Kernel Minidump and Trustzone Upgrade

- Kernel minidump and trust zone upgrade, on page 1

Kernel minidump and trust zone upgrade

The kernel minidump and trust zone upgrade feature is a diagnostic capability that

- collects and preserves kernel and driver data structures when a crash occurs
- stores these data structures for post-crash analysis in a standardized Type-Length-Value (TLV) format
- automatically upgrades the trust zone on supported devices so the system can collect CPU registers for comprehensive debugging.

Feature History for kernel minidump and trustzone upgrade support

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature history

Release	Feature information
Cisco IOS XE 17.18.1	This feature enhances control over minidump collection on Wi-Fi 7 (802.11be) APs. A new option has been added to limit the number of kernel core dump directories stored on the AP. This command has been modified: • **core-dump kernel dir-limit** Support has been added for these access points: • Cisco Wireless 9178 Series Access Points. • Cisco Wireless 9176 Series Access Points.

Release	Feature information
Cisco IOS XE 17.14.1	Kernel Minidump and Trustzone Upgrade feature offers a more effective method for diagnosing kernel issues. This command is introduced: • **core-dump kernel type**

Feature overview

Traditionally, when a kernel crash occurs on Wi-Fi 6 (802.11AX) access points, only AP console logs are available for troubleshooting. However, these logs often lack the detail needed to determine the root cause accurately.

The kernel minidump and trust zone upgrade feature, introduced in Cisco IOS XE 17.14.1, provides a more effective method for diagnosing kernel crashes. The feature captures and organizes internal data structures critical for debugging so you can troubleshoot problems more accurately.

How kernel minidumps work

When you enable the feature, the system collects references to key kernel or driver structures. It stores them in a Type-Length-Value (TLV) format in kernel memory.

After a crash and the access point reboots, the system writes the referenced data structures to the */storage/cores* directory on the access point flash memory. You can export these files for advanced analysis.

Trust zone upgrade

In AP using Qualcomm Software Development Kit (QSDK) version 11.3, the trust zone module collects CPU registers after a crash. It then preserves these registers for later retrieval by the crash dump process.

When you enable the kernel minidump and trust zone upgrade feature, the system automatically upgrades the trust zone to the latest version on supported access points.

Note The trust zone upgrade occurs only once. If you disable the Kernel Minidump and Trustzone Upgrade feature or downgrade the controller software to a release earlier than Cisco IOS XE 17.14.1, the trust zone upgrade does not roll back.

Supported APs

You can use the kernel minidump and trust zone upgrade feature on the following access points running Cisco IOS XE 17.14.1 or later:

- Cisco Catalyst 9124 Series Access Points
- Cisco Catalyst 9136 Series Access Points

Example: Kernel minidump and trust zone upgrade in action

After you enable the feature, if a supported access point experiences a kernel crash, you can access the TLV files in the */storage/cores* directory and export them. This provides comprehensive diagnostic data to accelerate root cause analysis and issue resolution.

Configure the Minidump from the AP (CLI)

Configure minidump collection on your access point. This lets you capture kernel coredump information for troubleshooting and diagnostics.

Before you begin

- Ensure that no clients are connected to the AP.
- Keep your AP in standalone mode. This prevents it from receiving conflicting payloads from the controller.
- Any configuration pushed from the controller overrides the value you set on your AP.

Procedure

Enable kernel coredump collection on the AP.

Example:

```
Device# configure boot minidump enable
```

After you enable kernel coredump collection, the AP stores critical kernel dump data for further analysis.

Configure the minidump from the controller (CLI)

Enable and customize collection of kernel core dumps (minidump) for access points to support troubleshooting and diagnostics.

Use this procedure when you need to collect kernel core dumps from access points to assist with root cause analysis of device crashes or unexpected reboots. Configuring the minidump feature allows you to control the number and type of core dumps stored for each AP.

Procedure

Step 1 Enters global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure an AP profile and enter AP profile configuration mode.

Example:

```
Device(config)# ap profile profile-name
```

Step 3 Configure the maximum number of kernel core dumps to be collected on an AP.

Example:

```
Device(config-ap-profile)# core-dump kernel limit limit
```

Valid range is from 0 to 5.

Step 4 Configure the maximum number of directories for AP minidump collection.

Example:

```
Device(config-ap-profile)# core-dump kernel dir-limit dir-limit
```

The valid range is from 15 to 25.

Step 5 Configure the type of kernel core dump to be collected on the AP.

Example:

```
Device(config-ap-profile)# core-dump kernel type mini-dump
```

Use the **core-dump kernel type disable** command to disable kernel core dump.

Note
Changing the core dump type from disabled to full-dump or mini-dump or vice versa will cause the APs to reboot.

When you enable the full-dump option, the kernel minidump feature gets deactivated.

Step 6 Return to global configuration mode.

Example:

```
Device(config-ap-profile)# end
```

The AP profile is configured to collect kernel minidumps according to the specified limits and type. AP using this profile will store core dumps as configured.

Verify minidump configuration

To view the mini-dump configuration on the controller, use this command:

```
Device# show ap name AP3C57.31C5.99D0 config general  | sec Kernel core dump

Kernel core dump :
  Configured limit                          : 3
  Kernel core dumps collected on AP         : 1
  Kernel core dump type                     : Mini dump
```

To view the mini-dump configuration on the AP, use this command:

```
AP# show boot

--- Boot Variable Table ---
BOOT path-list:      part1
Console Baudrate:    115200
Enable Break:        yes
Manual Boot:         yes
Memory Debug:        no
```

```
Crashkernel:          no
Minidump:             yes # Indicates Minidump is enabled.
SCRUB_LIMIT:          40 (default)
Kdump Limit:          5 # Configured limit. (this came from WLC via payload)
Kdump Collected:      0 # Number of times the feature ran after it was enabled.
Debug init:           0
```