

Tamper Detection

Tamper detection is a security feature implemented in Cisco 8000 Series Secure Routers to identify potential tampering events. Each router is shipped from the manufacturer with its 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, regardless of whether the device is powered on or off.

On boot up, the software reads the latest event index and compares it with previously known indices. When tamper detection notifications are enabled, the software generates a SYSlog message during startup to report the tamper event. When the device is in fully powered up state, a chassis open or close event will generate syslog message immediately, regardless of whether the Tamper Detection notifications are enabled or not.

Benefits

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

Limitations

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

- Configure Tamper Detection, on page 1
- Verify the Tamper Detection events, on page 2
- How to mark the events, on page 3
- Tamper Detection SYSlog, on page 4

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.

- Enable the Tamper Detection notification using this command in config mode (enabled by default):

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

- Disable the Tamper Detection notification using the command in config mode:

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

Verify the Tamper Detection events

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

Option	Description
power-off	The **power-off** option specifies the tampering events when router doesn't have power cable connected.
power-on	The **power-on** option specifies the tampering events when the router was powered on.
all	The **all** option specifies all the recorded tampering events. System can show maximum 500 entries. Every time 500 entries are recorded, the rollover counter increases by one.
lastx	The **lastx** option specifies the number of events to display. For example, "lastx 10" will show the last 10 events.
new	The **new** option specifies the new tampering events since last known events index.

The show command provides an event log which contains these details:

- Current event index
- Current time
- Rollover Status and Rollover Count:
  - When tamper event count is less than or equal to 500, the Rollover Count is 0, and the Rollover Status is No
  - When the log count reaches 500, the Rollover Count will be increased 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

During the manufacturing process, the device may trigger several cover open or cover close events. The manufactory mark these events as known events.

Thesee known events can be viewed when using this command.

```
show platform tamper-detection event power-off | power-on all
```

To view only the events that occurred after the device left the manufacturing site, use this command.

```
show platform tamper-detection event power-off | power-on new
```

To determine if a tamper event occurred after the device left the factory, refer to the `TAMPER_DETECTION_EVENT_MSG` in the system logs.

Verify events when system is not powered

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

```
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
```

Verify events when system is partially or fully powered on

When system power is available, the router records all chassis cover open or close events. 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
```

How to mark the events

Procedure

Step 1 request consent-token generate-challenge tamper-auth auth-timeout <timeout value in minutes>

Generates a challenge for consent token.

Step 2 request consent-token accept-response tamper-auth <response_string>

Accept the response with the generated challenge.

Step 3 request platform hardware tamper-detection event-mark

Post successful execution, the system confirms that the tamper event has been marked and terminate the authentication session.

Consent token authentication

The `event-mark` command requires consent token authentication for security. This is an example of the workflow:

```
Router# request consent-token generate-challenge tamper-auth auth-timeout 60
[redacted]
Router#
*Feb 11 08:48:39.682: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation
attempt: Tamper-auth 0).

8PP2B# request consent-token accept-response tamper-auth
61+O/gAAAQYBAAQAAAUBAgAEAAAAAAMBYlNVOHNvRmlIUDFiUEp4OU5yTVEwUCtK
SkMrNUp3MnpNMWlJcC9ibEJjakQxcFJaWGxtNDNkWGJVYnZ2bVpiRFUNCjV2ckt3
eDV4ajEabnVtUURNTFdxeExLb0IwMHhkMkRRdEQyUWJ2TlR5L0V4V1JNRjdDQ0VT
YjRKREFrVnBaMGkNCm43ZHlyMWsrTGpGV1FaeGkvc2lnUVgyOHR4ZEx6VHVsckxk
b3pGK3FnRmZCeWNhR3lmU3VwT0ZKcFU2T0ZGVWANCllhY01ZWXZ3aTF0WUZKaE1n
d1BBTVkxbFE4b3JoSXVNVTU5S1RhZ0YxNmw0V0tBK3dEbVpHc2F0Sk5ubDIrL3gN
CjdndmljMFNCNXR2aXR2YVNyVTNtaVFnWkM3MnNLdHhMb3R5Zi9nNVVwcWVkUFJR
K21aVXhlUysyakdFS1pNbmoNCnIrNkpIQnpXZ05lMm05SUpnUGhTVHc9PQoBYk9O
NCtGSi95Ym1LeVpHRmNBY28xQjZlUVBrcSswY3lWU0lsZkgyVGw1dFNHM0NjWHk4
bnpCa0xIYTN2NGZJMjQNClZ5aE96MldTZDRBMUk1bHFVVmtyekI3aHJqRjJsaUQ1
anRQOU1XcEVaMkR3eVMxcmh0bmhHNG1HRFFiQmFXVlENCmJXbVBQUkFiQ2xobG1a
L2RDUTdhMkxIVXA0RDI0RTJPWmtsdGlXeVpnT3dBVHZQUndXVWxmTm9HSlNxN3U4
a0QNClZBM2pqTW5MdHJXRzFkTkhZemg4UjM3Uy82SDVXY1dJOWpZMGlkS2NqRDVC
TzUzK21xYTdLNVU2T3ppaE5FZFcNCjQvRlk1OStldWs2d0kyeDZTdWE1V2dZKy8w
UnIzL3B4RTJjTDg5NUVvejYwWlNnaFc4d25LYU1RMEM0cWFlc1kNCmNYanc3alZm
ekpZY0dkTkpXK280a0E9PQ==

% Consent token authorization success

Router#
*Feb 11 08:49:29.826: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authentication success:
 Tamper-auth 0).

Router# request platform hardware tamper-detection event-mark
% Tamper-event marked successfully...terminating the tamper auth session
% Consent token authorization termination success

8PP2B#
*Feb 11 08:49:54.788: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (terminate authentication:
 Tamper-auth 0).
```

Tamper Detection SYSlog

When the Tamper Detection notifications are enabled, IOS will generate a warning-level SYSlog message at bootup. It reads the current event index from the event log, compares it with the last known index stored previously, and states the difference.

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.

Interpreting Syslog Messages

If the syslog displays a non-zero open or close count in the message, it indicates that the cover was accessed after the device left the manufacturing facility.

```
System cover was opened <open-count> times and closed <close-count> times during power
<down|up>
      since last known event index <index> at <timestamp>
```