Technical Report

Security and privacy of NetApp telemetry data

TR-4688

Brett Albertson and the Active IQ team, NetApp
March 2023 | TR-4688

Abstract

NetApp® Active IQ® Digital Advisor displays information about your NetApp systems by aggregating telemetry data from the predictive technology built into those systems. As a NetApp customer, you should understand how this telemetry data is kept secure and private.

TABLE OF CONTENTS

Introduction **3**

AutoSupport and the Active IQ predictive technology 4

SolidFire Active IQ Predictive Technology 4

Collection of Telemetry Data **4**

ONTAP 4

E-Series 6

SolidFire 6

NetApp HCI 6

Cloud Backup 7

StorageGRID 7

OnCommand Insight 7

Active IQ Unified Manager 7

SANtricity Web Services (REST API) 7

Active IQ OneCollect 8

Transfer of telemetry data **8**

On demand delivery of AutoSupport messages 9

Access and retention of telemetry data **10**

Where the data resides 10

Data handling and encryption 11

Data access 11

Security testing 11

Data retention period 12

Certifications 12

LIST OF TABLES

Table 1) Supported transport protocols for AutoSupport. 8

LIST OF FIGURES

Figure 1) Overview of Active IQ Digital Advisor. 3

Figure 2) How AutoSupport data is transferred. 9

Introduction

NetApp Active IQ Digital Advisor is a cloud service that provides predictions and recommendations based on peer comparisons and community learning. These insights can help you become a data-driven IT organization. Active IQ enables you to perform the following tasks:

- Monitor and predict capacity usage to stay a step ahead of users' rapidly growing data demands
- Improve security and protect your investments with automated upgrade alerts for software and firmware
- Get recommendations for optimizing configurations based on proven best practices
- Resolve performance issues fast with real-time insights into system bottlenecks
- Apply community wisdom from diagnostic data from across the NetApp user base

Active IQ Digital Advisor displays information about your NetApp systems by aggregating telemetry data from the predictive technology built into NetApp ONTAP® software (on premises and in the cloud), NetApp SolidFire® technology, NetApp E-Series storage controllers, NetApp StorageGRID® object storage, NetApp Cloud Backup (formerly AltaVault™), Active IQ OneCollect, and Active IQ Unified Manager.

Note: Data is also collected from NetApp OnCommand® Insight and NetApp SANtricity® Web Services, but that data is not currently displayed in Active IQ.

The guiding principle of NetApp telemetry handling is to provide predictive analytics and proactive support by processing functional data about your systems, such as configuration, status, performance, and log information. As described in this document, you have choices about the types of functional data collected. Most importantly, the underlying data stored on NetApp systems is never processed.

As a NetApp customer, you should understand what data is collected, how the data is transferred to NetApp, and how it is kept secure and private. The information in this document applies to the standalone Active IQ Digital Advisor website, the NetApp BlueXP™ digital advisor, and the Active IQ mobile application.

Figure 1) Overview of Active IQ Digital Advisor.

AutoSupport and the Active IQ predictive technology

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 packages telemetry data into status messages, which, in normal operating conditions, are regularly sent 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.

The telemetry data is made available to customers (product owners) and NetApp Customer Support through the NetApp Active IQ Digital Advisor interface. See the section on Data Access below for details on role-based restrictions.

SolidFire Active IQ predictive technology

Starting the moment you deploy a cluster, SolidFire Active IQ continuously and proactively monitors your systems to make sure that you experience the highest possible levels of availability and performance. This telemetry data is also uploaded to the Active IQ database, where it is processed and made available to customers (product owners) and support through the NetApp Active IQ interface.

Collection of telemetry data

AutoSupport and SolidFire Active IQ collect functional data such as configuration, status, and performance information about your systems. You can disable sending telemetry data to NetApp if you choose; however, doing so affects your access to predictive analytics and proactive support, such as automatic case creation. The procedure for disabling AutoSupport depends on the platform. See the product documentation for information about how to perform this action.

Note: AutoSupport is enabled by default on most NetApp systems.

Note: You may have to either configure a proxy or change your firewall settings to allow AutoSupport messages to be sent to NetApp.

For ONTAP, you also have the option to mask sensitive information from AutoSupport messages, but doing so can affect support as well. This option is disabled by default.

AutoSupport telemetry data is handled using security best practices and controls that address privacy regulations. NetApp also offers a Customer Data Processing Addendum (available here) that commits NetApp to compliance with any applicable legal requirements related to privacy and data protection.

Review section 4, Access and retention of telemetry data, before deciding to limit any data sent to NetApp. Doing so makes it more difficult to manage, monitor, maintain, and support your systems.

The following sections list the information collected from each type of system and software.

ONTAP

The following list is a representative sample of what is included in an AutoSupport message for ONTAP.

Note: You can identify the exact content sent in an AutoSupport message by reviewing the manifest for that message. To do so, use the `system node autosupport manifest show` command.

- Date and timestamp of the message
- ONTAP software version
- Serial number of the storage system
- Encrypted software licenses
- Host name of the storage system

- SNMP contact name and location (if specified)
- Console encoding type
- Output of commands that provide system information
- Checksum status
- Error-Correcting Code (ECC) memory scrubber statistics
- The following information, if a high-availability (HA) configuration is licensed:
  - System ID of the partner in an HA pair
  - Host name of the partner in an HA pair
  - HA node status, including the HA monitor and HA interconnect statistics
- Contents of non-privacy-related files under the `/etc` directory
- Expiration date of all NetApp SnapLock® volumes on the system
- Registry information
- Usage information
- Service statistics
- Boot time statistics
- NVLOG statistics
- NetApp WAFL® check log
- Modified configurations
- X-header information
- Information about the boot device (such as the CompactFlash card)

Certain portions of this data, either alone or in combination with other external data sources, may identify an individual or company, or contain confidential information. See section 4.2, Data encryption, for information about encryption of sensitive information in AutoSupport when it is received by NetApp. To give our customers additional control over the data they send to NetApp, ONTAP offers a solution that protects the privacy of sensitive customer-identifying data by masking or filtering that 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
- SVM names
- Cluster names
- Aggregate names
- Volume names
- Junction paths
- Policy names
- User IDs

- Group IDs
- LUNs
- Qtree names

You should remove private data only if you have a compliance reason requiring the most robust security. Removing the data has the following significant functional 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

E-Series

Each AutoSupport message for E-Series storage systems contains the following information:

- System log files
- Configuration data (formatted XML and unstructured command output)
- State data (subsystem up/down and capacity used)
- Performance metrics
- System inventory data

SolidFire

The following information is collected from SolidFire systems:

- Volume, snap, account node IDs, and so on
- Performance and capacity data for clusters and volumes
- Error and event history
- SolidFire software versions
- Hardware configuration information
- Quality-of-service (QoS) configurations
- Volume details (size, creation date, and so on)
- Volume access group and session configurations
- Node and cluster IPs

The following information is not collected:

- Any actual end-user data
- CHAP secrets
- Passwords
- Cluster administrative user information

NetApp HCI

The following information is collected from NetApp HCI compute systems in addition to the SolidFire storage systems noted in section 2.3:

- Hardware and configuration information for HCI compute nodes
- vCenter Alarm information for HCI compute nodes
- Support and monitoring data for HCI compute nodes

- Virtual machine configuration information
- vCenter license, version, and configuration information

Cloud Backup

Each AutoSupport message for Cloud Backup contains the following information:

- Alarm states
- Recent log messages
- Hardware and software diagnostic outputs
- Performance metrics
- Sanitized configuration information

StorageGRID

Each AutoSupport message for StorageGRID contains the following information:

- StorageGRID software version
- Operating system version
- System-level and location-level attribute information
- All alarms raised in the last 7 days
- Current status of all grid tasks, including historical data
- Events information as listed on the **SSM** > **Events** > **Overview** page
- Admin Node database usage
- Number of lost or missing objects
- Grid configuration settings
- NMS entities
- Active ILM policy
- Provisioned grid specification file

OnCommand Insight

AutoSupport messages for OnCommand Insight contain the following information:

- Basic information about the OnCommand Insight instance
- The licensed modules and protocols in the OnCommand Insight instance
- The arrays that the OnCommand Insight instance is monitoring (serial number, manufacturer, model number, capacity, and so on)
- The virtual disks that the OnCommand Insight is monitoring (data source, location, object identifier, capacity, and so on)

Active IQ Unified Manager

Each AutoSupport message for Active IQ Unified Manager contains the following information:

- Basic configuration information about the systems managed by a Unified Manager instance
- Log files
- Diagnostic contents from command outputs

SANtricity Web Services (REST API)

AutoSupport messages for SANtricity Web Services contain the following information:

- A configuration file of systems being managing
- Logs for the application
- Application-specific counters
- A web server configuration file

Active IQ OneCollect

AutoSupport messages for OneCollect contain the following information:

- Configuration information from the hosts, hypervisors, switches, and storage arrays from which a collection was run

Transfer of telemetry data

By default, most NetApp products use the HTTPS protocol to send telemetry data to NetApp technical support. HTTPS connections to NetApp are encrypted and authenticated using TLS 1.2 or later, except for old versions of ONTAP that are no longer supported. Older versions of TLS, as well as HTTP, will be rejected starting in March 2023. NetApp strongly recommends using HTTPS because it is more secure, it enables NetApp to provide better support, and it provides better analytics through Active IQ. However, SMTP is also offered for products that cannot support HTTPS.

Table 1) Supported transport protocols for AutoSupport.

Product	Default protocol	Additional protocols supported
Cloud Backup	HTTPS	None
E-Series	HTTPS	SMTP
OnCommand Insight	HTTPS	SMTP and FTP
Active IQ Unified Manager	HTTPS	None
ONTAP	HTTPS	SMTP
SANtricity Web Services	HTTPS	SMTP
SolidFire and NetApp HCI	HTTPS	None
StorageGRID	SMTP	None
Active IQ OneCollect	HTTPS	None

Note: AutoSupport messages are generally used by NetApp Support. Although you can configure AutoSupport to notify you of critical events on ONTAP systems, you should use event notifications from the Event Management System (EMS) so that you are notified of issues that require attention.

Figure 2 illustrates how AutoSupport transfers data from an ONTAP system to NetApp.

Figure 2) How AutoSupport data is transferred.

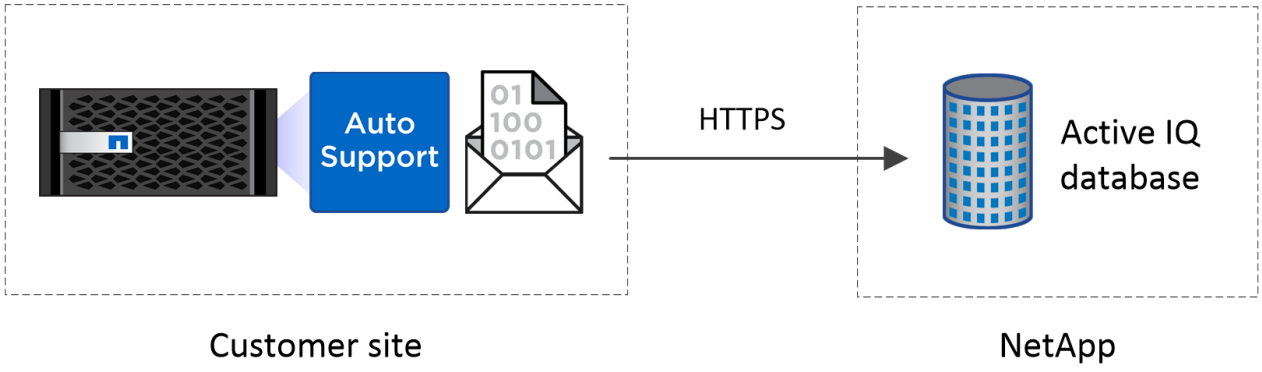
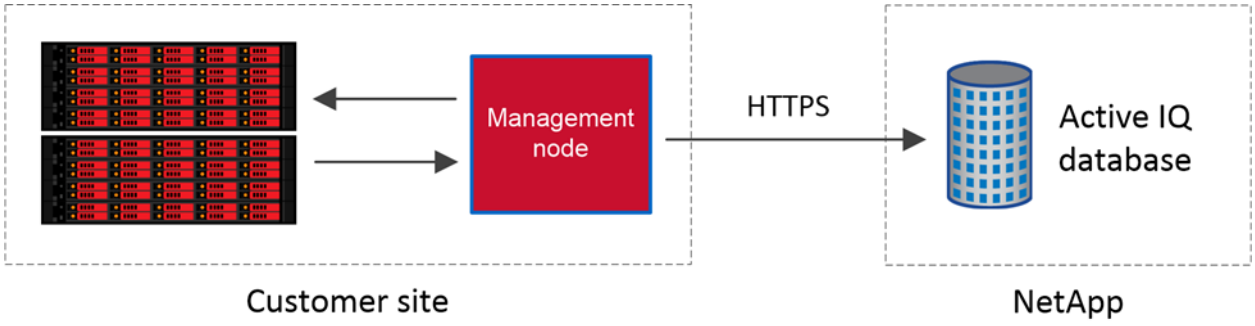


Figure 3 illustrates how SolidFire and NetApp HCI transfer telemetry data to NetApp.

Figure 3) How SolidFire and NetApp HCI telemetry data is transferred.



On demand delivery of AutoSupport messages

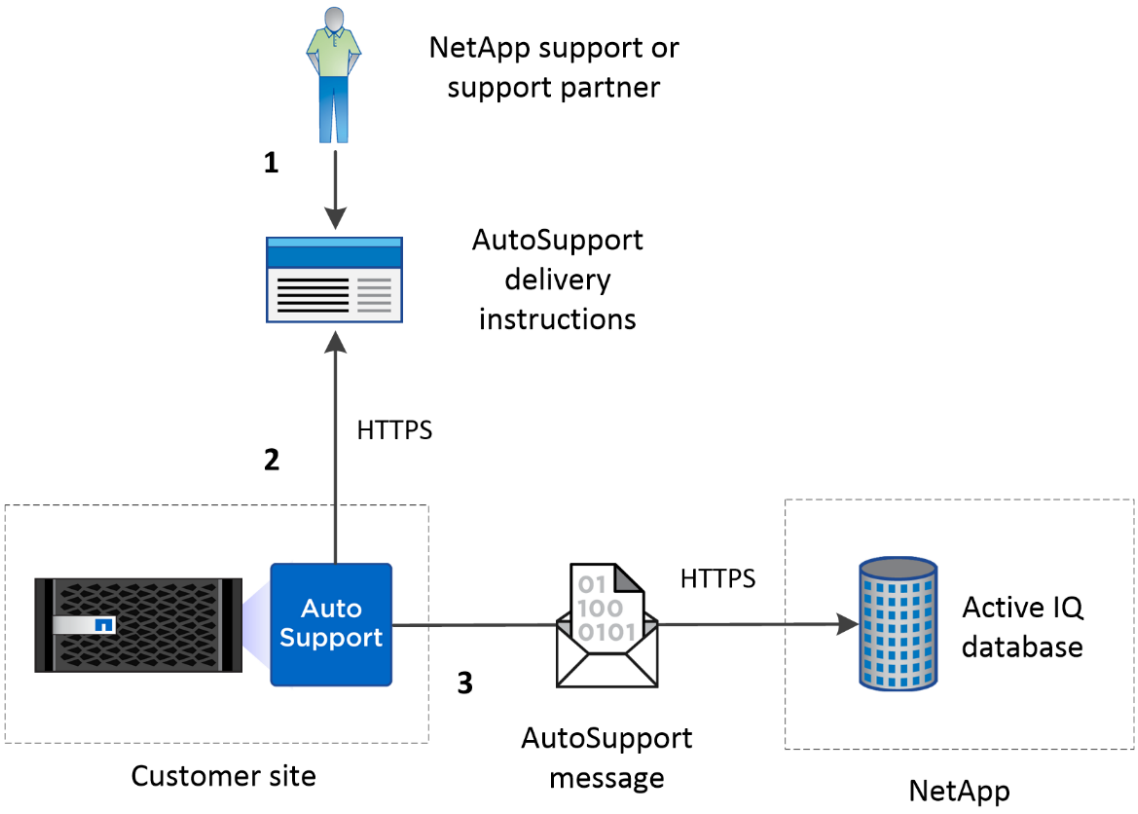
AutoSupport On Demand enables NetApp to request AutoSupport messages on demand to troubleshoot cases without the need for customer intervention. This feature is supported with ONTAP and E-Series systems that use HTTPS to deliver messages to NetApp.

AutoSupport On Demand is a delivery service through which the storage system polls support.netapp.com and looks in an inbox for instructions. The service works as follows:

1. As needed, NetApp Support or support partners create delivery instructions for particular systems. These instructions enable a limited set of predefined AutoSupport delivery instructions:
    a. Requests for new AutoSupport data to determine the current system state.
    b. Requests for more in-depth AutoSupport data to resolve complex cases (diagnostic AutoSupport messages, core files, and performance archives).
    c. Memory buffers containing customer data are excluded from the core files in AutoSupport messages.
    d. Notifications are sent of available software upgrades, including disk firmware, shelf firmware, management controller (SP or BMC) firmware, and time zone files (supported in ONTAP 9.10.1 and later).
2. Systems periodically poll the AutoSupport On Demand service to obtain delivery instructions through encrypted HTTPS. All transmissions are initiated from the system, not from the AutoSupport server.
3. If a system obtains delivery instructions, AutoSupport invokes a new message and sends it to NetApp using HTTPS.

Figure 4 illustrates the AutoSupport On Demand workflow. The numbers in the image correspond to the steps above.

Figure 4) AutoSupport On Demand workflow.



AutoSupport On Demand is restricted to users who have valid NetApp Support site credentials and appropriate business roles (technical support engineers, support account managers, and support partners authorized to work on a given storage system).

AutoSupport On Demand usage is transparent:

- Customers can review and execute all predefined delivery instructions by using the ONTAP CLI.
- Customers and partners receive a copy of the AutoSupport message if you configured the system to send AutoSupport messages to your internal support organization and to partners.
- On Demand usage is tracked and displayed:
  - On Demand requests are logged in daily management log AutoSupport messages.
  - Resulting AutoSupport messages contain On Demand in the title and can be viewed through Active IQ.

Access and retention of telemetry data

Where the data resides

AutoSupport data is sent to one or more NetApp data centers in the United States. The data is not archived at an offsite location. Some data processed or derived from AutoSupport is stored in Amazon Web Services.

Data handling and encryption

For all data, AutoSupport messages are scanned upon receipt, and personally identifiable information and all customer identifiable information (CII) is encrypted as the messages are saved, except any CII that a customer entered in a named item (for example a volume name). NetApp recommends against naming things using CII or any other private information. Subsequently, only customers, customers' partners, and NetApp individuals whose job requires access are allowed to request decryption of that information.

When data arrives, data from certain governmental entities is separated from the rest of the data and is stored separately from all other data. This data has additional security controls placed on it, including that only verified NetApp employees and contractors who are U.S. citizens can use it during support issues. See Who can access the data for details.

The rest of the data is then separated into potentially personally identifiable information and potentially CII. This data is then stored in an encrypted database, which has strong security controls and auditing placed on it. Only customers and specially authorized people can decrypt that data when needed, and then those decryptions are logged and audited. The rest of the non-identifying data is not encrypted at rest or in transit after receipt.

Data access

Who can access the data Access to NetApp telemetry data is secured by a data access layer that requires positive identification of each user requesting access. All requests for data must include a verifiable reference to the individual who is requesting access. The data access layer is implemented using the following:

- Security Assertion Markup Language (SAML) for authentication, which requires individual registration with NetApp
- Authenticated user attributes (employing company, geographic location, citizenship, and so on)
- Role-based access controls (job function)

The following people can access the data based on their job role:

- **NetApp customer success and account teams.** NetApp employees and approved agents can access capacity, performance, and configuration data for customer support and sales uses, to allow them to better help their customer.

  Note: For systems that have the SupportEdge Secure for Government support level or that are owned by the United States government, NetApp access to telemetry data is restricted to employees and contractors who are United States citizens working in the United States.

- **Customers.** Any user from a company that has registered with the NetApp Support site can access data for all their installed systems that have AutoSupport or SolidFire Active IQ enabled and have active support contracts.

  Users are only able to view systems that are registered with their company. Active IQ uses the product registration and support registration credentials from the NetApp Support site to control access.

- **Partners.** Partners who have registered with the NetApp Support site can access data for all systems that they sold or currently support for those systems that have AutoSupport enabled and that have active support contracts.

Security testing

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

Data retention period

NetApp retains AutoSupport telemetry messages for 7 years. While a support contract is in place, NetApp retains SolidFire telemetry data for up to 5 years. Customers can request that their data be deleted at any time by opening a support case.

Certifications

NetApp is ISO 27001:2013 certified. The scope of this certification includes AutoSupport. NetApp does not provide the audit reports to customers.

Where to find additional information

To learn more about the information described in this document, refer to the following resources. Some of these resources require a NetApp Support Site account, which is provided to NetApp customers.

- Active IQ
  https://mysupport.netapp.com/myautosupport/home.html
- NetApp Cloud Backup Resources
  https://mysupport.netapp.com/altavault/resources
- E-Series Documentation Center
  https://mysupport.netapp.com/eseries
- OnCommand Insight Resources
  https://mysupport.netapp.com/oncommandinsight/resources
- Active IQ Unified Manager Resources
  https://mysupport.netapp.com/unifiedmanager/resources
- ONTAP Resources
  https://mysupport.netapp.com/ontap/resources
- SolidFire Resources
  https://mysupport.netapp.com/solidfire/resources
- StorageGRID Resources
  https://mysupport.netapp.com/site/products/all/details/storagegrid/guideme-tab

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

Trademark information