

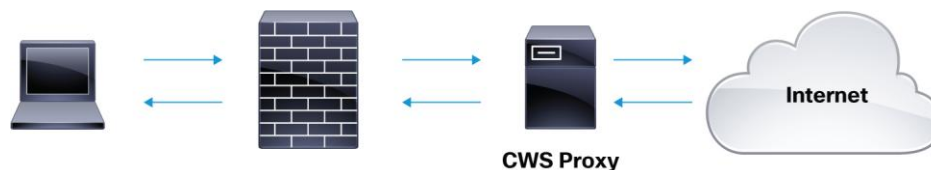
## Cisco Cloud Web Security: PIM Activation Guide



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.

PIM has been developed to provide user level granularity for Cisco's cloud-based web filtering and malware scanning solutions. It is a small Microsoft Windows application, typically executed via a logon script to obtain user or group information. This information is synchronized with the Cloud via an HTTPS request and an encrypted user identifier is embedded in the browser user-agent request header for all subsequent web requests. Please keep in mind that the identifier is meaningless to any person or system except Cisco's Web Scanning Services proxies. HTTP and HTTPS traffic is redirected to the Cisco Cloud using a proxy setting or proxy-auto config (PAC) file. There is no performance overhead or increased packet size because PIM sends User and Group data once only at the time of registration.

**Figure 1.** Passive Identity Management Traffic Flow



### Support Platforms

PIM supports Microsoft Windows XP, Windows Vista, and Windows 7. The supported web browsers are Internet Explorer 6, 7, 8, and 9, and Firefox 3.6, 4, and 5.

---

## 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.
- Ensure any anti-virus software solution allows the PIM executable to write to the Windows registry.

**Note:** User and Group information can be obtained only using the gpresult API (Active Directory). PIM does not integrate with LDAP or other authentication methods. Only cached groups on the domain will be used for lookups.

## 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](#)

### Configuring Passive Identity Management

This video details the configuration for Passive Identity Management. When run, this executable will obtain users information and sync it with the Cisco Cloud.

6. [How to Configure Passive Identity Management](#)

---

## 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.

7. [How to Create and Manage Groups in the CCWS Portal](#)
8. [How to Manage and Configure Web Filtering Policy](#)
9. [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)