

Configure a Basic Policy

Complete the initial configuration and then configure additional interfaces and network settings as well as customizing your policy.

- Log Into the Device Manager, on page 1
- Complete the Initial Configuration, on page 1
- Configure the Network Settings and Policy, on page 9

Log Into the Device Manager

Log into the device manager to configure your threat defense.

Procedure

Step 1 Enter the following URL in your browser, depending on which interface your computer is connected to.
Ethernet 1/2 through Ethernet 1/8 or 1/10—https://192.168.95.1
Management 1/1—https://management_ip (from DHCP)
Step 2 Log in with the username admin, and the default password Admin123.

Complete the Initial Configuration

Use the setup wizard when you first log into the device manager to complete the initial configuration. After you complete the setup wizard, you should have a functioning device with a couple of basic policies in place:

- inside \rightarrow outside traffic flow
- Interface PAT for all traffic to outside.

Procedure

Step 1 Accept the General Terms and change the admin password.

The **Device Setup** screen appears.

Figure 1: Device Setup

Device Setup	1 Configure Internet Connection	2 Configure Time Settings	3 Smart License Registration	
	Inside Network	Van1 (3 1/5 1/7 Poe MGMT (3 1/5 1/7 Poe MGMT (3 1/5 1/7 Poe CONSOLE (4 1/6 1/8 Poe CONSOLE 1/1	1 ISP/WAN/Gateway	Internet DNS Server NTP Server Marken Smart Lice

Note The exact port configuration depends on your model.

Step 2 Configure network settings for the outside and management interfaces.

L

Figure 2: Connect firewall to internet

Connect firewall to Internet

The initial access control policy will enforce the following actions. You can edit the policy after setup.

Rule 1 Trust Outbound Traffic	Default Action Block all other traffic
This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.	The default action blocks all other traffic.
Outside Interface Address	
Connect Ethernet1/1 (Outside) to your cable modem or router. Then, configure	SP/WAN device, for example, your the addresses for the outside interface.

Configure IPv4			
Using DHCP			~
Configure IPv6			
Using DHCP			~
	NEXT	Don't have internet conr Skip device setup	nection?

a) **Outside Interface**—Ethernet 1/1. You cannot select an alternative outside interface during initial device setup.

Configure IPv4—If you need PPPoE, you can configure it after you complete the wizard.

Configure IPv6

b) Management Interface—Sets parameters for the dedicated Management 1/1 interface. If you changed the IP address at the CLI, you will not see these settings because you already configured them.

DNS Servers—The default is the OpenDNS public DNS servers.

Firewall Hostname

- c) Click Next.
- **Step 3** Configure the system time settings.

Figure 3: Time Setting (NTP)

Time Setting (NTP)

S	ystem Time: 11:56:20AM October 03 2024 -06:00	
Т	ime Zone for Scheduling Tasks	
	(UTC+00:00) UTC	
N	ITP Time Server	
	Default NTP Servers	• •
S 0 1 2	ierver Name .sourcefire.pool.ntp.org .sourcefire.pool.ntp.org .sourcefire.pool.ntp.org	
	NEXT	
a) b) c)	Time Zone NTP Time Server Click Next.	

Step 4 Configure Smart Licensing.

Register with	Register with Cisco Smart Software Manager Cisco Smart Software Manager to use the full functionality of this device and to apply subscription licenses.
	What is smart license?[건
C re Re	ontinue with evaluation period: Start 90-day evaluation period without egistration ecommended if device will be cloud managed. Learn More [2] Please make sure you register with Cisco before the evaluation period ends. Otherwise you will not be able to make any changes to the device configuration.
O R	egister device with Cisco Smart Software Manager
	Please register your device at this time. If you do not register now, you can register later from the Device > Smart License page.
	Create or log in into your Cisco Smart Software Manager account.
	 On your assigned virtual account, under "General tab", click on "New Token" to create token.
	3 Copy the token and paste it here:
Ň	Token MDM4MTdhNWEtNmExMC00NzMyLWE3YWMtMzY1MWViOTM2Nm E0LTE3NDU0MzI2%0ANjQyMjV8dUNPZnRLWDJhSFJ6bWc0YkFqVW ZWQzJzd2JDN2dwRkxhbUhQeHhj%0AZUtnUT0%3D%0A
	 Select the region in which your device is operating. Percipe
	US Region v (i
	5 Enroll Cisco Success Network.
	Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.
	Check out the Sample Data that will be sent to Cisco. See more >
	Enroll Cisco Success Network
(For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide [2]
	BACK FINISH

- a) Click Register device with Cisco Smart Software Manager.
- b) Click the Cisco Smart Software Manager link.
- c) Click Inventory.

ſ

Cisco Software Central > Smart Software Licensing Smart Software Licensing

Alerts Inventory Convert to Smart Licensing

d) On the General tab, click New Token.

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances t

New Token		
Token	Expiration Date	Uses
OWFINTZiYTgtY2Ew 2	2024-May-18 17:41:53 (in 30 days)	0 of 10

e) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:

Create Registration	loken .	?	×
This will create a token that is use created, go to the Smart Licensin	ed to register product instances, so that they can use licenses from this virtual account.Once is g configuration for your products and enter the token, to register them with this virtual account account.	ťs L	
Virtual Account:			
Description:	Description		
* Expire After:	365 Days		
Max. Number of Uses:	Between 1 - 365, 30 days recommended		
Allow export-controlled fun	The token will be expired when either the expiration or the maximum uses is reached ctionality on the products registered with this token 1		
	Create Token	Cancel	

- Description
- Expire After—Cisco recommends 30 days.
- Max. Number of Uses
- Allow export-controlled functionality on the products registered with this token—Enables the export-compliance flag if you are in a country that allows for strong encryption. You must select this option now if you plan to use this functionality. If you enable this functionality later, you will need to re-register your device with a new product key and reload the device. If you do not see this option, your account does not support export-controlled functionality.

The token is added to your inventory.

f) Click the arrow icon to the right of the token to open the **Token** dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the threat defense.

Figure 4: View Token

General	Licenses	Product Instances	Event Log	
Virtual Acc	ount			
Description:				
Default Virtu	al Account:	No		
The registration	tokens below	can be used to register new	v product instances	s to this virtual account.
Token		Expiration Date	Uses	Export-Controlled
OWFINTZIYT	gtY2Ew. 🔽	2024-May-18 17:41:53 (in :	30 days) 0 of 10	D Allowed
ure 5: Copy T Token	oken	0	×	
MjM3ZjihYTitZ NmVhLTE1MD mFJN2dYQji50 0AMDd0ST0%	GQ4OS00Yjk2 I5MTI1%0AMT QWRhOEdscDU 3D%0A	LTgzMGItMThmZTUyYjky MxMzh8YzdQdmgzMjA2V J4cWI5NFNWRUtsa2wz%		
Press ctrl + c to	copy selected i	text to clipboard.		

- g) In the device manager, paste the token into the token field.
- h) Set the other options, and then click Finish

Step 5 Finish the setup wizard.

Figure 6: What's Next

	×
The Device Is Up and Ready to Be Configured! What's next?	
Device will be Cloud Managed Standalone Device	
Configure Interfaces Connect inside ports to internal devices	
Configure Policy Manage traffic	
GOT IT	

- a) Click Standalone Device to use the device manager.
- b) Click **Configure Interfaces** to go directly to the **Interfaces** page, **Configure Policy** to go to the **Policies** page, or **Got It** to go to the **Device** page.

For interfaces or policy configuration, see Configure the Network Settings and Policy, on page 9.

Step 6 Enable feature licenses.

- a) From the **Device** page, click **Smart License** > > **View Configuration**.
- b) Click the Enable/Disable control for each optional license.

SUBSCRIPTION LICENSES INCLUDED	
IPS ENABLE	Malware Defense
This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.	This license lets you perform malware defense. You must have this license to apply file policies that detect and block malware in files transmitted over your network.
Includes: 🌯 Intrusion Policy	Includes: C File Policy
URL ENABLE	Cisco Secure Client Type Advantage ~ ENABLE
This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.	Please select the license type that you purchased to enable remote access VPN. Note that Secure Firewall device manager does not support any of the advanced features covered by the Advantage license.
Includes: URL Reputation	Includes: RA-VPN

c) Choose **Resync Connection** from the gear drop-down list to synchronize license information with Cisco Smart Software Manager.

Go to	Cloud Services
	Resync connection
	Unregister Device

Configure the Network Settings and Policy

Configure additional interfaces, a DHCP server, and customize the security policy.

Procedure

- **Step 1** If you want to convert a switch port to a firewall interface, choose **Device**, and then click the link in the **Interfaces** summary.
 - a) Click the edit icon (\bigcirc) for the switch port.
 - b) Change the mode from Switch Port to Routed.

Figure 7: Change the Mode

Ethernet1/3 Edit Physical Interface		8 ×
Interface Name	Mode Switch Port V	Status
Most features work with named interfaces only, although some require unnamed interfaces.	Routed	
Description	Passive	
	Switch Port	
IPv4 Address IPv6 Address Advanced ^① VLAN		11.
Protected Port 1		
Usage Type Access Trunk		
Access VLAN		
inside (Vlan1)		~
	CANCEL	ОК

c) Set the name and IP address.

Figure 8: Edit Interface

Ethernet1/3 Edit Physical Interface											
Interface Name	Mode Status										
dmz	Routed Y										
Most features work with named interfaces only, although some require unnamed interfaces.											
Description											
		11.									
IPv4 Address IPv6 Address Advanced											
Туре											
Static Y											
IP Address and Subnet Mask											
192.168.1.4 / 24											
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0											
Standby IP Address and Subnet Mask											
1											
e.g. 192.168.5.16											
	CANCEL										

d) Click OK.

Step 2 If you configured new firewall interfaces, choose **Objects**, then select **Security Zones**.

Edit or create new zones as appropriate and assign the interface to the zone. Each interface must belong to a zone for which you configure policies.

The following example creates a new dmz_zone and then assigns the dmz interface to it.

Figure 9: Security Zone Object

Add Security Zone	e ×
Name dmz_zone	
Description	
Mode Routed Passive 	Inline
Interfaces	
<pre>Interfaces +</pre>	6
Interfaces	i) ANCEL OK
Interfaces	1 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
Interfaces	i i i i i i i i
Interfaces	i j nt1/1) i i j
Interfaces	i) ANCEL OK ht1/1) i () i

Step 3 If you want internal clients to use DHCP to obtain an IP address from the device, choose **Device** > **System Settings** > **DHCP Server**, then select the **DHCP Servers** tab.

There is already a DHCP server configured for the inside interface.

Figure 10: DHCP Server

Add Server		∂ ×
Enable DHCP Server		
Interface		
dmz (Ethernet1/3)		~
Address Pool		
192.168.1.50-192.168.1.254		0
e.g. 192.168.45.46-192.168.45.254		
	CANCEL	ОК

Step 4 Choose **Policies** and configure the security policies for the network.

The device setup wizard enables traffic flow between the inside_zone and outside_zone using a Trust rule. A Trust rule does not apply an intrusion policy. To use intrusion, specify the Allow action for the rule. The policy also includes interface PAT for all interfaces when going to the outside interface.

Figure 11: Default Security Policies

Security Policies													
\square \rightarrow \bigcirc SSL Decryption \rightarrow \bigcirc Identity \rightarrow \bigcirc Security Intelligence \rightarrow \oslash NAT \rightarrow \bigodot Access Control \rightarrow \circledast Intrusion													
1 rule	1 rule Tilter												
		SOURCE				DESTINATION		1					
#	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS		ACTIONS
> 1	Inside_Outside	✓ Trust	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	Q C.	
Defau	It Action Acc	ess Con	trol 😑 Block	9 E									

However, if you have interfaces in different zones, you need access control rules to allow traffic to and from those zones.

In addition, you can configure other policies to provide additional services and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies by clicking the policy type in the toolbar:

- SSL Decryption—If you want to inspect encrypted connections (such as HTTPS) for intrusions, malware, and so
 forth, you must decrypt the connections. Use the SSL decryption policy to determine which connections need to be
 decrypted. The system re-encrypts the connection after inspecting it.
- **Identity**—If you want to correlate network activity to individual users, or control network access based on user or user group membership, use the identity policy to determine the user associated with a given source IP address.
- Security Intelligence—(Requires the IPS license) Use the Security Intelligence policy to quickly drop connections from or to blacklisted IP addresses or URLs. By blacklisting known bad sites, you do not need to account for them in your access control policy. Cisco provides regularly updated feeds of known bad addresses and URLs so that the Security Intelligence blacklist updates dynamically. Using feeds, you do not need to edit the policy to add or remove items in the blacklist.

- NAT (Network Address Translation)—Use the NAT policy to convert internal IP addresses to externally routeable addresses.
- Access Control—Use the access control policy to determine which connections are allowed on the network. You can filter by security zone, IP address, protocol, port, application, URL, user or user group. You also apply intrusion and file (malware) policies using access control rules. Use this policy to implement URL filtering.
- Intrusion—Use the intrusion policies to inspect for known threats. Although you apply intrusion policies using access control rules, you can edit the intrusion policies to selectively enable or disable specific intrusion rules.

The following example shows how to allow traffic between the inside_zone and dmz_zone in the access control policy. In this example, no options are set on any of the other tabs except for **Logging**, where **At End of Connection** is selected.

Figure 12: Access Control Policy

Add Access Rule															
Order Title Action															
2 ~	2 ✓ inside-dmz 🔁 Allow ✓														
Source/Des	tination	Applications	URLs	Users ³	Intrusion	Policy ³ F	ile policy	Logging							
SOURCE DESTINATION															
Zones	+	Networks	+	Ports	+	SGT Groups	+	Zones	+	Networks	+	Ports	+	SGT Groups	+
inside_z	one	ANY		ANY		ANY		dmz_zone		ANY		ANY		ANY	

Step 5 Choose **Device**, then click **View Configuration** in the **Updates** group and configure the update schedules for the system databases.

If you are using intrusion policies, set up regular updates for the Rules and VDB databases. If you use Security Intelligence feeds, set an update schedule for them. If you use geolocation in any security policies as matching criteria, set an update schedule for that database.

Step 6Click the Deploy button in the menu, then click the Deploy Now button (Changes are not active on the device until you deploy them.