Cisco Cloud Web Security

WSA Deployment Guide

October 2014

Contents

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.

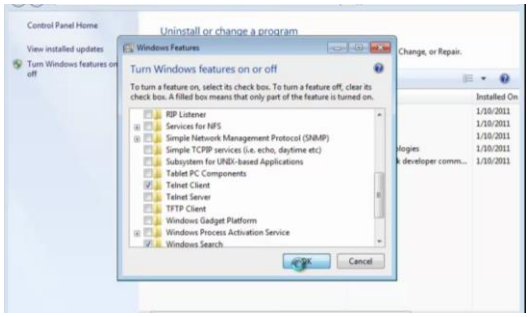

Figure 1.1

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.

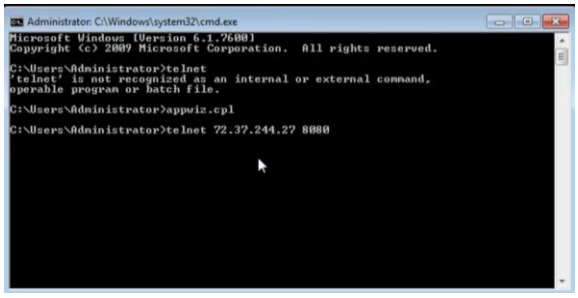

Figure 1.2

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.

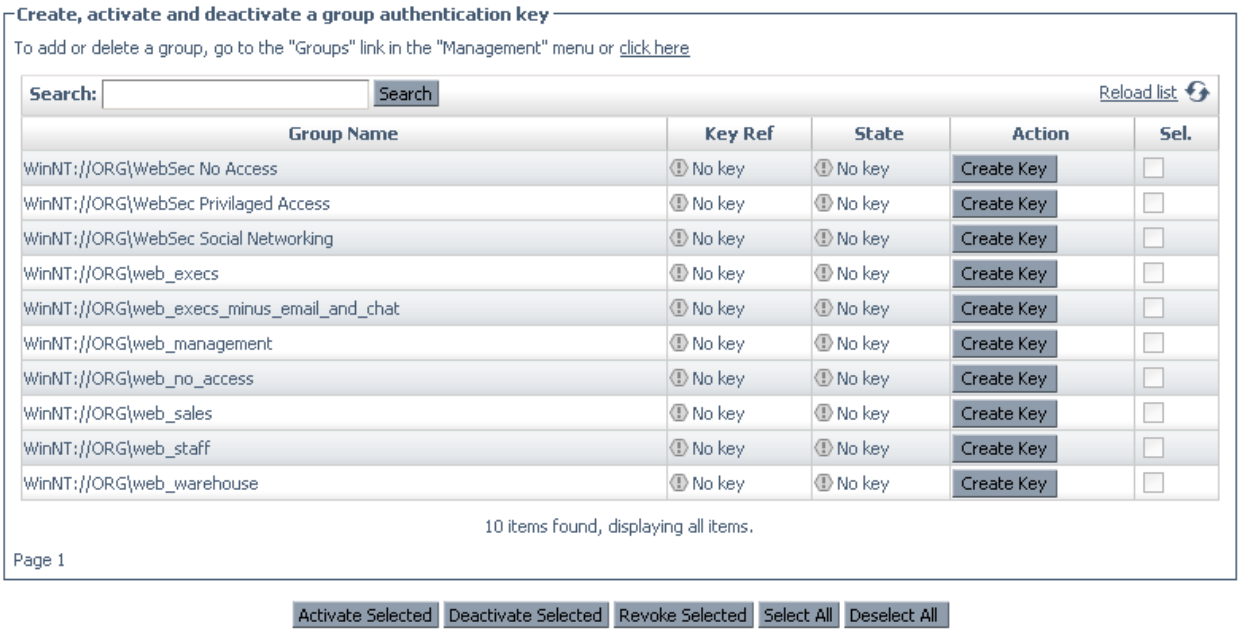

Figure 1.4

*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**

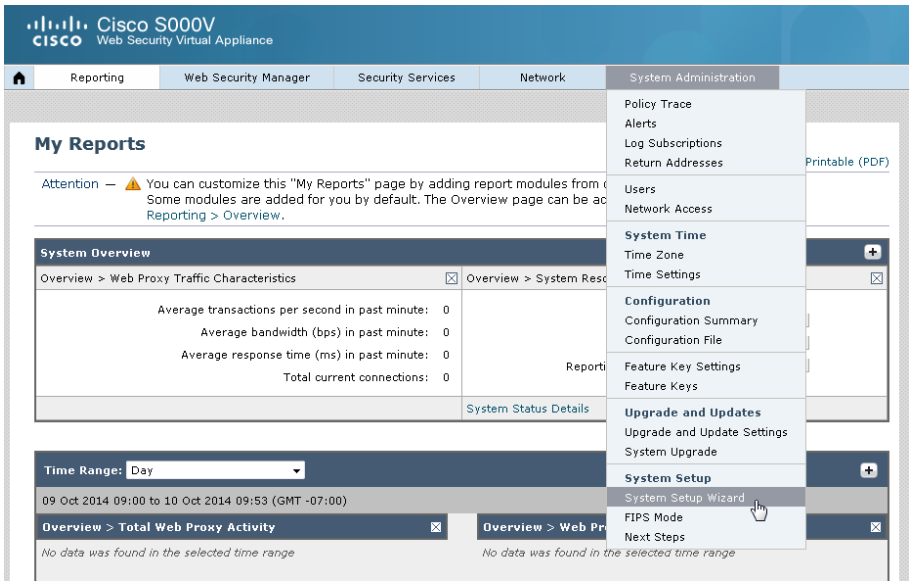

Figure 2.3

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**

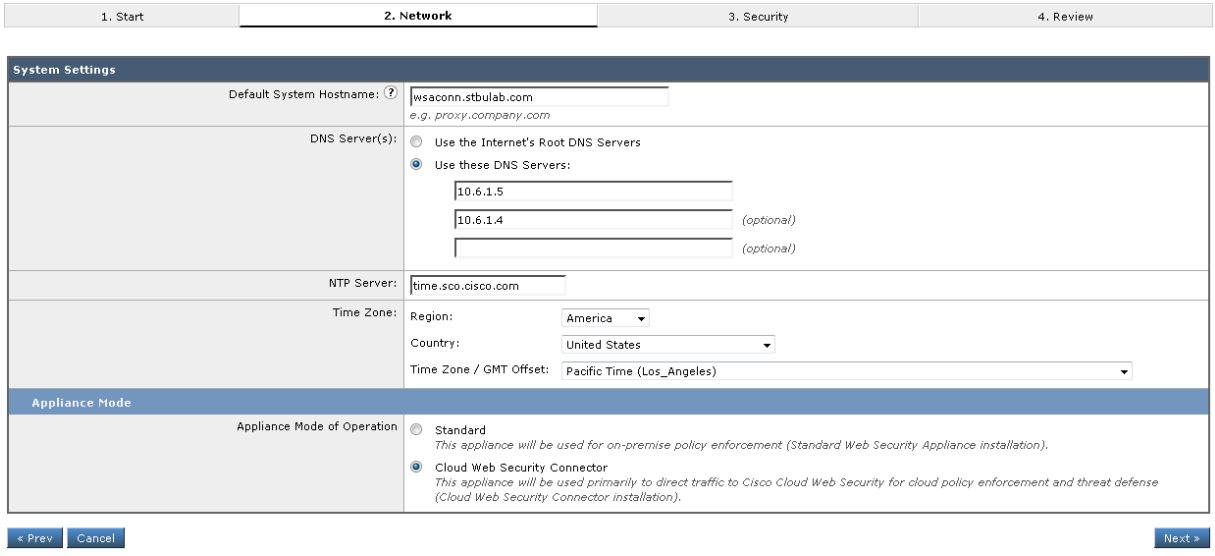

Figure 2.4

Step 4: **Define the Following:**

- Cloud Web Security Proxy Servers – supply the primary and secondary (backup) Cloud Web Security Proxy Server's host names of 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).

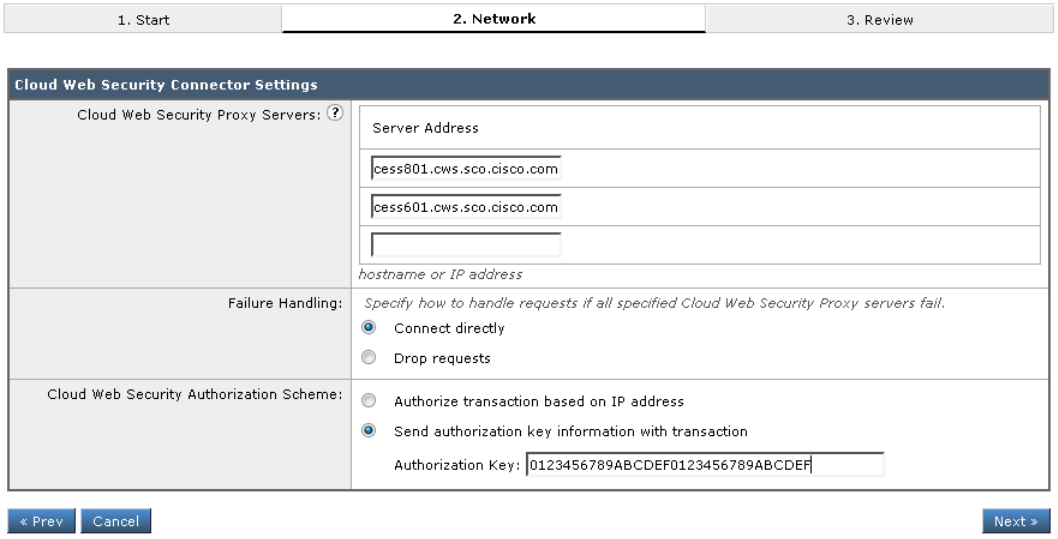

Figure 2.5

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

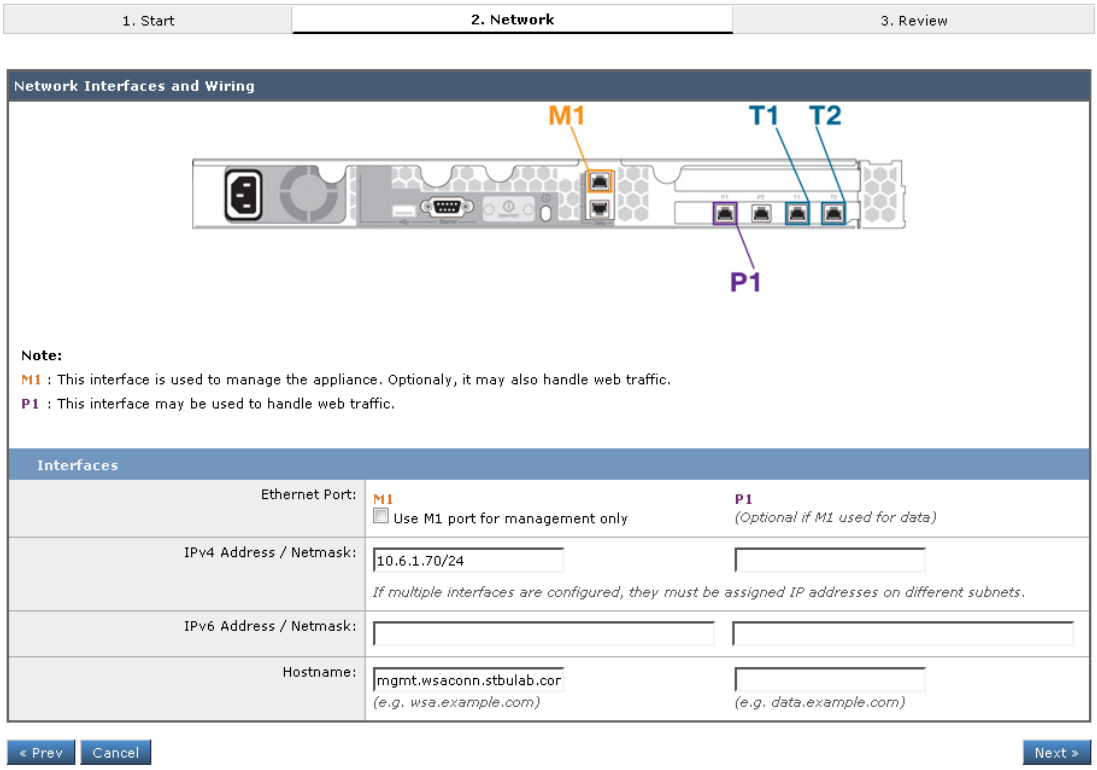

Figure 2.6

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

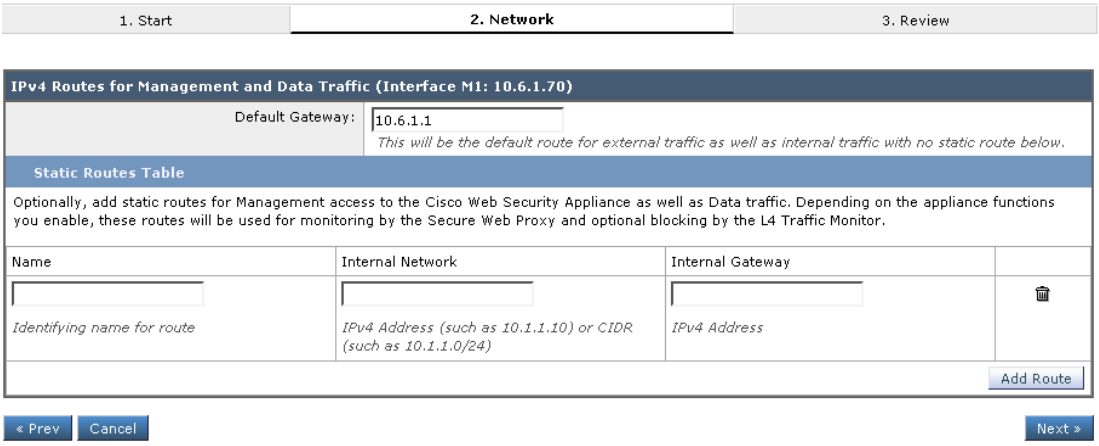

Figure 2.7

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*.

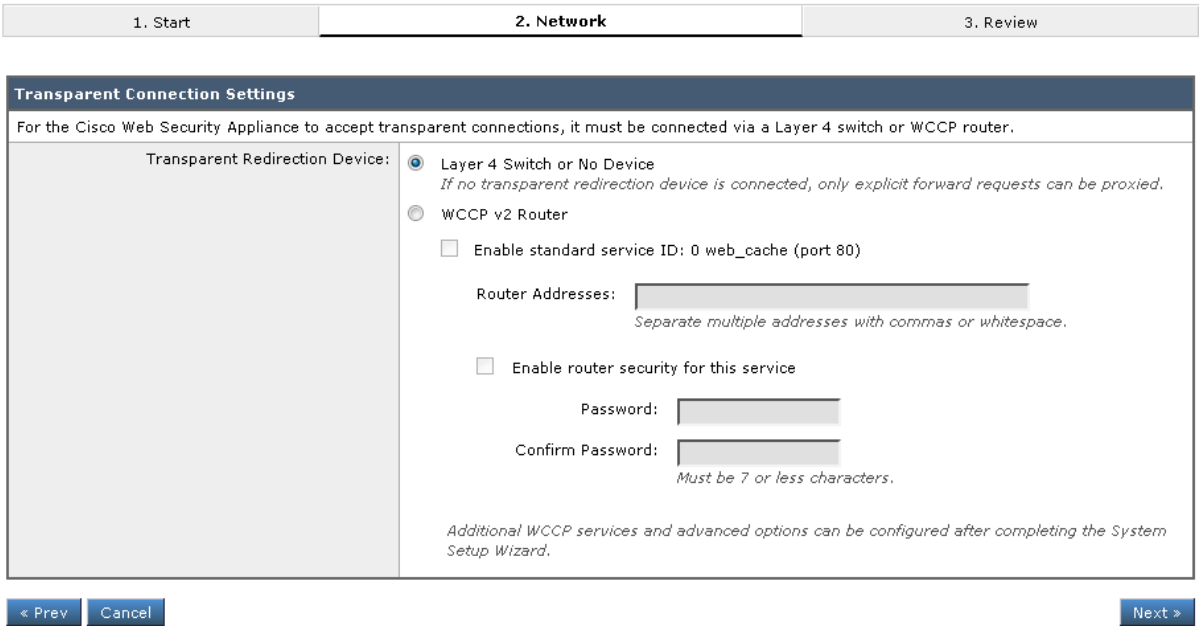

Figure 2.8

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

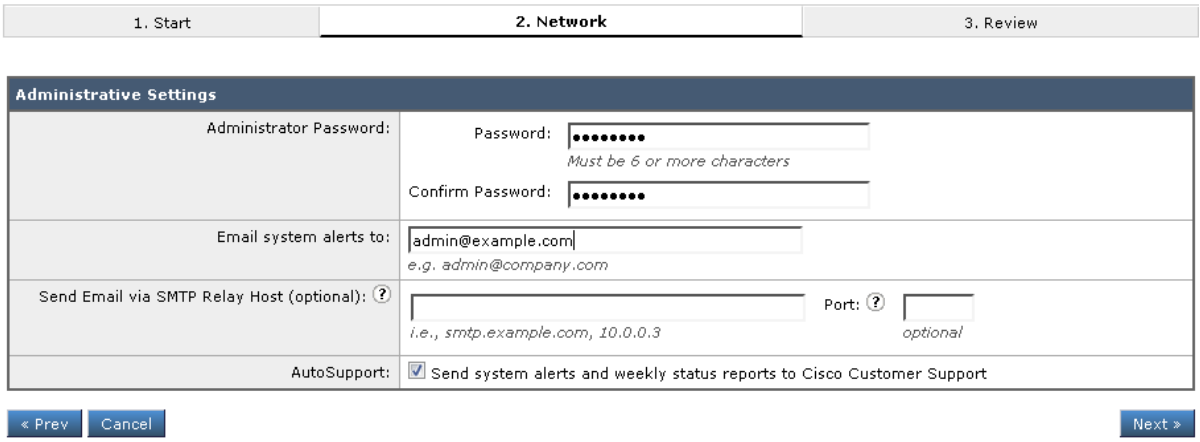

Figure 2.9

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**.

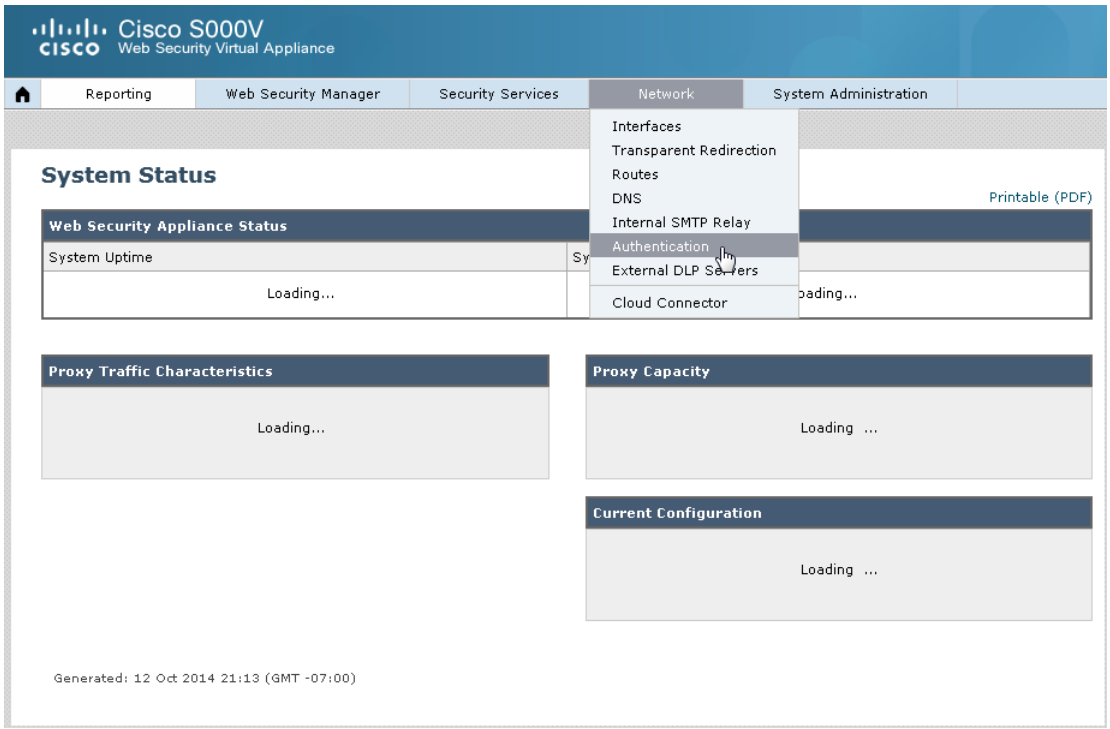

Figure 2.11

Step 2: Click **Add Realm**.

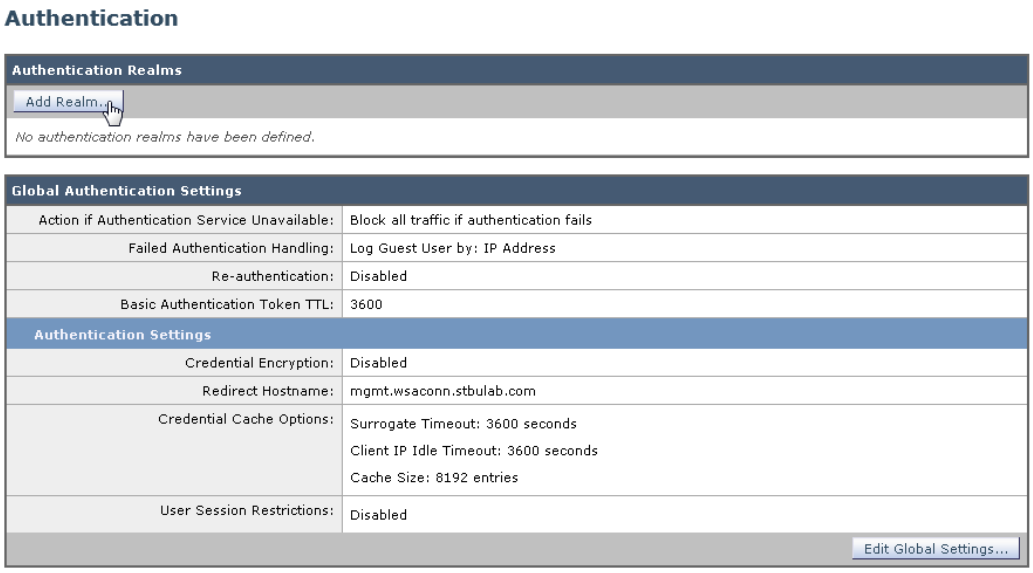

Figure 2.12

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.

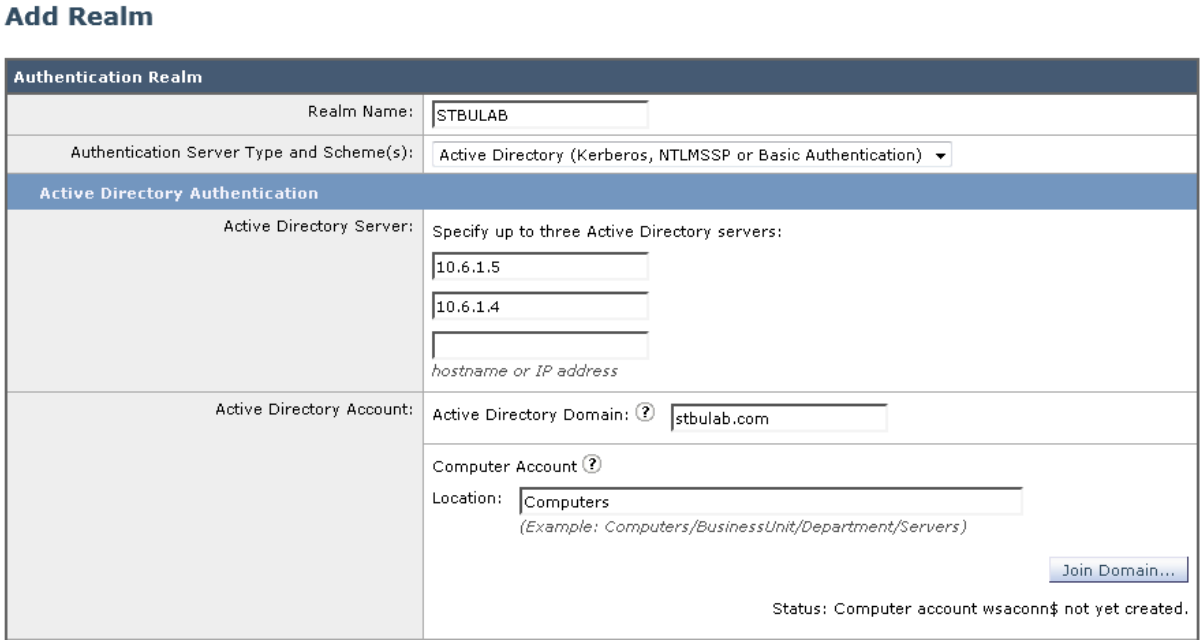

Figure 2.13

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.

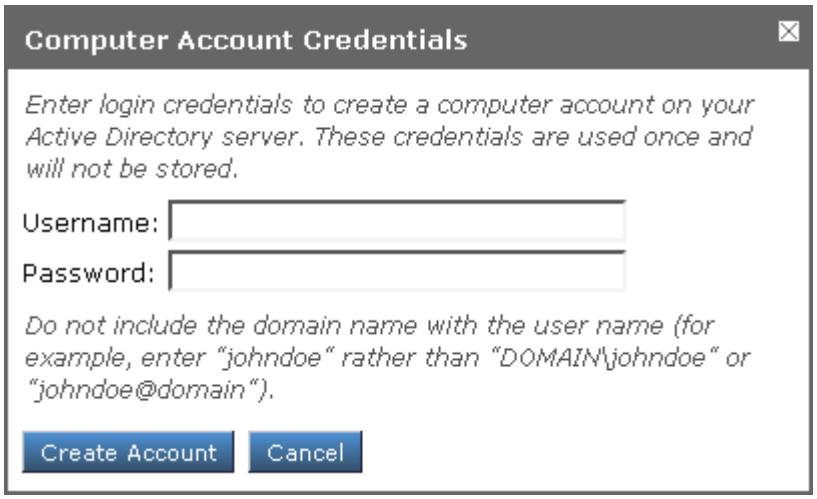

Figure 2.14

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**.

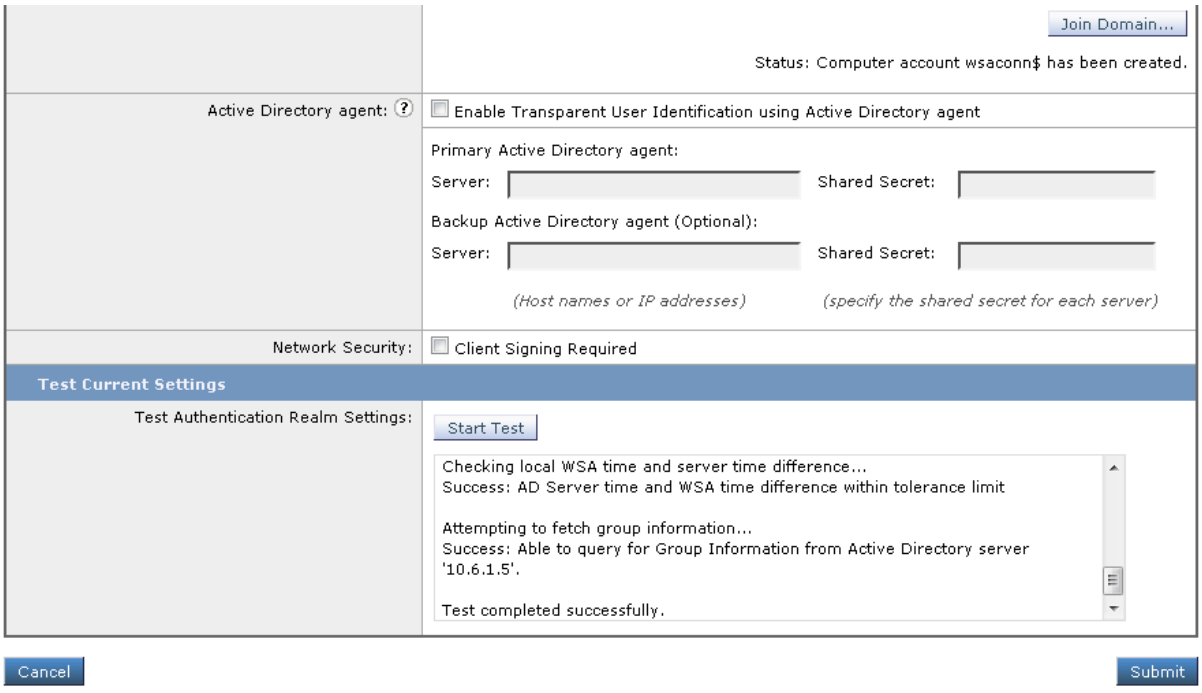

Figure 2.15

Configure Identity Management

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

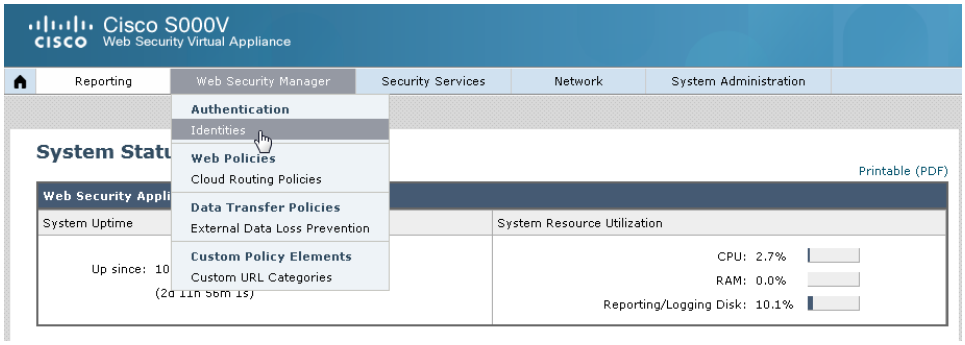

Figure 2.16

Step 2: Click **Add Identity**.

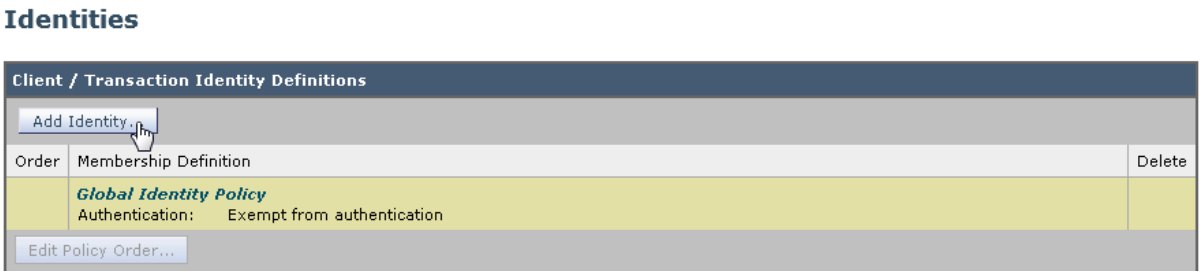

Figure 2.17

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.

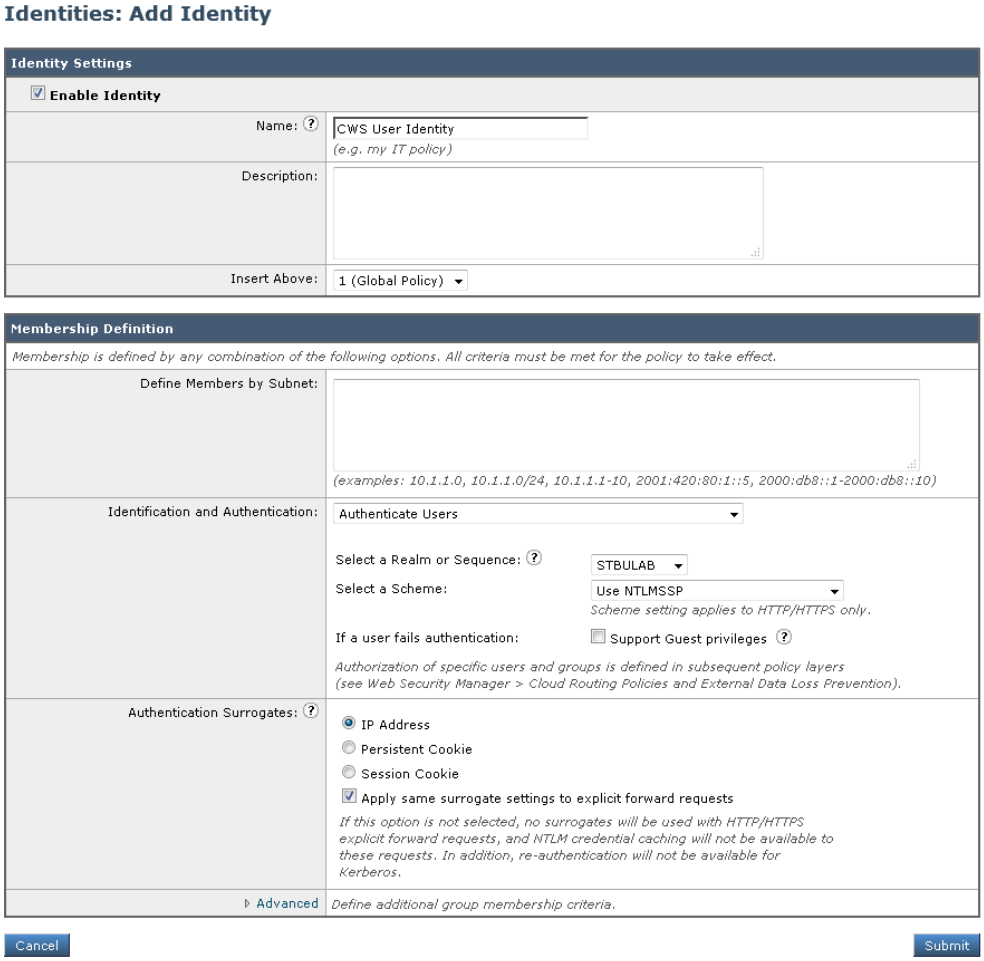

Figure 2.18

Configure Directory Groups

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

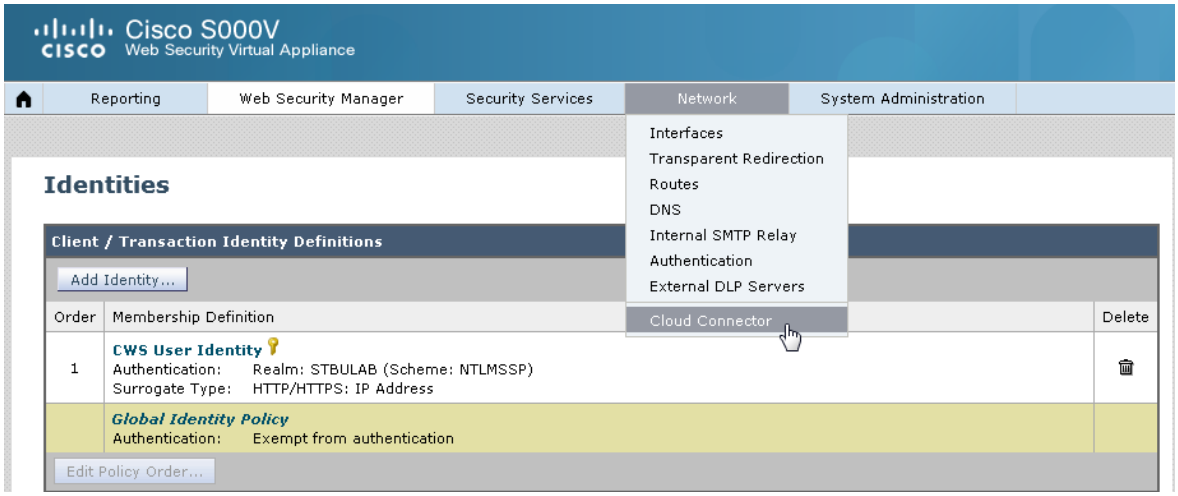

Figure 2.19

Step 2: Click **Edit Groups**.

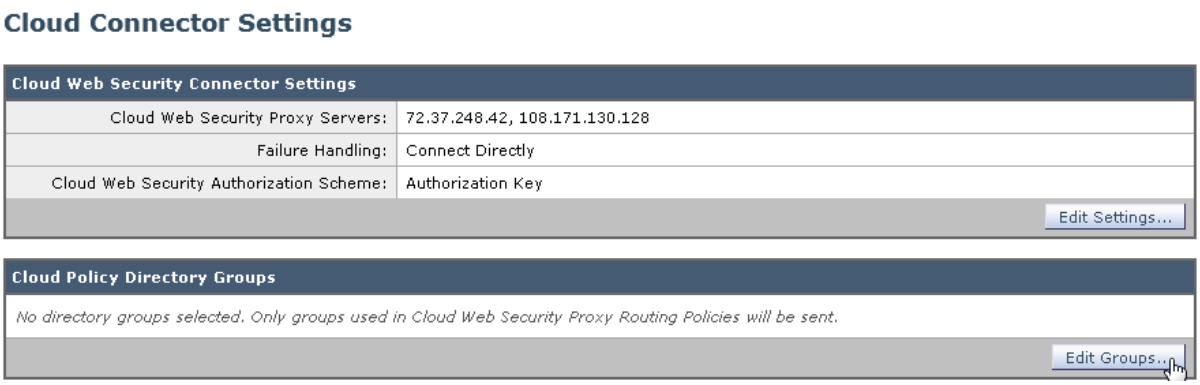

Figure 2.20

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**.

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.

Printed in USA C11-727200-00 04/13