

# Tenable Nessus and Cisco Identity Service Integration

---

## Table of Contents

About this Document.....	3
Introduction .....	4
Tenable Nessus Configuration .....	5
Cisco ISE Identity Engine 1.3 Configuration.....	6
Enabling the ISE Restful APIs.....	6
Create Authorization Policy for Quarantine .....	7
Running Nessus Scan and performing ISE mitigation actions.....	8
Troubleshooting.....	12
Cannot “Open Session” Records after Tenable Nessus Scan .....	12
References.....	13

## About this Document

---

This document is intended for Cisco engineers, partners and customers deploying Tenable Nessus & Cisco Identity Services Engine (ISE) 1.3 or Cisco Identity Services Engine (ISE) 1.2. The reader should be familiar with Tenable Nessus and ISE.

Tenable Nessus and ISE integration provide session record information from the results of vulnerability scans and perform Adaptive Network Control (ANC) quarantine/unquarantine mitigation actions on the endpoint through the Cisco ISE RESTful Services API.

Nessus Enterprise versions 6.1.x and 6.2x Nessus Manager 6.3 and higher will integrate with ISE. No special licensing is required. Note that Nessus Manager replaces Nessus Enterprise, which is not End of Sale, and has a per-host license model. This does not have any impact on the ISE integration.

## Introduction

---

Tenable Nessus is a vulnerability scanner providing vulnerability discovery, compliance auditing, control systems auditing and sensitive content auditing. Tenable is able to use the Cisco Identity Service Engine (ISE) external RESTful Services APIs to provide mitigation actions on the endpoint based on the results of the scan.

The ISE external RESTful Services are based on HTTPS and REST methodology and used by Tenable for obtaining more contextual information from the endpoint. This contextual information includes the user name, device information, quarantine/unquarantine posture status, last updated record.

This document covers the initial Tenable and ISE configuration and provides a scanning example, with the results displayed in Tenable and ISE.

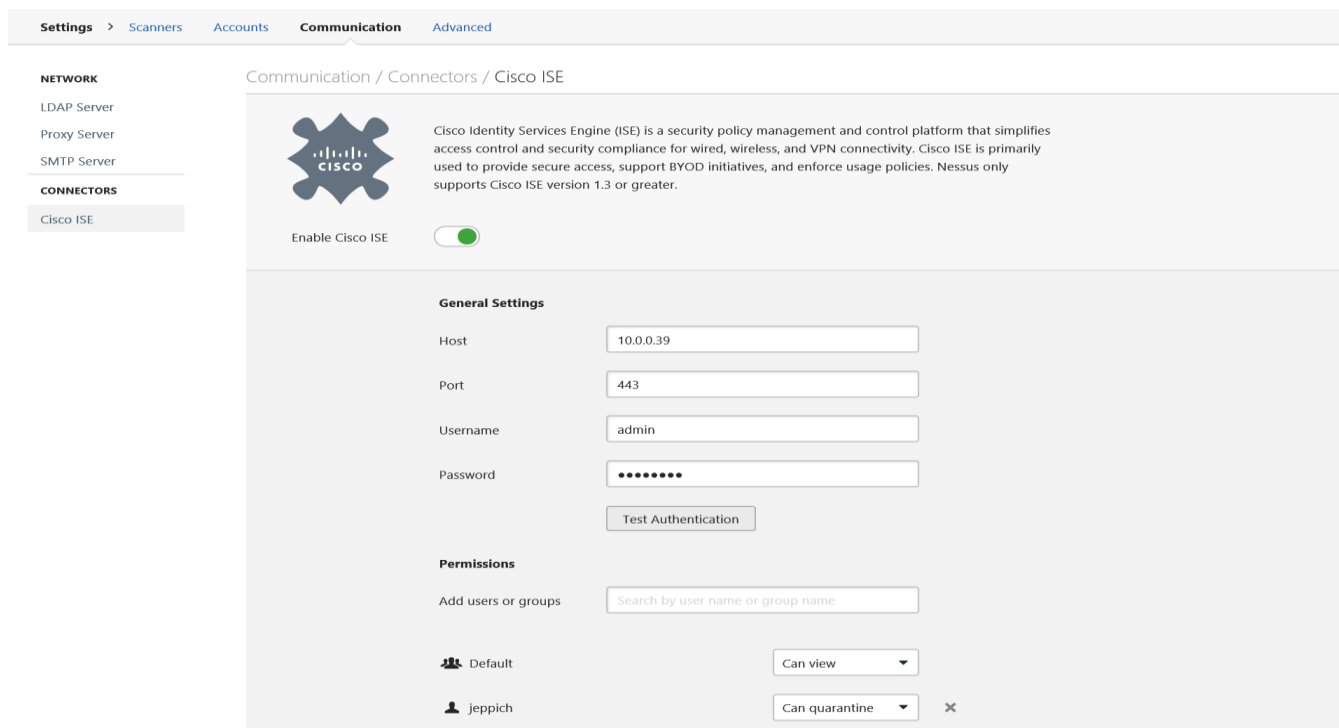
# Tenable Nessus Configuration

The Cisco ISE connection parameters are accessible under the Settings->Communication View.

The General settings parameters refer to ISE. The ISE host refers to the ISE MnT node IP address. The ISE Username and Password belong to the ISE ERS or ISE admin group. You can test the authentication between the web client where you have Nessus installed and ISE to ensure that there are no connection problems.

The Permissions parameters refer to the Nessus accounts. The “Default” group as indicated below can view the scan results. The Nessus user “jeppich” has the ability to quarantine and unquarantine hosts based on the vulnerability findings.

**Step 1** Listed below are initial ISE connection parameters  
Settings->Communication



The screenshot shows the Nessus configuration page for Cisco ISE. The breadcrumb navigation is Settings > Scanners > Accounts > Communication > Advanced. The left sidebar shows NETWORK (LDAP Server, Proxy Server, SMTP Server) and CONNECTORS (Cisco ISE). The main content area is titled "Communication / Connectors / Cisco ISE". It features a Cisco logo and a description: "Cisco Identity Services Engine (ISE) is a security policy management and control platform that simplifies access control and security compliance for wired, wireless, and VPN connectivity. Cisco ISE is primarily used to provide secure access, support BYOD initiatives, and enforce usage policies. Nessus only supports Cisco ISE version 1.3 or greater." Below this is a toggle switch for "Enable Cisco ISE" which is turned on. The "General Settings" section includes fields for Host (10.0.0.39), Port (443), Username (admin), and Password (masked with dots), along with a "Test Authentication" button. The "Permissions" section has a search box for "Add users or groups" and a table of permissions:

User/Group	Permission
Default	Can view
jeppich	Can quarantine

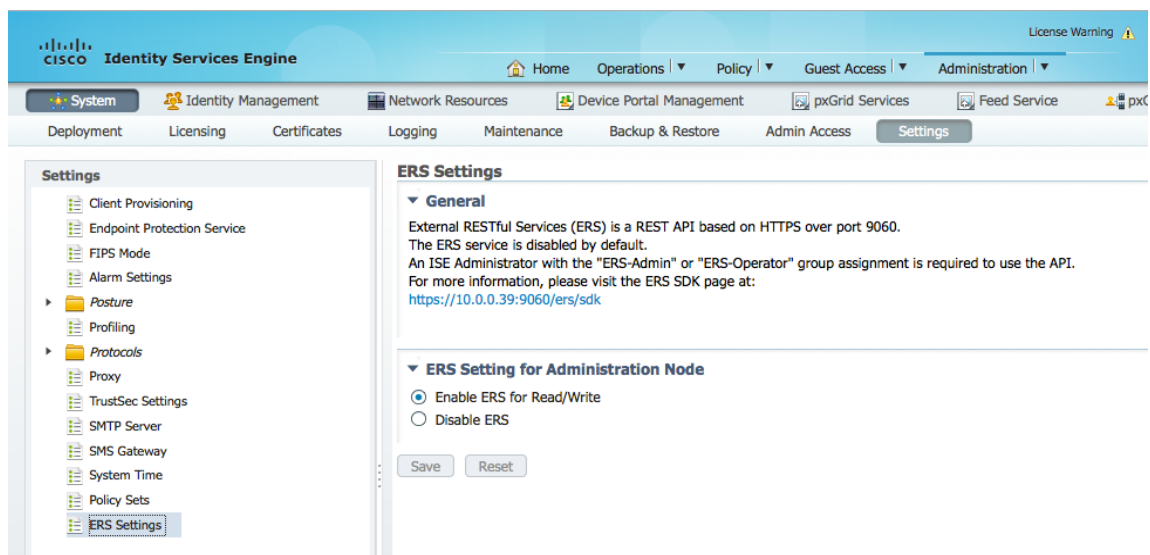
# Cisco ISE Identity Engine 1.3 Configuration

ISE will be configured to enable the RESTful APIs and Endpoint Protection Service to work. In addition an authorization profile and authorization profile for quarantining the endpoint will be created.

## Enabling the ISE Restful APIs

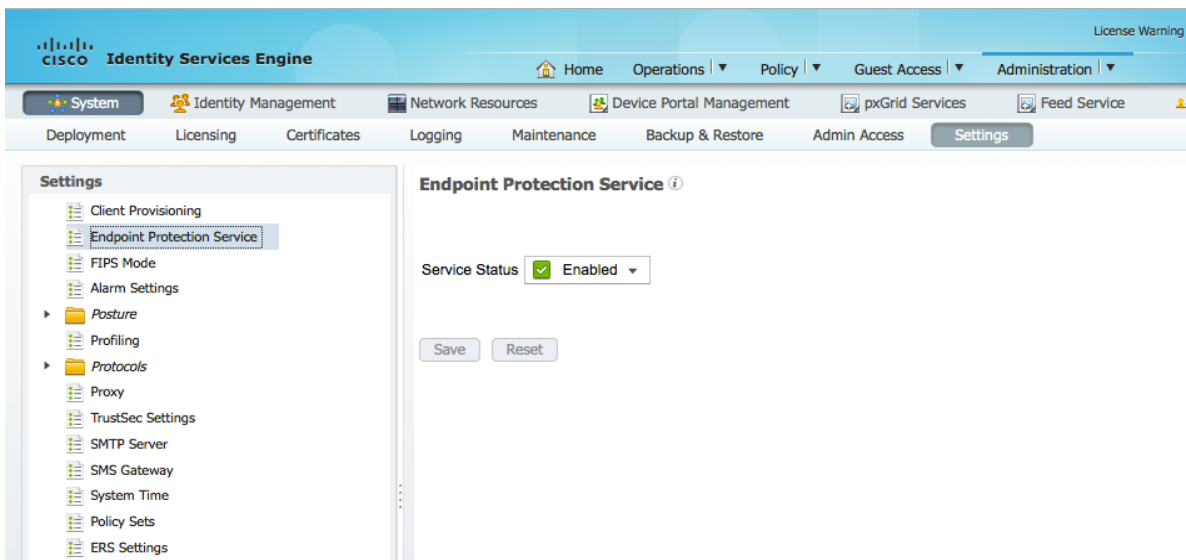
**Step 1** Enable ERS Settings  
Administration->System->Settings->ERS Settings then Save

**Note:** In a distributed ISE environment, you will also want to “enable” ERS settings for all other nodes



The screenshot shows the Cisco Identity Services Engine Administration console. The left sidebar contains a 'Settings' menu with 'ERS Settings' selected. The main content area displays the 'ERS Settings' configuration page. Under the 'General' section, there is a text block explaining that External RESTful Services (ERS) is a REST API based on HTTPS over port 9060 and is disabled by default. It also mentions that an ISE Administrator with the "ERS-Admin" or "ERS-Operator" group assignment is required to use the API. Below this, the 'ERS Setting for Administration Node' section has two radio buttons: 'Enable ERS for Read/Write' (which is selected) and 'Disable ERS'. 'Save' and 'Reset' buttons are visible at the bottom of the configuration area.

**Step 2** Enable Endpoint Protection Service  
Administration->System->Settings->enable Service Status then Save



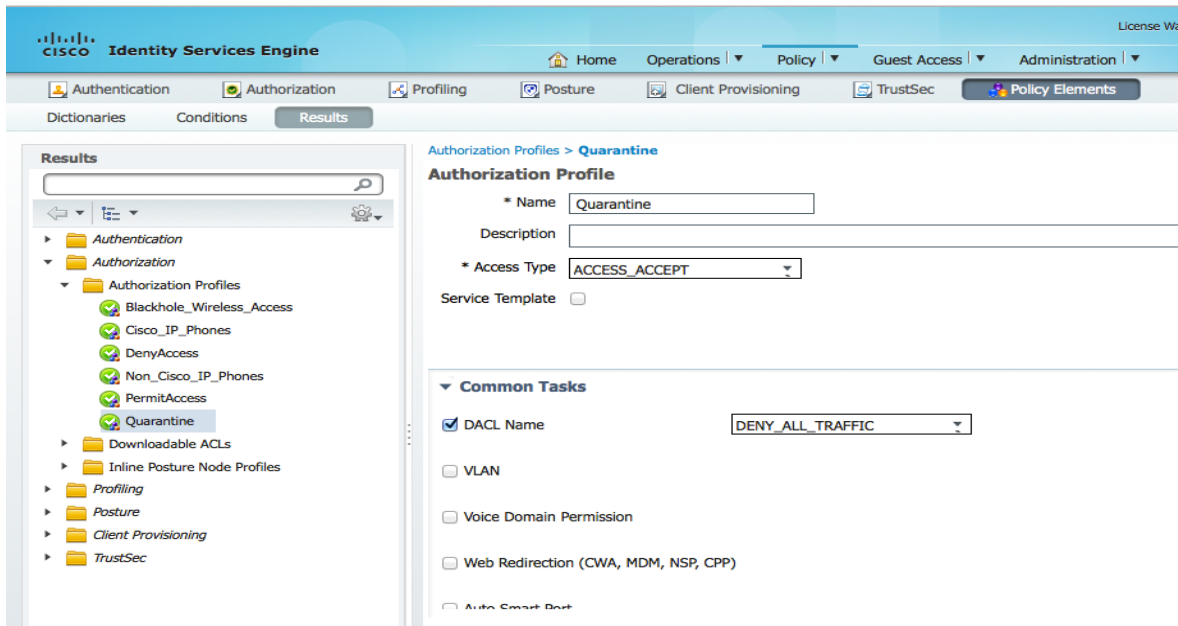
The screenshot shows the Cisco Identity Services Engine Administration console. The left sidebar contains a 'Settings' menu with 'Endpoint Protection Service' selected. The main content area displays the 'Endpoint Protection Service' configuration page. The 'Service Status' is set to 'Enabled' with a green checkmark icon. 'Save' and 'Reset' buttons are visible at the bottom of the configuration area.

## Create Authorization Policy for Quarantine

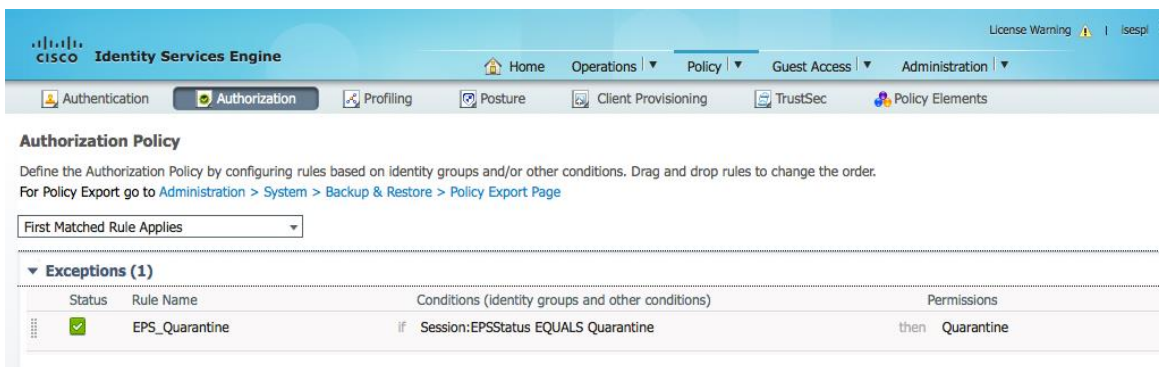
Here we create the EPS Quarantine Authorization Profile and Authorization Policy for quarantining the endpoint.

- Step 1** Create the Quarantine Authorization Profile  
 Policy->Policy Elements->Results->Authorization->Authorization Profiles->Add the Quarantine profile, then Submit

**Note:** You can elect to DENY or ALLOW all traffic for testing. The Authorization policy profile results will still be “Quarantine” in the ISE Operation Authentication Views



- Step 2** Create the EPS Quarantine Authorization Policy  
 Policy->Authorization->Exceptions and create a new rule with the following:
- Provide the Rule Name: EPS\_Quarantine
  - Create new Condition: Session:Equals:Quarantine
  - Permissions: Quarantine from Standard Profile
- Click->Done->Save



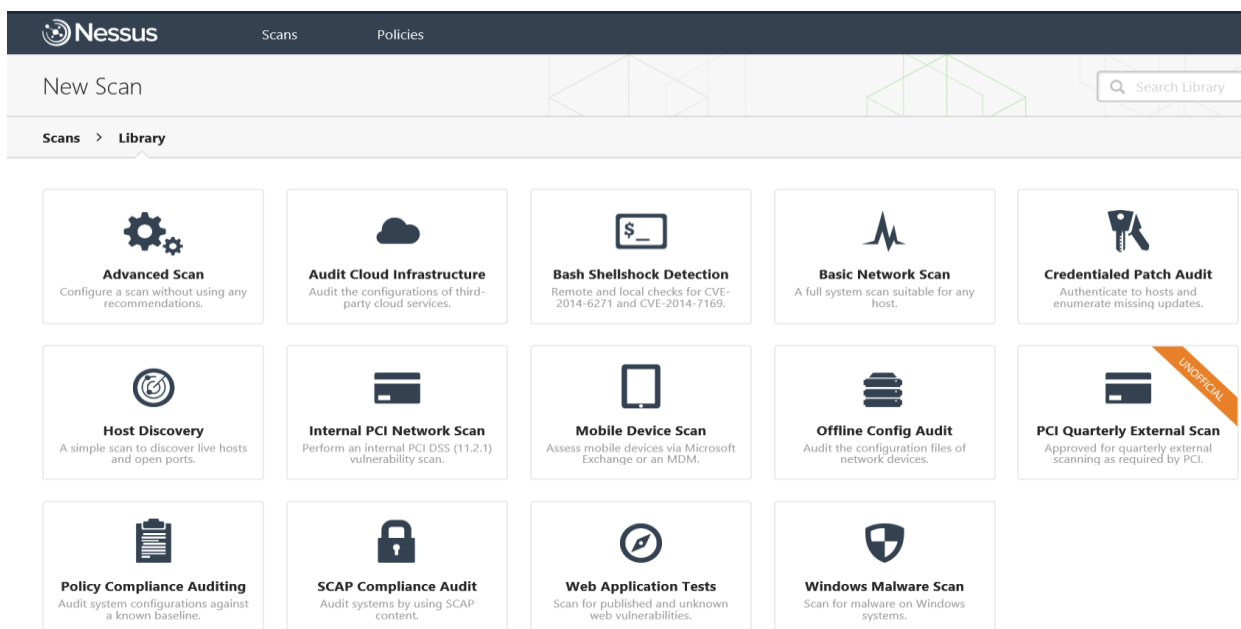
# Running Nessus Scan and performing ISE mitigation actions

These steps provide details on running a “Basic Network Scan” and quarantining/unquarantining the endpoint based on the results of the scan.

**Step 1** Run a “Basic Network Scan”  
New Scan->Scans->Basic Network Scan

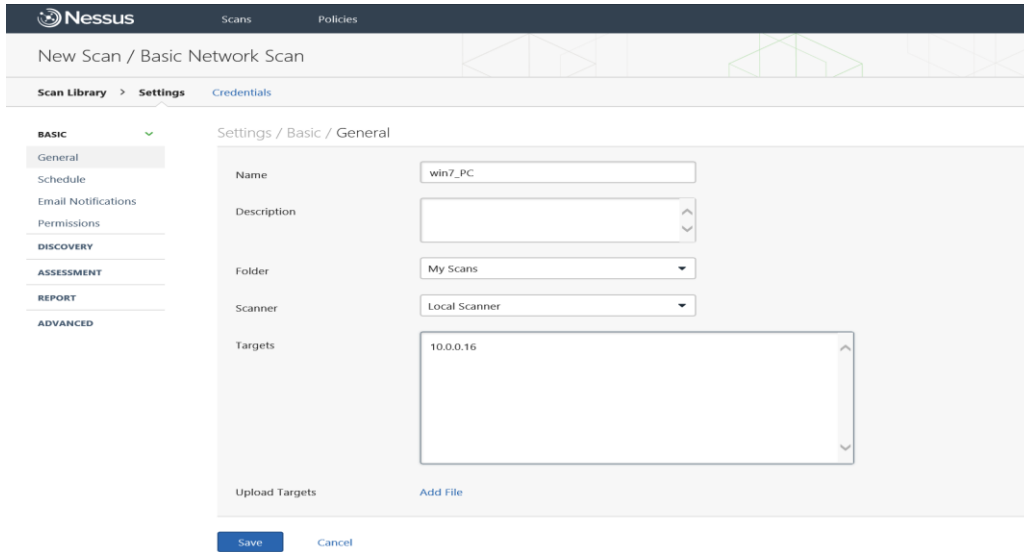
**Note:** Any Nessus Scan can be run to for ISE mitigations actions to appear, give the Nessus user account has “quarantine” permissions.

While the Cisco ISE connector may appear for all scans. It's unlikely Audit Cloud Infrastructure and Offline Config Audit scans will produce data relevant to quarantine, since they aren't directed at hosts.

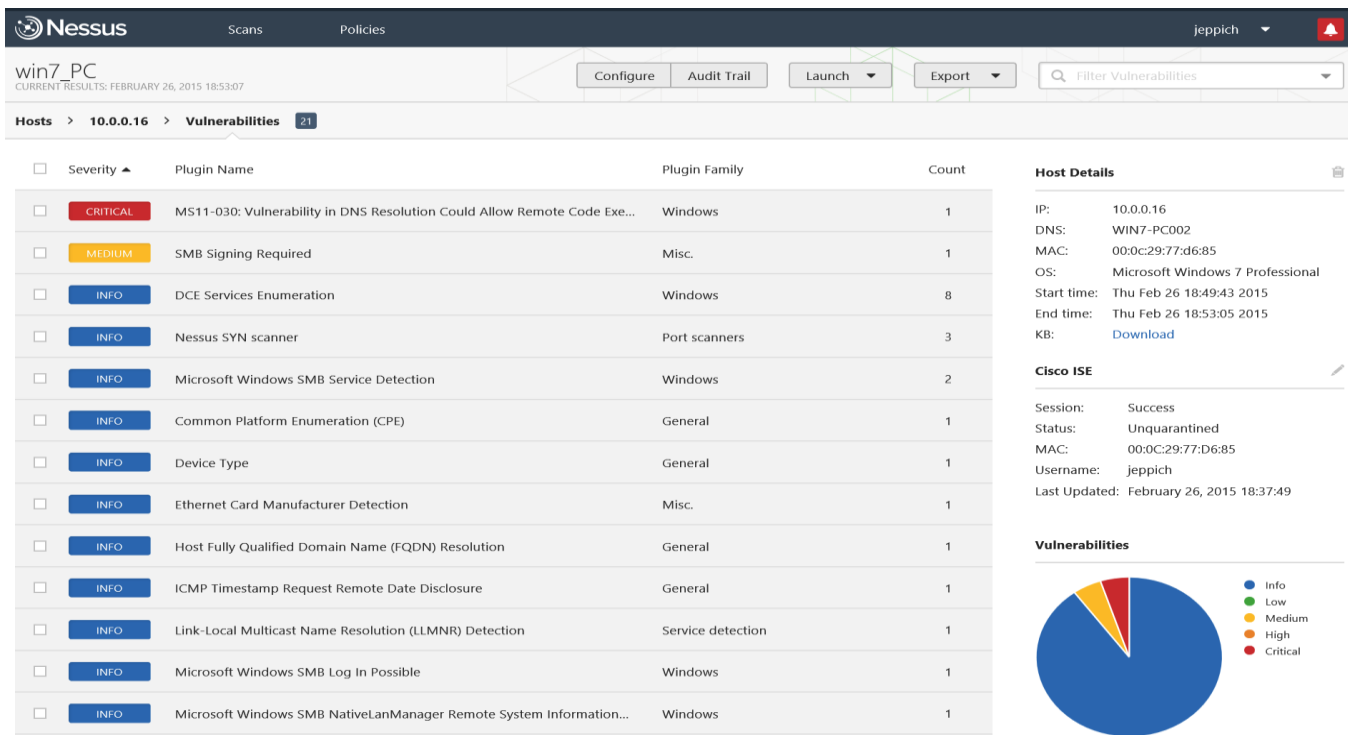


**Step 2** Provide the host name and target information then save, this will initiate the scan.

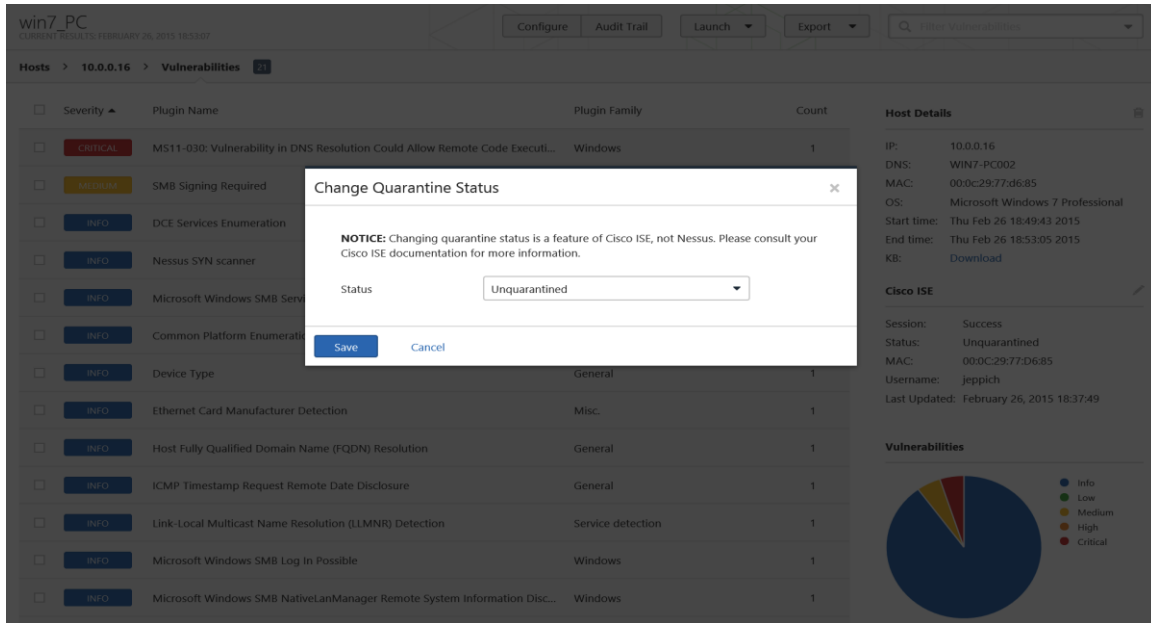




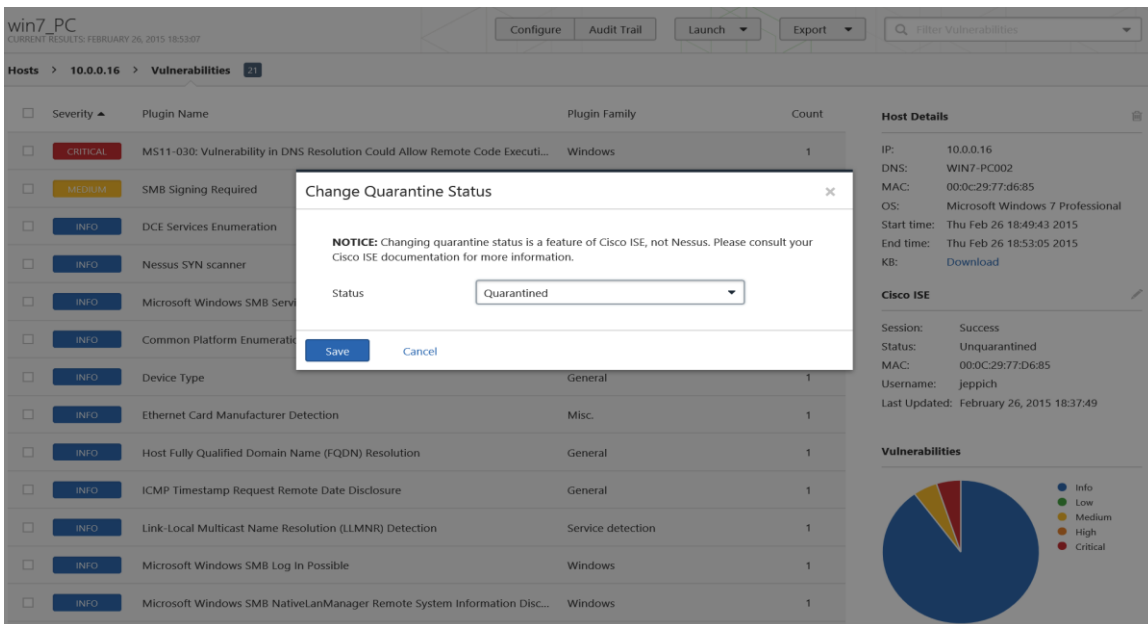
**Step 3** Once the scan completes select the host name to view the scan results  
 The Cisco ISE Session record provides IEE 802.1X authenticated host mitigation status information.



**Step 4** To quarantine the endpoint, click on the pencil next to Cisco ISE which brings up the mitigation action window.



**Step 5** Click on the drop-down and select “Quarantined”



**Step 6** You should that the device has been “Quarantined”

win7\_PC  
CURRENT RESULTS: FEBRUARY 26, 2015 18:53:07

Configure Audit Trail Launch Export Filter Vulnerabilities

Hosts > 10.0.0.16 > Vulnerabilities 21

Severity	Plugin Name	Plugin Family	Count
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Exe...	Windows	1
MEDIUM	SMB Signing Required	Misc.	1
INFO	DCE Services Enumeration	Windows	8
INFO	Nessus SYN scanner	Port scanners	3
INFO	Microsoft Windows SMB Service Detection	Windows	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1
INFO	Microsoft Windows SMB Log In Possible	Windows	1
INFO	Microsoft Windows SMB NativeLanManager Remote System Information...	Windows	1

**Host Details**

IP: 10.0.0.16  
 DNS: WIN7-PC002  
 MAC: 00:0c:29:77:d6:85  
 OS: Microsoft Windows 7 Professional  
 Start time: Thu Feb 26 18:49:43 2015  
 End time: Thu Feb 26 18:53:05 2015  
 KB: [Download](#)

**Cisco ISE**

Session: Success  
 Status: Quarantined  
 MAC: 00:0c:29:77:d6:85  
 Username: jeppich  
 Last Updated: February 26, 2015 18:37:49

**Vulnerabilities**

**Step 7** View in ISE  
 Operations->Authentications  
 Notice the endpoint has been quarantined

License Warning | isespl | admin | Logout | Feedback

**Identity Services Engine**

Home Operations Policy Guest Access Administration

Authentications Reports Endpoint Protection Service Troubleshoot

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

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port	Identity Group	Posture Status	Server	Event
2015-02-26 19:10:21.908	Info		0	jeppich	00:0c:29:77:d6:85	VMWare-Device								isespl	Session State is Started
2015-02-26 19:10:21.900	Success			jeppich	00:0c:29:77:d6:85	VMWare-Device	Default >> Dot1X >> ... Default >> EPS_Quar...	Quarantine	sw	GigabitEthernet1/0/23	Profiled			isespl	Authentication succeeded
2015-02-26 19:07:03.330	Success				00:0c:29:77:d6:85					sw				isespl	Dynamic Authorization succeeded
2015-02-26 18:37:49.508	Success			jeppich	00:0c:29:77:d6:85	VMWare-Device	Default >> Dot1X >> ... Default >> Basic_Aut...	PermitAccess	sw	GigabitEthernet1/0/23	Profiled			isespl	Authentication succeeded
2015-02-26 18:37:26.764	Success			host/WIN7-PC00	00:0c:29:77:d6:85	VMWare-Device	Default >> Dot1X >> ... Default >> Basic_Aut...	PermitAccess	sw	GigabitEthernet1/0/23	Profiled			isespl	Authentication succeeded

## Troubleshooting

---

### Cannot “Open Session” Records after Tenable Nessus Scan

If you receive cannot “Open session” record after a completed Tenable Nessus scan and you have verified the ISE connection parameters. Please check the switch configuration and ensure that you have:

```
# aaa accounting system default start-stop group radius
```

```
# aaa accounting update periodic {value in minutes}
```

For reference please see: [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_usr\\_aaa/configuration/xr-3s/sec\\_usr\\_aaa-xr-3s-book/sec-cfg-accountg.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xr-3s/sec_usr_aaa-xr-3s-book/sec-cfg-accountg.html)

## References

---

Cisco Identity Services Engine ISE 1.3 Administration Guide: [http://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin\\_guide/b\\_ise\\_admin\\_guide\\_13.html](http://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13.html)

Enabling ISE 1.3 RESTFUL APIs : [http://www.cisco.com/c/en/us/td/docs/security/ise/1-3/api\\_ref\\_guide/api\\_ref\\_book/ise\\_api\\_ref\\_ers1.html](http://www.cisco.com/c/en/us/td/docs/security/ise/1-3/api_ref_guide/api_ref_book/ise_api_ref_ers1.html)

Enabling ISE 1.2 RESTFUL APIs: [http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/api\\_ref\\_guide/api\\_ref\\_book/ise\\_api\\_ref\\_ers1.html](http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/api_ref_guide/api_ref_book/ise_api_ref_ers1.html)

Nessus 6.3 Installation and Configuration Guide:  
[http://static.tenable.com/documentation/nessus\\_6.3\\_installation\\_guide.pdf](http://static.tenable.com/documentation/nessus_6.3_installation_guide.pdf)