Setting Up Virtual Appliances

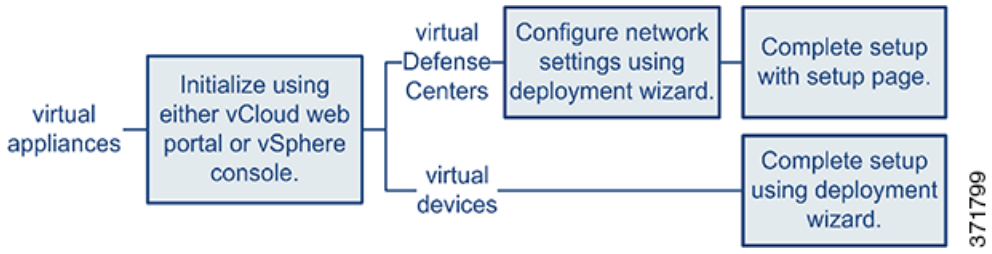
After you install a virtual appliance, you must complete a setup process that allows the new appliance to communicate on your trusted management network. You must also change the administrator password and accept the end user license agreement (EULA).

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.

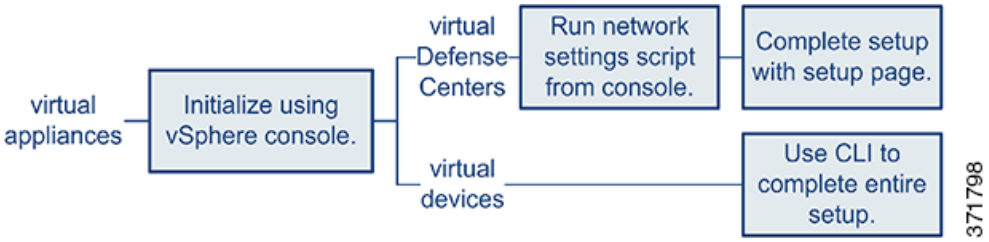
VI OVF Template Deployment

The following diagram shows the general process of setting up virtual Defense Centers and managed devices when you deploy with a VI OVF template.



ESXi OVF Template Deployment

The following diagram shows the general process of setting up virtual Defense Centers and managed devices when you deploy with a ESXi OVF template.



Regardless of how you deploy, begin by powering on the appliance to initialize it. After initialization completes, log in using the VMware console and complete the setup in one of the following ways, depending on the appliance type:

Virtual Devices

Virtual devices to not have a web interface. If you deploy with the VI OVF template, you can perform the device's initial setup, including registering it to a Defense Center, using the deployment wizard. If you deploy with the ESXi OVF template, you must use the interactive command line interface (CLI) to perform the initial setup.

Virtual Defense Centers

If you deploy with the VI OVF template, you can perform the network configuration using the wizard in the deployment. If you choose not to use the setup wizard or you deploy with the ESXi OVF template, configure network settings using a script. After your network is configured, complete the setup process using a computer on your management network to browse to the Defense Center's web interface.

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.

For more information, see:

- Initializing a Virtual Appliance, page 5-2
- Setting Up a Virtual Device Using the CLI, page 5-3
- Setting Up a Virtual Defense Center, page 5-6
- Enabling VMware Tools, page 5-12
- Next Steps, page 5-13

Initializing a Virtual Appliance

After you install a virtual appliance, initialization starts automatically when you power on the virtual appliance for the first time.

Caution Startup time depends on a number of factors, including server resource availability. It can take up to 40 minutes for the initialization to complete. Do **not** interrupt the initialization or you may have to delete the appliance and begin again.

Use the following procedure to initialize a virtual appliance.

To initialize a virtual appliance:

Step 1 Power on the appliance:

- In the VMware vCloud Director web portal, select the vApp from the display, then click **Start**.
- In the vSphere Client, right-click the name of your imported virtual appliance from the inventory list, then select **Power > Power On** from the context menu.

Step 2 Monitor the initialization on the VMware console tab.

Messages appear during the two lengthiest portions of the process. After the process concludes, a login prompt appears.

Your next step depends on the appliance type and deployment.

If you used a VI OVF template and configured your FireSIGHT System-required settings during deployment:

- For the virtual Defense Center, continue with Setting Up a Virtual Defense Center, page 5-6 to complete the setup.
- For the virtual device, no further configuration is required.

If you used an ESXi OVF template or you did not configure FireSIGHT System-required settings when you deployed with the VI OVF template:

- For the virtual Defense Center, continue with Setting Up a Virtual Defense Center, page 5-6 to set up a virtual Defense Center by configuring its network settings using a script.
- For the virtual device, continue with Setting Up a Virtual Device Using the CLI, page 5-3 to set up a virtual device using the CLI.

Setting Up a Virtual Device Using the CLI

Because virtual devices do not have web interfaces, you must set up a virtual device using the CLI if you deployed with an ESXi OVF template. You can also use the CLI to configure FireSIGHT System-required settings if you deployed with a VI OVF template and did not use the setup wizard during deployment.

Tip If you deployed with a VI OVF template and used the setup wizard, your virtual device is configured and no further action is required.

When you first log into a newly configured device, you must read and accept the EULA. Then, follow the setup prompts to change the administrator password, and configure the device's network settings and detection mode.

When following the setup 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 CLI prompts you for much of the same setup information that a physical device's setup web page does. For more information, see the *FireSIGHT System Installation Guide*.

Tip To change any of these settings for a virtual device after you complete the initial setup, you must use the CLI. For more information, see the Command Line Reference chapter in the *FireSIGHT System User Guide*.

Understanding Device Network Settings

The FireSIGHT System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway. You can also specify up to three DNS servers, as well as the host name and domain for the device. Note that the host name is not reflected in the syslog until after you reboot the device.

Understanding Detection Modes

The detection mode you choose for a virtual 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, virtual devices can perform network-based file and malware detection, and Security Intelligence monitoring, as well as network discovery.

Inline

Choose this mode if your device is deployed inline, as an intrusion prevention system (IPS).

Note Although general practice in IPS deployments is to fail open and allow non-matching traffic, inline sets on virtual devices lack bypass capability.

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
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 add the device to the Defense Center. At that time, if the appropriate zone (Internal, External, or Passive) already exists on the Defense Center, the system 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*.

To set up a virtual device using its CLI:

Access: Admin

Step 1 Log into the virtual device at the VMware console using `admin` as the username and the new admin account password that you specified in the deployment setup wizard.

If you did not change the password using the wizard or you are deploying with a ESXi OVF template, use `Cisco` as the password.

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 the Configuration CLI access level, 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.

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`.

The VMware console may display messages as your settings are implemented.

Step 5 Specify the detection mode based on how you deployed the device.

The VMware 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 6 To use the CLI to register the device to the Defense Center that will manage it, continue with the next section, Registering a Virtual Device to a Defense Center, page 5-5.

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.

Registering a Virtual Device to a Defense Center

Because virtual devices do not have web interfaces, you must use the CLI to register a virtual device to a Defense Center, which can be physical or virtual. 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 self-generated alphanumeric registration key is always required to register a device to a Defense Center. This is a simple key that you specify, and is not the same as a license key.

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

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

where *`XXX.XXX.XXX.XXX`* is the IP address of the managing Defense Center and *`my_reg_key`* is the registration key you entered for the virtual device.

Note When using the vSphere Client to register a virtual device to a Defense Center, you must use the IP address (not the hostname) of the managing Defense Center.

However, if the device and the Defense Center are separated by a Network Address Translation (NAT) device, enter a unique NAT ID along with the registration key, and specify `DONTRESOLVE` instead of the IP address, for example:

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

where *my_reg_key* is the registration key you entered for the virtual device and *my_nat_id* is the NAT ID of the NAT device.

To register a virtual device to a Defense Center:

Access: CLI Configuration

Step 1 Log into the virtual device as a user with CLI Configuration (Administrator) privileges:

- If you are performing the initial setup from the VMware console, you are already logged in as the `admin` user, which has the required access level.
- Otherwise, log into the device using the VMware console, or, if you have already configured network settings for the device, 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 the IP address of the Defense Center. If the Defense Center is not directly addressable, use `DONTRESOLVE`.
- *reg_key* is the unique alphanumeric registration key 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.

Step 4 Your next step depends on whether you have already set up the managing Defense Center, and on the Defense Center's model:

- If you have already set up the Defense Center, log into its web interface and use the Device Management (**Devices > Device Management**) page to add the device. For more information, see the Managing Devices chapter in the *FireSIGHT System User Guide*.
- If you have not already set up the Defense Center, see Setting Up a Virtual Defense Center, page 5-6 for a virtual Defense Center, or see the *FireSIGHT System Installation Guide* for a physical Defense Center.

Setting Up a Virtual Defense Center

The steps required to set up a virtual Defense Center depend on whether you deployed with a VI OVF template or an ESXi OVF template:

- If you deployed with a VI OVF template and used the setup wizard, log into the virtual Defense Center using the password you set when you configured the FireSIGHT System-required settings, then use the FireSIGHT System to set local appliance configurations, add licenses and devices, and apply policies to monitor and manage traffic. See the *FireSIGHT System User Guide* for more information.
- If you deployed with an ESXi OVF template or did not configure FireSIGHT System-required settings when deploying with a VI OVF template deployment, setting up a virtual Defense Center is a two-step process. After you initialize the virtual Defense Center, run a script at the VMware

console that helps you configure the appliance to communicate on your management network. Then, complete the setup process using a computer on your management network to browse to the appliance's web interface.

- If you deploy the virtual Defense Center with the ESXi OVF template and deploy all the virtual devices with the VI OVF template, you can register all the devices at the same time to the virtual Defense Center through the one page setup wizard. See Initial Setup Page: Virtual Defense Centers, page 5-8 for more information.

For more information, see:

- Automating Virtual Defense Center Network Settings, page 5-7
- Initial Setup Page: Virtual Defense Centers, page 5-8

Automating Virtual Defense Center Network Settings

After you initialize a new virtual Defense Center, you must configure settings that allow the appliance to communicate on your management network. Complete this step by running a script at the VMware 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.

To configure the Defense Center's network settings using a script:

Access: Admin

Step 1 After the initialization process completes, log into the virtual Defense Center at the VMware console using `admin` as the username and the password for the admin account that you specified in the setup wizard when you deployed with a VI OVF template.

If you did not change the password using the wizard, or you are deploying with an ESXi OVF template, use `Cisco` as the password.

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

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

Step 3 Follow the script's prompts.

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`.

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 VMware console may display messages as your settings are implemented.

Step 5 Log out of the appliance.

Step 6 Continue with Initial Setup Page: Virtual Defense Centers, page 5-8 to complete the setup using the Defense Center's web interface.

Initial Setup Page: Virtual Defense Centers

For virtual 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 have not 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.

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

Access: Admin

Step 1 From a computer on your management network, direct a supported browser to `https://DC_name/`, where *DC_name* is the host name or IP address you assigned to the Defense Center's management interface in the previous procedure.

The login page appears.

Step 2 Log in using `admin` as the username and the password for the admin account that you specified in the setup wizard with a VI OVF template deployment. If you did not change the password using the wizard, use `Cisco` as the password.

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

- Change Password, page 5-9
- Network Settings, page 5-9
- Time Settings, page 5-9
- Recurring Rule Update Imports, page 5-9
- Recurring Geolocation Updates, page 5-10
- Automatic Backups, page 5-10
- License Settings, page 5-10
- Device Registration, page 5-11
- Enabling VMware Tools, page 5-12
- End User License Agreement, page 5-12

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.

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 any 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 5-13.

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. Because you already used a script to configure the network settings, this section of the page should be pre-populated.

If you want to change the pre-populated settings, remember that 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.

Cisco recommends that you use a physical NTP server to set your time.

Recurring Rule Update Imports

As new vulnerabilities become known, the Cisco 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

You can use virtual 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 Understanding Virtual Appliance Capabilities, page 1-3 and Licensing Virtual Appliances, page 1-11.

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 then license each of them individually after the initial setup process is over.

Tip If you recreated a virtual Defense Center and used the same MAC address for its management interface as the deleted appliance, you can use your old licenses. If you could not use the same MAC address (for example, it was dynamically assigned), contact Support for new licenses.

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 **Submit License**. 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 virtual Defense Center can manage any device, physical or virtual, currently supported by the FireSIGHT System. You can add most pre-registered devices 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.

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 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.

For more information on detection modes on virtual devices, see Setting Up a Virtual Device Using the CLI, page 5-3; for physical devices, see the *FireSIGHT System Installation Guide*.

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, and is not the same as a license key.

Then, use the check boxes to add licensed capabilities to the device. Note that you can only select licenses you have already added to the Defense Center. Also, you cannot enable certain licenses until you enable others. For example, you cannot enable Control on a device until you first enable Protection.

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. 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, see Understanding Virtual Appliance Capabilities, page 1-3 and Licensing Virtual Appliances, page 1-11.

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: Virtual Defense Centers, page 5-8 to complete the initial setup of the Defense Center.

Enabling VMware Tools

VMware Tools is a suite of utilities installed in the operating system of a virtual machine to enhance the performance of the virtual machine and to make possible many of the ease-of-use features of VMware products. The system supports the following plugins on all virtual appliances:

- guestInfo
- powerOps
- timeSync
- vmbackup

For more information on the supported plugins and full functionality of VMware Tools, see the VMware website (http://www.vmware.com/).

After you setup your virtual appliance, you can enable VMware Tools on your virtual appliances on your managed device using the command line interface (CLI) or on your virtual Defense Center using your browser. For more information, see the following sections:

- Configuring VMware Tools on a Virtual Device, page 5-13
- Configuring VMware Tools on a Virtual Defense Center, page 5-13

Configuring VMware Tools on a Virtual Device

You can log into the virtual device and enter one or more of the following commands:

- `show vmware-tools` displays whether VMware Tools are running on the system.
- `configure vmware-tools enable` </code> enables VMware Tools on the virtual device.
- `configure vmware-tools disable` disables VMware Tools on the virtual device.

To enable VMware Tools on a virtual device:

Access: Admin

Step 1 At the console, log into the virtual device and, at the CLI prompt, enter the appropriate command to enable or disable VMware Tools, or display whether VMware Tools is enabled, and press **Enter**.

A message displays on the console indicating whether VMware Tools is running, enabled, or disabled.

Configuring VMware Tools on a Virtual Defense Center

You can select or clear a check box on the Configuration menu using the web interface. You cannot enable VMware Tools on a virtual Defense Center using the CLI.

To enable or disable VMware Tools on a virtual Defense Center:

Access: Admin

Step 1 Using a web browser, log into your Defense Center and select **System > Local > Configuration > VMware Tools**, then select or clear the **Enable VMware Tools** check box and click **Save**.

A success message appears indicating that your changes have been made.

Next Steps

After you complete the initial setup process for a virtual 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 of 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*.

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.