Initial Configuration

This chapter describes the Out-Of-Box experience (OBE) for the installer that provides the device with a basic working configuration. There is a factory default set of parameters that are available on the Cisco ISA 3000.

This chapter contains the following sections:

- Factory Default Configuration, page 4-1
  - Port Information, page 4-1
  - ASA Default Configuration, page 4-2
  - Factory Default Configuration from the CLI, page 4-4
- MIB Information, page 4-7
- Connecting to the Device for Configuration, page 4-7
  - Cabling Procedure, page 4-7
  - Power On the ISA3000, page 4-8
  - Launch ASDM, page 4-9
  - Run Other ASDM Wizards and Advanced Configuration, page 4-15
  - Configure the ASA Firepower Module, page 4-15
  - Where to Go Next, page 4-16
- Verifying the Initial Configuration, page 4-16

Factory Default Configuration

The ISA 3000 is slightly different from other ASA devices in the factory default configuration. This next section will describe some of these differences.

Port Information

Port Numbering

The port numbering, or interface numbering, is different from the other ASA devices. Typical ASA port numbering starts with 0, while the ISA 3000 port numbering starts with 1. The interface names for the ports are as follows:

- Gigabit Ethernet 1/1
Factory Default Configuration

Chapter 4      Initial Configuration

- Gigabit Ethernet 1/2
- Gigabit Ethernet 1/3
- Gigabit Ethernet 1/4

The management port is:
- Management 1/1

USB Ports

There are two externally accessible Type-A USB 2.0 (4-pin) connectors. These ports support mass storage devices. These 2 USB Ports when connected appear as disk1, disk2 in ASA, for example:

```
ciscoasa# show file system
File Systems:
  Size(b)   Free(b)   Type     Flags Prefixes
* 15621070848 15401517056 disk  rw  disk0: flash:
  -        -   disk  rw  disk1:
  -        -   disk  rw  disk2:
  -        -  network  rw  tftp:
```

These ports are enabled by default and cannot be turned off.

ASA Default Configuration

The default ASA configuration and Out-of Box behavior is described in this next section.

Firewall Mode

The ISA 3000 operates in transparent mode by default. Firewall policies are described later in this section.

Management Port

The management port is assigned a default static IP address, 192.168.1.1.

For example:

```
interface Management1/1
management-only
no shutdown
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
```

DHCP Server

DHCP enabled clients that are connected to the management port may obtain an IP address directly from the ISA 3000. The default configuration provides a DHCP server that is enabled on the management port of the ISA 3000. The range of IP addresses that can be leased to the DHCP clients are in a range that does not overlap the IP address assigned to the management port. This default range of IP addresses is selected to be between 192.168.1.5-192.168.1.254.
HTTP Server

The default configuration will provide Cisco ASDM access from clients on the management port to the ISA 3000. The default configuration will automatically enable a HTTP server on the management port. No password will be enforced for first-time Cisco ASDM access.

Data Ports

By default all data ports will be in a bridge group. This allows traffic flow through any interface to other interfaces (bridge mode). However, to utilize the hardware bypass feature when needed, using either Gigabit Ethernet 1/1 and 1/2 pair (or in Copper SKU Gigabit Ethernet 1/3 and 1/4 pair as well) for traffic is recommended.

An allowAll access-list is created which can be applied to the data interfaces using either CLI or ASDM. For SourceFire traffic a separate access-list sfrAccessList will be created.

For example:

```plaintext
interface BVI 1
!
interface GigabitEthernet1/1
  bridge-group 1
  no shutdown
  nameif outside1
  security-level 0
!
interface GigabitEthernet1/2
  bridge-group 1
  no shutdown
  nameif inside1
  security-level 100
!
interface GigabitEthernet1/3
  bridge-group 1
  no shutdown
  nameif outside2
  security-level 0
!
interface GigabitEthernet1/4
  bridge-group 1
  no shutdown
  nameif inside2
  security-level 100
!
access-list allowAll permit ip any any
access-list sfrAccessList extended permit ip any any
```

Note

ISA3000 dataports cannot have mask of /30 or /31

Firewall Policies

Data ports are enabled by default. Traffic is directed to SFR using a class map and policy map that would be present by default.

Note

The BVI interface needs to have a proper IP address to enable forwarding of data. Without an explicitly configured BVI IP address in the same network, traffic will cease to flow.
Default configuration of access-list sfrAccessList will match all the traffic. For example, the following can be used to identify the HTTP traffic only and get it to SFR:

```plaintext
access-list httpTraffic permit tcp any any eq http
class-map httpClass
match access-list httpTraffic

policy-map global_policy
class httpClass
  sfr fail-open
```

The default configuration of class map to identify traffic for FirePOWER inspection is as follows:

```plaintext
class-map sfrclass
match access-list sfrAccessList
```

Default configuration of policy map for the actions to be performed on the traffic identified:

```plaintext
policy-map global_policy
class sfrclass
  sfr fail-open monitor-only
```

Factory Default Configuration from the CLI

A typical factory default CLI configuration is shown as follows:

```
ciscoasa# show run
: Saved
:
: Serial Number: FCH1XXXXX
: Hardware:   ISA3000, 8xxx MB RAM, CPU Demo MHz, 1 CPU (4 cores)
: ASA Version 9.x(x)x
!
firewall transparent
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  no shutdown
!
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
!
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  no shutdown
!
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
```
security-level 100
no shutdown
!

**Note** Gigabit Ethernet 1/1-1/4 are on bridge-group 1 to allow traffic from any port to any other port.

interface Management1/1
management-only
no shutdown
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0

**Note** 192.168.1.1 is the default management IP Address. This is the address that can be used to manage the ISA 3000 with the Single Device manager ASDM or CLI

! interface BVI 1
no ip address
!

**Note** BVI interfaces need to have an IP address for data to flow between ports when ASA is in transparent mode

ftp mode passive
no hardware-bypass boot-delay module-up sfr
hardware-bypass Gigabit Ethernet 1/1-1/2
hardware-bypass Gigabit Ethernet 1/3-1/4

**Note** By default, the hardware bypass is enabled on both pairs of the copper SKU. Once ASA comes back up, the hardware bypass will be turned off.

access-list allowAll extended permit ip any any
access-list sfrAccessList extended permit ip any any

access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

pager lines 24
logging asdm informational
mtu management 1500
mtu inside1 1500
mtu outside1 1500
mtu inside2 1500
mtu outside2 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
http server enable
http 192.168.1.0 255.255.255.0 management

**Note** Enables ASDM access via Management Port.

no snmp-server location
no snmp-server contact
service sw-reset-button
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd address 192.168.1.5–192.168.1.254 management
dhcpd enable management

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record DfltAccessPolicy

! class-map inspection_default
  match default-inspection-traffic
!
class-map sfrclass
  match access-list sfrAccessList
!
policy-map type inspect dns preset_dns_map
  parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect smtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
    inspect ip-options
  class sfrclass
    sfr fail-open monitor-only
    !

**Note** In case of a FirePOWER module failure, "fail-open" mode will allow ASA to ignore and forward traffic. The command "monitor-only" causes copies of packets to flow from ASA to SFR for passive/offline inspection.
service-policy global_policy global
prompt hostname context

Cryptochecksum:61c9397c4e5eb7f0fffc14e902ccba3e7
: end

ciscoasa#

MIB Information

The ISA 3000 supports all the MIB currently supported by ASA software.
MIBs supported for ASA can be seen by going to the SNMP configuration guide URL:

From there you can find the network management MIBS URL:

Connecting to the Device for Configuration

The Cisco ISA 3000 has three options available to perform the initial configuration:

1. CLI using the USB Port
   With this option, the user connects a PC to the mini-USB port on the device with a USB cable.
   Provided the correct drivers are installed, you can launch a terminal program. If your laptop or PC
   warns you that you do not have the proper drivers to communicate with the router, you can obtain
   them from your computers manufacturer, or go here:
   https://www.silabs.com/products/mcu/Pages/USBtoUARTBridgeVCPDrivers.aspx

2. CLI using the RJ-45 Console Port
   With this option, the user connects a PC to the RJ-45 console port on the Cisco ISA 3000 using a
   standard RJ45 to DB9 connector and cable.

3. ASDM from the Management 1/1 interface
   If the configuring PC is on the same sub-network as the Cisco ISA 3000’s management interface,
   the user can use ASDM to configure the device. The IP address range is 192.168.1.5-192.168.1.254.
   The ASDM GUI can be launched to start to configure the device.

Cabling Procedure

The following diagram is of a basic network installation.
Connecting to the Device for Configuration

Chapter 4  Initial Configuration

Figure 4-1  Basic Network

**ISA3000 Typical Configuration**

---

**Step 1**  Cable the following directly to the device or to a Layer 2 Ethernet switch:
- Gigabit Ethernet 1/2 interface (inside)
- Management 1/1 interface (for the ASA Firepower module)

**Note**  You can connect inside and management on the same network because the management interface acts like a separate device that belongs only to the ASA Firepower module.

**Step 2**  Connect the Gigabit Ethernet 1/1 (outside) interface to your WAN device, for example, your cable modem.

**Note**  If the cable modem supplies an outside IP address that is on 192.168.1.0/24 or 192.168.10.0/24, then you must change the ISA 3000 configuration to use a different IP address.

---

**Power On the ISA3000**

**Step 1**  Refer to the instructions for proper wiring of the power plug in Chapter 3, “Connecting to DC Power”.
**Step 2**  Attach the power plug to the ISA3000 after wiring it to the DC power source.
Check the status of the LEDs to make sure the device is operating correctly. Refer to Chapter 3, “Verifying Connections”.

Launch ASDM

See the ASDM release notes on Cisco.com for the requirements to run ASDM.

This procedure assumes you want to use ASDM to manage the ASA Firepower Module. If you want to use the FireSIGHT System, then you need to connect to the module CLI and run the setup script; see the ASA Firepower quick start guide.

Procedure

Step 1  On the computer connected to the ISA 3000, launch a web browser.
Step 2  In the Address field, enter the following URL: https://192.168.1.1/admin.
Step 3  Your browser should ask if it is OK to allow running the untrusted application or not. Depending on your browser, you will answer in a different manner. Refer to Browser Responses to Security Questions for the proper responses.
Step 4  The Cisco ASDM web page appears.

Note  If you connected your management computer to the ASA as a wireless client, you can access ASDM at https://192.168.10.1/admin.
Step 5  Click one of the available options: Install ASDM Launcher, Run ASDM, or Run Startup Wizard.
Step 6  Follow the on screen instructions to launch ASDM according to the option you chose. The Cisco ASDM-IDM Launcher appears.

If you click Install ASDM Launcher, in some cases you need to install an identity certificate for the ISA3000 and a separate certificate for the ASA Firepower module according to Install an Identity Certificate for ASDM.
Step 7  Leave the username and password fields empty, and click OK. The main ASDM window appears.
Step 8  If you are prompted to provide the IP address of the installed ASA Firepower module, cancel out of the dialog box. You must first set the module IP address to the correct IP address using the Startup Wizard. ASDM can change the ASA Firepower module IP address settings over the ASA backplane; but for ASDM to then manage the module, ASDM must be able to reach the module (and its new IP address) on the Management 1/1 interface over the network. The recommended deployment allows this access because the module IP address is on the inside network. If ASDM cannot reach the module on the network after you set the IP address, then you will see an error.
Step 9  Choose Wizards > Startup Wizard.
Step 10  Ensure that the Bridge Group Management has an IP address configured explicitly set in the same subnet as the local network connect to traffic interfaces (Gigabit Ethernet 1/1-1/4).
Step 11 Configure additional ASA settings as desired, or skip screens until you reach the ASA Firepower Basic Configuration screen.
Set the following values to work with the default configuration:

- **IP Address**—192.168.1.2
- **Subnet Mask**—255.255.255.0
- **Gateway**—192.168.1.1

**Step 12** Click **I accept the agreement**, and click **Next** or **Finish** to complete the wizard.

**Step 13** Quit ASDM, and then relaunch. You should see ASA Firepower tabs on the Home page.

---

**Browser Responses to Security Questions**

This section shows how to respond to the security questions from Step 3 above in launching ASDM.
Connecting to the Device for Configuration

Internet Explorer

Safari
Chapter 4      Initial Configuration
Connecting to the Device for Configuration

Chrome Step 1

asdm launched from Google Chrome

Your connection is not private

Attackers might be trying to steal your information from 10.31.118.167 (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically report details of possible security incidents to Google. Privacy policy

Advanced

Chrome Step 2

asdm launched from Chrome

This server could not prove that it is 10.31.118.167; its security certificate is not trusted by your computer’s operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 10.31.118.167 (unsafe)
Connecting to the Device for Configuration

Chapter 4      Initial Configuration

Firefox Step 1

This Connection is Untrusted
You have asked Firefox to connect securely to 10.31.110.167, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn’t continue.

Get me out of here!

Technical Details

I Understand the Risks

Firefox Step 2

This Connection is Untrusted
You have asked Firefox to connect securely to 10.31.110.167, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn’t continue.

Get me out of here!

Technical Details

I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if you trust the site, this error could mean that someone is tampering with your connection.

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception....
Firefox Step 3

Run Other ASDM Wizards and Advanced Configuration

ASDM includes many wizards to configure your security policy. See the Wizards menu for all available wizards.

To continue configuring your ISA 3000, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.

Configure the ASA Firepower Module

Use ASDM to configure the module security policy and to send traffic to the module.

Note: You can alternatively use the FireSIGHT Management Center to manage the ASA Firepower module. See the ASA Firepower Module Quick Start Guide for more information.

Procedure

Step 1 Use the ASA Firepower pages in ASDM to configure your module security policy. You can click Help in any page, or choose Help > ASA Firepower Help Topics, to learn more about how to configure policies.

Step 2 To send traffic to the module, choose Configuration > Firewall > Service Policy Rules.

Step 3 Choose Add > Add Service Policy Rule.

Step 4 Choose whether to apply the policy to a particular interface or apply it globally and click Next.
**Step 5** Configure the traffic match. For example, you could match Any Traffic so that all traffic that passes your inbound access rules is redirected to the module. Or, you could define stricter criteria based on ports, ACL (source and destination criteria), or an existing traffic class. The other options are less useful for this policy. After you complete the traffic class definition, click Next.

**Step 6** On the Rule Actions page, click the ASA Firepower Inspection tab.

**Step 7** Check the Enable ASA Firepower for this traffic flow check box.

**Step 8** In the If ASA Firepower Card Fails area, click one of the following:

- Permit traffic—Sets the ISA 3000 to allow all traffic through, uninspected, if the module is unavailable.
- Close traffic—Sets the ISA 3000 to block all traffic if the module is unavailable.

**Step 9** (Optional) Check Monitor-only to send a read-only copy of traffic to the module, i.e. passive mode.

**Step 10** Click Finish and then Apply.

**Step 11** Repeat this procedure to configure additional traffic flows as desired.

---

**Where to Go Next**

For more information about the ASA Firepower module and ASA operation, see the “ASA Firepower Module” chapter in the ASA/ASDM firewall configuration guide, or the ASDM online help. You can find links to all ASA/ASDM documentation at Navigating the Cisco ASA Series Documentation.

For more information about ASA Firepower configuration, see the online help or the ASA Firepower Module User Guide or FireSIGHT System User Guide.

---

**Verifying the Initial Configuration**

To verify that the new interfaces are operating correctly, perform the following tests:

- To verify that the interfaces and line protocol are in the correct state—up or down—enter the show interfaces command.

- To display a summary status of the interfaces configured for IP, enter the show ip interface brief command.

- To verify that you configured the correct hostname and password, enter the show configuration command.

After you complete and verify the initial configuration, you can configure your Cisco ISA 3000 for specific functions.