Sensitive Data Collection and Security

AppDynamics collects data on application performance, health, and resources, in addition to the application components (transactions, code libraries) and related infrastructure (nodes, tiers). Before deploying AppDynamics, you should ensure that your application is secure and does not expose sensitive data. This page describes how to prevent sensitive data collection in your application environment.

Preventing Sensitive Data Collection

If your environment contains sensitive data that should not be processed by an AppDynamics product or sent to the AppDynamics SaaS environment, you should avoid the following:

- Applications that transmit sensitive data in URL query parameters
- Enabling HTTP request parameter capture
- Enabling bind variable capture
- Applications that send sensitive data in error logs and log files
- Allowing method invocation data collection
- Log captures

If you do capture logs, ensure that you mask values in those logs. The following sections cover additional measures that you can take to ensure you do not expose sensitive data.

SaaS Deployment

AppDynamics supports encryption at rest in its SaaS deployments on personally identifiable information and sensitive business data.

On-premises Deployment

AppDynamics offers an on-premises solution for customers who want to maintain full control over their deployment of the software. With this type of implementation, AppDynamics has no access to the software or the data it collects and processes. Customers subject to strict regulatory requirements for data security may want to consider an on-premises solution. On-premises customers are responsible for encrypting their data by either using self-encrypting drives or other non-product solutions.

Role-based Access Control

You can use role-based access controls (RBAC) to limit the number of users who can access data collection features. The controls let you restrict a user's access to specific functions, data, analytics queries, and APIs.

You can control user access to data by specifying permissions for each user role. To configure user access, navigate to Settings > Administration. For more information, see Analytics and Data Security and Roles and Permissions.

Suppress Raw SQL Capture

Application Monitoring collects raw SQL as prepared statements captured with dynamic parameters bound to runtime values.

You can disable the capture of raw SQL if it contains sensitive data. When you disable raw SQL capture, the SQL call appears in its original form, but with question mark parameters in place of sensitive data.

To disable the capture of raw SQL for an application, navigate to Configuration > Instrumentation > Call Graph Settings > SQL Capture Settings. Uncheck the Capture Raw SQL box.

You can also disable bind variable capture. Bind variables are placeholders for literal data in your SQL statements. When you disable bind variable capture, the values of bind variables are not displayed. For more information, see Call Graph Settings.
Hide Query Literals

Database Visibility hides query literals by default since queries can contain sensitive user data.

To verify that query literals are hidden for a database, navigate to Configuration. In the Security section, ensure that you have chosen the Remove literals from the queries option box. For more information, see Configure Query Literals Security.

You may also want to use bind variables as placeholders for literal data in your SQL statements.

Exclude Error Logs

Application Monitoring logs exceptions and errors that match parameters you specify in your custom logger. You may want to exclude sensitive payload data so that it does not show up in error logs.

To exclude a class in your application:

1. Navigate to Tiers & Nodes > Actions > Configure App Server Agent.
2. Select Use Custom Configuration.
3. Click the (+) button to create a new agent property.
4. Set the agent property name to exceptions-to-ignore.
5. Set the agent property value to the name of the class you want to exclude.

For more information, see Error Detection.

Mask Log Analytics Values

When configured, Application Analytics collects performance data from your app server agents, data from your log files, and performance and sessions data from End User Monitoring. You can mask sensitive information in your log analytics data.

To mask log analytics data:

1. Navigate to Analytics > Configuration > Log Analytics > Source Rules.
2. Click on the source rule that you want to specify masking for.
3. In the Field Management tab, next to ThreadName, you can specify the starting and ending position of the data you want to mask, and the character to use as the masking value.

For more information, see Configure Log Analytics Using Source Rules.

Disable the Data Collector

You can suppress data collection of HTTP request payloads, raw SQL, and other user data.

For the Java Agent, configure the disabled-features node property in the Controller UI.

For the .NET Agent, edit the config.xml file and set the disabled-features property to the names of features that you want to disable.

```xml
<property name="disabled-features" value="RAW_SQL,LOG_PAYLOAD,METHOD_INV_DATA_COLLECTOR,HTTP_DATA_COLLECTOR,CUSTOM_EXIT_SNAP_DATA"/>
```

For more information, see App Agent Node Properties Reference and .NET Agent Configuration Properties.

Filter Sensitive Data in Environment Variables
You can mask sensitive data found in Java environment variables and system properties. To mask sensitive data, add the `sensitive-data-filter` property to `app-agent-config.xml`. The valid attributes are `applies-to`, `match-type`, and `match-pattern`. For more information, see Filter Sensitive Data.

Data Privacy Policy Dialog

Data collection has regulatory, legal, and customer-defined policies that you must follow. AppDynamics provides a data privacy policy reminder, in the form of a UI dialog, when you or your users configure parts of the AppDynamics products that could be used to collect regulated or other protected information.

This customizable statement is present in all areas of the AppDynamics UI where you can configure data collection. AppDynamics displays a default message if you have not made any customizations.

AppDynamics logs an event when it displays the data privacy policy dialog to you or another user.