Configure Secure Web Appliance Initial Setup

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Installing SWA

Initial Setup

- Configure IP Address
- Configure Default Gateway
- Import Traditional License
- Configure DNS Server
- Configure Smart License
- System Setup Wizard

Network Configuration

Routing Table

Related Information

Introduction

This document describes the steps required to configure the Secure Web Appliance (SWA) for the first time.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SWA administration.
- Fundamental networking principles.

Cisco recommends that you have:

- Physical or Virtual SWA Installed.
- Administrative Access to the SWA Graphical User Interface (GUI).
- Administrative Access to the SWA Command Line Interface (CLI).
- Administrative Access to the SWA Console.
- Valid SWA License or Access to Smart License Management portal (In case you are using Smart License).

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Installing SWA

The Cisco SWA is a forward proxy solution designed to enhance web security and control for organizations. Available in both virtual and physical forms, the SWA provides flexible deployment options to meet diverse needs. The virtual SWA supports several hypervisor platforms, including Microsoft Hyper-V, VMware ESX and KVM, ensuring compatibility with a range of virtual environments. For those who prefer a physical appliance, Cisco offers three distinct models: S100, S300 and S600. Each model is designed to cater to different levels of performance and capacity requirements, ensuring that organizations can find the right fit for their specific web security needs.

To download your virtual machine image you can visit: https://software.cisco.com/download/home .

Installing the virtual Cisco SWA is a straightforward process that begins with selecting the appropriate hypervisor platform. First, download the virtual SWA installation file from the Cisco website. For VMware ESX, deploy the OVA file, ensuring you configure the network settings and allocate sufficient resources such as CPU, memory, and storage. For Microsoft Hyper-V, import the downloaded VHD file into the Hyper-V Manager, and configure the virtual machine settings accordingly. For KVM, use the **virt-manager** or **virsh** command-line tool to define and start the virtual machine using the downloaded image. Once the virtual machine is up and running, you can use steps in this article to do the initial setup.

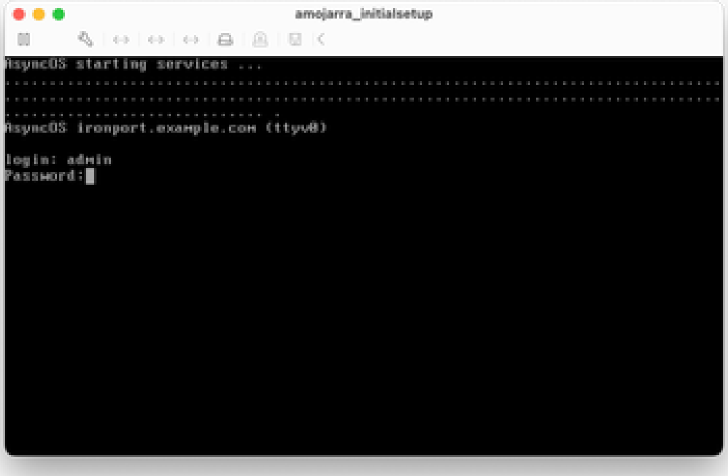
Initial Setup

After installing the SWA, Proceed with these steps for initial deployment.

Note: For the initial setup, you need to have access to SWA via Console, SSH and GUI.

Connection Method	Stage	Configuration Steps
Console	**Configure IP Address**	**Step 1.** Enter the Username and Password to log in to the CLI.

Tip: The default Username is **admin** and the default Password is **ironport**.



```
AsyncOS starting services ...
................................................................................
................................................................................
................................. .
AsyncOS ironport.example.com (ttyv0)

login: admin
Password:█
```

Image - login Screen

Step 2. Run **ifconfig**.

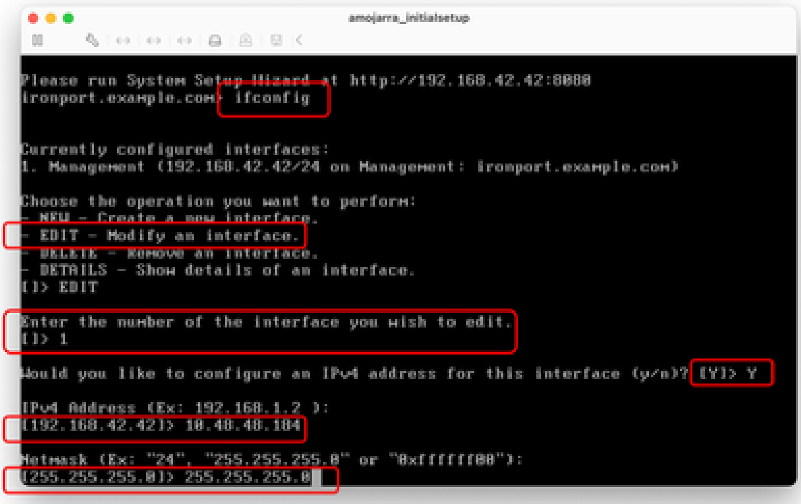
Step 3. Choose **Edit**.

Step 4. Enter the number associated with your **Management Interface**.

Step 5. Select **Y** to edit the default IPv4 Address.

Step 6. Enter the **IP** address

Step 7. Enter the **Subnet Mask**.



```
Please run System Setup Wizard at http://192.168.42.42:8080
ironport.example.com> ifconfig

Currently configured interfaces:
1. Management (192.168.42.42/24 on Management: ironport.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]> EDIT

Enter the number of the interface you wish to edit.
[]> 1

Would you like to configure an IPv4 address for this interface (y/n)? [Y]> Y

IPv4 Address (Ex: 192.168.1.2 ):
[192.168.42.42]> 10.48.48.184

Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 255.255.255.0
```

Image - Edit Management Interface IP address

Step 8. If you would like to configure IPv6, type **Y** in answer to the question "Would you like to Configure IPv6?", else you can leave this as default (**No**) and press Enter.

Step 9. Enter a fully qualified domain name (FQDN) as the **host name**.

Step 10. If you would like to enable the File Transfer Protocol (**FTP**) Access to the Management Interface, Choose **Y**, or else press **Enter**.

Step 11. The Secure Shell (SSH) is set to Enabled by default. it is advised to have the SSH enabled. Type **Y** to continue.

Step 12. (Optional) You can change the default SSH port from TCP 22 to any port number you would like as long as there are no port conflicts else, press enter to use the default port (TCP/22).

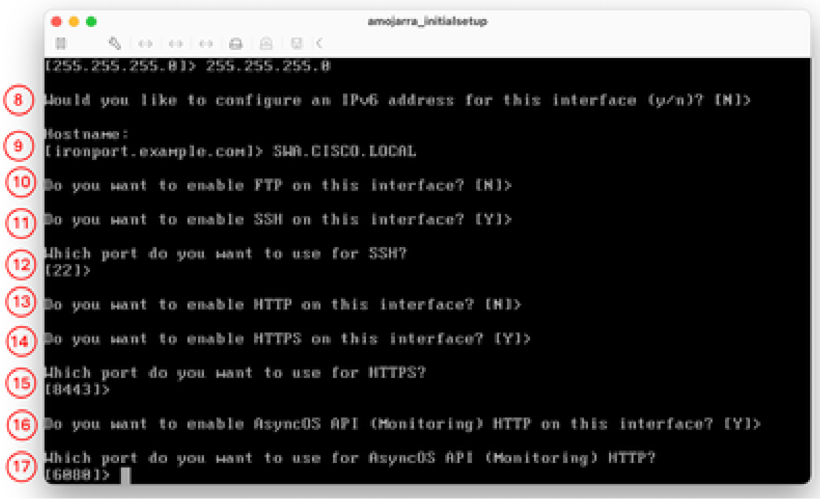
Step 13. If you would like to have Hypertext Transfer Protocol (HTTP) access to the Management Interface, type **Y** and set the Port number for HTTP access. Otherwise, you can choose **N** to only have Hypertext Transfer Protocol Secure (HTTPS) access to the management Interface.

Step 14. Type **Y** and press Enter to enable HTTPS access to the Managment Interface.

Step 15. You can change the default HTTPS port number from 8443 to any port number you would like as long as there are no port conflicts else, press enter to use the default port (TCP/8443).

Step 16. Application Programming Interface (API) by default is set to Enable, if you are not using API you can disable the API by typing **N** and press **Enter**.

Step 17. If you choose to have the API enabled, you can change the default API port number from 6080 to any port number you would like as long as there are no port conflicts else, press enter to use the default port (TCP/6080).



```
[255.255.255.0]> 255.255.255.0

Would you like to configure an IPv6 address for this interface (y/n)? [N]>

Hostname:
[ironport.example.com]> SWA.CISCO.LOCAL

Do you want to enable FTP on this interface? [N]>

Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?
[22]>

Do you want to enable HTTP on this interface? [N]>

Do you want to enable HTTPS on this interface? [Y]>

Which port do you want to use for HTTPS?
[8443]>

Do you want to enable AsyncOS API (Monitoring) HTTP on this interface? [Y]>

Which port do you want to use for AsyncOS API (Monitoring) HTTP?
[6080]>
```

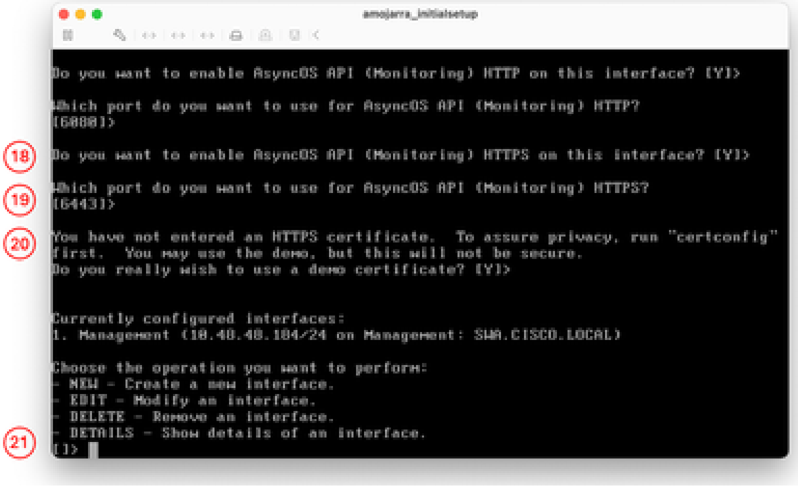
Image - Management Interface Service Configuration

Step 18. AsyncOS API (monitoring) is the new GUI on the SWA, if you would like to use the new user interface reports, set this option to **Y** (Default), Else you can type **N** and skip to Step 20

Step 19. You can change the default New GUI HTTPS port number from 6443 to any port number you would like as long as there are no port conflicts else, press enter to use the default port (TCP/6443).

Step 20. SWA Management Interface uses Cisco Demo Certificate. Type **Y** to accept the Demo certificate. you can change the GUI certificate after the initial setup.

Step 21. Press **Enter** to exit the **ifconfig** wizard.



```
Do you want to enable AsyncOS API (Monitoring) HTTP on this interface? [Y]>

Which port do you want to use for AsyncOS API (Monitoring) HTTP?
[6080]>

Do you want to enable AsyncOS API (Monitoring) HTTPS on this interface? [Y]>

Which port do you want to use for AsyncOS API (Monitoring) HTTPS?
[6443]>

You have not entered an HTTPS certificate.  To assure privacy, run "certconfig"
first.  You may use the demo, but this will not be secure.
Do you really wish to use a demo certificate? [Y]>


Currently configured interfaces:
1. Management (10.48.48.184/24 on Management: SWA.CISCO.LOCAL)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]>
```

Image - New GUI TCP Configuration

<table>
<tr>
<td></td>
<td><strong>Configure Default Gateway</strong></td>
<td>

Step 22. Run **setgateway**.

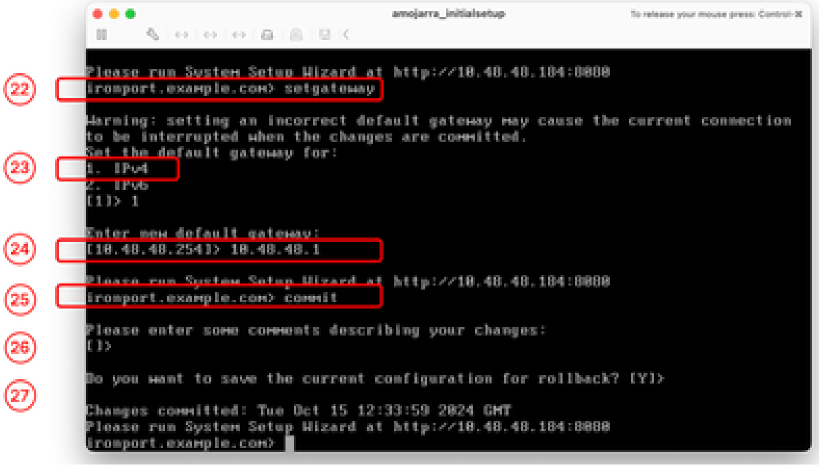
Step 23. Choose the IPv4 if your Management Interface has been configured with IPv4, else choose IPv6.

Step 24. Enter your default gateway IP address.

Step 25. Save the changes by running **commit**.

Step 26. (Optional) you can add Notes about the changes you are saving

Step 27. (Optional) you can have SWA to back up the configuration before applying the changes.



```
Please run System Setup Wizard at http://10.48.48.184:8080
ironport.example.com> setgateway

Warning: setting an incorrect default gateway may cause the current connection
to be interrupted when the changes are committed.
Set the default gateway for:
1. IPv4
2. IPv6
[1]> 1

Enter new default gateway:
[10.48.48.254]> 10.48.48.1

Please run System Setup Wizard at http://10.48.48.184:8080
ironport.example.com> commit

Please enter some comments describing your changes:
[]>

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Tue Oct 15 12:33:59 2024 GMT
Please run System Setup Wizard at http://10.48.48.184:8080
ironport.example.com>
```

Image - Configuring the Default Gateway

</td>
</tr>
<tr>
<td><strong>SSH</strong></td>
<td><strong>Import Traditional License</strong></td>
<td>

Note: If you are using Smart License skip to Step 36.

</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>

Step 28. Connect to SWA via **SSH**.

Step 29. Run **loadlicense**

Step 30. Choose **Paste via CLI.**

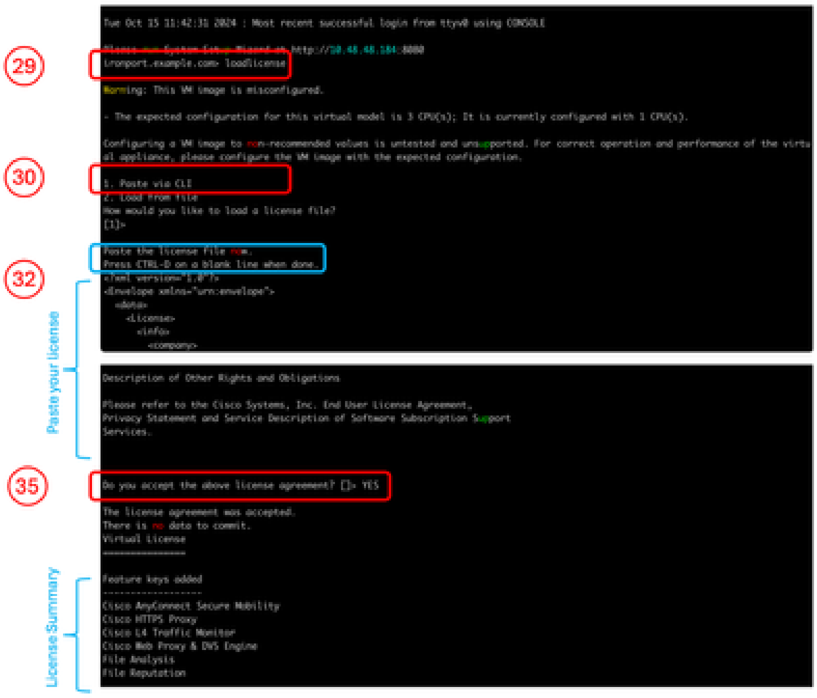
Step 31. Open your license file with a text editor. and copy all its content

Step 32. Paste the license in the SSH shell.

Step 33. Press **Enter** to navigate to a new line.

Step 34. Hold **Control** and press **D**.

Step 35. Read the License agreement and type **YES** to agree with the conditions.



```
Tue Oct 15 11:42:31 2024 : Most recent successful login from ttyv0 using CONSOLE

Please run System Setup Wizard at http://10.48.48.184:8080
ironport.example.com> loadlicense

Warning: This VM image is misconfigured.

- The expected configuration for this virtual model is 3 CPU(s); It is currently configured with 1 CPU(s).

Configuring a VM image to non-recommended values is untested and unsupported. For correct operation and performance of the virtu
al appliance, please configure the VM image with the expected configuration.

1. Paste via CLI
2. Load from file
How would you like to load a license file?
[1]>

Paste the license file now.
Press CTRL-D on a blank line when done.
<?xml version="1.0"?>
<Envelope xmlns="urn:envelope">
  <data>
    <License>
      <info>
        <company>
```

```
Description of Other Rights and Obligations

Please refer to the Cisco Systems, Inc. End User License Agreement,
Privacy Statement and Service Description of Software Subscription Support
Services.


Do you accept the above license agreement? []> YES

The license agreement was accepted.
There is no data to commit.
Virtual License
===============

Feature keys added
------------------
Cisco AnyConnect Secure Mobility
Cisco HTTPS Proxy
Cisco L4 Traffic Monitor
Cisco Web Proxy & DVS Engine
File Analysis
File Reputation
```

Image - Import Traditional License

Skip to Step 58.

</td>
</tr>
<tr>
<td>

GUI

</td>
<td>

Configure DNS Server

</td>
<td>

Step 37. Log in to the GUI (the default is HTTPS://<**SWA FQDN or IP Address**>:8443)

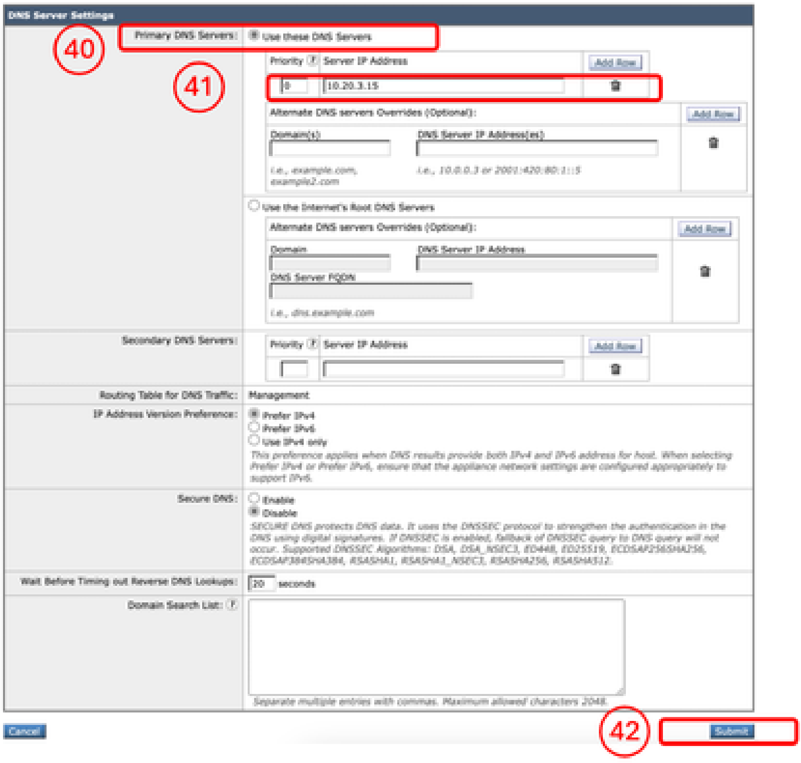
Step 38. Navigate to **Network** and choose **DNS**.

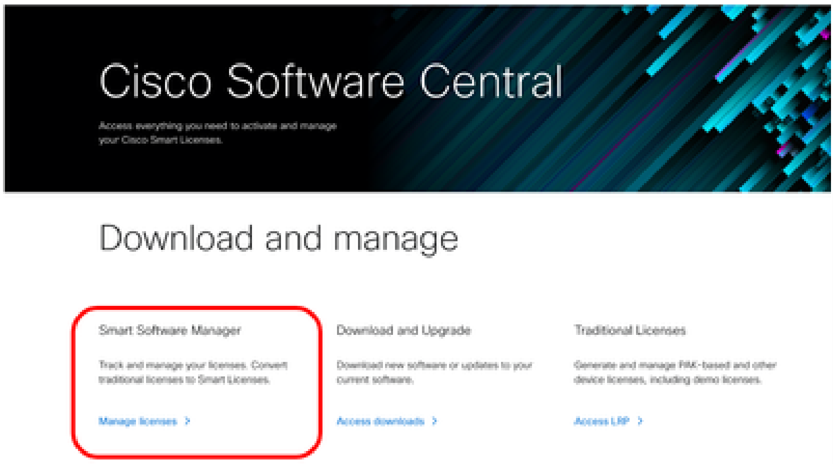
Step 39. Click **Edit Settings**.

Step 40. in the **Primary DNS Servers** section, select **Use these DNS Servers.**

Step 41. Set the Priority to 0 and enter your **DNS** server IP address.

</td>
</tr>
</table>

		Note: You can add more than one DNS server by choosing **Add Row**. **Step 42. Submit**. **Step 43. Commit** the changes.  DNS Server Settings Primary DNS Servers: ● Use these DNS Servers Priority: 0 Server IP Address: 10.20.3.15 Alternate DNS servers Overrides (Optional): Domain(s): DNS Server IP Address(es): i.e., example.com, example2.com i.e., 10.0.0.3 or 2001:420:80:1::5 ○ Use the Internet's Root DNS Servers Alternate DNS servers Overrides (Optional): Domain DNS Server IP Address DNS Server FQDN i.e., dns.example.com Secondary DNS Servers: Priority Server IP Address Routing Table for DNS Traffic: Management IP Address Version Preference: ● Prefer IPv4 ○ Prefer IPv6 ○ Use IPv4 only *This preference applies when DNS results provide both IPv4 and IPv6 address for host. When selecting Prefer IPv4 or Prefer IPv6, ensure that the appliance network settings are configured appropriately to support IPv6.* Secure DNS: ○ Enable ● Disable *SECURE DNS protects DNS data. It uses the DNSSEC protocol to strengthen the authentication in the DNS using digital signatures. If DNSSEC is enabled, fallback of DNSSEC query to DNS query will not occur. Supported DNSSEC Algorithms: DSA, DSA_NSEC3, ED448, ED25519, ECDSAP256SHA256, ECDSAP384SHA384, RSASHA1, RSASHA1_NSEC3, RSASHA256, RSASHA512.* Wait Before Timing out Reverse DNS Lookups: 20 seconds Domain Search List: *Separate multiple entries with commas. Maximum allowed characters 2048.* *Image - Configure DNS Server*
	Configure Smart	**Step 44.** In the GUI from **System Administration**, choose

	License	**Smart Software Licensing**. **Step 45.** Choose **EnableSmart Software Licensing**. ⚠ **Caution**: You cannot roll back from Smart License to Classic License, after you enable Smart License feature on your appliance. **Step 46.** Click **OK** to continue configuring Smart License. **Step 47. Commit** the changes. **Step 48.** To obtain the token to register your SWA, Log in to **Cisco Software Central** (https://software.cisco.com/#) **Step 49.** Click **Manage Licenses**.  Cisco Software Central Access everything you need to activate and manage your Cisco Smart Licenses. Download and manage Smart Software Manager Track and manage your licenses. Convert traditional licenses to Smart Licenses. Manage licenses › Download and Upgrade Download new software or updates to your current software. Access downloads › Traditional Licenses Generate and manage PAK-based and other device licenses, including demo licenses. Access LRP › *Image - Cisco Smart License Management* **Step 50.** In **Smart Software Licensing** choose **Inventory**.

Step 51. In the **General** Tab Create a **New Token** or use your available Tokens.

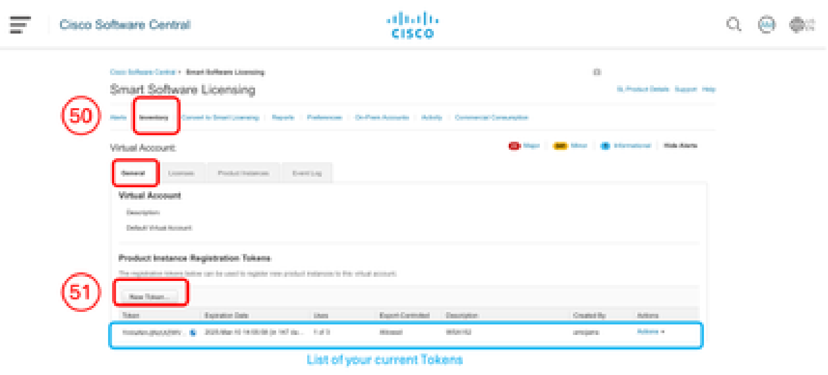
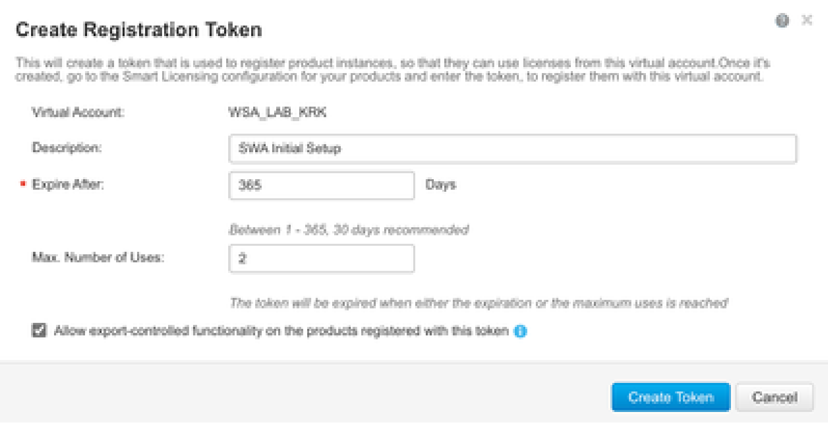


Image - Smart Software License Inventory Page

Step 52. Enter the required information and **Create Token**.



Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account.Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account: WSA_LAB_KRK

Description: SWA Initial Setup

* Expire After: 365 Days

Between 1 - 365, 30 days recommended

Max. Number of Uses: 2

The token will be expired when either the expiration or the maximum uses is reached

☑ Allow export-controlled functionality on the products registered with this token

Create Token | Cancel

Image - Generating a Token

Step 53. Click On the **Blue Icon** in front of the newly added token and copy its content.

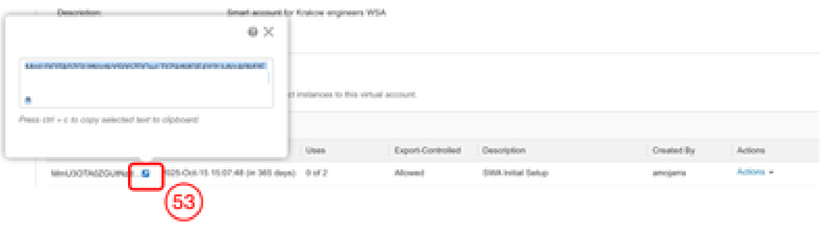


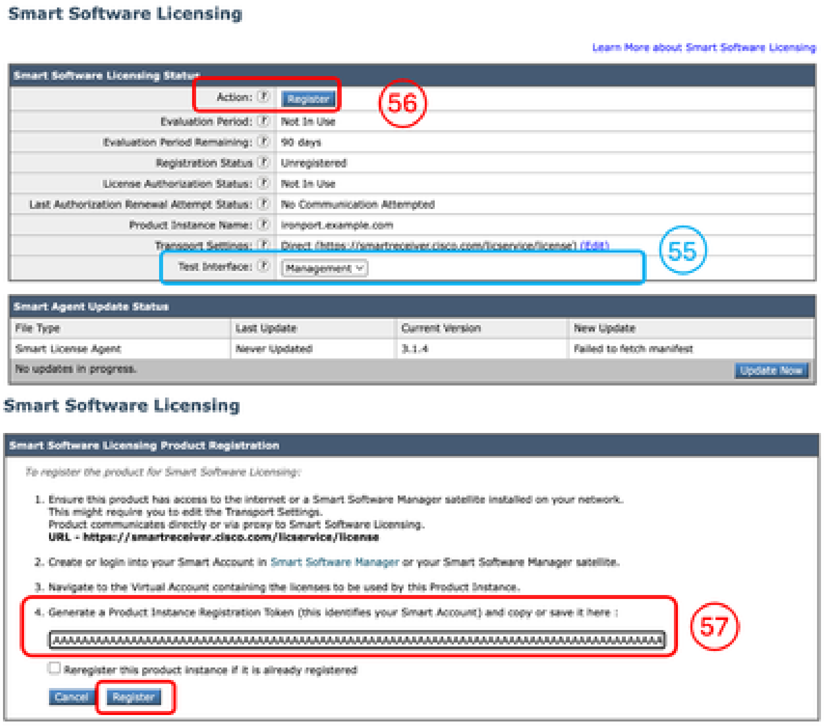
Image - Copy the Token

Step 54. In the SWA GUI navigate to **System Administration** and choose **Smart Software Licensing**.

		Note: If you are already on the **Smart Software Licensing** page, please refresh the page.
		Step 55. (Optional) If the SWA has no Internet access from the Management Interface, you can change the Test Interface to the Interfaces that are allowed to access the Internet.
		Tip: For more Information about multiple Interface configuration and routing tables, please check the Network Configuration section in this article.

Step 56. Click **Register**.

Step 57. Paste the **Token** and click **Register**.



Smart Software Licensing

Learn More about Smart Software Licensing

Smart Software Licensing Status	
Action:	Register
Evaluation Period:	Not In Use
Evaluation Period Remaining:	90 days
Registration Status	Unregistered
License Authorization Status:	Not In Use
Last Authorization Renewal Attempt Status:	No Communication Attempted
Product Instance Name:	ironport.example.com
Transport Settings:	Direct (https://smartreceiver.cisco.com/licservice/license) (Edit)
Test Interface:	Management

Smart Agent Update Status

File Type	Last Update	Current Version	New Update
Smart License Agent	Never Updated	3.1.4	Failed to fetch manifest

No updates in progress.

Smart Software Licensing

Smart Software Licensing Product Registration

To register the product for Smart Software Licensing:

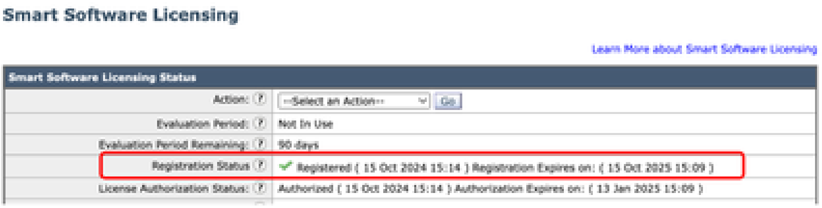
1. Ensure this product has access to the internet or a Smart Software Manager satellite installed on your network.
   This might require you to edit the Transport Settings.
   Product communicates directly or via proxy to Smart Software Licensing.
   URL - https://smartreceiver.cisco.com/licservice/license
2. Create or login into your Smart Account in Smart Software Manager or your Smart Software Manager satellite.
3. Navigate to the Virtual Account containing the licenses to be used by this Product Instance.
4. Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it here :

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

□ Reregister this product instance if it is already registered

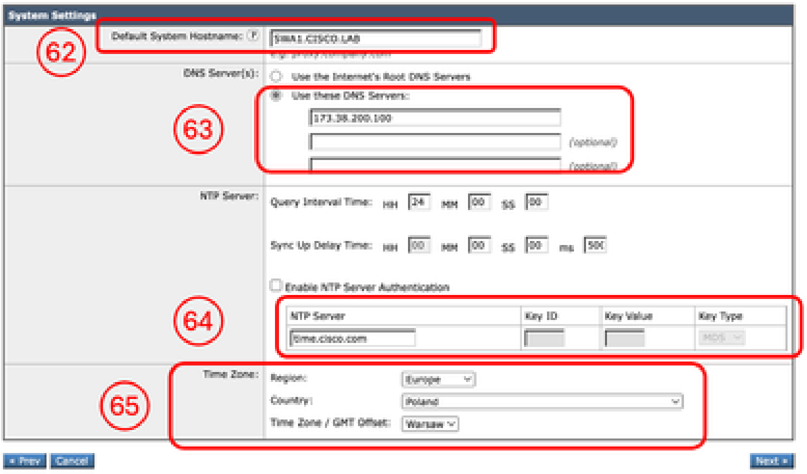
Image - Register SWA to Smart License

Note: To verify your registration, wait for a couple of minutes, refresh the Smart Licensing page in SWA, and check the **Registration Status.**

		 Smart Software Licensing Learn More about Smart Software Licensing Smart Software Licensing Status Action: --Select an Action-- Go Evaluation Period: Not In Use Evaluation Period Remaining: 90 days Registration Status: ✓ Registered (15 Oct 2024 15:14) Registration Expires on: (15 Oct 2025 15:09) License Authorization Status: Authorized (15 Oct 2024 15:14) Authorization Expires on: (13 Jan 2025 15:09) *Image - Smart License Registration Status*
	System Setup Wizard	**Step 58.** In the SWA GUI navigate to **System Administration** and choose **System Setup Wizard**. **Step 59.** Read and **accept** the terms of this license agreement **Step 60.** Click **Begin Setup**. **Step 61.** Choose **Standard** from the **Appliance Mode of Operation** section. **Step 62**. Enter the **Default System Hostname**. **Note**: Previous hostname that was created in **Step 9** was related to the Management Interface and not the SWA. **Step 63.** Enter the **DNS Server(s)** IP address. **Step 64.** you can configure your Network Time Protocol (**NTP**) Server.

Tip: If your NTP Server Requires Authentication, you can configure the Key parameters.

Step 65. Select the **Time Zone** that applies to the SWA and Click **Next**.



System Settings

Default System Hostname: SWA1.CISCO.LAB

DNS Server(s):
○ Use the Internet's Root DNS Servers
● Use these DNS Servers:
173.38.200.100
(optional)
(optional)

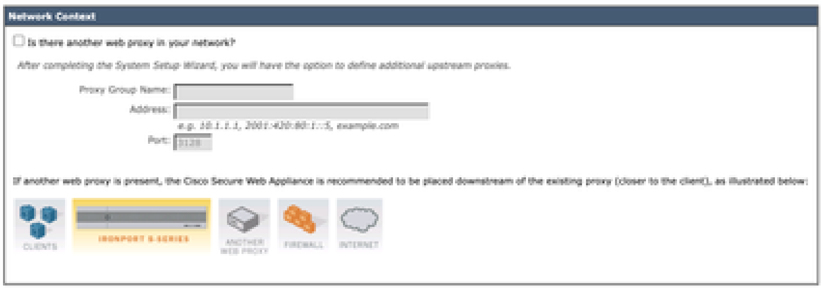
NTP Server:
Query Interval Time: HH 24 MM 00 SS 00
Sync Up Delay Time: HH 00 MM 00 SS 00 ms 500
□ Enable NTP Server Authentication

NTP Server	Key ID	Key Value	Key Type
time.cisco.com			MD5

Time Zone:
Region: Europe
Country: Poland
Time Zone / GMT Offset: Warsaw

Image - System Setup Wizard - System Settings

Step 66. (Optional) If you are using any upstream Proxy in your network, you can configure it on the **Network Context** page or else leave it as default and click **Next**.



Network Context

□ Is there another web proxy in your network?

After completing the System Setup Wizard, you will have the option to define additional upstream proxies.

Proxy Group Name:

Address:

e.g. 10.1.1.1, 2001:420:80:1::5, example.com

Port: 3128

If another web proxy is present, the Cisco Secure Web Appliance is recommended to be placed downstream of the existing proxy (closer to the client), as illustrated below:

Image - System Setup Wizard - Upstream Proxy Configuration

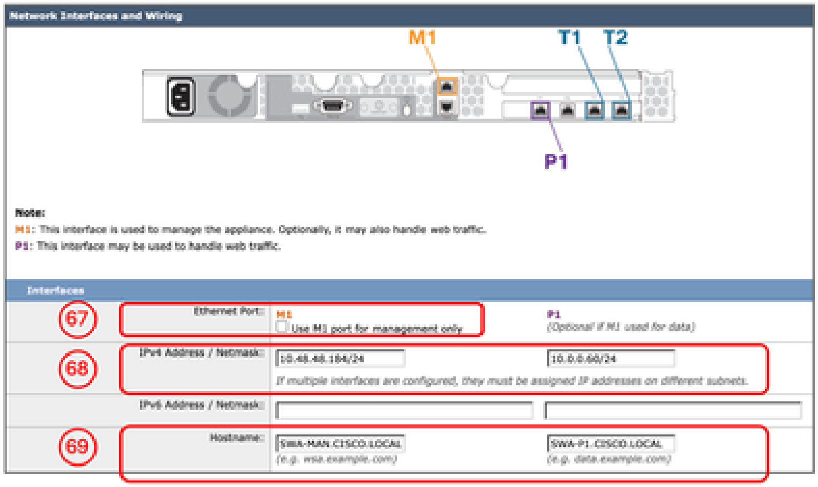
Step 67. (Optional) In case you need to separate the Management INterface Traffic from the Data Interfaces (P1 and P2 Interfaces) Traffic, Select **Use M1 port for management only**.

Step 68. (Optional) You can add or modify the Network Interfaces IP address from **IPv4 Address / Netmask** or **IPv6 Address / Netmask** section.

Step 69. (Optional) You can add or modify the Network Interfaces **Hostname** and click **Next**.

Note: The P1 port can be enabled and configured through the System Setup Wizard. If you wish to enable the P2 interface, this must be done after completing the System Setup Wizard.

<table>
<tr>
<td></td>
<td></td>
<td>



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 □ Use M1 port for management only | P1 (Optional if M1 used for data)

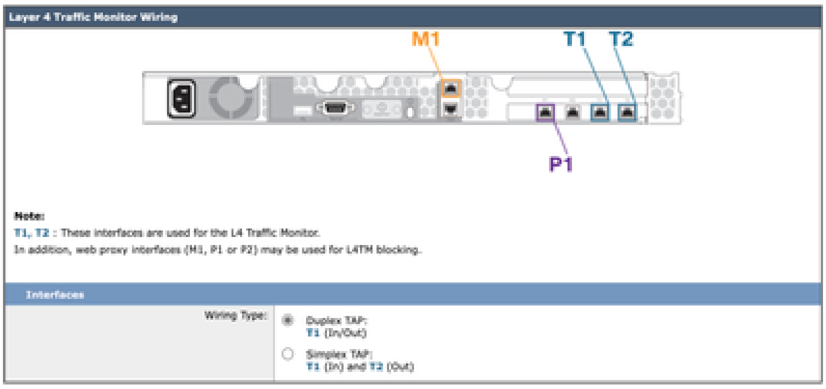
IPv4 Address / Netmask: 10.48.48.184/24 | 10.0.0.60/24
If multiple interfaces are configured, they must be assigned IP addresses on different subnets.

IPv6 Address / Netmask:

Hostname: SWA-MAN.CISCO.LOCAL (e.g. wsa.example.com) | SWA-P1.CISCO.LOCAL (e.g. data.example.com)

Image - System Setup Wizard - Network Interfaces Configuration

Step 70. (Optional) In case you are planing to configure Layer 4 Traffic Monitor (L4TM) you can configure the **Duplex** setting, or else you can leave as default and click **Next**.



Layer 4 Traffic Monitor Wiring

Note:
T1, T2 : These interfaces are used for the L4 Traffic Monitor.
In addition, web proxy interfaces (M1, P1 or P2) may be used for L4TM blocking.

Interfaces

Wiring Type:
● Duplex TAP: T1 (In/Out)
○ Simplex TAP: T1 (In) and T2 (Out)

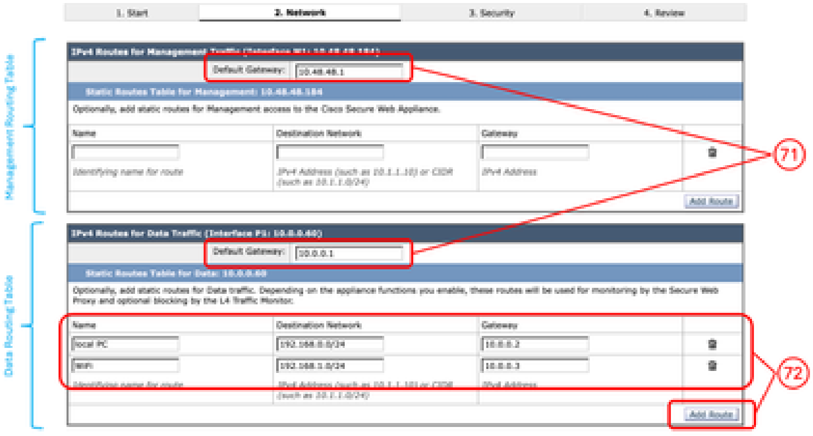
Image - System Setup Wizard - Layer 4 Traffic Monitor Setting

Step 71. (Optional) In **IPv4 Routes for Management** page you can Modify the **Default Gateway**

Step 72. (Optional) You can Add Route to create **Static Routes**.

</td>
</tr>
</table>

Note: In case you choose "**Use M1 port for management only**" on Step 67, there would be two separate Routing table for the Management Interface and the Data Interfaces (P1 and P2).



IPv4 Routes for Management Traffic (Interface M1: 10.48.48.184)

Default Gateway: 10.48.48.1

Static Routes Table for Management: 10.48.48.184

Optionally, add static routes for Management access to the Cisco Secure Web Appliance.

Name	Destination Network	Gateway
Identifying name for route	*IPv4 Address (such as 10.1.1.10) or CIDR (such as 10.1.1.0/24)*	*IPv4 Address*

IPv4 Routes for Data Traffic (Interface P1: 10.0.0.40)

Default Gateway: 10.0.0.1

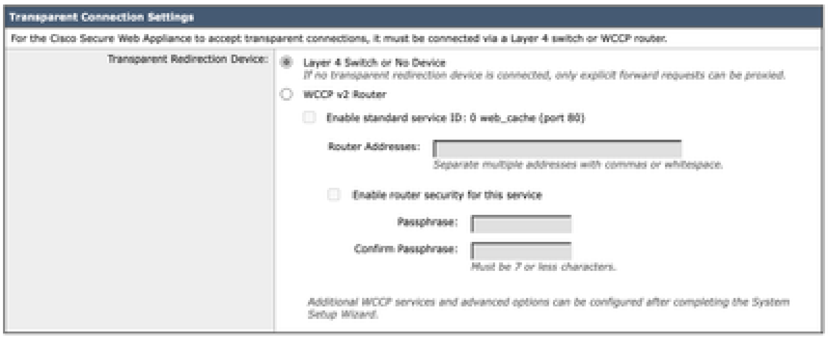
Static Routes Table for Data: 10.0.0.40

Optionally, add static routes for 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	Destination Network	Gateway
local PC	192.168.0.0/24	10.0.0.2
WiFi	192.168.1.0/24	10.0.0.3
Identifying name for route	*IPv4 Address (such as 10.1.1.10) or CIDR (such as 10.1.1.0/24)*	*IPv4 Address*

Image - System Setup Wizard - Add Route

Step 73. (Optional) If you would like to setup Transparent Proxy deployment, via Web Cache Communication Protocol (**WCCP**), you can configure WCCP settings, or else you can leave the default **Layer 4 Switch or No Device** and click **Next**.



Transparent Connection Settings

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

Transparent Redirection Device:

● Layer 4 Switch or No Device
If no transparent redirection device is connected, only explicit forward requests can be proxied.

○ WCCP v2 Router

□ Enable standard service ID: 0 web_cache (port 80)

Router Addresses:
Separate multiple addresses with commas or whitespace.

□ Enable router security for this service

Passphrase:

Confirm Passphrase:
Must be 7 or less characters.

Additional WCCP services and advanced options can be configured after completing the System Setup Wizard.

Image - System Setup Wizard - Proxy Deployment Configuration

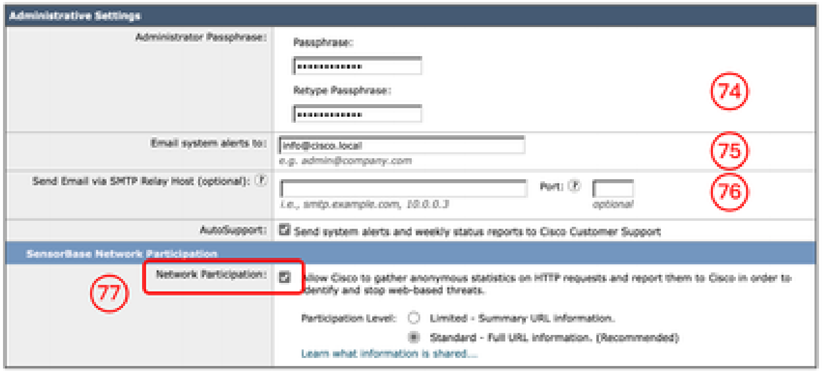
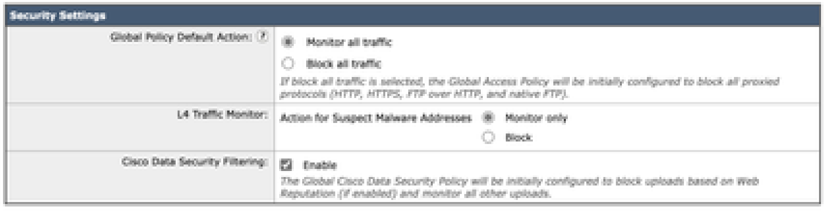
Step 74. Setup a new **password** for the admin account.

Step 75. Enter an Email address that is expected to receive system alerts.

Step 76. (Optional) Provide the Simple Mail Transfer Protocol (**SMTP**) Relay host information, else leave it as blank If no internal relay host is defined, SMTP uses DNS lookup of the MX record.

Step 77. (Optional) If you would like to disable Participating in the **Cisco SensorBase Network,** un-check the **Network Participation** check box, or else leave is as default and click **Next**.

Note: Participating in the Cisco **SensorBase** Network means that Cisco collects data and shares that information with the **SensorBase** threat management database.

		 Administrative Settings Administrator Passphrase: Passphrase: ************ Retype Passphrase: ************ Email system alerts to: info@cisco.local e.g. admin@company.com Send Email via SMTP Relay Host (optional): i.e., smtp.example.com, 10.0.0.3 Port: optional AutoSupport: ☑ Send system alerts and weekly status reports to Cisco Customer Support SensorBase Network Participation Network Participation: ☑ Allow Cisco to gather anonymous statistics on HTTP requests and report them to Cisco in order to identify and stop web-based threats. Participation Level: ○ Limited - Summary URL information. ● Standard - Full URL information. (Recommended) Learn what information is shared... *Image - System Setup Wizard - Administrative Settings* **Step 78.** (Optional) You can change the default actions for **Global Policy**, **L4TM**, and **Cisco Data Security Filtering**, or else you can leave them as default and click **Next**.  Security Settings Global Policy Default Action: ● Monitor all traffic ○ Block all traffic *If block all traffic is selected, the Global Access Policy will be initially configured to block all proxied protocols (HTTP, HTTPS, FTP over HTTP, and native FTP).* L4 Traffic Monitor: Action for Suspect Malware Addresses ● Monitor only ○ Block Cisco Data Security Filtering: ☑ Enable *The Global Cisco Data Security Policy will be initially configured to block uploads based on Web Reputation (if enabled) and monitor all other uploads.* *Image - System Setup Wizard - Security Settings* **Step 79.** Review your configuration. If you need to make changes, click the **Previous** button to return to the previous page, or else click **Install This Configuration**.

Network Configuration

To Configure the Network interface you can use both CLI or GUI.

	Command / Path	Action
Configure Network Interface Cards from CLI	**CLI** > **ifconfig**	**New**: If the Interface is not listed in the **ifconfig** output, but exists in the Virtual Machine or the physical Appliance, you can use this command to show the interface in the list. **Edit**: This action is to edit the IP address, Subnet Mask, Interface hostname or other related parameters. **Details**: Show details of an interface, such as MAC Address, Media Type, Duplex Mode and so

		on. **Delete**: Removes the Interface from the **ifconfig** list, and removes the IP address if assigned previously.
Configure Network Interface Cards from GUI	**GUI** > **Network** > **Interfaces**	You can Edit the Interface IP address and hostname. You can Enable, Disable or modify the port number of the **Appliance Management Services** such as FTP, SSH, HTTP access and HTTPS access.

Routing Table

Routes are essential for determining where to direct network traffic. The SWA handles these types of traffic:

- **Data traffic:** This includes traffic processed by the Web Proxy from end users browsing the Internet.
- **Management traffic:** This encompasses traffic generated by managing the appliance via the web interface, as well as traffic for management services such as SWA upgrades, component updates, DNS, authentication, and other related tasks.

By default, both types of traffic uses the routes defined for all configured network interfaces. However, you have the option to separate the routing so that management traffic uses a dedicated management routing table and data traffic uses a separate data routing table.

Management Traffic	**Data Traffic**
WebUI SSH SNMP Authentication, with domain controller (**configurable**) Syslogs FTP push DNS (**configurable**) Update/Upgrade/Feature Key (**configurable**)	HTTP Proxy HTTPS Proxy FTP Proxy WCCP negotiation ICAP request with external DLP server DNS (**configurable**) Update/Upgrade/Feature Key (**configurable**) Authentication with domain controller (**configurable**)

Note: If you select the "Use M1 port for management only" option, an additional routing table called the Data Routing table is added to the SWA. This routing table has only one configurable default gateway; any additional routing paths must be configured manually.

Related Information

- User Guide for AsyncOS 15.2 for Cisco Secure Web Appliance
- Cisco Secure Email and Web Virtual Appliance Installation Guide
- Configure Custom URL Categories in Secure Web Appliance - Cisco
- Use Secure Web Appliance Best Practices
- Configure Firewall for Secure Web Appliance
- Configure Decryption Certificate in Secure Web Appliance
- Configure and Troubleshoot SNMP in SWA
- Configure SCP Push Logs in Secure Web Appliance with Microsoft Server

- Enable Specific YouTube Channel/Video and Block Rest of YouTube in SWA
- Understand HTTPS Accesslog Format in Secure Web Appliance
- Access Secure Web Appliance Logs
- Bypass Authentication in Secure Web Appliance
- Block Traffic in Secure Web Appliance
- Bypass Microsoft Updates Traffic in Secure Web Appliance