CHAPTER 9

Configuring Basic Settings

This chapter describes how to configure basic settings on your ASASM that are typically required for a functioning configuration. This chapter includes the following sections:

- Configuring the Hostname, Domain Name, and Passwords, page 9-1
- Configuring the Master Passphrase, page 9-3
- Configuring the DNS Server, page 9-8

Configuring the Hostname, Domain Name, and Passwords

This section describes how to change the device name and passwords, and includes the following topics:

- Changing the Login Password, page 9-1
- Changing the Enable Password, page 9-2
- Setting the Hostname, page 9-2
- Setting the Domain Name, page 9-3

Changing the Login Password

To change the login password, enter the following command:

```
(passwd | password) password
```

Changes the login password. The login password is used for Telnet and SSH connections. The default login password is “cisco.”

You can enter `passwd` or `password`. The password is a case-sensitive password of up to 16 alphanumeric and special characters. You can use any character in the password except a question mark or a space.

The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. Use the `no password` command to restore the password to the default setting.
Changing the Enable Password

To change the enable password, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable password password</code></td>
<td>Changes the enable password, which lets you enter privileged EXEC mode. By default, the enable password is blank.</td>
</tr>
</tbody>
</table>

**Example:**

```
hostname(config)# passwd Pa$$w0rd
```

The `password` argument is a case-sensitive password of up to 16 alphanumeric and special characters. You can use any character in the password except a question mark or a space.

This command changes the password for the highest privilege level. If you configure local command authorization, you can set enable passwords for each privilege level from 0 to 15.

The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. Enter the `enable password` command without a password to set the password to the default, which is blank.

Setting the Hostname

To set the hostname, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hostname name</code></td>
<td>Specifies the hostname for the ASASM or for a context.</td>
</tr>
</tbody>
</table>

**Example:**

```
hostname(config)# hostname farscape
farscape(config)#
```

This name can be up to 63 characters. A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen.

When you set a hostname for the ASASM, that name appears in the command line prompt. If you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands. The default hostname depends on your platform.

For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts. The hostname that you optionally set within a context does not appear in the command line, but can be used by the `banner` command `$(hostname)` token.
Setting the Domain Name

To set the domain name, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-name <em>name</em></td>
<td>Specifies the domain name for the ASASM.</td>
</tr>
<tr>
<td></td>
<td>The ASASM appends the domain name as a suffix to unqualified names.</td>
</tr>
<tr>
<td></td>
<td>For example, if you set the domain name to “example.com,” and specify</td>
</tr>
<tr>
<td></td>
<td>a syslog server by the unqualified name of “jupiter,” then the ASASM</td>
</tr>
<tr>
<td></td>
<td>qualifies the name to “jupiter.example.com.”</td>
</tr>
<tr>
<td>hostname(config)# domain-name example.com</td>
<td>The default domain name is default.domain.invalid.</td>
</tr>
<tr>
<td></td>
<td>For multiple context mode, you can set the domain name for each context,</td>
</tr>
<tr>
<td></td>
<td>as well as within the system execution space.</td>
</tr>
</tbody>
</table>

Configuring the Master Passphrase

This section describes how to configure the master passphrase and includes the following topics:

- Information About the Master Passphrase, page 9-3
- Licensing Requirements for the Master Passphrase, page 9-4
- Guidelines and Limitations, page 9-4
- Adding or Changing the Master Passphrase, page 9-4
- Disabling the Master Passphrase, page 9-6
- Recovering the Master Passphrase, page 9-7
- Feature History for the Master Passphrase, page 9-8

Information About the Master Passphrase

The master passphrase feature allows you to securely store plain text passwords in encrypted format. The master passphrase provides a key that is used to universally encrypt or mask all passwords, without changing any functionality. Features that implement the master passphrase include the following:

- OSPF
- EIGRP
- VPN load balancing
- VPN (remote access and site-to-site)
- Failover
- AAA servers
- Logging
- Shared licenses
Licensing Requirements for the Master Passphrase

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>All models</td>
<td>Base License.</td>
</tr>
</tbody>
</table>

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

**Context Mode Guidelines**

Supported in single and multiple context mode.

Adding or Changing the Master Passphrase

This section describes how to add or change the master passphrase.

**Prerequisites**

- If failover is enabled but no failover shared key is set, an error message appears if you change the master passphrase, informing you that you must enter a failover shared key to protect the master passphrase changes from being sent as plain text.
- This procedure will only be accepted in a secure session, for example by console, SSH, or ASDM via HTTPS.

To add or change the master passphrase, perform the following steps:
## Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Sets the passphrase used for generating the encryption key. The passphrase must be between 8 and 128 characters long. All characters except a back space and double quotes are accepted for the passphrase.</td>
</tr>
<tr>
<td><code>key config-key password-encryption</code></td>
<td>If you do not enter the new passphrase in the command, you are prompted for it.</td>
</tr>
</tbody>
</table>
| `[
| new_passphrase `| If you later disable password encryption using the `no password encryption aes` command, all existing encrypted passwords are left unchanged, and as long as the master passphrase exists, the encrypted passwords will be decrypted, as required by the application. |
| `old_passphrase]`| When you want to change the passphrase, you also have to enter the old passphrase.                                                      |
| Example:                                     | See the “Examples” section on page 9-6 for examples of the interactive prompts.                                                        |
| `hostname(config)# key config-key password-encryption` | Note Use the interactive prompts to enter passwords to avoid having the passwords logged in the command history buffer.                   |
| `Old key: bumblebee` | Use the `no key config-key password-encryption` command with caution, because it changes the encrypted passwords into plain text passwords. You can use the `no` form of this command when downgrading to a software version that does not support password encryption. |
| `New key: haverford`                        |                                                                                                                                       |
| `Confirm key: haverford`                     |                                                                                                                                       |
| **Step 2**                                   | Enables password encryption. As soon as password encryption is turned on and the master passphrase is available, all the user passwords will be encrypted. The running configuration will show the passwords in the encrypted format. |
| `password encryption aes`                   | If the passphrase is not configured at the time that password encryption is enabled, the command will succeed in anticipation that the passphrase will be available in the future. |
| Example:                                     | If you later disable password encryption using the `no password encryption aes` command, all existing encrypted passwords are left unchanged, and as long as the master passphrase exists, the encrypted passwords will be decrypted, as required by the application. |
| `hostname(config)# password encryption aes` |                                                                                                                                       |
| **Step 3**                                   | Saves the runtime value of the master passphrase and the resulting configuration. If you do not enter this command, passwords in startup configuration may still be visible if they were not saved with encryption before. |
| `write memory`                               | In addition, in multiple context mode the master passphrase is changed in the system context configuration. As a result, the passwords in all contexts will be affected. If the `write memory` command is not entered in the system context mode, but not in all user contexts, then the encrypted passwords in user contexts may be stale. Alternatively, use the `write memory all` command in the system context to save all configurations. |
| Example:                                     |                                                                                                                                       |
| `hostname(config)# write memory`             |                                                                                                                                       |
Examples

In the following configuration example, no previous key is present:

```
hostname (config)# key config-key password-encryption 12345678
```

In the following configuration example, a key already exists:

```
Hostname (config)# key config-key password-encryption 23456789
Old key: 12345678
hostname (config)#
```

In the following configuration example, you want to key in interactively, but a key already exists. The Old key, New key, and Confirm key prompts will appear on your screen if you enter the `key config-key password-encryption` command and press `Enter` to access interactive mode.

```
hostname (config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

In the following example, you want to key in interactively, but no key is present. The New key and Confirm key prompts will appear on your screen if you are in interactive mode.

```
hostname (config)# key config-key password-encryption
New key: 12345678
Confirm key: 12345678
```

Disabling the Master Passphrase

Disabling the master passphrase reverts encrypted passwords into plain text passwords. Removing the passphrase might be useful if you downgrade to a previous software version that does not support encrypted passwords.

Prerequisites

- You must know the current master passphrase to disable it. If you do not know the passphrase, see the “Recovering the Master Passphrase” section on page 9-7.
- This procedure will only be accepted in a secure session, that is, by Telnet, SSH, or ASDM via HTTPS.
Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
   *no key config-key password-encryption [old_passphrase]*)  
   **Example:**  
   hostname(config)# no key config-key password-encryption  
   Warning! You have chosen to revert the encrypted passwords to plain text. This operation will expose passwords in the configuration and therefore exercise caution while viewing, storing, and copying configuration.  
   Old key: bumblebee  
   Removes the master passphrase.  
   If you do not enter the passphrase in the command, you are prompted for it. |
| **Step 2**  
   *write memory*  
   **Example:**  
   hostname(config)# write memory  
   Saves the run time value of the master passphrase and the resulting configuration. The non-volatile memory containing the passphrase will be erased and overwritten with the 0xFF pattern.  
   In multiple mode the master passphrase is changed in the system context configuration. As a result the passwords in all contexts will be affected. If the **write memory** command is not entered in the system context mode, but not in all user contexts, then the encrypted passwords in user contexts may be stale. Alternatively, use the **write memory all** command in the system context to save all configurations. |

**Recovering the Master Passphrase**

You cannot recover the master passphrase.

If the master passphrase is lost or unknown, you can remove it using the **write erase** command followed by the **reload** command. These commands remove the master key and the configuration that includes the encrypted passwords.
Feature History for the Master Passphrase

Table 9-1 lists each feature change and the platform release in which it was implemented.

### Table 9-1 Feature History for the Master Passphrase

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Passphrase</td>
<td>8.3(1)</td>
<td>This feature was introduced. We introduced the following commands: key config-key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>password-encryption, password encryption aes, clear configure password encryption aes,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>show running-config password encryption aes, show password encryption.</td>
</tr>
<tr>
<td>Password Encryption Visibility</td>
<td>8.4(1)</td>
<td>We modified the show password encryption command.</td>
</tr>
</tbody>
</table>

### Configuring the DNS Server

Some ASASM features require use of a DNS server to access external servers by domain name; for example, the Botnet Traffic Filter feature requires a DNS server to access the dynamic database server and to resolve entries in the static database. Other features, such as the ping or traceroute command, let you enter a name that you want to ping or traceroute, and the ASASM can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names.

**Note**
The ASASM has limited support for using the DNS server, depending on the feature. For example, most commands require you to enter an IP address and can only use a name when you manually configure the name command to associate a name with an IP address and enable use of the names using the names command.

For information about dynamic DNS, see the “Configuring DDNS” section on page 11-2.

### Prerequisites

Make sure that you configure the appropriate routing for any interface on which you enable DNS domain lookup so you can reach the DNS server. See the “Information About Routing” section on page 19-1 for more information about routing.

### Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>dns domain-lookup interface_name</td>
<td>Enables the ASASM to send DNS requests to a DNS server to perform a name lookup for supported commands.</td>
</tr>
</tbody>
</table>

**Example:**

hostname(config)# dns domain-lookup inside
Monitoring DNS Cache

The ASASM provides a local cache of DNS information from external DNS queries that are sent for certain clientless SSL VPN and certificate commands. Each DNS translation request is first looked for in the local cache. If the local cache has the information, the resulting IP address is returned. If the local cache cannot resolve the request, a DNS query is sent to the various DNS servers that have been configured. If an external DNS server resolves the request, the resulting IP address is stored in the local cache with its corresponding hostname.

DNS Cache Monitoring Commands

To monitor the DNS cache, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dns-hosts</td>
<td>Show the DNS cache, which includes dynamically learned entries from a DNS server as well as manually entered name and IP addresses using the name command.</td>
</tr>
</tbody>
</table>

Feature History for DNS Cache

Table 2 lists each feature change and the platform release in which it was implemented.

Table 2  Feature History for DNS Cache

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Cache</td>
<td>7.0(1)</td>
<td>DNS cache stores responses that allow a DNS server to respond more quickly to queries. We introduced the following command: show dns host.</td>
</tr>
</tbody>
</table>