Encrypted Visibility Engine

Encrypted Visibility Engine (EVE) is used to identify client applications and processes utilizing TLS encryption. It enables visibility and allows administrators to take actions and enforce policy within their environments. The EVE technology can also be used to identify and stop malware.

Overview of Encrypted Visibility Engine

The encrypted visibility engine (EVE) is used to provide more visibility into the encrypted sessions without the need to decrypt them. These insights into encrypted sessions are obtained by Cisco's open-source library that is packaged in Cisco's vulnerability database (VDB). The library fingerprints and analyzes incoming encrypted sessions and matches it against a set of known fingerprints. This database of known fingerprints is also available in the Cisco VDB.

Note The encrypted visibility engine feature is supported only on Firewall Management Center-managed devices running Snort 3. This feature is not supported on Snort 2 devices and Firewall Device Manager-managed devices.

Some of the important features of EVE are the following:

- You can take access control policy actions on the traffic using information derived from EVE.
- The VDB included in Cisco Secure Firewall has the ability to assign applications to some processes detected by EVE with a high confidence value. Alternatively, you can create custom application detectors to:
    - Map EVE-detected processes to new user-defined applications.
    - Override the built-in value of process confidence that is used to assign applications to EVE-detected processes.

See the **Configuring Custom Application Detectors** and **Specifying EVE Process Assignments** sections in the **Application Detection** chapter of the Cisco Secure Firewall Management Center Device Configuration Guide.

- EVE can detect the operating system type and version of the client that created a Client Hello packet in the encrypted traffic.
- EVE supports fingerprinting and analysis of Quick UDP Internet Connections (QUIC) traffic too. The server name from the Client Hello packet is displayed in the URL field of the **Connection Events** page.

Attention To use EVE on Firewall Management Center, you must have a valid IPS license on your device. In the absence of a IPS license, the policy displays a warning and deployment is not allowed.

Note

- EVE can detect the operating system type and version of SSL sessions. Normal usage of the operating system, such as running applications and package management software, can trigger OS detection. To view client OS detection, in addition to enabling the EVE toggle button, you must enable **Hosts** under **Policies** > **Network Discovery**. To view a list of possible operating systems on the host IP address, click **Analysis** > **Hosts heading** > **Network Map**, and then choose the required host.
- After enabling EVE for your access control policy, ensure that you have turned on logging for the access control rules within that policy to display the expected results on the EVE dashboard whenever any specific rule conditions are met. For more information on how to turn on logging, see Create and Edit Access Control Rules.

How EVE Works

The Encrypted Visibility Engine (EVE) inspects the Client Hello portion of the TLS handshake to identify client processes. The Client Hello is the initial data packet that is sent to the server. This gives a good indication of the client process on the host. This fingerprint, combined with other data such as destination IP address, provides the basis for EVE's application identification. By identifying specific application fingerprints in the TLS session establishment, the system can identify the client process and take appropriate action (allow/block).

EVE can identify over 5,000 client processes. The system maps a number of these processes to client applications for use as criteria in access control rules. This gives the system the ability to identify and control these applications without enabling TLS decryption. By using fingerprints of known malicious processes, EVE technology can also be used to identify and block encrypted malicious traffic without outbound decryption.

Through machine learning (ML) technology, Cisco processes over one billion TLS fingerprints and over 10000 malware samples daily to create and update EVE fingerprints. These updates are then delivered to customers using Cisco Vulnerability Database (VDB) package.

If EVE does not recognize a fingerprint, it identifies client application and estimates the threat score of the first flow using the destination details, such as IP address, port, and server name. At this point, the status of the fingerprints are randomized and the status can be viewed in the debug logs. For subsequent flows with the same fingerprint, EVE skips reanalysis and marks the fingerprint status as unlabeled. If you intend to block traffic based on EVE's Low or Very Low score thresholds, the initial flow is blocked. However, future flows will be allowed once the application's fingerprint is cached.

Indications of Compromise Events

The host's Indications of Compromise (IoC) events for encrypted visibility engine detection allows you to check connection events with a very high malware confidence level, as reported by EVE. IoC events are triggered for encrypted sessions generated from a host using a malicious client. You can view information, such as IP address, MAC address, and OS information of the malicious host, and the timestamp of the suspicious activity.

A session with Encrypted Visibility Threat Confidence score 'Very High' as seen in connection events genreates an IoC event. You must enable **Hosts** from **Policies** > **Network Discovery**. In the Firewall Management Center, you can view the IoC event existence from:

- **Analysis** > **Hosts heading** > **Indications of Compromise**, and then **Analysis** > **Indications of Compromise**.
- **Analysis** > **Hosts heading** > **Network Map** > Choose the host that must be checked.

  You can view the process information of the session that generated the IoC on the **Connection Events** page. Click **Analysis** > **Connections** > **Events** to access the **Connection Events** page. Note that you must manually select the Encrypted Visibility fields and IoC field from the **Table View of Connection Events** tab.

QUIC Fingerprinting in EVE

Snort can identify client applications in Quick UDP Internet Connections (QUIC sessions) based on EVE analysis. QUIC fingerprinting can:

- Detect applications over QUIC without enabling decryption.
- Identify malware without enabling decryption.
- Detect service applications. You can assign access control rules based on the service detected over the QUIC protocol.

Configure EVE

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **Edit** (✏) next to the access control policy you want to edit.

Step 3 Choose **Encrypted Visibility Engine** from the **More** drop-down arrow at the end of the packet flow line.

Step 4 On the **Encrypted Visibility Engine** page, enable the **Encrypted Visibility Engine (EVE)** toggle button.

Step 5 Choose the **Monitor** mode or the **Protect** mode.

- Choose the **Monitor** mode to detect client applications and monitor encrypted traffic.
- Choose the **Protect** mode to monitor and block encrypted traffic based on the threat confidence level of the client processes. You can use this mode to monitor and block malicious connections at two threat confidence levels:
  - **High**: Use this level to block connections with threat confidence levels ranging from High to Very High.
  - **Very High**: Use this level to block connections with threat confidence levels that are categorized as Very High.

Step 6 Click **Save** and then deploy the access control policy.

Note
To manage exceptions, see Configure EVE Exception Rules, on page 5.

What to do next

Deploy configuration changes.

View Encrypted Visibility Engine Events

After enabling the **Encrypted Visibility Engine** and deploying your access control policy, you can start sending live traffic through your system. You can view the logged connection events in the **Unified Events** page.

Perform this procedure to access the connection events in the Firewall Management Center.

Procedure

Step 1 Click **Analysis** > **Unified Events**.

The Encrypted Visibility Engine can identify the client process that initiated a connection and the operating system in the client, and indicate if the process contains malware or not.

Step 2 In the **Unified Events** page, explicitly enable these columns that are added for the Encrypted Visibility Engine:

- **Encrypted Visibility Process Name**
- **Encrypted Visibility Process Confidence Score**
- **Encrypted Visibility Threat Confidence**
- **Encrypted Visibility Threat Confidence Score**
- **Detection Type**
- **EVE Process Name**

- **EVE Process Confidence Score**
- **EVE Threat Confidence**
- **EVE Threat Confidence Score**
- **Detection Type**

For information about these fields, see Connection and Security-Related Connection Event Fields in the *Cisco Secure Firewall Management Center Administration Guide*.

Note
On the **Connection Events** page, if processes are assigned applications, the **Detection Type** column displays **Encrypted Visibility Engine**, indicating that the client application was identified by the Encrypted Visibility Engine. Without application assignments to process names, the **Detection Type** column displays **AppID**, indicating that the engine that identified the client application was AppID.

Configure EVE Exception Rules

You can create an encrypted visibility engine (EVE) exception rule to ensure the continuity of trusted connections and services by bypassing the EVE’s block action. You can add attributes such as process names and destination IP address to the exception rule. For example, you may want to bypass EVE's block verdict for trusted networks. All the connections in the bypassed networks are exempted from EVE’s block verdict based on the threat confidence level.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **Edit** (✎) next to the access control policy you want to edit.

Step 3 Choose **Encrypted Visibility Engine** from the **More** drop-down arrow at the end of the packet flow line.

Step 4 On the **Encrypted Visibility Engine** page, enable the **Encrypted Visibility Engine (EVE)** toggle button.

Step 5 Choose the **Protect** mode to monitor and block encrypted traffic based on the threat confidence level of the client processes. You can use this mode to monitor and block malicious connections at two threat confidence levels:

- **High**: Use this level to block connections with threat confidence levels ranging from High to Very High.
- **Very High**: Use this level to block connections with threat confidence levels that are categorized as Very High.

Step 6 Click **Manage exceptions** to view and add exception rules.

Step 7 On the **Encrypted Visibility Engine (EVE) Exception List** window, click **+Add Exception Rules** and add the required attributes.

a) Under the **Process Name** tab, enter an EVE-identified process name, and click **+Add** on the right side of the window.

You can add multiple process names to the same exception rule. EVE exception list based on process names works only with EVE-identified process names, which are case- and space-sensitive.

b) Under the **Network Objects** tab, perform one of the following:

- Choose one or more network objects from the **Available Networks** list and add the same to the **Selected Source Network** or **Selected Destination Network** list.
- To create a new network object, click **+Create Network Object**.

  1. Enter a **Name** and an optional **Description**.
  2. Choose the required network type - **Host, Range, Network, or FQDN**. Enter the relevant IP address if you choose **Host, Range, or Network**. If you choose **FQDN**, enter the fully Qualified Domain Name(**FQDN**) and choose the required option from the **Lookup** drop-down list.
  3. If you want to allow configuration overrides, check the **Allow overrides** checkbox.
  4. Click **Add**.

c) To create a new dynamic attribute, click **+Create Dynamic Attribute.**

1. Enter a **Name** and an optional **Description**.
2. Click **Add**. You can configure this object using Cisco Secure Dynamic Attribute Connector (CSDAC) or Management Center APIs.

d) (Optional) In the **Comment** field available on all the tabs, you can enter a reason for adding the required network objects and dynamic attributes to the EVE exception rule.

Step 8 Click **Save** and then deploy the access control policy.

Note When a connection matches an exception rule, it bypasses the EVE's block verdict. You can view EVE's action in the **Connection Events** or **Unified Events** page. The **Reason** column header displays **EVE Exempted** for identification of such EVE-bypassed traffic.

Add Exception Rule from Unified Events

Use the **Unified Events** page to add exception rules for connections that are blocked by EVE. The Firewall Management Center adds an exception rule to the **Encrypted Visibility Engine (EVE) exception list** object. Note that the exception rules added to this list are applicable for all the access control policies that have EVE enabled.

Before you begin

Exception list is supported only from threat defense Version 7.6.0 or later.

Procedure

Step 1 Click **Analysis** > **Unified Events**.

Step 2 In the **Reason** column with **Encrypted Visibility Block** as the reason, click the **Ellipsis**(⋮) icon inside the cell.

Step 3 Choose **Add EVE Exception Rule** from the drop-down list.

Step 4 In the **Encrypted Visibility Engine** window that is displayed, the rule is automatically added to the bottom of the exception list. You can review and make changes to the added rule before saving and deploying the configuration.

Upgrade EVE Exception Rules

On Secure Firewall version 7.7 and earlier, EVE exception rules are configured for each policy separately. From Secure Firewall version 10.0.0, the EVE exception list is part of the global domain. As a result, the EVE exception rules are configured in the global domain and applied to all the policies on which EVE is enabled to block traffic.

When you are upgrading the Management Center from version 7.7 to 10.0.0, all the EVE exception rules from the leaf domains that contain leaf domain network objects are identified and stored. After the upgrade is complete:

- All EVE exception rules from global domain policies, as well as rules from leaf domain policies that reference global domain objects or inline IP addresses, are consolidated into a single global EVE exception list. As a result, some policies may now include EVE exception rules that were not present before the upgrade.
- All policies that contain EVE exception rules are marked as out-of-date.

If the exception rules from leaf domains contain leaf domain network or dynamic objects, these rules are removed during the upgrade process. The upgrade script log file has a log of all the merged and deleted exception rules, along with the corresponding access control policy and domain from which each rule originated. The log file is located at *var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade10.0.0/800_post/1114_eve_rules.pl.log*.

When you deploy the configuration for the first time after the upgrade, a warning message on the Management Center lists all the deleted EVE exception rules. The warning message also states that there could be possible traffic impact if the rules are not reconfigured in the global EVE exception list. Note that the warning message appears only when you deploy the configuration for the first time after the upgrade is complete.

For Secure Firewall devices running version 7.7 and earlier that are mapped to Management Center running version 10.0.0, only **Very High** threat confidence connection events are sent to the **Security-Related Connection Events** table. For Secure Firewall devices running version 10.0.0, EVE **Blocked** and **Medium+** EVE threat confidence connection events are sent to the **Security-Related Connection Events** table.

Change Management Support during EVE Upgrade

When you upgrade the Management Center to version 10.0.0, all active change management tickets that contain access control policies on which EVE is enabled will have their EVE exception rules automatically merged with the global EVE exception list.

The merging of EVE exception rules with the global EVE exception list occurs regardless of the ticket's approval state. This ensures that no exception rules are lost during the upgrade.

EVE Ticket Preview Generation Behavior

If a change management ticket contains a policy that is locked and it contains only EVE-related modifications, such as EVE settings or exception rules, the EVE ticket preview will not be automatically regenerated after the upgrade. If the ticket contains other policy modifications in addition to EVE-related modifications, the EVE ticket preview will be generated normally.

Examples for EVE

About Encrypted Visibility Engine

You can use the Encrypted Visibility Engine (EVE) to identify client applications and processes using Transport Layer Security (TLS) encryption. EVE provides more visibility into the encrypted sessions without decryption. Based on EVE's findings, administrators can enforce policy actions on the traffic within their environments. You can also use the EVE to identify and stop malware.

Benefits

Administrators can leverage and adjust EVE's threat score to block malicious encrypted traffic. If the probability that the incoming traffic is malicious, then based on the threat score, you can configure EVE to block the connection.

Sample Business Scenario

A large corporate network uses Snort 3 as its primary intrusion detection and prevention system. In a rapidly evolving threat landscape, adoption of robust network security measures is necessary and important. The security team uses EVE to enhance encrypted traffic inspection without the need to implement full man-in-the-middle (MITM) decryption. The EVE technology uses fingerprints of known malicious processes to identify and stop malware. Network administrators must have the flexibility to configure EVE's block traffic thresholds to block potentially malicious connections, which are based on their configured block thresholds.

Prerequisites

- You must be running management center 7.4.0 or later, and the managed threat defense must also be 7.4.0 or later.
- Ensure that you have a valid Intrusion Prevention System (IPS) license and Snort 3 is the detection engine.

High-Level Workflow

1. EVE analyzes the incoming traffic and gives a verdict on the probability of incoming traffic being malware or not.
2. If EVE detects incoming traffic to be malware with a certain level of confidence, you can configure EVE to block that traffic.
3. The packets are first checked for malware probability or threat score, and the threat score is compared with the block threshold that you have set.
4. If the threat score is higher than the configured threshold, EVE blocks the traffic.
5. If the threat score is lesser than the configured threshold, EVE takes no action.

Configure Block Thresholds in EVE

This procedure shows how to block potentially malicious traffic, based on the EVE threat confidence score of 90 percent or higher.

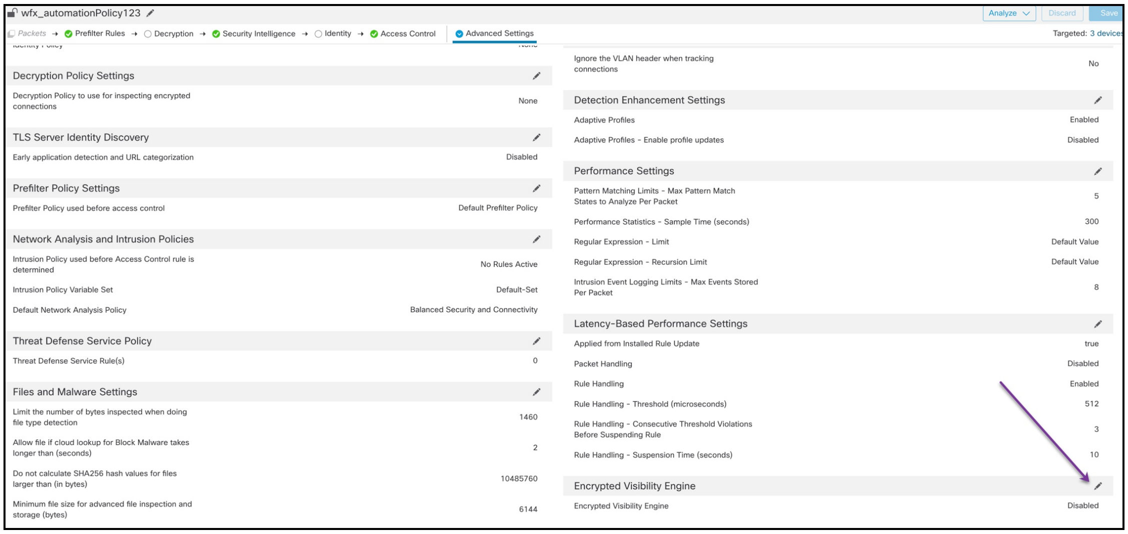
Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Access Control**.

Step 2 Click **Edit** (✎) next to the access control policy you want to edit.

Step 3 Choose **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

Step 4 Click **Edit** (✎) next to **Encrypted Visibility Engine**.



Decryption Policy Settings

Decryption Policy to use for inspecting encrypted connections	None

TLS Server Identity Discovery

Early application detection and URL categorization	Disabled

Prefilter Policy Settings

Prefilter Policy used before access control	Default Prefilter Policy

Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined	No Rules Active
Intrusion Policy Variable Set	Default-Set
Default Network Analysis Policy	Balanced Security and Connectivity

Threat Defense Service Policy

Threat Defense Service Rule(s)	0

Files and Malware Settings

Limit the number of bytes inspected when doing file type detection	1460
Allow file if cloud lookup for Block Malware takes longer than (seconds)	2
Do not calculate SHA256 hash values for files larger than (in bytes)	10485760
Minimum file size for advanced file inspection and storage (bytes)	6144

Ignore the VLAN header when tracking connections	No

Detection Enhancement Settings

Adaptive Profiles	Enabled
Adaptive Profiles - Enable profile updates	Disabled

Performance Settings

Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet	5
Performance Statistics - Sample Time (seconds)	300
Regular Expression - Limit	Default Value
Regular Expression - Recursion Limit	Default Value
Intrusion Event Logging Limits - Max Events Stored Per Packet	8

Latency-Based Performance Settings

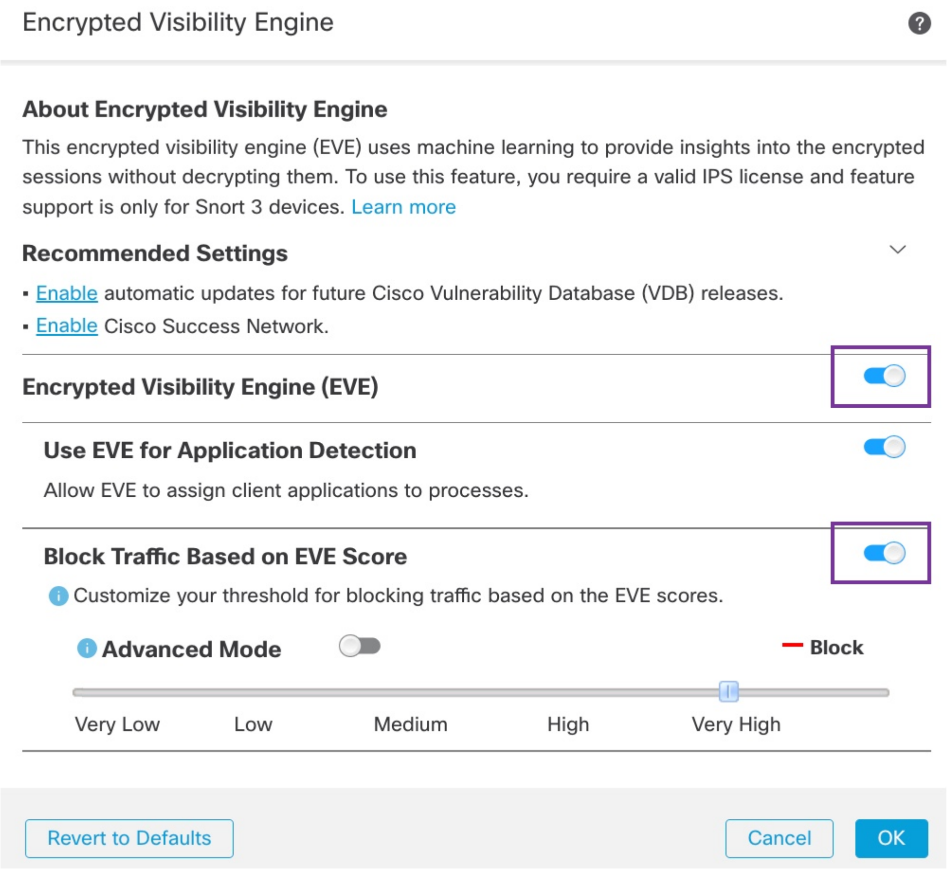
Applied from Installed Rule Update	true
Packet Handling	Disabled
Rule Handling	Enabled
Rule Handling - Threshold (microseconds)	512
Rule Handling - Consecutive Threshold Violations Before Suspending Rule	3
Rule Handling - Suspension Time (seconds)	10

Encrypted Visibility Engine

Encrypted Visibility Engine	Disabled

Step 5 In the **Encrypted Visibility Engine** page, enable the **Encrypted Visibility Engine (EVE)** toggle button.

Step 6 Enable the **Block Traffic Based on EVE Score** toggle button. Any incoming traffic that is a potential threat is blocked by default.



Encrypted Visibility Engine

About Encrypted Visibility Engine

This encrypted visibility engine (EVE) uses machine learning to provide insights into the encrypted sessions without decrypting them. To use this feature, you require a valid IPS license and feature support is only for Snort 3 devices. Learn more

Recommended Settings

- Enable automatic updates for future Cisco Vulnerability Database (VDB) releases.
- Enable Cisco Success Network.

Encrypted Visibility Engine (EVE)

Use EVE for Application Detection

Allow EVE to assign client applications to processes.

Block Traffic Based on EVE Score

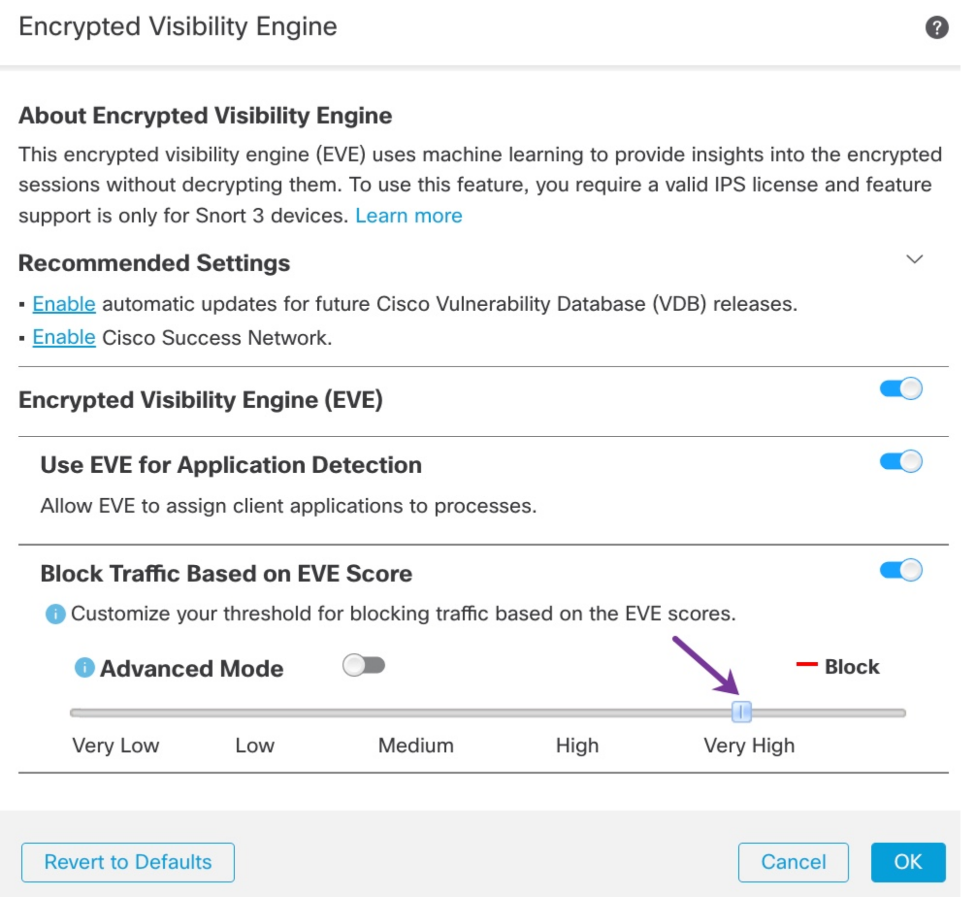
Customize your threshold for blocking traffic based on the EVE scores.

Note

By default, the threshold at which malware is blocked is 99 percent, which means:

- If EVE detects the traffic to be malware with 99 percent confidence or higher, EVE blocks the traffic.
- If EVE detects the traffic to be malware with less than 99 percent confidence, EVE takes no action.

Step 7 Use the slider to adjust the threshold for blocking based on EVE threat confidence. This ranges from **Very Low** to **Very High**. In this example, the slider is set to **Very High**.



Encrypted Visibility Engine

About Encrypted Visibility Engine

This encrypted visibility engine (EVE) uses machine learning to provide insights into the encrypted sessions without decrypting them. To use this feature, you require a valid IPS license and feature support is only for Snort 3 devices. Learn more

Recommended Settings

- Enable automatic updates for future Cisco Vulnerability Database (VDB) releases.
- Enable Cisco Success Network.

Encrypted Visibility Engine (EVE) ●

Use EVE for Application Detection ●

Allow EVE to assign client applications to processes.

Block Traffic Based on EVE Score ●

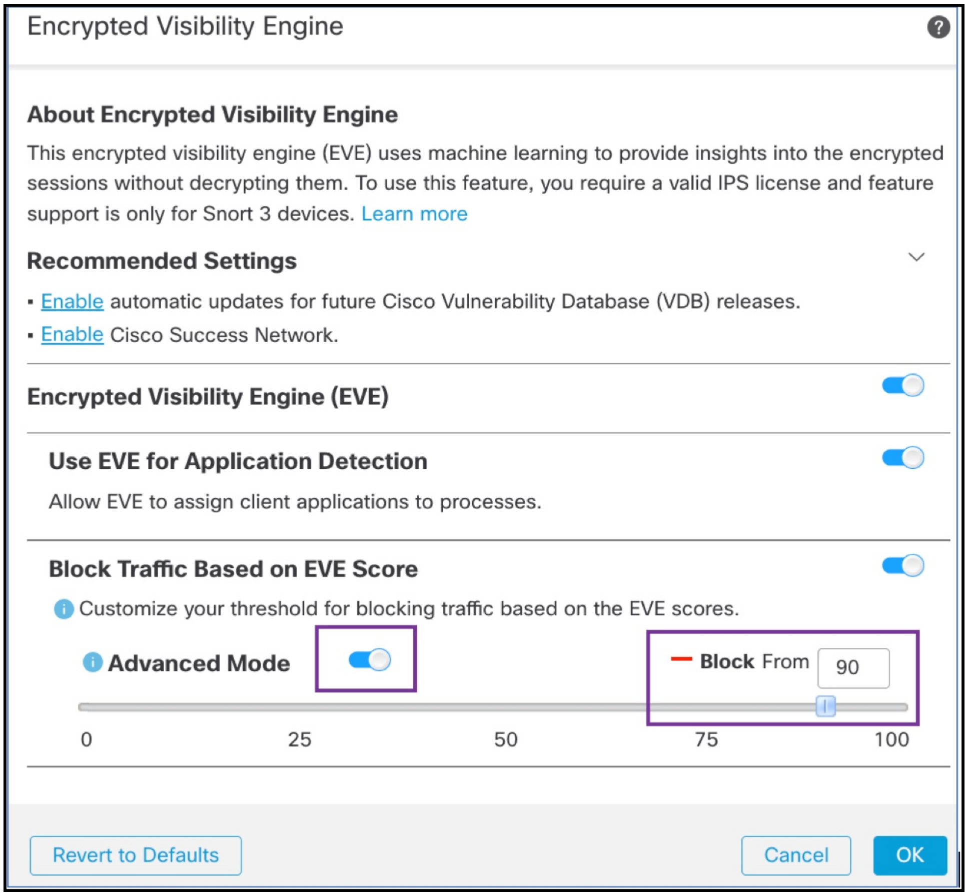
Customize your threshold for blocking traffic based on the EVE scores.

Step 8 For further granular control, enable the **Advanced Mode** toggle button. Now, you can assign a specific EVE Threat Confidence Score for blocking traffic. The default threshold is 99 percent.

Step 9 In this example, change the block threshold to **90** percent.

Attention

As a best practice, we recommend that you do not set the block threshold to below 50 percent to ensure optimum performance.



Encrypted Visibility Engine

About Encrypted Visibility Engine

This encrypted visibility engine (EVE) uses machine learning to provide insights into the encrypted sessions without decrypting them. To use this feature, you require a valid IPS license and feature support is only for Snort 3 devices. Learn more

Recommended Settings

- Enable automatic updates for future Cisco Vulnerability Database (VDB) releases.
- Enable Cisco Success Network.

Encrypted Visibility Engine (EVE)

Use EVE for Application Detection

Allow EVE to assign client applications to processes.

Block Traffic Based on EVE Score

Customize your threshold for blocking traffic based on the EVE scores.

Advanced Mode

Block From 90

Step 10 Click **OK**.

Step 11 Click **Save**.

What to do next

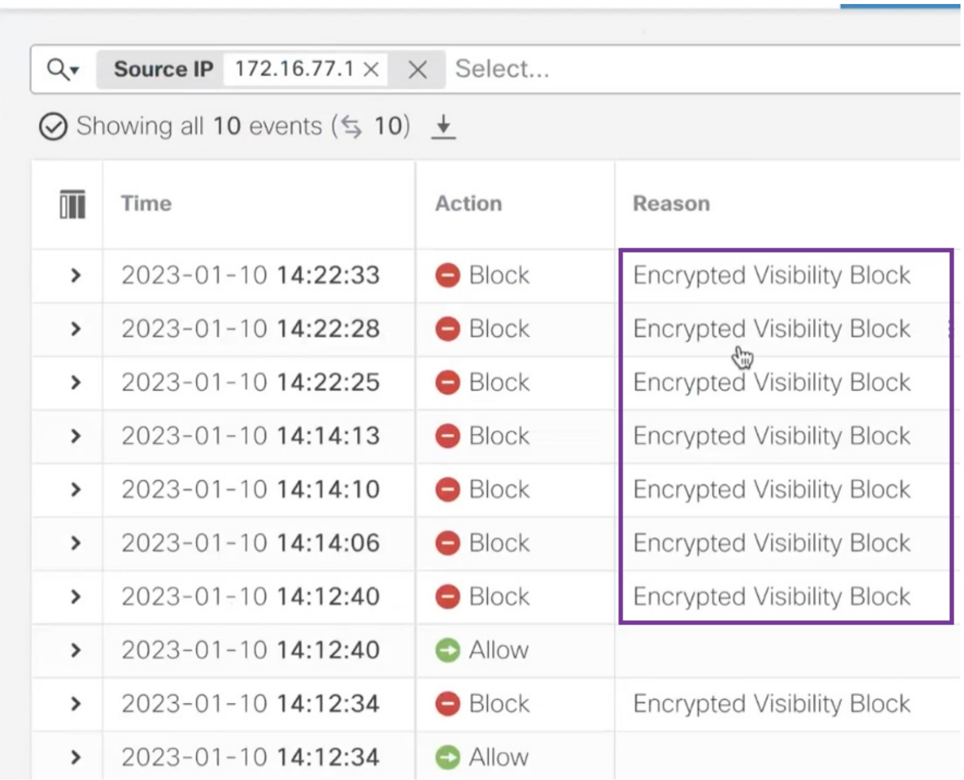
Deploy configuration changes.

View EVE Events

Procedure

Step 1 To verify the block action, choose **Analysis** > **Connections** > **Events**. You can also view the events from the **Unified Events** viewer.

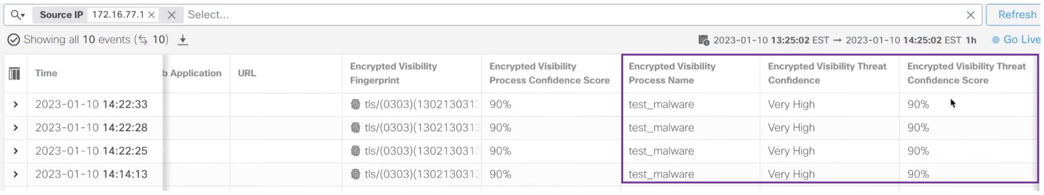
Step 2 If you have configured EVE to block traffic, the **Reason** field shows **Encrypted Visibility Block**.



Showing all 10 events (⇆ 10)

	Time	Action	Reason
>	2023-01-10 14:22:33	Block	Encrypted Visibility Block
>	2023-01-10 14:22:28	Block	Encrypted Visibility Block
>	2023-01-10 14:22:25	Block	Encrypted Visibility Block
>	2023-01-10 14:14:13	Block	Encrypted Visibility Block
>	2023-01-10 14:14:10	Block	Encrypted Visibility Block
>	2023-01-10 14:14:06	Block	Encrypted Visibility Block
>	2023-01-10 14:12:40	Block	Encrypted Visibility Block
>	2023-01-10 14:12:40	Allow	
>	2023-01-10 14:12:34	Block	Encrypted Visibility Block
>	2023-01-10 14:12:34	Allow	

Step 3 The following is an example of the **Encrypted Visibility Process Name** as **test_malware**, **Encrypted Visibility Threat Confidence** as **Very High**, and **Encrypted Visibility Threat Confidence Score** as **90** percent.



Showing all 10 events (⇆ 10)

2023-01-10 13:25:02 EST → 2023-01-10 14:25:02 EST 1h

	Time	b Application	URL	Encrypted Visibility Fingerprint	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score
>	2023-01-10 14:22:33			tls/(0303)(130213031	90%	test_malware	Very High	90%
>	2023-01-10 14:22:28			tls/(0303)(130213031	90%	test_malware	Very High	90%
>	2023-01-10 14:22:25			tls/(0303)(130213031	90%	test_malware	Very High	90%
>	2023-01-10 14:14:13			tls/(0303)(130213031	90%	test_malware	Very High	90%

Additional References

For detailed conceptual information, see the Encrypted Visibility Engine for Snort 3 chapter in this guide or the content in the following link:

Encrypted Visibility Engine