Application Detection

The following topics describe Firepower System application detection:

- Overview: Application Detection, on page 1
- Custom Application Detectors, on page 6
- Viewing or Downloading Detector Details, on page 14
- Sorting the Detector List, on page 15
- Filtering the Detector List, on page 15
- Navigating to Other Detector Pages, on page 16
- Activating and Deactivating Detectors, on page 17
- Editing Custom Application Detectors, on page 18
- Deleting Detectors, on page 18

Overview: Application Detection

When the Firepower System analyzes IP traffic, it attempts to identify the commonly used applications on your network. Application awareness is crucial to application control.

There are three types of applications that the system detects:

- *application protocols* such as HTTP and SSH, which represent communications between hosts
- *clients* such as web browsers and email clients, which represent software running on the host
- *web applications* such as MPEG video and Facebook, which represent the content or requested URL for HTTP traffic

The system identifies applications in your network traffic according to the characteristics specified in the detector. For example, the system can identify an application by an ASCII pattern in the packet header. In addition, Secure Socket Layers (SSL) protocol detectors use information from the secured session to identify the application from the session.

There are two sources of application detectors in the Firepower System:

- *System-provided detectors* detect web applications, clients, and application protocols.

  The availability of system-provided detectors for applications (and operating systems) depends on the version of the Firepower System and the version of the VDB you have installed. Release notes and advisories contain information on new and updated detectors. You can also import individual detectors authored by Professional Services.
Custom application protocol detectors are user-created and detect web applications, clients, and application protocols.

You can also detect application protocols through implied application protocol detection, which infers the existence of an application protocol based on the detection of a client.

The system identifies only those application protocols running on hosts in your monitored networks, as defined in the network discovery policy. For example, if an internal host accesses an FTP server on a remote site that you are not monitoring, the system does not identify the application protocol as FTP. On the other hand, if a remote or internal host accesses an FTP server on a host you are monitoring, the system can positively identify the application protocol.

If the system can identify the client used by a monitored host to connect to a non-monitored server, the system identifies the client's corresponding application protocol, but does not add the protocol to the network map. Note that client sessions must include a response from the server for application detection to occur.

The system characterizes each application that it detects; see Application Characteristics. The system uses these characteristics to create groups of applications, called application filters. Application filters are used to perform access control and to constrain search results and data used in reports and dashboard widgets.

You can also supplement application detector data using exported NetFlow records, Nmap active scans, and the host input feature.

Related Topics
Recommendations for Application Control
Application Detector Fundamentals, on page 2

Application Detector Fundamentals

The Firepower System uses application detectors to identify the commonly used applications on your network. Use the Detectors page (Policies > Application Detectors) to view the detector list and customize detection capability.

Whether you can modify a detector or change its state (active or inactive) depends on its type. The system uses only active detectors to analyze application traffic.

Note
Cisco-provided detectors may change with Firepower System and VDB updates. See the release notes and advisories for information on updated detectors.

Cisco-Provided Internal Detectors

Internal detectors are a special category of detectors for client, web application, and application protocol traffic. Internal detectors are delivered with system updates and are always on.

If an application matches against internal detectors designed to detect client-related activity and no specific client detector exists, a generic client may be reported.

Cisco-Provided Client Detectors

Client detectors detect client traffic and are delivered via VDB or system update, or are provided for import by Cisco Professional Services. You can activate and deactivate client detectors. You can export a client detector only if you import it.
Cisco-Provided Web Application Detectors

Web application detectors detect web applications in HTTP traffic payloads and are delivered via VDB or system update. Web application detectors are always on.

Cisco-Provided Application Protocol (Port) Detectors

Port-based application protocol detectors use well-known ports to identify network traffic. They are delivered via VDB or system update, or are provided for import by Cisco Professional Services. You can activate and deactivate application protocol detectors, and view a detector definition to use it as the basis for a custom detector.

Cisco-Provided Application Protocol (Firepower) Detectors

Firepower-based application protocol detectors analyze network traffic using Firepower application fingerprints and are delivered via VDB or system update. You can activate and deactivate application protocol detectors.

Custom Application Detectors

Custom application detectors are pattern-based. They detect patterns in packets from client, web application, or application protocol traffic. You have full control over imported and custom detectors.

Identification of Application Protocols in the Web Interface

The following table outlines how the Firepower System identifies detected application protocols:

<table>
<thead>
<tr>
<th>Identification</th>
<th>Description</th>
</tr>
</thead>
</table>
| application protocol name | The Firepower Management Center identifies an application protocol with its name if the application protocol was:  
- positively identified by the system  
- identified using NetFlow data and there is a port-application protocol correlation in /etc/sf/services  
- manually identified using the host input feature  
- identified by Nmap or another active source |
| pending         | The Firepower Management Center identifies an application protocol as pending if the system can neither positively nor negatively identify the application.  
Most often, the system needs to collect and analyze more connection data before it can identify a pending application.  
In the Application Details and Servers tables and in the host profile, the pending status appears only for application protocols where specific application protocol traffic was detected (rather than inferred from detected client or web application traffic). |
The Firepower Management Center identifies an application protocol as unknown if:
• the application does not match any of the system’s detectors
• the application protocol was identified using NetFlow data, but there is no port-application protocol correlation in /etc/sf/services

All available detected data has been examined, but no application protocol was identified. In the Application Details and Servers tables and in the host profile, the application protocol is left blank for non-HTTP generic client traffic with no detected application protocol.

### Implied Application Protocol Detection from Client Detection

If the system can identify the client used by a monitored host to access a non-monitored server, the Firepower Management Center infers that the connection is using the application protocol that corresponds with the client. (Because the system tracks applications only on monitored networks, connection logs usually do not include application protocol information for connections where a monitored host is accessing a non-monitored server.)

This process, or implied application protocol detection, has the following consequences:
• Because the system does not generate a New TCP Port or New UDP Port event for these servers, the server does not appear in the Servers table. In addition, you cannot trigger either discovery event alerts or correlation rules using the detection of these application protocol as a criterion.
• Because the application protocol is not associated with a host, you cannot view its details in host profiles, set its server identity, or use its information in host profile qualifications for traffic profiles or correlation rules. In addition, the system does not associate vulnerabilities with hosts based on this type of detection.

You can, however, trigger correlation events on whether the application protocol information is present in a connection. You can also use the application protocol information in connection logs to create connection trackers and traffic profiles.

### Host Limits and Discovery Event Logging

When the system detects a client, server, or web application, it generates a discovery event unless the associated host has already reached its maximum number of clients, servers, or web applications.

Host profiles display up to 16 clients, 100 servers, and 100 web applications per host.

Note that actions dependent on the detection of clients, servers, or web applications are unaffected by this limit. For example, access control rules configured to trigger on a server will still log connection events.
Special Considerations for Application Detection

**Squid**

The system positively identifies Squid server traffic when either:

- the system detects a connection from a host on your monitored network to a Squid server where proxy authentication is enabled, or
- the system detects a connection from a Squid proxy server on your monitored network to a target system (that is, the destination server where the client is requesting information or another resource).

However, the system cannot identify Squid service traffic if:

- a host on your monitored network connects to a Squid server where proxy authentication is disabled, or
- the Squid proxy server is configured to strip Via: header fields from its HTTP responses

**SSL Application Detection**

The system provides application detectors that can use session information from a Secure Socket Layers (SSL) session to identify the application protocol, client application, or web application in the session.

When the system detects an encrypted connection, it marks that connection as either a generic HTTPS connection or as a more specific secure protocol, such as SMTPS, when applicable. When the system detects an SSL session, it adds `SSL client` to the `Client` field in connection events for the session. If it identifies a web application for the session, the system generates discovery events for the traffic.

For SSL application traffic, managed devices can also detect the common name from the server certificate and match that against a client or web application from an SSL host pattern. When the system identifies a specific client, it replaces `SSL client` with the name of the client.

Because the SSL application traffic is encrypted, the system can use only information in the certificate for identification, not application data within the encrypted stream. For this reason, SSL host patterns can sometimes only identify the company that authored the application, so SSL applications produced by the same company may have the same identification.

In some instances, such as when an HTTPS session is launched from within an HTTP session, managed devices detect the server name from the client certificate in a client-side packet.

To enable SSL application identification, you must create access control rules that monitor responder traffic. Those rules must have either an application condition for the SSL application or URL conditions using the URL from the SSL certificate. For network discovery, the responder IP address does not have to be in the networks to monitor in the network discovery policy; the access control policy configuration determines whether the traffic is identified. To identify detections for SSL applications, you can filter by the `SSL protocol` tag, in the application detectors list or when adding application conditions in access control rules.

**Referred Web Applications**

Web servers sometimes refer traffic to other websites, which are often advertisement servers. To help you better understand the context for referred traffic occurring on your network, the system lists the web application that referred the traffic in the **Web Application** field in events for the referred session. The VDB contains a list of known referred sites. When the system detects traffic from one of those sites, the referring site is stored with the event for that traffic. For example, if an advertisement accessed via Facebook is actually hosted on Advertising.com, the detected Advertising.com traffic is associated with the Facebook web application. The
system can also detect referring URLs in HTTP traffic, such as when a website provides a simple link to another site; in this case, the referring URL appears in the HTTP Referrer event field.

In events, if a referring application exists, it is listed as the web application for the traffic, while the URL is that for the referred site. In the example above, the web application for the connection event for that traffic would be Facebook, but the URL would be Advertising.com. A referred application may appear as the web application if no referring web application is detected, if the host refers to itself, or if there is a chain of referrals. In the dashboard, connection and byte counts for web applications include sessions where the web application is associated with traffic referred by that application.

Note that if you create a rule to act specifically on referred traffic, you should add a condition for the referred application, rather than the referring application. To block Advertising.com traffic referred from Facebook, for example, add an application condition to your access control rule for the Advertising.com application.

### Custom Application Detectors

If you use a custom application on your network, you can create a custom web application, client, or application protocol detector that provides the system with the information it needs to identify the application. The type of application detector is determined by your selections in the Protocol, Type, and Direction fields.

Client sessions must include a responder packet from the server for the system to begin detecting and identifying application protocols in server traffic. Note that, for UDP traffic, the system designates the source of the responder packet as the server.

If you have already created a detector on another Firepower Management Center, you can export it and then import it onto this Firepower Management Center. You can then edit the imported detector to suit your needs. You can export and import custom detectors as well as detectors provided by Cisco Professional Services. However, you cannot export or import any other type of Cisco-provided detectors.

### Custom Application Detector and User-Defined Application Fields

You can use the following fields to configure custom application detectors and user-defined applications.

#### Custom Application Detector Fields: General

Use the following fields to configure basic and advanced custom application detectors.

**Application Protocol**

The application protocol you want to detect. This can be a system-provided application or a user-defined application.

If you want the application to be available for exemption from active authentication (configured in your identity rules), you must select or create an application protocol with the User-Agent Exclusion tag.

**Description**

A description for the application detector.

**Name**

A name for the application detector.
Detector Type

The type of detector, **Basic** or **Advanced**. Basic application detectors are created in the web interface as a series of fields. Advanced application detectors are created externally and uploaded as custom .lua files.

Custom Application Detector Fields: Detection Patterns

Use the following fields to configure the detection patterns for basic custom application detectors.

**Direction**

The source of the traffic the detector should inspect, **Client** or **Server**.

**Offset**

The location in a packet, in bytes from the beginning of the packet payload, where the system should begin searching for the pattern.

Because packet payloads start at byte 0, calculate the offset by subtracting 1 from the number of bytes you want to move forward from the beginning of the packet payload. For example, to look for the pattern in the fifth bit of the packet, type 4 in the **Offset** field.

**Pattern**

The pattern string associated with the **Type** you selected.

**Ports**

The port of the traffic the detector should inspect.

**Protocol**

The protocol you want to detect. Your protocol selection determines whether the **Type** or the **URL** field displays.

The protocol (and, in some cases, your subsequent selections in the **Type** and **Direction** fields) determine the type of application detector you create: web application, client, or application protocol.

<table>
<thead>
<tr>
<th>Detector Type</th>
<th>Protocol</th>
<th>Type or Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application</td>
<td>HTTP</td>
<td><strong>Type</strong> is <strong>Content Type</strong> or <strong>URL</strong></td>
</tr>
<tr>
<td></td>
<td>RTMP</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td>SSL</td>
<td>Any</td>
</tr>
<tr>
<td>Client</td>
<td>HTTP</td>
<td><strong>Type</strong> is <strong>User Agent</strong></td>
</tr>
<tr>
<td></td>
<td>SIP</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td>TCP or UDP</td>
<td><strong>Direction</strong> is <strong>Client</strong></td>
</tr>
<tr>
<td>Application Protocol</td>
<td>TCP or UDP</td>
<td><strong>Direction</strong> is <strong>Server</strong></td>
</tr>
</tbody>
</table>

**Type**

The type of pattern string you entered. The options you see are determined by the **Protocol** you selected. If you selected **RTMP** as the protocol, the **URL** field displays instead of the **Type** field.
If you select User Agent as the Type, the system automatically sets the Tag for the application to User-Agent Exclusion.

<table>
<thead>
<tr>
<th>Type Selection</th>
<th>String Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ascii</td>
<td>The string is ASCII encoded.</td>
</tr>
<tr>
<td>Common Name</td>
<td>The string is the value in the commonName field within the server response message.</td>
</tr>
<tr>
<td>Content Type</td>
<td>The string is the value in the content-type field within the server response header.</td>
</tr>
<tr>
<td>Hex</td>
<td>The string is in hexadecimal notation.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>The string is the value in the organizationName field within the server response message.</td>
</tr>
<tr>
<td>SIP Server</td>
<td>The string is the value in the From field within the message header.</td>
</tr>
<tr>
<td>SSL Host</td>
<td>The string is the value in the server_name field within the ClientHello message.</td>
</tr>
<tr>
<td>URL</td>
<td>The string is a URL. The detector assumes that the string you enter is a complete section of the URL. For example, entering cisco.com would match <a href="http://www.cisco.com/support">www.cisco.com/support</a> and <a href="http://www.cisco.com">www.cisco.com</a>, but not <a href="http://www.wearecisco.com">www.wearecisco.com</a>.</td>
</tr>
<tr>
<td>User Agent</td>
<td>The string is the value in the user-agent field within the GET request header. It is also available for the SIP protocol and indicates that the string is the value in the User-Agent field within the SIP message header.</td>
</tr>
</tbody>
</table>

URL

Either a full URL or a section of a URL from the swfURL field within the C2 message of a RTMP packet. This field displays instead of the Type field when you select RTMP as the Protocol.

Note: The detector assumes that the string you enter is a complete section of the URL. For example, entering cisco.com would match www.cisco.com/support and www.cisco.com, but not www.wearecisco.com.

User-Defined Application Fields

Use the following fields to configure user-defined applications within basic and advanced custom application detectors.
Business Relevance
The likelihood that the application is used within the context of your organization’s business operations, as opposed to recreationally: Very High, High, Medium, Low, or Very Low. Select the option that best describes the application.

Categories
A general classification for the application that describes its most essential function.

Description
A description for the application.

Name
A name for the application.

Risk
The likelihood that the application is used for purposes that might be against your organization’s security policy: Very High, High, Medium, Low, or Very Low. Select the option that best describes the application.

Tags
One or more predefined tags that provide additional information about the application. If you want an application to be available for exemption from active authentication (configured in your identity rules), you must add the User-Agent Exclusion tag to your application.

Configuring Custom Application Detectors

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Discovery Admin</td>
</tr>
</tbody>
</table>

You can configure basic or advanced custom application detectors.

Procedure

Step 1 Select Policies > Application Detectors.
Step 2 Click Create Custom Detector.
Step 3 Enter a Name and a Description.
Step 4 Select an Application Protocol. You have the following options:

- If you are creating a detector for an existing application protocol (for example, if you want to detect a particular application protocol on a non-standard port), select the application protocol from the drop-down list.

- If you are creating a detector for a user-defined application, follow the procedure outlined in Creating a User-Defined Application, on page 10.

Step 5 Select a Detector Type.
Step 6  Click **OK**.

Step 7  Configure **Detection Patterns** or **Detection Criteria**:

- If you are configuring a basic detector, specify preset **Detection Patterns** as described in **Specifying Detection Patterns in Basic Detectors**, on page 11.

- If you are configuring an advanced detector, specify custom **Detection Criteria** as described in **Specifying Detection Criteria in Advanced Detectors**, on page 12.

**Caution**  Advanced custom detectors are complex and require outside knowledge to construct valid .lua files. Incorrectly configured detectors could have a negative impact on performance or detection capability.

Step 8  If you are configuring an advanced detector, use **Packet Captures** to test the new detector as described in **Testing a Custom Application Protocol Detector**, on page 13. If you are configuring a basic detector, this step is optional.

Step 9  Click **Save**.

**Note**  If you include the application in an access control rule, the detector is automatically activated and cannot be deactivated while in use.

---

**What to do next**

- Activate the detector as described in **Activating and Deactivating Detectors**, on page 17.

**Related Topics**

- **Custom Application Detector and User-Defined Application Fields**, on page 6

---

**Creating a User-Defined Application**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Discovery/Any</td>
</tr>
</tbody>
</table>

Applications, categories, and tags created here are available in access control rules and in the application filter object manager as well.

**Before you begin**

- Begin configuring your custom application protocol detector as described in **Configuring Custom Application Detectors**, on page 9.

**Procedure**

Step 1  On the Create Detector page, click **Add**.

Step 2  Type a **Name**.

Step 3  Type a **Description**.
Step 4  Select a **Business Relevance**.
Step 5  Select a **Risk**.
Step 6  Click **Add** next to Categories to add a category and type a new category name, or select an existing category from the **Categories** drop-down list.
Step 7  Optionally, click **Add** next to Tags to add a tag and type a new tag name, or select an existing tag from the **Tags** drop-down list.
Step 8  Click **OK**.

---

**What to do next**
* Continue configuring your custom application protocol detector as described in Configuring Custom Application Detectors, on page 9. You must save and activate the detector before the system can use it to analyze traffic.

**Related Topics**
- Custom Application Detector and User-Defined Application Fields, on page 6

### Specifying Detection Patterns in Basic Detectors

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Discovery Admin</td>
</tr>
</tbody>
</table>

You can configure a custom application protocol detector to search application protocol packet headers for a particular pattern string. You can also configure detectors to search for multiple patterns; in that case the application protocol traffic must match all of the patterns for the detector to positively identify the application protocol.

Application protocol detectors can search for ASCII or hexadecimal patterns, using any offset.

**Before you begin**
* Begin configuring your custom application protocol detector as described in Configuring Custom Application Detectors, on page 9.

**Procedure**

Step 1  On the Create Detector page, in the Detection Patterns section, click **Add**.
Step 2  Select a **Protocol** for traffic the detector should inspect.
Step 3  Specify the pattern **Type** you want to detect.
Step 4  Type a **Pattern String** that matches the **Type** you specified.
Step 5  Optionally, type the **Offset** (in bytes).
Step 6  Optionally, to identify application protocol traffic based on the port it uses, type a port from 1 to 65535 in the **Port(s)** field. To use multiple ports, separate them by commas.
Step 7  Optionally, select a **Direction**: **Client** or **Server**.
Step 8  
Click OK.

Tip  
If you want to delete a pattern, click the delete icon (🗑️) next to the pattern you want to delete.

---

**What to do next**

- Continue configuring your custom application protocol detector as described in Configuring Custom Application Detectors, on page 9. You must save and activate the detector before the system can use it to analyze traffic.

**Related Topics**

- Specifying Detection Criteria in Advanced Detectors, on page 12

---

**Specifying Detection Criteria in Advanced Detectors**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Discovery Admin</td>
</tr>
</tbody>
</table>

---

**Caution**

Advanced custom detectors are complex and require outside knowledge to construct valid .lua files. Incorrectly configured detectors could have a negative impact on performance or detection capability.

---

**Caution**

Do not upload .lua files from untrusted sources.

Custom .lua files contain your custom application detector settings. Creating custom .lua files requires advanced knowledge of the lua programming language and experience with Cisco's C-lua API. Cisco strongly recommends you use the following to prepare .lua files:

- third-party instruction and reference material for the lua programming language
- The Open Source Detectors Developers Guide: https://www.snort.org/downloads
- OpenAppID Snort community resources: http://blog.snort.org/search/label/openappid

---

**Note**

The system does not support .lua files that reference system calls or file I/O.

---

**Before you begin**

- Begin configuring your custom application protocol detector as described in Configuring Custom Application Detectors, on page 9.
• Prepare to create a valid .lua file by downloading and studying the .lua files for comparable detectors. For more information about downloading detector files, see Viewing or Downloading Detector Details, on page 14.

• Create a valid .lua file that contains your custom application detector settings.

Procedure

**Step 1**
On the Create Detector page for an advanced custom application detector, in the Detection Criteria section, click **Add**.

**Step 2**
Click **Browse...** to navigate to the .lua file and upload it.

**Step 3**
Click **OK**.

What to do next

• Continue configuring your custom application protocol detector as described in Configuring Custom Application Detectors, on page 9. You must save and activate the detector before the system can use it to analyze traffic.

Related Topics

Specifying Detection Patterns in Basic Detectors, on page 11

Testing a Custom Application Protocol Detector

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Discovery Admin</td>
</tr>
</tbody>
</table>

If you have a packet capture (pcap) file that contains packets with traffic from the application protocol you want to detect, you can test a custom application protocol detector against that pcap file. Cisco recommends using a simple, clean pcap file without unnecessary traffic.

Pcap files must be 256 KB or smaller; if you try to test your detector against a larger pcap file, the Firepower Management Center automatically truncates it and tests the incomplete file. You must fix the unresolved checksums in a pcap before using the file to test a detector.

Before you begin

• Configure your custom application protocol detector as described in Configuring Custom Application Detectors, on page 9.

Procedure

**Step 1**
On the Create Detector page, in the Packet Captures section, click **Add**.

**Step 2**
Browse to the pcap file in the pop-up window and click **OK**.
Step 3 To test your detector against the contents of the pcap file, click the evaluate icon next to the pcap file. A message indicates whether the test succeeded.

Step 4 Optionally, repeat steps 1 to 3 to test the detector against additional pcap files.

Tip To delete a pcap file, click the delete icon ( ) next to the file you want to delete.

What to do next

- Continue configuring your custom application protocol detector as described in Configuring Custom Application Detectors, on page 9. You must save and activate the detector before the system can use it to analyze traffic.

Viewing or Downloading Detector Details

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Discovery Admin</td>
</tr>
</tbody>
</table>

You can use the detectors list to view application detector details (all detectors) and download detector details (custom application detectors only).

Procedure

Step 1 To view application detector details, do one of the following:


  - b. Filter the list to find a particular detector.
  - c. Click the information icon ( )

Step 2 To download detector details for a custom application detector, click the download icon ( ).

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have the necessary permissions.
Sorting the Detector List

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Discovery</td>
</tr>
</tbody>
</table>

By default, the Detectors page lists detectors alphabetically by name. An up or down arrow next to a column heading indicates that the page is sorted by that column in that direction.

**Procedure**

**Step 1** Select Policies > Application Detectors.

**Step 2** Click the appropriate column heading.

Filtering the Detector List

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Discovery</td>
</tr>
</tbody>
</table>

**Procedure**

**Step 1** Select Policies > Application Detectors.

**Step 2** Expand one of the filter groups described in Filter Groups for the Detector List, on page 15 and select the check box next to a filter. To select all filters in a group, right-click the group name and select Check All.

**Step 3** If you want to remove a filter, click the remove icon (×) in the name of the filter in the Filters field or disable the filter in the filter list. To remove all filters in a group, right-click the group name and select Uncheck All.

**Step 4** If you want to remove all filters, click Clear all next to the list of filters applied to the detectors.

Filter Groups for the Detector List

You can use several filter groups, separately or in combination, to filter the list of detectors.

**Name**

Finds detectors with names or descriptions containing the string you type. Strings can contain any alphanumeric or special character.
**Custom Filter**
Finds detectors matching a custom application filter created on the object management page.

**Author**
Finds detectors according to who created the detector. You can filter detectors by:
- any individual user who has created or imported a custom detector
- Cisco, which represents all Cisco-provided detectors *except* individually imported add-on detectors (you are the author for any detector that you import)
- *Any User*, which represents all detectors not provided by Cisco

**State**
Finds detectors according to their state, that is, *Active* or *Inactive*.

**Type**
Finds detectors according to the detector type, as described in Application Detector Fundamentals, on page 2.

**Protocol**
Finds detectors according to which traffic protocol the detector inspects.

**Category**
Finds detectors according to the categories assigned to the application they detect.

**Tag**
Finds detectors according to the tags assigned to the application they detect.

**Risk**
Finds detectors according to the risks assigned to the application they detect: *Very High*, *High*, *Medium*, *Low*, and *Very Low*.

**Business Relevance**
Finds detectors according to the business relevance assigned to the application they detect: *Very High*, *High*, *Medium*, *Low*, and *Very Low*.

# Navigating to Other Detector Pages

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Discovery Admin</td>
</tr>
</tbody>
</table>
### Activating and Deactivating Detectors

You must activate a detector before you can use it to analyze network traffic. By default, all Cisco-provided detectors are activated.

You can activate multiple application detectors for each port to supplement the system’s detection capability. When you include an application in an access control rule in a policy and that policy is deployed, if there is no active detector for that application, one or more detectors automatically activate. Similarly, while an application is in use in a deployed policy, you cannot deactivate a detector if deactivating leaves no active detectors for that application.

**Tip**
For improved performance, deactivate any application protocol, client, or web application detectors you do not intend to use.

### Procedure

**Step 1** Select Policies > Application Detectors.

**Step 2** Click the slider next to the detector you want to activate or deactivate. If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Note** Some application detectors are required by other detectors. If you deactivate one of these detectors, a warning appears to indicate that the detectors that depend on it are also disabled.
Editing Custom Application Detectors

Use the following procedure to modify custom application detectors.

**Procedure**

**Step 1** Select Policies > Application Detectors.

**Step 2** Click the edit icon (✏️) next to the detector you want to modify. If a view icon (👀) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 3** Make changes to the detector as described in Configuring Custom Application Detectors, on page 9.

**Step 4** You have the following saving options, depending on the state of the detector:

- To save an inactive detector, click Save.
- To save an inactive detector as a new, inactive detector, click Save as New.
- To save an active detector and immediately start using it, click Save and Reactivate.
- To save an active detector as a new, inactive detector, click Save as New.

Deleting Detectors

You can delete custom detectors as well as individually imported add-on detectors provided by Cisco Professional Services. You cannot delete any of the other Cisco-provided detectors, though you can deactivate many of them.

**Note**

While a detector is in use in a deployed policy, you cannot delete the detector.

**Procedure**

**Step 1** Select Policies > Application Detectors.
**Step 2**  
Click the delete icon (🗑️) next to the detector you want to delete. If a view icon (👀) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 3**  
Click **OK**.