



Configuring Basic Settings

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

- [Changing the Passwords, page 7-1](#)
- [Setting the Hostname, page 7-3](#)
- [Setting the Domain Name, page 7-4](#)
- [Setting the Prompt, page 7-4](#)
- [Configuring a Login Banner, page 7-5](#)
- [Configuring Connection Limits for Transparent Firewall Mode and Non-NAT Configurations, page 7-5](#)

Changing the Passwords

This section describes how to change the login and enable passwords and includes the following topics:

- [Changing the Login Password, page 7-1](#)
- [Changing the Enable Password, page 7-2](#)
- [Changing the Maintenance Software Passwords, page 7-2](#)



Note

In multiple context mode, every context and the system execution space has its own login policies and passwords.

Changing the Login Password

The login password is used for sessions from the switch as well as Telnet and SSH connections. By default, the login password is “cisco.” To change the password, enter the following command:

```
hostname(config)# {passwd | password} password
```

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

The enable password lets you enter privileged EXEC mode. By default, the enable password is blank. To change the enable password, enter the following command:

```
enable 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.

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.

Changing the Maintenance Software Passwords

The maintenance software is valuable for troubleshooting. For example, you can install new software to an application partition, reset passwords, or show crash dump information from the maintenance software. You can only access the maintenance software by sessioning in to the FWSM.

The maintenance software has two user levels with different access privileges:

- **root**—Lets you configure the network partition parameters, upgrade the software images on the application partitions, change the guest account password, and enable or disable the guest account.
The default password is “cisco.”
- **guest**—Lets you configure the network partition parameters and show crash dump information.
The default password is “cisco.”

To change the maintenance partition passwords for both users, perform the following steps:

-
- Step 1** To reboot the FWSM into the maintenance partition, enter the following command at the switch prompt:
- ```
Router# hw-module module mod_num reset cf:1
```
- Step 2** To session in to the FWSM, enter the following command:
- ```
Router# session slot mod_num processor 1
```
- Step 3** Log in as root by entering the following command:
- ```
Login: root
```
- Step 4** Enter the password at the prompt:
- ```
Password:
```
- The default password is “cisco”.
- Step 5** Change the root password by entering the following command:
- ```
root@localhost# passwd
```
- Step 6** Enter the new password at the prompt:
- ```
Changing password for user root
New password:
```

Step 7 Enter the new password again:

```
Retype new password:
passwd: all authentication tokens updated successfully
```

Step 8 Change the guest password by entering the following command:

```
root@localhost# passwd-guest
```

Step 9 Enter the new password at the prompt:

```
Changing password for user guest
New password:
```

Step 10 Enter the new password again:

```
Retype new password:
passwd: all authentication tokens updated successfully
```

This example shows how to set the password for the root account:

```
root@localhost# passwd
Changing password for user root
New password: *sh1p
Retype new password: *sh1p
passwd: all authentication tokens updated successfully
```

This example shows how to set the password for the guest account:

```
root@localhost# passwd-guest
Changing password for user guest
New password: f1rc8t
Retype new password: f1rc8t
passwd: all authentication tokens updated successfully
```

Setting the Hostname

When you set a hostname for the FWSM, 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.

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.

To specify the hostname for the FWSM or for a context, enter the following command:

```
hostname(config)# hostname name
```

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. The FWSM supports all 95 printable characters except the question mark (?). Avoid the use of non-ASCII characters.

This name appears in the command line prompt. For example:

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

Setting the Domain Name

The FWSM appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com,” and specify a syslog server by the unqualified name of “jupiter,” then the FWSM qualifies the name to “jupiter.example.com.”

The default domain name is default.domain.invalid.

For multiple context mode, you can set the domain name for each context, as well as within the system execution space.

To specify the domain name for the FWSM, enter the following command:

```
hostname(config)# domain-name name
```

For example, to set the domain as example.com, enter the following command:

```
hostname(config)# domain-name example.com
```

Setting the Prompt

You can configure the information shown in the CLI prompt, including the hostname, context name, domain name, slot, failover status, and failover priority. In multiple context mode, you can view the extended prompt when you log into the system execution space or the admin context. Within a non-admin context, you only see the default prompt, which is the hostname and the context name.

To configure the information included in the prompt, enter the following command:

```
hostname(config)# prompt [hostname] [context] [domain] [slot] [state] [priority]
```

The order in which you enter the keywords determines the order of the elements in the prompt, which are separated by a slash (/). See the following descriptions for the keywords:

- **hostname**—Displays the hostname.
- **domain**—Displays the domain name.
- **context**—(Multiple mode only) Displays the current context.
- **priority**—Displays the failover priority as pri (primary) or sec (secondary). Set the priority using the **failover lan unit** command.
- **slot**—Displays the slot location in the switch.
- **state**—Displays the traffic-passing state of the unit. The following values are displayed for the **state** keyword:
 - act—Failover is enabled, and the unit is actively passing traffic.
 - stby— Failover is enabled, and the unit is not passing traffic and is in a standby, failed, or other non-active state.
 - actNoFailover—Failover is not enabled, and the unit is actively passing traffic.
 - stbyNoFailover—Failover is not enabled, and the unit is not passing traffic. This might happen when there is an interface failure above the threshold on the standby unit.

For example, to show all available elements in the prompt, enter the following command:

```
hostname(config)# prompt hostname context priority slot state
```

The prompt changes to the following string:

```
hostname/admin/pri/6/act(config)#
```

Configuring a Login Banner

You can configure a message to display when a user connects to the FWSM, when a user logs in to the FWSM using Telnet, or when a user enters user EXEC mode.

To configure a login banner, enter the following command in the system execution space or within a context:

```
hostname(config)# banner {motd | login | exec} text
```

The **motd** keyword shows a banner when a user first connects.

The **login** keyword shows a banner when a user logs in to the FWSM using Telnet.

The **exec** keyword shows a banner when a user accesses user EXEC mode.

When a user connects to the FWSM, the message-of-the-day banner appears first, followed by the login banner and prompts. This banner does not appear for non-Telnet connections. After the user successfully logs in to the FWSM (for Telnet connections), the exec banner displays.

For the banner text, spaces are allowed but you cannot enter tabs using the CLI. You can dynamically add the hostname or domain name of the FWSM by including the strings **\$(hostname)** and **\$(domain)**. If you configure a banner in the system configuration, you can use that banner text within a context by using the **\$(system)** string in the context configuration.

To add more than one line, precede each line by the banner command.

For example, to add a message-of-the-day banner, enter:

```
hostname(config)# banner motd Welcome to $(hostname)
hostname(config)# banner motd Contact me at admin@example.com for any
hostname(config)# banner motd issues
```

Configuring Connection Limits for Transparent Firewall Mode and Non-NAT Configurations

The NAT configuration lets you set connection limits for traffic. For transparent firewall mode (which does not support NAT) or for routed mode configurations for which you do not want to configure NAT, you can configure static identity NAT to set these limits. Static identity NAT lets you specify the addresses for which you want to set limits, but no translation is performed. (For routed mode, you can set limits using any method for bypassing NAT, including NAT exemption. See the [“Bypassing NAT” section on page 12-30](#) for more information. For transparent mode, the FWSM supports only the following method.)

You can alternatively set connection limits (but not embryonic connection limits) using the Modular Policy Framework. See the [“Configuring Connection Limits and Timeouts” section on page 19-3](#) for more information. You can only set embryonic connection limits using NAT. If you configure these settings for the same traffic using both methods, then the FWSM uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the FWSM disables TCP sequence randomization.

Limiting the number of embryonic connections protects you from a DoS attack. The FWSM uses the embryonic limit to trigger TCP Intercept. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. TCP Intercept uses the SYN cookies algorithm to prevent TCP SYN-flooding attacks. A SYN-flooding attack consists of a series of SYN packets usually originating from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests. When the embryonic connection threshold of a connection is crossed, the FWSM acts as a proxy for the server and generates a SYN-ACK response to the client's SYN request. When the FWSM receives an ACK back from the client, it can then authenticate the client and allow the connection to the server.

To configure connection limits, enter the following command:

```
hostname(config)# static (real_interface,mapped_interface) real_ip real_ip [netmask mask]
[ dns ] [[ tcp ] tcp_max_conns [ emb_limit ] ] [ udp udp_max_conns ] [ norandomseq ]
```

Specify the same IP address for both *real_ip* arguments.

The **norandomseq** keyword disables TCP Initial Sequence Number (ISN) randomization. TCP sequence randomization should only be disabled if another in-line firewall is also randomizing sequence numbers and the result is scrambling the data. Each TCP connection has two Initial Sequence Numbers (ISNs): one generated by the client and one generated by the server. The FWSM randomizes the ISN that is generated by the host/server. At least one of the ISNs must be randomly generated so that attackers cannot predict the next ISN and potentially hijack the session.

The **tcp** *tcp_max_conns* and **udp** *udp_max_conns* keywords set the maximum number of simultaneous TCP and/or UDP connections for the entire subnet, up to 65,536. The default is 0 for both protocols, which means the maximum connections.

The *emb_limit* argument sets the maximum number of embryonic connections per host up to 65,536. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. This limit enables the TCP Intercept feature. The default is 0, which means the maximum embryonic connections. You must enter the **tcp** *tcp_max_conns* before you enter the *emb_limit*. If you want to use the default value for *tcp_max_conns*, but change the *emb_limit*, then enter **0** for *tcp_max_conns*.

For example, to set options for the host 10.1.1.1, enter the following command:

```
hostname(config)# static (inside,outside) 10.1.1.1 10.1.1.1 netmask 255.255.255.255 tcp
1000 200 udp 1000 norandomseq
```