**Bot Questions and Answers**

What is threat centric NAC service?

Threat Centric Network Access Control (TC-NAC) feature enables you to create authorization policies based on the threat and vulnerability attributes received from the threat and vulnerability adapters. Threat severity levels and vulnerability assessment results can be used to dynamically control the access level of an endpoint or a user.

You can configure the vulnerability and threat adapters to send high fidelity Indications of Compromise (IoC), Threat Detected events, and CVSS scores to Cisco ISE, so that threat-centric access policies can be created to change the privilege and context of an endpoint accordingly.

Does Cisco ISE trigger a CoA for a threat event?

No, Cisco ISE does not trigger a CoA for a threat event. Cisco ISE triggers CoA for an endpoint only when it receives a vulnerability event.

Can I use the vulnerability attributes to create authorization policies?

You can create an authorization policy by using the vulnerability attributes to automatically quarantine the vulnerable endpoints based on the attribute values. For example:

Any Identity Group & Threat:Qualys-CVSS\_Base\_Score > 7.0 -> Quarantine

What are the adapters that are supported by Cisco ISE Threat Centric NAC service?

Cisco ISE supports the following adapters:

* SourceFire FireAMP
* Cognitive Threat Analytics (CTA) adapter
* Qualys
* Rapid7 Nexpose
* Tenable Security Center

How can I clear the threat and vulnerabilities associated with an endpoint?

You can use the Clear Threat and Vulnerabilities option on the Compromised Endpoints page to clear the threat and vulnerabilities associated with an endpoint (from Cisco ISE system database).

What action does Cisco ISE take in the absence of an ANC policy?

When a threat event is detected for an endpoint, you can select the MAC address of the endpoint on the Compromised Endpoints page and apply an ANC policy, such as Quarantine. Cisco ISE triggers CoA for that endpoint and applies the corresponding ANC policy. If ANC policy is not available, Cisco ISE triggers CoA for that endpoint and applies the original authorization policy.

Which page displays the MAC addresses of compromised endpoints?

The Context Visibility > Endpoints > Compromised Endpoints page displays the MAC addresses of compromised endpoints.

When does Cisco ISE Threat Centric NAC service trigger a CoA?

When a vulnerability event is received for an endpoint, Cisco ISE triggers CoA for that endpoint. However, CoA is not triggered when a threat event is received.

What are the important points to be noted while enabling the Threat Centric NAC service?

Note the following points while enabling the Threat Centric NAC service:

* The Threat Centric NAC service requires an Apex license.
* You will need a separate Policy Service Node (PSN) for Threat Centric NAC service. You must enable only Threat Centric NAC persona on this node.
* Threat Centric NAC service can be enabled on only one node in a deployment.
* You can add only one instance of an adapter per vendor for Vulnerability Assessment service. However, you can add multiple instances of FireAMP adapter.
* You can stop and restart an adapter without losing its configuration. After configuring an adapter, you can stop the adapter at any point of time. The adapter would remain in this state even when the ISE services are restarted. Select the adapter and click Restart to start the adapter again.

Note: When an adapter is in Stopped state, you can edit only the name of the adapter instance; you cannot edit the adapter configuration or the advanced settings.

What are the options available in the Threat Centric NAC Live Logs page?

The Threat Centric NAC Live Logs page (Operations > TC NAC Live Log) lists all the threat and vulnerability events. It displays the incident type, adapter name, matching authorization rule, and authorization profiles (old and new) for an endpoint. You can also view the detailed information for an event.

What are the alarms that are triggered by the Threat Centric NAC service?

* Adapter not reachable (syslog ID: 91002)—Indicates that the adapter cannot be reached.
* Adapter Connection Failed (syslog ID: 91018)—Indicates that the adapter is reachable but the connection between the adapter and source server is down.
* Adapter Stopped Due to Error (syslog ID: 91006)—This alarm is triggered if the adapter is not in the desired state. If this alarm is displayed, check the adapter configuration and server connectivity. Refer to the adapter logs for more details.
* Adapter Error (syslog ID: 91009)—Indicates that the Qualys adapter is unable to establish a connection with or download information from the Qualys site.

What are the reports that are generated by the Threat Centric NAC service?

* Adapter Status—The Adapter Status report displays the status of the threat and vulnerability adapters.
* COA Events—When a vulnerability event is received for an endpoint, Cisco ISE triggers CoA for that endpoint. The CoA Events report displays the status of these CoA events. It also displays the old and new authorization rules and the profile details for these endpoints.
* Threat Events—The Threat Events report provides a list of all the threat events that Cisco ISE receives from the various adapters that you have configured. Vulnerability Assessment events are not included in this report.
* Vulnerability Assessment—The Vulnerability Assessment report provides information about the assessments that are happening for your endpoints. You can view this report to check if the assessment is happening based on the configured policy.

Which page displays the total number of received events, threat events, vulnerability events, and CoAs issued?

You can view the total number of received events, threat events, vulnerability events, and CoAs in the Operations > Reports > Diagnostics > ISE Counters > Threshold Counter Trends page. The values for these attributes are collected every 5 minutes, so these values represent the count for the last 5 minutes.

Describe the dashlets that are available in the Threat dashboard.

* Total Compromised Endpoints dashlet displays the total number of endpoints (both connected and disconnected endpoints) that are currently impacted on the network.
* Compromised Endpoints Over Time dashlet displays a historical view of the impact on endpoints for the specified time period.
* Top Threats dashlet displays the top threats based on the number of endpoints impacted and the severity of the threat.
* You can use the Threats Watchlist dashlet to analyze the trend of selected events.

What do you infer from the size of the bubbles in the Top Threats dashlet?

The size of the bubbles in the Top Threats dashlet indicates the number of endpoints impacted and the light shaded area indicates the number of disconnected endpoints. The color as well as the vertical scale indicate the severity of the threat.

What are the two categories of threat and their respective severity attributes?

There are two categories of threat—Indicators and Incidents. The severity attribute for Indicator is "Likely\_Impact" and the severity attribute for Incident is "Impact\_Qualification”.

Describe the dashlets that are available in the Threat dashboard.

The Vulnerability dashboard on the Home page contains the following dashlets:

* Total Vulnerable Endpoints dashlet displays the total number of endpoints that have a CVSS score greater than the specified value. Also displays the total number of connected and disconnected endpoints that have a CVSS score greater than the specified value.
* Top Vulnerability dashlet displays the top vulnerabilities based on the number of endpoints impacted or the severity of the vulnerability. The size of the bubbles in the Top Vulnerability dashlet indicates the number of endpoints impacted and the light shaded area indicates the number of disconnected endpoints. The color as well as the vertical scale indicates the severity of the vulnerability.
* You can use the Vulnerability Watchlist dashlet to analyze the trend of selected vulnerabilities over a period of time. Click the search icon in the dashlet and enter the vendor-specific id ("qid" for Qualys ID number) to select and view the trend for that particular ID number.
* The Vulnerable Endpoints Over Time dashlet displays a historical view of the impact on endpoints over time.

How do I find the CVSS scores related to security vulnerabilities?

The Endpoint Count By CVSS graph on the Vulnerable Endpoints page shows the number of endpoints that are affected and their CVSS scores. You can also view the list of affected endpoints on the Vulnerable Endpoints page. You can click on the device link to view the detailed vulnerability information for each endpoint.

Where can I locate the Threat Centric NAC service logs?

Threat Centric NAC service logs are included in the support bundle (see [Download Cisco ISE Log Files](https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/admin_guide/b_ise_admin_guide_23/b_ise_admin_guide_23_chapter_011011.html#task_B53D856F84594FF5A70647D5A64439E0)). Threat Centric NAC service logs are located at support/logs/TC-NAC/.

How do I enable the Cisco ISE Threat Centric NAC service?

To configure vulnerability and threat adapters, you must first enable the Threat Centric NAC service. This service can be enabled on only one Policy Service Node in your deployment.

Step 1: Choose Administration > System > Deployment.

Step 2: Check the check box next to the PSN on which you want to enable the Threat Centric NAC service and click Edit.

Step 3: Check the Enable Threat Centric NAC Service check.

What are the steps to be performed to configure the Nexpose adapter?

You must create a Nexpose adapter for Cisco ISE to communicate with Nexpose and obtain the VA results.

Before You Begin

* Ensure that you have enabled the Threat-Centric NAC service in Cisco ISE.
* Log in to Nexpose Security Console and create a user account with the following privileges:
* Manage sites
* Create reports
* Import the Nexpose server certificate in to the Trusted Certificates store in Cisco ISE (Administration > Certificates > Certificate Management > Trusted Certificates > Import). Ensure that the appropriate root and intermediate certificates are imported (or present) in the Cisco ISE Trusted Certificates store.
* Cisco ISE communicates with Nexpose over HTTPS/SSL (port 3780).

Step 1: Choose Administration > Threat Centric NAC > Third Party Vendors.

Step 2: Click Add.

Step 3: From the Vendor drop-down list, choose Rapid7 Nexpose:VA.

Step 4: Enter a name for the adapter instance. For example, Nexpose.

The listing page appears with a list of configured adapter instances.

Step 5: Refresh the Vendor Instances listing page. The status for the newly added Nexpose adapter should change to Ready to Configure.

Step 6: Click the Ready to Configure link.

Step 7: Enter the following values in the Nexpose configuration screen and click Next.

Nexpose Host: The hostname of the Nexpose server.

Nexpose Port: 3780.

Username: Nexpose Admin user account.

Password: Password for the Nexpose Admin user account.

HTTP Proxy Host: If you have a proxy server configured to route all Internet traffic, enter the hostname of the proxy server.

HTTP Proxy Port: Enter the port number used by the proxy server.

Step 8: Click Next to configure Advanced Settings.

Step 9: Enter the following values in the Advanced Settings page. The settings in this page determine whether an on-demand scan will be triggered or the last scan results will be used for VA.

Settings for checking latest scan results

Interval between checking the latest scan results in minutes: Time interval in minutes after which the last scan results must be checked again. Valid range is between 1 and 2880.

Number of pending requests that can trigger checking the latest scan results: If the number of queued scan requests exceeds the maximum number specified here, the last scan results are checked before the time interval specified in Interval between checking the latest scan results in minutes field. Valid range is between 1 and 1000.

Verify MAC address: True or False. When set to true, the last scan results from Nexpose would be used only if it includes the MAC address of the endpoint.

Scan settings

Scan trigger interval for each site in minutes: Time interval in minutes after which a scan is triggered. Valid range is between 1 and 2880.

Number of pending requests before a scan is triggered for each site: If the number of queued scan requests exceeds the maximum number specified here, a scan would be triggered before the time interval specified in Scan timeout in minutes field. Valid range is between 1 and 1000.

Scan timeout in minutes: Time in minutes after which the scan request will time out. If a scan request times out, an alarm is generated. Valid range is between 20 and 1440.

Number of sites for which scans could be triggered concurrently: The number of sites for which scans can be run concurrently. Valid range is between 1 and 200.

Timezone: Choose the time zone based on the time zone that is configured in the Nexpose server.

Http timeout in seconds: Time interval in seconds for Cisco ISE to wait for a response from Nexpose. Valid range is between 5 and 1200.

Choose the log level for adapter log files: Choose a log level for the adapter. The available options are ERROR, INFO, DEBUG, and TRACE.

Step 10: Click Next to review the Configuration Settings.

Step 11: Click Finish.

What are the steps to be performed to add a SourceFire FireAmp adapter?

Before You Begin:

* You must have an account with SourceFire FireAMP.
* You must deploy FireAMP clients on all endpoints.
* You must enable Threat Centric NAC service on the deployment node (see Enable Threat Centric NAC Service).

FireAMP adapter uses SSL for REST API calls (to the AMP cloud) and AMQP to receive the events. It also supports the use of proxy. FireAMP adapter uses port 443 for communication.

Step 1: Choose Administration > Threat Centric NAC > Third Party Vendors.

Step 2: Click Add.

Step 3: Select AMP : Threat from the Vendor drop-down list.

Step 4: Enter a name for the adapter instance.

Step 5: Click Save.

Step 6: Refresh the Vendor Instances listing page. You can configure the adapter only after the adapter status changes to Ready to Configure on the Vendor Instances listing page.

Step 7: Click the Ready to configure link.

Step 8: (Optional) If you have configured a SOCKS proxy server to route all the traffic, enter the hostname and the port number of the proxy server.

Step 9: Select the cloud to which you want to connect. You can select US cloud or EU cloud.

Step 10: Select the event source to which you want to subscribe. The following options are available:

* AMP events only
* CTA events only
* CTA and AMP events

Step 11: Click the FireAMP link and login as admin in FireAMP. Click Allow in the Applications pane to authorize the Streaming Event Export request. You will be redirected back to Cisco ISE.

Step 12: Select the events (for example, suspicious download, connection to suspicious domain, executed malware, java compromise) that you want to monitor.

When you change the advanced settings or reconfigure an adapter, if there are any new events added to the AMP cloud, those events are also listed in the Events Listing page.

You can choose a log level for the adapter. The available options are: Error, Info, and Debug.

The summary of the adapter instance configuration will be displayed in the Configuration Summary page.

How do I configure the Cognitive Threat Analytics Adapter?

Before You Begin

* You must enable Threat Centric NAC service on the deployment node (see Enable Threat Centric NAC Service).
* Log in to Cisco Cognitive Threat Analytics (CTA) portal via http:/​/​cognitive.cisco.com/​login and request CTA STIX/TAXII service. For more information, see Cisco ScanCenter Administrator Guide.
* Cognitive Threat Analytics (CTA) adapter uses TAXII protocol with SSL to poll the CTA cloud for detected threats. It also supports the use of proxy.
* Import the adapter certificate in to the Trusted Certificate Store. Choose Administration > System > Certificates > Trusted Certificates > Import to import the certificate.

Step 1: Choose Administration > Threat Centric NAC > Third Party Vendors.

Step 2: Click Add.

Step 3: Select CTA : Threat from the Vendor drop-down list.

Step 4: Enter a name for the adapter instance.

Step 5: Click Save.

Step 6: Refresh the Vendor Instances listing page. You can configure the adapter only after the adapter status changes to Ready to Configure on the Vendor Instances listing page.

Step 7: Click the Ready to configure link.

Step 8: Enter the following details:

* CTA STIX/TAXII service URL—URL of the CTA cloud service. By default, the following URL is used: https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService/
* CTA feed name—Enter the feed name of the CTA cloud service.
* CTA username and password—Enter the username and password for the CTA cloud service.
* Proxy host and port (optional)—If you have configured a proxy server to route all the traffic, enter the hostname and the port number of the proxy server.
* Polling interval—Time interval between each poll. Default value is 30 minutes.
* First Poll Duration in hours—Age of the data to be pulled at the first poll. Default value is 2 hours. Maximum value is 12 hours.
* Incident Type—The following options are available:
* CTA events only
* AMP events only
* CTA and AMP events

Step 9: Click Next.

Step 10: Click Advanced Settings to configure the following options:

* Impact Qualification—Select the severity level of the incident to be polled. The following options are available:
  + 1 - Insignificant
  + 2 - Distracting
  + 3 - Painful
  + 4 - Damaging
  + 5 - Catastrophic

For example, if you have selected "3-Painful", incidents with this severity level (3-Painful) and above (in this case, 4-Damaging and 5-Catastrophic) are polled.

* Logging level—Choose a log level for the adapter. The available options are: Error, Info, and Debug.

Step 11: Click Finish.

Note:

CTA works with user identities listed in the web proxy logs as IP addresses or usernames. Specifically, in the case of IP addresses, the IP address of a device that is available through the proxy logs may collide with the IP address of another device on the internal network. For example, roaming users connected via AnyConnect and a split-tunnel directly to the internet could acquire a local IP range address (for example, 10.0.0.X address), which may collide with an address in an overlapping private IP range used in an internal network. We recommend that you take into account the logical network architecture while defining the policies to avoid quarantine actions being applied on mismatched devices.

How do I configure authorization profiles for the CTA adapter?

For each threat event, the CTA adapter returns one of the following values for the Course of Action attribute: Internal Blocking, Monitoring, or Eradication. You can create authorization profiles based on these values.

Step 1: Choose Policy > Policy Elements > Authorization > Authorization Profiles.

Step 2: Click Add.

Step 3: Enter a name and description for the authorization profile.

Step 4: Select the Access Type.

Step 5: Enter the required details and click Submit.

How do I configure authorization polices using the Course of Action attribute?

You can use the CTA-Course\_Of\_Action attribute to configure authorization policies for the endpoints for which threat events are reported. This attribute is available in the Threat directory.

You can also create exception rules based on the CTA-Course\_Of\_Action attribute.

Step 1: Choose Policy > Policy Sets You can edit an existing policy rule or create a new exception rule for the endpoints with threat events.

Step 2: Create a condition to check for the CTA-Course\_Of\_Action attribute value and assign the appropriate authorization profile. For example:

Network\_Access\_Authentication\_Passed AND ThreatCTA-Course\_Of\_Action CONTAINS Internal Blocking then blocking (authorization profile)

Note:

"Internal Blocking" is the recommended Course of Action attribute to be used for quarantining the endpoints.

Step 3: Click Save.

When a threat event is received for an endpoint, Cisco ISE checks if there is any matching authorization policy for the endpoint and triggers CoA only if the endpoint is active. If the endpoint is offline, threat event details are added to the Threat Events report (Operations > Reports > Threat Centric NAC > Threat Events).

Note:

Sometimes CTA sends multiple risks and their associated Course of Action attributes in one incident. For example, it can send "Internal Blocking" and "Monitoring" (course of action attributes) in one incident. In this case, if you have configured an authorization policy to quarantine endpoints using "equals" operator, the endpoints will not be quarantined. For example:

CTA-Course\_Of\_Action EQUALS Internal Blocking then Quarantine\_Systems (authorization profile)

In such cases, you must use "contains" operator in the authorization policy to quarantine the endpoints. For example:

CTA-Course\_Of\_Action CONTAINS Internal Blocking then Quarantine\_Systems

Who are the Vulnerability Assessment (VA) Ecosystem Partners that obtain vulnerability assessment results of endpoints that connect to the Cisco ISE network?

Cisco Identity Services Engine integrates with the following Vulnerability Assessment (VA) Ecosystem Partners to obtain vulnerability results of endpoints that connect to the Cisco ISE network:

* Qualys—Qualys is a cloud-based assessment system with scanner appliances deployed in the network. Cisco ISE allows you to configure an adapter that communicates with Qualys and obtains the VA results. You can configure the adapter from the Admin portal. You need a Cisco ISE administrator account with Super Admin privileges to configure the adapter. The Qualys adapter uses REST APIs to communicate with the Qualys Cloud Service. You need a user account in Qualys with Manager privileges to access the REST APIs. Cisco ISE uses following Qualys REST APIs:
* Host Detection List API—To check the last scan results of the endpoint
* Scan API—To trigger an on-demand scan of the endpoint

Qualys enforces limits on the number of API calls that subscribed users can make. The default rate limit count is 300 per 24 hours. Cisco ISE uses Qualys API version 2.0 to connect to Qualys. Refer to the Qualys API V2 User Guide for more information on these API functions.

* Rapid7 Nexpose—Cisco ISE integrates with Rapid 7 Nexpose, a vulnerability management solution, to help detect vulnerabilities and enables you to respond to such threats quickly. Cisco ISE receives the vulnerability data from Nexpose and based on the policies that you configure in ISE, it quarantines the affected endpoints. From the Cisco ISE dashboard, you can view the affected endpoint and take appropriate action.
* Cisco ISE has been tested with Nexpose Release 6.4.1.
* Tenable Security Center (Nessus scanner)—Cisco ISE integrates with Tenable SecurityCenter and receives the vulnerability data from Tenable Nessus scanner (managed by Tenable SecurityCenter) and based on the policies that you configure in ISE, it quarantines the affected endpoints. From the Cisco ISE dashboard, you can view the affected endpoints and take appropriate action.

Cisco ISE has been tested with Tenable SecurityCenter 5.3.2.

How does Cisco ISE act upon the vulnerability assessment results?

The vulnerability assessment results that Cisco ISE obtains from the ecosystem partner are converted in to a Structured Threat Information Expression (STIX) representation and based on this value, a Change of Authorization (CoA) is triggered, if needed, and the appropriate level of access is granted to the endpoint.

Can Cisco ISE perform real-time vulnerability assessment?

No, the time taken to assess endpoints for vulnerabilities depends on various factors and hence Cisco ISE cannot perform VA real time.

What are the factors that affect the time taken to assess an endpoint for vulnerabilities?

The factors that affect the time taken to assess an endpoint for vulnerabilities include:

* Vulnerability assessment ecosystem
* Type of vulnerabilities scanned for
* Type of scans enabled
* Network and system resources allocated by the ecosystem for the scanner appliances

In Cisco ISE 2.3, only endpoints with IPv4 addresses can be assessed for vulnerabilities.

How do I enable and configure Vulnerability Assessment service?

To enable and configure Vulnerability Assessment Service in Cisco ISE, perform the following tasks:

Step 1: Enable Threat Centric NAC Service.

Step 2: To configure:

* Qualys adapter, see Configure Qualys Adapter.
* Nexpose adapter, see Configure Nexpose Adapter.
* Tenable adapter, see Configure Tenable Adapter.

Step 3: Configure Authorization Profile.

Step 4: Configure Exception Rule to Quarantine a Vulnerable Endpoint.

What are the steps to be performed to enable Threat Centric NAC service?

To configure vulnerability and threat adapters, you must first enable the Threat Centric NAC service. This service can be enabled on only one Policy Service Node in your deployment.

Step 1: Choose Administration > System > Deployment.

Step 2: Check the check box next to the PSN on which you want to enable the Threat Centric NAC service and click Edit.

Step 3: Check the Enable Threat Centric NAC Service check box.

Step 4: Click Save.

How do I configure the Qualys adapter?

Cisco ISE supports the Qualys Vulnerability Assessment Ecosystem. You must create a Qualys adapter for Cisco ISE to communicate with Qualys and obtain the VA results.

Before You Begin

* You must have the following user accounts:
* Admin user account in Cisco ISE with Super Admin privileges to be able to configure a vendor adapter.
* User account in Qualys with Manager privileges
* Ensure that you have appropriate Qualys license subscriptions. You need access to the Qualys Report Center, Knowledge Base (KBX), and API. Contact your Qualys Account Manager for details.
* Import the Qualys server certificate in to the Trusted Certificates store in Cisco ISE (Administration > Certificates > Certificate Management > Trusted Certificates > Import). Ensure that the appropriate root and intermediate certificates are imported (or present) in the Cisco ISE Trusted Certificates store.
* Refer to the Qualys API Guide for the following configurations:
* Ensure that you have enabled CVSS Scoring in Qualys (Reports > Setup > CVSS Scoring > Enable CVSS Scoring).
* Ensure that you add the IP address and subnet mask of your endpoints in Qualys (Assets > Host Assets).
* Ensure that you have the name of the Qualys option profile. The option profile is the scanner template that Qualys uses for scanning. We recommend that you use an option profile that includes authenticated scans (this option checks the MAC Address of the endpoint as well).
* Cisco ISE communicates with Qualys over HTTPS/SSL (port 443).

Step 1: Choose Administration > Threat Centric NAC > Third Party Vendors.

Step 2: Click Add.

Step 3: From the Vendor drop-down list, choose Qualys:VA.

Step 4: Enter a name for the adapter instance. For example, Qualys\_Instance.

The listing page appears with a list of configured adapter instances.

Step 5: Refresh the Vendor Instances listing page. The status for the newly added Qualys\_Instance adapter should change to Ready to Configure.

Step 6: Click the Ready to Configure link.

Step 7: Enter the following values in the Qualys configuration screen and click Next.

REST API Host: The hostname of the server that hosts the Qualys cloud. Contact your Qualys representative for this information.

REST API Port: 443

Username: User account in Qualys with Manager privileges.

Password: Password for the Qualys user account.

HTTP Proxy Host: If you have a proxy server configured to route all Internet traffic, enter the hostname of the proxy server.

HTTP Proxy Port: Enter the port number used by the proxy server.

If the connection to the Qualys server is established, the Scanner Mappings page appears with a list of Qualys scanners. The Qualys scanners from your network appear in this page.

Step 8: Choose the default scanner that Cisco ISE will use for on-demand scans.

Step 9: In the PSN to Scanner Mapping area, choose one or more Qualys scanner appliance(s) to the PSN node, and click Next.

The Advanced Settings page appears.

Step 10: Enter the following values in the Advanced Settings page. The settings in this page determine whether an on-demand scan will be triggered or the last scan results will be used for VA.

Given below are the fields with the corresponding description:

Option Profile: Choose the option profile that you want Qualys to use for scanning the endpoint. You can choose the default option profile, Initial Options.

Last Scan Results - Check Settings

Last scan results check interval in minutes: (Impacts the access rate of Host Detection List API) Time interval in minutes after which the last scan results must be checked again. Valid range is between 1 and 2880.

Maximum results before last scan results are checked: (Impacts the access rate of Host Detection List API) If the number of queued scan requests exceeds the maximum number specified here, the last scan results are checked before the time interval specified in Last scan results check interval in minutes field. Valid range is between 1 and 1000.

Verify MAC address: True or False. When set to true, the last scan results from Qualys would be used only if it includes the MAC address of the endpoint.

Scan Settings

Scan trigger interval in minutes: (Impacts the access rate of Scan API) Time interval in minutes after which an on-demand scan is triggered. Valid range is between 1 and 2880.

Maximum requests before scan is triggered: (Impacts the access rate of Scan API) If the number of queued scan requests exceeds the maximum number specified here, an on-demand scan would be triggered before the time interval specified in Scan trigger interval in minutes field. Valid range is between 1 and 1000.

Scan status check interval in minutes: Time interval in minutes after which Cisco ISE communicates with Qualys to check the status of the scan. Valid range is between 1 and 60.

Number of scans that can be triggered concurrently: (This option depends on the number of scanners you have mapped to each PSN in the Scanner Mappings screen) Each scanner can process only one request at a time. If you have mapped more than one scanner to the PSNs, then you can increment this value based on the number of scanners you have chosen. Valid range is between 1 and 200.

Scan timeout in minutes: Time in minutes after which the scan request will time out. If a scan request times out, an alarm is generated. Valid range is between 20 and 1440.

Maximum number of IP addresses to be submitted per scanner: Indicates the number of requests that can be queued into a single request to be sent to Qualys for processing. Valid range is between 1 and 1000.

Choose the log level for adapter log files: Choose a log level for the adapter. The available options are ERROR, INFO, DEBUG, and TRACE.

Step 11: Click Next to review the Configuration Settings.

Step 12: Click Finish.

How do I configure the Tenable adapter?

You must create a Tenable adapter for Cisco ISE to communicate with Tenable SecurityCenter (Nessus scanner) and obtain the VA results.

Before You Begin

Note: You must configure the following in Tenable SecurityCenter before you can configure the Tenable Adapter in Cisco ISE. Refer to Tenable SecurityCenter Documentation for these configurations.

* You must have Tenable Security Center and Tenable Nessus Vulnerability Scanner installed. While registering the Tenable Nessus scanner, ensure that you choose Managed by SecurityCenter in the Registration field.
* Create a user account with Security Manager privilege in Tenable SecurityCenter.
* Create a repository in SecurityCenter (Log in to Tenable SecurityCenter with Admin credentials and choose Repository > Add).
* Add the endpoint IP range to be scanned in the repository.
* Add Nessus scanner.
* Create scan zones and assign IP addresses to the scan zones and scanners that are mapped to these scan zones.
* Create a scan policy for ISE.
* Add an active scan and associate it with the ISE scan policy. Configure settings, targets (IP/DNS names).
* Export System and Root certificates from Tenable SecurityCenter and import it in to the Trusted Certificates store in Cisco ISE (Administration > Certificates > Certificate Management > Trusted Certificates > Import). Ensure that the appropriate root and intermediate certificates are imported (or present) in the Cisco ISE Trusted Certificates store.
* Cisco ISE communicates with Tenable SecurityCenter over HTTPS/SSL (port 443).

Step 1: Choose Administration > Threat Centric NAC > Third Party Vendors.

Step 2: Click Add.

Step 3: From the Vendor drop-down list, choose Tenable Security Center:VA.

Step 4: Enter a name for the adapter instance. For example, Tenable.

The listing page appears with a list of configured adapter instances.

Step 5: Refresh the Vendor Instances listing page. The status for the newly added Tenable adapter should change to Ready to Configure.

Step 6: Click the Ready to Configure link.

Step 7: Enter the following values in the Tenable SecurityCenter configuration screen and click Next.

Given below are the fields with the corresponding description:

Tenable SecurityCenter Host: The hostname of the Tenable SecurityCenter.

Tenable SecurityCenter Port: 443

Username: Username of the user account that has Security Manager privileges in Tenable SecurityCenter.

Password: Password of the user account that has Security Manager privileges in Tenable SecurityCenter.

HTTP Proxy Host: If you have a proxy server configured to route all Internet traffic, enter the hostname of the proxy server.

HTTP Proxy Port: Enter the port number used by the proxy server.

Step 8: Click Next.

Step 9: Enter the following values in the Advanced Settings page. The settings in this page determine whether an on-demand scan will be triggered or the last scan results will be used for VA.

Repository: Choose the repository that you created in Tenable SecurityCenter.

Scan Policy: Choose the scan policy that you have created for ISE in Tenable SecurityCenter.

Settings for checking latest scan results

Interval between checking the latest scan results in minutes: Time interval in minutes after which the last scan results must be checked again. Valid range is between 1 and 2880.

Number of pending requests that can trigger checking the latest scan results: If the number of queued scan requests exceeds the maximum number specified here, the last scan results are checked before the time interval specified in the Interval between checking the latest scan results in minutes field. Valid range is between 1 and 1000. The default is 10.

Verify MAC address: True or False. When set to true, the last scan results from Tenable SecurityCenter would be used only if it includes the MAC address of the endpoint.

Scan Settings

Scan trigger interval for each site in minutes: Time interval in minutes after which an on-demand scan is triggered. Valid range is between 1 and 2880.

Number of pending requests before a scan is triggered: If the number of queued scan requests exceeds the maximum number specified here, an on-demand scan would be triggered before the time interval specified in Scan trigger interval for each site in minutes field. Valid range is between 1 and 1000.

Scan timeout in minutes: Time in minutes after which the scan request times out. If a scan request times out, an alarm is generated. Valid range is between 20 and 1440.

Number of scans that could run in parallel: The number of scans that can be run concurrently. Valid range is between 1 and 200.

Http timeout in seconds: Time interval in seconds for Cisco ISE to wait for a response from Tenable SecurityCenter. Valid range is between 5 and 1200.

Choose the log level for adapter log files: Choose a log level for the adapter. The available options are ERROR, INFO, DEBUG, and TRACE.

Step 10: Click Next to review the Configuration Settings.

Step 11: Click Finish.

How do I create an authorization policy that scans endpoints for vulnerabilities?

The authorization profile in Cisco ISE now includes an option to scan endpoints for vulnerabilities. You can choose to run the scan periodically and also specify the time interval for these scans. After you define the authorization profile, you can apply it to an existing authorization policy rule or create a new authorization policy rule.

Before You Begin

You must have enabled the Threat Centric NAC service and configured a vendor adapter.

Step 1: Choose Policy > Policy Elements > Authorization > Authorization Profiles.

Step 2: Create a new authorization profile or edit an existing profile.

Step 3: From the Common Tasks area, check the Assess Vulnerabilities check box.

Step 4: From the Adapter Instance drop-down list, choose the vendor adapter that you have configured. For example, Qualys\_Instance.

Step 5: Enter the scan interval in hours in the Trigger scan if the time since last scan is greater than text box. Valid range is between 1 and 9999.

Step 6: Check the Assess periodically using above interval check box.

Step 7: Click Submit.

What are the steps that I should perform to configure an exception rule to quarantine a vulnerable endpoint?

You can use the following Vulnerability Assessment attributes to configure an exception rule and provide limited access to vulnerable endpoints:

Threat:Qualys-CVSS\_Base\_Score

Threat:Qualys-CVSS\_Temporal\_Score

Rapid7 Nexpose-CVSS\_Base\_Score

Tenable Security Center-CVSS\_Base\_Score

Tenable Security Center-CVSS\_Temporal\_Score

These attributes are available in the Threat directory. Valid value ranges from 0 to 10.

You can choose to quarantine the endpoint, provide limited access (redirect to a different portal), or reject the request.

Step 1: Choose Policy > Policy Sets. You can edit an existing policy rule or create a new exception rule to check for VA attributes.

Step 2: Create a condition to check for the Qualys score and assign the appropriate authorization profile. For example:

Any Identity Group & Threat:Qualys-CVSS\_Base\_Score > 5 -> Quarantine (authorization profile)

Step 3: Click Save.

What are the logs that Cisco ISE provides for troubleshooting VA services?

Cisco ISE provides the following logs for troubleshooting VA services.

* vaservice.log—Contains VA core information and is available in the node that runs the TC-NAC service.
* varuntime.log—Contains information about the endpoint and the VA flow; is available in the Monitoring node and the node that runs the TC-NAC service.
* vaaggregation.log—Contains hourly aggregation details about the endpoint vulnerability and is available in the Primary Administration Node.

What are the attributes in the Threat dictionary?

The following attributes are listed under the Threat dictionary:

* CTA-Course\_Of\_Action (values can be Internal Blocking, Eradication, or Monitoring)
* Qualys-CVSS\_Base\_Score
* Qualys-CVSS\_Temporal\_Score
* Rapid7 Nexpose-CVSS\_Base\_Score
* Tenable Security Center-CVSS\_Base\_Score
* Tenable Security Center-CVSS\_Temporal\_Score

The valid range is from 0 to 10 for both Base Score and Temporal Score attributes.