Secure data

AFX

NetApp
January 21, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-afx/secure-data/prepare-secure-data.html on January 21, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Secure data

Prepare to secure your AFX storage system data

Before managing your AFX data, you should be familiar with the major concepts and capabilities.

Terminology and options

There are several terms related to AFX data security you should be familiar with.

Ransomware

Ransomware is malicious software that encrypts files making them inaccessible to the user. There is typically some type of payment demanded to decrypt the data. ONTAP provides solutions to protect against ransomware through features like Autonomous Ransomware Protection (ARP).

Encryption

Encryption is the process of converting data into a secure format that cannot be easily read without proper authorization. ONTAP offers both software-based and hardware-based encryption technologies to protect data at rest. This ensures it cannot be read if the storage medium is repurposed, returned, misplaced, or stolen. These encryption solutions can be managed using either an external key management server or the Onboard Key Manager provided by ONTAP. Refer to Encrypt data at rest on an AFX storage system for more information.

Digital certificates and PKI

A digital certificate is an electronic document used to prove ownership of a public key. The public key and associated private key can be used in various ways, including to establish identity typically as part of a larger security framework such as TLS and IPsec. These keys, as well as the supporting protocols and formatting standards, form the basis for public key infrastructure (PKI). Refer to Manage certificates on an AFX storage system for more information.

Internet Protocol Security

IPsec is an Internet standard that provides in-flight data encryption, integrity, and authentication for traffic flowing among network endpoints at the IP level. It secures all IP traffic between ONTAP and clients including higher level protocols such as NFS and SMB. IPsec provides protection against malicious replay and man-in-the-middle attacks on your data. Refer to Secure IP connections on your AFX storage systems for more information.

Related information

- Additional AFX SVM administration
- Prepare to administer your AFX system

Encrypt data at rest on an AFX storage system

You can encrypt your data at the hardware and software level for dual-layer protection. When you encrypt data at rest, it can't be read if the storage medium is repurposed, returned, misplaced, or stolen.

NetApp Storage Encryption (NSE) supports hardware encryption using self-encrypting drives (SEDs). SEDs

encrypt data as it is written. Each SED contains a unique encryption key. Encrypted data stored on the SED can't be read without the SED's encryption key. Nodes attempting to read from an SED must be authenticated to access the SED's encryption key. Nodes are authenticated by obtaining an authentication key from a key manager, then presenting the authentication key to the SED. If the authentication key is valid, the SED will give the node its encryption key to access the data it contains.

Before you begin

Use the AFX onboard key manager or an external key manager to serve authentication keys to your nodes. In addition to NSE, you can also enable software encryption to add another layer of security to your data.

Steps

1. In System manager, select **Cluster** and then **Settings**.
2. In the **Security** section, under **Encryption**, select **Configure**.
3. Configure the key manager.

Option	Steps
Configure the Onboard key Manager	a. Select **Onboard Key Manager** to add the key servers. b. Enter a passphrase.
Configure an external key manager	a. Select **External key manager** to add the key servers. b. Select + Add to add the key servers. c. Add the KMIP server CA certificates. d. Add the KMIP client certificates.

4. Select **Dual-layer encryption** to enable software encryption.
5. Select **Save**.

Related information

- Encryption

Secure IP connections on your AFX storage systems

IP Security (IPsec) is an Internet protocol standard that provides data encryption, integrity, and authentication for traffic flowing among network endpoints at the IP level. You can use IPsec to enhance the security of the front-end network between an AFX cluster and the clients.

Configuring IPsec on an AFX system

The IPsec configuration procedures for AFX storage systems are the same as AFF and FAS systems, with the exception of the supported network interface controller (NIC) cards used with the hardware offload feature. Refer to Prepare to configure IP security for the ONTAP network for more information.

Hardware offload feature

Several of the IPsec cryptographic operations, such as encryption and integrity checks, can be offloaded to a supported NIC card on your AFX system. This can significantly improve the performance and throughput of the network traffic protected by IPsec.

Beginning with ONTAP 9.18.1, the IPsec hardware offload feature is extended to support IPv6 traffic.

The following NIC cards are supported for the IPsec hardware offload feature on AFX storage systems beginning with ONTAP 9.17.1:

- X50130B (2p, 40G/100G Ethernet controller)
- X50131B (2p, 40G/100G/200G/400G Ethernet controller)

Refer to the NetApp Hardware Universe for more information about the supported cards for the ONTAP release running on your AFX system.

Related information

- Prepare to configure IP security for the ONTAP network
- NetApp Hardware Universe

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.