

# Filter Traffic Destined to Cisco IOS XE Devices WebUI Using an Access List

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background](#)

### [Configure](#)

[HTTP Service Access Class Configuration](#)

[IPv4 Example](#)

[IPv6 Example](#)

### [Verify](#)

[Q: After applying the access-list I am getting a 403 response instead of no response. Why?](#)

---

## Introduction

This document describes how to configure an Access List (ACL) on a Cisco IOS XE device to filter traffic destined for the Web Services.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

This document is written for Enterprise devices running Cisco IOS® XE software.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

### Background

When HTTP Web Services are required to be enabled to have webUI access to manage the IOS XE device or for webauth/guest user access, traffic filtering features can be implemented to ensure only the necessary IP addresses can access the WebUI and guest users can continue to onboard to the network.

## Configure

## HTTP Service Access Class Configuration


The simplest method to define access can be done through the IP Access Class support on the HTTP Web Server. In this configuration example, the ipv4 subnet 192.168.10.0/24 is permitted, ipv6 subnet fd00::/64 is permitted, and everything else is denied. There is an implicit deny any any at the end of the access-list but you can also add an explicit deny any any if you wish. In the case of the C9800 Wireless Lan Controller be sure to consider HTTP/HTTPS access to the Wireless Management Interface (WMI) and out-of-band management/Service port.

### IPv4 Example

Step 1. Configure a Standard ACL and include the trusted devices/subnets that are allowed to access the Cisco IOS XE Device over HTTP/HTTPS

```
ip access-list standard restrict_ipv4_webui
permit 192.168.10.0 0.0.0.255
```

---

 **Note:** This ACL must only include subnets trusted to have web admin access to the IOS XE device. That is, any guest subnets must not be included in this ACL. Not including guest subnets does not break web auth, guest access, or web redirect.

---

Step 2. Assign the Standard ACL to the HTTP Web Service access-class.

```
ip http access-class ipv4 restrict_ipv4_webui
```

### IPv6 Example

Step 1. Configure an IPv6 ACL include the trusted devices/subnets that are allowed to access the Cisco IOS XE Device over HTTP/HTTPS

```
ipv6 access-list restrict_ipv6_webui
permit fd00::/64 any
```

Step 2. Assign the Standard ACL to the HTTP Web Service feature.

```
ip http access-class ipv6 restrict_ipv6_webui
```

## Verify

Check the IPv4 ACL entries

```
show ip access-list restrict_ipv4_webui
Standard IP access list restrict_ipv4_webui
10 permit 192.168.10.0 0.0.0.255
```

Check the IPv6 ACL entries

```
show ipv6 access restrict_ipv4_webui
IPv6 access list restrict_ipv6_webui
permit ipv6 FD00::/64 any sequence 10
```

## **Q: After applying the access-list I am getting a 403 response instead of no response. Why?**

A: This is expected behavior. The access-list is designed to limit who is allowed to access the http/https process. A 403 response indicates that you are forbidden to access this resource and is the proper response in this scenario since the access-list is applied to the HTTP/HTTPS process as opposed to an interface level access-list. If the access-list was applied to an interface instead of the HTTP/HTTPS process, then no response would be the appropriate