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 FDM 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.

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.

Procedure

Step 1 Click the name of the device in the menu, 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.

The list of rules defines which addresses are allowed access to the indicated port: 443 for the FDM (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.

Step 2 To create rules for the management address:

a) 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).

b) Click **Add**.

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 the name of the device in the menu, 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.
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. Log at this level only temporarily, when debugging issues. This log level can potentially generate so many messages that system performance can be affected.

Note ASA and FTD do 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. The FTD device can provide a DHCP server to DHCP clients attached to device interfaces. The DHCP server provides network configuration parameters directly to DHCP clients.

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.

Procedure

Step 1 Click the name of the device in the menu, 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 list shows the interfaces on which you have configured DHCP server, whether the server is enabled, and the address pool for the server.

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

Step 2 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 Server (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 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.

Step 4 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.
- **Address Pool**—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 selected interface 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, 10.100.10.12-10.100.10.250.

Step 5 Click **Add** for new servers, **Save** for existing servers.

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.

Procedure

Step 1 Click the name of the device in the menu, 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 IP Address

If you use the CLI setup wizard, you configure the management address and gateway for the device during initial system configuration. This is the address through which you access the FDM web interface and CLI.

If you use the FDM setup wizard, the management address and gateway remain the defaults.

If necessary, you can change these addresses through the FDM. You can also change the management address and gateway in the CLI using the **configure network ipv4 manual** and **configure network ipv6 manual** commands. Alternatively, you can set the management interface to use DHCP or IPv6 autoconfiguration if you configure it through the CLI.

Caution If you change the address to which you are currently connected, you will lose access to the FDM 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 the name of the device in the menu, then click the **System Settings** > **Device Management IP** link.

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

Step 2 Configure the management address, subnet mask or IPv6 prefix, and gateway for IPv4, IPv6, or both.

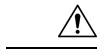
You must configure at least one set of properties. Leave one set blank to disable that addressing method.

Step 3 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 the FDM when you save the changes, as they are applied immediately. You will need to reconnect to the device.

Procedure

Step 1 Click the name of the device in the menu, 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.

The FTD device supports NTPv4.

Procedure

Step 1 Click the name of the device in the menu, 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.

- **Cisco 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 IPv4 or IPv6 address of the NTP server you want to use. For example, ntp1.example.com or 10.100.10.10. You can add up to 3 NTP servers.

Step 3 Click **Save**.

Configuring Cloud 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 the name of the device in the menu, then click the **System Settings** > **Cloud Preferences** link.

If you are already on the System Settings page, simply click **Cloud 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**.