

Data Collection and Processing

Mobile Real User Monitoring

Product Overview

At AppDynamics, we offer enterprise-grade software that enables our customers to monitor and analyze the performance of their business applications and supporting infrastructure. Our Mobile Real User Monitoring software (MRUM Software), one of our end user monitoring (EUM) products, monitors the performance of our customers' mobile applications through the lens of a user's journey and interaction with their monitored mobile applications.

The MRUM Software can be deployed to our customers as a fully on-premise installation, consumed by our customers as software-as-a-service (SaaS), or made available as a "hybrid deployment" where the customer's on-premise AppDynamics software controller instance leverages our SaaS-based EUM Collector and EUM Cloud services (both discussed below) for temporary data processing.

The information below addresses SaaS and "hybrid deployment" versions of the MRUM Software; for fully on-premise installations, we do not have access to the data collected by the MRUM Software.

What data does the MRUM Software collect?

Our MRUM Software is designed to collect the types of performance data about our customers' browser-based application listed below. Which data types set out below are actually collected and processed by a customer's unique instance of our MRUM Software depends on how the customer chooses to configure their MRUM Software and the nature of their monitored mobile application.

IP address for user device By default, the MRUM Software collects the geographic location of a user mobile device at the time the device makes a connection to the monitored application. To resolve the location data, the user mobile device IP address is combined with geo-location data. The resolved geo-location data are sent to our SaaS infrastructure. By default, the IP address of the relevant user device is discarded by our SaaS infrastructure and not retained. But the customer's MRUM Software administrator can choose to change the default setting and configure their MRUM Software settings to retain the user device IP address from the data beacon that is sent to our SaaS infrastructure for processing.

Application infrastructure usage data The MRUM Software can be enabled to collect information regarding the performance of infrastructure components that support the monitored mobile application during a user session. These performance data may include: operating system information (type, version), application information (type version), title of page visited, URL of page visited, and URLs of assets loaded on the relevant web page.

Metrics related to the session The MRUM Software can be configured to collect the following session metrics: length of browsing session and time on a specific URL during session.

Crash reports and error reports The MRUM Software customer administrator can enable the collection of call stacks of crashes and errors within the mobile application code.

Custom data collection The customer's MRUM Software administrator may choose to enable the collection of customer parameter and/or payload information using the MRUM Software SDK by writing application code to collect any data that is accessible within the customer's mobile application.

Mobile screen shots Screen shots of what a user viewed within a user's mobile application instance can be taken at the time of crash or error in the mobile application. The collection of mobile screen shots is disabled by default, and the MRUM Software customer administrator can choose to enable the collection of mobile screen shots using the RBAC supported configuration settings in the product UI.

Personal data collection and processing

The MRUM Software does not require the collection of personal data and does not collect personal data by default. The MRUM Software customer administrator can choose to configure the MRUM Software to collect and process IP addresses of user devices as well as payload and parameter information within their mobile application, and therefore our customer controls whether the MRUM Software collects and processes personal data.

Where a customer administrator chooses to configure the MRUM Software to collect and process personal data, we comply with applicable law when we make international transfers of such personal data. For international transfers, we employ the following legally-recognized data transfer mechanisms: the EU-US Privacy Shield, the Swiss-US Privacy Shield, and Standard Contractual Clauses (also commonly referred to as EU Model Clauses).

For more information about our privacy practices and how we process our customers' personal data, please visit our Privacy Center at <https://www.appdynamics.com/privacy>.

Does the MRUM Software “track” my customers around the internet?

The MRUM Software is designed to monitor a mobile application's performance via the performance metrics noted above. All of these data help our customers understand how a real user experiences the monitored mobile application. The MRUM Software does not track a customer's application users around the internet as those users visit third-party sites and applications via their mobile device. But, the AppDynamics customer administrator can choose to configure the MRUM Software to track user interaction over time across the customer's monitored mobile application. In order to provide this functionality (i.e., the ability to identify that the same user or set of users experienced a crash/problem or series of crashes/problems with the same instance of the monitored application or across multiple instances of the monitored application), the MRUM Software can be configured to use a technology that attaches a globally-unique identifier (“GUID”) to each instance of the monitored application. The GUID is generated using the native tools provided by the mobile OS (iOS and Android, as applicable) and is attached to the performance data package as it leaves the monitored application and is sent over the internet to the nearest EUM Collector (described below). If a customer chooses to use the GUID user identification method, the customer maintains the key needed to match the GUID with a specific user/device profile; this key is not stored within our SaaS infrastructure by default.

Where are data processed?

Data are collected by the AppDynamics MRUM Software javascript agent (which is installed in the customer's monitored mobile application code) and the data are sent to the AppDynamics EUM software collector service (the EUM Collector). The EUM Collector is hosted in Amazon Web Services (AWS) regions around the world in order to provide low latency connections to each customer device. The performance data are sent from the EUM Collector to the "EUM Cloud" where the data from worldwide EUM Collectors are aggregated. The AppDynamics controller downloads the aggregated data from the EUM Cloud once every minute for final processing, storage, and viewing by the customer.

For most SaaS deployments, the AppDynamics controller resides either in our co-located data center located in Chicago, IL, United States or AWS regions located in the United States. The EUM Cloud services are located in AWS regions in the United States and EUM Collectors are located in AWS regions worldwide. Additionally, AppDynamics offers a number of geographic hosting options where the AppDynamics controller and the MRUM Software are deployed in Amazon Web Services locations worldwide. For a list of the current deployment options or details about an existing deployment, customers should contact their account manager.

For "hybrid deployments," the AppDynamics controller resides in the customer's datacenter and leverages our EUM Collector and EUM Cloud services.

How is access to data controlled?

We use industry-standard techniques designed to restrict access to and to prevent unauthorized use of our information systems. We require the use of individual user accounts to maintain the integrity of audit trails. User and group management is centralized using single-sign-on systems and access to systems is subject to management approval. Access to all systems that process or store customer data are reviewed and re-approval is required periodically.

How long are data retained?

Information about data retention for the MRUM Software is set out in the relevant License Entitlement located at <https://docs.appdynamics.com/display/latest/License+Entitlements+and+Restrictions> .

Can I delete or rectify data?

Our customers may request information regarding the deletion of data, or make specific requests to have certain data deleted from our systems and records, by emailing privacy@appdynamics.com .

The MRUM Software collects data from various sources as described above. If the source data are incorrect then the collected data will be incorrect. It is not possible to correct the data within the product but if the source data are corrected, the next time the product collects the data, it will be accurate. Customers can submit deletion requests for inaccurate data.

Are the data encrypted?

Yes; our SaaS software products support encryption of customer data in transit and at rest, including backups.

How secure is the data?

We are committed at all levels to the security of customer data. We have developed a comprehensive security program and organization that is supported by leadership who are committed to proactively managing cybersecurity risk. By focusing on a secure-by-design approach, we seek to weave security into our development practices early and layer security across our architecture to protect its corporate services, supply chain, software distribution, and customer-facing services.

We implement process, and technical controls designed to manage cybersecurity risks. Controls may be physical, technical or administrative in their operation, and they may be preventative, detective, corrective, deterrent or recovery focused in their intent. Controls may include hardware and software functions, processes, and procedures, as well as organizational and managerial structures. Controls are reviewed periodically to ensure they are still appropriate.

We maintain a SOC 2 Type II certification. For more information, please visit <https://www.appdynamics.com/security>.

Third parties

We engage third-party service providers to help us provide our products and related services. We maintain an up-to-date list of such third parties and a description of their activities at <https://www.appdynamics.com/privacy/subprocessors>.