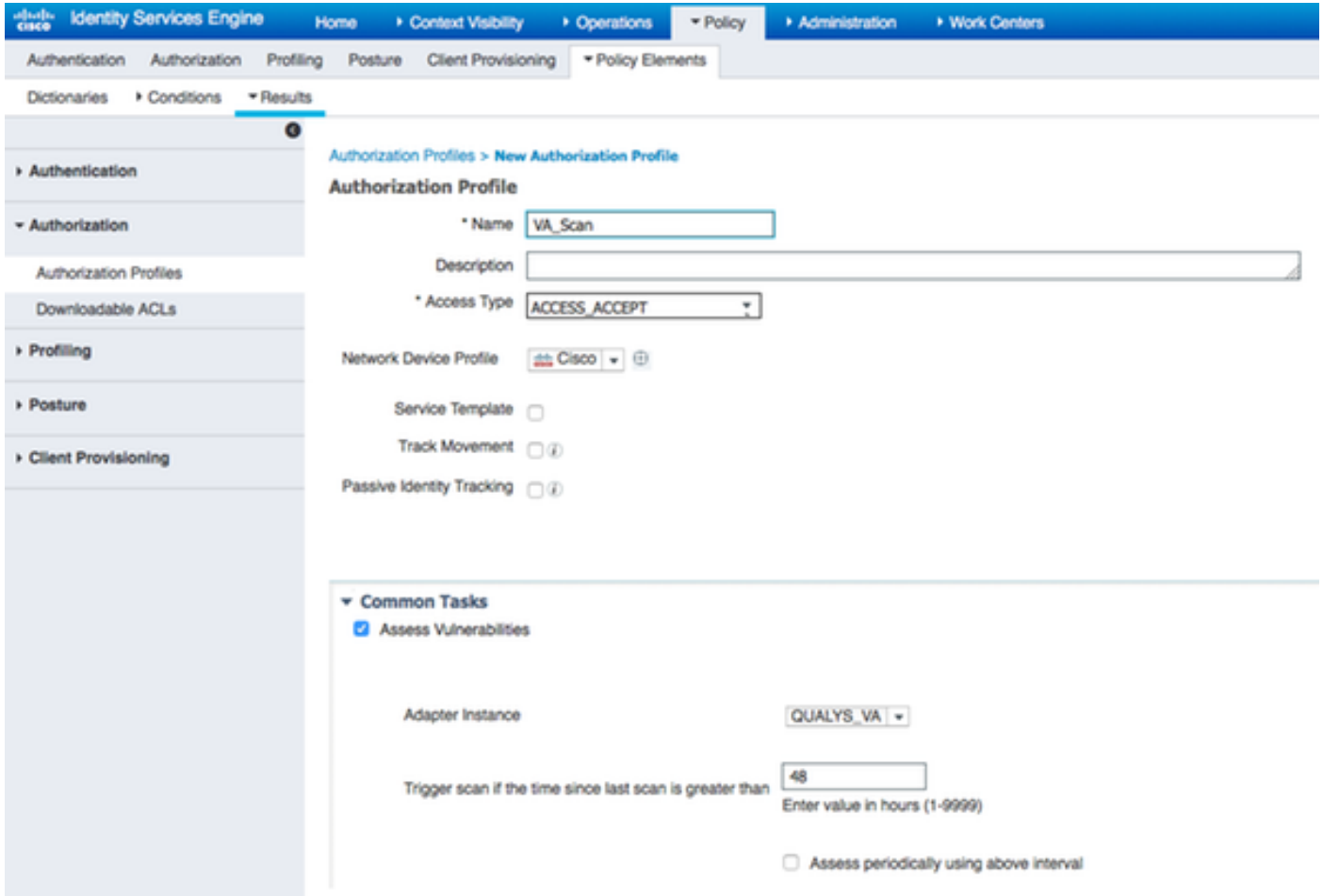
권한 부여 프로파일에는 다음과 같은 av 쌍이 포함되어 있습니다.

cisco-av-pair = on-demand-scan-interval=48

cisco av 쌍 = periodic-scan-enabled=0

cisco-av-pair = va-adapter-instance=796440b7-09b5-4f3b-b611-199fb81a4b99

MNT 노드에 스캔을 트리거해야 한다고 알리는 것이 진정한 목적이지만, 액세스 수락 패킷 내의 네트워크 디바이스로 전송됩니다.MNT는 TC-NAC 노드가 Qualys Cloud와 통신하도록 지시합니다.



## 5단계. 권한 부여 정책 구성

- 4단계에서 구성된 새 권한 부여 프로파일을 사용하도록 권한 부여 정책을 구성합니다. Policy(정책) > Authorization(권한 부여) > Authorization Policy(권한 부여 정책)로 이동하고 **Basic\_Authenticated\_Access** 규칙을 찾은 다음 Edit(수정)를 클릭합니다. PermitAccess에서 새로 생성된 **Standard VA\_Scan**으로 권한을 변경합니다. 이로 인해 모든 사용자에게 대한 취약성 검사가 수행됩니다. Save(저장)를 클릭합니다.
- 격리된 컴퓨터에 대한 권한 부여 정책을 만듭니다. Policy(정책) > Authorization(권한 부여) > Authorization Policy(권한 부여 정책) > Exceptions(예외)로 이동하고 **Exception Rule(예외 규칙)**을 생성합니다. Conditions(조건) > Create New Condition (Advanced Option)(새 조건 생성(고급 옵션)) > Select Attribute(특성 선택)를 클릭하고 아래로 스크롤하여 **Threat**를 선택합니다. Threat 특성을 확장하고 **Qualys-CVSS\_Base\_Score**를 선택합니다. 연산자를 **Greater Than(보다 큼)**으로 변경하고 보안 정책에 따라 값을 입력합니다. **쿼린틴** 권한 부여 프로파일은 취약한 시스템에 제한된 액세스를 제공해야 합니다.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

### 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 ThreatQualys-CVSS_Base_Score GREATER 8	then Quarantine

Standard

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

다음을 확인합니다.

## Identity Services Engine

첫 번째 연결은 VA Scan을 트리거합니다.검사가 완료되면 CoA 재인증이 트리거되어 일치하는 새 정책을 적용합니다.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

RADIUS TC-MAC Live Logs TACACS Reports Troubleshoot Adaptive Network Control

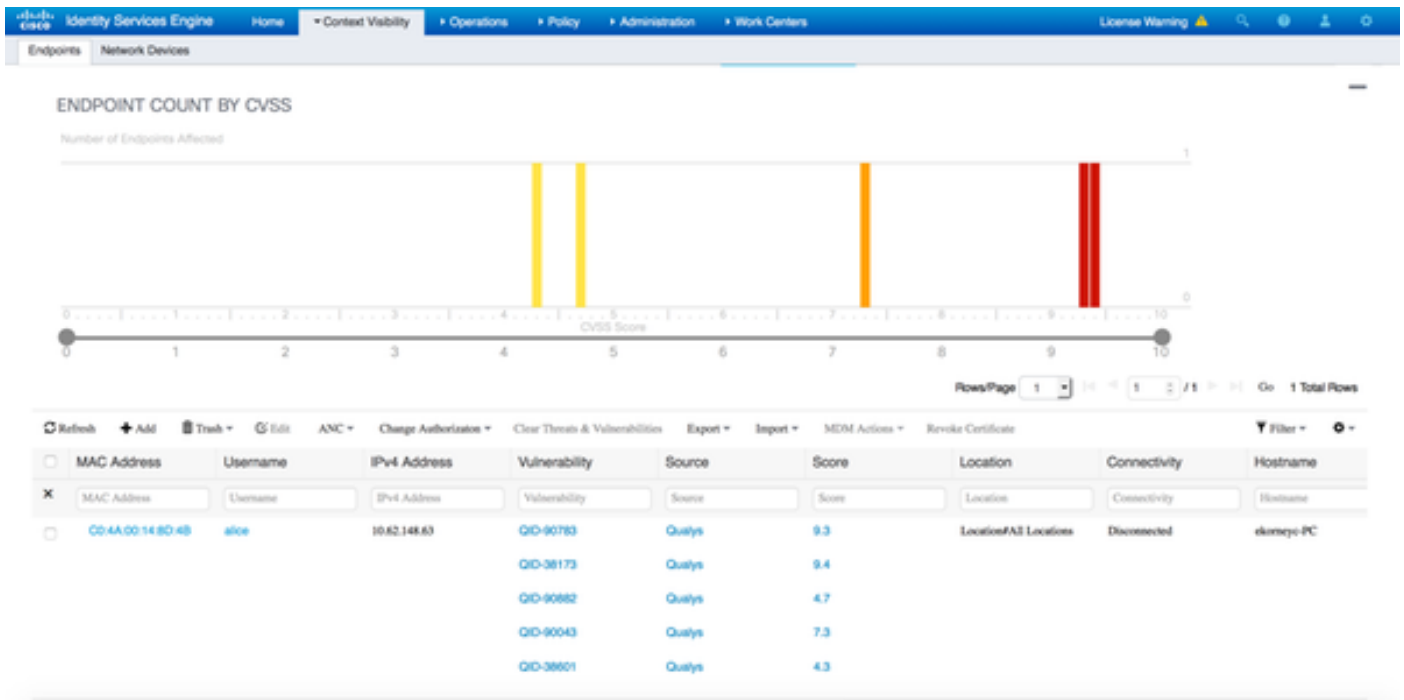
Live Logs Live Sessions

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

Refresh Reset Repeat Counts Export To

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati
Jun 28, 2016 07:25:10:971 PM	Auth Pass			alice	CO-4A:00:14:8D:4B	Endpoint Profi	Authentication Policy	Authorization Policy	Authorization
Jun 28, 2016 07:25:07:065 PM	Auth Pass			alice	CO-4A:00:14:8D:4B	Microsoft-Wo...	Default >> Dot1X >> Default	Default >> Exception Rule	Quarantine
Jun 28, 2016 07:06:23:437 PM	Auth Pass			alice	CO-4A:00:14:8D:4B	TP-LINK De...	Default >> Dot1X >> Default	Default >> Basic_Authenticated_Access	VA_Scan

탐지된 취약성을 확인하려면 Context Visibility(상황 가시성) > Endpoints(엔드포인트)로 이동합니다.Qualys에서 제공한 점수를 사용하여 엔드포인트별 취약성을 확인합니다.



특정 엔드포인트를 선택할 때 Title 및 CVEID를 비롯한 각 취약성에 대한 자세한 내용이 나타납니다

The screenshot shows the detailed view of the endpoint C0:4A:00:14:8D:4B. The endpoint profile is Microsoft-Workstation, with a current IP address of 10.62.148.63. The 'Vulnerabilities' tab is selected, showing the following details for QID-90783:

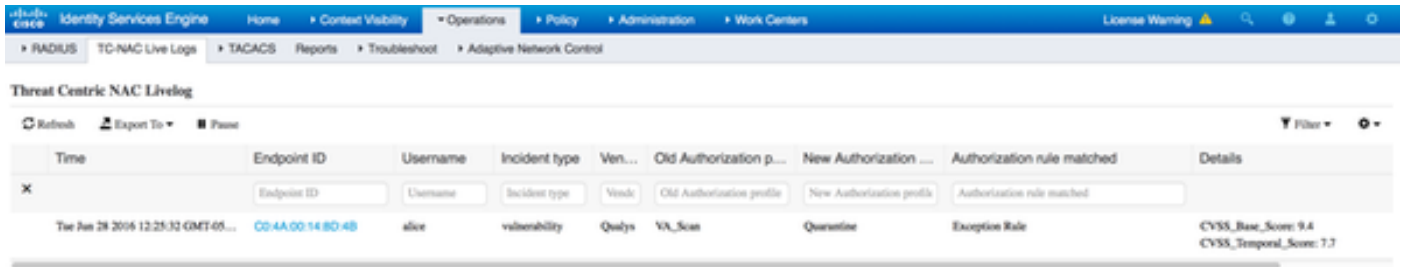
- Title:** Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
- CVSS score:** 9.3
- CVEIDS:** CVE-2012-0002, CVE-2012-0152,
- Reported by:** Qualys
- Reported at:**

The next vulnerability, QID-38173, is also shown with the following details:

- Title:** SSL Certificate - Signature Verification Failed Vulnerability
- CVSS score:** 9.4
- CVEIDS:**
- Reported by:** Qualys
- Reported at:**

Operations(운영) > TC-NAC Live Logs(TC-NAC 라이브 로그)에서 Old vs New authorization policies applied and details on CVSS\_Base\_Score를 볼 수 있습니다.

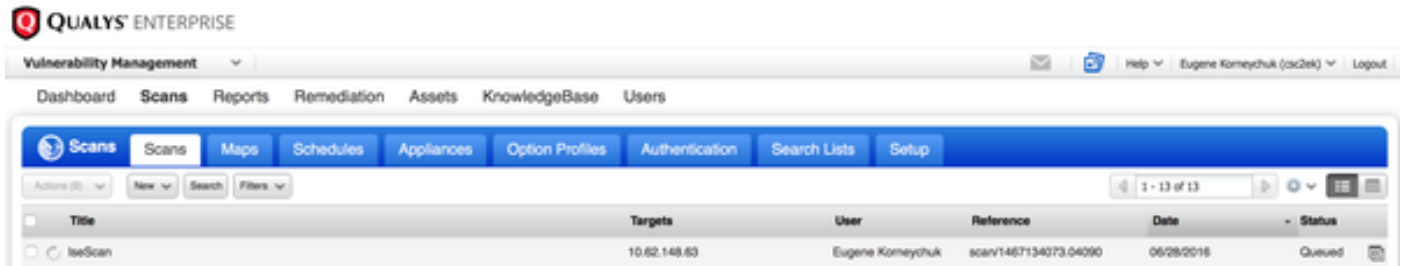
**참고:** 권한 부여 조건은 CVSS\_Base\_Score를 기반으로 수행됩니다. 이는 엔드포인트에서 탐지된 가장 높은 취약성 점수와 같습니다.



Time	Endpoint ID	Username	Incident type	Ven...	Old Authorization p...	New Authorization ...	Authorization rule matched	Details
Thu Jun 28 2016 12:25:32 GMT+05:...	CO-4A:00:14:8D:4B	alice	vulnerability	Qualys	VA_Scan	Quarantine	Exception Rate	CVSS_Base_Score: 9.4 CVSS_Temporal_Score: 7.7


### Qualys 클라우드

TC-NAC Qualys가 스캔을 대기열에 추가할 때 VA Scan은 Scans(스캔) > Scans(스캔)에서 볼 수 있습니다.



Title	Targets	User	Reference	Date	Status
IseScan	10.62.148.63	Eugene Komeychuk	scan/1467134073.04090	06/28/2016	Queued

Qualys 클라우드가 Running(실행 중)으로 전환되면 Qualys Scanner에 실제 검사를 수행하도록 지시했습니다.



Title	Targets	User	Reference	Date	Status
IseScan	10.62.148.63	Eugene Komeychuk	scan/1467134073.04090	06/28/2016	Running

스캐너가 스캔을 수행하는 동안 "스캐닝..."이 표시되어야 합니다. Qualys Guard 오른쪽 상단에 로그인

QualysGuard® Scanner Console

Name: ekorneyc\_qualys, LAN IP: 10.62.145.82

TIP:  
Press ENTER to access the menu.

스캔이 완료되면 Finished(완료) 상태로 전환됩니다. Scans(스캔) > Scans(스캔)에서 결과를 보고, 필요한 스캔을 선택하고 View Summary(요약 보기) 또는 View Results(결과 보기)를 클릭할 수 있습니다.

**QUALYS ENTERPRISE**

Vulnerability Management

Dashboard Scans Reports Remediation Assets KnowledgeBase Users

Scans Scans Maps Schedules Appliances Option Profiles Authentication Search Lists Setup

Title	Targets	User	Reference	Date	Status
IseScan	10.62.148.63	Eugene Komeychuk	scan/1467134073.04090	06/28/2016	Finished
IseScan	10.201.228.107	Eugene Komeychuk	scan/1467132757.03987	06/28/2016	Finished
IseScan	10.201.228.102	Eugene Komeychuk	scan/1467131435.03855	06/28/2016	Finished
IseScan	10.62.148.89	Eugene Komeychuk	scan/1464895232.91271	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Komeychuk	scan/1464855593.86436	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Komeychuk	scan/1464850315.85548	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Komeychuk	scan/1464847674.85321	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Komeychuk	scan/1464841736.84337	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Komeychuk	scan/1464836454.83651	06/02/2016	Finished

**Preview**

Vulnerability Scan - IseScan  
Target: 1 IP(s)

Scan launched by Eugene Komeychuk (sc2bk) | Start: 06/28/2016 at 21:58:55 (GMT+0400) | Ended: 06/28/2016 at 21:22:17 (GMT+0400) | Scan Finished (30:05:22)

Summary Scanner(s) are finished. Results from this scan have been processed.

Total Hosts Alive	Total appliances used	Aggregate Vulnerabilities	<a href="#">View Summary</a>   <a href="#">View Results</a>
1	1	7	

Report 자체에서 Detailed Results(세부 결과)를 확인할 수 있습니다. 여기서 탐지된 취약성이 표시 됩니다.



# Detailed Results

10.62.148.63 (ekorneyc-pc.example.com, EKORNEYC-PC)

## Vulnerabilities (6)

- 5 Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
- 3 SSL/TLS use of weak RC4 cipher
- 3 Windows Remote Desktop Protocol Weak Encryption Method Allowed
- 2 NetBIOS Name Accessible
- 2 SSL Certificate - Signature Verification Failed Vulnerability
- 1 ICMP Timestamp Request

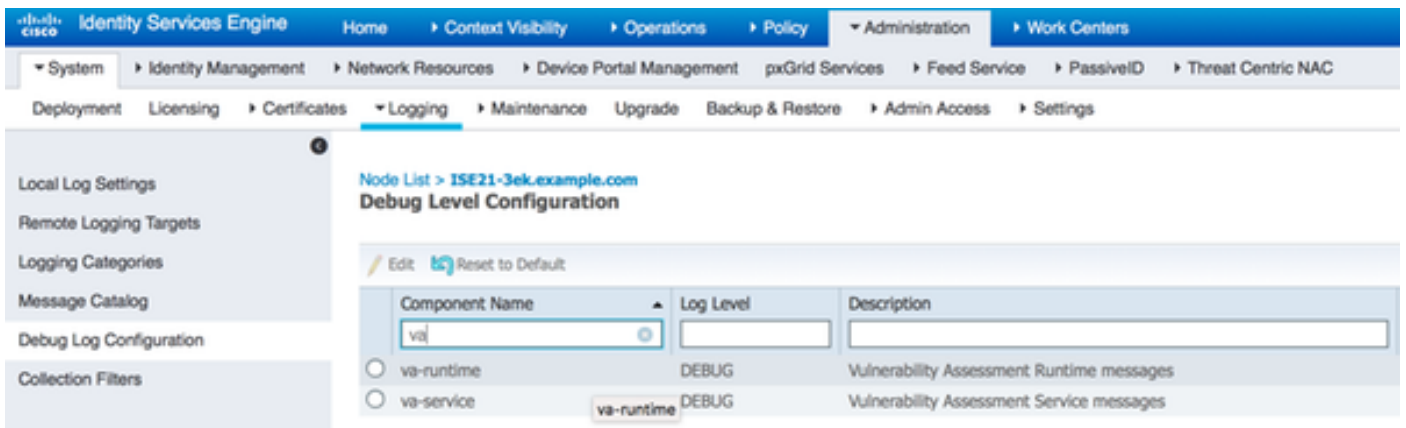
## Potential Vulnerabilities (1)

## Information Gathered (26)

## 문제 해결

### ISE의 디버깅

ISE에서 디버깅을 활성화하려면 Administration(관리) > System(시스템) > Logging(로깅) > Debug Log Configuration(디버깅 로그 컨피그레이션)으로 이동하여 TC-NAC Node(TC-NAC 노드)를 선택하고 Log Level(로그 레벨)va-runtime 및 va-service 구성 요소를 DEBUG로 변경합니다.



확인할 로그 - varuntime.log. ISE CLI에서 직접 확인할 수 있습니다.

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

TC-NAC Docker가 특정 엔드포인트 검사를 수행하는 명령을 받았습니다.

```
2016-06-28 19:06:30,823 DEBUG [Thread-70][] va.runtime.admin.mnt.EndpointFileReader -:::-- VA:
[{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","isPeriodicScanEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"79644b7-0b7-4b3-09b3-04b3-04b5-04b3-b611-199fb81a4b99","psnHostName":"ISE21-3ek","heartBeatTime":0,"lastScanTime":0}]
2016-06-28 19:06:30,824 DEBUG [Thread-70][] va.runtime.admin.vaservice.VaServiceRemotingHandler -:::-- VA:mnt
.{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","isPeriodicScanEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"796440b-0b7-0-4b3-09b3-0-4b3-
```

```
4b5-04b-4b5-4b5-04b-4b-4b-4b-4b5-4b5-4b-4b-b611-199fb81a4b99", "psnHostName": "ISE21-3ek", "heartBeatTime": 0, "lastScanTime": 0}
```

결과가 수신되면 모든 취약성 데이터가 컨텍스트 디렉토리에 저장됩니다.

```
2016-06-28 19:25:02,020 [pool-311-thread-8][]
va.runtime.admin.vaservice.VaServiceMessageListener -:::-- VaService
.[{"macAddress": "C0:4A:00:14:8D:4B", "ipAddress": "10.62.148.63", "lastScanTime": 146713439400, "vulnerabilities": [{"vulnerabilityId": "QID-90783", "cve3": "CVE-2012-0002,CVE-2012-0152", "cvssBaseScore": "9.3", "cvssTemporalScore": "7.7", "vulnerabilityTitle": "Microsoft Windows MS 12-020", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38173", "cveIds": "cvssBaseScore": "9.4", "cvssTemporalScore": "6.9", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90882", "cveIds": "", "cvssBaseScore": "4.7", "vulnerabilityTitle": "Windows Remote Desktop Protocol Weak Encryption Method Allowed", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90043", "cveIds": "", "cvssBaseScore": "7.3", "vulnerabilityTitle": "SMB", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38601", "cveIds": "CVE-2013-2566,CVE-2015-2808", "cvssBaseScore": "4.3", "cvss3 score": "3.7", "vulnerabilityTitle": "SSL/TLS RC4", "vulnerabilityVendor": "Qualys"}]}]
2016-06-28 19:25:02,127 DEBUG [pool-311-thread-8][]
va.runtime.admin.vaservice.VaServiceMessageListener -:::-- VA: DB ,
lastscantime:1467134394000, mac:C0:4A:00:14:8D:4B
2016-06-28 19:25:02,268 DEBUG [pool-311-thread-8][]
va.runtime.admin.vaservice.VaAdminServiceContext -:::-- VA:pri-lan json
2016-06-28 19:25:02,272 DEBUG [pool-311-thread-8][]
va.runtime.admin.vaservice.VaPanRemotingHandler -:::-- VA:
:{C0:4A:00:14:8D:4B=[{"vulnerabilityId": "QID-90783", "cveIds": "CVE-2012-0002,CVE-2012-0152", "cvssBaseScore": "9.3", "TemporalScore": "7.7", "vulnerabilityTitle": "Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38173", "cveScore": "9.4": "cvss9.4", "vssTemporalScore": "6.9", "vulnerabilityTitle": "SSL", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90882", "cveIds": "", "cvssBaseScore": "4.7", "cvssTemporalScore": "4", "title": "Windows Remote Desktop Protocol Weak Encryption Method Allowed", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-90043", "cveIds": "", "cvssBaseScore": "7.3", "cvssTemporalScore": "6.3", "vulnerabilityTitle": "SMB", "vulnerabilityVendor": "Qualys"}, {"vulnerabilityId": "QID-38601", "cveIds": "CVE-2013-2566,CVE-2015-2808", "cvssBaseScore": "4.3", "cvss3 score": "3.7", "vulnerabilityTitle": "SSL/TLS RC4", "vulnerabilityVendor": "Qualys"}]}]
```

확인할 로그 - vaservice.log.ISE CLI에서 직접 확인할 수 있습니다.

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

어댑터에 제출된 취약성 평가 요청

```
2016-06-28 17:07:13,200 [endpointPollerScheduler-3][] cpm.va.service.util.VaServiceUtil -
:::-- VA SendSyslog
systemMsg: [{"systemMsg": "91019", "isAutoInsertSelfAcInstance": true, "attributes": [{"TC-NAC.ServiceName", "TC-NAC.Status", "VA", "TC-NAC.Details", "VA VA tc-NAC.MACAddress", "C0:4A:00:14:8D:4B", "TC-NAC.IpAddress", "10.62.148.63", "TC-NAC.AdapterInstanceUuid", "79640b7-09b5-4f3b611-19 881a4b99", "TC-NAC.VendorName", "Qualys", "TC-NAC.AdapterInstanceName", "QUALYS_VA"}]}]
```

AdapterManager은 스캔이 완료될 때까지 매 5분 동안의 상태를 확인합니다.

```
2016-06-28 17:09:43,459 [SimpleAsyncTaskExecutor-2][]
```

```

cpm.va.service.processor.AdapterMessageListener -:::::-
:{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-0-627f30248ad0","VendorName":"Qualys","OperationMessageText":":1, :0, :{0}
2016-06-28 17:14:43,760 [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::-
:{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-0-627f30248ad0","VendorName":"Qualys","OperationMessageText":":0, :0, :1"}
2016-06-28 17:19:43,837 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::-
:{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-0-627f30248ad0","VendorName":"Qualys","OperationMessageText":":0, :0, :1"}
2016-06-28 17:24:43,867 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::-
:{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-0-627f30248ad0","VendorName":"Qualys","OperationMessageText":":0, :0, :1"}

```

어댑터는 QID를, CVE는 CVSS 점수와 함께 가져옵니다.

```

2016-06-28 17:24:57,556 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::-
:{"requestedMacAddress":"C0:4A:00:14:8D:4B","scanStatus":"ASSESSMENT_SUCCESS","lastScanTimeLong":146713439440000,"ipAddress":"10.62.148.63",":":[{"vulnerabilityID-3":"QID"
8173","CVEIds":"","CVSSBaseScore":"9.4","CVSSTemporalScore":"6.9","VULNERABILITYTitle":"SSL -
","vulnerabilityVendor"}, {"vulnerabilityId"},"QID-90043","cve3":
","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","vulnerabilityTitle":"SMB SMB
","vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-90783","CVE2120-21 0002,CVE-2012-
0152","cvssBaseScore":"9.3","cvssTemporalScore":"7.7","vulnerabilityTitle":"Microsoft Windows
Remote Desktop Protocol Remote Code Execution Vulnerability (MS.12-020)","":"Qualys":"Qualys"
ID":"QID-38601","cveIds":"CVE-2013-2566,CVE-2015-
2808","cvssBaseScore":"4.3","cvssTemporalScore":"3.7","":"SSL TLS/SSL RC4
","vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-
90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows
Remote Desktop Protocol Weak Encryption Method Vendor"Allowed","Allowed","Vendor" Qualys}}]}
2016-06-28 17:25:01,282 INFO [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::- IRF
{"C0:4A:00:14:8D:4B":{"vulnerability":{"VSS" Base_Score":9.4,"CVSS_Temporal_Score":7.7},"
":146713439400,"title":"","":"Qualys"}}
2016-06-28 17:25:01,853 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -
:::::- VA SendSyslog
systemMsg:[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","","TC-NAC.Status","VA successfully completed","TC-NAC.Details","VA
completed; :5","TC-NAC.MACAddress","C0:4A:00:14:8D:4B","TC-NAC.IpAddress","10.62.148.63","TC-
NAC.AdapterInstanceUuid","79640b7-09b5-4b3b-1111 99fb81a4b99","TC-NAC.VendorName","Qualys","TC-
NAC.AdapterInstanceName","QUALYS_VA"]}]}

```

## 일반적인 문제

문제점 1. ISE는 CVSS\_Base\_Score가 0.0이고 CVSS\_Temporal\_Score가 0.0인 취약성 보고서를 얻는 반면, Qualys 클라우드 보고서에는 탐지된 취약성이 포함되어 있습니다.

문제/장애:

Qualys Cloud에서 Report(보고서)를 확인하는 동안 탐지된 취약성을 볼 수 있지만, ISE에서는 이를 볼 수 없습니다.

vaservice.log에 표시되는 디버그:

```

2016-06-02 08:30:10,323 INFO [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::::- IRF {"C0:4A:00:15:75:C8":{"VSS8":
Base_Score":0.0,"CVSS_Temporal_Score":0.0},"":146485905000,"title":"","":"Qualys"}}}

```

## 해결책:

cvss 점수가 0인 이유는 취약성이 없거나 UI를 통해 어댑터를 구성하기 전에 Qualys Cloud에서 cvss 점수가 활성화되지 않았기 때문입니다. cvss 점수 부여 기능이 활성화된 지식 기반은 어댑터를 처음 구성한 후에 다운로드됩니다. CVSS 점수 부여가 활성화되었는지, 어댑터 인스턴스가 ISE에 생성되었는지 확인해야 합니다. Vulnerability Management(취약성 관리) > Reports(보고서) > Setup(설정) > CVSS > Enable CVSS Scoring(CVSS 점수 활성화)에서 수행할 수 있습니다.

**문제 2. ISE는 Qualys Cloud에서 올바른 권한 부여 정책을 적용했지만 결과를 가져오지 않습니다.**

## 문제/장애:

수정된 권한 부여 정책이 일치했으며, VA 검사를 트리거해야 합니다. 그 사실에도 불구하고 어떤 스캔도 수행되지 않습니다.

vaservice.log에 표시되는 디버그:

```
2016-06-28 16:19:15,401 [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::-- : (
:'[B@6da5e620(byte[311])'MessageProperties [headers={}, timestamp=null, messageId=null,
appId=null, clusterId=null, type=null, correlationId=null, replyTo=null,
contentType=application/octet-stream, contentEncoding=null, contentLength=0, deliveryMode=0,
persistent, persistent priority=0, redelivered=null, repriority=null false,
receivedExchange=irf.topic.va-reports, receivedRoutingKey=, deliveryTag=9830, messageCount=0])
2016-06-28 16:19:15,401 [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::--
:{"requestedMacAddress":"24:77:03:3D:CF:20","scanStatus":"SCAN_ERROR","scanStatusMessage":
:1904 . IP .","lastScanTimeLong":0,"ipAddress":"10.201.228.102"}
2016-06-28 16:19:15,771 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::-- Macaddress:24:77:03:3D:CF:20, IP
(DB):10.201.228.102,
2016-06-28 16:19:16,336 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -
:::-- VA SendSyslog
systemMsg:[{"systemMsg":"91008","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","","TC-NAC.Status","VA","TC-NAC.Details"," :1904 . IP IP
.", "TC-NAC.MACAddress","24:77:03:3D:CF:20","TC-NAC.IpAddress","10.201.228.102","TC-
NAC.AdapterUuid","79640b7-40b7 b5-4f3b-b611-199fb81a4b99","TC-NAC.VendorName","Qualys","TC-
NAC.AdapterInstanceName","QUALYS_VA"]}]
```

## 해결책:

Qualys Cloud는 엔드포인트의 IP 주소가 검사에 적합하지 않음을 나타냅니다. 엔드포인트의 IP 주소를 Vulnerability Management > Assets > Host Assets > New > IP Tracked Hosts에 추가했는지 확인하십시오.

## 참조

- [Cisco Identity Services Engine 관리자 가이드, 릴리스 2.1](#)
- [기술 지원 및 문서 - Cisco Systems](#)
- [비디오: ISE 2.1\(Qualys 포함\)](#)
- [Qualys 설명서](#)