

ExtremeLocation: Data Processing Description

1.0 Subject matter of processing

The subject matter of the data processing carried out by Extreme Networks is the provision of ExtremeLocation to the Customer, as further described in the end user license agreement between Extreme Networks and the Customer.

2.0 Duration of processing

Data will be processed over the period for which ExtremeLocation is provided to the Customer.

3.0 Nature and purpose of processing

Data will be subject to various types of processing, which may include presence detection, location determination, analytics, authorisation and configuration. Data is processed for ExtremeLocation's Customers to benefit from location visibility and analytics related to visitors to their facilities. Data is also processed for troubleshooting purposes.

4.0 Categories of data

The categories of data that ExtremeLocation processes may include:

- Device-specific data, including MAC addresses, device manufacturers, and Receive Signal Strength Indication (RSSI).
- Network access data, including Network/SSID connection data.
- Geographic location data, site name, and region name where the device is located or observed.
- Storage of contact information used to register a tenant account in ExtremeLocation (email address, phone number (optional), and address (optional)).

5.0 Categories of data subjects

The data that ExtremeLocation processes relates to categories of data subjects that may include:

- The Customer's employees, temporary employees, contractors, visitors and guests to the Customer's premises (or the vicinity), and actual and potential customers of the Customer's own products and/or services.
- Employees of the Customer's vendors, service providers and commercial partners.

6.0 Processing operations

The data that ExtremeLocation processes is subject to various processing operations, as set out under section 3.0 above.

7.0 Data transfers

In order to provide ExtremeLocation services to the customer, data may be transferred between Extreme Networks entities, some of which may be located outside of the EEA.

- The name and location of any such entities will be set out in the service agreement between Extreme Networks and the Customer.
- The categories of data and data subjects that these transfers may involve is listed under sections 4.0 and 5.0 above.
- Data transferred will be subject to various types of processing, which may include the processing listed under section 3.0 above.

8.0 Additional information regarding technical and organisational security measures

All instances of ExtremeLocation software, and customers' related data (configuration, statistics, etc.), currently are hosted in the Amazon cloud availability zone located in Frankfurt, Germany. The Amazon Web Services ("AWS") support team is not authorized to access/view data in ExtremeLocation. Visibility to AWS is limited to infrastructure level information (CPU, Memory, connectivity details). On March 26, 2018, AWS announced that it had "completed

the entirety of [its] GDPR service readiness audit, validating that all generally available services and features adhere to the high privacy bar and data protection standards required of data processors by the GDPR.” See <https://aws.amazon.com/compliance/gdpr-center/>.

In addition, data storage is done using MongoDB clusters deployed by DBaaS provider mLab and stored in the AWS Frankfurt region. Only our application cluster hosted in AWS has access to the database deployment, and this is enforced using an IP whitelisting for the nodes in the application cluster for connections to the database. For additional information about mLab’s data security features, see <https://docs.mlab.com/security/>.