System Settings

The following topics explain how to configure the various system settings that are grouped together on the System Settings page. The settings cover overall system function.

Configuring the Management Access List

By default, you can reach the device's Firepower Device Manager web or CLI interfaces on the management address from any IP address. System access is protected by username/password only. However, you can configure an access list to allow connections from specific IP addresses or subnets only to provide another level of protection.

You can also open data interfaces to allow Firepower Device Manager or SSH connections to the CLI. You can then manage the device without using the management address. For example, you could allow management access to the outside interface, so that you can configure the device remotely. The username/password protects against unwanted connections. By default, HTTPS management access to data interfaces is enabled on the inside interface but it is disabled on the outside interface. For device models that have a default “inside” bridge group, this means that you can make Firepower Device Manager connections through any data interface within the bridge group to the bridge group IP address (default is 192.168.1.1). You can open a management connection only on the interface through which you enter the device.

⚠

Caution If you constrain access to specific addresses, you can easily lock yourself out of the system. If you delete access for the IP address that you are currently using, and there is no entry for “any” address, you will lose access to the system when you deploy the policy. Be very careful if you decide to configure the access list.

Before you begin

You cannot configure both Firepower Device Manager access (HTTPS access) and AnyConnect remote access SSL VPN on the same interface for the same TCP port. For example, if you configure remote access SSL VPN on the outside interface, you cannot also open the outside interface for HTTPS connections on port 443. Because you cannot configure the port used by these features in Firepower Device Manager, you cannot configure both features on the same interface.

Procedure

Step 1 Click **Device**, then click the **System Settings** > **Management Access List** link.

If you are already on the System Settings page, simply click **Management Access List** in the table of contents.

Step 2 To create rules for the management address:

a) Select the **Management Interface** tab.

The list of rules defines which addresses are allowed access to the indicated port: 443 for Firepower Device Manager (the HTTPS web interface), 22 for the SSH CLI.

The rules are not an ordered list. If an IP address matches any rule for the requested port, the user is allowed to attempt logging into the device.

Note To delete a rule, click the trash can icon (🗑) for the rule. If you delete all of the rules for a protocol, no one can access the device on that interface using the protocol.

b) Click + and fill in the following options:

- **Protocol**—Select whether the rule is for HTTPS (port 443) or SSH (port 22).
- **IP Address**—Select the network object that defines the IPv4 or IPv6 network or host that should be able to access the system. To specify "any" address, select **any-ipv4** (0.0.0.0/0) and **any-ipv6** (::/0).

c) Click **OK**.

Step 3 To create rules for data interfaces:

a) Select the **Data Interfaces** tab.

The list of rules defines which addresses are allowed access to the indicated port on the interface: 443 for Firepower Device Manager (the HTTPS web interface), 22 for the SSH CLI.

The rules are not an ordered list. If an IP address matches any rule for the requested port, the user is allowed to attempt logging into the device.

Note To delete a rule, click the trash can icon (🗑) for the rule. If you delete all of the rules for a protocol, no one can access the device on that interface using the protocol.

b) Click + and fill in the following options:

- **Interface**—Select the interface on which you want to allow management access.
- **Protocols**—Select whether the rule is for HTTPS (port 443), SSH (port 22), or both. You cannot configure HTTPS rules for the outside interface if it is used in an remote access VPN connection profile.

- **Allowed Networks**—Select the network objects that define the IPv4 or IPv6 network or host that should be able to access the system. To specify "any" address, select **any-ipv4** (0.0.0.0/0) and **any-ipv6** (::/0).

c) Click **OK**.

Configuring Diagnostic Logging

Diagnostic logging provides syslog messages for events that are not related to connections. You configure connection logging within individual access control rules. The following procedure explains how to configure the logging of diagnostic messages.

Procedure

Step 1 Click **Device**, then click the **System Settings** > **Logging Settings** link.

If you are already on the System Settings page, simply click **Logging Settings** in the table of contents

Step 2 Click **Diagnostic Log Settings** > **On**.

Even if you configure the remaining fields on this page, diagnostic log messages are not generated unless you turn on this setting.

Step 3 Turn the slider to **On** for each of the locations where you want to see diagnostic log messages, and select a minimum severity level.

You can log messages to the following locations:

- **Console**—These messages appear when you log into the CLI on the Console port. You can also see these logs in an SSH session to other interfaces (including the management address) by using the **show console-output** command. In addition, you can see these messages in real time in the diagnostic CLI, enter **system support diagnostic-cli** from the main CLI.
- **Syslog**—These messages are sent to the external syslog servers that you specify. Click +, select the syslog server objects, and click **OK** in the popup dialog box. If the object for a server does not already exist, click **Add Syslog Server** to create it.

Step 4 Click **Save**.

Severity Levels

The following table lists the syslog message severity levels.

Table 1: Syslog Message Severity Levels

Level Number	Severity Level	Description
0	**emergencies**	System is unusable.

Level Number	Severity Level	Description
1	**alert**	Immediate action is needed.
2	**critical**	Critical conditions.
3	**error**	Error conditions.
4	**warning**	Warning conditions.
5	**notification**	Normal but significant conditions.
6	**informational**	Informational messages only.
7	**debugging**	Debugging messages only.

Note Firepower Threat Defense does not generate syslog messages with a severity level of zero (emergencies).

Configuring DHCP Server

A DHCP server provides network configuration parameters, such as IP addresses, to DHCP clients. You can configure a DHCP server on an interface to provide configuration parameters to DHCP clients on the attached network.

An IPv4 DHCP client uses a broadcast rather than a multicast address to reach the server. The DHCP client listens for messages on UDP port 68; the DHCP server listens for messages on UDP port 67. The DHCP server does not support BOOTP requests.

DHCP clients must be on the same network as the interface on which the server is enabled. That is, there cannot be an intervening router between the server and client, although there can be a switch.

Note Do not configure a DHCP server on a network that already has a DHCP server operating on it. The two servers will conflict and results will be unpredictable.

Procedure

Step 1 Click **Device**, then click the **System Settings** > **DHCP Server** link.

If you are already on the System Settings page, simply click **DHCP Server** in the table of contents.

The page has two tabs. Initially, the **Configuration** tab shows the global parameters.

The **DHCP Servers** tab shows the interfaces on which you have configured DHCP server, whether the server is enabled, and the address pool for the server.

Step 2 On the **Configuration** tab, configure auto-configuration and global settings.

DHCP auto configuration enables the DHCP Server to provide DHCP clients with DNS server, domain name, and WINS server information obtained from a DHCP client that is running on the specified interface. Typically, you would use auto-configuration if you are obtaining an address using DHCP on the outside interface, but you could choose any interface that obtains its address through DHCP. If you cannot use auto-configuration, you can manually define the required options.

a) Click **Enable Auto Configuration** > **On** (the slider should be on the right) if you want to use auto-configuration, and then select the interface that is obtaining its address through DHCP in **From Interface**.

b) If you do not enable auto-configuration, or if you want to override any of the automatically configured settings, configure the following global options. These settings will be sent to DHCP clients on all interfaces that host DHCP server.

- **Primary WINS IP Address**, **Secondary WINS IP Address**—The addresses of the Windows Internet Name Service (WINS) servers clients should use for NetBIOS name resolution.

- **Primary DNS IP Address**, **Secondary DNS IP Address**—The addresses of the Domain Name System (DNS) servers clients should use for domain name resolution. Click **Use OpenDNS** if you want to configure the OpenDNS public DNS servers. Clicking the button loads the appropriate IP addresses into the fields.

c) Click **Save**.

Step 3 Click the **DHCP Servers** tab and configure the servers.

a) Do one of the following:

- To configure DHCP server for an interface that is not already listed, click +.

- To edit an existing DHCP server, click the edit icon (✎) for the server.

To delete a server, click the trash can icon (🗑) for the server.

b) Configure the server properties:

- **Enable DHCP Server**—Whether to enable the server. You can configure a server but keep it disabled until you are ready to use it.

- **Interface**—Select the interface on which you will provide DHCP addresses to clients. The interface must have a static IP address; you cannot be using DHCP to obtain the interface address if you want to run a DHCP server on the interface. For bridge groups, you configure the DHCP server on the Bridge Virtual Interface (BVI), not the member interfaces, and the server operates on all member interfaces.

  You cannot configure DHCP server on the Diagnostic interface, configure it on the Management interface instead, on the **Device** > **System Settings** > **Management Interface** page.

- **Address Pool**—The range of IP addresses from lowest to highest that the server is allowed to provide to clients that request an address. Specify the start and end address for the pool, separated by a hyphen. For example, 10.100.10.12-10.100.10.250.

  The range of IP addresses must be on the same subnet as the selected interface and cannot include: the IP address of the interface itself, the broadcast address, or the subnet network address.

  The size of the address pool is limited to 256 addresses per pool on the FTD device. If the address pool range is larger than 253 addresses, the netmask of the FTD interface cannot be a Class C address (for example, 255.255.255.0) and needs to be something larger, for example, 255.255.254.0.

c) Click **OK**.

Configuring DNS

The Domain Name System (DNS) servers are used to resolve hostnames to IP addresses. These servers are used by the management interface. You configure DNS servers during initial system setup, but you can change them using the following procedure.

You can also change the DNS configuration in the CLI using the **configure network dns servers** and **configure network dns searchdomains** commands.

If you have problems with DNS resolution, see Troubleshooting DNS for the Management Interface.

Procedure

Step 1 Click **Device**, then click the **System Settings** > **DNS Server** link.

If you are already on the System Settings page, simply click **DNS Server** in the table of contents.

Step 2 In **Primary, Secondary, Tertiary DNS IP address**, enter the IP addresses of up to three DNS servers in order of preference.

The primary DNS server is used unless it cannot be contacted, in which case the secondary is tried, and finally the tertiary.

Click **Use OpenDNS** if you want to configure the OpenDNS public DNS servers. Clicking the button loads the appropriate IP addresses into the fields.

Step 3 In **Domain Search Name**, enter the domain name for your network, e.g. example.com.

This domain is added to hostnames that are not fully-qualified, for example, serverA instead of serverA.example.com.

Step 4 Click **Save**.

Configuring the Management Interface

The management interface is a virtual interface attached to the physical Management port. The physical port is named the Diagnostic interface, which you can configure on the Interfaces page with the other physical ports. On Firepower Threat Defense Virtual, this duality is maintained even though both interfaces are virtual.

The management interface has two uses:

- You can open web and SSH connections to the IP address and configure the device through the interface.
- The system obtains smart licensing and database updates through this IP address.

If you use the CLI setup wizard, you configure the management address and gateway for the device during initial system configuration. If you use the Firepower Device Manager setup wizard, the management address and gateway remain the defaults.

If necessary, you can change these addresses through Firepower Device Manager. You can also change the management address and gateway in the CLI using the **configure network ipv4 manual** and **configure network ipv6 manual** commands.

You can define static addresses, or obtain an address through DHCP if another device on the management network is acting as a DHCP server. By default, the management address is static, and a DHCP server runs on the port (except for Firepower Threat Defense Virtual, which does not have a DHCP server). Thus, you can plug a device directly into the management port and get a DHCP address for your workstation. This makes it easy to connect to and configure the device.

⚠

Caution If you change the address to which you are currently connected, you will lose access to Firepower Device Manager (or the CLI) when you save the changes, as they are applied immediately. You will need to reconnect to the device. Ensure that the new address is valid and available on the management network.

Procedure

Step 1 Click **Device**, then click the **System Settings** > **Management Interface** link.

If you are already on the System Settings page, simply click **Management Interface** in the table of contents

Step 2 Choose how you want to define the management gateway.

The gateway determines how the system can reach the Internet to obtain smart licenses, database updates (such as VDB, rule, Geolocation, URL), and to reach the management DNS and NTP servers. Choose from these options:

- **Use the Data Interfaces as the Gateway**—Select this option if you do not have a separate management network connected to the physical Management interface. Traffic is routed to the Internet based on the routing table, typically going through the outside interface. This is the default option. However, this option is not supported on Firepower Threat Defense Virtual devices.
- **Use Unique Gateways for the Management Interface**— Specify unique gateways (below) for IPv4 and IPv6 if you have a separate management network connected to the management interface.

Step 3 Configure the management address, subnet mask or IPv6 prefix, and gateway (if necessary) for IPv4, IPv6, or both.

You must configure at least one set of properties. Leave one set blank to disable that addressing method.

Select **Type** > **DHCP** to obtain the address and gateway through DHCP or IPv6 auto configuration. However, you cannot use DHCP if you are using the data interfaces as the gateway. In this case, you must use a static address.

Step 4 (Optional.) If you configure a static IPv4 address, configure a DHCP server on the port.

If you configure a DHCP server on the management port, directly-connected clients, or clients on the management network, can obtain their address from the DHCP pool. This option is not supported on Firepower Threat Defense Virtual devices.

a) Click **Enable DHCP Server** > **On**.

b) Enter the **Address Pool** for the server.

The address pool is the range of IP addresses from lowest to highest that the server is allowed to provide to clients that request an address. The range of IP addresses must be on the same subnet as the management address and cannot include: the IP address of the interface itself, the broadcast address, or the subnet network address. Specify the start and end address for the pool, separated by a hyphen. For example, 192.168.45.46-192.168.45.254.

Step 5 Click **Save**, read the warning, and click **OK**.

Configuring the Device Hostname

You can change the device hostname.

You can also change the hostname in the CLI using the **configure network hostname** command.

⚠

Caution If you change the hostname when connected to the system using the hostname, you will lose access to Firepower Device Manager when you save the changes, as they are applied immediately. You will need to reconnect to the device.

Procedure

Step 1 Click **Device**, then click the **System Settings** > **Hostname** link.

If you are already on the System Settings page, simply click **Hostname** in the table of contents

Step 2 Enter a new hostname.

Step 3 Click **Save**.

Configuring Network Time Protocol (NTP)

You must configure Network Time Protocol (NTP) servers to define the time on the system. You configure NTP servers during initial system setup, but you can change them using the following procedure. If you have problems with the NTP connection, see Troubleshooting NTP.

Procedure

Step 1 Click **Device**, then click the **System Settings** > **NTP** link.

If you are already on the System Settings page, simply click **NTP** in the table of contents

Step 2 In **NTP Time Server**, select whether you want to use your own or Cisco's time servers.

- **Default NTP Time Server**—If you select this option, the server list shows the server names that are used for NTP.
- **Manually Input**—If you select this option, enter the fully qualified domain name or IP address of the NTP server you want to use. For example, ntp1.example.com or 10.100.10.10. If you have more than one NTP server, click **Add Another NTP Time Server** and enter the address.

Step 3 Click **Save**.

Configuring URL Filtering Preferences

The system obtains the URL category and reputation database from Cisco Collective Security Intelligence (CSI). These preferences control database updates and how the system handles URLs with unknown category or reputation. You must enable the URL Filtering license to set these preferences.

Procedure

Step 1 Click **Device**, then click the **System Settings** > **URL Filtering Preferences** link.

If you are already on the System Settings page, simply click **URL Filtering Preferences** in the table of contents

Step 2 Configure the following options:

- **Enable Automatic Updates**—Allows the system to automatically check for and download updated URL data, which includes category and reputation information. The system checks for updates every 30 minutes, although the data is typically updated once per day. The default is to enable updates. If you deselect this option, and you are using category and reputation filtering, periodically enable it to get new URL data.
- **Query Cisco CSI for Unknown URLs**—Whether to check with Cisco CSI for updated information for URLs that do not have category and reputation data in the local URL filtering database. If the lookup returns this information within a reasonable time limit, it is used when selecting access rules based on URL conditions. Otherwise, the URL matches the Uncategorized category. Selecting this option is important for lower-end systems, which install a smaller URL database due to memory limitations.

Step 3 Click **Save**.

Configuring Cloud Management (Cisco Defense Orchestrator)

You can manage the device using the Cisco Defense Orchestrator cloud-based portal. Using Cisco Defense Orchestrator, you can approach device management using the following techniques:

- Initial configuration download—In this approach, you download the initial device configuration from Cisco Defense Orchestrator, but thereafter you configure the device locally using Firepower Device Manager.

Note After configuring the device using Firepower Device Manager, if you decide you want to instead manage the device through the cloud, ensure that you duplicate your local changes in the cloud-based configuration.

- Remote configuration management through the cloud—In this approach, you use Cisco Defense Orchestrator to create and update the device configuration. When using this approach, do not make local changes to the configuration, because on each cloud deployment, the configuration defined in the cloud replaces the local configuration on the device. If you make a local change, be sure to repeat the configuration in the cloud-based configuration if you want to preserve the change.

For more information about how cloud management works, refer to the Cisco Defense Orchestrator portal (http://www.cisco.com/go/cdo) or ask the reseller or partner with whom you are working.

Before you begin

Obtain a registration key for Cisco Defense Orchestrator.

Also, ensure that the device has a route to the Internet.

Procedure

Step 1 Click **Device**, then click the **System Settings** > **Cloud Management** link.

If you are already on the System Settings page, simply click **Cloud Management** in the table of contents

Step 2 Click **Get Started**.

Step 3 Paste the key in **Registration Key** and click **Connect**.

A registration request is sent to the cloud portal. If the key is valid, and there is a route to the Internet, the device should be successfully registered with the portal. You can then start using the portal to manage the device.

If you decide you no longer want to use cloud management, you can select **Unregister** from the gear drop-down list.