



## **Support center**

SANtricity 11.6

NetApp  
February 12, 2024

This PDF was generated from <https://docs.netapp.com/us-en/e-series-santricity-116/sm-support/autosupport-feature-overview.html> on February 12, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

- Support center ..... 1
  - Concepts ..... 1
  - How tos ..... 2
  - FAQs ..... 27

# Support center

## Concepts

### AutoSupport feature overview

The AutoSupport feature monitors the health of a storage array and sends automatic dispatches to technical support.

Technical support uses the AutoSupport data reactively to speed the diagnosis and resolution of customer issues and proactively to detect and avoid potential issues.

AutoSupport data includes information about a storage array's configuration, status, performance, and system events. The AutoSupport data does not contain any user data. Dispatches can be sent immediately or on a schedule (daily and weekly).

### Key benefits

Some key benefits of the AutoSupport feature include:

- Expedited case resolution times
- Sophisticated monitoring for faster incident management
- Automated reporting according to a schedule, as well as automated reporting about critical events
- Automated hardware replacement requests for selected components such as drives
- Nonintrusive alerting to notify you of a problem and provide information for technical support to take corrective action
- AutoSupport analysis tools that monitor dispatches for known configuration issues

### Individual AutoSupport features

The AutoSupport feature is made up of three individual features that you enable separately.

- **Basic AutoSupport** — Allows your storage array to automatically collect and send data to technical support.
- **AutoSupport OnDemand** — Allows technical support to request retransmission of a previous AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending retransmission requests and responds accordingly.
- **Remote Diagnostics** — Allows technical support to request a new, up-to-date AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending new requests and responds accordingly.

### Difference between AutoSupport and Collect Support Data

Two methods of collecting support data exist in the storage array:

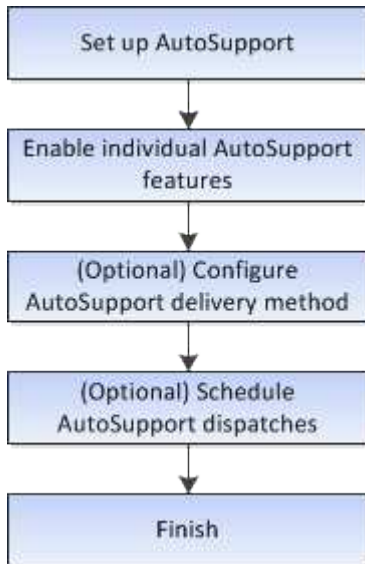
- The AutoSupport feature — Data is automatically collected.

- The Collect Support Data option — Data must be collected and sent manually.

The AutoSupport feature is easier to use because data is collected and sent automatically. AutoSupport data can be used proactively to prevent problems before they occur. The AutoSupport feature speeds troubleshooting because technical support already has access to the data. For these reasons, the AutoSupport feature is the preferred data collection method to use.

## Workflow for the AutoSupport feature

In SANtricity System Manager, you configure the AutoSupport feature by following these steps.



## How tos

### View storage array information

#### View storage array profile

The storage array profile provides a description of all of the components and properties of the storage array.

#### About this task

You can use the storage array profile as an aid during recovery or as an overview of the current configuration of the storage array. You might want to save a copy of the storage array profile on the management client and keep a hard copy of the storage array profile with the storage array. Create a new copy of the storage array profile if your configuration changes.

#### Steps

1. Select **Support > Support Center > Support Resources** tab.
2. Scroll down to **Launch detailed storage array information**, and then select **Storage Array Profile**.

The report appears on your screen.

## Field details

Section	Description
Storage Array	<p>Shows all of the options that you can configure and the system static options for your storage array. These options include the number of controllers, drive shelves, drives, disk pools, volume groups, volumes, and hot spare drives; the maximum number of drive shelves, drives, Solid State Disks (SSDs), and volumes allowed; the number of snapshot groups, snapshot images, snapshot volumes and consistency groups; information about features; information about firmware versions; information about the chassis serial number; AutoSupport status and AutoSupport schedule information; the settings for automatic support data collection and scheduled support data collection; the storage array World-Wide Identifier (WWID); and the media scan and cache settings.</p>
Storage	<p>Shows a list of all of the storage devices in the storage array. Depending on your storage array configuration, the Storage section might show these sub-sections.</p> <ul style="list-style-type: none"><li>• <b>Disk Pools</b> — Shows a list of all of the disk pools in the storage array.</li><li>• <b>Volume Groups</b> — Shows a list of all of the volume groups in the storage array. Volumes and free capacity are listed in the order in which they were created.</li><li>• <b>Volumes</b> — Shows a list of all of the volumes in the storage array. The information listed includes the volume name, the volume status, the capacity, the RAID level, the volume group or disk pool, the drive type, and additional details.</li><li>• <b>Missing Volumes</b> — Shows a list of all of the volumes in the storage array that currently have a missing status. The information listed includes the World Wide Identifier (WWID) for each missing volume.</li></ul>

Section	Description
Copy Services	<p>Shows a list of all the copy services that are used for the storage array. Depending on your storage array configuration, the Copy Services section might show these sub-sections:</p> <ul style="list-style-type: none"> <li>• <b>Volume Copies</b> — Shows a list of all copy pairs in the storage array. The information listed includes the number of copies, the copy pair names, the status, the start timestamp, and additional details.</li> <li>• <b>Snapshot Groups</b> — Shows a list of all snapshot groups in the storage array.</li> <li>• <b>Snapshot Images</b> — Shows a list of all snapshots in the storage array.</li> <li>• <b>Snapshot Volumes</b> — Shows a list of all snapshot volumes in the storage array.</li> <li>• <b>Consistency Groups</b> — Shows a list of all consistency groups in the storage array.</li> <li>• <b>Member Volumes</b> — Shows a list of all consistency group member volumes in the storage array.</li> <li>• <b>Mirror Groups</b> — Shows a list of all mirrored volumes.</li> <li>• <b>Reserved Capacity</b> — Shows a list of all reserved capacity volumes in the storage array.</li> </ul>
Host Assignments	<p>Shows a list of host assignments in the storage array. The information listed includes the volume name, logical unit number (LUN), controller ID, host name or host cluster name, and volume status. Additional information listed includes topology definitions and host type definitions.</p>

Section	Description
Hardware	<p>Shows a list of all of the hardware in the storage array. Depending on your storage array configuration, the Hardware section might show these sub-sections.</p> <ul style="list-style-type: none"> <li>• <b>Controllers</b> — Shows a list of all of the controllers in the storage array and includes the controller location, status, and configuration. In addition, it includes drive channel information, host channel information, and Ethernet port information.</li> <li>• <b>Drives</b> — Shows a list of all of the drives in the storage array. The drives are listed in shelf ID, drawer ID, slot ID order. The information listed includes the shelf ID, the drawer ID, the slot ID, the status, the raw capacity, the media type, the interface type, the current data rate, the product ID, and the firmware version for each drive. The Drive section also includes drive channel information, hot spare coverage information, and wear life information (only for SSD drives). The wear life information includes the percent endurance used, which is the amount of data written to the SSD drives to date, divided by the total theoretical write limit for the drives.</li> <li>• <b>Drive Channels</b> — Shows information for all of the drive channels in the storage array. The information listed includes the channel status, the link status (if applicable), drive counts, and cumulative error counts.</li> <li>• <b>Shelves</b> — Shows information for all of the shelves in the storage array. The information listed includes drive types, and status information for each component of the shelf. Shelf components might include battery packs, Small Form-factor Pluggable (SFP) transceivers, power-fan canisters, or input/output module (IOM) canisters.</li> </ul> <p>The Hardware section also shows the security key identifier if a security key is used by the storage array.</p>
Features	<p>Shows a list of the feature packs installed and maximum allowed number of snapshot groups, snapshots (legacy), and volumes per host or host cluster. The information in the Features section also includes Drive Security; that is, whether the storage array is security enabled or security disabled.</p>

3. To search the storage array profile, type a search term in the **Find** text box, and then click **Find**.

All matching terms are highlighted. To scroll through all the results one at a time, continue to click **Find**.

4. To save the storage array profile, click **Save**.

The file is saved in the Downloads folder for your browser with the name `storage-array-profile.txt`.

## View software and firmware inventory

The software and firmware inventory lists the firmware versions for each component in

your storage array.

### About this task

A storage array is made up of many components, which might include controllers, drives, drawers, and input/output modules (IOMs). Each of these components contains firmware. Some versions of firmware depend on other versions of firmware. To capture information about all of the firmware versions in your storage array, view the software and firmware inventory. Technical support can analyze the software and firmware inventory to detect any firmware mismatches.

### Steps

1. Select **Support > Support Center > Support Resources** tab.
2. Scroll down to **Launch detailed storage array information**, and then select **Software and Firmware Inventory**.

The software and firmware inventory report appears on the screen.

3. To save the software and firmware inventory, click **Save**.

The file is saved in the Downloads folder for your browser with the filename `firmware-inventory.txt`.

4. Follow the instructions provided by technical support to send the file to them.

## Collect diagnostic data

### Collect support data manually

You can gather various types of inventory, status, and performance data about your storage array in a single file. Technical support can use the file for troubleshooting and further analysis.

### About this task



If the AutoSupport feature is enabled, you can also collect this data by going to the **AutoSupport** tab and selecting **Send AutoSupport Dispatch**.

You can run only one collection operation at a time. If you try to start another operation, you receive an error message.



Perform this operation only when instructed to do so by technical support.

### Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **Collect Support Data**.
3. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name `support-data.7z`. If your shelf contains drawers, the diagnostic data for that shelf is archived in a separate zipped file named `tray-component-state-capture.7z`.



4. Follow the instructions provided by technical support to send the file to them.

## Retrieve recovery support files

Technical support can use recovery support files to troubleshoot issues. System Manager automatically saves these files.

### Before you begin

Technical support has requested that you send them additional files for troubleshooting.

### About this task

Recovery support files include these types of files:

- Support data files
- AutoSupport history
- AutoSupport log
- SAS/RLS diagnostics files
- Recovery profile data
- Database capture files

### Steps

1. Select **Support** › **Support Center** › **Diagnostics** tab.
2. Select **Retrieve Recovery Support Files**.

A dialog box lists all the recovery support files that your storage array has collected. To find particular files, you can sort any of the columns or type characters in the **Filter** box.

3. Select a file, and then click **Download**.

The file is saved in the Downloads folder for your browser.

4. If you need to save additional files, repeat the previous step.
5. Click **Close**.
6. Follow the instructions provided by technical support to send the file to them.

## Retrieve trace buffers

You can retrieve the trace buffers from the controllers and send the file to technical support for analysis.

### About this task

The firmware uses the trace buffers to record processing, especially exception conditions, that might be useful for debugging. You can retrieve trace buffers without interrupting the operation of the storage array and with minimal effect on performance.



Perform this operation only when instructed to do so by technical support.

### Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **Retrieve Trace Buffers**.
3. Select the check box next to each controller for which you want to retrieve trace buffers.

You can select one or both controllers. If the controller status message to the right of a check box is Failed or Disabled, the check box is disabled.

4. Click **Yes**.

The file is saved in the Downloads folder for your browser with the filename `trace-buffers.7z`.

5. Follow the instructions provided by technical support to send the file to them.

## Collect drive data

You can collect log data from all drives in your storage array and send the file to technical support for analysis.

### About this task

Log data consists of statistical information that is maintained by each of the drives in your storage array. Technical support can use this information to analyze the performance of your drives and for troubleshooting problems that might exist.



Perform this operation only when instructed to do so by technical support.

### Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **Collect Drive Data**.

A dialog box appears listing all drives in your storage array.

3. In the first column of the table, you can either select individual drives for which you want to collect data (click the check box next to each drive) or select all drives (select the check box in the table header).

To find particular drives, you can sort any of the columns or type characters in the **Filter** box.

4. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name `drive-data.7z`.

5. Follow the instructions provided by technical support to send the file to them.

## Collect I/O path statistics

You can save the I/O path statistics file and send it to technical support for analysis.

### About this task

Technical support uses the I/O path statistics to help diagnose performance issues. Application performance issues can be caused by memory utilization, CPU utilization, network latency, I/O latency, or other issues. The I/O path statistics are collected automatically during support data collection or you can collect them manually. In addition, if you have AutoSupport turned on, the I/O path statistics are automatically collected and sent to

technical support.

The counters for the I/O path statistics are reset after you confirm that you want to collect the I/O path statistics. The counters are reset even if you subsequently cancel the operation. The counters are also reset when the controller resets (reboots).



Perform this operation only when instructed to do so by technical support.

### Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **Collect I/O Path Statistics**.
3. Confirm that you want to perform the operation by typing `collect`, and then click **Collect**.

The file is saved in the Downloads folder for your browser with the filename `io-path-statistics.7z`.

4. Follow the instructions provided by technical support to send the file to them.

### Retrieve health image

You can review a health image for the controller. A health image is a raw data dump of the controller's processor memory that technical support can use to diagnose a problem with a controller.

#### About this task

The firmware automatically generates a health image when it detects certain errors. After a health image is generated, the controller that had the error reboots and an event is logged in the event log.

If you have AutoSupport turned on, the health image is automatically sent to technical support. If you do not have AutoSupport turned on, you need to contact technical support for instructions on retrieving the health image and sending it to them for analysis.



Perform this operation only when instructed to do so by technical support.

### Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **Retrieve Health Image**.

You can look at the details section to see the size of the health image before downloading the file.

3. Click **Collect**.

The file is saved in the Downloads folder for your browser with the name `health-image.7z`.

4. Follow the instructions provided by technical support to send the file to them.

### Take recovery action on storage array status

#### View unreadable sectors log

You can save the unreadable sectors log and send the file to technical support for

analysis.

### About this task

The unreadable sectors log contains detailed records of unreadable sectors caused by drives reporting unrecoverable media errors. Unreadable sectors are detected during normal I/O and during modification operations, such as reconstructions. When unreadable sectors are detected on a storage array, a Needs Attention alert appears for the storage array. The Recovery Guru distinguishes which unreadable sector condition needs attention. Any data contained in an unreadable sector cannot be recovered and should be considered lost.

The unreadable sectors log can store up to 1,000 unreadable sectors. When the unreadable sectors log reaches 1,000 entries, the following conditions apply:

- If new unreadable sectors are detected during reconstruction, the reconstruction fails, and no entry is logged.
- For new unreadable sectors detected during I/O, the I/O fails, and no entry is logged.



These actions include RAID 5 writes and RAID 6 writes that would have succeeded before the overflow.



**Possible loss of data** — Recovery from unreadable sectors is a complicated procedure that can involve several different methods. Perform this operation only when instructed to do so by technical support.

### Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **View/Clear Unreadable Sectors**.
3. To save the unreadable sectors log:
  - a. In the first column of the table, you can either select individual volumes for which you want to save the unreadable sectors log (click the check box next to each volume) or select all volumes (select the check box in the table header).

To find particular volumes, you can sort any of the columns or type characters in the **Filter** box.

- b. Click **Save**.

The file is saved in the Downloads folder for your browser with the name `unreadable-sectors.txt`.

4. If technical support instructs you to clear the unreadable sectors log, perform the following steps:
  - a. In the first column of the table, you can either select individual volumes for which you want to clear the unreadable sectors log (click the check box next to each volume) or select all volumes (select the check box in the table header).
  - b. Click **Clear**, and confirm that you want to perform the operation.

### Re-enable drive ports

You can indicate to the controller that corrective action has been taken to recover from a mis-wire condition.

## Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **Re-enable Drive Ports**, and confirm that you want to perform the operation.

This option appears only when the storage array has disabled drive ports.

The controller re-enables any SAS ports that were disabled when a mis-wire was detected.

## Clear recovery mode

After restoring a storage array configuration, use the Clear Recovery Mode operation to resume I/O on the storage array and return it to normal operations.

### Before you begin

- If you want to return the storage array to a previous configuration, you must restore the configuration from the backup before clearing recovery mode.
- You must perform validation checks or check with technical support to make sure that the restore was successful. After determining that the restore was successful, recovery mode can be cleared.

### About this task

The storage array contains a configuration database that includes a record of its logical configuration (pools, volume groups, volumes, and so on). If you intentionally clear the storage array configuration or if the configuration database gets corrupted, the storage array enters recovery mode. Recovery mode stops I/O and freezes the configuration database, which gives you time to do one of the following:

- Restore the configuration from the automatic backup that is stored in the controller's flash devices. You must contact technical support to do this.
- Restore the configuration from a previous Save Configuration Database operation. Save Configuration Database operations are performed through the command line interface (CLI).
- Reconfigure the storage array from scratch.

After the storage array configuration has been restored or redefined and you have verified that all is well, you must manually clear recovery mode.



You cannot cancel the Clear Recovery Mode operation after it starts. Clearing recovery mode can take a long time. Perform this operation only when instructed to do so by technical support.

## Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **Clear Recovery Mode**, and confirm that you want to perform this operation.

This option appears only if the storage array is in recovery mode.

## Manage iSCSI connections

### View iSCSI statistics packages

You can view data about the iSCSI connections to your storage array.

## About this task

System Manager shows these types of iSCSI statistics. All statistics are read-only and cannot be set.

- **Ethernet MAC statistics** — Provides statistics for the media access control (MAC). MAC also provides an addressing mechanism called the physical address or the MAC address. The MAC address is a unique address that is assigned to each network adapter. The MAC address helps deliver data packets to a destination within the subnetwork.
- **Ethernet TCP/IP statistics** — Provides statistics for the TCP/IP, which is the Transmission Control Protocol (TCP) and Internet Protocol (IP) for the iSCSI device. With TCP, applications on networked hosts can create connections to one another, over which they can exchange data in packets. The IP is a data-oriented protocol that communicates data across a packet-switched inter-network. The IPv4 statistics and the IPv6 statistics are shown separately.
- **Local Target/Initiator (Protocol) statistics** — Shows statistics for the iSCSI target, which provides block level access to its storage media, and shows the iSCSI statistics for the storage array when used as an initiator in asynchronous mirroring operations.
- **DCBX Operational States statistics** — Displays the operational states of the various Data Center Bridging Exchange (DCBX) features.
- **LLDP TLV statistics** — Displays the Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) statistics.
- **DCBX TLV statistics** — Displays the information that identifies the storage array host ports in a Data Center Bridging (DCB) environment. This information is shared with network peers for identification and capability purposes.

You can view each of these statistics as raw statistics or as baseline statistics. Raw statistics are all of the statistics that have been gathered since the controllers were started. Baseline statistics are point-in-time statistics that have been gathered since you set the baseline time.

## Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **View iSCSI Statistics Packages**.
3. Click a tab to view the different sets of statistics.
4. To set the baseline, click **Set new baseline**.

Setting the baseline sets a new starting point for the collection of the statistics. The same baseline is used for all iSCSI statistics.

## View the different types of iSCSI statistics

You can review different sets of statistics as either raw or baseline statistics: Ethernet MAC statistics, Ethernet TCP/IP statistics, Target (protocol) statistics, Local initiator (protocol) statistics, DCBX operational state statistics, LLDP TLV statistics, and DCBX TLV statistics.

### MAC transmit and MAC receive statistics

When you select Ethernet MAC statistics, these MAC transmit statistics appear. You can view each of these statistics as raw statistics or as baseline statistics.

<b>Statistic</b>	<b>Definition</b>
F	Frame count
B	Byte count
MF	Multicast frame count
BF	Broadcast frame count
PF	Pause frame count
CF	Control frame count
FDF	Frame deferral count
FED	Frame excess deferral count
FLC	Frame late collisions count
FA	Frame abort count
FSC	Frame single collision count
FMC	Frame multiple collisions count
FC	Frame collision count
FDR	Frame dropped count
JF	Jumbo frame count

When you select Ethernet MAC statistics, these MAC receive statistics appear.

<b>Statistic</b>	<b>Definition</b>
F	Frame count
B	Byte count
MF	Multicast frame count
BF	Broadcast frame count
PF	Pause frame count

Statistic	Definition
CF	Control frame count
FLE	Frame length error count
FD	Frame dropped count
FCRCE	Frame CRC error count
FEE	Frame encoding error count
LFE	Large frame error count
SFE	Small frame error count
J	Jabber count
UCC	Unknown control frame count
CSE	Carrier sense error count

#### Ethernet TCP/IP statistics

When you select Ethernet TCP/IP statistics, the TCP statistics in this table appear. You can view each of these statistics as raw statistics or as baseline statistics.

Statistic	Definition
TxS	Transmitted segment count
TxB	Transmitted byte count
RTxTE	Retransmit timer expired count
TxDACK	Transmit delayed ACK count
TxACK	Transmit ACK count
RxS	Received segment count
RxB	Received byte count
RxDACK	Received duplicate ACK count
RxACK	Received ACK count



Statistic	Definition
RxSEC	Received segment error count
RxSOOC	Received segment out-of-order count
RxWP	Received window probe count
RxWU	Received window update count

When you select Ethernet TCP/IP statistics, the IP statistics in this table appear.

Statistic	Definition
TxP	Transmitted packet count
TxB	Transmitted byte count
TxF	Transmitted fragment count
RxP	Packets received count. Select <b>Show IPv4</b> to show the IPv4 packets received count. Select <b>Show IPv6</b> to show the IPv6 packets received count.
RxB	Received byte count
RxF	Received fragment count
RxPE	Received packet error count
DR	Datagram reassembly count
DRE-OLFC	Datagram reassembly error, overlapped fragment count
DRE-OOFC	Datagram reassembly error, out-of-order fragment count
DRE-TOC	Datagram reassembly error, time-out count

#### iSCSI target statistics and local initiator statistics

When you select Target (protocol) statistics or Local initiator (protocol) statistics, the following statistics are shown. You can view each of these statistics as raw statistics or as baseline statistics.

Statistic	Definition
SL	Successful iSCSI login count
UL	Unsuccessful iSCSI login count
SA	Successful iSCSI authentication count (when authentication is enabled)
UA	Unsuccessful iSCSI authentication count (when authentication is enabled)
PDU	Correct iSCSI PDUs processed count
HDE	iSCSI PDUs with header digest errors count
DDE	iSCSI PDUs with data digest errors count
PE	PDUs with iSCSI protocol errors count
UST	Unexpected iSCSI session terminations count
UCT	Unexpected iSCSI connection termination count

#### DCBX operational state statistics

When you select Data Center Bridging Exchange (DCBX) Operational State Statistics, these statistics appear.

Statistic	Definition
iSCSI Host Port	Indicates the location of the detected host port in Controller #, Port # format.
Priority Group	Indicates the operational state of the Priority Group (PG) application. The state is either Enabled or Disabled.
Priority-based Flow Control	Indicates the operational state of the Priority-based Flow Control (PFC) feature. The state is either Enabled or Disabled.
iSCSI Feature	Indicates the operational state of the Internet Small Computer System Interface (iSCSI) application. The state is either Enabled or Disabled.
FCoE Bandwidth	Indicates the state of the Fibre Channel over Ethernet (FCoE) Bandwidth. The state is either True or False.

Statistic	Definition
No FCoE/FIP Map Mismatch	Indicates whether a map mismatch exists between FCoE and FCoE Initialization Protocol (FIP). The value is either True or False.

You can find additional DCBX operational state statistics in the state capture file.

#### LLDP TLV statistics

When you select Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) Statistics, these statistics appear. Two sets of statistics appear: one for the local device and one for the remote device. The local device refers to the controller. The remote device refers to the peer device that the controller is attached to, typically a switch.

Statistic	Definition
iSCSI Host Port	Indicates the location of the detected host port in Controller #, Port # format.
Chassis ID	Indicates the chassis ID.
Chassis ID Subtype	Indicates the chassis ID subtype.
Port ID	Indicates the port ID.
Port ID Subtype	Indicates the port ID subtype.
Time to Live	Indicates the number of seconds that the recipient LLDP agent considers the information to be valid.

You can find additional LLDP TLV statistics in the state capture file.

#### DCBX TLV statistics

When you select Data Center Bridging Exchange (DCBX) Type Length Value (TLV) Statistics, these statistics appear:

- **Local statistics** — The DCBX parameters configured on the controller at the factory.
- **Operational statistics** — The DCBX parameters that result from DCBX negotiations.
- **Remote statistics** — The DCBX parameters from the peer device that the controller is connected to, typically a switch.

Statistic	Definition
iSCSI Host Port	Indicates the location of the detected host port in Controller #, Port # format.

Statistic	Definition
Flow Control Mode	The Flow Control Mode of the entire port. Valid values are Disabled, Standard, Per Priority, or Indeterminate.
Protocol	The communication protocol. Valid values are FCoE, FIP, iSCSI, or UNKNOWN.
Priority	Integer value indicating the priority number of the communication.
Priority Group	Integer value representing the priority group to which the protocol has been assigned.
Priority Group % Bandwidth	Percentage value indicating the amount of bandwidth allocated to the priority group.
DCBX PFC Status	Priority-based Flow Control (PFC) status of the specific port. The value is either enabled or disabled.

You can find additional DCBX TLV statistics in the state capture file.

### View iSCSI sessions

You can view detailed information about the iSCSI connections to your storage array. iSCSI sessions can occur with hosts or remote storage arrays in an asynchronous mirror relationship.

#### Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **View/End iSCSI Sessions**.

A list of the current iSCSI sessions appears.

3. To see additional information about a specific iSCSI session, select a session, and then click **View Details**.

## Field Details

Item	Description
Session Identifier (SSID)	A hexadecimal string that identifies a session between an iSCSI initiator and an iSCSI target. The SSID is composed of the ISID and the TPGT.
Initiator Session ID (ISID)	The initiator part of the session identifier. The initiator specifies the ISID during login.
Target Portal Group	The iSCSI target.
Target Portal Group Tag (TPGT)	The target part of the session identifier. A 16-bit numerical identifier for an iSCSI target portal group.
Initiator iSCSI name	The worldwide unique name of the initiator.
Initiator iSCSI label	The user label set in System Manager.
Initiator iSCSI alias	A name that also can be associated with an iSCSI node. The alias allows an organization to associate a user-friendly string with the iSCSI name. However, the alias is not a substitute for the iSCSI name. The initiator iSCSI alias only can be set at the host, not in System Manager
Host	A server that sends input and output to the storage array.
Connection ID (CID)	A unique name for a connection within the session between the initiator and the target. The initiator generates this ID and presents it to the target during login requests. The connection ID is also presented during logouts that close connections.
Ethernet port identifier	The controller port associated with the connection.
Initiator IP address	The IP address of the initiator.
Negotiated login parameters	The parameters that are transacted during the login of the iSCSI session.
Authentication method	The technique to authenticate users who want access to the iSCSI network. Valid values are <b>CHAP</b> and <b>None</b> .
Header digest method	The technique to show possible header values for the iSCSI session. HeaderDigest and DataDigest can be either <b>None</b> or <b>CRC32C</b> . The default value for both is <b>None</b> .
Data digest method	The technique to show possible data values for the iSCSI session. HeaderDigest and DataDigest can be either <b>None</b> or <b>CRC32C</b> . The default value for both is <b>None</b> .

Item	Description
Maximum connections	The greatest number of connections allowed for the iSCSI session. The maximum number of connections can be 1 through 4. The default value is <b>1</b> .
Target alias	The label associated with the target.
Initiator alias	The label associated with the initiator.
Target IP address	The IP address of the target for the iSCSI session. DNS names are not supported.
Initial R2T	The initial ready to transfer status. The status can be either <b>Yes</b> or <b>No</b> .
Maximum burst length	The maximum SCSI payload in bytes for this iSCSI session. The maximum burst length can be from 512 to 262,144 (256 KB). The default value is <b>262,144 (256 KB)</b> .
First burst length	The SCSI payload in bytes for unsolicited data for this iSCSI session. The first burst length can be from 512 to 131,072 (128 KB). The default value is <b>65,536 (64 KB)</b> .
Default time to wait	The minimum number of seconds to wait before you attempt to make a connection after a connection termination or a connection reset. The default time to wait value can be from 0 to 3600. The default is <b>2</b> .
Default time to retain	The maximum number of seconds that connection is still possible following a connection termination or a connection reset. The default time to retain can be from 0 to 3600. The default value is <b>20</b> .
Maximum outstanding R2T	The maximum number of "ready to transfers" outstanding for this iSCSI session. The maximum outstanding ready to transfer value can be from 1 to 16. The default is <b>1</b> .
Error recovery level	The level of error recovery for this iSCSI session. The error recovery level value is always set to <b>0</b> .
Maximum receive data segment length	The maximum amount of data that either the initiator or the target can receive in any iSCSI payload data unit (PDU).
Target name	The official name of the target (not the alias). The target name with the <i>iqn</i> format.
Initiator name	The official name of the initiator (not the alias). The initiator name that uses either the <i>iqn</i> or <i>eui</i> format.

4. To save the report to a file, click **Save**.

The file is saved in the Downloads folder for your browser with the filename `iscsi-session-connections.txt`.

## End iSCSI session

You can end an iSCSI session that is no longer needed. iSCSI sessions can occur with hosts or remote storage arrays in an asynchronous mirror relationship.

### About this task

You might want to end an iSCSI session for these reasons:

- **Unauthorized access** — If an iSCSI initiator is logged on and should not have access, you can end the iSCSI session to force the iSCSI initiator off the storage array. The iSCSI initiator could have logged on because the None authentication method was available.
- **System downtime** — If you need to take down a storage array and you see that iSCSI initiators are still logged on, you can end the iSCSI sessions to get the iSCSI initiators off the storage array.

### Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **View/End iSCSI Sessions**.

A list of the current iSCSI sessions appears.

3. Select the session that you want to end.
4. Click **End Session**, and confirm that you want to perform the operation.

## View iSER over InfiniBand statistics

If your storage array's controller includes an iSER over InfiniBand port, you can view data about the host connections.

### About this task

System Manager shows the following types of iSER over InfiniBand statistics. All statistics are read-only and cannot be set.

- **Local Target (Protocol) statistics** — Provides statistics for the iSER over InfiniBand target, which shows block-level access to its storage media.
- **iSER over InfiniBand Interface statistics** — Provides statistics for all iSER ports on the InfiniBand interface, which includes performance statistics and link error information associated with each switch port.

You can view each of these statistics as raw statistics or as baseline statistics. Raw statistics are all of the statistics that have been gathered since the controllers were started. Baseline statistics are point-in-time statistics that have been gathered since you set the baseline time.

### Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **View iSER over InfiniBand Statistics**.

3. Click a tab to view the different sets of statistics.
4. To set the baseline, click **Set new baseline**.

Setting the baseline sets a new starting point for the collection of the statistics. The same baseline is used for all iSER over InfiniBand statistics.

## Manage NVMe connections

### View NVMe over Fabrics statistics

You can view data about the NVMe over Fabrics connections to your storage array.

#### About this task

System Manager shows these types of NVMe over Fabrics statistics. All statistics are read-only and cannot be set.

- **NVMe Subsystem statistics** — Shows statistics for the NVMe controller and its queue. The NVMe controller provides an access path between a host and the namespaces in the storage array. You can review the NVMe subsystem statistics for such items as connection failures, resets, and shutdowns.
- **RDMA Interface statistics** — Provides statistics for all NVMe over Fabrics ports on the RDMA interface, which includes performance statistics and link error information associated with each switch port. This tab only appears when NVMe over Fabrics ports are available.

You can view each of these statistics as raw statistics or as baseline statistics. Raw statistics are all of the statistics that have been gathered since the controllers were started. Baseline statistics are point-in-time statistics that have been gathered since you set the baseline time.

#### Steps

1. Select **Support > Support Center > Diagnostics** tab.
2. Select **View NVMe over Fabrics Statistics**.
3. To set the baseline, click **Set new baseline**.

Setting the baseline sets a new starting point for the collection of the statistics. The same baseline is used for all NVMe statistics.

## Manage AutoSupport

### Enable or disable AutoSupport features

You enable the AutoSupport feature and the individual AutoSupport features during initial setup or you can enable them later.

#### Before you begin

If you want to enable either AutoSupport OnDemand or Remote Diagnostics, the AutoSupport delivery method must be set to HTTPS.

#### About this task

You can disable the AutoSupport feature at any time, but you are strongly advised to leave it enabled. Enabling the AutoSupport feature can significantly speed problem determination and resolution should a problem occur on your storage array.



The AutoSupport feature is made up of three individual features that you enable separately.

- **Basic AutoSupport** — Allows your storage array to automatically collect and send data to technical support.
- **AutoSupport OnDemand** — Allows technical support to request retransmission of a previous AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending retransmission requests and responds accordingly.
- **Remote Diagnostics** — Allows technical support to request a new, up-to-date AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending new requests and responds accordingly.

### Steps

1. Select **Support > Support Center > AutoSupport** tab.
2. Select **Enable/Disable AutoSupport Features**.
3. Select the check boxes next to the AutoSupport features that you want to enable.

The features depend on each other as indicated by the indentation of the items in the dialog box. For example, you must enable AutoSupport OnDemand before you can enable Remote Diagnostics.

4. Click **Save**.

### Enable AutoSupport maintenance window

Enable the AutoSupport maintenance window to suppress automatic ticket creation on error events. Under normal operation mode, the storage array uses AutoSupport to open a case with Support if there is an issue.

### Steps

1. Select **Support > Support Center > AutoSupport** tab.
2. Select **Enable AutoSupport Maintenance window**.
3. Enter the email address to receive a confirmation that the maintenance window request has been processed.

Depending on your configuration, you may be able to enter up to five email addresses. If you want to add more than one address, select **Add another email** to open another field.

4. Specify the duration (in hours) to enable the maintenance window.

The maximum supported duration is 72 hours.

5. Click **Yes**.

AutoSupport automatic ticket creation on error events is temporarily suppressed for the specified duration window.

### After you finish

The maintenance window does not begin until the storage array's request is processed by the AutoSupport servers. Wait until you have received a confirmation email before performing any maintenance activities on

your storage array.

## Disable AutoSupport maintenance window

Disable the AutoSupport maintenance window to allow automatic ticket creation on error events. When AutoSupport maintenance window is disabled, the storage array will use AutoSupport to open a case with Support if there is an issue.

### Steps

1. Select **Support > Support Center > AutoSupport** tab.
2. Select **Disable AutoSupport Maintenance window**.
3. Enter the email address to receive a confirmation that the disable maintenance window request has been processed.

Depending on your configuration, you may be able to enter up to five email addresses. If you want to add more than one address, select **Add another email** to open another field.

4. Click **Yes**.

AutoSupport automatic ticket creation on error events is enabled.

### After you finish

The maintenance window will not end until the storage array's request has been processed by the AutoSupport servers. Wait until you have received a confirmation email before proceeding.

## Configure AutoSupport delivery method

The AutoSupport feature supports the HTTPS, HTTP, and SMTP protocols for delivering dispatches to technical support.

### Before you begin

- The AutoSupport feature must be enabled. You can see whether it is enabled on the AutoSupport page.
- A DNS server must be installed and configured in your network. The DNS server address must be configured in System Manager (this task is available from the Hardware page).

### About this task

Review the different protocols:

- **HTTPS** — Allows you to connect directly to the destination technical support server using HTTPS. If you want to enable either AutoSupport OnDemand or Remote Diagnostics, the AutoSupport delivery method must be set to HTTPS.
- **HTTP** — Allows you to connect directly to the destination technical support server using HTTP.
- **Email** — Allows you to use an email server as the delivery method for sending AutoSupport dispatches.



**Differences between the HTTPS/HTTP and Email methods.** The Email delivery method, which uses SMTP, has some important differences from the HTTPS and HTTP delivery methods. First, the size of the dispatches for the Email method are limited to 5MB, which means that some ASUP data collections will not be dispatched. Second, the AutoSupport OnDemand feature is available only on HTTP and HTTPS methods.

## Steps

1. Select **Support > Support Center > AutoSupport** tab.
2. Select **Configure AutoSupport Delivery Method**.

A dialog box appears, which lists the dispatch delivery methods.

3. Select the desired delivery method, and then select the parameters for that delivery method. Do one of the following:
  - If you selected HTTPS or HTTP, select one of the following delivery parameters:
    - **Directly** — This delivery parameter is the default selection. Choosing this option allows you to connect directly to the destination technical support system using the HTTPS or HTTP protocol.
    - **Via Proxy server** — Choosing this option allows you to specify the HTTP proxy server details required for establishing connection with the destination technical support system. You must specify the host address and port number. However, you only need to enter the host authentication details (user name and password) if required.
    - **Via Proxy auto-configuration script (PAC)** — Specify the location of a Proxy Auto-Configuration (PAC) Script file. A PAC file allows the system to automatically choose the appropriate proxy server for establishing a connection with the destination technical support system.
  - If you selected Email, enter the following information:
    - The mail server address as a fully qualified domain name, IPv4 address, or IPv6 address.
    - The email address that appears in the From field of the AutoSupport dispatch email.
    - **Optional:** If you want to perform a configuration test.) The email address where a confirmation is sent when the AutoSupport system receives the test dispatch.
4. Click **Test Configuration** to test the connection to the technical support server using the specified delivery parameters. If you enabled the AutoSupport On-Demand feature, the system will also test the connection for AutoSupport OnDemand dispatch delivery.

If the configuration test fails, check your configuration settings and run the test again. If the test continues to fail, contact technical support.

5. Click **Save**.

## Schedule AutoSupport dispatches

System Manager automatically creates a default schedule for AutoSupport dispatches. If you prefer, you can specify your own schedule.

### Before you begin

The AutoSupport feature must be enabled. You can see whether it is enabled on the AutoSupport page.

### About this task

- **Daily time** — Daily dispatches are collected and sent every day during the time range that you specify. System Manager selects a random time during the range. All times are in Coordinated Universal Time (UTC), which might be different from the storage array's local time. You must convert your storage array's local time into UTC.
- **Weekly day** — Weekly dispatches are collected and sent once a week. System Manager selects a random day from the days that you specify. Deselect any days on which you do not want to allow a weekly dispatch to occur. System Manager selects a random day from the days that you allow.

- **Weekly time** — Weekly dispatches are collected and sent once a week during the time range that you specify. System Manager selects a random time during the range. All times are in Coordinated Universal Time (UTC), which might be different from the storage array's local time. You must convert your storage array's local time into UTC.

### Steps

1. Select **Support** › **Support Center** › **AutoSupport** tab.
2. Select **Schedule AutoSupport Dispatches**.

The Schedule AutoSupport Dispatches wizard appears.

3. Follow the steps in the wizard.

### Send AutoSupport dispatches

System Manager allows you to send AutoSupport dispatches to technical support, without waiting for a scheduled dispatch.

#### Before you begin

The AutoSupport feature must be enabled. You can see whether it is enabled on the AutoSupport page.

#### About this task

This operation collects support data and automatically sends it to technical support, so they can troubleshoot issues.

### Steps

1. Select **Support** › **Support Center** › **AutoSupport** tab.
2. Select **Send AutoSupport Dispatch**.

The **Send AutoSupport Dispatch** dialog box appears.

3. Confirm the operation by selecting **Send**.

### View AutoSupport status

The AutoSupport page shows you whether the AutoSupport feature and the individual AutoSupport features are currently enabled.

### Steps

1. Select **Support** › **Support Center** › **AutoSupport** tab.
2. Look at the right side of the page just below the tabs to see whether the basic AutoSupport feature is enabled.
3. Hover your cursor over the question mark to see whether individual AutoSupport features are enabled.

### View AutoSupport log

The AutoSupport log provides information about status, dispatch history, and errors encountered during the delivery of AutoSupport dispatches.

#### About this task

Multiple log files can exist. When the current log file reaches 200 KB, it is archived and a new log file is created. The archived log file name is `ASUPMessages.n`, where `n` is an integer from 1 to 9. If multiple log files exist, you can choose to view the most current log or a previous log.

- **Current log** — Shows a list of the latest captured events.
- **Archived log** — Shows a list of earlier events.

### Steps

1. Select **Support** › **Support Center** › **AutoSupport** tab.
2. Select **View AutoSupport Log**.

A dialog box appears, which lists the current AutoSupport log.

3. If you want to see previous AutoSupport logs, select the **Archived** radio button, and then select a log from the **Select AutoSupport log** drop-down list.

The Archived option appears only if archived logs exist on the storage array.

The selected AutoSupport log appears in the dialog box.

4. **Optional:** To search the AutoSupport log, type a term in the **Find** box, and click **Find**.

Click **Find** again to search for additional occurrences of the term.

## FAQs

### What data am I collecting?

The AutoSupport feature and the manual Support Data Collection feature provide ways to collect data in a customer support bundle for remote troubleshooting and problem analysis by technical support.

The customer support bundle gathers all types of information about the storage array into a single compressed file. The information collected includes the physical configuration, logical configuration, version information, events, log files, and performance data. The information is used only by technical support to solve problems with the storage array.

### What does unreadable sectors data show me?

You can display detailed data about unreadable sectors detected on the drives in your storage array.

The unreadable sectors log shows the most recent unreadable sector first. The log contains the following information about the volumes that contain the unreadable sectors. The fields are sortable.

Field	Description
Affected Volume	Shows the label of the volume. If a missing volume contains unreadable sectors, the World Wide Identifier appears for the missing volume.

Field	Description
Logical Unit Number (LUN)	Shows the LUN for the volume. If the volume does not have a LUN, the dialog box shows NA.
Assigned To	Shows the hosts or host clusters that have access to the volume. If the volume is not accessible by a host, host cluster, or even a Default Cluster, the dialog box shows NA.

To see additional information about the unreadable sectors, click the plus (+) sign next to a volume.

Field	Description
Date/Time	Shows the date and the time that the unreadable sector was detected.
Volume Logical Block Address	Shows the logical block address (LBA) of the volume.
Drive Location	Shows the drive shelf, drawer (if your drive shelf has drawers), and the bay location.
Drive Logical Block Address	Shows the LBA of the drive.
Failure Type	Shows one of the following failure types: <ul style="list-style-type: none"> <li>• <b>Physical</b> — A physical media error.</li> <li>• <b>Logical</b> — A read error elsewhere in the stripe causing unreadable data. For example, an unreadable sector due to media errors elsewhere in the volume.</li> <li>• <b>Inconsistent</b> — Inconsistent redundancy data.</li> <li>• <b>Data Assurance</b> — A Data Assurance error.</li> </ul>

## What is a health image?

A health image is a raw data dump of the controller's processor memory that technical support can use to diagnose a problem with a controller.

The firmware automatically generates a health image when it detects certain errors. Under certain troubleshooting scenarios, technical support might request that you retrieve the health image file and send it to them.

## What else do I need to do to configure or diagnose iSCSI?

iSCSI sessions can occur with hosts or remote storage arrays in an asynchronous mirror relationship. The following tables list the System Manager functions that you can use to configure and manage these iSCSI sessions.



The iSCSI settings are only available if your storage array supports iSCSI.

## Configure iSCSI

Action	Location
Manage iSCSI settings	<ol style="list-style-type: none"><li>1. Select <b>Settings &gt; System</b>.</li><li>2. Scroll down to <b>iSCSI settings</b> to view all the management functions.</li></ol>
Configure iSCSI ports	<ol style="list-style-type: none"><li>1. Select <b>Hardware</b>.</li><li>2. Select <b>Show back of shelf</b>.</li><li>3. Select a controller.</li><li>4. Select <b>Configure iSCSI ports</b>.</li></ol>
Set the host CHAP secret	<ol style="list-style-type: none"><li>1. Select <b>Settings &gt; System</b>.</li><li>2. Scroll down to <b>iSCSI settings</b>, and then select <b>Configure Authentication</b>.</li></ol> <p>or</p> <ol style="list-style-type: none"><li>1. Select <b>Storage &gt; Hosts</b>.</li><li>2. Select a host member.</li><li>3. Click <b>View/Edit Settings &gt; Host Ports</b> tab.</li></ol>

## Diagnose iSCSI

Action	Location
View or end iSCSI sessions	<ol style="list-style-type: none"><li>1. Select <b>Settings &gt; System</b>.</li><li>2. Scroll down to <b>iSCSI settings</b>, and then select <b>View/End iSCSI Sessions</b>.</li></ol> <p>or</p> <ol style="list-style-type: none"><li>1. Select <b>Support &gt; Support Center &gt; Diagnostics</b> tab.</li><li>2. Select <b>View/End iSCSI Sessions</b>.</li></ol>

Action	Location
View iSCSI statistics	<ol style="list-style-type: none"> <li>1. Select <b>Settings › System</b>.</li> <li>2. Scroll down to <b>iSCSI settings</b>, and then select <b>View iSCSI Statistics Packages</b>.</li> </ol> <p>or</p> <ol style="list-style-type: none"> <li>1. Select <b>Support › Support Center › Diagnostics</b> tab.</li> <li>2. Select <b>View iSCSI Statistics Packages</b>.</li> </ol>

## What do the AutoSupport features do?

The AutoSupport feature is made up of three individual features that you enable separately.

- **Basic AutoSupport** — Allows your storage array to automatically collect and send data to technical support.
- **AutoSupport OnDemand** — Allows technical support to request retransmission of a previous AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending retransmission requests and responds accordingly.
- **Remote Diagnostics** — Allows technical support to request a new, up-to-date AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending new requests and responds accordingly.

## What type of data is collected through the AutoSupport feature?

The AutoSupport feature contains three standard dispatch types: event dispatches, scheduled dispatches, and on-demand and remote diagnostics dispatches.

The AutoSupport data does not contain any user data.

### • Event dispatches

When events occur on the system that warrant proactive notification to technical support, the AutoSupport feature automatically sends an event-triggered dispatch.

- Sent when a support event on the managed storage array occurs.
- Includes a comprehensive snapshot of what was going on with the storage array at the time the event occurred.

### • Scheduled dispatches

The AutoSupport feature automatically sends several dispatches on a regular schedule.

- **Daily dispatches** — Sent once every day during a user-configurable time interval. Includes the current system event logs and performance data.



- **Weekly dispatches** — Sent once every week during a user-configurable time interval and day. Includes configuration and system state information.

- **AutoSupport OnDemand and Remote Diagnostics dispatches**

- **AutoSupport OnDemand** — Allows technical support to request retransmission of a previous AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending retransmission requests and responds accordingly.
- **Remote Diagnostics** — Allows technical support to request a new, up-to-date AutoSupport dispatch when needed for troubleshooting an issue. All transmissions are initiated from the storage array, not from the AutoSupport server. The storage array checks in periodically with the AutoSupport server to determine if there are any pending new requests and responds accordingly.

## How do I configure the delivery method for the AutoSupport feature?

The AutoSupport feature supports the protocols HTTPS, HTTP, and SMTP for delivering AutoSupport dispatches to technical support.

### Before you begin

- The AutoSupport feature must be enabled. You can see whether it is enabled on the AutoSupport page.
- A DNS server must be installed and configured in your network. The DNS server address must be configured in System Manager (this task is available from the Hardware page).

### About this task

Review the different protocols:

- **HTTPS** — Allows you to connect directly to the destination technical support server using HTTPS. If you want to enable either AutoSupport OnDemand or Remote Diagnostics, the AutoSupport delivery method must be set to HTTPS.
- **HTTP** — Allows you to connect directly to the destination technical support server using HTTP.
- **Email** — Allows you to use an email server as the delivery method for sending AutoSupport dispatches.



**Differences between the HTTPS/HTTP and Email methods.** The Email delivery method, which uses SMTP, has some important differences from the HTTPS and HTTP delivery methods. First, the size of the dispatches for the Email method are limited to 5MB, which means that some ASUP data collections will not be dispatched. Second, the AutoSupport OnDemand feature is available only on HTTP and HTTPS methods.

### Steps

1. Select **Support > Support Center > AutoSupport** tab.
2. Select **Configure AutoSupport Delivery Method**.

A dialog box appears, which lists the dispatch delivery methods.

3. Select the desired delivery method, and then select the parameters for that delivery method. Do one of the following:
  - If you selected HTTPS or HTTP, select one of the following delivery parameters:
    - **Directly** — This delivery parameter is the default selection. Choosing this option allows you to

connect directly to the destination technical support system using the HTTPS or HTTP protocol.

- **Via Proxy server** — Choosing this option allows you to specify the HTTP proxy server details required for establishing connection with the destination technical support system. You must specify the host address and port number. However, you only need to enter the host authentication details (user name and password) if required.
- **Via Proxy auto-configuration script (PAC)** — Specify the location of a Proxy Auto-Configuration (PAC) Script file. A PAC file allows the system to automatically choose the appropriate proxy server for establishing a connection with the destination technical support system.

◦ If you selected Email, enter the following information:

- The mail server address as a fully qualified domain name, IPv4 address, or IPv6 address.
- The email address that appears in the From field of the AutoSupport dispatch email.
- **Optional:** If you want to perform a configuration test.) The email address where a confirmation is sent when the AutoSupport system receives the test dispatch.

4. Click **Test Configuration** to test the connection to the technical support server using the specified delivery parameters. If you enabled the AutoSupport On-Demand feature, the system will also test the connection for AutoSupport OnDemand dispatch delivery.

If the configuration test fails, check your configuration settings and run the test again. If the test continues to fail, contact technical support.

5. Click **Save**.

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.