



## **Release notes**

### E-Series storage systems

NetApp  
January 20, 2026

# Table of Contents

Release notes .....	1
What's new in SANtricity OS .....	1
New features in Version 11.90R4 .....	1
New features in Version 11.90R3 .....	1
New features in Version 11.90R2 .....	1
New features in Version 11.90R1 .....	1
New features in Version 11.90 .....	1
New features in Version 11.80.1R4 .....	2
New features in Version 11.80.1R3 .....	2
New features in Version 11.80.1R2 .....	2
New features in Version 11.80.1R1 .....	2
New features in Version 11.80.1 .....	3
New features in Version 11.80 .....	3
E-Series Release Notes .....	6

# Release notes

## What's new in SANtricity OS

The following table describes new features in the latest SANtricity OS releases for embedded management of E4000, EF300/EF300C, EF600/EF600C, E2800/EF280, and E5700/EF570 controllers.

### New features in Version 11.90R4

This version contains only minor changes and no new features. For more information on the changes in this release, please refer to the [E-Series 11.90 Release Notes](#).

### New features in Version 11.90R3

New feature	Description
SANtricity OS Support for IOM12C and DCM3	Support for IOM12C and DCM3 SAS-3 shelves is now available for controller firmware 11.90R3 or above. The IOM12C and DCM3 shelves are replacements for the IOM12B and DCM2 shelves.

### New features in Version 11.90R2

This version contains only minor changes and no new features. For more information on the changes in this release, please refer to the [E-Series 11.90 Release Notes](#).

### New features in Version 11.90R1

New feature	Description
New storage system models – EF300C and EF600C	This release introduces the EF300C and EF600C all flash NVMe storage systems. The EF300C and EF600C are high-capacity flash versions of the existing EF300 and EF600 storage systems. High-capacity NVMe SSD drives of 30TB or 60TB sizes are supported with the EF300C and EF600C. The EF300C/EF600C is compatible for Dynamic Disk Pool use only with no legacy RAID support.
Support for 12Gb SAS interfaces on E4000 controllers	The E4000 controller now supports 12Gb SAS host interface cards.

### New features in Version 11.90

New feature	Description
New storage system model – E4000	This release introduces the E4000 low-cost storage system. The E4000 supports 12 and 60 drives and a single host interface card (HIC) per controller. For the initial release, supported host interface cards include iSCSI and Fibre Channel. E4000 storage systems and other E-Series storage systems can be viewed and managed in Unified Manager.
Increased capacity for Dynamic Disk Pools	The capacity for Dynamic Disk Pools (DDP) has been increased to 12 PB whenever the capacity of each of the individual drives within the pool is greater than 23 TB in size. If the individual drive capacity is less than 23 TB in size, the DDP capacity is 6 PB.
Default media scan settings increased	The default media scan rate has been increased to 120 days.
Private key now accepted for External Key Management	Certificate signing request (CSR) file generated externally through private and public key pairs can now be imported through System Manager.
Login lockout feature now available for Web Services	Configurable through the REST API only, a new login lockout setting is now available for embedded and proxy Web Services.

## New features in Version 11.80.1R4

This version contains only minor changes and no new features or restrictions. For more information on the changes in this release, please refer to the README file.

## New features in Version 11.80.1R3

This version contains only minor changes and no new features or restrictions. For more information on the changes in this release, please refer to the README file.

## New features in Version 11.80.1R2

This version contains only minor changes and no new features or restrictions. For more information on the changes in this release, please refer to the README file.

## New features in Version 11.80.1R1

New feature	Description
Increased key size length of new self-signed and CA-signed management certificates.	The management certificate key size length for SANtricity System Manager and Unified Manager applications self-signed certificate have been modified from 2048 to 3072 bits. The change applies to newly generated self-signed and CA-signed certificates from the SANtricity applications. The key length is fixed and is not affected by the default key size definitions in NVSRAM.

## New features in Version 11.80.1

New feature	Description
-identifyDevices parameter	A new <code>-identifyDevices</code> parameter is now available in the SMcli. This new parameter allows you to look for all SCSI native block devices that are associated with your Storage Arrays. For more information, see <a href="#">xref:./ Downloadable SMcli command line parameters</a> .
Ethernet Kernel Statistics	A new Ethernet Kernel Statistics option is now available under the View iSCSI Statistics Packages page in System Manager. This new option allows you to view statistics for platform kernel drivers of the iSCSI device. For more information, see <a href="#">xref:./ View iSCSI Statistics Packages</a> .
Added ability to block IP addresses through REST API endpoint	Users can now block specific IP addresses through the Settings endpoint ( <code>/devmgr/v2/settings</code> ). Once configured through the Settings endpoint, only IP addresses specified through a whitelist can communicate with the storage device. This new feature supports IPv4 and IPv6 address lists.
vCenter Storage plugin	The vCenter Storage plugin has been updated for compatibility with the E-Series 11.80.1 release.
Web Services Proxy	The Web Services Proxy has been updated to version 6.1 for compatibility with the E-Series 11.80.1 release.

## New features in Version 11.80

New feature	Description
Enhanced Volume Parity Scan	Volume parity scan can now be launched as a background process either via the REST API or via CLI. The resulting parity scan will run in the background as long as is required to complete the scan operation. Scan operations will survive controller reboots and failover operations.
SAML Support for Unified Manager	Unified Manager now supports SAML (Security Assertion Markup Language). Once SAML is enabled for Unified Manager, users must use multi factor authentication against the identity provider in order to interact with the user interface. Note that once SAML is enabled on Unified Manager, the REST API cannot be used without going through the IdP to authenticate requests.
Auto Configuration Feature	Now supports the ability to set the volume block size parameter to use with the Auto Configuration feature for initial array setup. This feature is available in the CLI only as a "blockSize" parameter.

New feature	Description
Controller Firmware Cryptographic Signing	Controller firmware is cryptographically signed. Signatures are checked during initial download and at each controller boot. No end user impact expected. Signatures are backed by a CA issued Extended Validation certificate.
Drive Firmware Cryptographic Signing	Drive firmware is cryptographically signed. Signatures are checked during initial download and backed by a CA issued Extended Validation certificate. Drive firmware content is now delivered as a ZIP file, which contains the older non-signed firmware as well as the new signed firmware. The user must chose the appropriate file based on the release version of code that is running on the target system.
External Key Server Management - Certificate Key Size	<p>The new default certificate key size is 3072 bits (from 2048). Key sizes up to 4096 bits are supported. An NVSRAM bit must be changed in order to support the non-default key sizes.</p> <p>Key size selection values are as follows:</p> <ul style="list-style-type: none"> <li>• DEFAULT = 0</li> <li>• LENGTH 2048 = 1</li> <li>• LENGTH 3072 = 2</li> <li>• LENGTH 4096 = 3</li> </ul> <p>To change key size to 4096 via the SMcli:</p> <pre>set controller[b] globalnvrambyte[0xc0]=3; set controller[a] globalnvrambyte[0xc0]=3;</pre> <p>Interrogate the key size:</p> <pre>show allcontrollers globalnvrambyte[0xc0];</pre>
Disk Pool Improvements	<p>Disk pools created with controllers running 11.80 or above will be <i>Version 1</i> pools as opposed to <i>Version 0</i> pools. A downgrade operation is restricted when a <i>Version 1</i> disk pool exists.</p> <p>The version of a disk pool can be identified in the storage array profile.</p>
System Manager and Unified Manager will not launch unless minimum browser requirements are met	<p>A minimum version of the browser is required before either System Manager or Unified Manager will launch.</p> <p>The following are the minimum supported versions:</p> <ul style="list-style-type: none"> <li>• Firefox minimum version 80</li> <li>• Chrome minimum version 89</li> <li>• Edge minimum version 90</li> <li>• Safari minimum version 14</li> </ul>

New feature	Description
Support for FIPS 140-3 NVMe SSD drives	Netapp certified FIPS 140-3 NVMe SSD drives are now supported. They will be correctly identified as such in the storage array profile and in System Manager.
Support for SSD Read cache on EF300 and EF600	SSD Read cache is now supported on EF300 and EF600 controllers using HDD with a SAS expansion.
Support for iSCSI and Fibre Channel asynchronous remote mirroring on EF300 and EF600	Asynchronous remote mirroring (ARVM) is now supported on EF300 and EF600 controllers with NVMe and SAS based volumes.
Support EF300 and EF600 without drives on the base tray	EF300 and EF600 controller configurations without NVMe drives on the base tray is now supported.
USB ports disabled for all platforms	USB ports are now disabled on all platforms.
Increased SSD Read Cache maximum	SSD Read cache maximum increased from 5TB to 8TB.
Assign all flash read cache to a single volume in duplex configs	All SSD Read cache can now be assigned to the same volume on duplex systems whenever a single volume uses the entire SSD cache.
Drive serial number added to drive summary table of storage array profile	The drive serial number has been added to the drive summary table in the Storage Array profile.
Added dom0-misc-logs to daily ASUP	The dom0-misc logs for controller A and B have been added to the daily ASUPs.
Port 443 now used by default for application communicating with embedded web services	Port 443 is now used by the default when communicating with the embedded webserver. The <code>-useLegacyTransferPort</code> CLI command has been added for those who instead want to use the legacy 8443 transfer port. For more information on the new <code>-useLegacyTransferPort</code> CLI command, see the <a href="#">SANtricity CLI What's New</a> .
Scan volume parity progress capability	<p>The following CLI commands were implemented to support job-based volume parity scan operations:</p> <ul style="list-style-type: none"> <li>Start check volume parity</li> <li>Save check volume parity job errors</li> <li>Stop check volume parity job</li> <li>Show check volume parity job or jobs</li> </ul> <p>For more information on the new job-based volume parity scan CLI commands, see the <a href="#">SANtricity CLI What's New</a>.</p>

New feature	Description
MFA Support for Unified Manager	Multi-factor authentication (MFA) support is now supported under Unified Manager.
Toggle icon for front-back hardware view	<p>In the Hardware view of System Manager/Unified Manager, the following two tabs are now available to control the front and back view:</p> <ul style="list-style-type: none"> <li>• Drives tab</li> <li>• Controllers &amp; Components tab</li> </ul>
vCenter Storage plugin	The vCenter Storage plugin has been updated for compatibility with the E-Series 11.80 release.
Web Services Proxy 6.0	The Web Services Proxy has been updated to version 6.0 for compatibility with the E-Series 11.80 release.
Removed ASUP case creation flag for E-Series nominal and maximum temperature exceeded events	Case creation flag is now disabled for nominal and maximum temperature exceeded events requiring no action.
Priority case creation flag enabled for the 0x1209 MEL event	A case creation flag is now created for the MEL_EV_DEGRADE_CHANNEL 0x1209 MEL event.

## E-Series Release Notes

Release Notes are available outside this site. You will be prompted to log in using your NetApp Support Site credentials.

- [11.90 Release notes](#)
- [11.80 Release notes](#)
- [11.70 Release notes](#)
- [11.60 Release notes](#)
- [11.50 Release notes](#)

## Copyright information

Copyright © 2026 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.