Technical Report

NetApp Active IQ

Telemetry and UI Feature Security

The NetApp Active IQ Team, NetApp
May 2018 | TR-4699

Abstract

This document describes the NetApp® Active IQ® telemetry solution, including how it works, the content of the messages sent to NetApp, the benefits it provides, and options customers have in setting it up. It is intended to help you make an informed decision about using this service with your NetApp products.

NetApp®

TABLE OF CONTENTS

What is NetApp Active IQ and what is it used for?

Answer: NetApp Active IQ is a cloud service that provides predictive and proactive insights that help you optimize operations across the hybrid cloud. Active IQ displays information about your NetApp systems by aggregating telemetry data from NetApp AutoSupport®, which is a predictive technology built into NetApp ONTAP®, SolidFire®, E-Series, StorageGRID® Webscale, and NetApp Cloud Backup systems.

NetApp telemetry services work by accessing only your system's metadata. The underlying information stored on NetApp systems is never accessed or transferred.

As a NetApp customer, you should understand what data is collected, how the data is transferred to NetApp, and how NetApp keeps it secure and private.

Can I disable AutoSupport?

Answer: Yes, if you feel uncomfortable with using the AutoSupport feature, you can turn it off. However, consider the following innovative and efficiency-creating benefits offered by AutoSupport that are no longer available if you disable it:

- NetApp AutoSupport technology proactively monitors the health of your data, wherever it lives. It continuously watches your flash, traditional, and cloud storage, drawing on over 200 billion real-time and historical diagnostic records to spot potential problems before they affect your business.
- AutoSupport regularly sends status messages to NetApp. If a problem occurs, many of these messages automatically open a case, request additional data, and provide corrective solutions without requiring any action from your IT staff. This dramatically improves the speed of support case handling. In fact, systems that use AutoSupport experience, on average, 80% fewer P1 outages.
- Active IQ improves the self-service support and operational efficiency of NetApp systems and provides information about configurations, performance, and health checks (indicated by red, yellow, or green status levels in the dashboard). It also provides information about installed software and storage efficiency and provides access to many other tools.
- By leveraging machine learning using the anonymized data from our customer base, Active IQ can provide insights to your product usage. It can also make recommendations about configurations,

upgrades, and optimizations to help your NetApp products run more efficiently with optimal performance and storage utilization.

How does AutoSupport work?

Answer: AutoSupport collects configuration, status, and performance information about your systems and packages it into AutoSupport messages. This information is collected and stored locally, even if you disable the sending of AutoSupport messages.

Note: AutoSupport collects metadata about your systems. It never collects business data from your systems. It has no ability to collect or transmit data that is stored on a system. The data that AutoSupport collects is limited to information that is used to resolve problems with a system.

Does AutoSupport include customer-identifying information?

Answer: AutoSupport can collect data that might be considered customer-identifying if used in conjunction with other data sources outside of the systems, such as corporate or public phone directories. Examples include the e-mail addresses of storage administrators, which might include company domain names and thus can be mapped to the name of a company and potentially an individual within that company. DNS names are also included, which by definition contain the company domain name.

The following sections provide details about specific products.

ONTAP

ONTAP offers an innovative solution that protects sensitive customer-identifying data by masking or filtering sensitive information with the `–remove-private-data` parameter of the `node autosupport modify` command. When enabled (set to true), this parameter removes, encodes, or masks sensitive data from AutoSupport attachments and headers.

Eliminated data includes the following items:

• IP addresses • MAC addresses • URIs • DNS names • E-mail addresses • Port numbers	• Node names • Storage virtual machine names • Cluster names • Aggregate names • Volume names • Junction paths	• Policy names • User IDs • Group IDs • LUNs • Qtree names

NetApp recommends removing private data only if you have a sensitive environment that requires the most robust security. Removing the data has the following customer impacts:

- Limited system information visibility and functional capability in Active IQ (for example, when viewing the operational efficiency, performance, and system health dashboard views)
- Reduced value to customers from other NetApp services that depend on AutoSupport content analysis, such as Assessment Services and storage optimization and efficiency reports
- Increased support resolution times compared to complete AutoSupport information messages

Ninety-eight percent of issues detected by AutoSupport have a known resolution, and a solution is provided through the NetApp knowledgebase.

E-Series, NetApp Cloud Backup, and StorageGRID Webscale

AutoSupport messages for these products do not contain any customer or personally identifiable information.

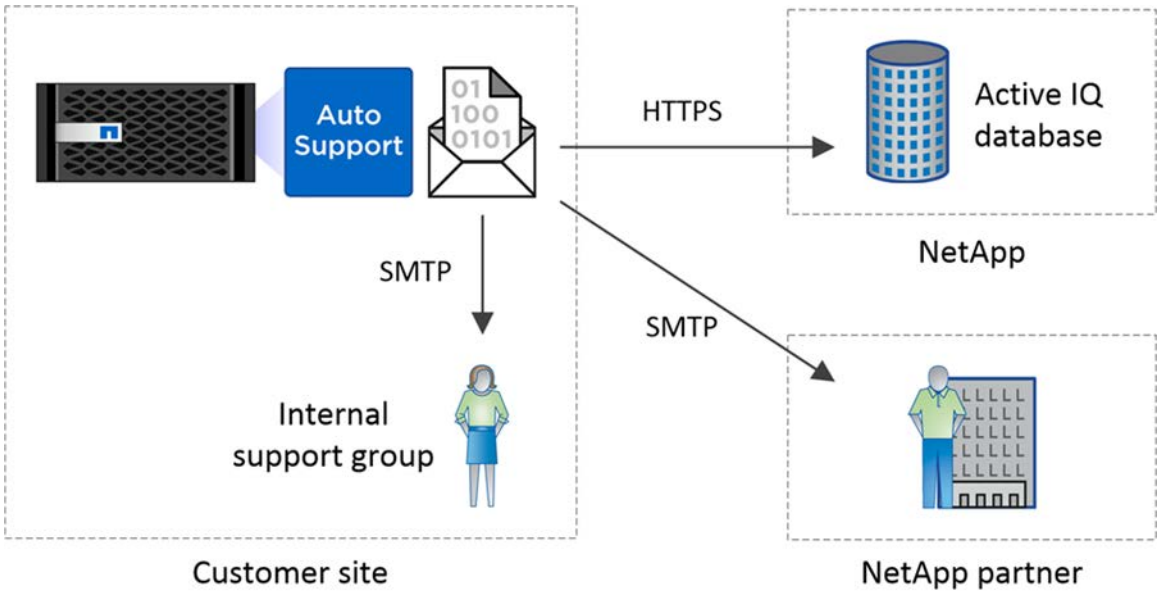
SolidFire

Data from SolidFire might contain customer name and user ID information.

How is AutoSupport data transferred?

Answer: By default, AutoSupport sends messages to NetApp technical support by using the HTTPS protocol, except for StorageGRID Webscale, which uses SMTP. AutoSupport also supports HTTP and SMTP; however, because of the sensitive nature of AutoSupport messages, NetApp strongly recommends using HTTPS. HTTPS connections to NetApp are encrypted and authenticated using modern standards.

You can also configure AutoSupport to send messages to your internal support organization and a support partner. Those messages are always sent using an SMTP server provided by customers.



To improve e-mail security, NetApp supports Transport Layer Security (TLS) through VeriSign 256-bit digital certificates for encryption and authentication between mail server gateways. To use this method, ask your e-mail administrator to enable TLS and install digital certificates on your mail servers. This provides authentication against “man-in-the-middle” attacks. TLS encrypts the AutoSupport e-mail content between your e-mail server and the NetApp e-mail servers.

Who can access Active IQ?

Answer: Users with valid, NetApp-provided credentials and proper product entitlements can access Active IQ by using NetApp single sign-on. Customers can only see and access their own Active IQ account (for example, systems that are owned by the customer account). The customer has full access control and can therefore limit access internally to certain systems or certain departments on a need-to-know basis within the customer’s organization or parts of it.

NetApp service personnel can access the data for service resolution and postsales support. For NetApp customers who are directly supported by partners, these partners have access to Active IQ but can view only those systems that they either directly sold or supported.

What do Active IQ reports contain?

Answer: AutoSupport messages contain only configuration data, state data (subsystem up/down, available capacity, and so on), system log files (Event Management System [EMS], messages, and user-space), and performance metrics of the respective NetApp system. No customer data stored on any NetApp system that uses AutoSupport is sent to NetApp, nor can the data be accessed through Active IQ.

Will Active IQ display any sensitive security data about my company?

Answer: No, Active IQ is based on AutoSupport, which only collects configuration and environmental data of AutoSupport enabled NetApp systems. An AutoSupport message includes the customer's point of contact, but you can configure it to show a generic title and e-mail address, such as "storage_admin@company.com." The following information is also sent in an AutoSupport message:

- Company name (if configured on the system)
- Some diagnostic logs might contain user names, such as the user name executing a command on the storage device.
- IP addresses of the storage device. These are "internal" IP addresses (for example, 10.x.y.z) that do not provide access to the device from outside a customer's network.
- Volume names

Will Active IQ display any data stored on the systems?

Answer: There is no access to any customer data stored on the systems where AutoSupport is enabled.

Neither NetApp nor NetApp partners can access any customer-sensitive data, because Active IQ only shows configuration data of the AutoSupport enabled NetApp system.

Does NetApp perform security testing?

Answer: NetApp tests access controls as part of monthly release cadence system integration testing. NetApp also runs monthly vulnerability assessments.

For how long is telemetry data retained?

Answer: While a support contract is in place, NetApp retains AutoSupport data for up to seven years. If a contract is terminated, NetApp deletes the data within one year after termination.

Are certifications available?

Answer: NetApp is ISO 27001:2013 certified. The scope of this certification includes AutoSupport.

NetApp does not provide any audit reports for customer consumption.

Can I reveal AutoSupport data to other parties?

Answer: Active IQ analytics and reporting derived from AutoSupport telemetry contain information about your system environment and configuration. Revealing this information might require consultation with your security officer.

In addition, AutoSupport reports contain NetApp technical and trade secrets. Therefore, revealing AutoSupport information to NetApp competitors is strictly prohibited.

If you have more questions about AutoSupport, please email ng-activeiq-feedback@netapp.com.

Where to Find Additional Information

To learn more about the information described in this document, refer to the following document:

- Active IQ: The Evolution of AutoSupport
  https://www.netapp.com/us/products/data-infrastructure-management/active-iq-predictive-technology.aspx
- Security and Privacy of NetApp Telemetry Data
  https://www.netapp.com/us/media/tr-4688.pdf

Version History

Version	Date	Document Version History
Version 1.0	May 2018	Initial release.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

Trademark Information

TR-4699-0518