Setting Up a FireSIGHT System Appliance

After you deploy and install an appliance, you must complete a setup process that allows the new appliance to communicate on your trusted management network. You must also change the administrator password and accept the end user license agreement (EULA).

The setup process also allows you to perform many initial administrative-level tasks, such as setting the time, registering and licensing devices, and scheduling updates. The options you choose during setup and registration determine the default interfaces, inline sets, zones, and policies that the system creates and applies.

The purpose of these initial configurations and policies is to provide an out-of-the-box experience and to help you quickly set up your deployment, not to restrict your options. Regardless of how you initially configure a device, you can change its configuration at any time using the Defense Center. In other words, choosing a detection mode or access control policy during setup, for example, does not lock you into a specific device, zone, or policy configuration.

Note See the ASA documentation for information on setting up ASA FirePOWER devices.

For more information on each of the steps in the initial setup process, see the following sections:

- Understanding the Setup Process, page 5-2 outlines the setup process, which depends on the appliance's model and whether you have physical access to the appliance.

Note If you are not already familiar with the setup process, Cisco **strongly** recommends you read this section first.

- Configuring Network Settings Using a Script, page 5-4 explains how to use a script to specify network settings that allow a new appliance to communicate on your management network. This step is required for all Defense Centers that you are accessing using a keyboard and monitor.
- Performing Initial Setup on a Series 3 Device Using the CLI, page 5-5 explains how to use an interactive command line interface (CLI) to perform the setup process on a Series 3 device.
- Initial Setup Page: Devices, page 5-7 explains how to use any device's web interface to complete its initial setup.
- Initial Setup Page: Defense Centers, page 5-11 explains how to use a Defense Center's web interface to complete its initial setup.
- Next Steps, page 5-16 contains guidance on the post-setup tasks you may want to perform as you set up your FireSIGHT System deployment.

Caution The procedures in this chapter explain how to set up an appliance without powering it down. However, if you need to power down for any reason, use the procedure in the Managing Devices chapter in the *FireSIGHT System User Guide*, the `system shutdown` command from the CLI on a Series 3 device, or the `shutdown -h now` command from an appliance's shell (sometimes called expert mode).

Understanding the Setup Process

After you deploy and install a new FireSIGHT System appliance, as described in earlier chapters of this guide, you must complete a setup process. Before you begin the setup, make sure that you can meet the following conditions.

Appliance Model

You must know which appliance you are setting up. A FireSIGHT System *appliance* is either a traffic-sensing managed *device* or a managing *Defense Center*: There are several *models* of each appliance type; these models are further grouped into *series* and *family*. For more information, see FireSIGHT System Appliances, page 1-2.

Access

To set up a new appliance, you must connect using either keyboard and monitor/KVM (keyboard, video, and mouse) or a direct Ethernet connection to the appliance's management interface. After initial setup, you can configure the appliance for serial access. For more information, see Installing the Appliance in a Rack, page 4-24.

Note Do **not** use a KVM console with USB mass storage to access the appliance for the initial setup because the appliance may attempt to use the mass storage device as a boot device.

Information

You have, at minimum, the information needed to allow the appliance to communicate on your management network: an IPv4 or IPv6 management IP address, a netmask or prefix length, and a default gateway.

If you know how the appliance is deployed, the setup process is also a good time to perform many initial administrative-level tasks, including registration and licensing.

Tip If you are deploying multiple appliances, set up your devices first, then their managing Defense Center. The initial setup process for a device allows you to preregister it to a Defense Center; the setup process for a Defense Center allows you to add and license preregistered managed devices.

After you complete setup, you will use the Defense Center's web interface to perform most management and analysis tasks for your deployment. Physical managed devices have a restricted web interface that you can use only to perform basic administration. For more information, see Next Steps, page 5-16.

For details on how to set up each type of appliance, see:

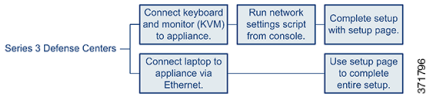
- Setting Up a Series 3 Defense Center, page 5-3
- Setting Up a Series 3 Device, page 5-3

Tip If you are setting up an appliance after restoring it to factory defaults (see Restoring a FireSIGHT System Appliance to Factory Defaults, page 8-1) and you did not delete the appliance's license and network settings, you can use a computer on your management network to browse directly to the appliance's web interface to perform the setup. Skip to Initial Setup Page: Devices, page 5-7 or Initial Setup Page: Defense Centers, page 5-11.

Setting Up a Series 3 Defense Center

Supported Defense Centers: , Series 3

The following diagram illustrates the choices you can make when setting up Series 3 Defense Centers:



To set up a Series 3 Defense Center:

Access: Admin

Step 1 If you are using a keyboard and monitor, run a script that helps you configure settings to allow the appliance to communicate on your management network; see Configuring Network Settings Using a Script, page 5-4.

If you are setting up a reimaged appliance and you kept your network settings as part of the restore process, or if you are accessing the appliance via a direct Ethernet connection, skip to the next step.

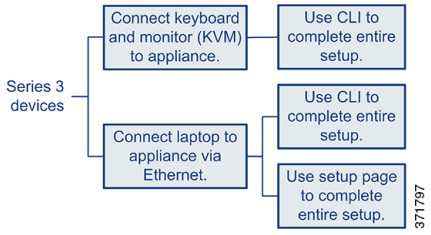
Step 2 Complete the setup process by browsing to the appliance's web interface from a computer on your management network:

- To complete the setup of a managed device using its web interface, see Initial Setup Page: Devices, page 5-7.
- To complete the setup of a Defense Center using its web interface, see Initial Setup Page: Defense Centers, page 5-11.

Setting Up a Series 3 Device

Supported Devices: Series 3

The following diagram illustrates the choices you can make when setting up Series 3 devices:



Your access to a Series 3 device determines how you set it up. You have the following options:

- Regardless of how you are connected to the device, you can use the CLI to set it up; see Performing Initial Setup on a Series 3 Device Using the CLI, page 5-5.
- If you are accessing the appliance via a direct Ethernet connection, you can browse to the appliance's web interface from a local computer; see Initial Setup Page: Devices, page 5-7.

If you are setting up a reimaged device and you kept your network settings as part of the restore process, you can access the CLI via SSH or a Lights-Out Management (LOM) connection. You can also browse to the device's web interface from a computer on your management network.

Configuring Network Settings Using a Script

Supported Devices: Series 2

After you install a new Defense Center or Series 2 device, or delete its network settings as part of a reimage, you must configure the appliance to communicate on your management network. Complete this step by running a script at the console.

The FireSIGHT System provides a dual stack implementation for both IPv4 and IPv6 management environments. First, the script prompts you to configure (or disable) IPv4 management settings, then IPv6. For IPv6 deployments, you can retrieve settings from a local router. You must provide the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway.

When following the script's prompts, for multiple-choice questions, your options are listed in parentheses, such as `(y/n)`. Defaults are listed in square brackets, such as `[y]`. Press Enter to confirm a choice.

Note that the script prompts you for much of the same setup information that the appliance's setup web page does. For more information, see Network Settings, page 5-9 (device) and Network Settings, page 5-13 (Defense Center).

To configure network settings using a script:

Access: Admin

Step 1 At the console, log into the appliance. Use `admin` as the username and `Sourcefire` as the password.

Note that on a Series 3 or virtual managed device, you must type `expert` to display the shell prompt.

Step 2 At the admin prompt, run the following script:

```
sudo /usr/local/sf/bin/configure-network
```

Step 3 Follow the script's prompts.

Configure (or disable) IPv4 management settings first, then IPv6. If you manually specify network settings, you must:

- enter IPv4 addresses, including the netmask, in dotted decimal form. For example, you could specify a netmask of 255.255.0.0.
- enter IPv6 addresses in colon-separated hexadecimal form. For an IPv6 prefix, specify the number of bits; for example, a prefix length of 112.

Step 4 Confirm that your settings are correct.

If you entered settings incorrectly, type `n` at the prompt and press Enter. You can then enter the correct information. The console may display messages as your settings are implemented.

Step 5 Log out of the appliance.

Step 6 Your next step depends on the appliance:

- To complete the setup of a managed device using its web interface, continue with Initial Setup Page: Devices, page 5-7.
- To complete the setup of a Defense Center using its web interface, continue with Initial Setup Page: Defense Centers, page 5-11.

Performing Initial Setup on a Series 3 Device Using the CLI

Supported Devices: Series 3

Optionally, you can use the CLI to configure Series 3 devices instead of using the device's web interface. When you first log in to a newly configured device using the CLI, you must read and accept the EULA. Then, follow the setup prompts to change the administrator password, configure the device's network settings and detection mode. Finally, register the device to the Defense Center that will manage it.

When following the setup prompts, options are listed in parentheses, such as `(y/n)`. Defaults are listed in square brackets, such as `[y]`. Press Enter to confirm a choice.

Note that the CLI prompts you for much of the same setup information that a device's setup web page does. For detailed information on these options, see Initial Setup Page: Devices, page 5-7.

To complete the initial setup on a Series 3 device using the CLI:

Access: Admin

Step 1 Log into the device. Use `admin` as the username and `Sourcefire` as the password.

- For a Series 3 device attached to a monitor and keyboard, log in at the console.
- If you connected a computer to the management interface of a Series 3 device using an Ethernet cable, SSH to the interface's default IPv4 address: 192.168.45.45.

The device immediately prompts you to read the EULA.

Step 2 Read and accept the EULA.

Step 3 Change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.

This password allows the `admin` user to log into the device's web interface and its CLI; the `admin` user has Configuration CLI access. Changing any user's password for an appliance's web interface also changes the password for the CLI, and vice versa.

Cisco recommends that you use strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary. For more information, see Change Password, page 5-8.

Step 4 Configure network settings for the device.

First configure (or disable) IPv4 management settings, then IPv6. If you manually specify network settings, you must:

- enter IPv4 addresses, including the netmask, in dotted decimal form. For example, you could specify a netmask of 255.255.0.0.
- enter IPv6 addresses in colon-separated hexadecimal form. For an IPv6 prefix, specify the number of bits; for example, a prefix length of 112.

For more information, see Network Settings, page 5-9. The console may display messages as your settings are implemented.

Step 5 Select whether you want to allow changing of the device's network settings using the LCD panel.

Caution Enabling this option can present a security risk. You need only physical access, not authentication, to configure network settings using the LCD panel. For more information, see Using the LCD Panel on a Series 3 Device, page 6-1.

Step 6 Specify the detection mode based on how you deployed the device.

For more information, see Detection Mode, page 5-10. The console may display messages as your settings are implemented. When finished, the device reminds you to register this device to a Defense Center, and displays the CLI prompt.

Step 7 To use the CLI to register the device to the Defense Center that will manage it, continue with the next section, Registering a Series 3 Device to a Defense Center Using the CLI.

You must manage devices with a Defense Center. If you do not register the device now, you must log in later and register it before you can add it to a Defense Center.

Step 8 Log out of the appliance.

Registering a Series 3 Device to a Defense Center Using the CLI

Supported Devices: Series 3

If you configured a Series 3 device using the CLI, Cisco recommends that you use the CLI to register the device to a Defense Center at the conclusion of the setup script. It is easiest to register a device to its Defense Center during the initial setup process, because you are already logged into the device's CLI.

To register a device, use the `configure manager add` command. A unique alphanumeric registration key is always required to register a device to a Defense Center. This is a simple key that you specify, up to 37 characters in length, and is not the same as a license key.

In most cases, you must provide the Defense Center's hostname or the IP address along with the registration key, for example:

```
configure manager add DC.example.com my_reg_key
```

However, if the device and the Defense Center are separated by a NAT device, enter a unique NAT ID along with the registration key, and specify `DONTRESOLVE` instead of the hostname, for example:

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

To register a device to a Defense Center:

Access: Configuration CLI

Step 1 Log in to the device as a user with Configuration CLI access level:

- If you are performing the initial setup from the console, you are already logged in as the `admin` user, which has the required access level.
- Otherwise, SSH to the device's management IP address or host name.

Step 2 At the prompt, register the device to a Defense Center using the `configure manager add` command, which has the following syntax:

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE}
reg_key [nat_id]
```

where:

- `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}` specifies either the fully qualified host name or IP address of the Defense Center. If the Defense Center is not directly addressable, use `DONTRESOLVE`.
- *`reg_key`* is the unique alphanumeric registration key, up to 37 characters in length, required to register a device to the Defense Center.
- *`nat_id`* is an optional alphanumeric string used during the registration process between the Defense Center and the device. It is required if the hostname is set to `DONTRESOLVE`.

Step 3 Log out of the appliance.

The device is ready to be added to a Defense Center.

Initial Setup Page: Devices

For all managed devices (except Series 3 devices that you configured using the CLI; see Performing Initial Setup on a Series 3 Device Using the CLI, page 5-5), you must complete the setup process by logging into the device's web interface and specifying initial configuration options on a setup page.

You must change the administrator password, specify network settings if you have not already, and accept the EULA. You can also preregister the device to a Defense Center and specify a detection mode; the detection mode and other options you choose during registration determine the default interfaces, inline sets, and zones that the system creates, as well as the policies that it initially applies to managed devices.

To complete the initial setup on a physical managed device using its web interface:

Access: Admin

Step 1 Direct your browser to `https://mgmt_ip/`, where *mgmt_ip* is the IP address of the device's management interface.

- For a device connected to a computer with an Ethernet cable, direct the browser on that computer to the default management interface IPv4 address: `https://192.168.45.45/`.
- For a device where network settings are already configured, use a computer on your management network to browse to the IP address of the device's management interface.

The login page appears.

Step 2 Log in using `admin` as the username and `Sourcefire` as the password.

The setup page appears. See the following sections for information on completing the setup:

- Change Password, page 5-8
- Network Settings, page 5-9
- Series 3 Device LCD Panel Configuration, page 5-9
- Remote Management, page 5-9
- Time Settings, page 5-9
- Detection Mode, page 5-10
- Automatic Backups, page 5-11
- End User License Agreement, page 5-11

Step 3 When you are finished, click **Apply**.

The device is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the `admin` user, which has the Administrator role.

Step 4 Log out of the device.

The device is ready to be added to its Defense Center.

Note If you connected directly to the device using an Ethernet cable, disconnect the computer and connect the device's management interface to the management network. If you need to access the device's web interface at any time, direct a browser on a computer on the management network to the IP address or host name that you configured during setup.

Change Password

You must change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.

This password allows the `admin` user to log into the device's web interface and its CLI; the `admin` user has Configuration CLI access. Changing any user's password for an appliance's web interface also changes the password for the CLI, and vice versa.

Cisco recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

Network Settings

A device's network settings allow it to communicate on your management network. If you already configured the device's network settings, this section of the page may be prepopulated.

The FireSIGHT System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must specify the management network protocol (**IPv4**, **IPv6**, or **Both**). Depending on your choice, the setup page displays various fields where you must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway:

- For IPv4, you must set the address and netmask in dotted decimal form (for example: a netmask of 255.255.0.0).
- For IPv6 networks, you can select the **Assign the IPv6 address using router autoconfiguration** check box to automatically assign IPv6 network settings. Otherwise, you must set the address in colon-separated hexadecimal form and the number of bits in the prefix (for example: a prefix length of 112).

You can also specify up to three DNS servers, as well as the host name and domain for the device.

Series 3 Device LCD Panel Configuration

Supported Devices: Series 3

If you are configuring a Series 3 device, select whether you want to allow changing of the device's network settings using the LCD panel.

Caution Enabling this option can represent a security risk. You need only physical access, not authentication, to configure network settings using the LCD panel. For more information, see Using the LCD Panel on a Series 3 Device, page 6-1.

Remote Management

You must manage a Cisco device with a Defense Center. In this two-step process, you first configure remote management on the device, then add the device to a Defense Center. For your convenience, the setup page allows you to preregister the device to the Defense Center that will manage it.

Leave the **Register This Device Now** check box enabled, then specify the IP address or fully qualified domain name of the managing Defense Center as the **Management Host**. Also, type the alphanumeric **Registration Key** you will later use to register the device to the Defense Center. Note that this is a simple key that you specify, up to 37 characters in length, and is not the same as the license key.

Note If the device and Defense Center are separated by a network address translation (NAT) device, defer device registration until after you complete the initial setup. See the Managing Devices chapter in the *FireSIGHT System User Guide* for more information.

Time Settings

You can set the time for a device either manually or via network time protocol (NTP) from an NTP server, including the Defense Center. Cisco recommends that you use the Defense Center as the NTP server for its managed devices.

You can also specify the time zone used on the local web interface for the `admin` account. Click the current time zone to change it using a pop-up window.

Detection Mode

The detection mode you choose for a device determines how the system initially configures the device's interfaces, and whether those interfaces belong to an inline set or security zone.

The detection mode is not a setting you can change later; it is simply an option you choose during setup that helps the system tailor the device's initial configurations. In general, you should choose a detection mode based on how your device is deployed:

Passive

Choose this mode if your device is deployed passively, as an intrusion detection system (IDS). In a passive deployment, you can perform file and malware detection, Security Intelligence monitoring, as well as network discovery.

Inline

Choose this mode if your device is deployed inline, as an intrusion prevention system. An intrusion prevention system usually fails *open* and *allows* non-matching traffic.

In an inline deployment, you can also perform network-based advanced malware protection (AMP), file control, Security Intelligence filtering, and network discovery.

Although you can select the inline mode for any device, keep in mind that inline sets using the following interfaces lack bypass capability:

- non-bypass NetMods on 8000 Series devices
- SFP transceivers on 71xx Family devices

Note Reimaging resets devices in inline deployments to a non-bypass configuration; this disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process, page 8-2.

Access Control

Choose this mode if your device is deployed inline as part of an access control deployment, that is, if you want to perform application, user, and URL control. A device configured to perform access control usually fails *closed* and *blocks* non-matching traffic. Rules explicitly specify the traffic to pass.

You should also choose this mode if you want to take advantage of your device's specific hardware-based capabilities, which include (depending on model): clustering, strict TCP enforcement, fast-path rules, switching, routing, DHCP, NAT, and VPN.

In an access control deployment, you can also perform malware protection, file control, Security Intelligence filtering, and network discovery.

Network Discovery

Choose this mode if your device is deployed passively, to perform host, application, and user discovery only.

The following table lists the interfaces, inline sets, and zones that the system creates depending on the detection mode you choose.

Table 5-1 Initial Configurations Based on Detection Mode

Detection Mode	Security Zones	Inline Sets	Interfaces
Inline	Internal and External	Default Inline Set	first pair added to Default Inline Set—one to the Internal and one to the External zone
Passive	Passive	none	first pair assigned to Passive zone
Access Control	none	none	none
Network Discovery	Passive	none	first pair assigned to Passive zone

Note that security zones are a Defense Center-level configuration which the system does not create until you actually register the device to the Defense Center. Upon registration, if the appropriate zone (Internal, External, or Passive) already exists on the Defense Center, the registration process adds the listed interfaces to the existing zone. If the zone does not exist, the system creates it and adds the interfaces. For detailed information on interfaces, inline sets, and security zones, see the *FireSIGHT System User Guide*.

Automatic Backups

The device provides a mechanism for archiving data so that configuration and event data can be restored in case of failure. As part of the initial setup, you can **Enable Automatic Backups**.

Enabling this setting creates a scheduled task that creates a weekly backup of the configurations on the device.

End User License Agreement

Read the EULA carefully and, if you agree to abide by its provisions, select the check box. Make sure that all the information you provided is correct, and click **Apply**. The device is configured according to your selections and is ready to be added to its managing Defense Center.

Initial Setup Page: Defense Centers

For all Defense Centers, you must complete the setup process by logging into the Defense Center's web interface and specifying initial configuration options on a setup page. You must change the administrator password, specify network settings if you haven't already, and accept the EULA.

The setup process also allows you to register and license devices. Before you can register a device, you must complete the setup process on the device itself, as well as add the Defense Center as a remote manager, or the registration will fail.

For more information, see Supported Capabilities by Managed Device Model, page 1-8 and Licensing the FireSIGHT System, page 1-13.

To complete the initial setup on a Defense Center using its web interface:

Access: Admin

Step 1 Direct your browser to `https://mgmt_ip/`, where *mgmt_ip* is the IP address of the Defense Center's management interface:

- For a Defense Center connected to a computer with an Ethernet cable, direct the browser on that computer to the default management interface IPv4 address: `https://192.168.45.45/`.
- For a Defense Center where network settings are already configured, use a computer on your management network to browse to the IP address of the Defense Center's management interface.

The login page appears.

Step 2 Log in using `admin` as the username and `Sourcefire` as the password.

The setup page appears. See the following sections for information on completing the setup:

- Change Password, page 5-12
- Network Settings, page 5-13
- Time Settings, page 5-13
- Recurring Rule Update Imports, page 5-13
- Recurring Geolocation Updates, page 5-13
- Automatic Backups, page 5-14
- License Settings, page 5-14
- Device Registration, page 5-14
- End User License Agreement, page 5-16

Step 3 When you are finished, click **Apply**.

The Defense Center is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the `admin` user, which has the Administrator role.

Note If you connected directly to the device using an Ethernet cable, disconnect the computer and connect the Defense Center's management interface to the management network. Use a browser on a computer on the management network to access the Defense Center at the IP address or host name that you just configured, and complete the rest of the procedures in this guide.

Step 4 Use the Task Status page (**System > Monitoring > Task Status**) to verify that the initial setup was successful.

The page auto-refreshes every ten seconds. Monitor the page until it lists a status of **Completed** for the initial device registration and policy apply tasks. If, as part of setup, you configured an intrusion rule or geolocation update, you can also monitor those tasks.

The Defense Center is ready to use. See the *FireSIGHT System User Guide* for more information on configuring your deployment.

Step 5 Continue with Next Steps, page 5-16.

Change Password

You must change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.

Cisco recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

Network Settings

A Defense Center's network settings allow it to communicate on your management network. If you already configured the network settings, this section of the page may be prepopulated.

The FireSIGHT System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must specify the management network protocol (**IPv4**, **IPv6**, or **Both**). Depending on your choice, the setup page displays various fields where you must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway:

- For IPv4, you must set the address and netmask in dotted decimal form (for example: a netmask of 255.255.0.0).
- For IPv6 networks, you can select the **Assign the IPv6 address using router autoconfiguration** check box to automatically assign IPv6 network settings. Otherwise, you must set the address in colon-separated hexadecimal form and the number of bits in the prefix (for example: a prefix length of 112).

You can also specify up to three DNS servers, as well as the host name and domain for the device.

Time Settings

You can set the time for a Defense Center either manually or via network time protocol (NTP) from an NTP server.

You can also specify the time zone used on the local web interface for the `admin` account. Click the current time zone to change it using a pop-up window.

Recurring Rule Update Imports

License: Protection

As new vulnerabilities become known, the Vulnerability Research Team (VRT) releases intrusion rule updates. Rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates may also delete rules and provide new rule categories and system variables.

If you plan to perform intrusion detection and prevention in your deployment, Cisco recommends that you **Enable Recurring Rule Update Imports**.

You can specify the **Import Frequency**, as well as configure the system to perform an intrusion **Policy Reapply** after each rule update. To perform a rule update as part of the initial configuration process, select **Install Now**.

Note Rule updates may contain new binaries. Make sure your process for downloading and installing rule updates complies with your security policies. In addition, rule updates may be large, so make sure to import rules during periods of low network use.

Recurring Geolocation Updates

Supported Defense Centers: Any except DC500

You can use most Defense Centers to view geographical information about the routed IP addresses associated with events generated by the system, as well as monitor geolocation statistics in the dashboard and Context Explorer.

The Defense Center's geolocation database (GeoDB) contains information such as an IP address's associated Internet service provider (ISP), connection type, proxy information, and exact location. Enabling regular GeoDB updates ensures that the system uses up-to-date geolocation information. If you plan to perform geolocation-related analysis in your deployment, Cisco recommends that you **Enable Recurring Weekly Updates**.

You can specify the weekly update frequency for the GeoDB. Click the time zone to change it using a pop-up window. To download the database as part of the initial configuration process, select **Install Now**.

Note GeoDB updates may be large and may take up to 45 minutes to install after download. You should update the GeoDB during periods of low network use.

Automatic Backups

The Defense Center provides a mechanism for archiving data so configurations can be restored in case of failure. As part of the initial setup, you can **Enable Automatic Backups**.

Enabling this setting creates a scheduled task that creates a weekly backup of the configurations on the Defense Center.

License Settings

You can license a variety of features to create an optimal FireSIGHT System deployment for your organization. A FireSIGHT license on the Defense Center is required to perform host, application, and user discovery. Additional model-specific licenses allow your managed devices to perform a variety of functions. Because of architecture and resource limitations, not all licenses can be applied to all managed devices; see Supported Capabilities by Managed Device Model, page 1-8 and Licensing the FireSIGHT System, page 1-13.

Cisco recommends that you use the initial setup page to add the licenses your organization has purchased. If you do not add licenses now, any devices you register during initial setup are added to the Defense Center as unlicensed; you must license each of them individually after the initial setup process is over. Note that if you are setting up a reimaged appliance and you kept your license settings as part of the restore process, this section may be prepopulated.

If you have not already obtained your licenses, click the link to navigate to `https://keyserver.sourcefire.com/` and follow the on-screen instructions. You need your license key (listed on the initial setup page), as well as the activation key previously emailed to the contact associated with your support contract.

Add a license by pasting it into the text box and clicking **Add/Verify**. After you add a valid license, the page updates so you can track which licenses you have added. Add licenses one at a time.

Device Registration

A Defense Center can manage any device, physical or virtual, currently supported by the FireSIGHT System.

Note You **must** configure remote management on the device before you can register the device to a Defense Center.

You can add most pre-registered devices (see Remote Management, page 5-9) to the Defense Center during the initial setup process. However, if a device and the Defense Center are separated by a NAT device, you must add it after the setup process completes.

Note You must configure both traffic channels to use the same management interface when you use a non-default management interface to connect your Defense Center and managed device and those appliances are separated by a NAT device. See Deploying on a Management Network, page 2-1 for more information.

When you register a managed device to a Defense Center, leave the **Apply Default Access Control Policies** check box enabled if you want to automatically apply access control policies to devices upon registration. Note that you cannot choose which policy the Defense Center applies to each device, only whether to apply them. The policy that is applied to each device depends on the detection mode (see Detection Mode, page 5-10) you chose when configuring the device, as listed in the following table.

Table 5-2 Default Access Control Policy Applied Per Detection Mode

Detection Mode	Default Access Control Policy
Inline	Default Intrusion Prevention
Passive	Default Intrusion Prevention
Access Control	Default Access Control
Network Discovery	Default Network Discovery

An exception occurs if you previously managed a device with a Defense Center and you changed the device's initial interface configuration. In this case, the policy applied by this new Defense Center page depends on the changed (current) configuration of the device. If there are interfaces configured, the Defense Center applies the Default Intrusion Prevention policy. Otherwise, the Defense Center applies the Default Access Control policy.

Note If a device is incompatible with an access control policy, the policy apply fails. This incompatibility could occur for multiple reasons, including licensing mismatches, model restrictions, passive vs inline issues, and other misconfigurations. If the initial access control policy apply fails, the initial network discovery policy apply also fails. After you resolve the issue that caused the failure, you must manually apply access control and network discovery policies to the device. For more information about issues that could cause access control policy apply to fail, see the *FireSIGHT System User Guide*.

To add a device, type its **Hostname** or **IP Address**, as well as the **Registration Key** you specified when you registered the device. Remember this is a simple key that you specified, up to 37 characters in length, and is not the same as a license key.

Then, use the check boxes to add licensed capabilities to the device. You can only select licenses you have already added to the Defense Center; see License Settings, page 5-14.

Because of architecture and resource limitations, not all licenses are supported on all managed devices. However, the setup page does **not** prevent you from enabling unsupported licenses on managed devices, or enabling a capability for which you do not have a model-specific license. This is because the Defense Center does not determine the device model until later. The system cannot enable an invalid license, and attempting to enable an invalid license does not decrement your available license count.

For more information on licensing, including which Defense Centers you can use to apply each license to each device model, see Supported Capabilities by Defense Center Model, page 1-7, Supported Capabilities by Managed Device Model, page 1-8, and Licensing the FireSIGHT System, page 1-13.

After you enable licenses, click **Add** to save the device's registration settings and, optionally, add more devices. If you selected the wrong options or mis-typed a device name, click **Delete** to remove it. You can then re-add the device.

End User License Agreement

Read the EULA carefully and, if you agree to abide by its provisions, select the check box. Make sure that all the information you provided is correct, and click **Apply**.

The Defense Center is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the `admin` user, which has the Administrator role. Continue with step 3 in Initial Setup Page: Defense Centers, page 5-11 to complete the initial setup of the Defense Center.

Next Steps

After you complete the initial setup process for an appliance and verify its success, Cisco recommends that you complete various administrative tasks that make your deployment easier to manage. You should also complete any tasks you skipped during the initial setup, such as device registration and licensing. For detailed information on any the tasks described in the following sections, as well as information on how you can begin to configure your deployment, see the *FireSIGHT System User Guide*.

Tip If you want to use a serial or LOM/SOL connection to access your appliance's console, you should redirect console output; see Testing an Inline Bypass Interface Installation, page 4-27. If you want to use LOM specifically, you must enable the feature as well as enable at least one LOM user; see Enabling LOM and LOM Users, page 8-19.

Individual User Accounts

After you complete the initial setup, the only user on the system is the `admin` user, which has the Administrator role and access. Users with that role have full menu and configuration access to the system, including via the shell or CLI. Cisco recommends that you limit the use of the `admin` account (and the Administrator role) for security and auditing reasons.

Creating a separate account for each person who will use the system allows your organization not only to audit actions and changes made by each user, but also to limit each person's associated user access role or roles. This is especially important on the Defense Center, where you perform most of your configuration and analysis tasks. For example, an analyst needs access to event data to analyze the security of your network, but may not require access to administrative functions for the deployment.

The system includes ten predefined user roles designed for a variety of administrators and analysts. You can also create custom user roles with specialized access privileges.

Health and System Policies

By default, all appliances have an initial system policy applied. The system policy governs settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. Cisco recommends that you use the Defense Center to apply the same system policy to itself and all the devices it manages.

By default, the Defense Center also has a health policy applied. A health policy, as part of the health monitoring feature, provides the criteria for the system continuously monitoring the performance of the appliances in your deployment. Cisco recommends that you use the Defense Center to apply a health policy to all the devices it manages.

Software and Database Updates

You should update the system software on your appliances before you begin any deployment. Cisco recommends that all the appliances in your deployment run the most recent version of the FireSIGHT System. If you are using them in your deployment, you should also install the latest intrusion rule updates, VDB, and GeoDB.

Caution Before you update any part of the FireSIGHT System, you **must** read the release notes or advisory text that accompanies the update. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.