



# How-To Threat Centric NAC Qualys and Cisco Identity Service Engine (ISE) Integration using STIX Technology

Author: John Eppich

## Table of Contents

<b>About this Document</b> .....	<b>3</b>
<b>Introduction</b>	<b>4</b>
<b>Technical Details</b> .....	<b>5</b>
<b>Qualys Settings</b> .....	<b>6</b>
Configuring and Installing Qualys Virtual Scanner on ESX .....	6
Adding Scanner Personalization Code .....	11
Configure IP Addresses to Scan.....	15
Enable CVSS Scoring.....	17
<b>Cisco Identity Service Engine (ISE) Settings</b> .....	<b>19</b>
Enabling TC-NAC Service in ISE.....	19
Creating VA Authorization Profile .....	24
Creating Threat-based CVSS Authorization Condition Rule.....	25
Add the Qualys Scan authorization profile to the Basic Authentication rule .....	26
<b>Triggering a Scan</b> .....	<b>28</b>

## About this Document

---

This document is for Cisco Engineers and customers deploying Cisco Threat Centric NAC using Qualys with Cisco Identity Services Engine (ISE) 2.1. A cloud Qualys Managers license with API is required. Please speak to your Qualys representative to obtain the license. Qualys integration does not use Cisco platform Exchange Grid (pxGrid) for ISE integration, instead it uses Structured Threat Information Expression (STIX). STIX is an information exchange language and used to exchange cyber threat intelligence with organizations. It allows a common framework for organizations to share cyber threat information and adapter quicker to computer-based attacks.

Cisco Threat Centric NAC using Qualys also falls into the Rapid Threat Containment category. Cisco Security Solutions and Ecosystem and CSTA partner solutions that fall into this category use Adaptive Network Control (ANC) mitigation actions to respond to or contain threats by issuing mitigation actions either from pxGrid, ISE EPS RESTful API or STIX.

Cisco Threat Centric NAC using Qualys performs vulnerability scans on the endpoint. Based on the CVSS scoring rating in the Qualys reports and the ISE Threat mitigation CSVSS authorization condition rule, vulnerable endpoints can be quarantined or provided limited access based on the organization's security policy.

This document covers the following:

- Qualys VMware ESX VM (virtual machine) installation and configuration
- Enabling CVSS scoring Qualys Reports
- ISE Qualys Adapter Configuration
- ISE Vulnerability Assessment (VA) authorization profile configuration
- ISE Threat CVSS Condition rules.

## Introduction

---

Qualys is a vulnerability management solution and scans assets for vulnerability detection based on their vulnerability database and Common Vulnerability Scoring System (CVSS).

Cisco ISE (Identity Services Engine) is an identity solution, providing ISE 802.1X authentication for wired, wireless and virtual environments. In addition, ISE can perform additional functions such as Guest, Posture, and incorporate SGT (Security Group Tags) which is a component for the Cisco TrustSec solution. When a user or device authenticates to the network, there is rich contextual information that is available from these authenticated session. This session information may include the username, IP address, MAC address, posture status, SGT, and endpoint profile information that provides more information around the IP event. Cisco platform exchange protocol (pxGrid) allows the sharing of this contextual information ecosystem and CSTA partners.

Currently ISE cannot consume information from ecosystem and CSTA partners, this is where STIX technology comes in. STIX is a framework for sharing cyber threat information among security solutions. ISE consumes the Qualys CVSS rating found in vulnerabilities on the scanned assets and provides compliance in an organization's security policy by enforcing an ISE authorization policy based on CVSS base and or CVSS temporal score.

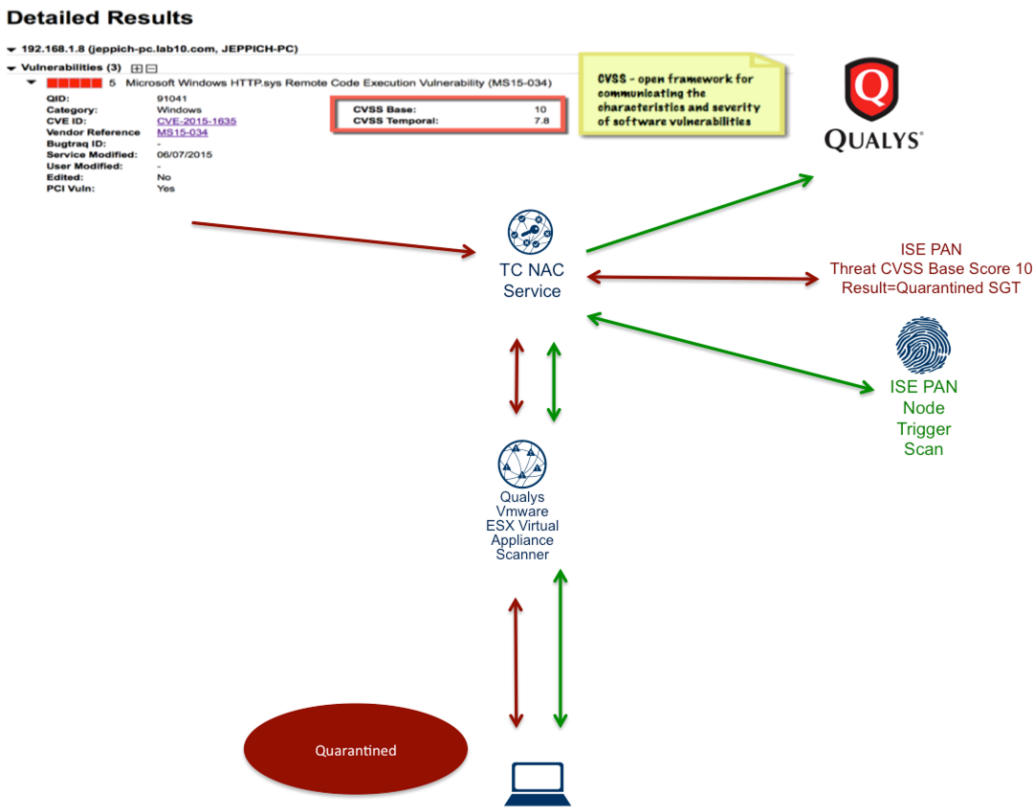
The CVSS base score represents the fundamental, unchanging qualities of the vulnerability and is mostly provided by NIST. The CVSS represents time dependent qualities of the vulnerability.

# Technical Details

The TC NAC service is enabled on the Policy Services Node (PSN) node. The administrator configures the ISE Qualys Connector and adapter instance, scanning attributes and scanning intervals as defined by the authorization profile. The vulnerability assessment (VA) scan will be triggered by an organization’s security policy or ISE authorization policy. This information will be sent to the vulnerability assessment framework (VAF) service or TC NAC service.

The TC NAC service will receive and consume the endpoint details and the ISE Qualys adapter will connect to Qualys Cloud instance and send the scanned endpoints to Qualys via HTTPS via workflow APIs for scanning. Assets or IP addresses are defined in the Qualys scanned settings. These API’s will trigger the Qualys Virtual scanning appliance to begin scanning.

Once the scan completes the Qualys cloud instance will send the scan results to the TC NAC service. The TC NAC service will send the results to PAN context for viewing and will perform the COA based on the authorization CVSS score condition rule. This ISE authorization policy is determined by the administrator and can set an organization’s security compliance policy.



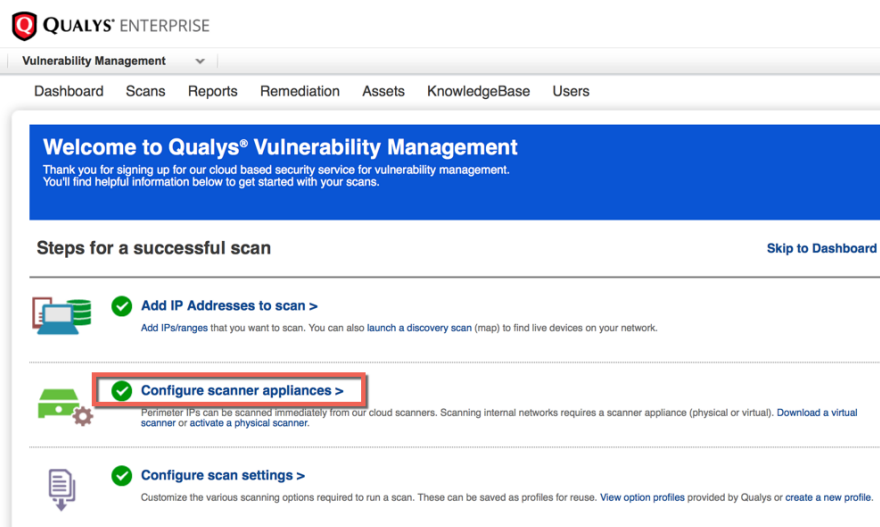
## Qualys Settings

These settings step through the process of installing, configuring, registering the Qualys ESX VMware virtual appliance and enabling CVSS scoring in Qualys reports.

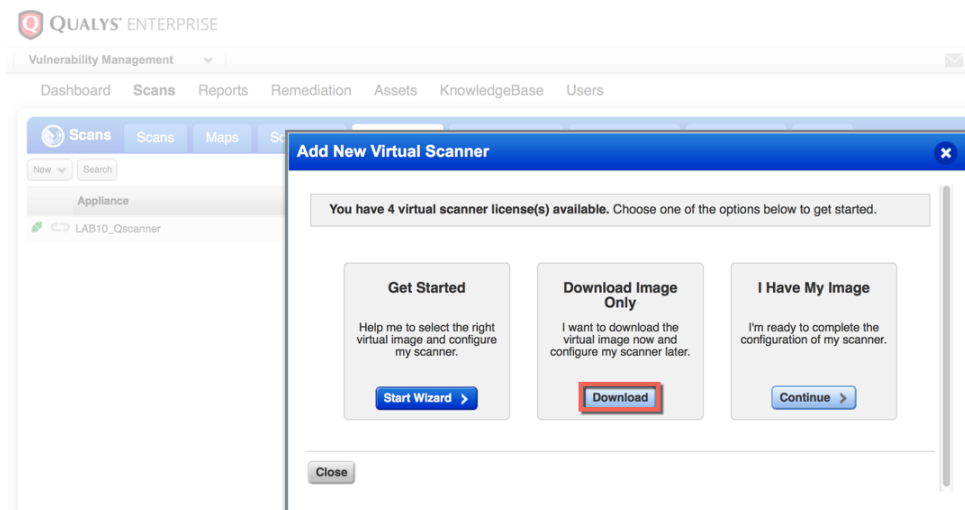
### Configuring and Installing Qualys Virtual Scanner on ESX

Here we download and install the VMware ESX virtual appliance.

#### Step 1 Login to Qualys Cloud Account and select **Configure scanner appliances**



#### Step 2 Select **New->Virtual Scanner Appliances->Download Image Only->Download**



**Step 3** Select the VM Platform. In this example, the **Standard** Distribution Package was selected

**Note:** OVF9 Distribution Package not shown in diagram

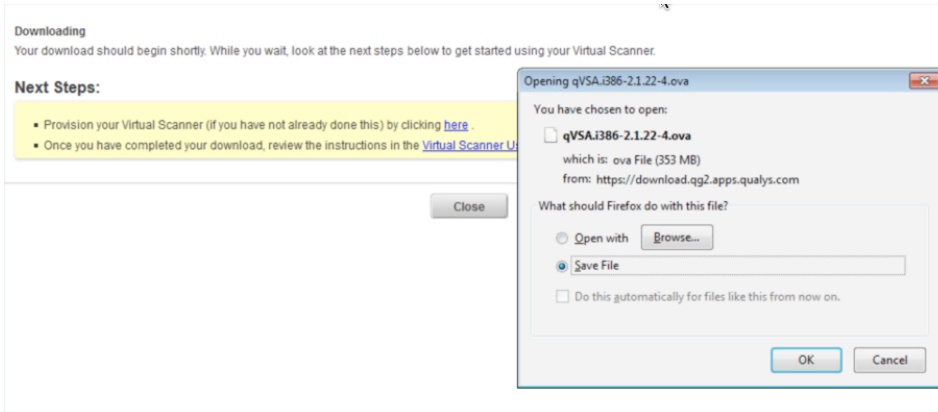
Distribution Package	Target Platforms	File/Package Type	Download/Launch
Standard	<ul style="list-style-type: none"> <li>VMware vCenter Server (+ESXi or ESX)</li> <li>VMware ESXi; ESX</li> <li>VMware Workstation; Player; Fusion</li> <li>Oracle VM VirtualBox</li> <li>Citrix XenServer</li> </ul>	OVA (w/ VMDK virtual disk format)	<a href="#">link</a>
VMDK	<ul style="list-style-type: none"> <li>older VMware platforms lacking support for OVA and OVF formats</li> <li>miscellaneous platforms (note: Extract the VMDK and convert to the virtual disk format of your choosing).</li> </ul>	ZIP (w/ VMware VMX file + VMDK virtual disk format)	<a href="#">link</a>
Microsoft Hyper-V	<ul style="list-style-type: none"> <li>Microsoft Windows 2008 R2, Windows 2008, Windows 2012, Windows 8</li> </ul>	ZIP (w/ VHD virtual disk format)	<a href="#">link</a>
Amazon Machine Image (Pre-Authorized Scanning)	<ul style="list-style-type: none"> <li>Amazon EC2-Classical, Amazon EC2-VPC</li> </ul>	AMI (Not a download. Published at AWS Marketplace)	<a href="#">link</a>
Amazon Machine Image	<ul style="list-style-type: none"> <li>Amazon EC2-Classical, Amazon EC2-VPC</li> </ul>	AMI (Not a download. Published at AWS Marketplace)	<a href="#">link</a>
VMware vApp	<ul style="list-style-type: none"> <li>VMware vCenter</li> <li>VMware vCloud</li> </ul> <p>Note: This is a very specialized vApp package. It must be deployed through VMware vCenter Server or vCloud Director. The <i>IP Pools</i> feature must be configured and enabled in</p>	VMware vApp OVA (w/ VMDK virtual disk format)	<a href="#">link</a>

**Step 4** Review and Agree to the Virtual Scanner License

**Review and Agree to Virtual Scanner License**

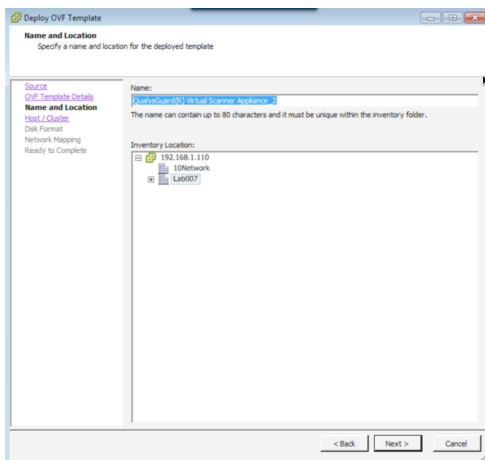
By downloading or otherwise using the Qualys® Virtual Machine Image Software ("Software"), you acknowledge and agree to be bound by the applicable Qualys® Software license terms as set forth in the applicable [Qualys® Service Agreement](#) electronic terms ("E-terms") or as otherwise mutually agreed by parties in writing.

**Step 5** The image should start downloading. Once the download is complete, save the file locally.

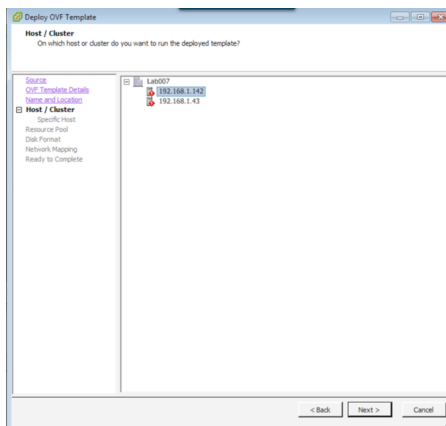


**Step 6** Open OVA file

**Step 7** Deploy the OVA template

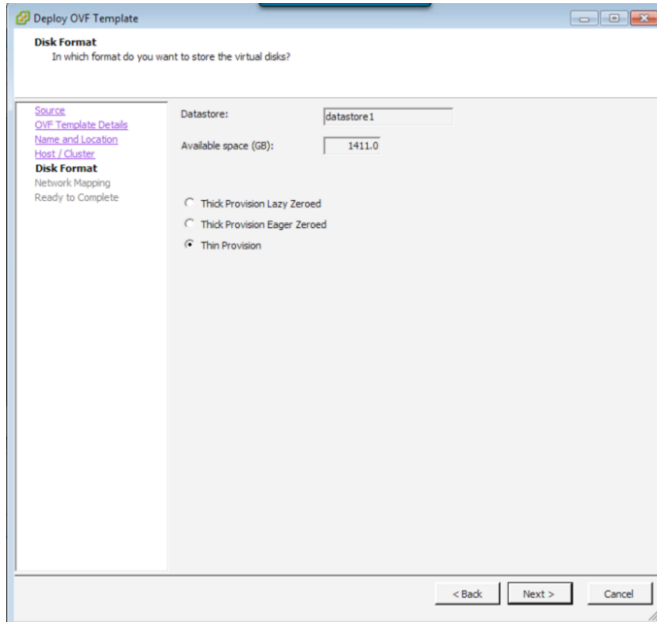


**Step 8** Select Next

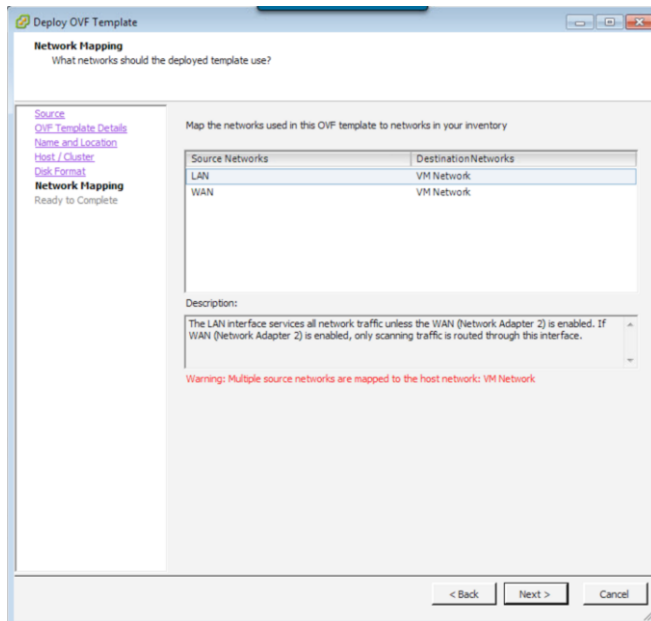




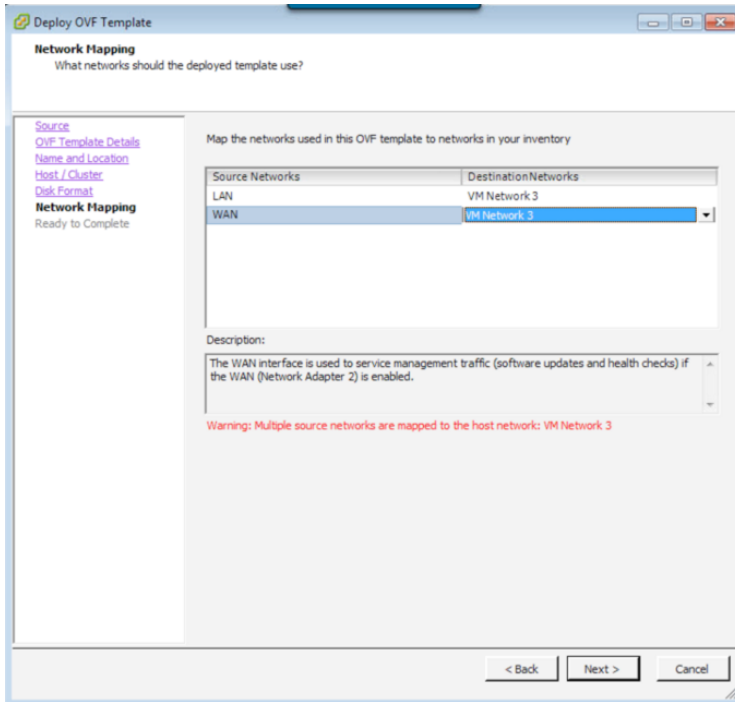
- Step 9 Select Next
- Step 10 Select Thin Provisioning



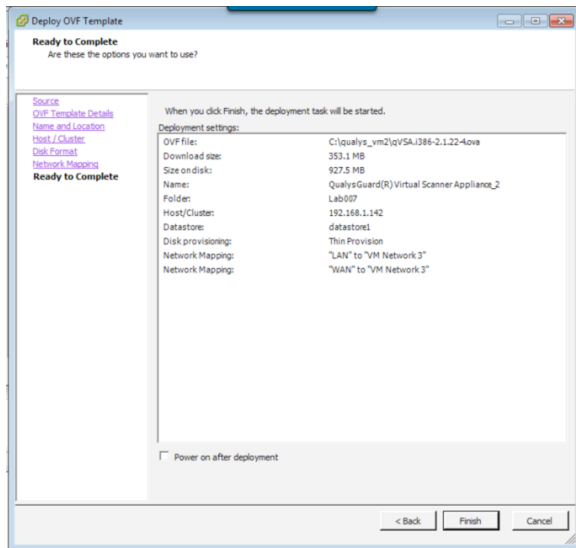
- Step 11 Select Next
- Step 12 Add the VM network for the LAN interface



**Step 13** Add the VM network for the WAN interface.



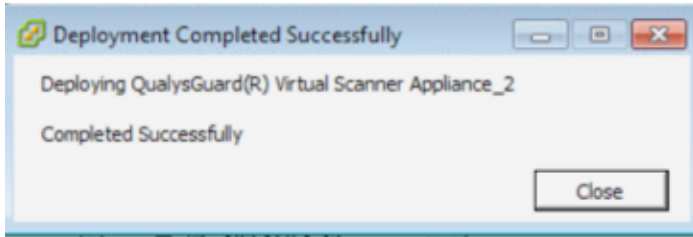
**Step 14** Select **Next**



**Step 15** Select **Power on after deployment**

**Step 16** Select **Finish**

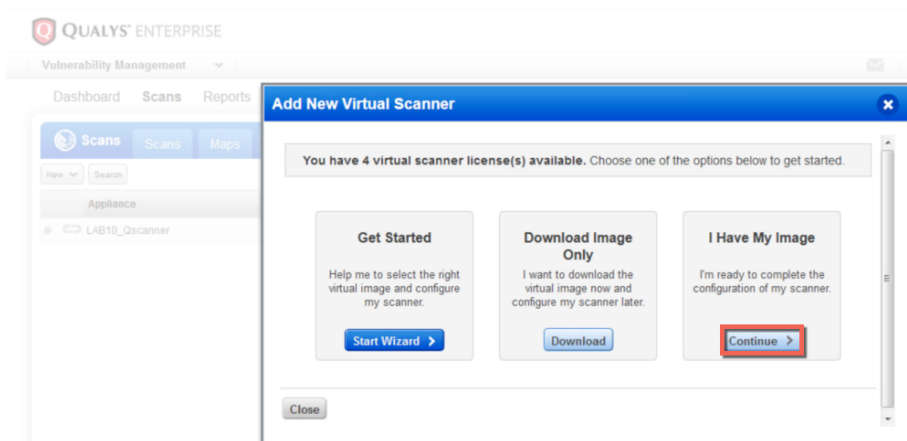
**Step 17** You should the VM deployed successfully



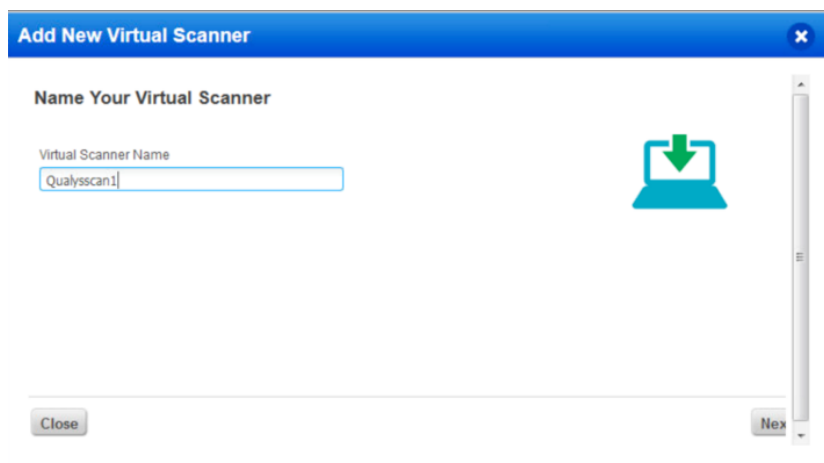
## Adding Scanner Personalization Code

The Qualys Personalization code is required for making the scanner operational. Here we add the personalization scanner code to the installed image.

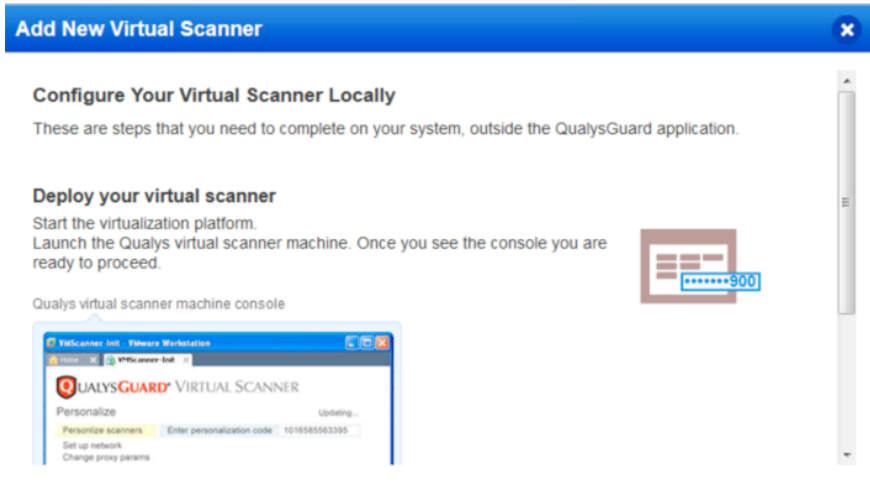
**Step 1** From the Qualys GUI, select **I Have My image->Continue**



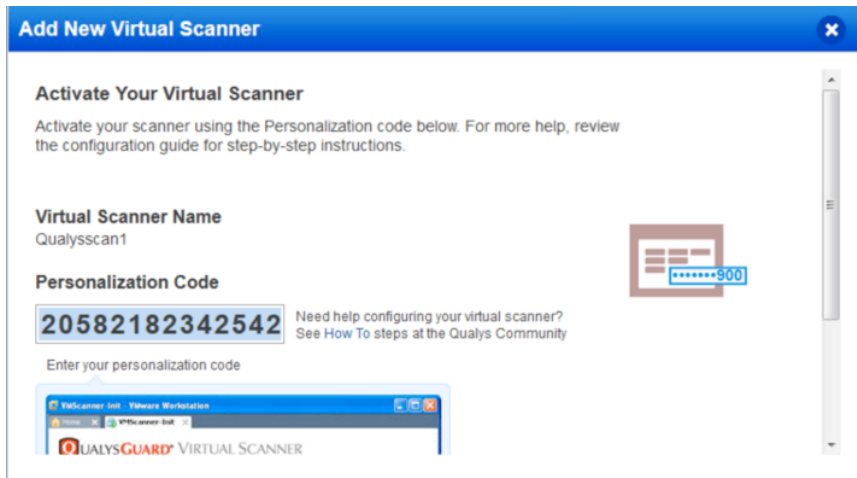
**Step 2** Enter your Virtual Scanner name



- Step 3** Select **Next**
- Step 4** You should see the following:

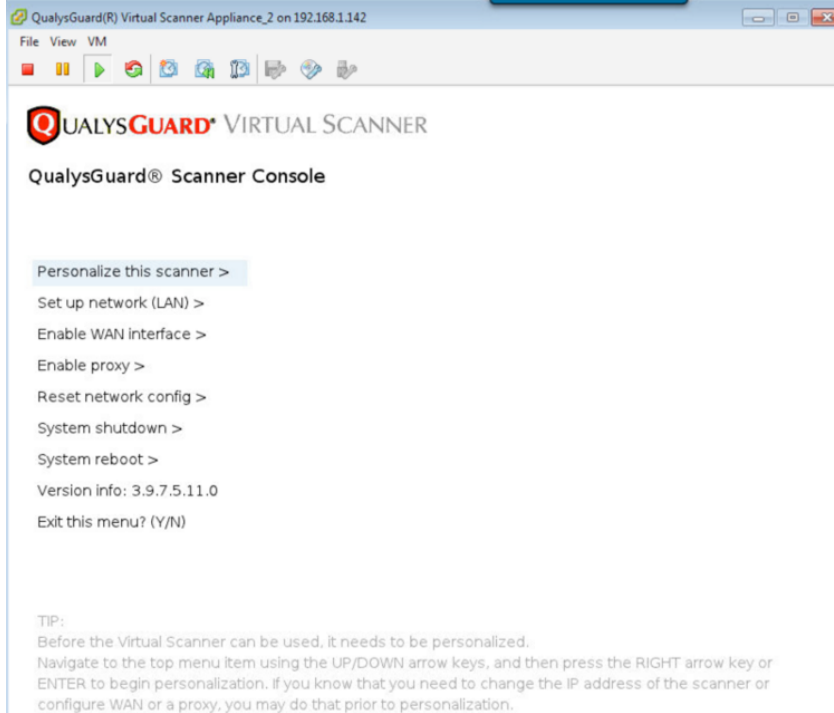


- Step 5** Select **Next**
- Step 6** You should see your personalization code



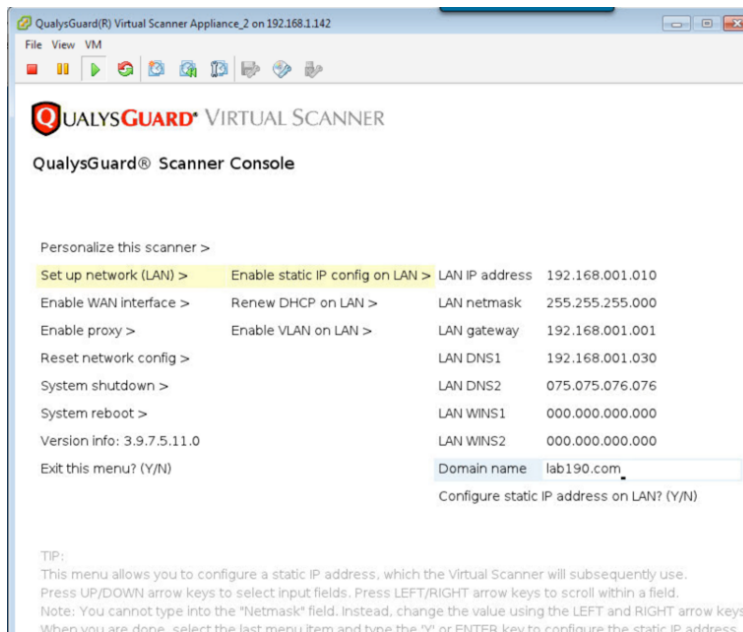
- Step 7** Enter the personalization code in the VM scanner
- Step 8** Select **Check Activation**

**Step 9** You should see the following:

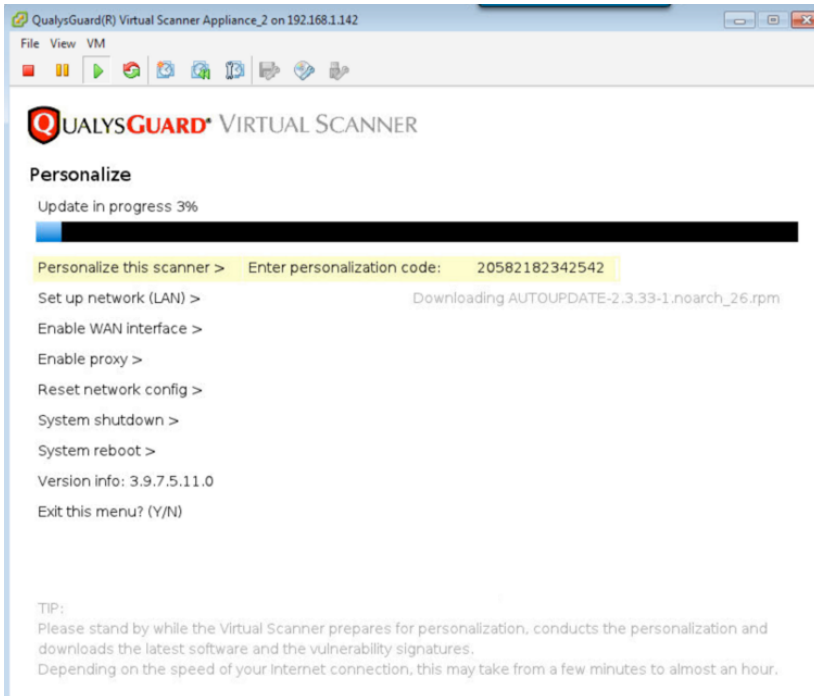


**Step 10** Click the up arrow key to continue without the personalization code

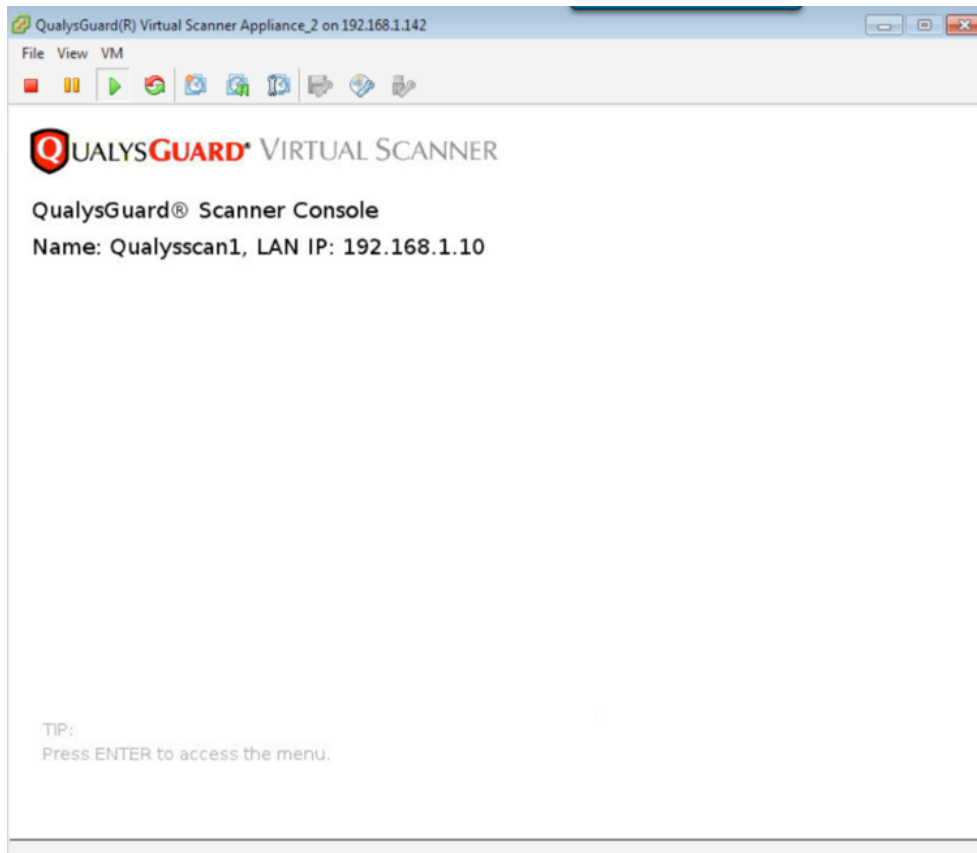
**Step 11** Enter the static LAN settings



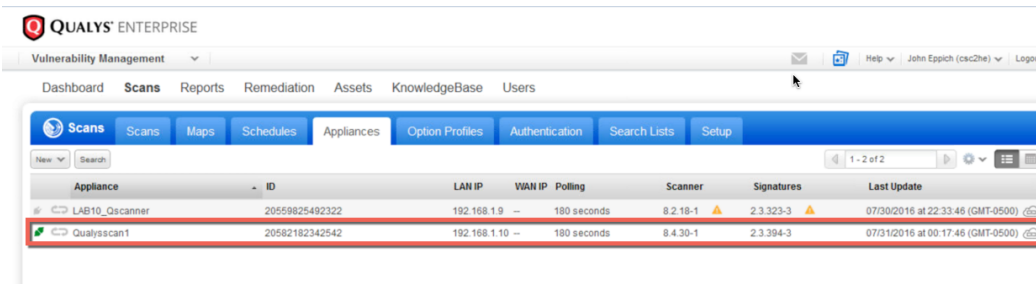
**Step 12** Go back and enter the personalization code you should see the following:



**Step 13** The installation should take a couple of minutes to complete. When completed you should see:



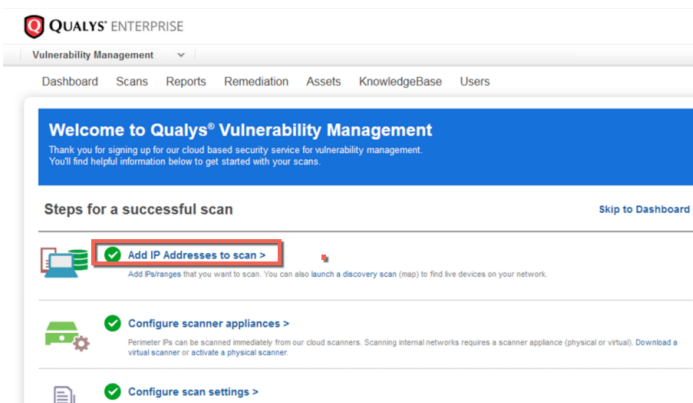
**Step 14** Refresh the page, you should see the VM scanned appliance



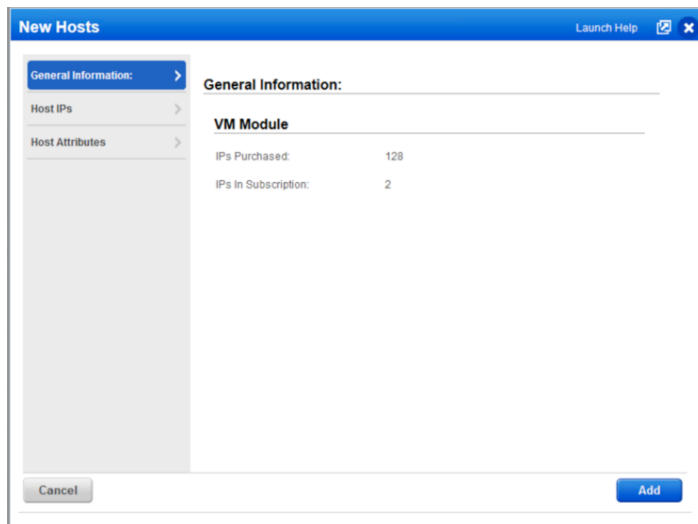
## Configure IP Addresses to Scan

Enter the IP addresses that you want to scan in your environment.

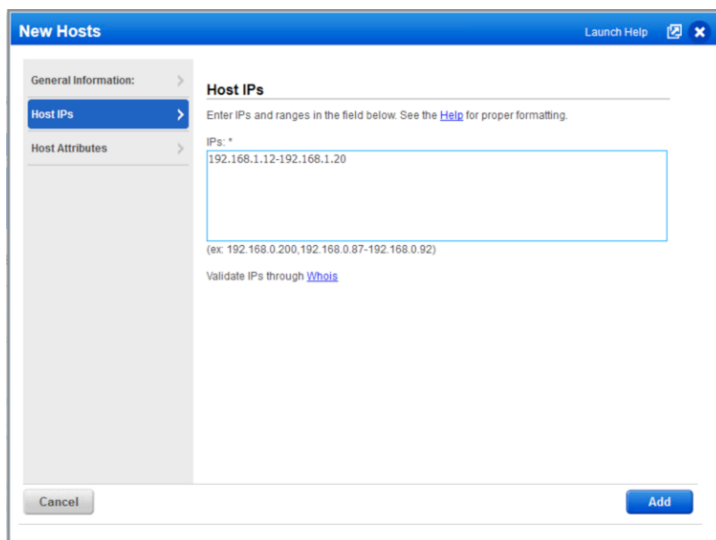
**Step 1** Configure IP Addresses to Scan



**Step 2** You should see the following



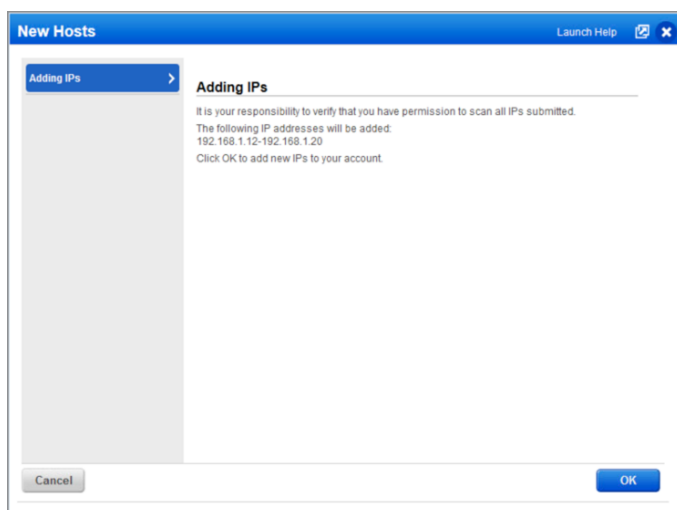
**Step 3** Select **Host IPs**, enter a range of IP addresses



The screenshot shows the 'New Hosts' dialog box with the 'Host IPs' tab selected. The 'Host IPs' section contains a text input field with the value '192.168.1.12-192.168.1.20'. Below the input field, there is a note: '(ex: 192.168.0.200,192.168.0.87-192.168.0.92)' and a link to 'Validate IPs through Whois'. The dialog box has a 'Cancel' button on the left and an 'Add' button on the right.

**Step 4** Select **Add**

**Step 5** You should see the following:

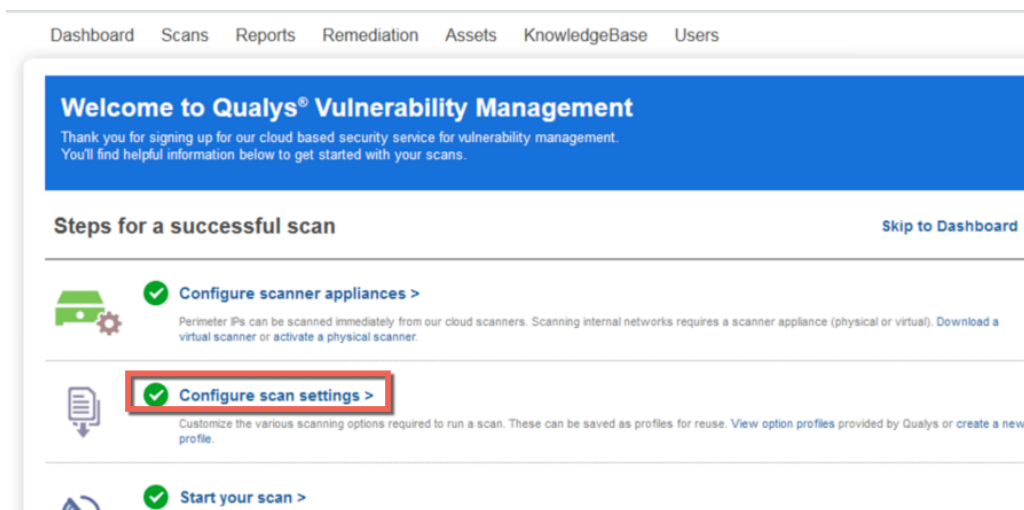


The screenshot shows the 'New Hosts' dialog box with the 'Adding IPs' tab selected. The 'Adding IPs' section contains the following text: 'It is your responsibility to verify that you have permission to scan all IPs submitted. The following IP addresses will be added: 192.168.1.12-192.168.1.20. Click OK to add new IPs to your account.' The dialog box has a 'Cancel' button on the left and an 'OK' button on the right.

**Step 6** Select **OK**



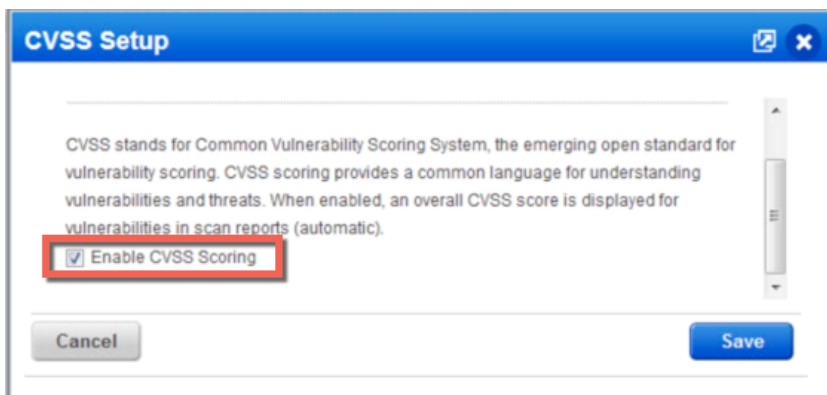
**Step 7** Select **Configure Scan Settings** to view the Standard Scan Settings



## Enable CVSS Scoring

Enable CVSS Scoring in the Qualys vulnerable reports. The CVSS threat authorizations condition rules are dependent on the CVSS scoring in the vulnerable reports.

**Step 1** Enable **CVSS Scoring**, select **Reports->Setup->CVSS Scoring->Enable CVSS Scoring**



**Step 2** Select **Save**

**Step 3** Select **Hosts-Assets** and verify the range of IP address are there for valid scans

Info	Tracking	IP	DNS	NetBIOS	OS	Comments
<input type="checkbox"/>			192.168.1.8	jeppich-pc.lab10.com	JEPPICH-PC	Windows 7 Service Pack 1
<input type="checkbox"/>			192.168.1.10	jeppich-pc.lab10.com	JEPPICH-PC	Windows 7 Service Pack 1
<input type="checkbox"/>			192.168.1.12-192.168.1.20			[expand IP range to see comments ...]

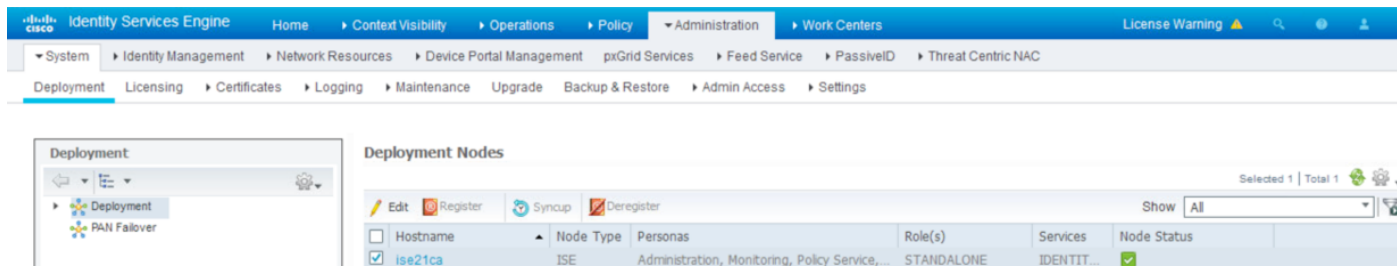
# Cisco Identity Service Engine (ISE) Settings

## Enabling TC-NAC Service in ISE

Enable the TC-NAC service and verify the services have started.

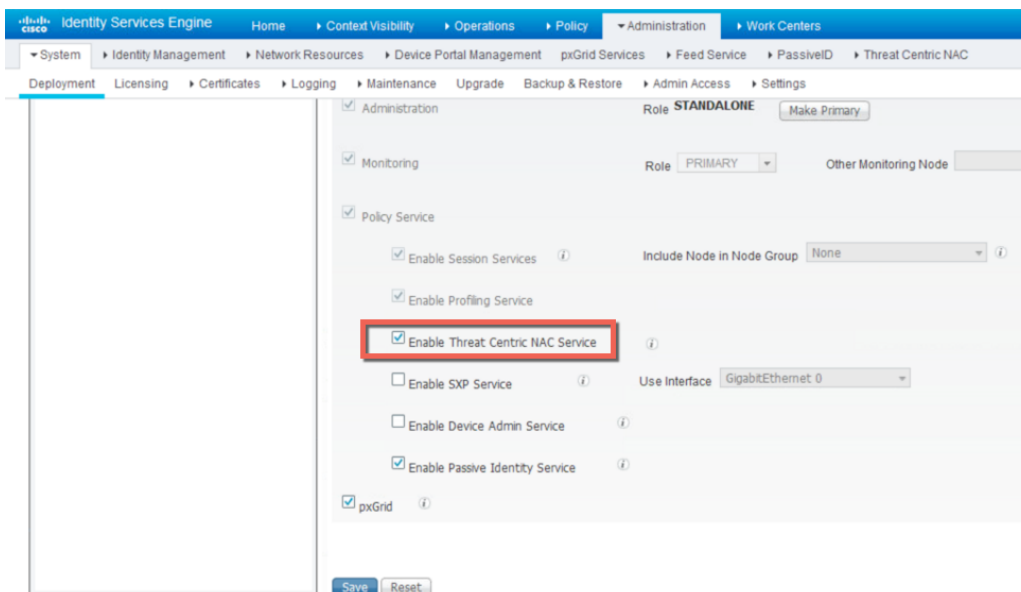
**Step 1** Enable TC-NAC

**Step 2** Select **Administration->System->Deployment->Select the node->Edit**



The screenshot shows the ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the 'Deployment' menu. The main content area displays a table of 'Deployment Nodes' with the following columns: Hostname, Node Type, Personas, Role(s), Services, and Node Status. One node is selected, 'ise21ca', which is of type 'ISE' and has the role 'STANDALONE'. The 'Services' column for this node shows 'IDENTIT...' and a green checkmark in the 'Node Status' column.

**Step 3** Enable Threat Centric-NAC



The screenshot shows the configuration page for a node in the ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the 'Deployment' menu. The main content area displays the configuration for a node with the role 'STANDALONE'. The 'Services' section is expanded, and the checkbox for 'Enable Threat Centric NAC Service' is checked and highlighted with a red box. Other services listed include Administration, Monitoring, Policy Service, Enable Session Services, Enable Profiling Service, Enable SXP Service, Enable Device Admin Service, Enable Passive Identity Service, and pxGrid. The 'Use Interface' is set to 'GigabitEthernet 0'. There are 'Save' and 'Reset' buttons at the bottom.

**Step 4** Select **Save**

**Step 5** Run “application status ise’ to view the Threat Centric NAC services have started

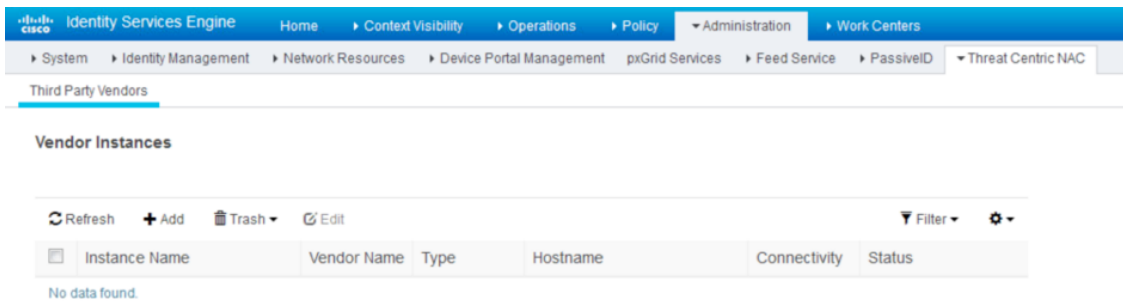
```
application status ise
```

You should see the TC-NAC services initialize and then in a running state

```
ise21ca/admin# sh application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	3684
Database Server	running	69 PROCESSES
Application Server	running	7261
Profiler Database	running	4994
ISE Indexing Engine	running	7672
AD Connector	running	8681
M&T Session Database	running	3861
M&T Log Collector	running	8272
M&T Log Processor	running	8185
Certificate Authority Service	running	8819
EST Service	running	16282
SVN Engine Service	disabled	
TC-MAC Docker Service	running	3335
TC-MAC MongoDB Container	running	6849
TC-MAC RabbitMQ Container	running	6854
TC-MAC Core Engine Container	running	7685
UA Database	running	8245
UA Service	running	8446
pxGrid Infrastructure Service	running	8732
pxGrid Publisher-Subscriber Service	running	9882

**Step 6** Select **Administration->Threat Centric NAC->Third Party Vendors->**  
You should see the following:



**Step 7** Select Add->select **Qualys-VA** as the vendor

**Step 8** Provide an Instance name->**Qualys-Lab**

**Note:** this can be any name

You should see the following:

**Step 9** Select **Save**

**Step 10** You should see the following;

Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
Qualys-Lab	Qualys	VA		Disconnected	Ready to configure

**Step 11** Select **Ready to configure**

**Step 12** Enter you Qualys cloud and account information

- Step 13 Select Next
- Step 14 Map the PSN node to the VM scanner appliance

The screenshot shows the Identity Services Engine (ISE) Administration console. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > PassivelD > Threat Centric NAC > Third Party Vendors > Vendor Instances > Qualys-Lab. The main content area is titled "Scanner Mappings" and contains two sections:

- Default Scanner:** A dropdown menu is set to "Qualyscan1". Below it is the text: "Default scanner to use for scans."
- PSN to Scanner Mapping:** A section titled "Map Policy Service Node (PSN) to a Qualys scanner appliance. This configuration ensures that the selected scanner appliance for scan is based on the PSN which authorizes the endpoint." Below this is a field labeled "Map ise21ca to:" with a dropdown menu set to "Qualyscan1".

- Step 15 Leave the default settings

The screenshot shows the "Advanced Settings" page for the Qualys-Lab vendor instance. The breadcrumb trail is: Vendor Instances > Qualys-Lab. The main content area is titled "Advanced Settings" and contains three sections:

- Option Profile:** A text input field is set to "Initial Options". Below it is the text: "Enter the name of the Option Profile configured in Qualys platform for scans."
- Last Scan Results - Check Settings:** A section titled "Use the following settings to configure the access rate of Host List Detection API". It contains two input fields:
  - Last scan results check interval in minutes:** Set to "10". Below it is the text: "Valid range is between 1 and 2880."
  - Maximum requests before last scan results are checked:** Set to "100". Below it is the text: "If the number of queued requests exceeds the maximum number, the last scan results are checked before the specified time interval. Valid range is between 1 and 1000."
- Verify MAC Address:** A dropdown menu is set to "true". Below it is the text: "When set to true, the last scan results from Qualys are used only if the MAC address in the request is found in the last scan results. Otherwise, a scan is triggered."

### Scan Settings

Use the following settings to tune the access rate of Scan API

**Scan trigger interval in minutes**

10

Valid range is between 1 and 2880.

**Maximum requests before scan is triggered**

100

If the number of queued requests exceeds the maximum number, a scan is triggered before the specified time interval. Valid range is between 1 and 1000.

**Scan status check interval in minutes**

10

Valid range is between 1 and 60.

**Number of scans that can be triggered concurrently**

2

Valid range is between 1 and 200.

**Scan timeout in minutes**

240

**Maximum number of IP addresses to be submitted per scanner**

256

Valid range is between 1 and 1000.

**Choose the log level for adapter log files**

INFO

- Step 16** Select **Next**
- Step 17** Review the **Configuration**, select->**Finish**
- Step 18** You should see the Active Configuration

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

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

Third Party Vendors

### Vendor Instances

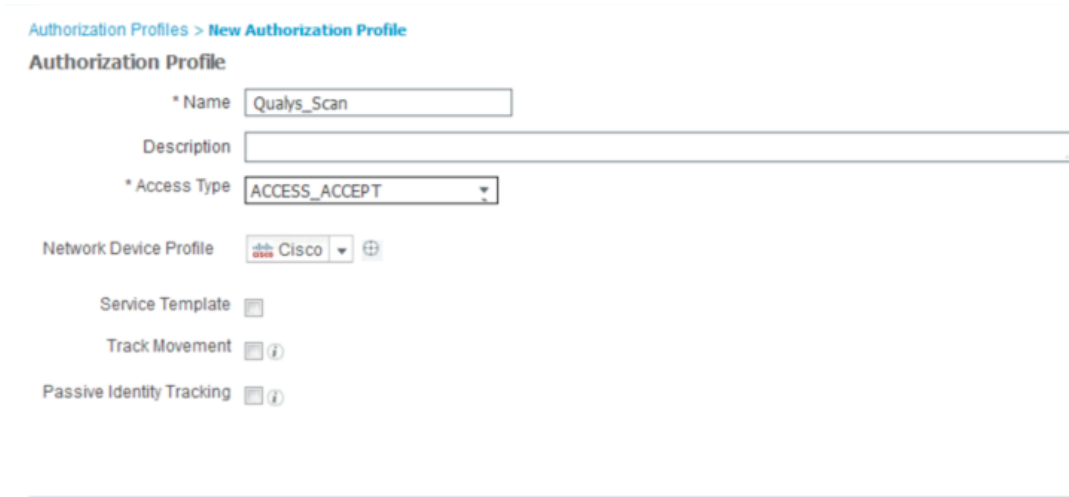
Refresh Add Trash Edit Filter Settings

Instance Name	Vendor Name	Type	Hostname	Connectivity	Status	
<input type="text" value="Instance Name"/>	<input type="text" value="Vendor Name"/>	<input type="text" value="Type"/>	<input type="text" value="Hostname"/>	<input type="text" value="Connectivity"/>	<input type="text" value="Status"/>	
<input type="checkbox"/>	Qualys-Lab	Qualys	VA	qualysguard.qg2.apps.qualys.c...	Connected	Active

## Creating VA Authorization Profile

The authorization profile contains the VA scanning settings triggering the initial VA scan.

- Step 1** Select **Policy->Policy Elements->Results->Authorization->Authorization Profiles-Add->provide policy name: Qualys\_Scan**



Authorization Profiles > New Authorization Profile

**Authorization Profile**

\* Name

Description

\* Access Type

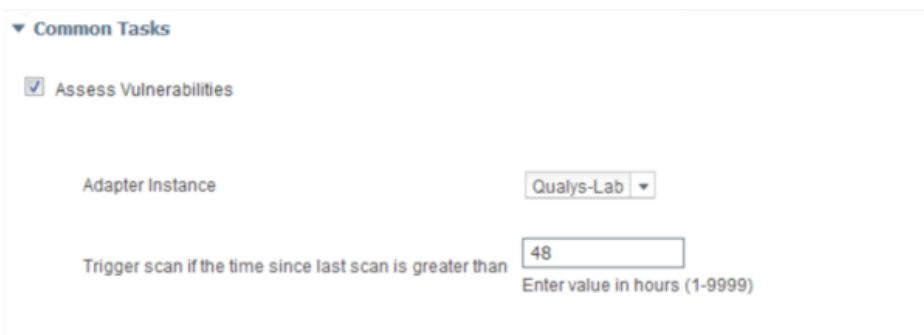
Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

- Step 2** Under Common Tasks, enable **Assess Vulnerabilities**-> select Qualys adapter instance and default trigger scan time.



▼ Common Tasks

Assess Vulnerabilities

Adapter Instance

Trigger scan if the time since last scan is greater than   
Enter value in hours (1-9999)

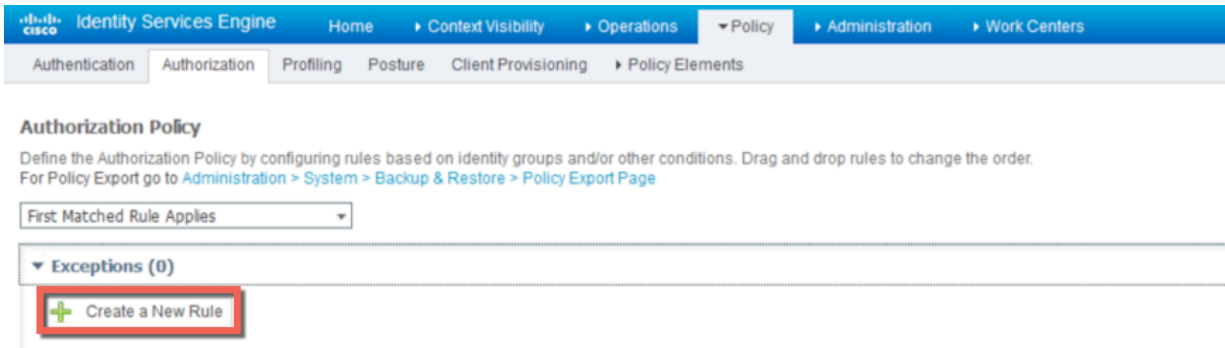
- Step 3** Select **Submit**



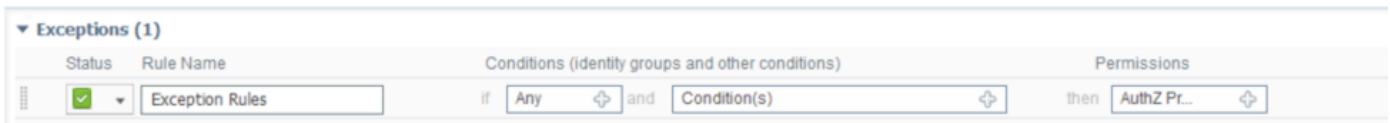
## Creating Threat-based CVSS Authorization Condition Rule

The threat-based CVSS Authorization condition rule gets triggered when the results of the returned scan match the CVSS based score. The CVSS score rating is based from 1-10. This is dependent on the having the CVSS rating in the Qualys reports. Please make sure that CVSS is enabled in Qualys, before you create this rule.

**Step 1** Select **Policy->Authorization->Exception->Create a new Rule**

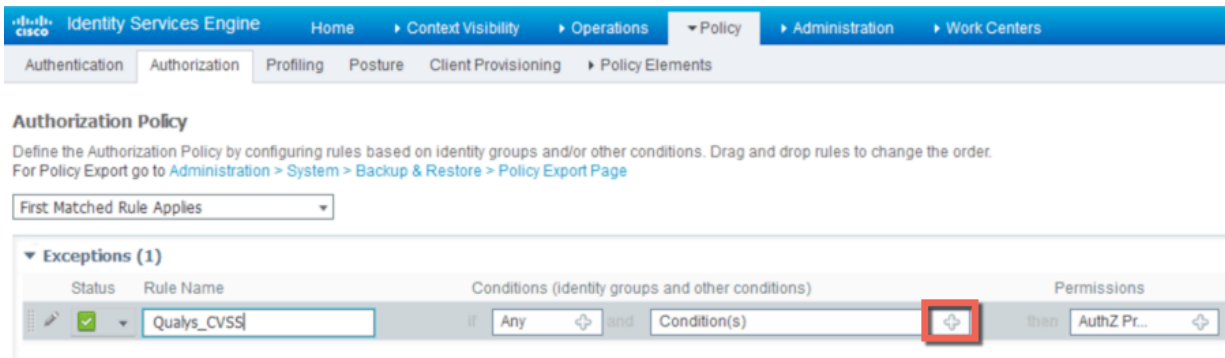


**Step 2** You should see the following

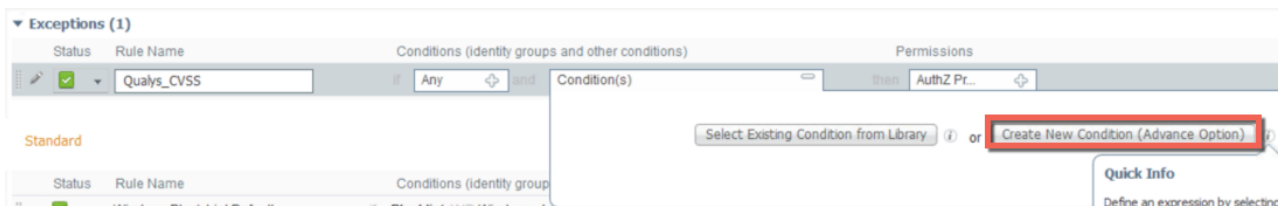


**Step 3** Provide a rule name: **Qualys\_CVSS**

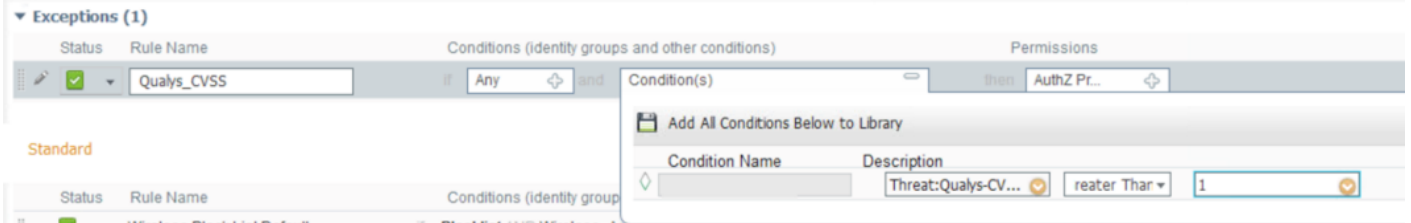
**Step 4** Under Conditions (identity groups and other conditions)->select Condition(s) +



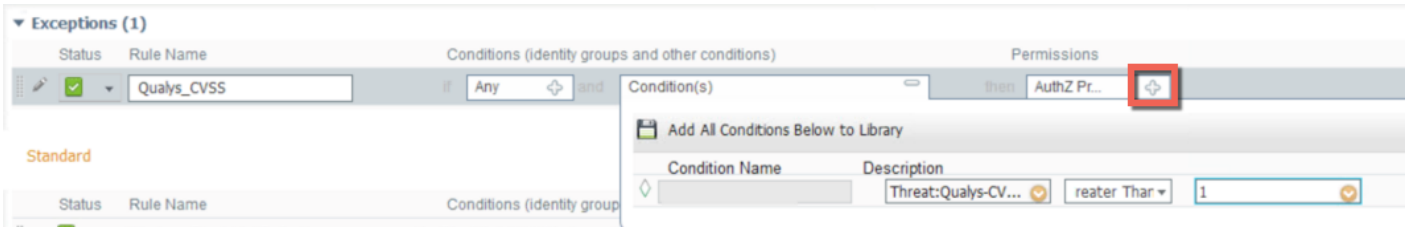
**Step 5** Select Create New Condition (Advance Option)



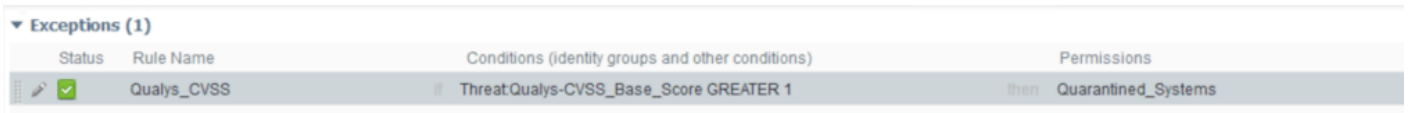
**Step 6** Under Description, select Attribute select **Threat->Qualys\_CVSS\_Base\_Score->Greater than 1**



**Step 7** Under Permissions, select **Authz Profiles +**



**Step 8** Select **Security Group->Quarantined Systems** from down arrow ->**Done**



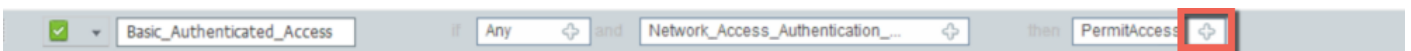
**Step 9** Select **Save**

## Add the Qualys Scan authorization profile to the Basic Authentication rule

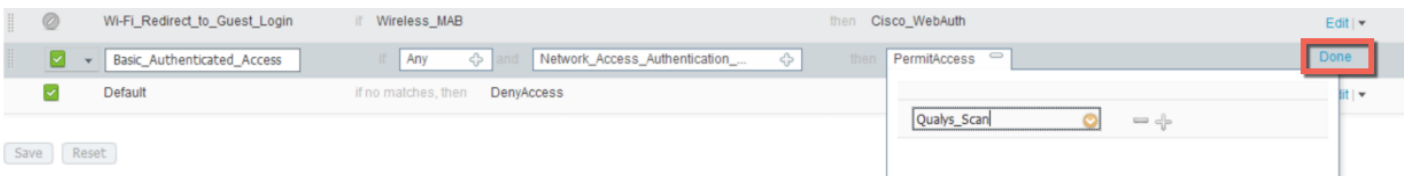
**Step 1** Select **Edit** for the **Under Basic\_Authentication\_Access** rule



**Step 2** Select **PermitAccess +**



**Step 3** From the **down arrow->Profile->Standard->Qualys\_Scan->Done**



**Step 4** Select **Save**

**Step 5** You should see the following:

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

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

▼ Exceptions (1)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Qualys_CVSS	if ThreatQualys-CVSS_Base_Score GREATER 1	then Quarantined_Systems

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
✓	Employee	if pxGridUsers:ExternalGroups EQUALS lab10.com/Users/Domain Users	then Employees
⊘	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 Qualys_Scan
✓	Default	if no matches, then	DenyAccess

# Triggering a Scan

The end-user successfully authenticates to ISE. The end-user is assigned a security group tag of Employee and triggers the initial VA scan.

- Step 1** Login to ISE
- Step 2** Select **Operations->Radius Live Log**

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...
Jul 31, 2016 03:30:50.967 PM	<span style="color: blue;">●</span>		0	jeppich@lab10.com	00:0C:29:CF:07:17	Microsoft-W...	Default >> D...	Default >> E...	Employees
Jul 31, 2016 03:30:50.255 PM	<span style="color: green;">✓</span>			jeppich@lab10.com	00:0C:29:CF:07:17	Microsoft-W...	Default >> D...	Default >> E...	Employees
Jul 31, 2016 03:30:00.534 PM	<span style="color: green;">✓</span>			hostjeppich-PC.lab10.com	00:0C:29:CF:07:17	Microsoft-W...	Default >> D...	Default >> B...	Qualys_Scan
Jul 31, 2016 02:59:47.841 PM	<span style="color: green;">✓</span>			hostjeppich-PC.lab10.com	00:0C:29:CF:07:17	Microsoft-W...	Default >> D...	Default >> B...	PermitAccess

**Step 3** Login to Qualys, select **Scans->Scans**, you should see the queued scan.

Title	Targets	User	Reference	Date	Status
IseScan	192.168.1.19	John Eppich	scan/1469980839.52977	07/31/2016	Queued
IseScan	192.168.1.8	John Eppich	scan/1464069519.09378	05/24/2016	Finished

**Step 4** After a couple of minute you should see the completed scan.

Title	Targets	User	Reference	Date	Status
IseScan	192.168.1.19	John Eppich	scan/1469980839.52977	07/31/2016	Finished
IseScan	192.168.1.8	John Eppich	scan/1464069519.09378	05/24/2016	Finished

**Step 5** Select the completed scan and select **View Results**

**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
<input checked="" type="checkbox"/> IseScan	192.168.1.19	John Eppich	scan/1469980839.5
<input type="checkbox"/> IseScan	192.168.1.8	John Eppich	scan/1464069519.0

**Preview**

**Vulnerability Scan - IseScan**  
Target: 1 IP(s)

Scan launched by John Eppich (csc2he) | Start: 07/31/2016 at 12:02:30 (GMT-0400) | Ended: 07/31/2016 at 12:07:13 (GMT-0400) | Scan Finished (00:04:43)

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	4		

**Step 6** Scroll down to **Detail Results** click on **IP address, Vulnerabilities**, you should see the CVSS base score

**Scan Results**

File View Help

Hosts: 1

**Services Detected**

1 netbios ns
1 microsoft-ds
1 DCERPC Endpoint Mapper
1 http

Services: 1

**Detailed Results**

▼ 192.168.1.19 (jeplich-pc.lab10.com, JEPPICH-PC)

▼ Vulnerabilities (3)

▼ 5 Microsoft Windows HTTP.sys Remote Code Execution Vulnerability (MS15-034)

QID:	91041	CVSS Base:	10
Category:	Windows	CVSS Temporal:	7.8
CVE ID:	<a href="#">CVE-2015-1635</a>	CVSS3 Base:	-
Vendor Reference:	<a href="#">MS15-034</a>	CVSS3 Temporal:	-
Bugtraq ID:	-		
Service Modified:	06/07/2015		
User Modified:	-		
Edited:	No		
PCI Vuln:	Yes		
Ticket State:			
THREAT:			

**Step 7** Note the **ISE Radius Live Logs**

**Step 8** Select Context Visibility->Endpoints->Vulnerable Endpoints

**Step 9** Click on the MAC Address to drill down into the details

**Step 10** You should see the attribute details:

The screenshot shows the Cisco Identity Services Engine interface. The breadcrumb navigation is: Endpoints > 00:0C:29:CF:07:17. The endpoint details are as follows:

- MAC Address: 00:0C:29:CF:07:17
- Username: LAB10\jeppich
- Endpoint Profile: Microsoft-Workstation
- Current IP Address: 192.168.1.9
- Location:

Below the details are tabs for Attributes, Authentication, Threats, and Vulnerabilities. The 'Attributes' tab is active, showing 'General Attributes' and 'Custom Attributes' sections. The 'General Attributes' section contains the following data:

Attribute Name	Attribute Value
Description	
Static Assignment	false
Endpoint Policy	Microsoft-Workstation
Static Group Assignment	false
Identity Group Assignment	Workstation

**Step 11** Select **Vulnerabilities**, you should see the following. The unique Qualys Identifier QID assigned to the vulnerability.

The screenshot shows the 'Vulnerabilities' tab selected in the Cisco Identity Services Engine interface. The breadcrumb navigation is: Endpoints > Network Devices > Vulnerabilities. Two vulnerabilities are listed:

- QID-91041**  
 Title: Microsoft Windows HTTP.sys Remote Code Execution Vulnerability (MS15-034)  
 CVSS score: 10  
 CVEIDS: CVE-2015-1635,  
 Reported by: Qualys  
 Reported at:
- QID-90043**  
 Title: SMB Signing Disabled or SMB Signing Not Required  
 CVSS score: 7.3  
 CVEIDS:  
 Reported by: Qualys  
 Reported at: