



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.

Cisco ISE supports the following adapters:

- SourceFire FireAMP
- Cognitive Threat Analytics (CTA) adapter
- Qualys



Note Only the Qualys Enterprise Edition is currently supported for TC-NAC flows.

- Rapid7 Nexpose
- Tenable Security Center

When a threat event is detected for an endpoint, you can select the MAC address of the endpoint on the **Compromised Endpoints** window 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. You can use the **Clear Threat and Vulnerabilities** option on the **Compromised Endpoints** window to clear the threat and vulnerabilities associated with an endpoint (from Cisco ISE system database).

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.

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.

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
```

To view the logs of an endpoint that is automatically quarantined during CoA events, choose **Operations > Threat-Centric NAC Live Logs**. To view the logs of an endpoint that is quarantined manually, choose **Operations > Reports > Audit > Change Configuration Audit**.

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

- The Threat Centric NAC service requires a Cisco ISE Apex license.
- 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.

You can view the threat information for the endpoints on the following pages:

- **Home page > Threat dashboard**
- **Context Visibility > Endpoints > Compromised Endpoints**

The following alarms 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.

The following reports are available for 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.

You can view the following information from **Operations > Reports > Diagnostics > ISE Counters > Threshold Counter Trends:**

- Total number of events received
- Total number of threat events
- Total number of vulnerability events
- Total number of CoAs issued (to PSN)

The values for these attributes are collected every 5 minutes, so these values represent the count for the last 5 minutes.

The Threat dashboard contains the following dashlets:

- **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.

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. 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".

The Compromised Endpoint window displays the matrix view of the endpoints that are impacted and the severity of the impact for each threat category. You can click on the device link to view the detailed threat information for an endpoint.

The Course Of Action chart displays the action taken (Internal Blocking, Eradication, or Monitoring) for the threat incidents based on the CTA-Course_Of_Action attribute received from the CTA adapter.

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.

The Endpoint Count By CVSS graph on the **Vulnerable Endpoints** window 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** window. You can click the device link to view the detailed vulnerability information for each endpoint.

Threat Centric NAC service logs are included in the support bundle. Threat Centric NAC service logs are located at support/logs/TC-NAC/

- [Enable Threat Centric NAC Service, on page 4](#)
- [Add SourceFire FireAMP Adapter, on page 5](#)
- [Configure Cognitive Threat Analytics Adapter, on page 6](#)
- [Configure Authorization Profiles for CTA Adapter, on page 6](#)
- [Configure Authorization Policy using the Course of Action Attribute, on page 7](#)
- [Support for Vulnerability Assessment in Cisco ISE, on page 7](#)
- [Enable and Configure Vulnerability Assessment Service, on page 8](#)

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

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**.

Related Topics

- [Add SourceFire FireAMP Adapter, on page 5](#)
- [Configure Cognitive Threat Analytics Adapter, on page 6](#)
- [Configure Authorization Profiles for CTA Adapter, on page 6](#)
- [Configure Authorization Policy using the Course of Action Attribute, on page 7](#)
- [Threat Centric NAC Service, on page 1](#)

Add 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, on page 4](#)).
- 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

Click **Add**.

Step 2 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 window. You can configure the adapter only after the adapter status changes to **Ready to Configure** on the Vendor Instances listing window.

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** window.

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** window.

Configure Cognitive Threat Analytics Adapter

Before you begin

- You must enable Threat Centric NAC service on the deployment node (see [Enable Threat Centric NAC Service, on page 4](#)).
- 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.




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.

Configure Authorization Profiles for 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** ChooseIn the Cisco ISE GUI, click the **Menu** icon () and 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**.

Configure Authorization Policy 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
```

Support for Vulnerability Assessment in Cisco ISE

Cisco ISE 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 SecurityCenter (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.

The results 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.

The time taken to assess endpoints for vulnerabilities depends on various factors and hence VA cannot be performed in real time. 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 this release of Cisco ISE, only endpoints with IPv4 addresses can be assessed for vulnerabilities.

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, on page 4.](#)

Step 2 To configure:

- Qualys adapter, see [Configure Qualys Adapter, on page 9.](#)
- Nexpose adapter, see [Configure Nexpose Adapter, on page 12.](#)
- Tenable adapter, see [Configure Tenable Adapter, on page 14.](#)

- Step 3** [Configure Authorization Profile, on page 16.](#)
- Step 4** [Configure Exception Rule to Quarantine a Vulnerable Endpoint, on page 16.](#)
-

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**
- 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**.
-

Related Topics

- [Add SourceFire FireAMP Adapter, on page 5](#)
- [Configure Cognitive Threat Analytics Adapter, on page 6](#)
- [Configure Authorization Profiles for CTA Adapter, on page 6](#)
- [Configure Authorization Policy using the Course of Action Attribute, on page 7](#)
- [Threat Centric NAC Service, on page 1](#)

Configure 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

Click **Add**.

Step 2

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

Step 3**Step 4**

Enter a name for the adapter instance. For example, Qualys_Instance.

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

Step 5

Refresh the Vendor Instances listing window. 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**.

Field Name	Description
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 window appears with a list of Qualys scanners. The Qualys scanners from your network appear in this window.

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** window appears.

Step 10

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

Field Name	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.

Field Name	Description
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**.

Configure 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

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 window appears with a list of configured adapter instances.

Step 5 Refresh the Vendor Instances listing window. 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**.

Field Name	Description
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** window. The settings in this window determine whether an on-demand scan will be triggered or the last scan results will be used for VA.

Field Name	Description
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**.

Configure 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 and 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

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 window appears with a list of configured adapter instances.

Step 5 Refresh the Vendor Instances listing window. 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 window and click **Next**.

Field Name	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** window. The settings in this window determine whether an on-demand scan will be triggered or the last scan results will be used for VA.

Field Name	Description
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.

Field Name	Description
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**.

Configure Authorization Profile

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

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**.

Configure 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**.
-

Vulnerability Assessment Logs

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.

