



New Features for Cisco IOS XE 17.10.1a

This chapter contains the following sections:

- [Support for the P-5GS6-GL Pluggable Module on the ESR6300, on page 1](#)
- [MAB 802.1x Support, on page 1](#)
- [Enable Secure Data Wipe Capabilities, on page 1](#)
- [Rawssocket Keepalive Configuration CLI, on page 2](#)

Support for the P-5GS6-GL Pluggable Module on the ESR6300

Support for the P-5GS6-GL Pluggable Module works the same on the ESR6300 as it does on the other IoT Routers. For details, see [5G Sub-6 GHz Pluggable Interface Module](#) and [Cellular Pluggable Interface Module Configuration Guide](#).

MAB 802.1x Support

Standalone MAC Authentication Bypass (MAB) is an authentication method that grants network access to specific MAC addresses regardless of 802.1X capability or credentials. As a result, devices such as cash registers, fax machines, and printers can be readily authenticated, and network features that are based on authorization policies can be made available.

For further information, see the [Authentication Authorization and Accounting Configuration Guide, Cisco IOS XE](#)

Enable Secure Data Wipe Capabilities

Secure data wipe is a Cisco wide initiative to ensure storage devices on all the IOS XE based platforms to be properly purged using NIST SP 800-88r1 compliant secure erase commands. Whenever possible, IoT platforms will leverage the corresponding ENG design and implementation available so far on their platforms.

This feature is supported on the following IoT platforms:

- IR1101
- IR1800
- IR8140

- ESR6300

When the enable secure data wipe is executed, the following will get wiped out:

- IR1101, IR1800, IR8140: NVRAM, rommon variables, and bootflash
- ESR6300: NVRAM, rommon variables, bootflash

The router will be in rommon prompt with default factory settings (baud rate 9600) after the command is executed. The bootflash will not get formatted until booting with IOS image thru usbflash or tftp download if the platform is supported.

Performing a Secure Data Wipe

To enable the feature, perform the following:

```
Router#factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]Y
```



Important This operation may take hours. Please do not power cycle.

To check the log after the command is executed, and booting up IOS XE, perform the following:

```
Router#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IR1800
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 15:17:29.
```

Rawsocket Keepalive Configuration CLI

Rawsocket keepalive for async interfaces is a feature that existed in classic IOS platforms. As part of 17.10.1a, the feature will be extended to IOS-XE based platforms. A new CLI with the following syntax will be added under rawsocket.

```
Router(config-line)#raw-socket tcp keepalive interval
```

CLI Changes

On IOS-XE platforms starting from 17.10.1a, there is a CLI correction and an additional CLI was added as part of raw-socket.

The correction is for the **raw-socket idle timeout** command. There is now an option to configure the timeout based on minutes and seconds, whereas the previous configuration used only minutes.

```
Router(config-line)# raw-socket tcp idle-timeout [0-1440] [<0-59> | cr]
```

The additional CLI is for clearing the raw-socket TCP clients. The command syntax is **clear raw-socket line** [1-145/tty/x/y/z] for example:

```
Router# clear raw-socket line 0/2/0
```



Note When initiating clear raw-socket line, raw-socket sessions will be cleared for raw-socket clients from the **show raw-socket tcp sessions** command. Connections will be re-established after a TCP hand-shake, which can be done by doing shut/no shut on TCP connection interface.
