clf - cz

cluster disable

To disable clustering on a unit, use the **cluster disable** command.

cluster disable

Command History

Release	Modification
6.5	This command was introduced.

Usage Guidelines

This command lets you manually remove a cluster unit from the cluster. This command leaves the clustering configuration intact so you can later re-add it to the cluster using the **cluster enable** command.

Examples

The following example disables clustering on a unit:

```
> cluster disable
```

Related Commands

Command	Description
cluster enable	Enables clustering.
cluster master unit	Sets a new unit as the master unit of a cluster.
cluster remove unit	Removes the unit from the cluster.
show cluster info	Shows cluster information.
cluster exec	Sends a command to all cluster members.

cluster enable

To enable clustering on a unit, use the **cluster enable** command.

cluster enable

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

For the first unit enabled, a master unit election occurs. Because the first unit should be the only member of the cluster so far, it will become the master unit. Do not perform any configuration changes during this period.

Examples

The following example enables clustering on a unit:

```
> cluster enable
```

Related Commands

Command	Description
cluster disable	Disables clustering.
cluster master unit	Sets a new unit as the master unit of a cluster.
cluster remove unit	Removes the unit from the cluster.
show cluster info	Shows cluster information.
cluster exec	Sends a command to all cluster members.

cluster exec

To execute a command on all units in the cluster, or on a specific member, use the **cluster exec** command.

cluster exec [**unit** *unit_name*] *command*

Syntax Description

unit *unit_name*	(Optional) Performs the command on a specific unit. To view member names, enter **cluster exec unit ?** (to see all names except the current unit), or enter the **show cluster info** command.
command	Specifies the command you want to execute.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Sending a **show** command to all members collects all output and displays it on the console of the current unit. Other commands, such as **capture** and **copy**, can also take advantage of cluster-wide execution.

Examples

To copy the same capture file from all units in the cluster at the same time to a TFTP server, enter the following command on the master unit:

```
> cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as capture1_device1.pcap, capture1_device2.pcap, and so on. In this example, device1 and device2 are cluster unit names.

The following sample output for the **cluster exec show port-channel** summary command shows EtherChannel information for each member in the cluster:

```
> cluster exec show port-channel summary
primary(LOCAL):*********************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 secondary:*****************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

Related Commands

Command	Description
cluster enable	Enables clustering on a unit.
cluster master unit	Sets a new unit as the master unit of a cluster.
cluster remove unit	Removes the unit from the cluster.
show cluster info	Shows cluster information.
cluster exec	Sends a command to all cluster members.

cluster exec clear rule hits

To clear rule hit information for all evaluated rules of access control policies and prefilter policies and reset them to zero, from all nodes in a cluster, use the **cluster exec clear rule hits** command.

cluster exec clear rule hits [*id*]

Syntax Description

id	(Optional) The ID of a rule. Including this argument clears the rule hit information only of the specified rule . Use the **show access-list** command to identify a rule ID. However, not all the rules are listed in the output of this command. You can trigger a REST API GET operation on the following URLs to see all the rules and their IDs: • `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true` • `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`

Command Default

If you do not specify a rule ID, the rule hit information for all the rules are cleared and reset to zero.

Note Exercise caution while using this command as the action is irreversible.

Command History

Release	Modification
6.4	This command was introduced.

Usage Guidelines

The rule hit information covers only the access control rules and prefilter rules.

Examples

Following is an example of clearing all rule hit information:

```
> cluster exec clear rule hits
```

Related Commands

Command	Description
show cluster rule hits	Display rule hit information for all evaluated rules of access control policies and prefilter policies from all nodes of a cluster in an aggregated format.
cluster exec show rule hits	Display rule hit information for all evaluated rules of access control policies and prefilter policies from each node of a cluster in a segregated format.

Command	Description
show rule hits	Displays the rule hit information for all evaluated rules of access control policies and prefilter policies.
clear rule hits	Clears the rule hit information for all evaluated rules of access control policies and prefilter policies and resets them to zero.

cluster exec show rule hits

To display rule hit information for all evaluated rules of access control policies and prefilter policies, from each node of a cluster in a segregated format, use the **cluster exec show rule hits** command.

cluster exec show rule hits [*id* | **raw** | **gt** *#hit-count* | **lt** *#hit-count* | **range** *#hit-count1 #hit-count2*]

Syntax Description

id	(Optional) The ID of a rule. Including this argument limits the displayed information to the specified rule. Use the **show access-list** command to identify a rule ID. However, not all the rules are listed in the output of this command. You can trigger a REST API GET operation on the following URLs to see all the rules and their IDs: • `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true` • `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`
raw	(Optional) Displays the rule hit information in .csv format.
gt *#hit-count*	(Optional) Displays all the rules that have a hit count greater than #hit-count.
lt *#hit-count*	(Optional) Displays all the rules that have a hit count lesser than #hit-count.
range *#hit-count1 #hit-count2*	(Optional) Displays all the rules that have a hit count in-between #hit-count1 and #hit-count2.

Command Default

If you do not specify a rule ID, the rule hit information for all the rules are shown.

Command History

Release	Modification
6.4	This command was introduced.

Usage Guidelines

The rule hit information covers only the access control rules and prefilter rules.

Examples

The following example displays rule hit information from each node of a cluster in a segregated format:

```
> cluster exec show rule hits
unit-1-1(LOCAL):*******************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
-------------------------------------------------------------------------------------
268435260            1                   06:55:17 Mar 8 2019     06:55:17 Mar 8 2019
268435261            1                   06:55:19 Mar 8 2019     06:55:19 Mar 8 2019
```

```
unit-1-3:**************************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
-------------------------------------------------------------------------------------
268435264            1                   06:54:43 Mar 8 2019     06:54:43 Mar 8 2019
268435265            1                   06:54:57 Mar 8 2019     06:54:57 Mar 8 2019


unit-1-2:**************************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
-------------------------------------------------------------------------------------
268435270            1                   06:54:53 Mar 8 2019     06:54:53 Mar 8 2019
268435271            1                   06:55:01 Mar 8 2019     06:55:01 Mar 8 2019
```

Related Commands

Command	Description
cluster exec clear rule hits	Clears rule hit information for all evaluated rules of access control policies and prefilter policies and reset them to zero, from all nodes in a cluster.
show cluster rule hits	Display rule hit information for all evaluated rules of access control policies and prefilter policies from all nodes of a cluster in an aggregated format.
show rule hits	Displays the rule hit information for all evaluated rules of access control policies and prefilter policies.
clear rule hits	Clears the rule hit information for all evaluated rules of access control policies and prefilter policies and resets them to zero.

cluster master unit

To set a new unit as the master unit of a device cluster, use the **cluster master unit** command.

cluster master unit *unit_name*

Syntax Description

unit_name	Specifies the local unit name to be the new master unit. To view member names, enter **cluster master unit ?** (to see all names except the current unit), or enter the **show cluster info** command.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

You will need to reconnect to the main cluster IP address.

Examples

The following example sets **device2** as the master unit:

```
> cluster master unit device2
```

Related Commands

Command	Description
cluster enable	Enables clustering on a unit.
cluster exec	Sends a command to all cluster members.
cluster remove unit	Removes the unit from the cluster.
show cluster info	Shows cluster information.

cluster remove unit

To remove the unit from the cluster, use the **cluster remove unit** command.

cluster remove unit *unit_name*

Syntax Description

unit_name	Specifies the local unit name to remove from the cluster. To view member names, enter **cluster remove unit ?**, or enter the **show cluster info** command.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The bootstrap configuration remains intact, as well as the last configuration synced from the master unit, so you can later re-add the unit without losing your configuration. If you enter this command on a slave unit to remove the master unit, a new master unit is elected.

Examples

The following example checks for unit names, and then removes device2 from the cluster:

```
> cluster remove unit ?
Current active units in the cluster:
device2
> cluster remove unit device2
WARNING: Clustering will be disabled on unit device2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

Related Commands

Command	Description
cluster enable	Enables clustering on a unit.
cluster exec	Sends a command to all cluster members.
cluster master unit	Sets a new unit as the master unit of a cluster.
show cluster info	Shows cluster information.

cluster reset-interface-mode

To convert a cluster unit to standalone mode after disabling clustering, use the **cluster reset-interface-mode** command.

cluster reset-interface-mode

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You must first disable clustering using the **cluster disable** command. The **cluster reset-interface-mode** command clears the threat defense configuration and reboots the logical device. In FXOS for the 4100 series, the logical device is also converted to a standalone type device. The bootstrap configuration and interface assignments are maintained.

Examples

The following example disables clustering and then removes the clustering configuration:

```
> cluster disable
> cluster reset-interface-mode

Broadcast message from root@firepower (Tue Apr 27 18:36:12 2021):

The system is going down for reboot NOW!
```

Related Commands

Command	Description
cluster enable	Enables clustering on a unit.
cluster exec	Sends a command to all cluster members.
cluster master unit	Sets a new unit as the master unit of a cluster.
show cluster info	Shows cluster information.

configure cert-update auto-update

To enable or disable the automatic update of CA certificates on the threat defense device, use the **configure cert-update auto-update** command.

configure cert-update auto-update { **enable** | **disable** }

Syntax Description

enable	Enables automatic update of CA certificates.
disable	Disables automatic update of CA certificates.

Command History

Release	Modification
7.0.5	This command was introduced.

Usage Guidelines

By default, the CA certificates are automatically updated when you install or upgrade threat defense to version 7.0.5. If you want to disable this feature, use the **disable** keyword. To re-enable the automatic update of the CA bundles, use the **enable** keyword. When you enable the automatic update on the CA certificates, the update process is executed daily at a system-defined time.

Examples

The following is sample output from the **configure cert-update auto-update** command:

```
> configure cert-update auto-update disable
Autoupdate is disabled
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

Related Commands

Command	Description
show cert-update	Displays the status of automatic update of CA certificates.
configure cert-update run-now	Instantly attempt to update CA certifications.
configure cert-update test	Performs connection checks using the latest CA certificates from the Cisco server.

configure cert-update run-now

To instantly execute automatic update of CA certificates, use the **configure cert-update run-now** command.

configure cert-update run-now [**force**]

Syntax Description

force	Performs CA certificate updates, even when connection check fails.

Command History

Release	Modification
7.0.5	This command was introduced.

Usage Guidelines

When you want to instantly update the CA certificates, use the **configure cert-update run-now**. However, if the SSL connectivity check fails for even one of the Cisco servers, the process is terminated. To proceed with the update despite connection failures, use the **force** keyword. For example, the local CA bundle has certificates to access several Cisco services such as smart licensing, AMP registration, and ThreatGrid service, and if the connection to the Cisco smart licensing service fails, the certificates update process is still executed if you use the **configure cert-update run-now force** command.

Note In an IPv6-only deployment, the automatic update of CA certificates may fail, because, some of the Cisco servers do not support IPv6. In such cases, force update the CA certificates using the **configure cert-update run-now force** command.

Examples

Following is a sample output from the **configure cert-update run-now** command when the connection check fails:

```
> configure cert-update run-now
Certs failed some connection checks.
```

Following is a sample output from the **configure cert-update run-now** command when the connection check succeeds and local CA bundle is updated:

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

Following is a sample output from the **configure cert-update run-now force** command:

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

Related Commands

Command	Description
configure cert-update auto-update	Enables or disables automatic update of CA certificates every day.

Command	Description
show cert-update	Displays the status of automatic update of CA certificates.
configure cert-update test	Performs connection checks using the latest CA certificates from the Cisco server.

configure cert-update test

To verify the CA certificates in the local system are the latest, and if they are out of date, to test the SSL connectivity to the servers using the new CA bundle, use the **configure cert-update test** command.

configure cert-update test

Command History

Release	Modification
7.0.5	This command was introduced.

Usage Guidelines

The **configure cert-update test** command compares the CA bundle on the local system with the latest CA bundle (from the Cisco server). If the CA bundle is up to date, no check is executed and the test result is displayed as shown in the Examples section below. If the CA bundle is out of date, the connection check is executed on the downloaded CA bundle and the results are displayed as shown in the Examples section below.

Examples

Following is a sample output from the **configure cert-update test** command when the local CA bundle is up to date:

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

Following is a sample output from the **configure cert-update test** command when the local CA bundle is out of date and the connection check on the downloaded bundle fails:

```
> configure cert-update test
Test failed, not able to fully connect.
```

Following is a sample output from the **configure cert-update test** command when the local CA bundle is out of date and the connection check on the downloaded bundle succeeds or the CA bundle is already up to date:

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

Related Commands

Command	Description
configure cert-update auto-update	Enables or disables automatic update of CA certificates every day.
show cert-update	Displays the status of automatic update of CA certificates.
configure cert-update run-now	Instantly attempt to update CA certifications.

configure coredump packet-engine

To enable or disable packet-engine coredump generation, use the **configure coredump packet-engine** command.

configure coredump packet-engine {**enable** | **disable**}

Syntax Description

disable	Disables the packet-engine coredump generation.
enable	Enables the packet-engine coredump generation.

Command History

Release	Modification
6.2.1	This command was introduced.

Usage Guidelines

Packet-engine coredump generation is enabled by default.

This command is only available on the Firepower 2100 series. When you run this command on an unsupported platform, the system returns the following message:

```
This command is not available on this platform.
```

Examples

The following example disables packet-engine coredump generation.

```
> configure coredump packet-engine disable
```

Related Commands

Command	Description
show coredump	Displays the packet-engine coredump generation settings.

configure coredump snort3

To enable or disable the Snort 3 core dump generation, use the **configure coredump snort3** command.

configure coredump snort3 { **enable** [**daily** | **weekly** | **once**] | **disable** }

Syntax Description

disable	Disables the Snort 3 full core dump generation.
enable	Enables the Snort 3 full core dump generation at all times, removing additional conditions, if present. The additional conditions are the core dump collection time periods, that is, **daily**, **weekly**, and **once**.

Command Default

Snort 3 full core dump generation is disabled by default for a standalone setup. For high availability and cluster setups, the default core dump generation is **daily**.

Command History

Release	Modification
6.7	This command was introduced.

Usage Guidelines

Use the **configure coredump snort3** command to trigger the generation of a core dump in case of a Snort 3 crash.

High Availability

For high-availability setups, use the **configure coredump snort3** command to avoid traffic disruption and outage. Snort 3 core dump collection occurs:

- If the standby device is in **Healthy** state on active devices.
- If the device is not in **Active** state.

Cluster

For cluster setups, use the **configure coredump snort3** command to avoid traffic disruption and outage. Snort 3 core collection occurs for a Snort 3 crash only if there are at least two nodes in a cluster and the traffic passes through the second node.

Examples

The following example shows how to enable the Snort 3 core dump generation at all times:

```
> configure coredump snort3 enable
```

Related Commands

Command	Description
show coredump	Displays the packet-engine core dump generation settings.

configure disable-https-access

To clear the HTTPS access list, configuring the device to reject HTTPS connection attempts from all IP addresses, use the **configure disable-https-access** command.

configure disable-https-access

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to disable HTTPS access to the device. HTTPS access is required when using the local manager, device manager.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

Examples

The following example configures the device to reject HTTPS connections from any address:

```
> configure disable-https-access
```

Related Commands

Command	Description
configure https-access-list	Configures the device to accept HTTPS connections from specified IP addresses.
show https-access-list	Shows the current HTTPS access list.

configure disable-ssh-access

To clear the SSH access list, configuring the device to reject SSH connection attempts from all IP addresses, use the **configure disable-ssh-access** command.

configure disable-ssh-access

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to disable SSH access to the device. This prevents CLI access except through the Console port.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

Examples

The following example configures the device to reject SSH connections from any address:

```
> configure disable-ssh-access
```

Related Commands

Command	Description
configure ssh-access-list	Configures the device to accept SSH connections from specified IP addresses.
show ssh-access-list	Shows the current SSH access list.

configure firewall

To set the firewall mode to transparent or routed mode, use the **configure firewall** command.

configure firewall {**routed** | **transparent**}

Syntax Description

routed	Sets the firewall mode to routed firewall mode.
transparent	Sets the firewall mode to transparent firewall.

Command Default

By default, the device is in routed mode.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

A transparent firewall is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices.

When you change modes, the device clears the configuration because many commands are not supported for both modes. If you already have a populated configuration, be sure to back up your configuration before changing the mode; you can use this backup for reference when creating your new configuration.

Note You cannot switch to transparent firewall mode if you are using the device manager. If you are using the local manager and you want to convert to transparent mode, you must first use **configure manager delete** to remove the manager, convert to transparent mode, then use **configure manager add** to point to the management center.

Examples

The following example changes the firewall mode to transparent:

```
> configure firewall transparent
```

Related Commands

Command	Description
show running-config	Shows the running configuration.
show firewall	Shows the firewall mode.

configure flow-offload

This command enables or disables accelerating certain flows (that is, traffic) by processing them in hardware. Offloading flow processing to hardware increases performance, and is enabled by default.

Dynamic flow offload is supported on the threat defense on the Firepower 4100/9300 chassis. Dynamic flow offload enables you to select traffic to be offloaded to hardware, which means it is not processed by the software or CPU of your threat defense device.

configure flow-offload dynamic whitelist {enable | disable}

Syntax Description

dynamic whitelist enable	Enable dynamic offload.
dynamic whitelist disable	Disable dynamic offload.

Command Default

Enabled by default.

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

For information about dynamic flow offload support and limitations, see the chapter on common rule characteristics in the *Management CenterConfiguration Guide*.

Examples

Following is an example of disabling dynamic offload:

```
> configure flow-offload dynamic whitelist disable
```

Following is an example of enabling dynamic offload:

```
> configure flow-offload dynamic whitelist enable
```

Related Commands

Commands	Description
show flow-offload	Displays dynamic flow offload counters, statistics, and information.
clear flow-offload	Clears dynamic flow offload flows, counters, or statistics.

configure high-availability

To disable, suspend, or resume a high-availability configuration (also known as failover) between devices, use the **configure high-availability** command.

configure high-availability { **disable** [**clear-interfaces**] | **resume** | **suspend** [**clear-interfaces**] }

Syntax Description

clear-interfaces	(Optional) Clears interface configurations upon disabling or suspending high availability.
disable	Breaks the high-availability relationship between this device and its peer. You cannot use this option on a locally-managed device; use device manager instead. If you mistakenly use the **disable** command, you must follow it with an threat defense API call using the BreakHAStatus resource to complete the action.
resume	Resumes a temporarily suspended high-availability configuration between this device and its peer. The unit will negotiate active/standby status with the peer unit. You cannot resume a disabled configuration.
suspend	Temporarily suspends a high-availability configuration between this device and its peer. You can later resume the configuration. If you suspend high availability from the active unit, the configuration is suspended on both the active and standby unit. If you suspend it from the standby unit, it is suspended on the standby unit only, but the active unit will not attempt to fail over to a suspended unit.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

You can configure two devices as a high-availability pair. This is also known as a failover configuration, where one device can take over if the other device in the pair fails.

You can use the **configure high-availability** command to manage the high-availability pair if for some reason you cannot update the configuration in the device manager.

Disabling High Availability

When you disable a high-availability pair, the high-availability configuration is removed from both units.

When using the Management interface for manager access: The active unit remains up and passing traffic. The standby unit interface configuration is erased.

When using a data interface for manager access: See the following details.

- The active unit remains up and passing traffic.
- The standby unit data interfaces are shut down except for the manager access interface, which remains up using the standby IP address so it can maintain the management connection.
- If the primary unit is in the standby state:

- The IP addresses for manager access are swapped permanently in the management center configuration: the primary unit uses the standby IP address, and the secondary unit uses the active IP address.
- If the management center initiated the management connection, and you specified a hostname for the device, then you need to update the DNS server so the swapped IP addresses are associated with the correct hostnames.
- Breaking high availability causes a deployment to the standby unit. If the management connection is not yet reestablished because of the swapped IP addresses, the deployment may fail. In this case, you will need to manually trigger the deployment after the management connection is established. Be sure to complete the standby deployment before deploying changes to the active unit.

Suspending High Availability

You can suspend a unit in a high-availability pair, which is useful when:

- Both units are in an active-active situation, and fixing the communication on the failover link does not correct the problem.
- You want to troubleshoot an active or standby unit and do not want the units to fail over during that time.
- You want to prevent failover while installing a software upgrade on the standby device.

When you suspend high availability, the currently active device remains active, handling all user connections. However, failover criteria are no longer monitored, and the system will never fail over to the now pseudo-standby device.

When using the Management interface for manager access: The standby unit interface configuration is erased.

When using a data interface for manager access: The standby unit data interfaces are shut down except for the manager access interface, which remains up using the standby IP address so it can maintain the management connection.

The key difference between suspending high availability and breaking high availability is that on a suspended high-availability device, the high-availability configuration is retained. When you break high availability, the configuration is erased. Thus, you have the option to resume high availability on a suspended system, which enables the existing configuration and makes the two devices function as a failover pair again.

Note Suspending high availability is a temporary state. If you reload a unit, it resumes the high-availability configuration automatically and negotiates the active/standby state with the peer.

Examples

The following example shows how to temporarily suspend and then resume a high-availability configuration.

```
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
```

```
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
        This host: Primary - Active
                Active time: 776671 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and
'NO' if you wish to abort: Yes
Successfully suspended high-availability.
> show failover
Failover Off
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
> configure high-availability resume
Successfully resumed high-availablity.
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Unit Enrollment Hold action is active, timeout in 1792 seconds
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate Unknown
Last Failover at: 20:26:06 UTC Nov 4 2016
        This host: Primary - Active
                Active time: 778071 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
```

```
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - App Sync
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Unknown (Waiting)
                  Interface inside (0.0.0.0): Unknown (Waiting)
                  Interface diagnostic (0.0.0.0): Unknown (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
```

Related Commands

Command	Description
show failover	Shows the failover (high-availability) configuration.
show high-availability config	Shows the failover (high-availability) configuration. Provides the same output as **show failover**.

configure https-access-list

To configure the device to accept HTTPS connections from specified IP addresses, use the **configure https-access-list** command.

configure https-access-list *address_list*

Syntax Description

address_list	A comma separated list of IP addresses for hosts or networks, in IPv4 Classless Inter-Domain Routing (CIDR) notation or IPv6 prefix length notation. For example, 10.100.10.0/24 or 2001:DB8::/96. To specify all IPv4 hosts, enter 0.0.0.0/0. To specify all IPv6 hosts, specify ::/0.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

You must include all supported hosts or networks in a single command. Addresses specified in this command overwrite the current contents of the HTTPS access list.

Merely allowing HTTPS access does not permit users to log into the local manager. Access to the configuration software is controlled by username and password.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

Examples

The following example configures the device to accept HTTPS connections from any IPv4 or IPv6 address:

```
> configure https-access-list 0.0.0.0/0,::/0
The https access list was changed successfully.
> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:https
```

Related Commands

Command	Description
configure disable-https-access	Clears the HTTPS access list.
show https-access-list	Shows the HTTPS access list.

configure identity-subnet-filter

To exclude subnets from receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings from ISE, use the **configure identity-subnet-filter** command. You should typically do this for lower-memory managed devices to prevent Snort identity health monitor memory errors.

configure identity-subnet-filter { **add** | **remove** } *subnet*

Syntax Description

add	Adds the specified subnet to the list of excluded subnets.
remove	Removes the specified subnet from the list of excluded subnets.
subnet	Specifies which subnet to add or exclude.

Command History

Release	Modification
6.7	This command was introduced.

Examples

The following example configures a static IPv6 address for the management interface.

```
> configure identity-subnet-filter 192.0.2.0/24
```

Related Commands

Command	Description
show identity-subnet-filter	Shows the subnets currently being excluded from user-to-IP and SGT-to-IP mappings.

configure inspection

To enable or disable the default application protocol inspection engines, use the **configure inspection** command.

configure inspection *protocol* {**enable** | **disable**}

Syntax Description

disable	Disables the inspection engine.
enable	Enables the inspection engine.
protocol	The inspection protocol that you want to enable or disable. See the usage guidelines section for a list of options.

Command History

Release	Modification
6.2	This command was introduced.

Usage Guidelines

Disable the default inspection engines only at the direction of Cisco Technical Support, or if you are certain that the associated types of traffic do not occur on your network. For example, if you block all traffic on an inspected port, you can safely disable inspection on that port. These inspections are applied to all data interfaces.

These inspection engines are separate from Snort inspection. These engines provide the following services:

- Pinhole creation—Some application protocols open secondary TCP or UDP connections either on standard or negotiated ports. Inspection opens pinholes for these secondary ports so that you do not need to create access control rules to allow them.
- NAT rewrite— Protocols such as FTP embed IP addresses and ports for the secondary connections in packet data as part of the protocol. If there is NAT translation involved for either of the endpoints, the inspection engines rewrite the packet data to reflect the NAT translation of the embedded addresses and ports. The secondary connections would not work without NAT rewrite. For NAT limitations, see the NAT chapter in the configuration guide for the manager you are using to configure the device (management center or device manager).
- Protocol enforcement—Some inspections enforce some degree of conformance to the RFCs for the inspected protocol.

You can disable, and subsequently enable, the following inspection engines. To see what is currently enabled, use the **show running-config policy-map** command and look for the **inspect** commands. To see details of the default parameters for each inspection, use the **show running-config all policy-map** command.

- **dcerpc**—(TCP port 135.) Distributed Computing Environment/Remote Procedure Calls. The DCERPC inspection engine inspects for native TCP communication between the Endpoint Mapper (EPM) and client on well known TCP port 135. Microsoft Remote Procedure Call (MSRPC), based on DCERPC, is a protocol widely used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely. Inspection provides pinhole creation and NAT services.
- **dns**—(UDP port 53.) Domain Name System. DNS is inspected on UDP port 53. Inspection provides NAT services and protocol enforcement. You must enable this inspection engine to use the NAT rewrite option on NAT rules. NAT rewrite is frequently required when doing NAT between IPv4 and IPv6 networks (NAT64/46).

- **esmtp**—(TCP port 25.) Extended Simple Mail Transfer Protocol. ESMTP inspection detects attacks, including spam, phising, malformed message attacks, and buffer overflow/underflow attacks. It also provides support for application security and protocol conformance, which enforces the sanity of the ESMTP messages as well as block senders/receivers, and block mail relay. For details on the controls applied during inspection, use the **show running-config all policy-map** command and look for the "policy-map type inspect esmtp _default_esmtp_map" line and subsequent parameters.

  ESMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns. It provides NAT services and protocol conformance. ESMTP inspection performs three primary tasks:

  - Restricts SMTP requests to seven basic SMTP commands and eight extended commands. Supported commands are the following:

    Extended SMTP—AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML, STARTTLS, and VRFY.

    SMTP (RFC 821)—DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET.

  - Monitors the SMTP command-response sequence.
  - Generates an audit trail. Syslog audit record 108002 is generated when an invalid character embedded in the mail address is replaced. For more information, see RFC 821.

- **ftp**—(TCP port 21.) File Transfer Protocol. Inspection provides pinhole and NAT services.
- **h323_h225**—(TCP port 1720, UDP port 1718.) H.323 inspection supports RAS, H.225, and H.245, and its functionality translates all embedded IP addresses and ports. It performs state tracking and filtering. H.323 inspection provides support for H.323 compliant applications such as Cisco CallManager. H.323 is a suite of protocols defined by the International Telecommunication Union for multimedia conferences over LANs. The device supports H.323 through Version 6, including H.323 v3 feature Multiple Calls on One Call Signaling Channel.

  The two major functions of H.323 inspection are as follows:

  - NAT the necessary embedded IPv4 addresses in the H.225 and H.245 messages. Because H.323 messages are encoded in PER encoding format, the ASA uses an ASN.1 decoder to decode the H.323 messages.
  - Dynamically allocate the negotiated H.245 and RTP/RTCP connections. The H.225 connection can also be dynamically allocated when using RAS.

- **h323_ras**—(UDP ports 1718-1719.) See the description for **h323_h225**. This inspection is for RAS signaling.
- **icmp**—(ICMP traffic only.) The ICMP inspection engine allows ICMP traffic to have a "session" so it can be inspected like TCP and UDP traffic. Without the ICMP inspection engine, we recommend that you do not allow ICMP through the device (block with an access control rule). Without stateful inspection, ICMP can be used to attack your network. The ICMP inspection engine ensures that there is only one response for each request, and that the sequence number is correct. Inspection also provides NAT services.
- **icmp_error**—(ICMP traffic only.) When ICMP Error inspection is enabled, the device creates translation sessions for intermediate hops that send ICMP error messages, based on the NAT configuration. The device overwrites the packet with the translated IP addresses. This is necessary to provide meaningful information in traceroutes that go through the device.

- **ip-options**—(RSVP traffic only.) IP Options inspection controls which IP packets are allowed based on the contents of the IP Options field in the packet header. Packets with the Router Alert option are allowed. Packets with any other options are dropped.
- **netbios**—(UDP source ports 137, 138.) NetBIOS Name Server over IP. NetBIOS application inspection performs NAT for the embedded IP address in the NetBIOS name service (NBNS) packets and NetBIOS datagram services packets. It also enforces protocol conformance, checking the various count and length fields for consistency.
- **rsh**—(TCP port 514.) The RSH protocol uses a TCP connection from the RSH client to the RSH server on TCP port 514. The client and server negotiate the TCP port number where the client listens for the STDERR output stream. RSH inspection opens pinholes and supports NAT of the negotiated port number if necessary.
- **rtsp**—(TCP port 554.) Real-Time Streaming Protocol. The RTSP inspection engine lets the device pass RTSP packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime, RealPlayer, and Cisco IP/TV connections. RTSP applications use the well-known port 554 with TCP (rarely UDP) as a control channel. The device only supports TCP, in conformity with RFC 2326. This TCP control channel is used to negotiate the data channels that are used to transmit audio/video traffic, depending on the transport mode that is configured on the client. The supported RDT transports are: rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp, and x-pn-tng/udp.
- **sqlnet**—(TCP port 1521.) The inspection engine supports SQL*Net versions 1 and 2, but only the Transparent Network Substrate (TNS) format. Inspection does not support the Tabular Data Stream (TDS) format. SQL*Net messages are scanned for embedded addresses and ports, and NAT rewrite is applied when necessary.

  Disable SQL*Net inspection when SQL data transfer occurs on the same port as the SQL control TCP port 1521. The security appliance acts as a proxy when SQL*Net inspection is enabled and reduces the client window size from 65000 to about 16000 causing data transfer issues.
- **sip**—(TCP/UDP port 5060.) Session Initiation Protocol. SIP is a widely used protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. Partially because of its text-based nature and partially because of its flexibility, SIP networks are subject to a large number of security threats. SIP application inspection provides address translation in message header and body, dynamic opening of ports and basic sanity checks.
- **skinny**—(TCP port 2000.) Skinny Client Control Protocol (SCCP). SCCP (Skinny) application inspection performs translation of embedded IP address and port numbers within the packet data, and dynamic opening of pinholes. It also performs additional protocol conformance checks and basic state tracking.
- **sunrpc**—(TCP/UDP port 111.) Sun RPC is used by NFS and NIS. Sun RPC services can run on any port. When a client attempts to access a Sun RPC service on a server, it must learn the port that service is running on. It does this by querying the port mapper process, usually rpcbind, on the well-known port of 111.

  The client sends the Sun RPC program number of the service and the port mapper process responds with the port number of the service. The client sends its Sun RPC queries to the server, specifying the port identified by the port mapper process. When the server replies, the device intercepts this packet and opens both embryonic TCP and UDP connections on that port. NAT or PAT of Sun RPC payload information is not supported.
- **tftp**—(UDP port 69.) Trivial File Transfer Protocol. The inspection engine inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR), and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server.

A dynamic secondary channel and a PAT translation, if necessary, are allocated on a reception of a valid read (RRQ) or write (WRQ) request. This secondary channel is subsequently used by TFTP for file transfer or error notification. Only the TFTP server can initiate traffic over the secondary channel, and at most one incomplete secondary channel can exist between the TFTP client and server. An error notification from the server closes the secondary channel. TFTP inspection must be enabled if static PAT is used to redirect TFTP traffic.

- **xdmcp**—(UDP port 177.) X Display Manager Control Protocol. XDMCP is a protocol that uses UDP port 177 to negotiate X sessions, which use TCP when established. For successful negotiation and start of an XWindows session, the device must allow the TCP back connection from the Xhosted computer. Use access control rules to permit the back connection through the TCP ports.

  During the XWindows session, the manager talks to the display Xserver on the well-known port 6000 | n. Each display has a separate connection to the Xserver, as a result of the following terminal setting: **setenv DISPLAY Xserver:***n*, where *n* is the display number.

  When XDMCP is used, the display is negotiated using IP addresses, which the device can NAT if needed. XDCMP inspection does not support PAT.

Examples

The following example shows the current inspection configuration and disables XDMCP inspection. You can enable or disable inspection engines, but you cannot change their default behavior. For example, this output shows that DNS/TCP inspection is disabled. You cannot configure DNS inspection to apply to TCP traffic using the **configure inspection** command.

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
!
> configure inspection xdmcp disable
Building configuration...
Cryptochecksum: 46dbea1d 51c2089a fcc3e42f 3dafd2d5
12386 bytes copied in 0.160 secs
```

```
[OK]
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
  inspect ftp
!
```

Related Commands

Command	Description
show running-config policy-map	Shows the policy maps for service policies, including the inspection configuration.
show service-policy	Shows service-policy statistics, including those for inspection.

configure log-events-to-ramdisk

To enable or disable connection event logging to RAM disk to improve system performance and reduce disk wear associated with writing connection events to the Solid State Drive (SSD), use the **configure log-events-to-ramdisk** command.

configure log-events-to-ramdisk {**enable** | **disable**}

Syntax Description

enable	Enables connection event logging to RAM disk.
disable	Disables connection event logging to RAM disk. Connection events are then logged to the SSD.

Command Default

The default is enabled on the platforms that support the feature.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to toggle between using RAM disk or a physical SSD to log connection events. If enabled, connection events are logged to RAM disk. If disabled, connection events are logged to the SSD. In the event of a power loss, connection events logged to RAM disk will be lost.

This command is not available on all device types. When you run this command on an unsupported platform, the system returns the following message:

```
This command is not available on this platform.
```

Examples

The following example disables RAM disk logging.

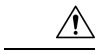
```
> configure log-events-to-ramdisk disable
```

Related Commands

Command	Description
show log-events-to-disk	Display the current logging status.
show disk-manager	Displays detailed disk usage information for each part of the system, including silos, low watermarks, and high watermarks.

configure manager add

To configure the device to accept a connection from or initiate a connection to the management center and/or CDO, use the **configure manager add** command.



Caution Adding a remote manager resets the configuration to the factory default.

configure manager add { *hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*] [*display_name*]

Syntax Description

hostname	Specifies the hostname of the management center.
IPv4_address	Specifies the IPv4 address of the management center.
IPv6_address	Specifies the IPv6 address of the management center.
display_name	Provide a display name for showing this manager with the **show managers** command. This option is useful if you are identifying CDO as the primary manager and an on-prem management center for analytics only. If you don't specify this argument, the firewall auto-generates a display name using one of the following methods: • *hostname* | *IP_address* (if you don't use the **DONTRESOLVE** keyword) • **manager-***timestamp*
DONTRESOLVE	If the management center is not directly addressable, use **DONTRESOLVE**. If you use **DONTRESOLVE**, then a *nat_id* is required. When you add this device to the management center, make sure that you specify both the device IP address and the *nat_id* ; one side of the connection needs to specify an IP address, and both sides need to specify the same, unique NAT ID.
regkey	Specifies the unique alphanumeric registration key required to register a device to the management center. Alphanumeric characters and hyphens (-) are allowed.
nat_id	Specifies an alphanumeric string used during the registration process between the management center and the device when one side does not specify an IP address. Specify the same NAT ID on the management center. If you use a data interface for management, then you must specify the NAT ID on both the threat defense and management center for registration.

Command History

Release	Modification
6.1	This command was introduced.

Release	Modification
7.2	Added support for multiple managers: a primary cloud-delivered management center (CDO) and an on-prem management center for analytics only.

Usage Guidelines

A unique alphanumeric registration key is always required to register a device to the management center.

Normally, you need both IP addresses: the management center specifies the device IP address, and the device specifies the management center IP address. However, if you only know one of the IP addresses, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. If you do not know the management center IP address, then use the **DONTRESOLVE** keyword instead of the IP address or hostname.

Note If you use a data interface for management, then you must specify the NAT ID on both the threat defense and management center for registration.

If you registered a management center and a device using IPv4 and want to convert them to IPv6, you must delete and re-register the device on the management center.

To change from management center to the local device manager, use the **configure manager delete** command, and then use the **configure manager local** command.

Note Before moving a device from one management center to another or changing to the local manager, delete it from the current management center.

Examples

```
> configure manager add DONTRESOLVE abc123 efg456
```

Related Commands

Command	Description
configure manager delete	Removes the managing management center.
configure manager edit	Edits the managing management center.
configure manager local	Configures the local manager.
show managers	Shows the current manager.

configure manager delete

To disable the current manager and enter No Manager Mode, use the **configure manager delete** command.

Caution Deleting the manager resets the threat defense configuration to the factory default. However, the management bootstrap configuration is maintained.

configure manager delete *identifier*

Syntax Description

identifier	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.

Command History

Release	Modification
6.1	This command was introduced.
6.3	The check for high availability mode was added.
7.2	The *identifier* variable was added for when you have multiple managers configured.

Usage Guidelines

Use this command to remove the current device manager(s). The device is placed in No Manager Mode, where you can then either add a remote manager (management center) or use the local manager (device manager). You would use this command when switching between local and remote management, or when a remote manager is no longer active.

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

The command behavior differs based on the current manager.

- Remote—The management center cannot be reachable. If the management center is still communicating with the threat defense, first remove the device from the management center's inventory. Then you can use this command.
- Local—No restrictions. You are immediately moved to No Manager Mode.

Examples

The following example removes the current manager and enters No Manager Mode.

```
> configure manager delete

If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
```

```
Cisco Smart Software Manager.
Do you want to continue[yes/no]:yes

DHCP Server Disabled
>
```

Related Commands

Command	Description
configure manager add	Configures a managing management center for the device.
configure manager local	Configures a local manager.
show managers	Shows the current manager.

configure manager edit

To edit the management center IP address in the threat defense configuration, use the **configure manager edit** command.

configure manager edit *identifier* { **hostname** { *ip_address* | *hostname* } | **displayname** *display_name* }

Syntax Description

identifier	Specifies the identifier (UUID) of the management center. Use the **show managers** command to view the identifier (7.2 or later) or obtain the UUID from the management center CLI **show version** command.
hostname {*ip_address* | *hostname*}	Changes the hostname/IP address.
displayname *display_name*	Changes the display name.

Command History

Release	Modification
6.7	This command was introduced.
7.2	Added the **hostname** and **displayname** keywords.

Usage Guidelines

If you change the management center IP address or hostname, you should also change the value at the device CLI so the configurations match. Although in most cases, the management connection will be reestablished without changing the management center IP address or hostname on the device, in at least one case, you must perform this task for the connection to be reestablished: when you added the device to the management center and you specified the NAT ID only. Even in other cases, we recommend keeping the management center IP address or hostname up to date for extra network resiliency.

If the management center was originally identified by **DONTRESOLVE** and a NAT ID, you can change the value to a hostname or IP address using this command. You cannot change an IP address or hostname to **DONTRESOLVE**.

The management connection will go down, and then reestablish. You can monitor the state of the connection using the **sftunnel-status** command.

Examples

The management center UUID definitively identifies the management center; for example, in the case of management center High Availability, you need to specify the active management center on the threat defense device.

Enter the **show managers** command to view the identifier:

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
```

```
Management type           : Configuration
```

Once you obtain the UUID, you can edit the IP address on the threat defense device. For example:

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

Related Commands

Command	Description
configure manager delete	Removes the managing management center.
configure manager add	Configures the management center.
show managers	Shows the current manager.

configure manager local

To configure the device to use the local manager, device manager, use the **configure manager local** command.

configure manager local

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to enable the local manager, device manager. Use the local manager when you do not want to use a separate management center. By enabling the local manager, you can open the device manager using a browser at **http://***management_ip_address*.

Note It can take up to 4-6 minutes for the command to complete, because the system must reinitialize its database. Please be patient.

The local manager is available for most platforms starting with 6.5. If it is not available for your platform, configure a remote manager using the **configure manager add** command.

Additional Restrictions

- The device must be in No Manager Mode before you can switch to the local manager. Use the **configure manager delete** command to enter No Manager Mode. Use the **show managers** command to determine your current manager.
- The device cannot be operating in transparent firewall mode (see the **configure firewall** command). The local manager supports routed mode only.

Examples

The following example shows how to configure the local manager.

```
> configure manager local
```

Related Commands

Command	Description
configure manager add	Configures a managing management center for the device.
configure manager delete	Removes the managing management center.
show managers	Shows the current manager.

configure mini-coredump

To enable or disable mini-coredump generation, use the **configure mini-coredump** command.

configure mini-coredump { **enable** | **disable** }

Syntax Description

enable	Enables the mini-coredump generation.
disable	Disables the mini-coredump generation.

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Mini-coredump generation is enabled by default.

Snort 3 process dumps huge core files because of its multi-threaded nature. These dumps take a while to be written onto the hard disk. Until the core is written and a new process is started, Snort's traffic inspection is interrupted. Creating mini-coredumps avoid time delays. Mini-coredumps have essential details of the stack and memory values which aid in debugging.

Example

The following example disables mini-coredump generation.

```
> configure mini-coredump disable
```

Related Commands

Command	Description
show mini-coredump status	Displays the mini-coredump generation settings.

configure network dns searchdomains

To configure the list of DNS search domains, use the **configure network dns searchdomains** command.

configure network dns searchdomains [*dnslist*]

Syntax Description

dnslist	Specifies a comma-separated list of DNS search domains.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to replace the current list of DNS search domains with a new list. These domains are add to hostnames when you do not specify a fully-qualified domain name in a command, for example, **ping system**. The domains are use on the management interface, or for commands that go through the management interface, only.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

Examples

The following example configures a new search domains list and then ping's a hostname that is not fully-qualified.

```
> configure network dns searchdomains example.com
> show dns system
search example.com
nameserver 10.163.47.11
> ping system www
PING www.example.com (10.163.4.161) 56(84) bytes of data.
64 bytes from www.example.com (10.163.4.161): icmp_seq=1 ttl=242 time=8.01 ms
64 bytes from www.example.com (10.163.4.161): icmp_seq=2 ttl=242 time=16.7 ms
^C
--- origin-www.cisco.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 7.961/10.216/16.718/3.755 ms
```

Related Commands

Command	Description
configure network dns servers	Configures DNS servers.
show dns system	Shows the current DNS configuration for the management interface.

configure network dns servers

To configure the DNS servers for the management interface, use the **configure network dns servers** command.

configure nework dns servers [*dnslist*]

Syntax Description

dnslist	Specifies a comma-separated list of DNS servers.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to replace the current list of DNS servers with a new list. The servers are used on the management interface only. They cannot resolve fully-qualified domain names for commands that go through the data interfaces.

Starting with version 6.3, for locally-managed devices only, if the data and management interfaces are using the same DNS group, the group is updated on your next deployment from the manager, which means that the changes are also applied to the DNS group used on the data interfaces. The changes for the management interface are immediate. We recommend that you make all DNS changes from the local manager rather than use this command.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

Examples

The following example configures the DNS servers for the management interface.

```
> configure network dns servers 10.163.47.11,10.124.1.10
> show dns system
search example.com
nameserver 10.163.47.11
nameserver 10.124.1.10
```

Related Commands

Command	Description
configure network dns searchdomains	Configures DNS search domains.
show dns system	Shows the current DNS configuration for the management interface.

configure network hostname

To configure the hostname for the device's management interface, use the **configure network hostname** command.

configure network hostname *name*

Syntax Description

name	Specifies the new hostname.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The system hostname is defined in more than one place. If you update the hostname from the manager, the system synchronizes the hostname across all processes. If you use this command when using device manager (the local manager), you need to deploy changes from device manager to complete the update so that the same name is used by all system processes.

If the unit is part of a high-availability group, the name applies to the current device only for all processes except Lina. For the Lina process, the name is synchronized on both units, so you should see the same hostname in the prompt when access the diagnostic CLI (using **system support diagnostic-cli**).

Examples

The following example sets the hostname to sfrocks.

```
> configure network hostname sfrocks
```

Related Commands

Command	Description
show network	Shows the management interface configuration.

configure network http-proxy

To configure an HTTP proxy for the management interface, use the **configure network http-proxy** command.

configure network http-proxy

Command History

Release	Modification
6.1	This command was introduced.
6.6	This command now works for a locally-managed system.

Usage Guidelines

Use this command to set up an HTTP Proxy address for the device. After issuing the command, you are prompted for the HTTP proxy address and port, whether proxy authentication is required, and if it is required, the proxy username, proxy password, and confirmation of the proxy password.

Examples

The following example configures an HTTP proxy for the management interface. In this example, authentication is configured. The CLI does not display the password that you type.

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

Related Commands

Command	Description
configure network http-proxy-disable	Disables HTTP Proxy settings.
show network	Shows the management interface configuration.

configure network http-proxy-disable

To remove the HTTP proxy for the management interface, use the **configure network http-proxy-disable** command.

configure network http-proxy-disable

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example removes the HTTP proxy for the management interface.

```
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                       : Enabled
HTTP Proxy                  : 10.100.10.10
Port                        : 80
Authentication              : Enabled
Username                    : proxyuser
> configure network http-proxy-disable
Are you sure that you wish to delete the current http-proxy configuration? (y/n): y
Configuration successfully deleted.
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                       : Disabled
Authentication              : Disabled
```

Related Commands

Command	Description
configure network http-proxy	Configures HTTP Proxy settings.
show network	Shows the management interface configuration.

configure network ipv4 delete

To disable the IPv4 configuration of the device's management interface, use the **configure network ipv4 delete** command.

configure network ipv4 delete [*management_interface*]

Syntax Description

management_ interface	Specifies the management interface. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the **configure management-interface** commands to enable more than one management interface. Multiple management interfaces are supported on Firepower 4100 and 9300 series devices only. Do not specify this parameter for other platforms. The management interface IDs on the Firepower 4100 and 9300 are **management0** for the default management interface and **management1** for the optional event interface.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to disable the IPv4 configuration of the device's management interface. If you are connected to the IP address you delete, you will lose your connection to the device. Ensure that you have an IPv6 address configured before removing the IPv4 address.

You do not need to delete the configuration to change the IPv4 address. Use the **configure network ipv4 manual** or **configure network ipv4 dhcp** commands if you want to keep IPv4 addressing but you simply want to change the address.

Examples

The following example deletes the IPv4 address configuration.

```
> configure network ipv4 delete
```

Related Commands

Command	Description
configure network ipv4 dhcp	Configures IPv4 to obtain an address from a DHCP server.
configure network ipv4 manual	Configures IPv4 manually with a static IP address.
show network	Shows the management interface configuration.

configure network ipv4 dhcp

To configure the management interface to obtain an IPv4 address from a DHCP server, use the **configure network ipv4 dhcp** command.

configure network ipv4 dhcp [*management_interface*]

Syntax Description

management_ interface	Specifies the management interface. DHCP is supported only on the default management interface, so you do not need to use this argument.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to specify that the device's management interface receives its IPv4 configuration from a DHCP server. The management interface communicates with the DHCP server to obtain its configuration information.

Note If you configure a data interface for management center access using the **configure network management-data-interface** command, you cannot use DHCP for the Management interface; you must set a manual IP address because the default route, which must be **data-interfaces**, might be overwritten with one received from the DHCP server. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address. This IP address is NATted when the traffic is forwarded to the data interface.

Examples

The following example configures the management interface to obtain its IPv4 address using DHCP.

```
> configure network ipv4 dhcp
```

Related Commands

Command	Description
configure network ipv4 delete	Disables IPv4 networking.
configure network ipv4 manual	Configures IPv4 manually.
show network	Shows the management interface configuration.

configure network ipv4 dhcp-dp-route

To restore the management interface default IP address, network mask, and gateway, use the **configure network ipv4 dhcp-dp-route** command. This command does not change other network settings, such as DNS servers.

Note This command is not supported on the Secure Firewall Threat Defense Virtual (threat defense virtual), Firepower 4100/9300, or ISA 3000.

configure network ipv4 dhcp-dp-route

Command History

Release	Modification
6.6	This command was introduced.

Usage Guidelines

You must enter both the IPv4 and IPv6 versions of this command to restore the configuration to the factory default, even if you did not identify an IP address for one of the versions.

Examples

The following example restores the default configuration for the management interface.

```
> configure network ipv4 dhcp-dp-route
Creating /etc/sf/sftunnel.conf with header line
Set up management0 as DHCP ipv4 client with the default route through data interfaces.
>
```

Related Commands

Command	Description
configure network ipv4 delete	Disables IPv4 networking.
configure network ipv4 dhcp	Configures IPv4 via DHCP.
configure network ipv4 manual	Configures IPv4 manually.
show network	Shows the management interface configuration.

configure network ipv4 dhcp-server-disable

To disable the DHCP server on the management interface, use the **configure network ipv4 dhcp-server-disable** command.

configure network ipv4 dhcp-server-disable

Command History

Release	Modification
6.2	This command was introduced.

Usage Guidelines

If there is an active DHCP server on the management interface, you can disable it. When disabled, clients on the management network will either have to configure static addresses, or you will need to configure a different device on the network to provide DHCP server services.

If you change the management IP address to use DHCP to obtain an address, the DHCP server (if enabled) is automatically disabled.

Examples

The following example shows how to check whether DHCP server is enabled, and then how to disable it.

```
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
> configure network ipv4 dhcp-server-disable
DCHP Server Disabled
> show network-dhcp-server
DHCP Server Disabled
```

Related Commands

Command	Description
configure network ipv4 dhcp-server-enable	Enables the DHCP server on the management interface.
show dhcp-server	Shows the status of the DHCP server on the management interface.

configure network ipv4 dhcp-server-enable

To enable the optional DHCP server on the management interface, use the **configure network ipv4 dhcp-server-enable** command.

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

Syntax Description

start_ip_address *end_ip_address*	Specifies the starting and ending IPv4 addresses for the DHCP address pool. When the management interface receives a DHCP client request, it provides an address from this pool. The pool must be on the same subnet as the management IPv4 address. Do not include the network address, management address, or broadcast address in the DHCP address pool.

Command History

Release	Modification
6.2	This command was introduced.

Usage Guidelines

If you configure a manual (static) IPv4 address for the management interface, you can configure a DHCP server to supply addresses to endpoints on the management network.

Before enabling the server, ensure that there is no other DHCP server on the management network. You can have at most one DHCP server per network, or results can be unpredictable.

Note This command is not supported on threat defense virtual devices.

Examples

The following example shows how to configure the DHCP server and show its status.

```
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
```

Related Commands

Command	Description
configure network ipv4 dhcp-server-disable	Disables the DHCP server on the management interface.
show dhcp-server	Shows the status of the DHCP server on the management interface.

configure network ipv4 manual

To configure a static IPv4 address on the management interface, use the **configure network ipv4 manual** command.

configure network ipv4 manual *ipaddr netmask gw* [*management_interface*]

Syntax Description

ipaddr	Specifies the IP address.
netmask	Specifies the subnet mask.
gw	Specifies the IPv4 address of the default gateway. You have the option of specifying **data-interfaces**, which uses the data interfaces on the device as a gateway instead of an explicit gateway on the management network. Use the data interfaces if you do not want to wire the management physical interface to a separate management network. For management center data interface management, see the **configure network management-data-interface** command. Note that the *gw* in this command is used to create the default route for the device. If you configure an event-only interface, then you must enter the *gw* as part of the command; however, this entry just configures the default route to the value you specify and does not create a separate static route for the eventing interface. If you are using an event-only interface on a different network from the management interface, we recommend that you set the *gw* for use with the management interface, and then create a static route separately for the event-only interface using the **configure network static-routes** command.
management_ interface	Specifies the management interface. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the **configure management-interface** commands to enable more than one management interface. Multiple management interfaces are supported on Firepower 4100 and 9300 series devices only. Do not specify this parameter for other platforms. The management interface IDs on the Firepower 4100 and 9300 are **management0** for the default management interface and **management1** for the optional event interface.

Command History

Release	Modification
6.1	This command was introduced.
6.2	The **data-interfaces** keyword was added for gateway.
6.7	The **data-interfaces** keyword is now available for the management center management on a data interface.

Usage Guidelines

If you configure a data interface for the management center access using the **configure network management-data-interface** command, you must set a manual IP address (either IPv4 or IPv6). Although you do not plan to use the Management interface, you must set an IP address, for example, a private address.

This IP address is NATted when the traffic is forwarded to the data interface. You cannot use DHCP (the default) because the default route, which must be **data-interfaces**, might be overwritten with one received from the DHCP server.

Examples

The following example configures a static IPv4 address on the management interface.

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

Related Commands

Command	Description
configure network ipv4 delete	Disables IPv4 networking.
configure network ipv4 dhcp	Configures IPv4 via DHCP.
show network	Shows the management interface configuration.

configure network ipv6 delete

To disable the IPv6 configuration of the device's management interface, use the **configure network ipv4 delete** command.

configure network ipv6 delete [*management_interface*]

Syntax Description

management_ interface	Specifies the management interface. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the **configure management-interface** commands to enable more than one management interface. Multiple management interfaces are supported on Firepower 4100 and 9300 series devices only. Do not specify this parameter for other platforms. The management interface IDs on the Firepower 4100 and 9300 are **management0** for the default management interface and **management1** for the optional event interface.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to disable the IPv6 configuration of the device's management interface. If you are connected to the IP address you delete, you will lose your connection to the device. Ensure that you have an IPv4 address configured before removing the IPv6 address.

You do not need to delete the configuration to change the IPv6 address. Use the **configure network ipv6** {**manual** | **dhcp** | **router**} commands if you want to keep IPv6 addressing but you simply want to change the address.

Examples

The following example deletes the IPv6 address configuration.

```
> configure network ipv6 delete
```

Related Commands

Command	Description
configure network ipv6 dhcp	Configures IPv6 via DHCP.
configure network ipv6 manual	Configure IPv6 manually.
configure network ipv6 router	Configure IPv6 via router.
show network	Shows the management interface configuration.

configure network ipv6 destination-unreachable

To enable or disable ICMPv6 Destination Unreachable packets when using IPv6 on the management interface, use the **configure network ipv6 destination-unreachable** command.

configure network ipv6 destination-unreachable {**enable** | **disable**}

Syntax Description

enable	Enables Destination Unreachable packets. This setting is the default.
disable	Disables Destination Unreachable packets.

Command Default

Enabled by default.

Command History

Release	Modification
6.4.0	Command added.

Usage Guidelines

You might want to disable these packets to guard against potential denial of service attacks.

Examples

The following example disables the Destination Unreachable message.

```
> configure network ipv6 destination-unreachable disable
```

Related Commands

Command	Description
configure network ipv6 delete	Disables IPv6 networking.
configure network ipv6 echo-reply	Enables or disables Echo Reply packets.
configure network ipv6 manual	Configures IPv6 manually.
configure network ipv6 router	Configures IPv6 via router.
show network	Shows the management interface configuration.

configure network ipv6 dhcp

To configure the management interface to obtain an IPv6 address from a DHCP server, use the **configure network ipv6 dhcp** command.

configure network ipv6 dhcp [*management_interface*]

Syntax Description

management_ interface	Specifies the management interface. DHCP is supported only on the default management interface, so you do not need to use this argument.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to specify that the device's management interface receives its IPv6 configuration from a DHCP server. The management interface communicates with the DHCP server to obtain its configuration information.

Note If you configure a data interface for management center access using the **configure network management-data-interface** command, you cannot use DHCP for the Management interface; you must set a manual IP address because the default route, which must be **data-interfaces**, might be overwritten with one received from the DHCP server. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address. This IP address is NATted when the traffic is forwarded to the data interface.

Examples

The following example configures the management interface to obtain its IPv6 address using DHCP.

```
> configure network ipv6 dhcp
```

Related Commands

Command	Description
configure network ipv6 delete	Disables IPv6 networking.
configure network ipv6 manual	Configure IPv6 manually.
configure network ipv6 router	Configure IPv6 via router.
show network	Shows the management interface configuration.

configure network ipv6 dhcp-dp-route

To restore the management interface default IP address, network mask, and gateway, use the **configure network ipv6 dhcp-dp-route** command. This command does not change other network settings, such as DNS servers.

Note This command is not supported on the threat defense virtual, Firepower 4100/9300, or ISA 3000.

configure network ipv6 dhcp-dp-route

Command History

Release	Modification
6.6	This command was introduced.

Usage Guidelines

You must enter both the IPv4 and IPv6 versions of this command to restore the configuration to the factory default, even if you did not identify an IP address for one of the versions.

Examples

The following example restores the default configuration for the management interface.

```
> configure network ipv6 dhcp-dp-route
Set up management0 as DHCP ipv6 client with the default route through data interfaces.
>
```

Related Commands

Command	Description
configure network ipv6 delete	Disables IPv6 networking.
configure network ipv6 dhcp	Configures IPv6 via DHCP.
configure network ipv6 manual	Configures IPv6 manually.
show network	Shows the management interface configuration.

configure network ipv6 echo-reply

To enable or disable ICMPv6 Echo Reply packets when using IPv6 on the management interface, use the **configure network ipv6 echo-reply** command.

configure network ipv6 echo-reply {**enable** | **disable**}

Syntax Description

enable	Enables Echo Reply packets. This setting is the default.
disable	Disables Echo Reply packets.

Command Default

Enabled by default.

Command History

Release	Modification
6.4.0	Command added.

Usage Guidelines

You might want to disable these packets to guard against potential denial of service attacks. Disabling Echo Reply packets means you cannot use IPv6 ping to the device management interfaces for testing purposes.

Examples

The following example disables the Echo Reply message.

```
> configure network ipv6 echo-reply disable
```

Related Commands

Command	Description
configure network ipv6 delete	Disables IPv6 networking.
configure network ipv6 destination-unreachable	Enables or disables Destination Unreachable packets.
configure network ipv6 manual	Configures IPv6 manually.
configure network ipv6 router	Configures IPv6 via router.
show network	Shows the management interface configuration.

configure network ipv6 manual

To configure a static IPv6 address on the management interface, use the **configure network ipv6 manual** command.

configure network ipv6 manual *ip6addr ip6prefix* [*ip6gw*] [*management_interface*]

Syntax Description

ip6addr	Specifies the IP address.
ip6prefix	Specifies the prefix length.
ip6gw	Specifies the IPv6 address of the default gateway. You have the option of specifying **data-interfaces**, which uses the data interfaces on the device as a gateway instead of an explicit gateway on the management network. Use the data interfaces if you do not want to wire the management physical interface to a separate management network. For management center data interface management, see the **configure network management-data-interface** command. Note that the *ip6gw* in this command is used to create the default route for the device. If you configure an event-only interface, then you must enter the *ip6gw* as part of the command; however, this entry just configures the default route to the value you specify and does not create a separate static route for the eventing interface. If you are using an event-only interface on a different network from the management interface, we recommend that you set the *ip6gw* for use with the management interface, and then create a static route separately for the event-only interface using the **configure network static-routes** command.
management_ interface	Specifies the management interface. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the **configure management-interface** commands to enable more than one management interface. Multiple management interfaces are supported on Firepower 4100 and 9300 series devices only. Do not specify this parameter for other platforms. The management interface IDs on the Firepower 4100 and 9300 are **management0** for the default management interface and **management1** for the optional event interface.

Command History

Release	Modification
6.1	This command was introduced.
6.2	The **data-interfaces** keyword was added for gateway.
6.7	The **data-interfaces** keyword is now available for management center management on a data interface.

Usage Guidelines

If you configure a data interface for management center access using the **configure network management-data-interface** command, you must set a manual IP address (either IPv4 or IPv6). Although you do not plan to use the Management interface, you must set an IP address, for example, a private address.

This IP address is NATted when the traffic is forwarded to the data interface. You cannot use DHCP (the default) because the default route, which must be **data-interfaces**, might be overwritten with one received from the DHCP server.

Examples

The following example configures a static IPv6 address for the management interface.

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff 64
```

Related Commands

Command	Description
configure network ipv6 delete	Disables IPv6 networking.
configure network ipv6 dhcp	Configures IPv6 via DHCP.
configure network ipv6 router	Configure IPv6 via router.
show network	Shows the management interface configuration.

configure network ipv6 router

To configure the management interface to obtain an IPv6 address from a router using stateless autoconfiguration, use the **configure network ipv6 router** command.

configure network ipv6 router [*management_interface*]

Syntax Description

management_ interface	Specifies the management interface. If you do not specify an interface, this command configures the default management interface. This parameter is needed only if you use the **configure management-interface** commands to enable more than one management interface. Multiple management interfaces are supported on Firepower 4100 and 9300 series devices only. Do not specify this parameter for other platforms. The management interface IDs on the Firepower 4100 and 9300 are **management0** for the default management interface and **management1** for the optional event interface.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to specify that the device's management interface receives its IPv6 configuration from a router. The management interface communicates with the IPv6 router to obtain its configuration information.

Examples

The following example configures the management interface to receive its IPv6 address from a router using stateless autoconfiguration.

```
> configure network ipv6 router
```

Related Commands

Command	Description
configure network ipv6 delete	Disables IPv6 networking.
configure network ipv6 dhcp	Configures IPv6 via DHCP.
configure network ipv6 manual	Configure IPv6 manually.
show network	Shows the management interface configuration.

configure network management-data-interface

To configure a data interface for management center management instead of the Management interface, use the **configure network management-data-interface** command.

configure network managament-data-interface [{ **ipv4** { **dhcp** | [**manual** *ip_address netmask*] [**default-gw** *gateway_ip*] } | **ipv6** [**manual** *ip_address prefix*] [**default-gw** *gateway_ip*] } | **ddns update-url** **https://** *username* **:** *password* **@** *provider-domain* **/** *path* **?hostname=<h>&myip=<a>** | **nameif** *name* | **client** *ip_address mask-or-prefix* | } **interface** *id* | **disable**]

Syntax Description

ipv4	Specifies IPv4 for the IP address.
ipv6	Specifies IPv6 for the IP address.
dhcp	Specifies DHCP for the IPv4 address.
manual *ip_address netmask-or-prefix*	Specifies a manual IP address and netmask or prefix.
default-gw *gateway_ip*	Specifies the address of the default gateway. If you edit the secondary interface at the CLI, you cannot configure the gateway or otherwise alter the default route, because the static route for this interface can only be edited in the management center.
ddns update-url **https://** *username* **:** *password* **@** *provider-domain* **/** *path* **?hostname=<h>&myip=<a>**	Specifies the DDNS Web type update URL. Specify the username and password at the DDNS provider. Check with your DDNS provider for the correct path. Before entering the question mark (?) character, press the control (Ctrl) key and the v key together on your keyboard. This will allow you to enter the ? without the software interpreting the ? as a help query. Although these keywords look like arguments, you need to enter this text verbatim at the end of the URL. The threat defense will automatically replace the <h> and <a> fields with the hostname and IP address when it sends the DDNS update.
nameif *name*	Sets the name of the interface.
client *ip_address*	Limits data interface access to an management center on a specific network. Note that this keyword is not part of the wizard when you enter the **configure network managament-data-interface** command without arguments.
interface *id*	Specifies the data interface ID that you want to use for management center management access. You can only specify one data interface for management center access.
disable	Disables management center management access on a data interface.

Command History

Release	Modification
6.7	This command was introduced.

Release	Modification
7.3	After you add a secondary management interface in the management center, you can edit some of its settings at the CLI using this command.
7.4	High Availability support was added.

Usage Guidelines

If you do not specify any arguments when you first configure this command, you are prompted with a wizard to configure basic network settings for the data interface.

Note You should use the console port when using this command. If you use SSH to the Management interface, you might get disconnected and have to reconnect to the console port. See below for more information about SSH usage.

If you configure a secondary management interface in the management center, you can edit it using this command. You cannot manually add the secondary interface at the CLI; you must use the management center.

See the following details for using this command:

- The original Management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network** {**ipv4** | **ipv6**} **manual** command. If you did not already set the Management interface gateway to **data-interfaces**, this command will set it now.
- management center access from a data interface has the following limitations:
  - You can only enable manager access on a physical, data interface. You cannot use a subinterface or EtherChannel. You can also use the management center to enable manager access on a single secondary interface for redundancy.
  - This interface cannot be management-only.
  - Routed firewall mode only, using a routed interface.
  - PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the threat defense and the WAN modem.
  - The interface must be in the global VRF only.
  - SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the management center. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command. For threat defense virtual on Amazon Web Services, a console port is not available, so you should maintain your SSH access to the Management interface: add a static route for Management before you continue with your configuration. Alternatively, be sure to finish all CLI configuration (including the **configure manager add** command) before you configure the data interface for manager access and you are disconnected.
  - You cannot use separate management and event-only interfaces.
  - Clustering is not supported. You must use the Management interface in this case.

- When you add the threat defense to the management center, the management center discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. In management center, you can later make changes to the management center access interface configuration, but make sure you don't make changes that can prevent the threat defense or management center from re-establishing the management connection. If the management connection is disrupted, the threat defense includes the **configure policy rollback** command to restore the previous deployment.
- If you configure a DDNS server update URL, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).
- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

  On the management center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to the management center, 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 threat defense 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 management center and the threat defense into sync.

  Also, local DNS servers are only retained by management center if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in management center, including the DNS servers, to match the threat defense configuration.
- You can change the management interface after you register the threat defense to the management center, to either the Management interface or another data interface.
- The FQDN that you set in the setup wizard will be used for this interface.
- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
- To disable data managemement, enter the **configure network management-data-interface disable** command.

Examples

The following example sets Ethernet1/1 as the management center management interface using DHCP.

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
```

```
Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

The following example sets Ethernet1/1 as the management center management interface using a manual IP address.

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Related Commands

Command	Description
configure network ipv4 manual	Configures the Management interface with a manual IPv4 IP address.
configure network ipv6 manual	Configures the Management interface with a manual IPv6 IP address.
configure policy rollback	Restores the previous deployment if the management connection is disrupted.
show network	Shows the management interface configuration.

configure network management-interface

To configure management interface settings, such as enabling or disabling management and event channels, MTU, or TCP port for management center communication, use the **configure network management-interface** command.

configure network management-interface { [**disable** | **disable-event-channel** | **disable-management-channel** | **enable** | **enable-event-channel** | **enable-management-channel** | **fec**] *interface_id* [*fec_mode*]] | **tcpport** *number* | **mtu-event-channel** [*bytes*] | **mtu-management-channel** [*bytes*] }

Syntax Description

disable	Disables the specified management interface.
disable-event-channel	Disables the event channel on the specified interface.
disable-management-channel	Disables the management channel on the specified interface.
enable	Enables the specified management interface.
enable-event-channel	Enables the event channel on the specified interface.
enable-management-channel	Enables the management channel on the specified interface.
fec	Sets the Forward Error Correction (FEC) method for 25 Gbps interfaces.

fec_mode	Sets the FEC mode:
	• **auto** (the default)—Sets the mode depending on the transceiver type:
	  • 25G-SR—Clause 108 RS-FEC
	  • 25G-LR—Clause 108 RS-FEC
	  • 10/25G-CSR—Clause 74 FC-FEC
	  • 25G-AOC*x*M—Clause 74 FC-FEC
	  • 25G-CU2.5/3M—Auto-Negotiate
	  • 25G-CU4/5M—Auto-Negotiate
	  • 25/50/100G—Clause 91 RS-FEC
	• **cl108-rs**—Clause 108 RS-FEC
	• **cl74-fc**—Clause 74 FC-FEC
	• **cl91-rs**—Clause 91 RS-FEC
	• **disable**—Disables FEC

interface_id	Specifies the management interface that you want to enable or disable, **management0** or **management1**. management0 and management1 are the internal names of these interfaces, regardless of the physical interface ID.

tcpport *number*	Configures the TCP port used for communications with the management center. The default is 8305. Do not specify the SSH (22) or HTTPS (443) ports if you change the default. Keep the number in the high range above 1024, up to 65535. This command is equivalent to the **configure network management-port** command.
mtu-event-channel [*bytes*]	Sets the MTU of the eventing interface in bytes, between 64 and 9000 if you enable IPv4, and 1280 to 9000 if you enable IPv6. If you enable both IPv4 and IPv6, then the minimum is 1280. If you do not enter the *bytes*, you are prompted for a value. This command is equivalent to the **configure network mtu** command.
mtu-management-channel [*bytes*]	Sets the MTU of the management interface in bytes, between 64 and 1500 if you enable IPv4, and 1280 to 1500 if you enable IPv6. If you enable both IPv4 and IPv6, then the minimum is 1280. If you do not enter the *bytes*, you are prompted for a value. This command is equivalent to the **configure network mtu** command. **Note** If you set a *very* low MTU, device manager performance can be affected.

Command Default

The management0 interface is enabled, and used for both event and management traffic. management1 is disabled.

The default TCP port is 8305.

The default MTU is 1500 for both management and eventing.

The default FEC for 25Gbps is auto.

Command History

Release	Modification
6.1	This command was introduced.
6.6	We added the **mtu-event-channel** and **mtu-management-channel** keywords.
7.4	We added the **fec** keyword for the Secure Firewall 4200 management interfaces when running at 25Gbps.

Usage Guidelines

For device management, the management center management interface carries two separate traffic channels: the management traffic channel carries all internal traffic (such as inter-device traffic specific to the management of the device), and the event traffic channel carries all event traffic (such as web events).

You can optionally configure a separate event-only interface on the management center to handle event traffic from separate event interfaces on devices, if available (see the management center web interface do perform this configuration). You can only configure one event-only interface. Event traffic can use a large amount of bandwidth, so separating event traffic from management traffic can improve the performance of the management center.

Event traffic is sent between the device event interface and the management center event interface if possible. If the event network goes down, then event traffic reverts to the default management interface. Separate event interfaces are used when possible, but the management interface is always the backup.

On the Firepower 4100/9300, the mgmt-type interface that you assign to the logical device is designated as the default management0 interface in the threat defense application. You can also configure a separate eventing-type interface, management1. After you assign the event interface to the logical device, this interface is not enabled or configured with network settings. You must access the threat defense CLI and use the **configure network management-interface** command to enable it. Then use the **configure network** {**ipv4** | **ipv6**} **manual** commands to configure the address(es) for this interface.

The Secure Firewall 4200 includes two management interfaces, one of which can be used for management, and the other for events.

To configure a management1 event interface, enable the interface and then disable management events on the interface. You can optionally disable events for the management0 interface. In either case, the device will try to send events on the event-only interface, and if that interface is down, it will send events on the management0 interface even if you disable the event channel.

Examples

The following example enables management1, and disables the management channel. By default, both channels are enabled.

```
> configure network management-interface enable management1
> configure network management-interface disable-management-channel management1
>
```

The following example changes the port used for communications with the management center.

```
> configure network management-interface tcpport 8306
Management port changed to 8306.
```

The following example sets the MTU on the eventing interface to 9000.

```
> configure network management-interface mtu-event-channel 9000
MTU set successfully to 9000 from 1500 for management1
Refreshing Network Config...
Interface management1 speed is set to '10000baseT/Full'
>
```

The following example sets the MTU on the management interface to 1400 using the CLI prompts.

```
> configure network management-interface mtu-management-channel
Do you want to change the MTU [1500] for management0 interface?(Yes/No): Yes
Enter the new value for MTU [1500]> 1400
MTU set successfully to 1400 from 1500 for management0
Refreshing Network Config...
Interface management0 speed is set to '10000baseT/Full'
>
```

Related Commands

Command	Description
configure network mtu	Sets the management or eventing interface MTU.

Command	Description
configure network static-routes ipv4/ipv6	Configures static routes for the management interface.
show network	Shows the management interface configuration.

configure network management-port

To configure the TCP port used for communicating with management center, use the **configure network management-port** command.

configure network management-port *number*

Syntax Description

number	Configures the TCP port used for communications with the management center. The default is 8305. Do not specify the SSH (22) or HTTPS (443) ports if you change the default. Keep the number in the high range above 1024, up to 65535.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to change the port used for management connections to the management center. This command does not change the port used for the local manager, device manager. This command is equivalent to the **configure network management-interface tcpport** command; you do not need to use both commands.

Examples

The following example changes the port used for communications with the management center.

```
> configure network management-port 8306
Management port changed to 8306.
```

Related Commands

Command	Description
configure network ipv4	Configures IPv4 addressing for the management interface.
configure network ipv6	Configures IPv6 addressing for the management interface.
show network	Shows the management interface configuration.

configure network mtu

To configure the MTU for the management or eventing interface, use the **configure network mtu** command.

configure network mtu [*interface_id*] [*bytes*]

Syntax Description

bytes	(Optional) Sets the MTU in bytes. For the management interface, the value can be between 64 and 1500 if you enable IPv4, and 1280 to 1500 if you enable IPv6. For the eventing interface, the value can be between 64 and 9000 if you enable IPv4, and 1280 to 9000 if you enable IPv6. If you enable both IPv4 and IPv6, then the minimum is 1280. If you do not enter the *bytes*, you are prompted for a value. **Note** If you set a *very* low MTU, device manager performance can be affected.
interface_id	(Optional) Specifies the interface ID on which to set the MTU. Use the **show network** command to see available interface IDs, for example management0, management1, br1, and eth0, depending on the platform. If you do not specify an interface, then the management interface is used.

Command Default

The default MTU is 1500 for both management and eventing.

Command History

Release	Modification
6.6	This command was introduced.

Usage Guidelines

This command is equivalent to the **configure network management-interface mtu-event-channel** and **configure network management-interface mtu-management-channel** commands; you do not need to use both commands.

Examples

The following example sets the MTU on the eventing interface, management1, to 8192.

```
> configure network mtu 8192 management1
MTU set successfully to 8192 from 1500 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

The following example sets the MTU on the management interface to 1400 using the CLI prompts.

```
> configure network mtu
Do you want to change the MTU [1500] for management0 interface?(Yes/No): Yes
```

```
Enter the new value for MTU [1500]> 1400
MTU set successfully to 1400 from 1500 for management0
Refreshing Network Config...
Interface management0 speed is set to '10000baseT/Full'
>
```

Related Commands

Command	Description
configure network ipv4	Configures IPv4 addressing for the management interface.
configure network ipv6	Configures IPv6 addressing for the management interface.
configure network management-interface	Sets the management or eventing interface MTU.
show network	Shows the management interface configuration.

configure network speed

To set the speed for the management interface or a data interface, use the **configure network speed** command.

Note This command is only supported on the Secure Firewall 3100.

configure network speed { *speed* | **sfp-detect** [*interface_id*]

Syntax Description

interface_id	(Optional) Specifies the interface ID on which to set the speed. The default is management0.
sfp-detect	Detects the speed of the installed SFP module and uses the appropriate speed. This setting is the default. Duplex is always Full, and auto-negotiation is always enabled. This option is useful if you later change the network module to a different model, and want the speed to update automatically.
speed	Sets the speed to a specific speed. Available speeds depend on the interface.

Command Default

The default speed is **sfp-detect**.

Command History

Release	Modification
7.1	This command was introduced for the Secure Firewall 3100.

Usage Guidelines

We recommend using the default **sfp-detect** unless you want to set the speed to a specific speed regardless of the SFP capability.

Examples

The following example sets the speed on the management interface, management0, to 1gbps.

```
> configure network speed 1gbps
```

Related Commands

Command	Description
configure network ipv4	Configures IPv4 addressing for the management interface.
configure network ipv6	Configures IPv6 addressing for the management interface.
configure network management-interface	Sets the management or eventing interface MTU.
show network	Shows the management interface configuration.

configure network static-routes

To add or remove static routes, use the **configure network static-routes** command.

configure network static-routes {**ipv4** | **ipv6**} {**add** *interface destination netmask_or_prefix gateway* | **delete**}

Syntax Description

add	Adds a static route for the management interface.
delete	Removes a static route for the management interface. You are prompted to choose which route to delete.
interface	The ID of the management interface. Use the **show network** command to view the Management interface ID for your model.
ipv4	Adds or deletes a static route for the IPv4 management address.
ipv6	Adds or deletes a static route for the IPv6 management address.
destination	The destination IP address to add or remove, in IPv4 or IPv6 format as appropriate. For example, 10.100.10.10 or 2001:db8::201.
netmask_or_prefix	The network address mask for IPv4, or prefix for IPv6. The IPv4 netmask must be in dotted decimal format, for example, 255.255.255.0. The IPv6 prefix is a standard prefix number, such as 96.
gateway	The gateway address to add or remove, in IPv4 or IPv6 format as appropriate.

Command History

Release	Modification
6.0.1	This command was introduced.

Usage Guidelines

If you configure an event-only interface using the **configure network management-interface** commands, you need to configure a static route if this interface is on a separate network from the management interface. Static routes do not affect through-the-box traffic, i.e. traffic on data interfaces. Without static routes, all management traffic uses the default route specified as the gateway for the default management interface. You typically do not need static routes when using a single management interface, or if the event-only interface is on the same network.

Note For the *default* route, do not use this command; you can only change the default route gateway IP address when you use the **configure network ipv4** or **ipv6** commands for the default management interface.

Examples

The following example adds an IPv4 static route for management interface **management1**, using a destination address of **10.115.24.0**, a network address mask of **255.255.255.0**, and a gateway address of **10.115.9.2**:

```
> configure network static-routes ipv4 add management1 10.115.24.0 255.255.255.0 10.115.9.2
```

The following example adds an IPv6 static route for management interface **management1**, using a destination address of **2001:db8::201**, an IPv6 prefix length of **64**, and a gateway address of **2001:db8::3657**.

```
> configure network static-routes ipv6 add management1 2001:db8::201 64 2001:db8::3657
```

The following example shows how to delete a static route.

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 10.1.1.0
Gateway                   : 192.168.0.254
Netmask                   : 255.255.255.0
> configure network static-routes ipv4 delete
Please select which IPv4 Static Route to delete:
1) management1:   dest 10.1.1.0          nmask 255.255.255.0     gw 192.168.0.254
Please enter number of route to delete: 1
Interface:    management1
Destination:  10.1.1.0
Netmask:      255.255.255.0
Gateway:      192.168.0.254
Are you sure that you want to delete this route?  (y/n) [n]: y
Configuration updated successfully
> show network-static-routes
No static routes currently configured.
```

Related Commands

Command	Description
configure network management-interface	Configures multiple management interfaces.
configure network static-routes ipv4	Adds or removes an IPv4 static route for the management interface.
show network-static-routes	Shows static routes configured for the management interfaces.

configure password

To change the password for the user account you are current logged into, use the **configure password** command.

configure password

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Using this command, the current user can change their password in CLI. After issuing the command, the CLI prompts the user for their current (or old) password, then prompts the user to enter the new password twice.

Examples

The following example changes the password for the current user account.

```
> configure password
Enter current password: oldpassword
Enter new password: newpassword
Confirm new password: newpassword
```

Related Commands

Command	Description
configure user add	Adds a user account for CLI access.

configure policy rollback

To roll back the configuration on the threat defense to the last-deployed configuration, use the **configure policy rollback** command.

configure policy rollback

Command History

Release	Modification
6.7	This command was introduced.
7.2	Rollback is supported for high availability.

Usage Guidelines

If you use a data interface on the threat defense for management center management (see the **configure network management-data-interface** command), and you deploy a configuration change from the management center that affects the network connectivity, you can roll back the configuration on the threat defense to the last-deployed configuration so you can restore management connectivity. You can then adjust the configuration settings in management center so that the network connectivity is maintained, and re-deploy. You can use the rollback feature even if you do not lose connectivity; it is not limited to this troubleshooting situation.

See the following guidelines:

- Only the previous deployment is available locally on the threat defense; you cannot roll back to any earlier deployments.
- Rollback is supported for high availability from management center 7.2 onwards.
- Rollback is not supported for clustering deployments.
- The rollback only affects configurations that you can set in management center. For example, the rollback does not affect any local configuration related to the dedicated Management interface, which you can only configure at the threat defense CLI. Note that if you changed data interface settings after the last management center deployment using the **configure network management-data-interface** command, and then you use the rollback command, those settings will not be preserved; they will roll back to the last-deployed management center settings.
- UCAPL/CC mode cannot be rolled back.
- Out-of-band SCEP certificate data that was updated during the previous deployment cannot be rolled back.
- During the rollback, connections will drop because the current configuration will be cleared.

After the rollback, the threat defense notifies the management center that the rollback was completed successfully. In management center, the deployment screen will show a banner stating that the configuration was rolled back.

If the rollback failed, refer to https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html for common deployment problems. In some cases, the rollback can fail after management center management access is restored; in this case, you can resolve the management center configuration issues, and redeploy from management center.

Examples

The following example rolls back the last deployed configuration.

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....................
.....................
>
```

Related Commands

Command	Description
configure network management-data-interface	Configures a data interface for management center management.

configure raid

To manage the SSDs in a RAID, use the **configure raid** command.

Note This command is only supported on the Secure Firewall 3100.

configure raid { **add** | **remove** | **remove-secure** } **local-disk** { **1** | **2** } [*psid*]

Syntax Description

add	Adds an SSD to the RAID. It can take several hours to complete syncing the new SSD to the RAID, during which the firewall is completely operational. You can even reboot, and the sync will continue after it powers up.
psid	If you add an SSD that was previously used on another system, and is still locked, enter the *psid*. The *psid* is printed on the label attached to the back of the SSD. Alternatively, you can reboot the system, and the SSD will be reformatted and added to the RAID.
remove	Removes the SSD from the RAID and keeps the data intact.
remove-secure	Removes the SSD from the RAID, disables the self-encrypting disk feature, and performs a secure erase of the SSD.
local-disk {**1** | **2**}	Specifies the SSD, disk1 or disk2.

Command Default

If you have two SSDs, they form a RAID when you boot up.

Command History

Release	Modification
7.1	This command was introduced for the Secure Firewall 3100.

Usage Guidelines

You can perform the following tasks at the threat defense CLI while the firewall is powered up:

- Hot swap one of the SSDs—If an SSD is faulty, you can replace it. Note that if you only have one SSD, you cannot remove it while the firewall is powered on.
- Remove one of the SSDs—If you have two SSDs, you can remove one.
- Add a second SSD—If you have one SSD, you can add a second SSD and form a RAID.

Caution Do not remove an SSD without first removing it from the RAID using this procedure. You can cause data loss.

Examples

The following example removes disk2 from the RAID and performs a secure erase.

```
> configure raid remove-secure local-disk 2
```

Related Commands

Command	Description
show raid	Shows the RAID status.
show ssd	Shows the SSD status.

configure snort

To configure advanced behavior for the Snort inspection engine, use the **configure snort** command.

configure snort preserve-connection {**enable** | **disable**}

Syntax Description

preserve-connection {**enable** | **disable**}	Whether to preserve existing TCP/UDP connections on routed and transparent interfaces in case the Snort process goes down. This option is enabled by default, but you can disable it. When enabled, connections that were already allowed remain established, but new connections cannot be established until Snort is again available. When disabled, all new or existing connections are dropped when Snort goes down. Non-TCP/UDP connections, such as ICMP pings, are not preserved. To view the current setting, use the **show running-config snort** command. When viewing the entire running configuration, the **no** form of the **snort preserve-connection** command indicates the feature is disabled.

Command History

Release	Modification
6.2.0.2, 6.2.3	This command was introduced. However, **preserve-connection disable** is not supported with device manager (local management), which re-enables preserve-connection every time it deploys the configuration. This command is not available when the threat defense or management center is running Version 6.2.1, 6.2.2 , 6.2.2.x, or a version earlier than 6.2.0.2, in which case the device behaves as if the command is disabled, whereby all new or existing connections are dropped when Snort goes down.

Usage Guidelines

With **preserve-connection** enabled, if Snort goes down, any existing connections remain established. When Snort becomes available, these established connections continue to bypass Snort inspection. Any new connections that require Snort inspection are dropped until Snort becomes available again.

Example

The following example disables **preserve-connection**.

```
> configure snort preserve-connection disable
```

Related Commands

Commands	Description
show conn	Shows connections.
show conn detail	Includes snort inspection information in connection details.
show conn detail long	Includes snort inspection information in long-format connection details.

configure ssh-access-list

To configure the device to accept SSH connections from specified IP addresses, use the **configure ssh-access-list** command.

configure ssh-access-list *address_list*

Syntax Description

address_list	A comma separated list of IP addresses for hosts or networks, in IPv4 Classless Inter-Domain Routing (CIDR) notation or IPv6 prefix length notation. For example, 10.100.10.0/24 or 2001:DB8::/96. To specify all IPv4 hosts, enter 0.0.0.0/0. To specify all IPv6 hosts, specify ::/0.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

You must include all supported hosts or networks in a single command. Addresses specified in this command overwrite the current contents of the SSH access list.

Merely allowing SSH access does not permit users to log into the local manager. Access to the configuration software is controlled by username and password.

If you exclude the IP address from which you are currently logged into the CLI, your connect will be broken. You will need to change your IP address to regain entry into the CLI.

If the device is a unit in a locally-managed high availability group, your change will be overwritten the next time the active unit deploys configuration updates. If this is the active unit, your change will be propagated to the peer during deployment.

Examples

The following example configures the device to accept SSH connections from any IPv4 or IPv6 address:

```
> configure ssh-access-list 0.0.0.0/0,::/0
The ssh access list was changed successfully.
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh
ACCEPT     tcp      anywhere            anywhere            state NEW tcp dpt:ssh
```

Related Commands

Command	Description
configure disable-ssh-access	Clears the SSH access list.
show ssh-access-list	Shows the SSH access list.

configure ssl-protocol

To configure the SSL protocols clients can use in HTTPS connections to the device, when using the local manager, use the **configure ssl-protocol** command.

configure ssl-protocol {*protocol_list* | **default**}

Syntax Description

default	Enables the default SSL protocol list: **TLSv1.1**, **TLSv1.2**.
protocol_list	A comma-separated list specifying any of the following protocols: **TLSv1**, **TLSv1.1**, **TLSv1.2**, **SSLv3**.

Command Default

The default setting is **TLSv1.1**, **TLSv1.2**.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command sets the protocols clients can use for HTTPS web access to the device. This is used with the local manager, device manager. It is not used with a remote manager.

Note If you use this command to disable the protocol you are currently using to communicate with the device, you will lose the connection.

Examples

The following example configures the device to accept all SSL protocols for HTTPS connections.

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
> configure ssl-protocol TLSv1,TLSv1.1,TLSv1.2,SSLv3
The following ssl protocols are now enabled:  TLSv1 TLSv1.1 TLSv1.2 SSLv3
> show ssl-protocol
The supported ssl protocols are  TLSv1 TLSv1.1 TLSv1.2 SSLv3
```

Related Commands

Command	Description
show ssl-protocol	Shows the currently configured SSL protocols.

configure tcp-randomization

To disable TCP sequence number randomization, use the **configure tcp-randomization** command.

configure tcp-randomization {**enable** | **disable**}

Syntax Description

enable	Change TCP sequence numbers in incoming and outgoing packets randomly to prevent attackers from anticipating the next packet's sequence number.
disable	Do not change TCP sequence numbers in incoming and outgoing packets.

Command Default

TCP sequence number randomization is enabled by default.

Command History

Release	Modification
6.2	This command was introduced.

Usage Guidelines

Each TCP connection has two initial sequence numbers (ISNs): one generated by the client and one generated by the server. The threat defense device randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.

Randomizing the ISN of the protected host prevents an attacker from predicting the next ISN for a new connection and potentially hijacking the new session.

You can disable TCP initial sequence number randomization if necessary, for example, because data is getting scrambled. For example, you might be using a software test tool, software product, or hardware device that depends on TCP packets having sequential numbering. Changing the TCP randomization setting affects all interfaces and all traffic on the device; you cannot change it for specific interfaces or traffic classes.

You should disable TCP sequence number randomization only if you encounter specific problems due to randomization.

Note Although you can disable TCP sequence number randomization when using device manager, each time you deploy the configuration from device manager, the feature is re-enabled. If you want to keep TCP sequence number randomization disabled, you must re-enter the command after each deployment.

Example

The following example disables TCP sequence number randomization.

```
> configure tcp-randomization disable
```

To determine if TCP sequence number randomization is currently enabled or disabled, look in the running configuration for the **set connection random-sequence-number disable** command. This command will be in the global_policy policy map, so you can limit your view of the configuration by using the **show running-config policy-map** command. If the **set connection**

random-sequence-number command does not appear in the configuration, then TCP sequence number randomization is enabled.

For example, the following shows that TCP sequence number randomization is disabled (the relevant command is highlighted).

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
 class tcp
  set connection random-sequence-number disable
!
```

The following example shows that TCP sequence number randomization is enabled because the **set connection random-sequence-number** command is not in the global_policy policy map.

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
```

```
inspect icmp
inspect icmp error
```

configure unlock_time

To set the length of time after which a user account is automatically unlocked after being locked for exceeding the maximum number of failed logins, use the **configure unlock_time** command. This command works in CC/UCAPL compliance mode only.

configure unlock_time *number*

Syntax Description

number	Specifies the unlock time in minutes, from 1 to 9999.

Command Default

When running in CC/UCAPL mode, the default unlock time is 30 minutes.

When not running in CC/UCAPL mode, user accounts remain locked until you unlock them using the **configure user unlock** command. You cannot set an automatic unlock time.

Command History

Release	Modification
6.2.1	This command was introduced.

Usage Guidelines

If you are running in CC/UCAPL compliance mode, you can set a global unlock time for locked out users. After the time expires for a given user who has exceeded the maximum failed login attempts for the user account, the account is unlocked and the user can try again. Use the **configure user maxfailedlogins** command to set the maximum number of failed login attempts you will allow.

Even with an unlock time set, you can unlock a user account at any time using the **configure user unlock** command. The user does not need to wait for the unlock time to expire.

Example

The following example configures an unlock time of 60 minutes.

```
> configure unlock_time 60
```

Related Commands

Command	Description
configure user add	Adds a new user.
configure user maxfailedlogins	Sets the maximum number of failed logins allowed for a user.
configure user unlock	Unlocks the account for the specified user.
show user	Shows user accounts.

configure user access

To change the access authorization level for an existing user, use the **configure user access** command.

configure user access *username* {**basic** | **config**}

Syntax Description

username	Specifies the name of the existing user.
basic	Gives the user basic access. This does not allow the user to enter configuration commands.
config	Gives the user configuration access. This gives the user full administrator rights to all commands.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

When you create a user account, you specify the user's access rights. Use the **configure user access** command to modify the access level of the specified user. The command takes effect the next time the user logs in.

Examples

The following example changes user jdoe's access rights to Basic.

```
> configure user access jdoe basic
```

Related Commands

Command	Description
configure user add	Adds a new user.
show user	Shows the user accounts and access rights.

configure user add

To create a new user account for CLI access, use the **configure user add** command.

configure user add *username* {**basic** | **config**}

Syntax Description

username	Specifies the name of the existing user.
basic	Gives the user basic access. This does not allow the user to enter configuration commands.
config	Gives the user configuration access. This gives the user full administrator rights to all commands.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to create a new user with a specified name, access level, and password. The command prompts for the password. All other account properties are configured with default properties.

Examples

The following example adds a user account named joecool with config access rights. The password is not shown as you type it.

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

Related Commands

Command	Description
configure user access	Sets user access level.
configure user aging	Sets user password aging.
configure user delete	Deletes specified user.
configure user disable	Disables specified user.
configure user enable	Enables specified user.
configure user forcereset	Forces password reset for specified user.

Command	Description
configure user maxfailedlogins	Sets maximum failed logins for specified user.
configure user password	Sets password for specified user.
configure user strengthcheck	Sets strength check requirement on password for specified user.
configure user unlock	Unlocks account for specified user.
show user	Shows user accounts.

configure user aging

To set an expiration date for a user's password, use the **configure user aging** command.

configure user aging *username max_days warn_days* [*grace_period*]

Syntax Description

username	Specifies the name of the user. You cannot change the **admin** user aging settings.
max_days	Specifies the maximum number of days that the password is valid. Values range from 1 to 9999.
warn_days	Specifies the number of days that the user is given to change the password before it expires. Values range from 1 to 9999, but must be less than the maximum days value.
grace_period	(Optional, FXOS platforms only.) Specifies the number of days after the password expires that the user can still change the password. On non-FXOS platforms, the parameter is accepted but the **show user** output shows the grace period is disabled.

Command History

Release	Modification
6.1	This command was introduced.
7.0	The *grace_period* parameter was added.

Examples

The following example sets the user's password to expire in 100 days, and starts warning the user 30 days before password expiration. In the show user output, note the numbers in the Exp and Warn columns.

```
> configure user aging jdoe 100 30
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

The following example sets the password to expire in 180 days, starts warning the user 7 days before expiration, and includes a 7-day grace period.

```
> configure user aging joeuser 180 7 7
> show user
Login          UID   Auth Access  Enabled Reset   Exp   Warn    Grace  MinL Str Lock Max
admin          100  Local Config  Enabled    No  10000     7  Disabled    8 Ena   No N/A
extuser        501 Remote Config Disabled   N/A  99999     7  Disabled    1 Dis   No N/A
joeuser       1000  Local Config  Enabled   Yes    180     7         7    8 Dis   No   5
```

Related Commands

Command	Description
configure user add	Adds a new user.
configure user forcereset	Forces password reset for specified user.
configure user password	Sets password for specified user.
show user	Shows user accounts.

configure user delete

To delete a user account, use the **configure user delete** command.

configure user delete *username*

Syntax Description

username	Specifies the name of the user. You cannot delete the **admin** user.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example deletes a user account.

```
> configure user delete jdoe
```

Related Commands

Command	Description
configure user add	Adds a new user.
configure user disable	Disables a user account without deleting it.
show user	Shows user accounts.

configure user disable

To disable a user account without deleting it, use the **configure user disable** command.

configure user disable *username*

Syntax Description

username	Specifies the name of the user. You cannot disable the **admin** user.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to disable a user account without deleting it. Disabled users cannot login. Use the **configure user enable** command to reenable a disabled user account.

Examples

The following example disables a user account.

```
> configure user disable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
```

Related Commands

Command	Description
configure user add	Adds a new user.
configure user delete	Deletes specified user.
configure user enable	Enables specified user.
configure user unlock	Unlocks account for specified user.
show user	Shows user accounts.

configure user enable

To enable a previously disabled user, use the **configure user enable** command.

configure user enable *username*

Syntax Description

username	Specifies the name of the user.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to enable a user and allow login.

Examples

The following example enables a disabled user account. Note the change in the **show user** Enabled column.

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
> configure user enable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

Related Commands

Command	Description
configure user add	Adds a new user.
configure user disable	Disables specified user.
configure user forcereset	Forces password reset for specified user.
configure user unlock	Unlocks account for specified user.
show user	Shows user accounts.

configure user forcereset

To force the user to change their password the next time they log in, use the **configure user forcereset** command.

configure user forcereset *username*

Syntax Description

username	Specifies the name of the user.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to force the user to reset their password the next time they login. When the user logs in and changes the password, strength checking is automatically enabled.

Examples

The following example forces the user to reset the password on the next log in.

```
> configure user forcereset jdoe
```

Related Commands

Command	Description
configure user password	Sets password for specified user.
configure user strengthcheck	Sets strength check requirement on password for specified user.
show user	Shows user accounts.

configure user maxfailedlogins

To set the maximum number of consecutive failed logins for a user, use the **configure user maxfailedlogins** command.

configure user maxfailedlogins *username number*

Syntax Description

username	Specifies the name of the user.
number	Specifies the maximum number of consecutive failed logins, from 1 to 9999.

Command Default

No default behaviors or values. However, when you create a new account, the default maximum number of consecutive failed logins is 5.

Command History

Release	Modification
6.1	This command was introduced.
6.2.2	When running in CC/UCAPL compliance mode, you can also configure the maximum failed login attempts for the **admin** user.

Usage Guidelines

Use this command to set the maximum number of consecutive failed logins for the specified user before their account is locked. If the user account becomes locked, use the **configure user unlock** command to unlock it.

Examples

The following example sets the maximum number of consecutive failed logins to 3.

```
> configure user maxfailedlogins jdoe 3
```

Related Commands

Command	Description
configure user add	Adds a new user.
configure user password	Sets password for specified user.
configure user unlock	Unlocks the account for the specified user.
show user	Shows user accounts.

configure user minpasswdlen

To set the minimum length for the password for a user, use the **configure user minpasswdlen** command.

configure user minpasswdlen *username number*

Syntax Description

username	Specifies the name of the user.
number	Specifies the minimum length of the password, from 1 to 127.

Command Default

There is no minimum password length.

Command History

Release	Modification
6.1	This command was introduced.
6.2.2	You can now configure a minimum password length for the **admin** user.

Usage Guidelines

Use this command to set the minimum length of the password for the specified user. You are prompted for the current password for the user account. If the minimum length is longer than the current password length, you are also prompted to set a new password.

Example

The following example sets the minimum password length to 8 characters. In this example, the current password is less than the new minimum, so you need to set a new password.

```
> configure user minpasswdlen jdoe 8
Setting minimum password length to 8
Enter current password: <enter old password>
Enter new password for user jdoe: <enter new password>
Confirm new password for user jdoe: <enter new password>

Setting Minimum password length succeeded
```

Related Commands

Command	Description
configure user add	Adds a new user.
show user	Shows user accounts.

configure user password

To set the password on another user's account, use the **configure user password** command.

configure user password *username*

Syntax Description

username	Specifies the name of the user.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to set a specified user's password. This command prompts for the user's password. To change your own password, use the **configure password** command instead of this command.

Examples

The following example sets the password on another user's account. The password is not shown as you type it.

```
> configure user password jdoe
Enter new password for user jdoe: newpassword
Confirm new password for user jdoe: newpassword
```

Related Commands

Command	Description
configure password	Changes the currently logged-in user's password.
configure user add	Adds a new user.
configure user aging	Sets user password aging.
configure user forcereset	Forces password reset for specified user.
configure user maxfailedlogins	Sets maximum failed logins for specified user.
configure user strengthcheck	Sets strength check requirement on password for specified user.
show user	Shows user accounts.

configure user strengthcheck

To enable or disable the strength requirement for a user's password, user the **configure user strengthcheck** command.

configure user strengthcheck *username* {**enable** | **disable**}

Syntax Description

username	Specifies the name of the user.
enable	Sets the requirement for the specified user's password.
disable	Removes the requirement for the specified user's password.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to enable or disable a strength check, which requires a user to meet specific password criteria when changing their password. When a user's password expires or if the **configure user forcereset** command is used, this requirement is automatically enabled the next time the user logs in.

Examples

The following example enables strength checking on a user account.

```
> configure user strengthcheck jdoe enable
```

Related Commands

Command	Description
configure user add	Adds a new user.
configure user forcereset	Forces password reset for specified user.
configure user maxfailedlogins	Sets maximum failed logins for specified user.
configure user password	Sets password for specified user.
configure user unlock	Unlocks account for specified user.
show user	Shows user accounts.

configure user unlock

To unlocks a user account that has exceeded the maximum number of failed logins, use the **configure user unlock** command.

configure user unlock *username*

Syntax Description

username	Specifies the name of the user.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example unlocks a user account.

```
> configure user unlock jdoe
```

Related Commands

Command	Description
configure user add	Adds a new user.
configure user maxfailedlogins	Sets maximum failed logins for specified user.
show user	Shows user accounts.

conn data-rate

To view the connections on the device that are passing heavy loads of data, use the **conn data-rate** command. This command displays per-flow data rate along with the existing connection information. To disable the collection of connections by data-rate, use the **no** form of the command.

conn data-rate

no conn data-rate

Command History

Release	Modification
6.6	This command was introduced.

Usage Guidelines

The **conn data-rate** command is most useful to determine which connections, and users, might be contributing the most to the overall load on the device.

When enabled, the **conn data-rate** feature tracks two statistics for all connections:

- The current (1-second) data rate in the forward and reverse direction of a connection.
- The maximum 1-second data rate in the forward and reverse direction of a connection.

Examples

The following example shows how to enable the connection data rate collection, verify that the feature is enabled, and view data rates:

```
> conn data-rate
> show conn data-rate
Connection data rate tracking is currently enabled.
Use 'show conn detail' to see the data rates of active connections.

> show conn detail

TCP outside: 198.51.100.1/46994 NP Identity Ifc: 203.0.113.1/22,
flags UOB , idle 0s, uptime 9m24s, timeout 1h0m, bytes 68627
Initiator: 198.51.100.1, Responder: 203.0.113.1
data-rate forward/reverse
current rate: 1194/0 bytes/sec <----------------current data rate for forward/reverse flows
max rate: 2520/0 bytes/sec <----------------max data rate for forward/reverse flows
time since last max 0:08:54/NA <----------------time since last max data rate for
forward/reverse flows
```

Related Commands

Command	Description
show conn data-rate	Displays the current state of the connection data rate tracking.
show conn detail	Displays filtered connections by data-rate value.
clear conn data-rate	Clears the current maximum data-rate value.

connect fxos

To enter the FXOS Service Manager CLI mode, use the **connect fxos** command.

connect fxos

Command History

Release	Modification
6.2.1	This command was introduced.

Usage Guidelines

FXOS is the underlying software on Firepower 2100, 4100, and 9300 series devices.

Examples

The following example shows how to enter the FXOS CLI when you started in the threat defense CLI. Enter ? to see the available commands in FXOS.

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2015, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

(...remaining copyrights omitted...)

kp-fpr2100-2#
```

The following example shows what happens if you originally entered the threat defense CLI from the FXOS CLI (using the **connect ftd** FXOS command).

```
> connect fxos
You came from FXOS Service Manager. Please enter 'exit' to go back.
```

copy

To copy a file to or from flash memory, use the **copy** command.

copy [**/noconfirm** | **/noverify**] [*interface_name*] { **/pcap capture:/** [*buffer_name*] | *src_url* | **running-config** | **startup-config** } *dest_url*

Syntax Description

/noverify	(Optional) Skips the signature verification when copying development key signed images.
/noconfirm	(Optional) Copies the file without a confirmation prompt.
interface_name	(Optional) Specifies the interface name through which the file will be copied. If you do not specify the interface, the threat defense checks the data routing table. To use **management** or any other management-only interface, which is not part of the data routing table, you must specify it using this option.
/pcap capture: [*buffer_name*]	Copies the raw packet capture dump of the **capture** command from the specified buffer.
running-config	Specifies the running configuration stored in system memory.
startup-config	Specifies the startup configuration stored in flash memory. The startup configuration is a hidden file in flash memory.

src-url *dest-url*	Specifies the source file, the file you are copying, and the destination file, the file you are creating through the copy. You cannot copy between two remote locations, so if the source file is local, the destination file can be local or remote. If the source file is remote, the destination file must be local. Use the following URL syntax for file locations: • **disk0:/**[[*path/*]*filename*] or **flash:/**[[*path/*]*filename*]—Both **flash** and **disk0** indicates the internal Flash memory. You can use either option. • **disk***n***:/**[[*path/*]*filename*]—Indicates optional external flash drive, where *n* specifies the drive number. • **smb:/**[[*path/*]*filename*]—Indicates Server Message Block, a UNIX server local file system. • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]—The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode). • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]—Indicates an SCP server. The **;int=***interface* option bypasses the route lookup and always uses the specified interface to reach the Secure Copy (SCP) server. • **system:/**[[*path/*]*filename*]—Represents the system memory. • **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]—Indicates a TFTP server. The pathname cannot contain spaces. The **;int=***interface* option bypasses the route lookup and always uses the specified interface to reach the TFTP server. • **cluster_trace:** —Indicates the cluster_trace file system.

Command History

Release	Modification
7.1	If you do not specify the interface, the threat defense checks the data routing table. There is no fallback to the management routing table. Formerly, the default lookup was the management routing table with fallback to the data routing table. Due to the merging of the Management and Diagnostic interfaces, the management routing table is no longer used automatically; you must specify the Management interface if you want to use it.
6.1	This command was introduced.

Usage Guidelines

After you have performed a cluster-wide capture, you can simultaneously copy the same capture file from all units in the cluster to a TFTP server by entering the following command on the master unit:

cluster exec copy /noconfirm /pcap capture:*cap_name* **tftp://***location*/*path*/*filename***.pcap**

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as filename_A.pcap, filename_B.pcap, where A and B are cluster unit names.

Note A different destination name gets generated if you add the unit name at the end of the filename.

Examples

The following example makes a copy of the install log.

```
> copy /noconfirm flash:/install.log flash:/install.save.log
Copy in progress...CC
INFO: No digital signature found
150498 bytes copied in 0.20 secs
```

The following example shows how to copy a file from the disk to a TFTP server in the system execution space:

```
> copy /noconfirm disk0:/install.log
tftp://10.7.0.80/install.log
```

The following example shows how to copy the running configuration to a TFTP server:

```
> copy /noconfirm running-config tftp://10.7.0.80/firepower/device1.cfg
```

The following example shows how to copy a development key signed image without verifying it:

```
> copy /noverify /noconfirm lfbff.SSA exa_lfbff.SSA
Source filename [lfbff.SSA]?
Destination filename [exa_lfbff.SSA]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Writing file disk0:/exa_lfbff.SSA...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Digital Signature was not verified
124125968 bytes copied in 61.740 secs (2034851 bytes/sec)
```

Related Commands

Command	Description
write net	Copies the running configuration to a TFTP server.

cpu hog granular-detection

To provide real-time hog detection and set the CPU hog threshold in a short period of time, use the **cpu hog granular-detection** command.

cpu hog granular-detection [**count** *number*] [**threshold** *value*]

Syntax Description

count *number*	Specifies the number of code execution interruptions performed. Values are from 1-10000000. The default and recommended value is 1000.
threshold *value*	Ranges from 1 to 100. If not set, the default is used, which varies among platforms.

Command Default

The default **count** is 1000. The default **threshold** varies among platforms.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **cpu hog granular-detection** command interrupts the current code execution every 10 milliseconds, and the total number of interruptions is the count. The interruption checks for CPU hogging. If there is any, it is logged. This command reduces the granularity of CPU hog detection in the data path.

Each scheduler-based hog is associated with up to 5 interrupt-based hog entries; each entry could have up to 3 tracebacks. The interrupt-based hog cannot be overwritten; if there is no space, the new one is discarded. The scheduler-based hog is still reused according to the LRU policy, and its associated interrupt-based hog is cleared by then.

Examples

The following example show how to trigger CPU hog detection:

```
> cpu hog granular-detection count 1000 threshold 10
Average time spent on 1000 detections is 10 seconds, and it may take longer
under heavy traffic.
Please leave time for it to finish and use show process cpu-hog to check results.
```

Related Commands

Command	Description
show processes cpu-hog	Displays the processes that are hogging the CPU.
clear process cpu-hog	Clears the processes that are hogging the CPU.

cpu profile activate

To start CPU profiling, use the **cpu profile activate** command.

cpu profile activate [*n_samples* [**sample-process** *process_name*] [**trigger cpu-usage** *cpu%* [*process_name*]]]

Syntax Description

n_samples	Allocates memory for storing *n* number of samples. Valid values are from 1 to 100,000.
sample-process *process_name*	Samples only a specific process.
trigger cpu-usage *cpu%* [*process_name*]	Prevents the profiler from starting until the global 5-second CPU percentage is greater and stops the profiler if the CPU percentage drops below this value. If you specify a process name, it uses the process's 5-second CPU percentage as a trigger.

Command Default

The *n_samples* default value is 1000.

The *cpu%* default value is 0.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The CPU profiler can help you determine which process is using more CPU. Profiling the CPU captures the address of the process that was running on the CPU when the timer interrupt fired. This profiling occurs every 10 milliseconds, regardless of the CPU load. For example, if you take 5000 samples, the profiling takes exactly 50 seconds to complete. If the amount of CPU time that the CPU profiler uses is relatively low, the samples take longer to collect. The CPU profile records are sampled in a separate buffer.

Use the **show cpu profile** command in conjunction with the **cpu profile activate** command to display information that you can collect and that the TAC can use for troubleshooting CPU issues. The **show cpu profile dump** command output is in hexadecimal format.

If the CPU profiler is waiting for a starting condition to occur, the **show cpu profile** command displays the following output:

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

Examples

The following example activates the profiler and instructs it to store 1000 samples, the default. Next, the **show cpu profile** command shows that the profiling is in progress. After waiting some time, the next **show cpu profile** command shows that profiling has completed. Finally, we use the **show cpu profile dump** command to get the results. Copy the output and provide it to Cisco Technical Support. You might need to log your SSH session to get the full output.

```
> cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU profiling currently in progress:
    Core 0: 501 out of 1000 samples collected.
    CP: 586 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU Profiling has stopped.
    Core 0 done with 1000 samples
    CP done with 1000 samples
Use "show cpu profile dump" to see the results.
> show cpu profile dump
(...output omitted...)
```

Related Commands

Command	Description
show cpu profile	Displays the CPU profiling progress.
show cpu profile dump	Displays incomplete or completed results for profiling.

cpu profile dump

To save the results of CPU profiling to a text file, use the **cpu profile dump** command.

cpu profile dump *dest_url*

Syntax Description

dest_url	• **disk0:**/[[*path/*]*filename*] or **flash:**/[[*path/*]*filename*]—Both **flash** and **disk0** indicates the internal Flash memory. Can use either option. • **disk***n***:**/[[*path/*]*filename*]—Indicates optional external flash drive, where *n* specifies the drive number. • **smb:**/[[*path/*]*filename*]—Indicates a UNIX server local file system. Use Server Message Block file-system protocol in LAN managers and similar network systems to package data and exchange information with other systems. • **ftp:**//[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]—The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode). • **http**[**s**]**:**//[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp:**//[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]—The **;int=***interface* option bypasses the route lookup and always uses the specified interface to reach the Secure Copy (SCP) server. • **tftp:**//[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]—The pathname cannot contain spaces. The **;int=***interface* option bypasses the route lookup and always uses the specified interface to reach the TFTP server. • **cluster:**—Indicates the cluster file system.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **CPU profile dump** command writes the CPU profiler output to a specified text file in hexadecimal format.

Examples

The following example stores the most recent CPU profile dump to a file named cpudump.txt:

```
> cpu profile dump disk0:/cpudump.txt
```

Related Commands

Command	Description
show cpu profile dump	Displays incomplete or completed results for profiling.

crashinfo force

To force the device to crash, use the **crashinfo force** command.

crashinfo force /noconfirm {**page-fault** | **watchdog** | **process** *process_ID*}

Syntax Description

page-fault	Forces a crash as a result of a page fault.
watchdog	Forces a crash as a result of watchdogging.
process *process_ID*	Forces a crash of the process specified by process_ID. Use the **show kernel process** command to see process IDs.

Command Default

The device saves the crash information file to flash memory by default.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

You can use the **crashinfo force** command to test the crash output generation. In the crash output, there is nothing that differentiates a real crash from a crash resulting from the **crashinfo force page-fault** or **crashinfo force watchdog** command (because these are real crashes). The device reloads after the crash dump is complete.

Caution Do not use the **crashinfo force** command in a production environment. The **crashinfo force** command crashes the device and forces it to reload.

Examples

The following example forces a crash due to a page fault.

```
> crashinfo force /noconfirm page-fault
```

Related Commands

Command	Description
clear crashinfo	Clears the contents of the crash information file.
crashinfo test	Tests the ability of the device to save crash information to a file in flash memory.
show crashinfo	Displays the contents of the crash information file.

crashinfo test

To test the ability of the device to save crash information to a file in flash memory, use the **crashinfo test** command.

crashinfo test

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Entering the **crashinfo test** command does not crash the device. If a previous crash information file already exists in flash memory, that file is overwritten.

Examples

The following example shows the output of a crash information file test.

```
> crashinfo test
```

Related Commands

Command	Description
clear crashinfo	Clears the contents of the crash information file.
crashinfo force	Forces the device to crash.
show crashinfo	Displays the contents of the crash information file.

crypto ca trustpool export

To export the certificates that constitute the PKI trustpool, use the **crypto ca trustpool export** command.

crypto ca trustpool export *filename*

Syntax Description

filename	The file in which to store the exported trustpool certificates.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command copies the entire contents of the active trustpool to the indicated filepath in pem-coded format.

Examples

```
> crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
>
> more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE
<More>
```

Related Commands

Command	Description
crypto ca trustpool import	Imports the certificates that constitute the PKI trustpool.
crypto ca trustpool remove	Removes a single certificate from the PKI trustpool.
show crypto ca trustpool	Shows the PKI trustpool.

crypto ca trustpool import

To import the certificates that constitute the PKI trustpool, use the **crypto ca trustpool import** command.

crypto ca trustpool import [**clean**] **url** *url* **noconfirm** [**signature-required**]
crypto ca trustpool import [**clean**] **default noconfirm**

Syntax Description

clean	Removes all downloaded trustpool certificates prior to import.
default	Restores the device's default trusted CA list.
noconfirm	Suppresses all interactive prompts.
signature-required	Indicates that only signed files are accepted. If the **signature-required** keyword is included but the signature is not present or cannot be verified, the import fails.
url *url*	Specifies the location of the trustpool file to be imported. • **disk0:/**[[*path/*]*filename*]—Indicates the internal Flash memory. • **disk***n***:/**[[*path/*]*filename*]—Indicates optional external flash drive, where *n* specifies the drive number. • **smb:/**[[*path/*]*filename*]—Indicates a UNIX server local file system. Use Server Message Block file-system protocol in LAN managers and similar network systems to package data and exchange information with other systems. • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]—The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode). • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]—The **;int=***interface* option bypasses the route lookup and always uses the specified interface to reach the Secure Copy (SCP) server. • **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]—The pathname cannot contain spaces. The **;int=***interface* option bypasses the route lookup and always uses the specified interface to reach the TFTP server.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command provides the ability to validate the signature on the file when a trustpool bundle is downloaded from cisco.com. A valid signature is not mandatory when downloading bundles from other sources or in a

format that does not support signatures. Users are informed of the signature status and are given the option to accept the bundle or not.

The possible interactive warnings are:

- Cisco bundle format with invalid signature
- Non-cisco bundle format
- Cisco bundle format with valid signature

Note Unless you have verified the legitimacy of the file through some other means, do not install the certificates if a file signature cannot be verified.

Examples

The following example restores the default trustpool.

```
> crypto ca trustpool import clean default noconfirm
```

Related Commands

Command	Description
crypto ca trustpool export	Exports the certificates that constitute the PKI trustpool.
crypto ca trustpool remove	Removes a single certificate from the PKI trustpool.
show crypto ca trustpool	Shows the PKI trustpool.

crypto ca trustpool remove

To remove a single specified certificate from the PKI trustpool, use the **crypto ca trustpool remove** command.

crypto ca trustpool remove *cert_fingerprint* [**noconfirm**]

Syntax Description

cert_fingerprint	The certificate fingerprint in hexadecimal.
noconfirm	Specify this keyword to suppress all interactive prompting.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example removes a certificate.

```
> crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0
```

Related Commands

Command	Description
clear crypto ca trustpool	Removes all certificates from the trustpool.
crypto ca trustpool export	Exports the certificates that constitute the PKI trustpool.
crypto ca trustpool import	Imports the certificates that constitute the PKI trustpool.
show crypto ca trustpool	Shows the PKI trustpool.