



## 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 Management Access, on page 1](#)
- [Configuring System Logging Settings, on page 4](#)
- [Configuring the DHCP Server, on page 8](#)
- [Configuring DNS, on page 10](#)
- [Configuring the Management Interface, on page 14](#)
- [Configuring the Device Hostname, on page 15](#)
- [Configuring Network Time Protocol \(NTP\), on page 16](#)
- [Configuring URL Filtering Preferences, on page 17](#)
- [Configuring Cloud Services, on page 17](#)

## Configuring Management Access

Management access refers to the ability to log into the FTD device for configuration and monitoring purposes. You can configure the following items:

- AAA to identify the identity source to use for authenticating user access. You can use the local user database or an external AAA server. For more information about administrative user management, see [Managing FDM and FTD User Access](#).
- Access control to the management interface and to data interfaces. There are separate access lists for these interfaces. You can decide which IP addresses are allowed for HTTPS (used for the FDM) and SSH (used for CLI). See [Configuring the Management Access List, on page 1](#).
- Management Web Server certificate, which users must accept to connect to the FDM. By uploading a certificate your web browsers already trust, you can avoid users being ask to trust an unknown certificate. See [Configuring the FTD Web Server Certificate, on page 3](#).

## 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.

You can also open data interfaces to allow the FDM 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 the Firepower 1010 that has a default “inside” bridge group, this means that you can make the FDM 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 the FDM access (HTTPS access) and 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 the FDM, you cannot configure both features on the same interface.

### Procedure

---

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

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

You can also configure AAA on this page to allow management access for users defined in an external AAA server. For details, see [Managing FDM and FTD User Access](#).

**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 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.

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 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.

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 the FTD Web Server Certificate

When you log into the web interface, the system uses a digital certificate to secure communications using HTTPS. The default certificate is not trusted by your browser, so you are shown an Untrusted Authority warning and asked whether you want to trust the certificate. Although users can save the certificate to the Trusted Root Certificate store, you can instead upload a new certificate that browsers are already configured to trust.

### Procedure

---

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

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

**Step 2** Click the **Management Web Server** tab.

**Step 3** In **Web Server Certificate**, select the internal certificate to use for securing HTTPS connections to the FDM.

If you have not uploaded or created the certificate, click the **Create New Internal Certificate** link at the bottom of the list and create it now.

The default is the pre-defined DefaultWebserverCertificate object.

**Step 4** Click **Save**.

The change is applied immediately, and the system restarts the web server. You do not need to deploy the configuration.

Wait a few minutes to allow the restart to finish, then refresh your browser.

## Configuring System Logging Settings

You can enable system logging (syslog) for FTD devices. Logging information can help you identify and isolate network or device configuration problems. You can enable syslog for diagnostic logging and for connection-related logging, including access control, intrusion prevention, and file and malware logging.

Diagnostic logging provides syslog messages for events related to device and system health, and the network configuration, that are not related to connections. You configure connection logging within individual access control rules.

Diagnostic logging generates messages for features running on the data plane, that is, features that are defined in the CLI configuration that you can view with the **show running-config** command. This includes features such as routing, VPN, data interfaces, DHCP server, NAT, and so forth.

For information on these messages, see *Cisco Threat Defense Syslog Messages* at [https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b\\_ftpd\\_syslog\\_guide.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_ftpd_syslog_guide.html).

The following topics explain how to configure the logging of diagnostic and file/malware messages to various output locations.

## Severity Levels

The following table lists the syslog message severity levels.

**Table 1: Syslog Message Severity Levels**

Level Number	Severity Level	Description
0	<b>emergencies</b>	System is unusable.
1	<b>alert</b>	Immediate action is needed.
2	<b>critical</b>	Critical conditions.
3	<b>error</b>	Error conditions.
4	<b>warning</b>	Warning conditions.
5	<b>notification</b>	Normal but significant conditions.
6	<b>informational</b>	Informational messages only.
7	<b>debugging</b>	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).

---

## Configure Logging to a Remote Syslog Server

You can configure the system to send syslog messages to an external syslog server. This is the best option for system logging. By using an external server, you can provide more room to hold messages, and use the facilities of the server to view, analyze, and archive messages.

In addition, if you apply file policies to traffic in access control rules, to control file access or malware, or both, you can configure the system to send file event messages to an external syslog server. If you do not configure a syslog server, the events are available in the FDM Event Viewer only.

The following procedure explains how to enable syslog for diagnostic (data) logging and file/malware logging. You can also configure external logging for the following:

- Connection events, by selecting the syslog server on individual access control rules, SSL decryption rules, or Security Intelligence policy settings.
- Intrusion events, by selecting the syslog server in the intrusion policy settings.

### Before you begin

The syslog setting for file/malware events is relevant only if you apply file or malware policies, which require the Threat and Malware licenses.

In addition, you must ensure that the **File Events > Log Files** option is selected on the access control rules that apply the policies. Otherwise, no events are generated at all, either for syslog or Event Viewer.

### 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** Under **Remote Server**, turn the **Data Logging** slider to **On** to enable logging diagnostic data-plane-generated messages to an external syslog server. Then, configure the following options:
- **Syslog Server**—Click + and select one or more syslog server object and click **OK**. If the objects do not exist, click the **Add Syslog Server** link and create them now. For more information, see [Configuring Syslog Servers](#).
  - **Severity Level for Filtering FXOS Chassis Syslogs**—For certain device models that use FXOS, the severity level for syslog messages generated by the base FXOS platform. This option appears only if it is relevant for your device. Select the severity level. Messages at this level or higher are sent to the syslog server.
  - **Message Filtering**—Select one of the following options to control the messages generated for the FTD operating system.
    - **Severity Level for Filtering All Events**—Select the severity level. Messages at this level or higher are sent to the syslog server.

- **Custom Logging Filter**—If you want to do additional message filtering, so you get only those messages that interest you, select the event list filter that defines the messages you want to generate. If the filter does not already exist, click **Create New Event List Filter** and create it now. For more information, see [Configure Event List Filters, on page 7](#).

**Step 3** Turn the **File/Malware** slider to **On** to enable logging to an external syslog server for file and malware events. Then, configure the options for file/malware logging:

- **Syslog Server**—Select the syslog server object. If the object does not exist, click the **Add Syslog Server** link and create it now.
- **Log at Severity Level**—Select a severity level that should be assigned to the file/malware events. Because all file/malware events are generated at the same severity, no filtering is performed; you will see all events no matter which level you pick. This will be the level shown in the severity field of the message (that is, the x in FTD-x-<message\_ID>). File events are message ID 430004, malware events are 430005.

**Step 4** Click **Save**.

---

## Configure Logging to the Internal Buffer

You can configure the system to save syslog messages to an internal logging buffer. Use the **show logging** command in the CLI or CLI Console to view the contents of the buffer.

New messages append to the end of the buffer. When the buffer fills up, the system clears the buffer and continues adding messages to it. When the log buffer is full, the system deletes the oldest message to make room in the buffer for new 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** Turn the **Internal Buffer** slider to **On** to enable the buffer as a logging destination.

**Step 3** Configure the options for internal buffer logging:

- **Severity Level for Filtering All Events**—Select the severity level. Messages at this level or higher are sent to the internal buffer.
- **Custom Logging Filter**—(Optional.) If you want to do additional message filtering, so you get only those messages that interest you, select the event list filter that defines the messages you want to generate. If the filter does not already exist, click **Create New Event List Filter** and create it now. For more information, see [Configure Event List Filters, on page 7](#).
- **Buffer Size**—The size of the internal buffer to which syslog messages are saved. When the buffer fills up, it is overwritten. The default is 4096 bytes. The range is 4096 to 52428800.

**Step 4** Click **Save**.

---

## Configure Logging to the Console

You can configure the system to send messages to the 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.

### 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** Turn the **Console Filter** slider to **On** to enable the console as a logging destination.
- Step 3** Select the **Severity** level. Messages at this level or higher are sent to the console.
- Step 4** Click **Save**.
- 

## Configure Event List Filters



An event list filter is a custom filter you can apply to a logging destination to control which messages are sent to the destination. Normally, you filter messages for a destination based on severity only, but you can use a to fine-tune which messages are sent based on a combination of event class, severity, and message identifier (ID).

You would use a filter only if limiting messages by severity level alone is insufficient for your purposes.

The following procedure explains how to create the filter from the **Objects** page. You can also create a filter when you are configuring a logging destination that can use a filter.

### Procedure

---

- Step 1** Select **Objects**, then select **Event List Filters** from the table of contents.
- Step 2** Do one of the following:
- To create an object, click the + button.
  - To edit an object, click the edit icon () for the object.
- To delete an unreferenced object, click the trash can icon () for the object.
- Step 3** Configure the filter properties:
- **Name**—The name of the filter object.
  - **Description**—An optional description of the object.
  - **Severity and Log Class**—If you want to filter by message class, click +, select a severity level for the class filter and click **OK**. Then, click the drop-down arrow within the severity level, select one or more classes to filter at that severity level, and click **OK**.

The system will send syslog messages for the specified classes of messages only if they are at that severity level or higher. You can add at most one row for each severity level.

If you want to filter all classes at a given severity level, leave the Severity list empty and instead select the global severity level for the logging destination when you enable it.

- **Syslog Range/Message ID**—If you want to filter by the syslog message ID, enter a single message ID, or a range of ID numbers for which you want to generate messages. Separate the starting and ending number for a range with a hyphen, for example, 100000-200000. The IDs are 6 digit numbers. For specific message IDs and the related messages, see *Cisco Threat Defense Syslog Messages* at [https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b\\_ftpd\\_syslog\\_guide.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_ftpd_syslog_guide.html).

**Step 4** Click **Save**.

You can now select this object in the custom filtering option for logging destinations that allow it. Go to **Device > System Settings > Logging Settings**.

## Configuring the 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. You configure DNS servers during initial system setup, and these servers are applied to the data and management interfaces. You can change them after setup, and use separate sets of servers for the data and management interfaces.

At minimum, you must configure DNS for the management interface. You must also configure DNS for the data interfaces if you want to use FQDN-based access control rules, or if you want to use hostnames in CLI commands such as **ping**.

Configuring DNS is a two-step process: you configure DNS groups, then you configure DNS on the interfaces.

The following topics explain the process in more detail.

## Configuring DNS Groups

DNS groups define a list of DNS servers and some associated attributes. You can configure DNS separately on the management and data interfaces. DNS servers are needed to resolve fully-qualified domain names (FQDN), such as `www.example.com`, to IP addresses.

After you complete the device setup wizard, you will have one or both of the following system-defined DNS groups:



- **CiscoUmbrellaDNSServerGroup**—This group includes the IP addresses of the DNS servers available with Cisco Umbrella. If you selected these servers during initial setup, this is the only system-defined group. You cannot change the name or server list in this group, but you can edit the other properties.
- **CustomDNSServerGroup**—If you do not select the Umbrella servers during device setup, the system creates this group with your list of servers. You can edit any property in this group.


### Procedure

---

**Step 1** Select **Objects**, then select **DNS Groups** from the table of contents.

**Step 2** Do one of the following:

- To create a group, click the **Add Group**  button.
- To edit a group, click the edit icon  for the group.

To delete an unreferenced object, click the trash can icon  for the object.

**Step 3** Configure the following properties:

- **Name**—The name of the DNS server group. The name `DefaultDNS` is reserved: you cannot use it.

- **DNS IP Addresses**—Enter the IP address of a DNS server. Click **Add Another DNS IP Address** to configure more than one server. If you want to remove a server address, click the delete icon (🗑️) for the address.  

The list is in priority order: the first server in the list is always used, and subsequent servers are used only if a response is not received from the servers above it. You can configure up to 6 servers. However, 6 servers are supported on data interfaces only. For the management interface, only the first 3 servers will be used.
- **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. The name must be shorter than 63 characters to use the group for data interfaces.
- **Retries**—The number of times, from 0 to 10, to retry the list of DNS servers when the system does not receive a response. The default is 2. This setting applies to DNS groups used on the data interfaces only.
- **Timeout**—The number of seconds, from 1 to 30, to wait before trying the next DNS server. The default is 2 seconds. Each time the system retries the list of servers, this timeout doubles. This setting applies to DNS groups used on the data interfaces only.

**Step 4** Click **OK**.

---

## Configuring DNS for Data and Management Traffic

The Domain Name System (DNS) servers are used to resolve hostnames to IP addresses. There are two DNS server settings that apply to different types of traffic: data and special management traffic. Data traffic includes any services that use FQDNs for which a DNS lookup is necessary, such as Access Control Rules and Remote Access VPN. Special management traffic includes traffic originating on the Management interface such as Smart Licensing and database updates.

If you use the CLI setup wizard, you configure the management DNS servers during initial system configuration. You can also set the data and management DNS servers in the FDM setup wizard. You can change the DNS servers defaults using the following procedure.

You can also change the management DNS configuration in the CLI using the **configure network dns servers** and **configure network dns searchdomains** commands. If the data and management interfaces are using the same DNS group, the group is updated and on your next deployment, the changes are also applied to the data interfaces.

To determine the correct interface for DNS server communications, the FTD uses a routing lookup, but which routing table is used depends on the interfaces for which you enable DNS. See the interface settings below for more information.

If you have problems with DNS resolution, see:

- [Troubleshooting General DNS Problems, on page 13](#)
- [Troubleshooting DNS for the Management Interface](#)

### Before you begin

- Ensure you have created a DNS server group. For instructions, see [Configuring DNS Groups, on page 10](#).

- Ensure that the FTD device has appropriate static or dynamic routes to access the DNS servers.

## Procedure

---

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

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

**Step 2** Configure DNS for the **Data Interface**.

- a) Enable DNS lookups on all interfaces or on specific interfaces. These choices also affect which routing tables are used.

Note that enabling DNS lookups on an interface is not the same as specifying the source interface for lookups. The device always uses a route lookup to determine the source interface.

- **ANY** (do not choose any interfaces)—Enables DNS lookups on all interfaces, including Management and management-only interfaces. The device checks the data routing table, and if no route is found, falls back to the management-only routing table.
  - Interfaces selected but not the Diagnostic interface or a management-only interface—Enables DNS lookups on the specified interfaces. The device checks the data routing table only.
  - Interfaces selected plus the Diagnostic interface or a management-only interface—Enables DNS lookups on the specified interfaces. The device checks the data routing table, and if no route is found, falls back to the management-only routing table.
  - Only the Diagnostic interface or a management-only interface selected—Enables DNS lookups on Diagnostic or a management-only interface. The device checks only the management-only routing table.
- b) Select the **DNS Group** that defines the servers to use on the data interfaces. If the group does not exist yet, click **Create New DNS Group** and create it now. Select **None** if you want to prevent lookups on the data interfaces.
- c) (Optional.) Configure the **FQDN DNS Settings** if you use FQDN network objects in access control rules.

These options are used when resolving FQDN objects only, and are ignored for any other type of DNS resolution.

- **Poll Time**—The time, in minutes, of the polling cycle used to resolve FQDN network objects to IP addresses. FQDN objects are resolved only if they are used in the access control policy. The timer determines the maximum time between resolutions; the DNS entry's time-to-live (TTL) value is also used to determine when to update the IP address resolution, so individual FQDNs might be resolved more frequently than the polling cycle. The default is 240 (four hours). The range is 1 to 65535 minutes.
  - **Expiry**—The number of minutes after a DNS entry expires (that is, the TTL obtained from the DNS server has passed) that the entry is removed from the DNS lookup table. Removing an entry requires that the table be recompiled, so frequent removals can increase the processing load on the device. Because some DNS entries can have very short TTL (as short as three seconds), you can use this setting to virtually extend the TTL. The default is 1 minute (that is, the entry is removed one minute after the TTL has passed). The range is 1 to 65535 minutes.
- d) Click **Save**. You must also deploy the configuration to apply the changes to the device.

**Step 3** Configure DNS for the **Management Interface**.

- a) Select the **DNS Group** that defines the servers to use on the Management interface. If the group does not exist yet, click **Create New DNS Group** and create it now.
- b) Click **Save**. Your changes are immediately applied to the device. You do not run a deployment job to apply this change.

## Troubleshooting General DNS Problems

You must separately configure DNS servers for the Management and data interfaces. Some features do name resolution through one or the other type of interface, but not both. Sometimes, a given feature will use different resolution methods depending on how you use it.

For example, the **ping hostname** and **ping interface interface\_name hostname** commands use the data interface DNS servers to resolve the name, whereas the **ping system hostname** command uses the Management interface DNS servers. This makes it possible for you to test connectivity through specific interfaces and through the routing table.

Keep this in mind when you are troubleshooting problems with hostname lookup.

For troubleshooting DNS for the Management interface, also see [Troubleshooting DNS for the Management Interface](#).

### When You Get No Name Resolution

Following are some troubleshooting tips if name resolution is simply not happening.

- Verify that you have configured DNS servers for both the management and data interfaces. For data interfaces, use Any for the interface. Specify interfaces explicitly only if you do not want to allow DNS on some interfaces.
- If you are using the diagnostic interface for lookups on data interfaces, verify that you configured an IP address on the interface. Lookups require that the interface has an IP address.
- You cannot reach the DNS server through the Diagnostic interface or through a management-only interface, because the route lookup finds a match in the data routing table so there is no fall back to the management-only routing table. If you want to use the Diagnostic interface, make sure that is the only interface selected.
- Ping the IP address of each DNS server to verify that it is reachable. Use the **system** and **interface** keywords to test specific interfaces. If ping is unsuccessful, check your static routes and gateways. You might need to add static routes for the servers.
- If ping is successful, but name resolution is failing, check your access control rules. Verify that you are allowing DNS traffic (UDP/53) for the interfaces through which the servers are reachable. It is also possible that this traffic is getting blocked by a device that is between your system and the DNS server, so you might need to use different DNS servers.
- If ping works, there are adequate routes, and access control rules are not the problem, consider that the DNS server might not have a mapping for the FQDN. You might need to use different servers.

### When You Get Wrong Name Resolution

If you are getting name resolution, but the IP address for a name is not current, there might be a caching issue. This problem would affect data-interface based features only, such as FQDN network objects used in access control rules.

The system has a local cache of DNS information obtained from previous lookups. When a new lookup is required, the system first looks in the local cache. If the local cache has the information, the resulting IP address is returned. If the local cache can not resolve the request, a DNS query is sent to the DNS servers. If an external DNS server resolves the request, the resulting IP address is stored in the local cache with its corresponding hostname.

Each lookup has a time to live value, which is defined by the DNS server, and expires from the cache automatically. In addition, the system periodically refreshes the value for FQDNs that are used in access control rules. At minimum, this refresh happens at the poll time interval (by default, every 4 hours), but it can be more frequent based on the entry's time to live value.

Use the **show dns-hosts** and **show dns** commands to check the local cache. If the IP addresses for an FQDN are wrong, you can use the **dns update [host hostname]** command to force the system to refresh the information. If you use the command without specifying a host, all hostnames are refreshed.

You can remove cached information using the **clear dns [host fqdn]** and **clear dns-hosts cache** commands.

## Configuring the Management Interface

The Management interface is a virtual interface attached to the physical Management port. Note that the physical interface also includes the Diagnostic virtual interface, which you can configure on the **Interfaces** page with other physical interfaces. See [Management/Diagnostic Interface](#) for more information about the Diagnostic interface.

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 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.

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 FTDv, 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 the FDM (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, 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:
- (Static IP only) **Use the Data Interfaces as the Gateway**—Select this option if you do not have a separate management network connected to the Management interface. Traffic is routed to the internet based on the routing table, typically going through the outside interface. This option is not supported on the FTDv 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. For DHCP IP addressing, the gateway is provided by the DHCP server.
- 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 interface.
- If you configure a DHCP server on the management interface, clients on the management network can obtain their address from the DHCP pool. This option is not supported on the FTDv 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 the FDM 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**.
- The hostname change is immediately applied for some system processes. However, you must deploy changes to complete the update so that the same name is used by all system processes.
- 

## 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.



---

**Note** For the Firepower 4100/9300, you do not set NTP through the FDM. Configure NTP in FXOS.

---

### 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 Servers**—If you select this option, the server list shows the server names that are used for NTP.
  - **User-Defined NTP Servers**—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 URL Filtering Preferences

The system obtains the URL category and reputation database from Cisco Collective Security Intelligence (CSI) (Cisco Talos Intelligence Group (Talos)). 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.
  - **URL Time to Live** (available if you select **Query Cisco CSI for Unknown URLs**)—How long to cache the category and reputation lookup values for a given URL. When the time to live expires, the next attempted access of the URL results in a fresh category/reputation lookup. A shorter time results in more accurate URL filtering, a longer time results in better performance for unknown URLs. You can set the TTL to 2, 4, 8, 12, 24, or 48 hours, one week, or Never (the default).
- Step 3** As needed, you can **Check the Category for a URL**.
- You can check on the category and reputation for a particular URL. Enter the URL in the **URL to Check** box and click **Go**. You will be taken to an external website to see the results. If you disagree with a categorization, click the **Submit a URL Category Dispute** link and let us know.
- Step 4** Click **Save**.
- 

# Configuring Cloud Services

Use the Cloud Services page to manage the cloud-based services used by the device from the device side. After you register for certain services, you need to manage them from the cloud.

The following topics explain the cloud service options.

## Configuring Cloud Management (Cisco Defense Orchestrator)

You can manage the device using the Cisco Defense Orchestrator (CDO) cloud-based portal.

Using CDO, you can approach device management using the following techniques:

- Initial configuration download—In this approach, you download the initial device configuration from CDO, but thereafter you configure the device locally using FDM.



---

**Note** After configuring the device using FDM, 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 CDO 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 CDO 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 CDO. You can also get a key from your Cisco Cloud Services account.

If you have already registered the device with Cisco Smart Software Manager (CSSM), we strongly recommend that you first unregister the device from the Smart Licensing page. You can re-register after you enable CDO using a token.

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



---

**Note** If you intend to configure high availability, you must register both devices that you will use in the high availability group.

---

### Procedure

---

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

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

**Step 2** Click **Get Started** in the **Cisco Defense Orchestrator** group.

**Step 3** Paste the key in **Registration Key**, select your cloud services region, 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 click the **Disable** button.

---

## Connecting to the Cisco Success Network

When you register the device, you decide whether to enable the connection to the Cisco Success Network. See [Registering the Device](#).

By enabling Cisco Success Network, you are providing usage information and statistics to Cisco that are essential for Cisco to provide you with technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

When you enable the connection, your device establishes a secure connection to the Cisco Cloud so that your device can participate in additional service offerings from Cisco such as technical support services, cloud management and monitoring services. Your device will establish and maintain this secure connection at all times. For information on completely disconnecting from the cloud, see [Disabling Cisco Cloud Services Enrollment, on page 20](#).

After you have registered the device, you can change the Cisco Success Network setting.



---

**Note** When the system sends data to Cisco, the task list shows a Telemetry Job.

---

### Before you begin

To enable Cisco Success Network the device must be enrolled with the cloud. To enroll the device, either register the device with Cisco Smart Software Manager (on the Smart Licensing page), electing the Cisco Success Network option during registration, or enroll with CDO by entering a registration key (legacy device manager mode in CDO only).



---

**Note** If you enable Cisco Success Network on the active unit in a high availability group, you are also enabling the connection on the standby unit.

---

### Procedure

---

- Step 1** Click **Device**, then click the **System Settings > Cloud Services** link.  
If you are already on the System Settings page, simply click **Cloud Services** in the table of contents.
- Step 2** Click the **Enable/Disable** control for the Cisco Success Network feature to change the setting as appropriate.  
You can click the **sample data** link to see the type of information that is sent to Cisco.  
When enabling the connection, read the disclosure and click **Accept**.
-

## Disabling Cisco Cloud Services Enrollment

When you register the device to Cisco Defense Orchestrator, enable Cisco Success Network, send events to the Cisco cloud, or register the device with the Cisco Smart Software Manager, the device is enrolled with Cisco Cloud Services. Even if you disable all cloud services, the device remains enrolled.

When you enable the connection, your device establishes a secure connection to Cisco Cloud Services so that your device can participate in additional service offerings from Cisco such as technical support services, cloud management and monitoring services. Your device will establish and maintain this secure connection at all times.

You might want to remove the device's Cisco Cloud Services enrollment so that you can register under a different Smart Licensing account, or otherwise remove the device from service.

### Procedure

---

- Step 1** Disable all cloud services on the **Device > System Settings > Cloud Services** page.
- Step 2** Choose **Device > Smart License** and select **Unregister Device** from the gear drop-down list.
- Step 3** If you want to re-register the device with the cloud, do one of the following:
- To use your Cisco Security account, choose **Device > System Settings > Cloud Services** and re-register with Cisco Defense Orchestrator using a token. You can then go **Device > Smart License** and re-register the device.
  - To use your Smart License account, register the device on the **Device > Smart License** page. You can now return to the Cloud Services page and re-enable the desired services.
- 

## Enabling or Disabling Web Analytics

Enabling web analytics provides anonymous product usage information to Cisco based on page hits. The information includes pages viewed, the time spent on a page, browser versions, product version, device hostname, and so forth. This information can help Cisco determine feature usage patterns and help Cisco improve the product. All usage data is anonymous and no sensitive data is transmitted.

Web analytics is enabled by default.

### Procedure

---

- Step 1** Click **Device**, then click the **System Settings > Cloud Services** link.
- If you are already on the System Settings page, simply click **Cloud Services** in the table of contents.
- Step 2** Click the **Enable/Disable** control for the **Web Analytics** feature to change the setting as appropriate.
-

## Sending Events to the Cisco Cloud

You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as Cisco Threat Response, to analyze the events and to evaluate threats that the device might have encountered. When you enable this service, this device will send connection and high-priority intrusion, file, and malware events to the Cisco cloud.

The cloud tools determine whether the events you send are used. Consult the tool's documentation, or examine the event data, to ensure you are not sending unused events to the cloud, wasting both your bandwidth and storage space. Keep in mind that the tools pull the events from the same source, so your selection should reflect all the tools you use, not just the most restrictive tool. For example:

- The Security Analytics and Logging tool in CDO can make use of all connection events.
- Cisco Threat Response and SecureX use high priority connection events only, so there is no need to send all connection events to the cloud if you use these tools only. In addition, these tools will use only the Security Intelligence high-priority events.

### Before you begin

You must register the device with Cisco Smart Software Manager before you can enable this service.

You can connect to Cisco Threat Response at <https://visibility.amp.cisco.com/> in the US region, <https://visibility.eu.amp.cisco.com> in the EU region. You can watch videos about the use and benefits of the application on YouTube at <http://cs.co/CTRvideos>. For more information about using Cisco Threat Response with FTD, see *Cisco Secure Firewall Threat Defense and SecureX threat response Integration guide*, which you can find at <https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html>.

### Procedure

- 
- Step 1** Click **Device**, then click the **System Settings > Cloud Services** link.
- If you are already on the System Settings page, simply click **Cloud Services** in the table of contents.
- Step 2** Click the **Enable/Disable** control for the **Send Events to the Cisco Cloud** option to change the setting as appropriate.
-

