Cisco CMX 10.5
EU General Data Protection Regulation

What is personal data?

Personal data or personal identifiable information (PII), a complex category of information, broadly means a piece of information that can be used to identify a person. This can be a name, an address, an IP address, a phone number, etc. Pseudonymized personal data can also fall under the General Data Protection Regulation if it is possible that a person still could be identified.

What is the EU General Data Protection Regulation?

The General Data Protection Regulation (GDPR) is a new framework for data protection laws in the European Union (EU). The EU's GDPR website says the legislation is designed to "harmonize" data privacy laws across Europe as well as give greater protection and rights to individuals. The GDPR was ratified in early 2016 and became widely enforceable on May 25, 2018. The goal of the GDPR is to enable individuals to better control their personal data.

The GDPR can be found at the EU website:
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

More information is available here:
https://ec.europa.eu/info/law/law-topic/data-protection_en

Why does the GDPR apply to CMX?

Cisco® Connected Mobile Experiences (CMX) is a system that allows you to collect the location of wireless clients. To identify the client, CMX uses the wireless device's MAC address. Under GDPR, a device's MAC address, IP address, etc. are considered to be personal identifiable information. CMX allows you to store location information in multiple ways and processes it to create analytics data. In the context of the GDPR, CMX is used to process personal data; you are the data controller as well as the data processor.

Does Cisco guarantee that CMX is GDPR compliant?

No. Cisco does not have control over your individual CMX configuration. Furthermore, there might be other local laws besides the EU GDPR that you have to follow. Please consult your legal department and your GDPR data privacy officer to achieve a CMX configuration that complies with your requirements. This document helps you understand the features available in CMX on-premises.

What is the best practice to improve data privacy?

- Collect the consent of the individual before collecting data.
  - Inform the user about your privacy policy. Explain how you are collecting the data and your intent.
- Collect only the data needed for the current purpose.
- Keep the data only for as long as necessary.
  - Set the data retention interval as short as possible for your purpose.
- Keep data protected while in transport or at rest.
  - Use HTTPS and strong passwords.
  - Restrict physical and network access to CMX.
  - Use full disk encryption.

What data does CMX store?

The client history database stores the following device information:

- Timestamp
- MAC address or hashed MAC address if hashing is enabled
- Location (campus, building, floor, zone, X- and Y-coordinates in relation to a map, and GPS coordinates)
- RF information such as Wi-Fi bands used, strongest received signal strength indication (RSSI), and nearest access point
- 802.1X username

The default configurable client history pruning interval is 30 days. Analytics has a table for raw visits, which stores:

- Timestamp
- MAC address or hashed MAC address if hashing is enabled
- Location (campus, building, floor, zone)

This data is used to count visits and detect repeat visits.

How long is data stored in CMX?

The following pruning intervals are configurable:

- Client history pruning interval (default: 30 days)
- Rogues history pruning interval (default: 30 days)
- Analytics raw data pruning interval (default: 365 days)

All the history data for clients, rogues, and raw data for analytics will be deleted under this retention policy. No aggregate data for analytics will be affected by this retention policy, unless the aggregate involves user-specific information such as MAC address.

Which CMX data privacy features are available?

The following features are available to support you in achieving GDPR compliance.

Please refer to the Cisco CMX Configuration Guide for a detailed configuration description.

Tracking settings

Configure only the specific device category that needs to be located for your business application. For example, you might want to locate asset tags (active RFID) only. Asset tags used for assets and not people might not be considered to be PII. The following device types can be enabled and disabled individually:

- Wireless clients
- Rogue access points
- Rogue clients
- Interferers
- RFID tags
- Bluetooth Low Energy (BLE) tags

Filtering parameters

The following global filtering parameters are available:

- Exclude probing only clients
  Allows you to track only users who have given their consent before connecting to your network.
- Enable location MAC filtering
  Allows you to track only clients in the list or to exclude specific clients from tracking.
- Enable location SSID filtering
  Restricts tracking to individual SSIDs only or excludes SSIDs from being tracked.

Data privacy settings

CMX 10.5 introduces the following data privacy settings.

MAC hashing
This feature allows you to anonymize the MAC address of a client as soon as it is received from the wireless controller. CMX will continue with the hashed MAC address only. The hashing algorithm will use a salt that is user configurable, and salt changes can also be scheduled.

The hash function is as follows:

hash(mac bytes, org secret)=

SHA1(mac bytes ++ org secret).takeRight(4)v

The hash function truncates the hash to 4 bytes. This produces a theoretical information loss, as the domain of the function is larger than the range: a 6-byte MAC allows (2^48) possibilities, whereas a 4-byte hash allows (2^32) possibilities. This results in 65,000 possible (org + MAC) combinations for each 4-byte hashed MAC address. Therefore, given a MAC that has been salted, hashed, and truncated with the unique CMX algorithm, it would be mathematically impossible to know with a reasonable degree of certainty what the original client MAC address was.

When the salt is changed, the hash of the MAC changes. CMX is able to detect repeat devices for CMX Analytics and CMX Connect only as long as the salt does not change. When the salt is changed, all devices will be identified as new devices.

Opt-in and opt-out APIs
Additional APIs are available starting with CMX 10.5 to register MAC addresses that you want to use for location or analytics. There are individual MAC address tables for location and analytics. APIs allow third-party applications (such as captive portal software) to collect individual consent and register the device MAC addresses individually. This allows you to restrict the processing of the data. For example, a client might be tracked to use the location information for wayfinding, but the data should not be used for analytics.

Third-party software integration
The preferred way to integrate third-party software for purposes such as analytics is to use northbound notifications. CMX will send data in JSON format to a web-hook via HTTPS-POST. The notification has the following data:

- Timestamp
- MAC address or hashed MAC address if hashing is enabled
- Location (campus, building, floor, zone, X, Y)
- RF information such as Wi-Fi bands used, strongest RSSI, and nearest access point
- 802.1X username

In addition to the hashing of the MAC address on ingress to CMX, the configuration of the northbound notifications allows hashing with an individual salt. This will prevent data processed by multiple third-party systems from being combined.

Full disk encryption
CMX 10.5 allows you to enable disk encryption on the OS level for data protection.

Q How do the data privacy features affect CMX Connect?

A The hashing and later changing of the hashing salt will prevent CMX Connect from recognizing an already known device. It also might not be possible to provide the captive portal based on client location. In this case CMX Connect will fall back to the location of the access point the client is connected to.

If data privacy is turned on and MAC hashing is turned off, an additional content element for opt-in will become available. CMX Connect users will be tracked only if they enable this opt-in check box.

Q How can I comply with the "right to be forgotten"?

A GDPR allows individuals to request the deletion of the personal data stored. You would need the MAC address to delete the data.

CMX data is stored in different formats, depending on the different configuration options. Please contact the Cisco Technical Assistance Center (TAC) if you receive a request to delete individual data. A script will be provided based on your configuration that will completely delete this data.

Data might already have been deleted based on the individual data retention settings. It also might not be possible to identify data after the salt has been changed and the old salt has been deleted.

Q How can I access individual data for export?

A The GDPR allows individuals to request all personal information stored. You would need the MAC address to fetch the data.

Please use the following REST APIs to fetch the data:

- Client History API to collect the location data stored in the history table:
  macaddress/api/location/v1/history/
  clients/:macaddress?date=20180525
- Repeat Device API to fetch the data from the repeat device list
  area/api/analytics/v1/isRepeatDevice/:macaddress

Both APIs will return the data in JSON format.

Please see the Cisco CMX REST API Getting Started Guide for more information on how to use CMX APIs.

Q What privacy features are available in the various CMX releases?

A There are two different types of installations:

- CMX Location and Analytics
- CMX Presence and Connect

Depending on the privacy requirements, you should consider moving from CMX Presence and Connect to CMX Engage. CMX Engage is a cloud-based captive portal solution offering similar site configuration options but with much better analytics capabilities. CMX Engage is hosted in EU data centers and is fully GDPR compliant. Visit https://cmxcisco.eu/cmxengage/ for more information or to sign up for a trial account.

Table 1 shows the privacy features available in **CMX Location and Analytics releases 10.3 through 10.5**.

Table 1. Privacy features in CMX Location and Analytics

Feature	CMX 10.3	CMX 10.4	CMX 10.5
Configure tracking of			
Wireless clients, RFID tags, interferers	✔	✔	✔
Rogue access points, rogue clients	-	✔	✔
BLE tags	-	✔	✔
MAC filtering			
Exclude probing clients	✔	✔	✔
Location MAC filtering	✔	✔	✔
Location SSID filtering	✔	✔	✔
Data retention			
Client history	Default 30 days	Default 30 days	Default 30 days
Rogue access point and rogue client history	-	Default 30 days	Default 30 days
Analytics raw data	Fixed 365 days	Fixed 365 days	Default 30 days
MAC hashing			
Northbound notifications	✔	✔	✔
Ingress	No	No	✔
Opt-in/opt-out			
Opt-out option for CMX Connect users	✔	✔	✔
Opt-in option for CMX Connect users	No	No	✔
Opt-in/opt-out APIs to support external portals	No	No	✔
Data protection			
Full disk encryption	No	No	✔
Strong password enforced for cmxadmin and root	No	No	✔

Table 2 shows the privacy features available in **CMX Presence and Connect** releases 10.3 to 10.5. There are currently no plans to add additional features.

Table 2. Privacy features in CMX Presence and Connect

Feature	CMX 10.3	CMX 10.4	CMX 10.5
Exclusion filters			
Exclude SSIDs	✔	✔	✔
Exclude device MAC addresses	✔	✔	✔
Repeat filters	✔	✔	✔
Data retention			
Analytics raw data	Fixed 365 days	Fixed 365 days	Fixed 365 days
MAC hashing			
Northbound notifications	✔	✔	✔
Ingress	No	No	No
Opt-in/opt-out			
Opt-out option for CMX Connect users	✔	✔	✔
Data protection			
Full disk encryption	No	No	✔
Strong password enforced for cmxadmin and root	No	No	✔

Upgrading to CMX 10.5

Inline upgrade to CMX 10.5 from a previous release is not supported. You have to back up your existing CMX and restore it on a fresh installation of CMX 10.5. Make sure your current installation is updated to CMX 10.4.1 before starting your backup.

You can exclude the history database by restricting the backup if you do not want to restore previously captured personal data.

Enabling data privacy on CMX 10.5

Enabling data privacy on CMX 10.5 will take a few minutes and will not be immediately reflected in the Settings UI.

If you enable data privacy on CMX 10.5 at a later point, you might want to delete data you have already collected. This can be done via the command-line interface (CLI):cmxctl config data deleteAll.