

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 5
- Configuring DHCP, on page 9
- Configuring Dynamic DNS, on page 13
- Configuring DNS, on page 15
- Configuring the Management Interface, on page 20
- Configuring the Device Hostname, on page 21
- Configuring Network Time Protocol (NTP), on page 22
- Configuring Precision Time Protocol (ISA 3000), on page 23
- Configuring HTTP Proxy for Management Connections, on page 25
- Configuring Cloud Services, on page 26
- Enabling or Disabling Web Analytics, on page 31
- Configuring URL Filtering Preferences, on page 31
- Switch from the Firewall Device Manager to the Firewall Management Center or Security Cloud Control, on page 32
- Switch from the Firewall Management Center or Security Cloud Control to the Firewall Device Manager, on page 37
- Configuring TLS/SSL Cipher Settings, on page 39

Configuring Management Access

Management access refers to the ability to log into the Firewall Threat Defense 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 Firewall Device Manager and Firewall Threat Defense 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 Firewall Device Manager) and SSH (used for CLI). See Configuring the Management Access List, on page 2.

- Management Web Server certificate, which users must accept to connect to the Firewall Device Manager. By uploading a certificate your web browsers already trust, you can avoid users being ask to trust an unknown certificate. See Configuring the Firewall Threat Defense Web Server Certificate, on page 4.

Configuring the Management Access List

By default, you can reach the device's Firewall 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 the Firewall 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 the Firepower 1010 that has a default “inside” bridge group, this means that you can make the Firewall Device Manager connections through any data interface within the bridge group to the bridge group IP address (default is 192.168.95.1). 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 Firewall Device Manager 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. If you configure both features on the same interface, ensure that you change the HTTPS port for at least one of these services to avoid a conflict.

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 Firewall Device Manager and Firewall Threat Defense 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 Firewall 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 the Firewall 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) (Optional.) If you want to change the HTTPS Data Port number, click the number and enter a new port. See Configuring the HTTPS Port for Management Access on Data Interfaces, on page 3.

d) Click **OK**.

Configuring the HTTPS Port for Management Access on Data Interfaces

By default, accessing the device for management purposes, either for the Firewall Device Manager or the Firewall Threat Defense API, goes through port TCP/443. You can change the management access port for data interfaces.

If you change the port, users must include the custom port on the URL to access the system. For example, if the data interface is ftd.example.com, and you change the port to 4443, then users must modify the URL to https://ftd.example.com:4443.

All data interfaces will use the same port. You cannot configure different ports per interface.

Note You cannot change the management access port for the management interface. The management interface always uses port 443.

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 **Data Interfaces** tab.

Step 3 Click the **HTTPS Data Port** number.

Step 4 In the Data Interfaces Setting dialog box, change the **HTTPS Data Port** to the one you want to use.

You cannot specify the following numbers:

- 22, which is used for SSH connections.
- The port used for remote access VPN, if you configured it for any interfaces that you are also allowing for management access. Remote access VPN uses port 443 by default, but you can configure a custom port for it.
- The port used for active authentication in the identity policy, which is 885 by default.

Step 5 Click **OK**.

Configuring the Firewall Threat Defense 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 Firewall Device Manager.

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 If the certificate is not self-signed, add all intermediate and root certificates in the full trust chain to the **Trusted Chain** list.

You can add up to 10 certificates in the chain. Click + to add each intermediate certificate, and finally, the root certificate. When you click **Save** (and then **Proceed** on the dialog that warns you that the web server will restart), if a certificate is missing, you will get an error message with the common name of the next certificate in the chain that is missing. You will also get an error if you add a certificate that is not in the chain. Examine these messages carefully to identify the certificate you need to add or remove.

You can upload the certificates from here by clicking **Create New Trusted CA Certificate** after clicking +.

Step 5 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 Firewall Threat Defense 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_fptd_syslog_guide.html.

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

Syslog message severity levels

The syslog message severity levels define the importance of system messages.

Table 1: Syslog message severity levels

Level Number	Severity Level	Description
0	**emergencies**	You cannot use the system.
1	**alert**	You need to take immediate action.

Level Number	Severity Level	Description
2	**critical**	The system has critical conditions to be addressed.
3	**error**	Error conditions.
4	**warning**	The system has warnings you should review.
5	**notification**	The system reports significant events you should monitor.
6	**informational**	Informational messages only.
7	**debugging**	The system generates only debugging messages Log at this level only temporarily, when debugging issues. This log level can generate many messages, which might affect system performance.



Note Firewall Threat Defense does 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 Firewall Device Manager 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 IPS and malware defense 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 Firewall Threat Defense 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 8.

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 8.
- **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_fptd_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 DHCP

A DHCP server provides network configuration parameters, such as IP addresses, to DHCP clients. You can either configure DHCP servers on interfaces to provide configuration parameters to DHCP clients on the attached network, or enable DHCP relay on the interfaces to forward requests to an external DHCP server that is operating on another device in the network.

These features are mutually exclusive: you can configure one or the other, but not both.

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.



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.

Before you begin

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.

If you must support multiple networks, and do not want to configure a DHCP server on each interface, you can instead configure DHCP relay to forward DHCP requests from one network to a DHCP server that resides on a different network. In this case, the DHCP server must reside on a different device in the network: you cannot configure a DHCP server on one interface and DHCP relay on another interface on the same device. When using DHCP relay, ensure that you configure the DHCP server with address pools for each network address space that the DHCP server will manage.

To configure DHCP relay, see Configuring DHCP Relay, on page 12.

Procedure

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

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

If you configure virtual routers, you can use DHCP server auto configuration on an interface in the global virtual router only. Auto configuration is not supported for interfaces assigned to a user-defined virtual router.

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. If the address pool range is larger than 253 addresses, the netmask of the Firewall Threat Defense 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 DHCP Relay

You can configure a DHCP relay agent to forward DHCP requests received on an interface to one or more DHCP servers.

DHCP clients use UDP broadcasts to send their initial DHCPDISCOVER messages because they do not have information about the network to which they are attached. If the client is on a network segment that does not include a server, UDP broadcasts normally are not forwarded by the Firewall Threat Defense device because it does not forward broadcast traffic. The DHCP relay agent lets you configure the interface of the Firewall Threat Defense device that is receiving the broadcasts to forward DHCP requests to a DHCP server that is available through another interface.

Thus, clients on subnets that do not host a DHCP server can still get IP address leases from a DHCP server that resides on a different subnet.

Before you begin

- Configure the DHCP server with address pools for each of the subnets you are adding. For example, if you enable the DHCP relay client on an interface with the 192.168.1.1/24 address, to support clients on the 192.168.1.0/24 network, the DHCP server must be able to supply IP addresses on the 192.168.1.0/24 subnet, for example, 192.168.1.2-192.168.1.254.
- Create host network objects for each of the DHCP servers, specifying the IP address of the server.
- Ensure that you have removed or disabled all servers on the **DHCP** > **DHCP Servers** page. You cannot host a DHCP server on any interface with DHCP relay enabled on an interface, even if they are different interfaces.
- Interface limitations—An interface must have a name to be used for either server or agent. In addition:
  - The interface cannot be a member of a routing ECMP traffic zone.
  - The interface cannot obtain its address using DHCP.
  - You can configure both DHCP server and DHCP relay on physical interfaces, subinterfaces, VLAN interfaces, and EtherChannels (but not their members).
  - You can also configure DHCP relay server on virtual tunnel interfaces (VTI).
  - Neither service supports the management interface, or bridge groups and their members.

Procedure

Step 1 Click **Device**, then click the **System Settings** > **DHCP Server / Relay** link, then click **DHCP** > **DHCP Relay** in the table of contents.

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

Step 2 (Optional.) Adjust the **IPv4 Relay Timeout** and **IPv6 Relay Timeout** settings as needed.

These timeouts set the number of seconds that are allowed for DHCP relay address negotiation for the given IP version. The default is 60 seconds (1 minute), but you can set a different timeout from 1-3600 seconds. Longer timeouts might be appropriate if there is significant lag between the subnet and the DHCP server.

Step 3 Configure the **DHCP Relay Servers**.

The DHCP relay servers are the DHCP servers in the network that should service DHCP relay requests. These DHCP servers reside on different devices in the network from the device you are configuring.

a) Click **+**, select a host network object that has the IP address of a DHCP server, and click **OK**.

If the object does not yet exist, click **Create New Network** and create it now. If you no longer want to use a DHCP server you had added, click the **X** on the right of the server's entry to delete it.

b) Click the DHCP server entry you added, and select the interface through which the DHCP server can be reached.

Step 4 Configure the DHCP Relay Agents.

The DHCP relay agents run on the interfaces. They forward DHCP requests from clients on their network segment to the DHCP servers, then return the responses to the client.

a) Click **+**, select the interfaces that should run the DHCP relay agent, and click **OK**.

If you no longer want run the DHCP relay agent on an interface, click the **X** on the right of the server's entry to delete it. Optionally, you can simply disable all DHCP relay services without removing the interface from the table.

b) Click the interface entry you added, select the DHCP services you want the agent to provide, and click **OK**.

- **Enable IPv4**—Forward IPv4 address requests to the DHCP server. If you do not select this option, any IPv4 address requests are ignored, and the client cannot obtain an IPv4 address.
- **Set Route** (IPv4 only)—Change the first default router address in the packet sent from the DHCP server to the address of the Firewall Threat Defense device interface that is running the DHCP relay agent. This action allows the client to set its default route to point to the Firewall Threat Defense device even if the DHCP server specifies a different router. If there is no default router option in the packet, the DHCP relay agent adds one containing the interface address.
- **Enable IPv6**—Forward IPv6 address requests to the DHCP server. If you do not select this option, any IPv6 address requests are ignored, and the client cannot obtain an IPv6 address.

Step 5 Click **Save**.

Configuring Dynamic DNS

You can configure the system to use the web update method to send Dynamic Domain Name System (DDNS) changes to Dynamic DNS services. These services then update the DNS server to use the new IP address associated with a fully-qualified domain name (FQDN). Thus, when users try to access the system using a hostname, DNS will resolve the name to the correct IP address.

Using DDNS can help ensure that the FQDNs defined for the interfaces on the system always resolve to the correct IP address. This is especially important if you configure an interface to get its address using DHCP. But there is also value in using it for static IP addresses, to ensure the DNS server has the correct addresses, and that it can be easily updated if you change the static address.

You can configure DDNS to use a select group of DDNS service providers, or use the custom option to direct updates to any other DDNS provider that supports web updates. The FQDNs you specify for interfaces should be registered with these service providers.

Note You can use the Firewall Device Manager to configure web update DDNS only. You cannot configure DDNS for the method defined in IETF RFC 2136.

Before you begin

The system must have a trusted CA certificate that will validate the provider's certificate, or the DDNS connection will not succeed. You can download the certificates from the service provider's site. Please ensure the appropriate certificate is uploaded and deployed. Also ensure that you set the **Validation Usage** for the uploaded certificate to include **SSL Server**. See Uploading Trusted CA Certificates.

Procedure

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

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

The page shows a list of DDNS update methods, including the service provider, interface, fully-qualified domain name (FQDN) for the interface, and how often the DNS server will be updated for changes to the FQDN's IP address. You can click the **Show Status** link for an entry to check whether it is working correctly.

Step 2 Do one of the following:

- To create a new Dynamic DNS update method, click **+** or the **Create DDNS Service** button.
- To edit an existing Dynamic DNS update method, click the edit icon ( ) for the method.

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

Step 3 Configure Dynamic DNS Service properties:

- **Name**—A name for the service.
- **Web Type Update**—Select the types of addresses to be updated, based on what is supported by your DDNS service provider. The default is to update **All Addresses**, both IPv4 and IPv6. You can instead update the **IPv4 Address**, **IPv4 and One IPv6 Address**, **One IPv6 Address**, **All IPv6 Addresses**.

  Please note the following for IPv6 addresses:

  - Global addresses only are updated. The link local address is never updated.
  - Because the Firewall Device Manager allows you to configure a single IPv6 address per interface, in practice, only one IPv6 address will ever be updated.

- **Service Provider**—Select the service provider that will receive and process the dynamic DNS updates. You can use the following service providers.
  - **No-IP**—The No-IP DDNS service provider, https://www.noip.com/.

- **Dynamic DNS**—The Oracle Dynamic DNS service provider, https://account.dyn.com/.
- **Google**—The Google Domains service provider, https://domains.google.com.
- **Custom URL**—Any other DDNS service provider. You will need to enter the URL required by your selected provider, including username and password, into the **Web URL** field. The DDNS service should abide by the standards described at https://help.dyn.com/remote-access-api/.

- **Username**, **Password** (non-Custom URL methods)—The username and password, defined on the service provider's platform, to use when sending dynamic DNS updates.

  Note:

  - The username cannot include spaces, or the @ and : characters, because they would act as delimiters.
  - The password cannot include spaces, or the @ character, because it acts as delimiter. Any : character after the first : and before @ is considered part of the password.

- **Web URL** (Custom URL method)—If you selected a custom URL as the service provider, enter the URL for your dynamic DNS service. The URL must be in the following format, limited to 511 characters:

  http(s)://username:password@provider-domain/xyz?hostname=<h>&myip=<a>

  https://username:password@domain-provider/xyz?hostname=%3Ch%3E&myip=%3Ca%3E

- **Interfaces and Fully-Qualified Domain Name**—Select the interfaces whose DNS records you want updated with this service provider, then enter the fully-qualified domain name for each interface. For example, interface.example.com. Interfaces are restricted as follows:
  - You can select named physical and subinterfaces only.
  - You cannot select the following types of interface: management, BVI/EtherChannel or its members, VLANs, virtual tunnel interfaces (VTI).
  - A given interface can be selected in one DDNS update method only. You can select all interfaces that should use a service provider in the same DDNS update object.

- **Update Interval**—How often the dynamic DNS update should be sent. The default is **On Change**, which sends an update whenever the IP address for the interface changes. Alternatively, you can select **Hourly**, **Daily**, or **Monthly**. For daily and monthly, also configure the time of the day, and for monthly, the day of the month, to send updates.

Step 4 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 3 servers.
- **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 Firewall Device Manager 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 Firewall Threat Defense 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 18
- 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 16.
- Ensure that the Firewall Threat Defense 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**. You must deploy changes to update the management DNS servers.

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 uses 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 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 Firewall Device Manager setup wizard, the management address and gateway remain the defaults.

If necessary, you can change these addresses through the Firewall 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. To restore the default management interface settings, use the **configure network** {**ipv4** | **ipv6**} **dhcp-dp-route** command.

You can define static addresses, or obtain an address through DHCP if another device on the management network is acting as a DHCP server. For most platforms, the Management interface obtains an IP address from DHCP by default.



Caution If you change the address to which you are currently connected, you will lose access to the Firewall 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, 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 Options:

- **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 Firewall 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.

DHCP IP Options:

- **Use Unique Gateways for the Management Interface with Fallback to Data Interfaces**—If the DHCP server provides a gateway, the system routes management traffic through the Management interface to the gateway. If the DHCP server does not provide a gateway, then the system routes management traffic based on the data interface routing table, typically sending traffic through the outside interface. This option is not supported on the Firewall Threat Defense Virtual devices.
- **Use Unique Gateways for the Management Interface (no Fallback)**—The system routes management traffic through the Management interface to the gateway provided by the DHCP server. If the DHCP server does not provide a gateway, the system will only be able to reach local hosts on the Management interface. To route through data interfaces, choose the Fallback option.

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.

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 Firewall 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 the Firewall 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**.

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 Firewall Threat Defense device supports NTPv4.

Note For the Firepower 4100/9300, you do not set NTP through the Firewall Device Manager. Configure NTP in FXOS.

Procedure

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

If you are already on the System Settings page, simply click **Time Services** 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 Precision Time Protocol (ISA 3000)

The Precision Time Protocol (PTP) is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. These device clocks are generally of varying precision and stability. The protocol is designed specifically for industrial, networked measurement and control systems, and is optimal for use in distributed systems because it requires minimal bandwidth and little processing overhead.

A PTP system is a distributed, networked system consisting of a combination of PTP and non-PTP devices. PTP devices include ordinary clocks, boundary clocks and transparent clocks. Non-PTP devices include network switches, routers and other infrastructure devices.

You can configure the Firewall Threat Defense device to be a transparent clock. The Firewall Threat Defense device does not synchronize its clock with the PTP clocks. The Firewall Threat Defense device will use the PTP default profile, as defined on the PTP clocks.

When you configure the PTP devices, you define a domain number for the devices that are meant to function together. Thus, you can configure multiple PTP domains, and then configure each non-PTP device to use the PTP clocks for one specific domain.

Before you begin

Determine the domain number configured on the PTP clocks that the device should use. Also, determine the interfaces through which the system can reach the PTP clocks in the domain.

Following are guidelines for configuring PTP:

- This feature is only available on the Cisco ISA 3000 appliance.
- Cisco PTP supports multicast PTP messages only.
- PTP is available only for IPv4 networks, not for IPv6 networks.
- PTP configuration is supported on physical Ethernet data interfaces, whether routed or bridge group members. It is not supported on the management interface, subinterfaces, EtherChannels, Bridge Virtual Interfaces (BVI), or any other virtual interfaces.
- PTP flows on VLAN subinterfaces are supported, assuming the appropriate PTP configuration is present on the parent interface.
- You must ensure that PTP packets are allowed to flow through the device. PTP traffic is identified by UDP destination ports 319 and 320, and destination IP address 224.0.1.129, so any access control rule that allows this traffic should work.
- When PTP packets flow between routed interfaces, you must enable multicast routing and each interface should join the 224.0.1.129 IGMP multicast group. When PTP packets flow between interfaces in the same bridge group, you do not need to enable multicast routing and configure the IGMP group.

Procedure

Step 1 Verify the configuration of the PTP clock-facing interfaces.

The default configuration places all interfaces in the same bridge group, but you can remove interfaces from the bridge group. It is important that you determine whether the interfaces are routed, or bridge group members, because you must configure them differently with respect to multicast IGMP groups.

The following procedure explains how to determine which interfaces are part of the bridge group. Check whether the interfaces you are configuring for PTP are bridge group members.

a) Click **View All Interfaces** in **Device** > **Interfaces**.
b) Find the interfaces in the list, and check the Mode column. BridgeGroupMember means it is part of a bridge group, otherwise it should be Routed.

Step 2 Click **Device**, then click the **System Settings** > **Time Services** link.

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

Step 3 Configure the PTP settings:

- **Domain Number**—The domain number that is configured on the PTP devices in your network, from 0-255. Packets received on a different domain are treated like regular multicast packets and will not undergo any PTP processing.
- **Clock Mode**—Select **EndToEndTransparent**. You can operate the device as a PTP transparent clock only.

  You can alternatively select **Forward**, but this is essentially the same as not configuring PTP. The domain number is ignored. PTP packets pass through the device based on the routing table for multicast traffic. This is the default PTP configuration.
- **Interfaces**—Select all of the interfaces through which the system can connect to the PTP clock in your network. PTP is enabled on these interfaces only.

Step 4 Click **Save**.

Step 5 If any of the interfaces you selected are routed interfaces, that is, they are not bridge group members, you need to use FlexConfig to enable multicast routing and to join the routed interfaces to the correct IGMP group.

Do not complete this step if all selected interfaces are bridge group members. You will get a deployment failure if you try to configure IGMP on a bridge group member.

a) Click **View Configuration** in **Device** > **Advanced Configuration**.
b) Click **FlexConfig** > **FlexConfig Objects** in the Advanced Configuration table of contents.
c) Create the object needed to enable multicast routing and to configure the IGMP join for the routed interfaces.

   Following would be the base template for the object. In this example, GigabitEthernet1/2 is the one routed interface on which you are enabling PTP. Change the interface hardware name as appropriate, and if you have more than one routed interface, repeat the **interface** and **igmp** commands for each additional interface.

   The **igmp** command joins the 224.0.1.129 IGMP group. This is the correct IP address for all interfaces regardless of network address.

```
multicast-routing
interface GigabitEthernet1/2
 igmp join-group 224.0.1.129
```

   The negate template would look like the following:

```
no multicast-routing
```

```
interface GigabitEthernet1/2
 no igmp join-group 224.0.1.129
```

d) Click **FlexConfig Policy** in the table of contents, add this object to the FlexConfig policy, and click **Save**.

Verify that the preview shows the expected commands from your object.

What to do next

After you deploy changes, you can verify the PTP settings. From the Firewall Device Manager CLI Console, or an SSH or Console session, issue the various **show ptp** commands. For example, if you configured PTP for domain 10 for GigabitEthernet1/2 only, the output might look like the following:

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/3
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 3
  PTP version: 2
  Port state: Disabled

 PTP PORT DATASET: GigabitEthernet1/4
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 4
  PTP version: 2
  Port state: Disabled
```

Configuring HTTP Proxy for Management Connections

If there is not a direct connection between the system and the Internet, you can set up an HTTP proxy for the management interface. The system will then use the proxy for all management connections, including connections to the Firewall Device Manager and from the system to Cisco for downloading database updates.

You can also configure an HTTP proxy in the Firewall Threat Defense CLI using the **configure network http-proxy** command.

Procedure

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

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

Step 2 Click the toggle to enable the proxy, then configure the proxy settings:

- **HTTP Proxy**—The IP address of the proxy server.
- **Port**—The port number the proxy server is configured to listen to for HTTP connections.
- **Use Proxy Authentication**—Select this option if the server is configured to require authentication for proxied connections. If you select this option, also enter the **Username** and **Password** of an account that can log into the proxy server.

Step 3 Click **Save**, then confirm that you want to make the change.

Your changes are applied immediately. A deployment job is not needed.

Because you are changing how the system completes management connections, you will lose your connection to the Firewall Device Manager. Wait a few minutes for the change to be complete, then refresh your browser window and log in again.

Configuring Cloud Services

You can enroll in Cloud Services so that you can use various cloud-based applications, such as Security Cloud Control, Cisco Threat Response, and the Cisco Success Network.

Once registered in the cloud, the page will show registration status and the type of tenancy, and the account name under which the device is registered.

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.

If your device is not registered, this page shows enrollment methods for registering with the Cisco cloud. After you register with the cloud, you will be able to enable or disable individual cloud services.

Step 2 To register with the Cisco cloud (in evaluation mode or after unregistering from Cloud Services), select one of the following options:

- **Security**/Security Cloud Control **Account**—You can use one of the following methods:
  - **Auto-enroll with Tenancy from Security Cloud Control** (Firepower 1000, 2100, Secure Firewall 3100 only). You can use auto-enrollment instead of obtaining a registration key. First, go to Security Cloud Control and add the device using the device's serial number. Then, in the Firewall Device

Manager, select this check box, and initiate enrollment. Get the serial number from the device chassis or packing slip. For FXOS, you can go into the FXOS CLI and use the **show chassis detail** command to retrieve the correct serial number, labeled Serial (SN). Note that the Firewall Threat Defense command **show serial-number** provides a different serial number, which is not recommended for Security Cloud Control registration. This method works for the cloud-delivered Firewall Management Center in Security Cloud Control, as well as the legacy device manager mode in Security Cloud Control.

Note
Legacy device manager mode is only available to existing users who are already managing Firewall Threat Defense devices in this mode.

- Log into your Security Cloud Control or other security account and generate a registration key. Then return to this page, select your **Cloud Services Region**, and paste in your **Registration Key**. This method only works for the legacy device manager mode in Security Cloud Control. For the cloud-delivered management center in Security Cloud Control, see Switch from the Device Manager to the Management Center or Security Cloud Control.

  Note
  Legacy device manager mode is only available to existing users who are already managing Firewall Threat Defense devices in this mode.

  You can also at this time enable **Security Cloud Control** and **Cisco Success Network**. These are enabled by default.

- **Smart License**—(Only if you will not use Security Cloud Control.) Click the link to go to the Smart Licensing page and register with CSSM. Registering with CSSM also registers the device with Cloud Services.

  Note
  If you unregistered from Cloud Services, then the Smart License approach to registration has some additional steps. In this case, select your **Cloud Services Region**, then click **Register**. Read the disclosure and click **Accept**.

Step 3 Once you have registered for Cloud Services, you can enable or disable features as needed. See the following topics:

- Enabling or Disabling Security Cloud Control (Legacy Device Manager Mode)
- Connecting to the Cisco Success Network, on page 28
- Sending Events to the Cisco Cloud, on page 29
- Unregistering from Cloud Services, on page 30

Enabling or Disabling Security Cloud Control (Legacy Device Manager Mode)

Note This section only applies to the legacy device manager mode in Security Cloud Control, not the cloud-delivered management center.

If you enrolled in Cloud Services using a registration key from Security Cloud Control, as recommended in Configuring Cloud Services, on page 26, the device is already registered with Security Cloud Control. Afterward, you can disable or re-enable the connection as desired.

If the device is registered to Cloud Services using Smart Licensing, you will have problems if you enable Security Cloud Control: the device will not show up in the Security Cloud Control inventory. We strongly recommend that you first unregister the device from the Cloud Services; select **Unregister Cloud Services** from the gear ( ) drop-down list. After you unregister, get a registration token from Security Cloud Control and re-register using the token and your security account as explained in Configuring Cloud Services, on page 26.

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

Before you begin

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 the **Enable**/**Disable** button for the Security Cloud Control feature to change the setting as appropriate.

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 Unregistering from Cloud Services, on page 30.

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 Security Cloud Control by entering a registration key (legacy device manager mode in Security Cloud Control 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**.

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 to analyze the events and to evaluate threats that the device might have encountered.

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 Security Cloud Control can make use of all connection events.
- Threat Reponse uses high priority connection events only, so there is no need to send all connection events to the cloud. In addition, it will use only the Security Intelligence high-priority events.

Before you begin

You must enroll the device with Cloud Services before you can enable this service.

You can connect to Threat Response at https://visibility.amp.cisco.com/ in the US region, https://visibility.eu.amp.cisco.com in the EU region, and https://visibility.apjc.amp.cisco.com in the APJC region. You can watch videos about the use and benefits of the application on YouTube at http://cs.co/CTRvideos. For more information, 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.

Step 3 When you are enabling the service, you are prompted to select the events to send to the cloud. Later, you can change these selections by clicking **Edit** next to the list of selected events. Select the types of events to send and click **OK**.

- **File/Malware**—For any file policies you have applied in any access control rule.
- **Intrusion**—For any intrusion policies you have applied in any access control rule.
- **Connection**—For access control rules where you have enabled logging. When you select this option, you can also elect to send All Connection Events, or only send the High Priority connection events. High-priority connection events are those related to connections that trigger intrusion, file, or malware events, or that match Security Intelligence blocking policies.

Unregistering from Cloud Services

If you no longer want to use any cloud services, you can unregister the device from the cloud. You might want to unregister when you are removing the device from service or otherwise disposing of it. If you need to change your cloud services region, you unregister, then select the new region when you re-register.

Unregistering from the cloud using this procedure has no impact on Smart Licensing registration.

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 Select **Unregister Cloud Services** from the gear ( ) drop-down list.

Step 3 Read the warning and click **Unregister**.

Any cloud services you had enabled will be automatically disabled, and your ability to enable them again will be removed. However, you will now see the controls for registering with the cloud, and you can re-register.

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** > **Web Analytics** link.

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

Step 2 Click the **Enable**/**Disable** control for the **Web Analytics** feature to change the setting as appropriate.

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.
- **URL Query Source**—Which source to query to obtain the category and reputation for a URL.

- **Local Database Only**—Look for category and reputation in the local URL filtering database only. If there are no matches, the URL will be uncategorized with no reputation. This method can be limited, especially on lower-end systems that have limited storage, and thus a smaller URL filtering database.
- **Local Database and Cisco Cloud**—If there are no matches in the local database, the Cisco Cloud is queried for updated category/reputation information. If a response is received in a timely fashion, it is used for matching purposes. Otherwise, and if there is no match, the URL will be uncategorized with no reputation.
- **Cisco Cloud Only**—Always query the Cisco Cloud for category and reputation information. Do not use the local URL database.

- **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**.

Switch from the Firewall Device Manager to the Firewall Management Center or Security Cloud Control

You can configure the Firewall Threat Defense device to connect to the Firewall Management Center or Security Cloud Control for management if you want to switch from the Firewall Device Manager.

Note Security Cloud Control can manage Firewall Threat Defense devices using the cloud-delivered management center. The simplified, device manager functionality in Security Cloud Control is only available to existing users who are already managing Firewall Threat Defenses in this mode. This procedure only applies to the cloud-delivered management center.

When you perform the Firewall Management Center/Security Cloud Control setup using the Firewall Device Manager, *all* interface configuration completed in the Firewall Device Manager is retained when you switch to the Firewall Management Center/Security Cloud Control for management, in addition to the Management interface and the manager access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. When you use the Firewall Threat Defense CLI for initial setup for the Firewall Management Center/Security Cloud Control, only the Management interface and the manager access settings are retained (for example, the default inside interface configuration is not retained).

After you switch to the Firewall Management Center/Security Cloud Control, you can no longer use the Firewall Device Manager to manage the Firewall Threat Defense device.

Before you begin

If the firewall is configured for high availability, you must first break the high availability configuration using the Firewall Device Manager (if possible) or the **configure high-availability disable** command. Ideally, break high availability from the active unit.

Procedure

Step 1 If you registered the firewall to the Cisco Smart Software Manager, you must unregister before switching managers. See Unregistering the Device.

Unregistering the firewall frees the base license and all feature licenses. If you do not unregister the firewall, those licenses remain assigned to the firewall in Cisco Smart Software Manager.

Step 2 (Might be required) Configure the Management interface. See Configuring the Management Interface, on page 20.

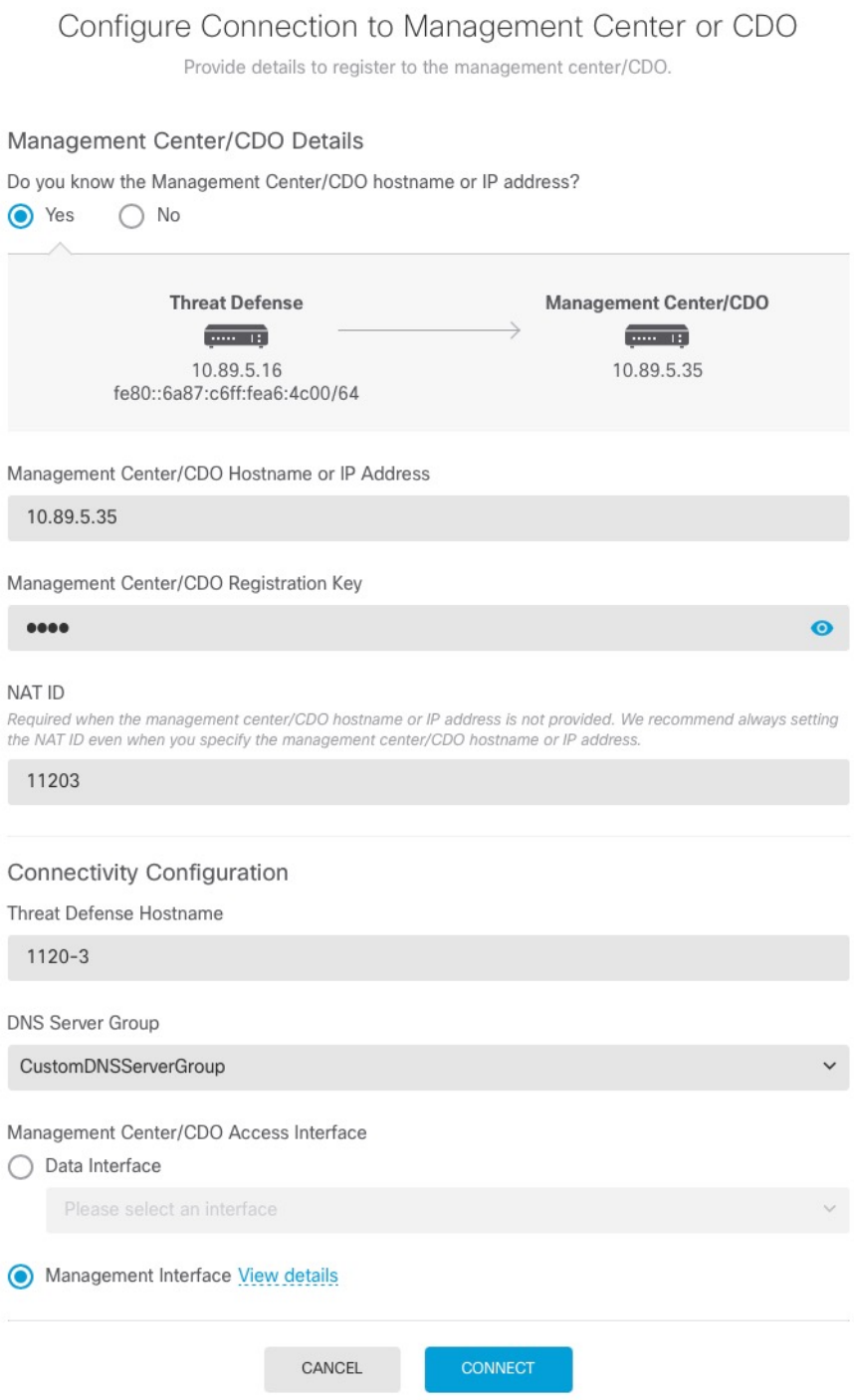
You may need to change the Management interface configuration, even if you intend to use a data interface for manager access. You will have to reconnect to the Firewall Device Manager if you were using the Management interface for the Firewall Device Manager connection.

- Data interface for manager access—The Management interface must have the gateway set to data interfaces. By default, the Management interface receives an IP address and gateway from DHCP. If you do not receive a gateway from DHCP (for example, you did not connect this interface to a network), then the gateway will default to data interfaces, and you do not need to configure anything. If you did receive a gateway from DHCP, then you need to instead configure this interface with a static IP address and set the gateway to data interfaces.
- Management interface for manager access—If you want to configure a static IP address, be sure to also set the default gateway to be a unique gateway instead of the data interfaces. If you use DHCP, then you do not need to configure anything assuming you successfully get the gateway from DHCP.

Step 3 Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the Firewall Management Center/Security Cloud Control management.

Step 4 Configure the **Management Center/CDO Details**.

Figure 1: Management Center/Security Cloud Control Details



a) For **Do you know the Management Center/CDO hostname or IP address?**, click **Yes** if you can reach the Firewall Management Center/Security Cloud Control using an IP address or hostname, or **No** if the Firewall Management CenterSecurity Cloud Control is behind NAT or does not have a public IP address or hostname.

At least one of the devices, either the Firewall Management Center/Security Cloud Control or the Firewall Threat Defense device, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices.

b) If you chose **Yes**, then enter the **Management Center/CDO Hostname or IP Address**.

c) Specify the **Management Center/CDO Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the Firewall Management Center/Security Cloud Control when you register the Firewall Threat Defense device. The registration key must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple devices registering to the Firewall Management Center/Security Cloud Control.

a) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the Firewall Management Center/Security Cloud Control. The NAT ID must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID *cannot* be used for any other devices registering to the Firewall Management Center/Security Cloud Control. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked. We recommended that you always use the NAT ID even when it is optional, but it is required if:

- You set the Firewall Management Center IP address to **DONTRESOLVE**.
- When adding the device on the Firewall Management Center, you do not specify a reachable device IP address or hostname.
- You use the data interface for management, even if you specify IP addresses on both sides.
- The Firewall Management Center uses multiple management interfaces.

Step 5 Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

If you use a data interface for the **Management Center/CDO Access Interface** access, then this FQDN will be used for this interface.

b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

If you intend to choose a data interface for the **Management Center/CDO Access Interface**, then this setting sets the *data* interface DNS server. The Management DNS server that you set with the setup wizard is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface. You are likely to choose the same DNS server group that you used for Management, because both management and data traffic reach the DNS server through the outside interface.

On the Firewall Management Center/Security Cloud Control, the data interface DNS servers are configured in the Platform Settings policy that you assign to this Firewall Threat Defense device. When you add the Firewall Threat Defense device to the Firewall Management Center/Security Cloud Control, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the Firewall Threat Defense device that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively

configure the DNS Platform Settings to match this setting to bring the Firewall Management Center/Security Cloud Control and the Firewall Threat Defense device into sync.

Also, local DNS servers are only retained by the Firewall Management Center/Security Cloud Control if the DNS servers were discovered at initial registration.

If you intend to choose the Management interface for the **Management Center/CDO Access Interface**, then this setting configures the Management DNS server.

c) For the **Management Center/CDO Access Interface**, choose any configured interface.

You can change the manager interface after you register the Firewall Threat Defense device to the Firewall Management Center/Security Cloud Control, to either the Management interface or another data interface.

Step 6 (Optional) If you chose a data interface, and it was not the outside interface, then add a default route.

You will see a message telling you to check that you have a default route through the interface. If you chose outside, you already configured this route as part of the setup wizard. If you chose a different interface, then you need to manually configure a default route before you connect to the Firewall Management Center/Security Cloud Control. See Configuring Static Routes for more information about configuring static routes.

If you chose the Management interface, then you need to configure the gateway to be a unique gateway before you can proceed on this screen. See Configuring the Management Interface, on page 20.

Step 7 (Optional) If you chose a data interface, click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the Firewall Management Center/Security Cloud Control can reach the Firewall Threat Defense device at its Fully-Qualified Domain Name (FQDN) if the IP address changes. See **Device** > **System Settings** > **DDNS Service** to configure DDNS.

If you configure DDNS before you add the Firewall Threat Defense device to the Firewall Management Center/Security Cloud Control, the Firewall Threat Defense device automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the Firewall Threat Defense device can validate the DDNS server certificate for the HTTPS connection. Firewall Threat Defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

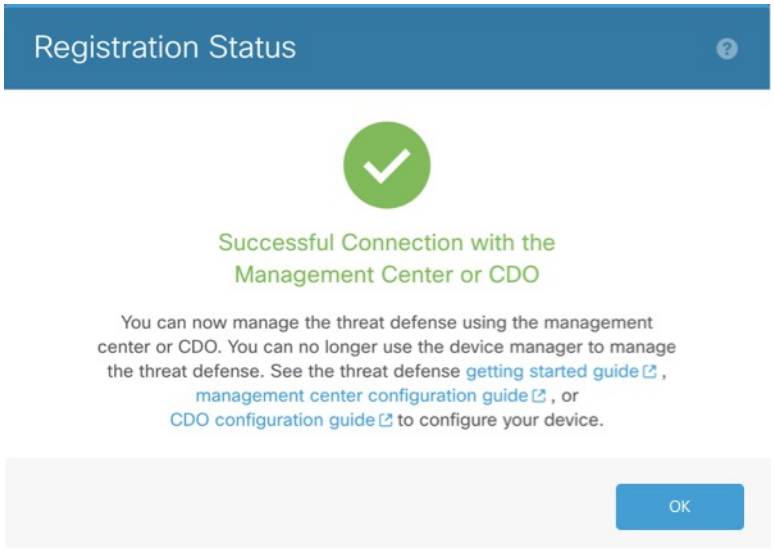
DDNS is not supported when using the Management interface for manager access.

Step 8 Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the Firewall Management Center/Security Cloud Control. After the **Saving Management Center/CDO Registration Settings** step, go to the Firewall Management Center/Security Cloud Control, and add the firewall.

If you want to cancel the switch to the Firewall Management Center/Security Cloud Control, click **Cancel Registration**. Otherwise, do not close the Firewall Device Manager browser window until after the **Saving Management Center/CDO Registration Settings** step. If you do, the process will be paused, and will only resume when you reconnect to the Firewall Device Manager.

If you remain connected to the Firewall Device Manager after the **Saving Management Center/CDO Registration Settings** step, you will eventually see the **Successful Connection with Management Center/CDO** dialog box, after which you will be disconnected from the Firewall Device Manager.

Figure 2: Successful Connection



Switch from the Firewall Management Center or Security Cloud Control to the Firewall Device Manager

You can configure the Firewall Threat Defense device currently being managed by the on-premises or cloud-delivered Firewall Management Center to use the Firewall Device Manager instead.

You can switch from the Firewall Management Center to the Firewall Device Manager without reinstalling the software. Before switching from the Firewall Management Center to the Firewall Device Manager, verify that the Firewall Device Manager meets all of your configuration requirements. If you want to switch from the Firewall Device Manager to the Firewall Management Center, see Switch from the Firewall Device Manager to the Firewall Management Center or Security Cloud Control, on page 32.

Caution Switching to the Firewall Device Manager erases the device configuration and returns the system to the default configuration. However, the Management IP address and hostname are preserved.

Procedure

Step 1 In the Firewall Management Center, delete the firewall from the **Devices** > **Device Management** page.

Step 2 Connect to the Firewall Threat Defense CLI using SSH or the console port. For SSH, open a connection to the **management IP address**, and log into the Firewall Threat Defense CLI with the **admin** username (or any other user with admin privileges).

The console port defaults to the FXOS CLI. Connect to the Firewall Threat Defense CLI using the **connect ftd** command. The SSH session connects directly to the Firewall Threat Defense CLI.

If you cannot connect to the management IP address, do one of the following:

- Ensure that the Management physical port is wired to a functioning network.
- Ensure that the management IP address and gateway are configured for the management network. Use the **configure network ipv4/ipv6 manual** command.

Step 3 Verify you are currently in remote management mode.

show managers

Example:

```
> show managers
Type                      : Manager
Host                      : 10.89.5.35
Display name              : 10.89.5.35
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
```

Step 4 Delete the remote manager and go into no manager mode.

configure manager delete *uuid*

You cannot go directly from remote management to local management. If you have more than one manager defined, you need to specify the identifier (also known as the UUID; see the **show managers** command). Delete each manager entry separately.

Example:

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

Step 5 Configure the local manager.

configure manager local

You can now use a web browser to open the local manager at **https://***management-IP-address*.

Example:

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

Configuring TLS/SSL Cipher Settings

The SSL cipher settings control which TLS versions and encryption cipher suites are allowed for TLS/SSL connections to the device.

Normally, the cipher suite you configure should have more than one available encryption cipher suite. The system will determine the highest TLS version that both the client and Firewall Threat Defense device support, then pick a cipher suite that both support that is compatible with the TLS version. The system will select the strongest TLS version and cipher suite supported by both endpoints to ensure the most secure connection possible among the ciphers you allow.

Before you begin

By default, the system uses the DefaultSSLCipher object to define the allowed cipher suites. You can instead choose one of the other pre-defined cipher objects, or create your own custom object. Ideally, create a single object that includes all and only the TLS versions and ciphers that you want to allow. To create your own object, see Configure TLS/SSL Cipher Objects, on page 39.

Procedure

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

Step 2 Configure the **SSL Settings**:

These settings control the ciphers clients are allowed to use when establishing remote access VPN connections.

- **Ciphers**—Select the SSL Cipher objects that define the TLS versions and encryption algorithms that are allowed.

  Click **Create New Cipher** at the bottom of the list if you need to create an object now.

- **Ephemeral Diffie-Hellman Group**—The DH group to use for ephemeral encryption algorithms. For an explanation of the DH groups, see Decide which Diffie-Hellman modulus group to use. The default is 14.

- **Elliptical Curve DH Group**—The DH group to use for elliptical curve encryption algorithms. The default is 19.

Step 3 Click **Save**.

Configure TLS/SSL Cipher Objects

SSL Cipher objects define a combination of security level, TLS/DTLS protocol versions, and encryption algorithms that can be used when establishing an SSL connection to an Firewall Threat Defense device. Use these objects in **Device** > **System Settings** > **SSL Settings** to define the security requirements for users who make SSL connections to the box.

The TLS versions and ciphers that you can select is controlled by your Smart License account. If you satisfy export compliance requirements, you can select any combination of options. If your license is not export

compliant, you are limited to TLSv1.0 and DES-CDC-SHA, which are the lowest security options. Evaluation mode is considered a non-compliant mode, so your options are limited until you license the system.

The system includes several pre-defined objects. You need to create new objects only if the pre-defined objects do not fit your security requirements. The objects are:

- DefaultSSLCipher—This is a low-security level group. It is the default used in the SSL settings, to ensure that as many clients as possible can complete connections to the system. It includes all protocol versions and ciphers supported by the system.
- CiscoRecommendedCipher—This is a high-security level group, which includes only the most secure ciphers and TLS version. This group provides the highest security, but you need to ensure that your clients can use the matching ciphers. There is a greater likelihood that some clients will be unable to complete connections due to cipher miss-match problems.

Procedure

Step 1 Select **Objects**, then select **SSL Ciphers** 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 Enter a **Name** for the object and optionally, a description.

Step 4 Configure the following options:

- **Security Level**—The relative security level for the object. Note that if you edit the protocol versions or cipher suite list after selecting a security level, the actual level of security provided by the object might not match the security level. Choose one of the following:
  - **All**—Include all TLS levels and cipher suites in the object, from low to high security.
  - **Low**—Includes all the TLS versions and ciphers, which allows users to complete connections with the least secure ciphers. For a non-export compliant license, this includes TLSv1.0 and DES-CBC-SHA.
  - **Medium**—Includes all of the TLS versions, but removes some relatively insecure ciphers. There is only a minimal difference between this option and the Low/All option. You cannot use this option with non-export compliant licenses.
  - **High**—Allows the latest DTLS and TLS versions only, and the ciphers that work with these versions. This option limits connections to the currently most-secure ciphers available. You cannot use this option with non-export compliant licenses.
  - **Custom**—Select this option if you want to select TLS versions and ciphers individually. The options you select will dictate whether you are defining a high or low security encryption setting. Although there are no defaults for a custom object, if you selected another level before selecting custom, the previously displayed options remain selected for your convenience.

- **Protocol Versions**—The TLS/DTLS versions that a client is allowed to use when establishing a TLS/SSL connection to the Firewall Threat Defense device. For a custom object, select the versions you want to support. For other security levels, ideally you should not edit the list, but you can add or remove versions as desired.
- **Applicable Cipher Suites**—The encryption algorithms that the client can use. Click **+** to add new suites; click **x** on a suite to remove it.

  Your selection of protocol version controls which suites are available in this list. If you change the protocol versions, any selected suite that no longer works with the selected versions is flagged: you must remove these, or add back the required protocol version.

Step 5 Click **OK**.