



Cisco Cloud Web Security

WSA Deployment Guide

October 2014

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

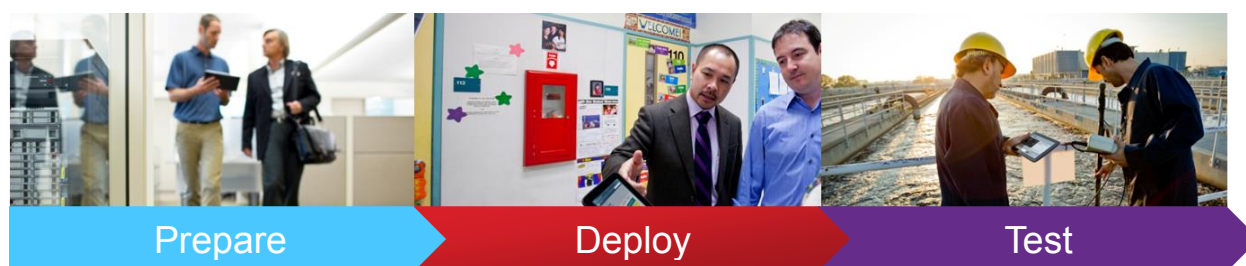
Integrate CWS and WSA to enable identity information to the cloud and extend other on-premises enterprise features to Cloud Web Security customers.

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



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.

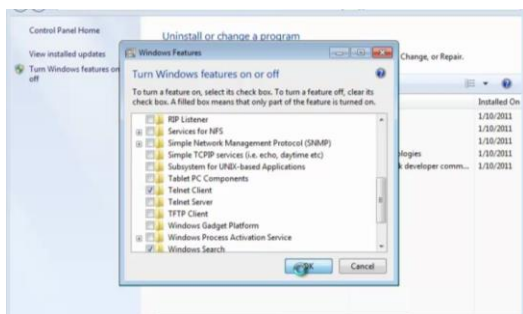


Figure 1.1

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.

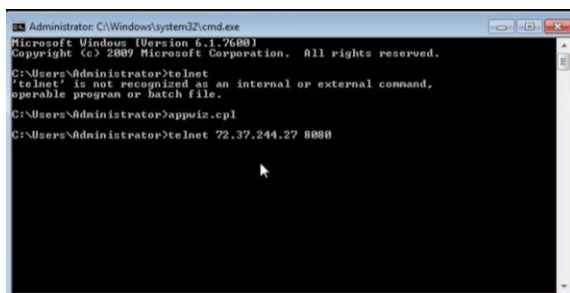


Figure 1.2

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).



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](#)

Search: Reload list 

Group Name	Key Ref	State	Action	Sel.
WinNT://ORG\WebSec No Access	 No key	 No key	<input type="button" value="Create Key"/>	<input type="checkbox"/>
WinNT://ORG\WebSec Privileged Access	 No key	 No key	<input type="button" value="Create Key"/>	<input type="checkbox"/>
WinNT://ORG\WebSec Social Networking	 No key	 No key	<input type="button" value="Create Key"/>	<input type="checkbox"/>
WinNT://ORG\web_execs	 No key	 No key	<input type="button" value="Create Key"/>	<input type="checkbox"/>
WinNT://ORG\web_execs_minus_email_and_chat	 No key	 No key	<input type="button" value="Create Key"/>	<input type="checkbox"/>
WinNT://ORG\web_management	 No key	 No key	<input type="button" value="Create Key"/>	<input type="checkbox"/>
WinNT://ORG\web_no_access	 No key	 No key	<input type="button" value="Create Key"/>	<input type="checkbox"/>
WinNT://ORG\web_sales	 No key	 No key	<input type="button" value="Create Key"/>	<input type="checkbox"/>
WinNT://ORG\web_staff	 No key	 No key	<input type="button" value="Create Key"/>	<input type="checkbox"/>
WinNT://ORG\web_warehouse	 No key	 No key	<input type="button" value="Create Key"/>	<input type="checkbox"/>

10 items found, displaying all items.

Page 1

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

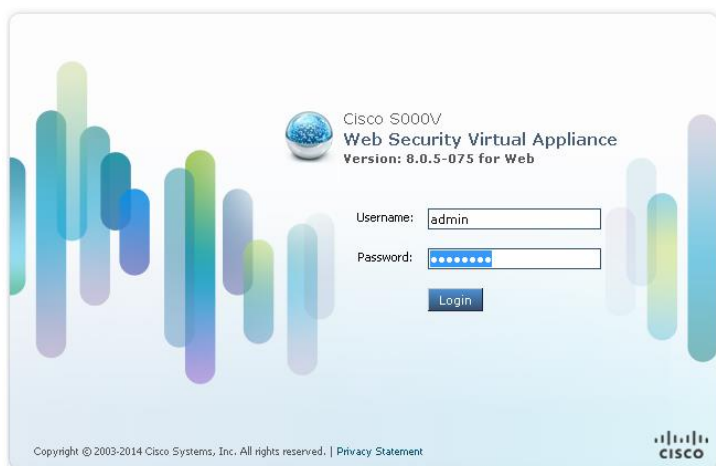


Figure 2.2

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

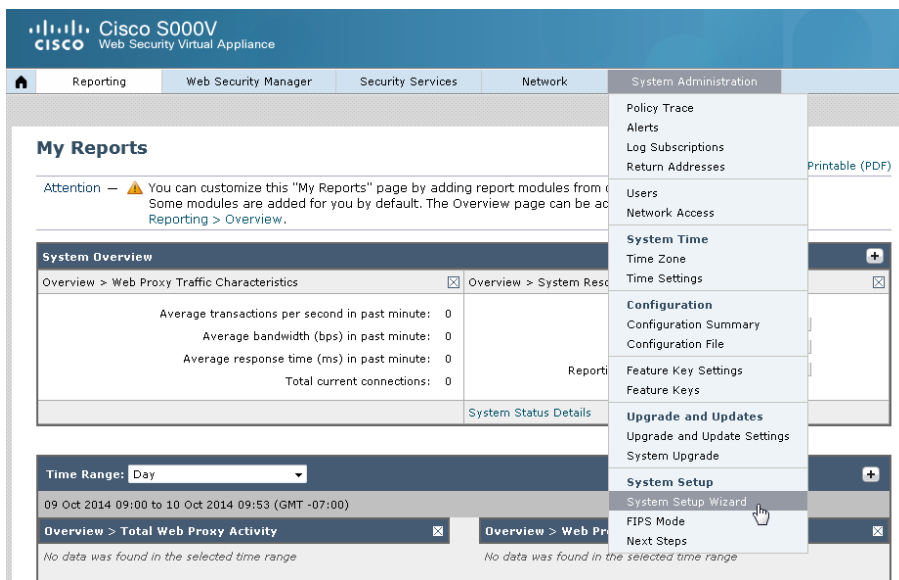


Figure 2.3

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**

1. Start	2. Network	3. Security	4. Review
System Settings			
Default System Hostname: ?	<input type="text" value="wsaconn.stbulab.com"/> <small>e.g. proxy.company.com</small>		
DNS Server(s):	<input type="radio"/> Use the Internet's Root DNS Servers <input checked="" type="radio"/> Use these DNS Servers: <input type="text" value="10.6.1.5"/> <input type="text" value="10.6.1.4"/> (optional) <input type="text"/> (optional)		
NTP Server:	<input type="text" value="time.sco.cisco.com"/>		
Time Zone:	Region: <input type="text" value="America"/> Country: <input type="text" value="United States"/> Time Zone / GMT Offset: <input type="text" value="Pacific Time (Los Angeles)"/>		
Appliance Mode			
Appliance Mode of Operation	<input type="radio"/> Standard <small>This appliance will be used for on-premise policy enforcement (Standard Web Security Appliance installation).</small> <input checked="" type="radio"/> Cloud Web Security Connector <small>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).</small>		
<input type="button" value="Prev"/> <input type="button" value="Cancel"/>		<input type="button" value="Next >"/>	

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, 7 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: ?	Server Address <input type="text" value="cws801.cws.sco.cisco.com"/> <input type="text" value="cws601.cws.sco.cisco.com"/> <input type="text"/> <i>hostname or IP address</i>	
Failure Handling:	Specify how to handle requests if all specified Cloud Web Security Proxy servers fail. <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 Authorization Key: <input type="text" value="0123456789ABCDEF0123456789ABCDEF"/>	
<input type="button" value=" < Prev"/> <input type="button" value=" Cancel"/>		<input type="button" value=" 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:	<input checked="" type="checkbox"/> M1 <input type="checkbox"/> Use M1 port for management only	<input type="checkbox"/> P1 <i>(Optional if M1 used for data)</i>
IPv4 Address / Netmask:	<input type="text" value="10.6.1.70/24"/> <i>If multiple interfaces are configured, they must be assigned IP addresses on different subnets.</i>	<input type="text"/>
IPv6 Address / Netmask:	<input type="text"/>	<input type="text"/>
Hostname:	<input type="text" value="mgmt.wsaconn.stbulab.cor"/> <i>(e.g. wsa.example.com)</i>	<input type="text"/> <i>(e.g. data.example.com)</i>
<input type="button" value=" < Prev"/> <input type="button" value=" Cancel"/>		<input type="button" value=" Next >"/>

Figure 2.6

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

1. Start	2. Network	3. Review												
<p>IPv4 Routes for Management and Data Traffic (Interface M1: 10.6.1.70)</p> <p>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></p> <p>Static Routes Table</p> <p>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.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Internal Network</th> <th>Internal Gateway</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td></td> </tr> <tr> <td><i>Identifying name for route</i></td> <td><i>IPv4 Address (such as 10.1.1.10) or CIDR (such as 10.1.1.0/24)</i></td> <td><i>IPv4 Address</i></td> <td></td> </tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Add Route"/></p>			Name	Internal Network	Internal Gateway		<input type="text"/>	<input type="text"/>	<input type="text"/>		<i>Identifying name for route</i>	<i>IPv4 Address (such as 10.1.1.10) or CIDR (such as 10.1.1.0/24)</i>	<i>IPv4 Address</i>	
Name	Internal Network	Internal Gateway												
<input type="text"/>	<input type="text"/>	<input type="text"/>												
<i>Identifying name for route</i>	<i>IPv4 Address (such as 10.1.1.10) or CIDR (such as 10.1.1.0/24)</i>	<i>IPv4 Address</i>												
<p><input type="button" value="Prev"/> <input type="button" value="Cancel"/> <input type="button" value="Next >"/></p>														

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
<p>Transparent Connection Settings</p> <p>For the Cisco Web Security Appliance to accept transparent connections, it must be connected via a Layer 4 switch or WCCP router.</p> <p>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></p> <p><input type="radio"/> WCCP v2 Router</p> <p><input type="checkbox"/> Enable standard service ID: 0 web_cache (port 80)</p> <p>Router Addresses: <input type="text"/> <i>Separate multiple addresses with commas or whitespace.</i></p> <p><input type="checkbox"/> Enable router security for this service</p> <p>Password: <input type="text"/></p> <p>Confirm Password: <input type="text"/> <i>Must be 7 or less characters.</i></p> <p><i>Additional WCCP services and advanced options can be configured after completing the System Setup Wizard.</i></p>		
<p><input type="button" value="Prev"/> <input type="button" value="Cancel"/> <input type="button" value="Next >"/></p>		

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.

1. Start	2. Network	3. Review
Administrative Settings		
Administrator Password:	Password: <input type="password" value="••••••"/> <i>Must be 6 or more characters</i>	
	Confirm Password: <input type="password" value="••••••"/>	
Email system alerts to:	<input type="text" value="admin@example.com"/> <i>e.g. admin@company.com</i>	
Send Email via SMTP Relay Host (optional): ?	<input type="text" value=""/> <i>i.e., smtp.example.com, 10.0.0.3</i>	Port: ? <input type="text" value=""/> <i>optional</i>
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**.

[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 configuration interface. The top navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The 'Network' tab is active, and a dropdown menu is open, highlighting 'Authentication'. The main content area is titled 'System Status' and contains several sections: 'Web Security Appliance Status' (with 'System Uptime' showing 'Loading...'), 'Proxy Traffic Characteristics' (showing 'Loading...'), 'Proxy Capacity' (showing 'Loading ...'), and 'Current Configuration' (showing 'Loading ...'). A 'Printable (PDF)' link is visible in the top right of the 'System Status' section. The footer indicates the page was generated on 12 Oct 2014 at 21:13 (GMT -07:00).

Figure 2.11

Step 2: Click **Add Realm**.

Authentication

The screenshot shows the 'Authentication' configuration page. At the top, there is a section titled 'Authentication Realms' with an 'Add Realm...' button and the message 'No authentication realms have been defined.' Below this is the 'Global Authentication Settings' section, which is a table with the following rows:

Action if Authentication Service Unavailable:	Block all traffic if authentication fails
Failed Authentication Handling:	Log Guest User by: IP Address
Re-authentication:	Disabled
Basic Authentication Token TTL:	3600

Below the global settings is the 'Authentication Settings' section, also a table:

Credential Encryption:	Disabled
Redirect Hostname:	mgmt.wsaconn.stbulab.com
Credential Cache Options:	Surrogate Timeout: 3600 seconds Client IP Idle Timeout: 3600 seconds Cache Size: 8192 entries
User Session Restrictions:	Disabled

An 'Edit Global Settings...' button is located at the bottom right of the configuration area.

Figure 2.12

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

- Ream 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. The 'Realm Name' is set to 'STBULAB'. The 'Authentication Server Type and Scheme(s)' is set to 'Active Directory (Kerberos, NTLMSSP or Basic Authentication)'. The 'Active Directory Authentication' section is expanded, showing the following fields:

- Active Directory Server:** Specify up to three Active Directory servers:
 - 10.6.1.5
 - 10.6.1.4
 - hostname or IP address
- Active Directory Account:**
 - Active Directory Domain: ? stbulab.com
 - Computer Account ?
 - Location: Computers
(Example: Computers/BusinessUnit/Department/Servers)

A 'Join Domain...' button is located at the bottom right. The status at the bottom reads: '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.

Computer Account Credentials

Enter login credentials to create a computer account on your Active Directory server. These credentials are used once and will not be stored.

Username:

Password:

Do not include the domain name with the user name (for example, enter "johndoe" rather than "DOMAIN\johndoe" or "johndoe@domain").

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**.

Status: Computer account wsaconn\$ has been created.

Active Directory agent: Enable Transparent User Identification using Active Directory agent

Primary Active Directory agent:
 Server: Shared Secret:

Backup Active Directory agent (Optional):
 Server: Shared Secret:

(Host names or IP addresses) (specify the shared secret for each server)

Network Security: Client Signing Required

Test Current Settings

Test Authentication Realm Settings:

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'.

Test completed successfully.

Figure 2.15

Configure Identity Management

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

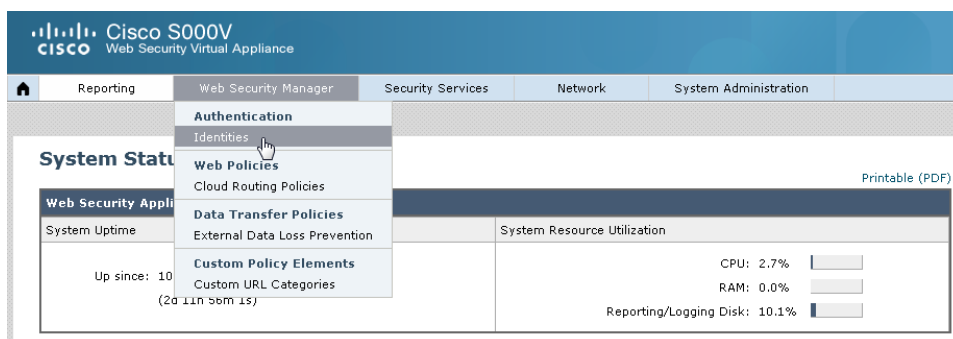


Figure 2.16

Step 2: Click **Add Identity**.

Identities

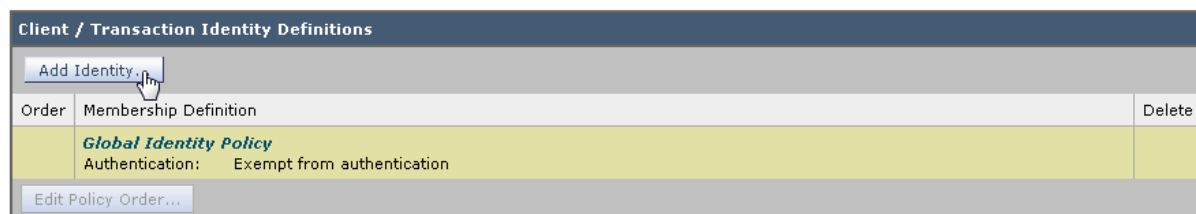


Figure 2.17

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: (e.g. my IT policy)

Description:

Insert Above: 1 (Global Policy) ▾

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:

(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

Identification and Authentication: Authenticate Users ▾

Select a Realm or Sequence: STBULAB ▾

Select a Scheme: Use NTLMSSP ▾
Scheme setting applies to HTTP/HTTPS only.

If a user fails authentication: Support Guest privileges ?

Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Cloud Routing Policies and External Data Loss Prevention).

Authentication Surrogates: ?

IP Address

Persistent Cookie

Session Cookie

Apply same surrogate settings to explicit forward requests

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.

▶ Advanced Define additional group membership criteria.

Cancel
Submit

Figure 2.18

Configure Directory Groups

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

Cisco S000V
Web Security Virtual Appliance

Reporting
Web Security Manager
Security Services
Network
System Administration

Identities

Client / Transaction Identity Definitions

Add Identity...

Order	Membership Definition	Delete
1	<p>CWS User Identity <small>?</small></p> <p>Authentication: Realm: STBULAB (Scheme: NTLMSSP) Surrogate Type: HTTP/HTTPS: IP Address</p>	
	<p>Global Identity Policy</p> <p>Authentication: Exempt from authentication</p>	

Edit Policy Order...

- Interfaces
- Transparent Redirection
- Routes
- DNS
- Internal SMTP Relay
- Authentication
- External DLP Servers
- Cloud Connector

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
Edit Settings...	

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	
<p>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.</p> <p>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.</p> <p>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.</p>	
<p>Realm: All Realms ▼</p> <p>Directory Search: <input type="text"/></p> <p>Directory search completed (69 matches).</p> <p>Realm: STBULAB</p> <ul style="list-style-type: none"> STBULAB\SM31000-0870AQDG0EA3 STBULAB\Account Operators 	<p>Add »</p> <p>Authorized Groups:</p> <p>Realm: STBULAB</p> <ul style="list-style-type: none"> 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 1OR)