



HTTP/HTTPS Proxy Policy

- [About the HTTP/HTTPS Proxy Policy, on page 1](#)
- [Cisco APIC Features That Use the HTTP/HTTPS Proxy, on page 1](#)
- [Configuring the HTTP/HTTPS Proxy Policy Using the GUI, on page 2](#)

About the HTTP/HTTPS Proxy Policy

Beginning with release 5.2(1), you can configure the HTTP or HTTPS proxy address on Cisco Application Policy Infrastructure Controller (APIC) for features that need Internet access. In addition to Cisco APIC features that automatically use the configured proxy addresses, the surrounding ecosystems of the Cisco APIC can also query the object `proxyServer` on the Cisco APIC so that the ecosystems can use the same proxy server as the Cisco APIC without needing you to configure the proxy information on multiple platforms.

The HTTP/HTTPS proxy policy itself does not control nor alter the management network (out-of-band or in-band) that each Cisco APIC feature uses. You can specify the management network setting in the Cisco APIC Connectivity Preferences. For more information, see the "Adding Management Access" section in the "Management" chapter of the *Cisco APIC Basic Configuration Guide*.

Cisco APIC Features That Use the HTTP/HTTPS Proxy

If you configured an HTTP or HTTPS proxy server, the following Cisco Application Policy Infrastructure Controller (APIC) features send the traffic through the proxy server:

- Cisco Intersight - Device Connector
- Cisco APIC GUI built-in feedback feature



Note

Before release 5.2(1), Cisco Intersight - Device Connector had a built-in proxy setting. This functionality now exists in the HTTP/HTTPS proxy policy in Cisco APIC.

Configuring the HTTP/HTTPS Proxy Policy Using the GUI

The following procedure configures the HTTP or HTTPS proxy policy. You can also configure the proxy settings through the First Time Setup wizard. For more information about First Time Setup wizard, see the chapter "First Time Setup Wizard" in the *Cisco APIC Basic Configuration Guide*.

Procedure

Step 1 On the menu bar, choose **System > System Settings**.

Step 2 In the Navigation pane, choose **Proxy Policy**.

Step 3 In the Work pane, enter a URL in the **HTTP URL** or **HTTPS URL** field as appropriate.

When a proxy server requires authentication, use the following format:

```
http[s]://[username:password]@proxy-server[:proxyport]
```

Step 4 (Optional) In the **Ignore Hosts** table, click +, enter the hostname or IP address of a host that should not use the HTTP or HTTPS proxy, and click **Update**.

Repeat this step if you want to add more hosts that should not use the HTTP or HTTPS proxy.
