



Cisco Cloud Web Security

WSA Deployment Guide

Contents

Introduction.....	1
Cloud Deployment.....	1
Additional Redirect Methods	1
Prepare.....	2
Verify connection to a tower.....	2
Create authentication license key	3
Deploy	5
Configure WSA Connector.....	5
Run the System Setup Wizard.....	5
Add an Authentication Realm	9
Configure Identity Management.....	12
Configure Directory Groups	13
Configure WSAv Connector	14
Test	16
Verify web redirection to the cloud	16

Introduction

Integrate CWS and WSA to enable identity information to the cloud and extend other on-premises enterprise features to Cloud Web Security customers.

This document provides directions to redirect network traffic to CWS through the WSA/WSAv Connectors.

*Note: we refer to our cloud proxies as towers. You will see the terms “proxy” and “tower” used interchangeably throughout the document.

Cloud Deployment

Deployment is divided into the following three sections



Prepare

Deploy

Test

Additional Redirect Methods

There are 4 additional redirection methods that have corresponding deployment guides. Deployment guides for each redirection methods can be found [here](#), under Technical Collateral.

 Cisco Integrated Services Router (ISR G2 with CWS Connector)	Save bandwidth, money and resources by intelligently redirecting Internet traffic from branch offices directly to the cloud to enforce security and control policies. Apply acceptable use policy to all users regardless of location.
 Next Generation Firewall (ASA/ASAv with CWS Connector)	Capitalize ASA investments by offloading content scanning to Cisco's cloud through CWS. Apply acceptable use policy to the company, groups or individual users.
 Cisco AnyConnect Secure Mobility Client (AnyConnect)	Authenticate and redirect web traffic securely whenever the end user is off the corporate network. CWS leverages cached user credentials and directory information when they are away from the office or VPN, ensuring that exactly the same web-usage policies are applied.
 Standalone Deployment	Deploy a simple web security solution that does not require any additional hardware. Connect to Cisco's Cloud Web Security service using existing browser settings and PAC/WPAD files.

Prepare

Verify connection to a tower

Site-to-tower communication is accomplished over TCP port 8080. HTTP and HTTPS requests are sent to a cloud scanning tower in this method. Therefore, TCP port 8080 outbound is required to be open for all users within the organization. For security reasons, Cisco recommends that port 8080 outbound destinations be limited to the scanning towers provisioned for the customer's account.

Reference video: [Verify connection to a tower](#)

Step 1: Log on to a client computer inside the customer's network.

Step 2: Click on the Control Panel and go to Programs and Features.

Step 3: Click Turn on Windows features on or off. Scroll down the list of available features until you find the Telnet Client. Check the box and click OK. Now that the Telnet Client is installed, we can resume our test.



Figure 1.1

Step 4: Open the command line window and type command 'telnet [tower IP address] 8080.' A successful connection is noted by a blank screen and blinking cursor.

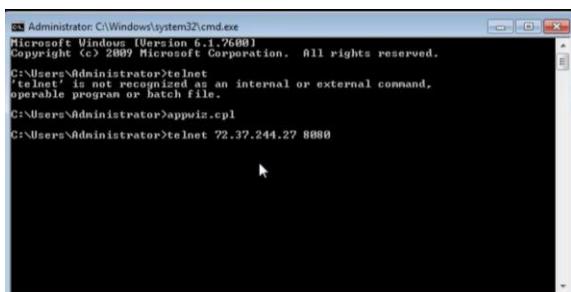


Figure 1.2

Create authentication license key

Reference video: [Authentication license key creation and management](#)

Step 1: Log on to the Cisco Cloud Web Security portal at <https://scancenter.scansafe.com/>.

Step 2: From the *Admin* tab, mouse over *Authentication*, and select the key that you would like to generate. The options are *Company Key* and *Group Key*. To have a single key for all users in the company (can be used in various Connectors), AnyConnect, or a mixture of them all, select *Company Key*.

Step 3: Notice that no Company Key currently exists in this account. Click the *Create Key* button to create the Company Key . If one already exists and you don't know the whole string (only the last four characters will be seen), then you will have to revoke it before you can create a new one, but then if it is in use anywhere (Connectors or AnyConnect) then it will have to be replaced with the new one.

Step 4: The key is active immediately. The email option below is only for the admin to have a backup of the key. **Note:** Once you navigate away from the page you'll no longer see the complete string of the key (only the last 4 characters will be displayed henceforth).

Name	Authentication Key Type	Authentication Key
Cisco Demo	Company	7048C89ABDEDEF628F6C6DC6D57A105A

Figure 1.3

Step 5: Copy the entire alphanumeric string in the *Authentication Key* field and record it in a document that will be backed up.

*Note: The second option is to create a group key by selecting *Group Key* under *Authentication*. To create a group key you may either use an existing directory group or you may create a custom group under → Admin → Management → Groups.

Step 6: Click on the *Create Key* button which corresponds to the group for which you are creating a key.

Create, activate and deactivate a group authentication key				
To add or delete a group, go to the "Groups" link in the "Management" menu or click here				
Group Name	Key Ref	State	Action	Sel.
WinNT://ORG\WebSec No Access	ⓘ No key	ⓘ No key	Create Key	<input type="checkbox"/>
WinNT://ORG\WebSec Privileged Access	ⓘ No key	ⓘ No key	Create Key	<input type="checkbox"/>
WinNT://ORG\WebSec Social Networking	ⓘ No key	ⓘ No key	Create Key	<input type="checkbox"/>
WinNT://ORG\web_execs	ⓘ No key	ⓘ No key	Create Key	<input type="checkbox"/>
WinNT://ORG\web_execs_minus_email_and_chat	ⓘ No key	ⓘ No key	Create Key	<input type="checkbox"/>
WinNT://ORG\web_management	ⓘ No key	ⓘ No key	Create Key	<input type="checkbox"/>
WinNT://ORG\web_no_access	ⓘ No key	ⓘ No key	Create Key	<input type="checkbox"/>
WinNT://ORG\web_sales	ⓘ No key	ⓘ No key	Create Key	<input type="checkbox"/>
WinNT://ORG\web_staff	ⓘ No key	ⓘ No key	Create Key	<input type="checkbox"/>
WinNT://ORG\web_warehouse	ⓘ No key	ⓘ No key	Create Key	<input type="checkbox"/>

10 items found, displaying all items.

Page 1

[Activate Selected](#) [Deactivate Selected](#) [Revoke Selected](#) [Select All](#) [Deselect All](#)

Figure 1.4

*Note: It is the same UI and process for creating a Company Key

Deploy

Configure WSA Connector

This document is intended to provide an overview of the deployment process. For more detailed information and troubleshooting, please refer to the [Admin Guide](#).

Typically when configuration changes are submitted on the WSA they are not immediately committed. When you see the yellow *Commit Changes* button appear in the upper right after making a configuration change, you must click it and then you will be presented with an option to commit the change with notes or abandon the changes. Please be sure to commit your changes as you complete the recommended configurations in this guide.



Figure 2.1

Run the System Setup Wizard

Step 1: Logon to the WSA/WSAv appliance. Default credentials are:

- Username – admin
- Password – ironport



Figure 2.2

Step 2: To begin setup, select **System Administrator > System Setup Wizard**

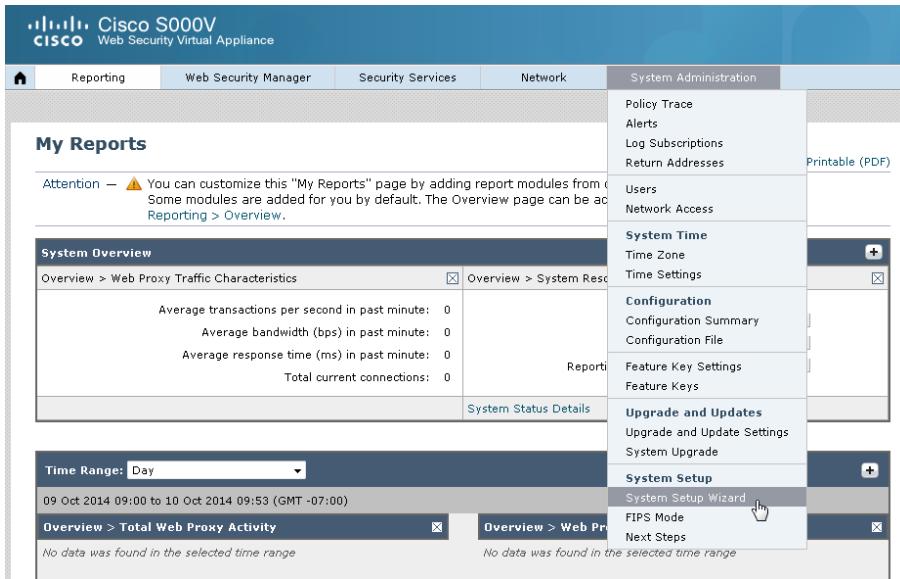


Figure 2.3

Step 3: Configure the following:

- Default System Hostname – a DNS name that will resolve to the IP address of this WSA
- DNS Server – supply at least one DNS server
- NTP Server – supply a server where this WSA may automatically configure time from
- Time Zone – select the time zone for which this WSA resides in
- Appliance Mode of Operation – select **Cloud Web Security Connector**

The screenshot shows the Cisco WSA deployment wizard, Step 2: Network. The top navigation bar includes tabs for 1. Start, 2. Network, 3. Security, and 4. Review. The 2. Network tab is active. The main form is divided into sections: **System Settings** and **Appliance Mode**. In the System Settings section, the 'Default System Hostname' field contains 'wsacomm.stbulab.com'. The 'DNS Server(s)' section has two options: 'Use the Internet's Root DNS Servers' (radio button) and 'Use these DNS Servers' (radio button, selected), with two input fields containing '10.6.1.5' and '10.6.1.4'. The 'NTP Server' field contains 'time.sco.cisco.com'. The 'Time Zone' section includes 'Region' (set to 'America'), 'Country' (set to 'United States'), and 'Time Zone / GMT Offset' (set to 'Pacific Time (Los_Angeles)'). In the **Appliance Mode** section, the 'Appliance Mode of Operation' dropdown has two options: 'Standard' (radio button) and 'Cloud Web Security Connector' (radio button, selected). A note under 'Standard' states: 'This appliance will be used for on-premise policy enforcement (Standard Web Security Appliance installation)'. A note under 'Cloud Web Security Connector' states: 'This appliance will be used primarily to direct traffic to Cisco Cloud Web Security for cloud policy enforcement and threat defense (Cloud Web Security Connector installation)'. At the bottom of the form are buttons for '< Prev' and 'Cancel' on the left, and 'Next >' on the right.

Figure 2.4

Step 4: Define the Following:

- Cloud Web Security Proxy Servers – supply the primary and secondary (backup) Cloud Web Security Proxy Server's host names or IP addresses.
- Failure Handling – this is how the WSA will handle web requests if it loses connection with both primary and secondary *Cloud Web Security Proxy Servers*.

- Cloud Web Security Authorization Scheme bullet *Send authorization key information with transaction*, and provide the **Authentication Key** generated from ScanCenter (see above).

1. Start 2. Network 3. Review

Cloud Web Security Connector Settings

Cloud Web Security Proxy Servers:	<input type="text" value="cess801.cws.sco.cisco.com"/> <input type="text" value="cess601.cws.sco.cisco.com"/> <input type="text" value=""/> <small>hostname or IP address</small>
Failure Handling:	<small>Specify how to handle requests if all specified Cloud Web Security Proxy servers fail.</small> <input checked="" type="radio"/> Connect directly <input type="radio"/> Drop requests
Cloud Web Security Authorization Scheme:	<input type="radio"/> Authorize transaction based on IP address <input checked="" type="radio"/> Send authorization key information with transaction <small>Authorization Key: 0123456789ABCDEF0123456789ABCDEF</small>

< Prev Cancel Next >

Figure 2.5

Step 5: Provide an IP address, either IPv4 and/or IPv6, to be associated with this WSA. Subnet mask should be in CIDR notation.

1. Start 2. Network 3. Review

Network Interfaces and Wiring

Note:

M1 : This interface is used to manage the appliance. Optionally, it may also handle web traffic.
P1 : This interface may be used to handle web traffic.

Interfaces

Ethernet Port:	M1	<input type="checkbox"/> Use M1 port for management only	P1 (Optional if M1 used for data)
IPv4 Address / Netmask:	<input type="text" value="10.6.1.70/24"/>	<input type="text" value=""/>	<small>If multiple interfaces are configured, they must be assigned IP addresses on different subnets.</small>
IPv6 Address / Netmask:	<input type="text"/>	<input type="text"/>	
Hostname:	<input type="text" value="mgmt.wsacomm.stbulab.cor"/> (e.g. wsa.example.com)	<input type="text"/>	<small>(e.g. data.example.com)</small>

< Prev Cancel Next >

Figure 2.6

Step 6: Configure the **Default Gateway** this WSA will use.

1. Start **2. Network** 3. Review

IPv4 Routes for Management and Data Traffic (Interface M1: 10.6.1.70)

Default Gateway: <input type="text" value="10.6.1.1"/>		<i>This will be the default route for external traffic as well as internal traffic with no static route below.</i>	
Static Routes Table			
Optionally, add static routes for Management access to the Cisco Web Security Appliance as well as Data traffic. Depending on the appliance functions you enable, these routes will be used for monitoring by the Secure Web Proxy and optional blocking by the L4 Traffic Monitor.			
Name <input type="text"/>	Internal Network <input type="text"/>	Internal Gateway <input type="text"/>	<input type="button" value="Delete"/>
Identifying name for route	IPv4 Address (such as 10.1.1.10) or CIDR (such as 10.1.1.0/24)	IPv4 Address	<input type="button" value="Add Route"/>

[« Prev](#) [Cancel](#) [Next »](#)

Figure 2.7

Step 7: If clients will use a PAC/WPAD file or layer 4 switch to forward web traffic to this WSA, select *Layer 4 Switch or No Device*. If clients will transparently redirect traffic to this WSA, select *WCCP v2 Router*.

1. Start **2. Network** 3. Review

Transparent Connection Settings

For the Cisco Web Security Appliance to accept transparent connections, it must be connected via a Layer 4 switch or WCCP router.

Transparent Redirection Device:	<input checked="" type="radio"/> Layer 4 Switch or No Device <i>If no transparent redirection device is connected, only explicit forward requests can be proxied.</i> <input type="radio"/> WCCP v2 Router
	<input type="checkbox"/> Enable standard service ID: 0 web_cache (port 80)
	Router Addresses: <input type="text"/> <i>Separate multiple addresses with commas or whitespace.</i>
	<input type="checkbox"/> Enable router security for this service
	Password: <input type="password"/>
	Confirm Password: <input type="password"/> <i>Must be 7 or less characters.</i>
<i>Additional WCCP services and advanced options can be configured after completing the System Setup Wizard.</i>	

[« Prev](#) [Cancel](#) [Next »](#)

Figure 2.8

Step 8: Supply a secure password, an email address to send system alerts to, and (optionally) an SMTP relay to send email through.

The screenshot shows the 'Administrative Settings' configuration page. It includes fields for Administrator Password, Password (must be 6 or more characters), Confirm Password, Email system alerts to (admin@example.com), Send Email via SMTP Relay Host (optional) (smtp.example.com, 10.0.0.3), Port (optional), and AutoSupport (checkbox). Navigation buttons at the bottom include < Prev, Cancel, and Next >.

Administrative Settings	
Administrator Password:	<input type="password"/> Password: ***** <small>Must be 6 or more characters</small> <input type="password"/> Confirm Password: *****
Email system alerts to:	<input type="text"/> admin@example.com <small>e.g. admin@company.com</small>
Send Email via SMTP Relay Host (optional): <small>(?)</small>	<input type="text"/> i.e., smtp.example.com, 10.0.0.3 <small>Port: <small>(?)</small> optional</small>
AutoSupport:	<input checked="" type="checkbox"/> Send system alerts and weekly status reports to Cisco Customer Support

< Prev Cancel Next >

Figure 2.9

Step 9: Once configuration is complete, click **Install This Configuration**.



Figure 2.10

Add an Authentication Realm

Step 1: To create an authentication realm, click **Network > Authentication**.

The screenshot shows the Cisco S000V Web Security Virtual Appliance interface. The 'Network > Authentication' menu item is highlighted with a cursor. Other menu items include Interfaces, Transparent Redirection, Routes, DNS, Internal SMTP Relay, External DLP Servers, and Cloud Connector. The 'System Status' and 'Web Security Appliance Status' sections are also visible.

Figure 2.11

Step 2: Click **Add Realm**.

Authentication

The screenshot shows the 'Authentication' configuration page. At the top, there's a section titled 'Authentication Realms' with a button labeled 'Add Realm'. Below it, a message says 'No authentication realms have been defined.' Under the main title, there are two sections: 'Global Authentication Settings' and 'Authentication Settings'. In 'Global Authentication Settings', there are four rows: 'Action if Authentication Service Unavailable' (Block all traffic if authentication fails), 'Failed Authentication Handling' (Log Guest User by: IP Address), 'Re-authentication' (Disabled), and 'Basic Authentication Token TTL' (3600). In 'Authentication Settings', there are four rows: 'Credential Encryption' (Disabled), 'Redirect Hostname' (mgmt.wsacomm.stbulab.com), 'Credential Cache Options' (Surrogate Timeout: 3600 seconds, Client IP Idle Timeout: 3600 seconds, Cache Size: 8192 entries), and 'User Session Restrictions' (Disabled). A 'Edit Global Settings...' button is located at the bottom right.

Figure 2.12

Step 3: Configure the following and then click **Join Domain**:

- Realm Name – is a friendly name that identifies the authentication realm.
- Authentication Server Type and Scheme(s) – select *Active Directory* (or *LDAP* if not using Microsoft Active Directory).
- Active Directory Server – supply at least one domain controller host name or IP address that will manage authenticating users.
- Active Directory Domain – supply the FQDN of the active directory domain.

Add Realm

The screenshot shows the 'Add Realm' configuration page. It has three main sections: 'Authentication Realm', 'Active Directory Authentication', and a status message at the bottom. In the 'Authentication Realm' section, 'Realm Name' is set to 'STBULAB' and 'Authentication Server Type and Scheme(s)' is set to 'Active Directory (Kerberos, NTLMSSP or Basic Authentication)'. In the 'Active Directory Authentication' section, 'Active Directory Server' is configured with two IP addresses: '10.6.1.5' and '10.6.1.4', with a placeholder 'hostname or IP address'. In the 'Active Directory Account' section, 'Active Directory Domain' is set to 'stbulab.com', 'Computer Account' is selected, and 'Location' is set to 'Computers'. A note says '(Example: Computers/BusinessUnit/Department/Servers)'. At the bottom, a 'Join Domain...' button is available, and a status message says 'Status: Computer account wsaconn\$ not yet created.'

Figure 2.13

Step 4: After clicking **Join Domain**, you will be presented with an authentication challenge. The credentials used should have permissions to add objects to Active Directory. These credentials will NOT be saved and are used this one time to create a computer account in Active Directory for the WSA.

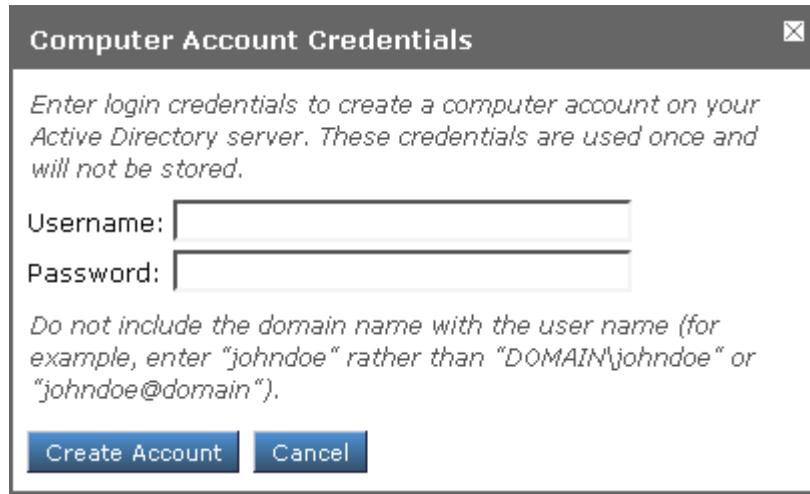


Figure 2.14

Step 5: Once the computer account for the WSA has been completed, click **Start Test** to ensure all authentication operations function as expected. Once the test has completed successfully, click **Submit**.

The page has a 'Join Domain...' button at the top right. The main area has sections for 'Active Directory agent' (checkbox for 'Enable Transparent User Identification using Active Directory agent') and 'Network Security' (checkbox for 'Client Signing Required'). Below is a 'Test Current Settings' section with a 'Start Test' button. The results log shows: 'Checking local WSA time and server time difference... Success: AD Server time and WSA time difference within tolerance limit', 'Attempting to fetch group information... Success: Able to query for Group Information from Active Directory server '10.6.1.5'.', and 'Test completed successfully.'

Figure 2.15

Configure Identity Management

Step 1: To configure identity management, select **Web Security Manager > Identities**.

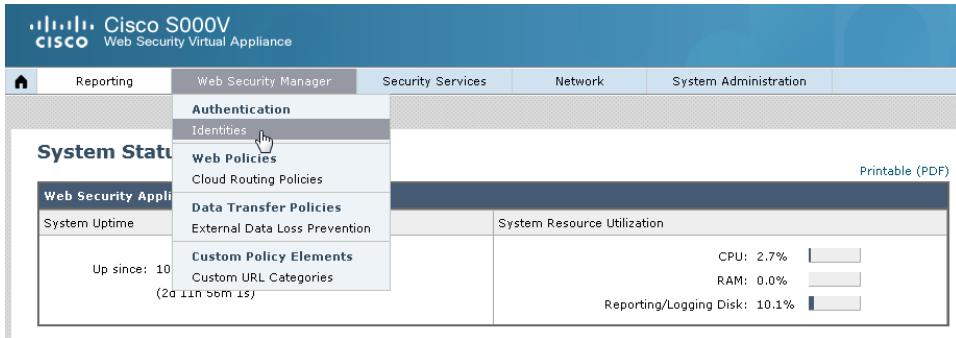


Figure 2.16

Step 2: Click **Add Identity**.

Identities

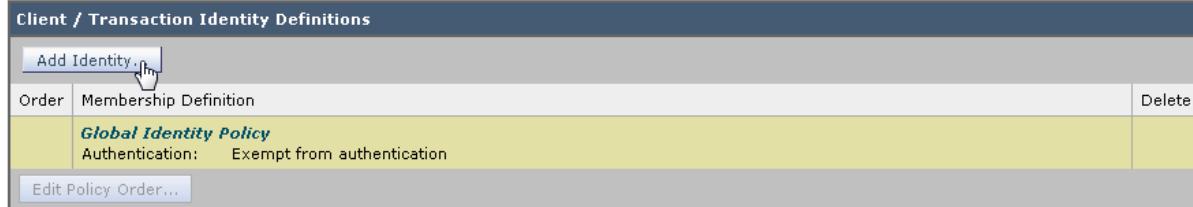


Figure 2.17

Step 3: Configure the following and then click **Submit**:

- Name – is a friendly name that identifies these identity settings.
- Identification and Authentication – select **Authenticate Users** from the dropdown list.
- Select a Realm or Sequence – select your authentication realm.
- Select a Scheme – select **Use NTLMSSP**.
- Authentication Surrogates – bullet **IP Address**.

*Note: cookie surrogates may not work with non-browser apps, such as desktop widgets or agents.

Identities: Add Identity

Identity Settings

Enable Identity

Name: <small>(e.g. my IT policy)</small>	<input type="text" value="CWS User Identity"/>
Description:	<input type="text"/>
Insert Above:	1 (Global Policy) <input type="button" value="▼"/>

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by Subnet:	<input type="text"/>
Identification and Authentication:	<input type="button" value="Authenticate Users"/> Select a Realm or Sequence: <small>(?)</small> STBULAB <input type="button" value="▼"/> Select a Scheme: <small>(?)</small> Use NTLMSSP <input type="button" value="▼"/> <small>Scheme setting applies to HTTP/HTTPS only.</small> If a user fails authentication: <input type="checkbox"/> Support Guest privileges <small>(?)</small> <small>Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Cloud Routing Policies and External Data Loss Prevention).</small>
Authentication Surrogates:	<small>(?)</small> <input checked="" type="radio"/> IP Address <input type="radio"/> Persistent Cookie <input type="radio"/> Session Cookie <input checked="" type="checkbox"/> Apply same surrogate settings to explicit forward requests <small>If this option is not selected, no surrogates will be used with HTTP/HTTPS explicit forward requests, and NTLM credential caching will not be available to these requests. In addition, re-authentication will not be available for Kerberos.</small>
<input type="button" value="Advanced"/> Define additional group membership criteria.	

Figure 2.18

Configure Directory Groups

Step 1: To identify directory groups that should be used with CWS, select **Network > Cloud Connector**.

Cisco S000V
CISCO Web Security Virtual Appliance

Reporting	Web Security Manager	Security Services	Network	System Administration												
Identities <table border="1"> <thead> <tr> <th colspan="2">Client / Transaction Identity Definitions</th> </tr> <tr> <th colspan="2"><input type="button" value="Add Identity..."/></th> </tr> <tr> <th>Order</th> <th>Membership Definition</th> </tr> </thead> <tbody> <tr> <td>1</td> <td> CWS User Identity <small>?</small> Authentication: Realm: STBULAB (Scheme: NTLMSSP) Surrogate Type: HTTP/HTTPS: IP Address </td> </tr> <tr> <td></td> <td> Global Identity Policy Authentication: Exempt from authentication </td> </tr> <tr> <td colspan="2"><input type="button" value="Edit Policy Order..."/></td> </tr> </tbody> </table>					Client / Transaction Identity Definitions		<input type="button" value="Add Identity..."/>		Order	Membership Definition	1	CWS User Identity <small>?</small> Authentication: Realm: STBULAB (Scheme: NTLMSSP) Surrogate Type: HTTP/HTTPS: IP Address		Global Identity Policy Authentication: Exempt from authentication	<input type="button" value="Edit Policy Order..."/>	
Client / Transaction Identity Definitions																
<input type="button" value="Add Identity..."/>																
Order	Membership Definition															
1	CWS User Identity <small>?</small> Authentication: Realm: STBULAB (Scheme: NTLMSSP) Surrogate Type: HTTP/HTTPS: IP Address															
	Global Identity Policy Authentication: Exempt from authentication															
<input type="button" value="Edit Policy Order..."/>																

Figure 2.19

Step 2: Click **Edit Groups**.**Cloud Connector Settings**

Cloud Web Security Connector Settings

Cloud Web Security Proxy Servers:	72.37.248.42, 108.171.130.128
Failure Handling:	Connect Directly
Cloud Web Security Authorization Scheme:	Authorization Key

Cloud Policy Directory Groups

No directory groups selected. Only groups used in Cloud Web Security Proxy Routing Policies will be sent.

Edit Groups...

Figure 2.20

Step 3: Select the groups to use with CWS in the *Directory Search* pane on the left, and click **Add** to place those groups in the *Authorized Groups* pane on the right. When complete click **Done**.

Edit Cloud Policy Directory Groups

Authorized Groups

Directory groups that are used to define Cloud Routing Policy membership will automatically be sent to the Web Cloud Security proxy server. Use the fields below to select additional group information that will be sent to the cloud for use in policy enforcement and reporting.

Start typing a group name into the Directory Search field to see matching entries from the directory. For Active Directory groups, omit the domain name (for instance, type "group" to find "DOMAIN\Group1"). The search is case-insensitive. The wildcard character "*" may be used. However, it cannot be used as the last character.

Select items from the Directory Search list and press Add to add them to the Authorized Groups list. Alternatively, you can type the entire name (for instance, to add a group that belongs to a trusted domain or a group that is not yet available in the directory). If group(s) are added that already exist in the Authorized Group list, the duplicates will be automatically omitted.

Realm: All Realms ▾

Directory Search: ?

Directory search completed (69 matches).

Realm: STBULAB

- STBULAB\\$M31000-0870A0DG0EA3
- STBULAB\Account Operators

Add »

Authorized Groups:

Realm: STBULAB

- STBULAB\Help Desk
- STBULAB\Human Resources
- STBULAB\Managers
- STBULAB\Marketing

Figure 2.21

Configure WSAv Connector

[This guide](#) should serve as a supplement to the current instructions.

Step 1: Download the WSAv Image

- Please contact your SE to obtain the WSAv license.

Step 2: Apply the WSAv Connector License

- Follow the video guide for help with installation:
<https://www.youtube.com/watch?v=3syECpx68HQ>

Step 3: Size the WSAv based on the Number of Transactions

- Set up the number of WSAvs needed based on the sizing. Since the WSAv Connector is not performing any security services, the “Essentials” RPS numbers can be used as guidance. The license you downloaded in the previous step can be used to activate all the WSAvs.
- The WSAV sizing guidelines for the Connector are in the table below.

	S300V	S100V	S000V
Peak RPS (Requests per Second)	608	316	147
Sustained RPS	608	316	147
Sustained Bandwidth	90 Mbps	47 Mbps	22 Mbps

Step 4: Download GD virtual image at or above ASyncOS 8.0.6

- Go to the Cisco Product Download page [here](#)
- Navigate to Security → Web Security → Web Security Virtual Appliance

Test

Verify web redirection to the cloud

Step 1: From a client machine, browse to whoami.scansafe.net. If a message is displayed, “User is not currently using the service,” then the traffic is not redirected to the Cisco cloud. This can be useful in determining if: the user is being resolved correctly, any groups being discovered, the internal/external IP of the user/location, and what Connector is in use.

This is an example of a successful whoami.scansafe.net output:

```
authUserName: "WinNT://CISCO\\user"
authenticated: true
companyName: Cisco
connectorGuid: 0123456789ABCDEF1234-0123456789AB
connectorVersion: coeus-x-x-x-xxx
countryCode: US
externalIp: 12.34.56.78
groupNames:
  - "WinNT://CISCO\\Group"
internalIp: 1.2.3.4
logicalTowerNumber: 1782
staticGroupNames:
  - "WinNT://CISCO\\Group"
userName: "WinNT://CISCO\\user"
```

Step 2: From a client machine, browse to policytrace.scansafe.net and enter a URL to see how the web request is processed against the current web filtering policy.

Step 3: With *SearchAhead* enabled in ScanCenter (the CWS admin portal), browse to Google, Bing, or Yahoo and search for something. The *SearchAhead* data should be prepended to each search result in the form of a green, yellow, or red dot. Mouse over the dot to see what information is contained within.

*Note: the search engine may enforce search results being displayed using HTTPS (such as Google). In this case you must enable HTTPS Inspection to see the *Search Ahead* results.



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.

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. 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. (1 1 OR)