

# Cisco Cloud Web Security: Direct-to-Tower Activation Guide

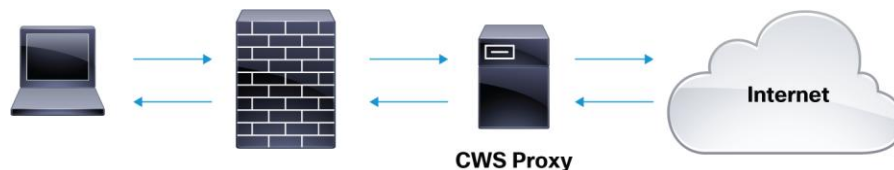


This document outlines the deployment of the Cisco Cloud Web Security (CCWS) service. Included are the deployment description, configuration checklist, and step-by-step video tutorials that detail all the steps necessary to successfully activate the Filtering and Scanning of Web traffic.

This deployment configures the browser to send web requests directly to the Cisco Cloud. There is no end-user granularity since using this method only considered redirection, but company-wide trends can be observed (If user details are needed for policy enforcement or reporting, then authentication solutions like EasyID or SAML can be used).

If a Customer has various offices globally (coming from different external IPs) then it is possible for each office to have its own Policy. Exceptions (sites the customer does not want Cisco to browse) can be easily managed by using the PAC file located on the Cisco Tower. Settings on the Browser would need to be managed using centralized software or manually on each machine.

**Figure 1.** Direct-to-Tower Traffic Flow



---

## Client Checklist

- Configure the firewall to allow port 8080 outbound to the allocated Web Security tower. If exceptions are configured, port 80 outbound access will also be required.
- Provide your public facing external IP addresses that we can expect traffic from to your Technical Account Manager (see video 2a). This is used to authorize your traffic into the Cisco Cloud.
- Ensure that there is no rate limiting on the firewall that will prevent or hinder connections to our tower. This may be rate limiting or DoS Protection.
- Gather any supplier sites that are TCP wrapped, or rely on traffic originating from a static source IP and will not accept connections via our towers. These need to be noted for exception.
- Gather any internal or external domains or URLs that need exception.

## Video Tutorials

### Cisco Cloud Web Security Preparation

These videos are a good reference for gathering the needed items for the configuration. It also reviews how to test basic connectivity.

1. [Verify Connection to Tower](#)
2. [Determining Your Egress IP](#)

### Web Traffic Redirection

These videos review how the Hosted PAC files can be used to manage web traffic. PAC files give administrators a convenient way to redirect traffic and manage exceptions.

3. [How to Configure a PAC File](#)
4. [How to Host a PAC File in the Cisco Cloud](#)
5. [How to Configure Clients to use a PAC File](#)

---

## Portal Configuration

After traffic is successfully redirected and user credentials are being passed to the Cloud, it's time to configure the Web Filtering policy.

6. [How to Create and Manage Groups in the CCWS Portal](#)
7. [How to Manage and Configure Web Filtering Policy](#)
8. [Cisco Cloud Web Security Portal Overview](#)



---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)