Introduction to Tamper Detection

Tamper detection

Tamper detection is a security feature that helps you identify tampering events on Cisco 8400 Series Secure Routers running IOS XE release 17.19.1 or later.

Each router is shipped from the manufacturer with the chassis cover securely fastened. If the chassis cover is opened after shipment, the hardware records all chassis cover open and close events in tamper-proof memory. This occurs whether the device is powered on or off.

During boot up, the software reads the latest event index and compares it with previously known indices. If here is a discrepancy, a syslog message reports the tamper event during a startup. When the device is in a fully powered up state, a syslog message and an SNMP trap are generated immediately.

Benefits of tamper detection

Tamper detection notification detects unauthorized physical access or attempts to compromise the device, helping protect sensitive data and network integrity.

Limitations of tamper detection

- Tamper detection feature is currently not supported on SDWAN/SD-Routing mode.

Configure tamper detection

Tamper detection is enabled by default on the router. The open or close events of the chassis cover are auto recorded.

The tamper event notification can be enabled or disabled using these commands in config mode.

Procedure

Step 1 Enable the tamper detection notification using this command in config mode (enabled by default):

```
Router(config)#platform tamper detection
```

Step 2 Disable the tamper detection notification using the command in config mode:

```
Router(config)#no platform tamper detection
```

Verify the tamper detection events

Use the **show platform tamper-detection event** command to verify tamper detection events.

```
Router# show platform tamper-detection event [power-off | power-on] [all | lastx | new]
```

Table 1: Tamper detection event command options

Option	Description
power off	Displays tampering events recorded when the router was not powered on.
power on	Displays tampering events recorded when the router was powered on.
all	Displays all recorded tampering events. The system displays a maximum of 500 entries. Each set of 500 entries increases the rollover counter by one.
lastx	Displays the specified number of events. For example, `lastx 10` displays the last 10 events.
new	Displays new tampering events recorded since the last known event index.

The **show** command provides an event log with these details:

- Current event index
- Current time
- Rollover Status and Rollover Count:
  - When tamper event count <= 500, the Rollover Count is 0, Rollover Status is No
  - When the log count reaches 500, the Rollover Count increases by 1:
    - When 501-1000 overwrites 1-500, the Rollover Count is 1, Rollover Status: Yes
    - When 1001-1500 overwrites 501-1000, the Rollover Count is 2, Rollover Status: Yes

- The events indicating event type and timestamp

Verify events when system is not powered on

This topic shows an example event log for tamper detection when the system is not powered up.

When the system is not powered on, the router uses battery power to record any tampering events. The router records the first chassis cover open event between last power off and the next power on. If the chassis cover was opened or closed multiple times when the system was powered off, only the first open event is recorded. The following example shows the event log when the system was not powered on:

```
Router#show platform tamper-detection event power-off all
Current Time: 2025/04/25 19:55:03 Rollover Status: No Rollover Count: 0
Tamper event index | Tamper event timestamp | Tamper events description


#2 2024/08/08 02:36:41 Chassis is opened
#1 2000/00/00 00:00:00 Battery not present or used
up
```

Table 2: Power-off tamper events

#2	2024/08/08 02:36:41	Chassis is opened
#1	2000/00/00 00:00:00	Battery not present or used

Verify events when system is partially or fully powered on

This topic shows an example event log for tamper detection when the system is partially or fully powered on.

When system is powered on, the router records all chassis cover open or close events. The following is an example of the event log when the system is partially or fully powered on:

```
Router show platform tamper-detection event power-on lastx 10
Current Time: 2025/04/25 19:54:46 Rollover Status: No Rollover Count: 0
Tamper event index | Tamper event timestamp | Tamper events description


#2 025/04/24 22:10:14 Chassis is opened
#1 025/04/24 22:02:33 Chassis is closed
```

Table 3: Power-On tamper events

#2	025/04/24 22:10:14	Chassis is opened
#1	025/04/24 22:02:33	Chassis is closed

Syslog messages for tamper detection

This topic provides examples of tamper detection syslog events.

When the router boots up, it reads the current event index from the event log and compares it with the last known index stored previously. If there is a mismatch between the indices or the timestamps differ, when the tamper detection notifications are enabled, IOS generates a warning-level syslog message at bootup.

This section provides examples of distinct syslog events.

- Syslog for power-on events

  When tamper detection is enabled and the system is powered on, a power-on syslog message is displayed during boot-up.

```
Apr 25 20:15:01.064: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
 opened 0 times and closed 0 times during power up since last known event index 7 at
2025/04/24 22:11:51
```

- Syslog for power-off events

  When tamper detection is enabled and the system is not powered, a power-off syslog message is displayed during boot-up.

```
Apr 25 20:15:01.064: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
 opened 0 times and closed 0 times during power down since last known event index 5 at
 2025/04/24 22:11:51
```

- Syslog for runtime events

```
*Aug 29 06:56:34.560: %CMRP-4-INTRUSION_ALERT: R0/0: cmand: The system cover has been
opened !!
*Aug 29 06:56:36.130: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
 opened 2 times and closed 0 times during power down since last known event index 50
at 2025/06/04 08:03:06
*Aug 29 06:56:36.130: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
 opened 20 times and closed 20 times during power up since last known event index 1638
 at 2025/06/05 07:08:12
*Aug 29 06:57:04.563: %CMRP-4-INTRUSION_ALERT: R0/0: cmand: The system cover has been
closed !!
*Aug 29 06:57:06.137: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
 opened 2 times and closed 0 times during power down since last known event index 50
at 2025/06/04 08:03:06
*Aug 29 06:57:06.137: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
 opened 20 times and closed 21 times during power up since last known event index 1638
 at 2025/06/05 07:08:12
```

Note If the tamper detection feature is disabled, the syslog messages will not be displayed at boot up.