Firewall Management Center Virtual Initial Administration and Configuration

After you complete the initial setup process for the Firewall Management Center Virtual and verify its success, we recommend 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 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 complete Secure Firewall Management Center Configuration Guide for your version.

Individual User Accounts

After you complete the initial setup, the only web interface 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. We recommend that you limit the use of the **admin** account (and the Administrator role) for security and auditing reasons. In the Firewall Management Center Virtual GUI, manage user accounts on the **System** > **Users** > **User** page.

Note The **admin** accounts for accessing the Firewall Management Center Virtual using the shell and accessing the Firewall Management Center Virtual using the web interface are not the same, and may use different passwords.

Creating a separate account for each person who uses 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 Firewall Management Center Virtual, 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 using the web interface. You can also create custom user roles with specialized access privileges.

Device Registration

The Firewall Management Center can manage any device, physical or virtual, currently supported by the system:

- Firewall Threat Defense—Provides a unified next-generation firewall and next-generation IPS device.
- Firewall Threat Defense Virtual—A 64-bit virtual device that is designed to work in multiple hypervisor environments, reduce administrative overhead, and increase operational efficiency.
- Cisco ASA with FirePOWER Services (or an ASA FirePOWER module)—Provides the first-line system policy and passes traffic to the system for discovery and access control. However, you cannot use the Firewall Management Center web interface to configure ASA FirePOWER interfaces. Cisco ASA with FirePOWER Services has a software and CLI unique to the ASA platform that you can use to install the system and to perform other platform-specific administrative tasks.
- 7000 and 8000 Series appliances—Physical devices purpose-built for the system. 7000 and 8000 Series devices have a range of throughputs, but share most of the same capabilities. In general, 8000 Series devices are more powerful than 7000 Series devices; they also support additional features such as 8000 Series fastpath rules, link aggregation, and stacking. You must configure remote management on the device before you can register the device to the Firewall Management Center.
- NGIPSv—A 64-bit virtual device deployed in the VMware VSphere environment. NGIPSv devices do not support any of the system's hardware-based features such as redundancy and resource sharing, switching, and routing.

To register managed devices to the Firewall Management Center use the **Devices** > **Device Management** page on the Firewall Management Center GUI; see the device management information in the Secure Firewall Management Center Configuration Guide for your version.

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. We recommend that you use the Firewall Management Center to apply the same system policy to itself and all the devices it manages.

By default, the Firewall Management Center also has a health policy applied. A health policy, as part of the health monitoring feature, provides the criteria for the system to continuously monitor the performance of the appliances in your deployment. We recommend that you use the Firewall Management 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. We recommend that all the appliances in your deployment run the most recent version of the 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 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.

If your Firewall Management Center is running Versions 6.5+:

As a part of configuration the Firewall Management Center establishes the following activities to keep your system up-to-date and your data backed up:

- Weekly automatic GeoDB updates
- A weekly task to download the latest software for the Firewall Management Center and its managed devices

Important This task only downloads software updates to the Firewall Management Center. It is your responsibility to install any updates this task downloads. See the *Cisco Secure Firewall Management Center Upgrade Guide* for more information.

- A weekly task to perform a locally-stored configuration-only the Firewall Management Center backup

If your Firewall Management Center is running Versions 6.6+, as a part of initial configuration the Firewall Management Center downloads and installs the latest vulnerability (VDB) update from the Cisco support site. This is a one-time operation.

You can observe the status of these activities using the web interface Message Center. If the system fails to configure any of these activities and your Firewall Management Center has internet access, we recommend you configure these activities yourself as described in the *Secure Firewall Management Center Configuration Guide* for your version.

Troubleshooting

This section provides you with some basic troubleshooting steps related to your Firewall Management Center Virtual deployment on your virtual machine.

SSH Connection Failure

The Firewall Management Center Virtual is fully operational, with the user interface and console connection functioning correctly, except for the SSH connection. In certain scenarios, the SSH host key files might become corrupted during the initial boot of the Firewall Management Center Virtual, resulting in SSH connection failures.

You can check for the following indications that suggest an SSH connection failure:

1. A disk I/O error might occur during the initial boot of the Firewall Management Center Virtual, specifically when the SSH daemon (sshd) is starting. This results in the SSH key files (ssh_host* files generated by sshd) being empty.

```
ls -lrt /etc/ssh total 16

-rw-r--r-- 1 root root 1746 Jan 17 23:31 ssh_config-openssh
-rw-r--r-- 1 root root 6027 Jan 17 23:42 sshd_config
-rw-r--r-- 1 root root 1293 Jan 17 23:42 ssh_config
```

```
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key.pub
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key.pub
```

2. For the disk I/O issue, you can check the `/var/log/messages` file, which may contain erroneous data (indicating an I/O error) around the same timestamp when the SSH key files were generated.

To resolve the SSH failure that might occur during the initial boot of Firewall Management Center Virtual, as described above, you should perform the following steps:

1. Log in to Firewall Management Center Virtual.
2. Run the **sudo reboot** command in **expert** mode on the Firewall Management Center Virtual CLI to initiate a graceful reboot.
3. Run the following command to remove the empty SSH key files:

```
cd /etc/ssh/
rm ssh_host*
```

4. Run the following command to restart the `sshd` service to regenerate the SSH key files properly.

```
/etc/rc.d/init.d/sshd stop
/etc/rc.d/init.d/sshd start
```

Note Follow this workaround steps only if you are certain that the SSH key files are empty. If you are uncertain, it is advisable to submit a TAC case for further investigation.