Reference

NetApp Console local deployment

NetApp
August 10, 2026

This PDF was generated from https://docs.netapp.com/us-en/console-local/task-iam-rename-organization.html on August 10, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Reference

NetApp Console local deployment API

Manage your NetApp Console local deployment organization and fleet IDs

In NetApp Console local deployment, your NetApp Console organization has a name and an ID. You can choose a name for your organization to help identify it. You may also need to retrieve the organization ID for certain integrations.

Required access roles

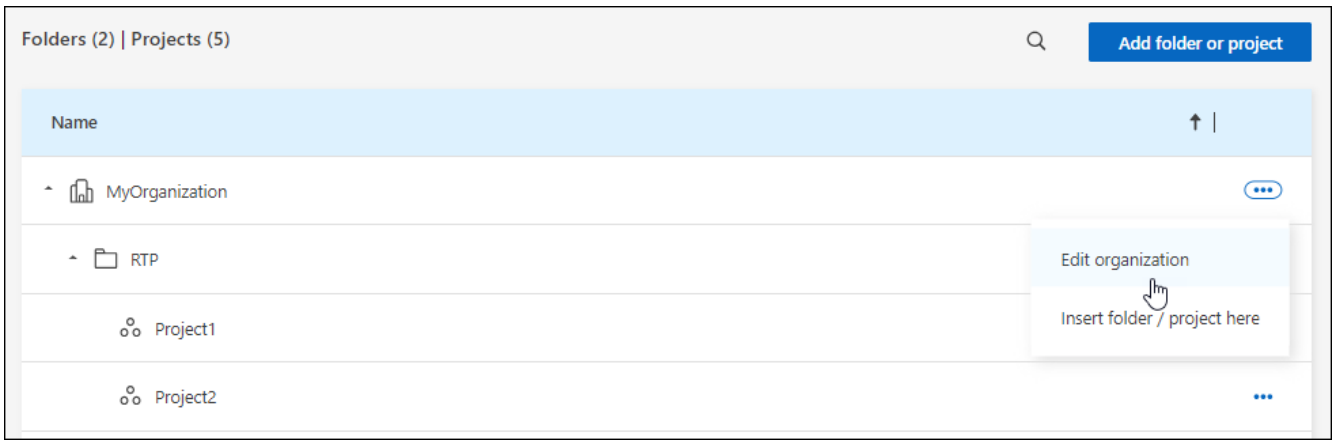
Super admin or Organization admin. Learn about access roles.

Rename your organization

You can rename your organization.

Steps

1. Select **Administration > Identity and access**.
2. Select **Organization**.
3. From the **Organization** page, navigate to the first row in the table, select ••• and then select **Edit organization**.



4. Enter a new organization name and select **Apply**.

Get the organization ID

The organization ID is used for certain integrations with the Console.

You can view the organization ID from the Organizations page and copy it to the clipboard for your needs.

Steps

1. Select **Administration > Identity and access** > **Organization**.
2. On the **Organization** page, look for your organization ID in the summary bar and copy it to the clipboard. You can save this for use later or copy it directly to where you need to use it.

Obtain the ID for a fleet

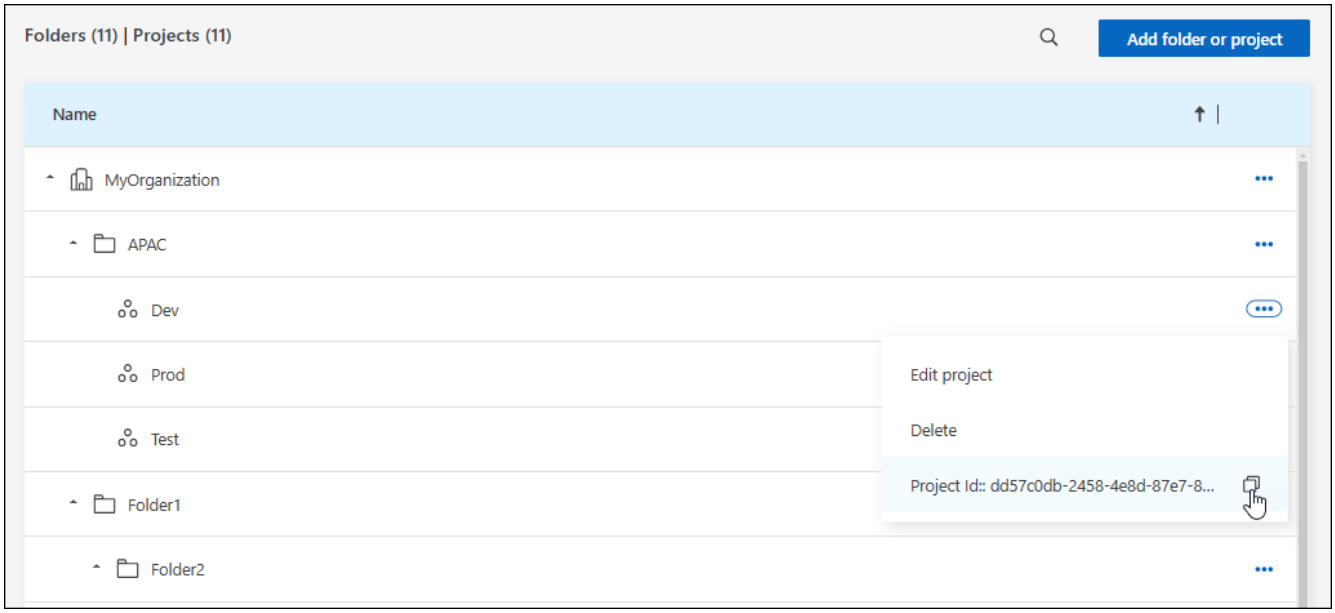
You'll need to obtain the ID for a fleet if you are using the API.

Steps

1. From the **Organization** page, navigate to a fleet in the table and select •••

   The fleet ID displays.

2. To copy the ID, select the copy button.



Related information

- Learn about identity and access management
- Get started with identity and access in NetApp Console
- Learn about the API for identity and access

Supported LLM providers and models in NetApp Console local deployment

NetApp Console local deployment supports OpenAI, OpenAI-compatible, and Anthropic LLM provider types. The models you can select depend on the provider type and endpoint you configure.

This documentation regarding connecting an LLM to the Console assistant to enable AI features is provided as a technology preview. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before General Availability.

Choose a model that matches your performance, cost, and governance requirements.

See how provider type affects model availability

The provider type you choose determines which models appear in the Console local deployment model list:

- **OpenAI** — provides models for direct OpenAI integration.
- **OpenAI-compatible** — provides models that your organization's compatible endpoint exposes.
- **Anthropic** — provides models for direct Anthropic integration.

The models you see can vary based on endpoint configuration, proxy or gateway behavior, and organizational policy. Provider types differ by the endpoint you connect to and the models that endpoint exposes, not the transport protocol.

Supported OpenAI models

- GPT-5.4
- GPT-5.5

Supported Anthropic models

- Claude Sonnet 4.6
- Claude Opus 4.6, 4.7 & 4.8

Related information

- Connect your LLM and enable the NetApp Console assistant.
- Learn about LLM integration in NetApp Console local deployment.

ONTAP alerts reference in NetApp Console local deployment

This reference lists the ONTAP alerts that NetApp Console local deployment can monitor, organized by impact category.

Severity mapping

The same EMS alert can appear as Critical, Warning, or Info, depending on the ONTAP event that caused it:

- **Critical**: Maps from ONTAP severities `alert`, `emergency`
- **Warning**: Maps from ONTAP severity `error`
- **Info**: Maps from ONTAP severities `notice`, `informational`
- **Other**: Passed through as-is

Dynamic mapping lets a single alert rule emit different severities depending on the runtime context of the EMS event.

The sections below group alerts by impact category and sort each table alphabetically by alert name.

Availability alerts

These alerts can affect system, service, or data availability.

Alert name	Severity	Type	Description
Active Directory Server Connection Down	Critical	EMS	All configured AD/LDAP servers for this SVM are unreachable.
Aggregate isn’t online	Critical	Metric	Some aggregates are offline. Volume creation could cause duplicate FSIDs.
Antivirus server busy	Critical, Warning, Info	EMS	The antivirus server is overloaded and can’t accept additional scan requests.
AWS credentials not initialized	Critical, Warning, Info	EMS	A module attempted to access AWS IAM role-based credentials before they were initialized.
Cloud tier unreachable	Critical, Warning, Info	EMS	A storage node cannot connect to Cloud Tier object store API. Some data will be inaccessible.
Disk failure	Critical	Metric	A disk has failed, is being sanitized, or is in Maintenance mode.
Disk out of service	Critical, Warning, Info	EMS	A disk was taken out of service due to failure, sanitization, or maintenance.
Disk shelves power supply removed	Critical, Warning, Info	EMS	A power supply unit was removed from the disk shelf.
FC target port commands exceeded	Critical, Warning, Info	EMS	The number of outstanding commands on the physical FC target port exceeds the supported limit.
Giveback of storage pool failed	Critical, Warning, Info	EMS	This event occurs during the relocation of a storage pool (aggregate) as part of a storage failover (SFO) giveback, when the destination node cannot reach the object stores.
HA interconnect down	Critical, Warning, Info	EMS	The high-availability (HA) interconnect is down. Risk of service outage when failover is not available.
InstanceDown	Critical	Metric	The monitored instance is unreachable and may be down or experiencing network issues.
LUN destroyed	Critical, Warning, Info	EMS	A LUN was destroyed and is no longer accessible.
LUN offline	Critical, Warning, Info	EMS	A LUN was taken offline manually.

Alert name	Severity	Type	Description
Main unit fan failed	Critical, Warning, Info	EMS	One or more main unit fans have failed. The system remains operational.
Main unit fan in warning state	Critical, Warning, Info	EMS	One or more main unit cooling fans are in a warning state.
Max sessions per user exceeded	Critical, Warning, Info	EMS	You have exceeded the maximum number of sessions allowed per user over a TCP connection.
Max times open per file exceeded	Critical, Warning, Info	EMS	You have exceeded the maximum number of times that you can open the file over a TCP connection.
MetroCluster automatic unplanned switchover disabled	Critical, Warning, Info	EMS	Automatic unplanned switchover capability has been disabled on this cluster.
MetroCluster monitoring	Critical, Warning, Info	EMS	The system health monitor alert is detected.
NFSv4 store pool exhausted	Critical, Warning, Info	EMS	A NFSv4 store pool has been exhausted.
NetBIOS name conflict	Critical, Warning, Info	EMS	The NetBIOS Name Service has received a negative response to a name registration request, from a remote machine.
No registered scan engine	Critical, Warning, Info	EMS	The antivirus connector notified ONTAP that it does not have a registered scan engine.
No Vscan connection	Critical, Warning, Info	EMS	ONTAP has no Vscan connection to service virus scan requests. This might cause data unavailability if the scan-mandatory option is enabled.
Non-responsive antivirus server	Critical, Warning, Info	EMS	ONTAP detected a non-responsive antivirus server and forcibly closed its Vscan connection.
Nonexistent admin share	Critical, Warning, Info	EMS	Vscan issue: a client has attempted to connect to a nonexistent ONTAP_ADMIN$ share.
NVRAM battery low	Critical, Warning, Info	EMS	The NVRAM battery capacity is critically low. There might be a potential data loss if the battery runs out of power.
NVMe namespace destroyed	Critical, Warning, Info	EMS	An NVMe namespace was destroyed and is no longer accessible.

Alert name	Severity	Type	Description
NVMe namespace offline	Critical, Warning, Info	EMS	An NVMe namespace was taken offline manually.
NVMe namespace online	Critical, Warning, Info	EMS	An NVMe namespace was brought back online.
NVMe-oF license grace period active	Critical, Warning, Info	EMS	This event occurs on a daily basis when the NVMe over Fabrics (NVMe-oF) protocol is in use and the grace period of the license is active.
NVMe-oF license grace period expired	Critical, Warning, Info	EMS	The NVMe over Fabrics (NVMe-oF) license grace period is over and the NVMe-oF functionality is disabled.
NVMe-oF license grace period start	Critical, Warning, Info	EMS	The NVMe over Fabrics (NVMe-oF) configuration was detected during the upgrade to ONTAP 9.5 software.
Object store host unresolvable	Critical, Warning, Info	EMS	The object store server host name cannot be resolved to an IP address.
Object store intercluster LIF down	Critical, Warning, Info	EMS	The object-store client cannot find an operational LIF to communicate with the object store server.
Object store signature mismatch	Critical, Warning, Info	EMS	The request signature sent to the object store server does not match the signature calculated by the client.
Port Status Down	Critical	EMS	This Ethernet port is down. Traffic on that link may be affected.
READDIR timeout	Critical, Warning, Info	EMS	A READDIR file operation has exceeded the timeout that it is allowed to run in WAFL.
Relocation of storage pool failed	Critical, Warning, Info	EMS	This event occurs during the relocation of an storage pool (aggregate), when the destination node cannot reach the object stores.
SAN "active-active" state changed	Critical, Warning, Info	EMS	The SAN pathing is no longer symmetric.
Service Processor heartbeat missed	Critical, Warning, Info	EMS	ONTAP is not receiving an expected heartbeat signal from the Service Processor (SP).
Service Processor heartbeat stopped	Critical, Warning, Info	EMS	ONTAP is no longer receiving heartbeats from the Service Processor (SP).
Service Processor not configured	Critical, Warning, Info	EMS	This event occurs on a weekly basis, to remind you to configure the Service Processor (SP).

Alert name	Severity	Type	Description
Service Processor offline	Critical, Warning, Info	EMS	The Service Processor (SP) is offline.
SFP in FC target adapter receiving low power	Critical, Warning, Info	EMS	This alert occurs when the power received (RX) by a small form-factor pluggable transceiver (SFP in FC target) is at a level below the defined threshold.
SFP in FC target adapter transmitting low power	Critical, Warning, Info	EMS	This alert occurs when the power transmitted (TX) by a small form-factor pluggable transceiver (SFP in FC target) is at a level below the defined threshold.
Shadow copy failed	Critical, Warning, Info	EMS	A Volume Shadow Copy Service (VSS), a Microsoft Server backup and restore service operation, has failed.
Shelf fan failed	Critical, Warning, Info	EMS	The indicated cooling fan or fan module of the shelf has failed.
SnapMirror lag time is high	Critical	Metric	The SnapMirror relationship is more than one hour behind its expected update schedule.
Storage Failover Interconnect One Or More Links Down	Warning	EMS	One or more HA interconnect links to the partner node are down. Failover redundancy is reduced.
Storage switch power supplies failed	Critical, Warning, Info	EMS	There is a missing power supply in the cluster switch. Redundancy is reduced.
Storage VM stop succeeded	Critical, Warning, Info	EMS	The storage VM was stopped successfully.
SVM Configuration Replication License Invalid	Warning	EMS	The SVM-DR configuration replication license is missing, expired, or not applied
System cannot operate due to main unit fan failure	Critical, Warning, Info	EMS	One or more main unit fans have failed, disrupting system operation. This might lead to a potential data loss.
Too many CIFS authentication	Critical, Warning, Info	EMS	Many authentication negotiations have occurred simultaneously. There are 256 incomplete new session requests from this client.
Unassigned disks	Critical, Warning, Info	EMS	System has unassigned disks - capacity is being wasted.
Volume state offline	Information al	Metric	The volume has been taken offline.

Alert name	Severity	Type	Description
Volume restricted	Critical, Warning, Info	EMS	This event indicates that a flexible volume is made restricted.
Virus detected	Critical, Warning, Info	EMS	A Vscan server reported that a file might be infected with a virus.

Capacity alerts

These alerts indicate storage consumption or capacity pressure.

Alert name	Severity	Type	Description
FabricPool mirror replication resync completed	Critical, Warning, Info	EMS	The FabricPool mirror resync process completed successfully from the primary object store to the mirror object store.
FabricPool space usage limit nearly reached	Critical, Warning, Info	EMS	The total cluster-wide FabricPool space usage of object stores from capacity-licensed providers has nearly reached the licensed limit.
FabricPool space usage limit reached	Critical, Warning, Info	EMS	The total cluster-wide FabricPool space usage of object stores from capacity-licensed providers has reached the license limit.
Node root volume space low	Critical, Warning, Info	EMS	The system has detected that the root volume is dangerously low on space.
QoS monitor memory maxed out	Critical, Warning, Info	EMS	A QoS subsystem's dynamic memory has reached its limit for the current platform hardware.
Volume automatic resizing succeeded	Critical, Warning, Info	EMS	The volume was automatically resized because automatic volume growth is enabled.
Volume full	Critical	Metric	The volume is over 90% full. Free up space or add capacity to prevent write failures.

Configuration alerts

These alerts point to configuration changes or inventory updates.

Alert name	Severity	Type	Description
Disk shelf power supply discovered	Critical, Warning, Info	EMS	A power supply unit was added to the disk shelf.
Volume created	Info	Metric	A volume was created.
Volume deleted	Warning	Metric	A volume was deleted.
Volume modified	Info	Metric	A volume was modified.

Alert name	Severity	Type	Description
WAFL Consistency Check Overdue	Warning	EMS	WAFL consistency checks on this aggregate exceeded the hourly limit.

Performance alerts

These alerts point to latency or node performance issues.

Alert name	Severity	Type	Description
Node NFS latency is high	Critical	Metric	NFS operations on this node are experiencing high latency (>5000 us).
Node panic	Critical, Warning, Info	EMS	The node panicked and was restarted.

Protection alerts

These alerts affect replication, failover, or recovery.

Alert name	Severity	Type	Description
Fanout SnapMirror relationship common snapshot deleted	Critical, Warning, Info	EMS	An older Snapshot copy is deleted as part of a SnapMirror Synchronous resynchronize or update operation.
ONTAP Mediator added	Critical, Warning, Info	EMS	The ONTAP Mediator was successfully added to this cluster.
ONTAP Mediator CA certificate expired	Critical, Warning, Info	EMS	The ONTAP Mediator certificate authority (CA) certificate has expired.
ONTAP Mediator CA certificate expiring	Critical, Warning, Info	EMS	The ONTAP Mediator certificate authority (CA) certificate is due to expire within the next 30 days.
ONTAP Mediator client certificate expired	Critical, Warning, Info	EMS	The ONTAP Mediator client certificate has expired.
ONTAP Mediator client certificate expiring	Critical, Warning, Info	EMS	The ONTAP Mediator client certificate is due to expire within the next 30 days.
ONTAP Mediator not accessible	Critical, Warning, Info	EMS	The ONTAP Mediator is not accessible, either because it has been repurposed or the Mediator package is no longer installed.
ONTAP Mediator removed	Critical, Warning, Info	EMS	The ONTAP Mediator was successfully removed from this cluster.

Alert name	Severity	Type	Description
ONTAP Mediator unreachable	Critical, Warning, Info	EMS	The ONTAP Mediator is unreachable, which means SnapMirror failover is not possible until connectivity is restored.
ONTAP Mediator server certificate expired	Critical, Warning, Info	EMS	The ONTAP Mediator server certificate has expired.
ONTAP Mediator server certificate expiring	Critical, Warning, Info	EMS	The ONTAP Mediator server certificate is due to expire within the next 30 days.
SnapMirror active sync relationship out of sync	Critical, Warning, Info	EMS	The SnapMirror synchronous relationship moved from in-sync to out-of-sync. Data protection is affected.
SnapMirror active sync automatic unplanned failover completed	Critical, Warning, Info	EMS	The SnapMirror Business Continuity (SMBC) automatic unplanned failover operation completed.
SnapMirror active sync automatic unplanned failover failed	Critical, Warning, Info	EMS	The SnapMirror Business Continuity (SMBC) automatic unplanned failover operation failed.
SnapMirror active sync planned failover completed	Critical, Warning, Info	EMS	The SnapMirror Business Continuity (SMBC) planned failover operation completed.
SnapMirror active sync planned failover failed	Critical, Warning, Info	EMS	The SnapMirror Business Continuity (SMBC) planned failover operation failed.
SnapMirror relationship common snapshot failed	Critical, Warning, Info	EMS	There is a failure in creating a common Snapshot copy.
SnapMirror relationship initialization failed	Critical, Warning, Info	EMS	The SnapMirror initialize command fails and no more retries will be attempted.
SnapMirror relationship out of sync	Critical, Warning, Info	EMS	The SnapMirror synchronous relationship moved from in-sync to out-of-sync. Data protection is affected.
SnapMirror relationship resync attempt failed	Critical, Warning, Info	EMS	A SnapMirror synchronization attempt between the source and destination volumes failed.
SnapMirror relationship snapshot is not replicated	Critical, Warning, Info	EMS	The Snapshot copy for SnapMirror Synchronous relationship is not successfully replicated.

Security alerts

These alerts point to threats or unauthorized access.

Alert name	Severity	Type	Description
Ransomware activity detected	Critical, Warning, Info	EMS	To protect the data from the detected ransomware, a Snapshot copy has been taken that can be used to restore original data.
Storage VM anti-ransomware monitoring	Critical, Warning, Info	EMS	The anti-ransomware state of the Storage VM has changed.
Unauthorized user access to admin share	Critical, Warning, Info	EMS	A client tried to connect to the privileged ONTAP_ADMIN$ share, but the logged-in user isn't part of any active Vscan scanner pool on this SVM.
Volume anti-ransomware monitoring	Critical, Warning, Info	EMS	The anti-ransomware state of a volume is changed.

Cluster security compliance categories in NetApp Console local deployment

Use this reference to review the cluster security compliance categories shown in NetApp Console local deployment, including the recommended value and whether each category affects overall compliance status.

These categories are based on ONTAP security posture checks.

Category	What the category checks	Recommended value	Affects overall compliance
Global FIPS	Whether FIPS 140-2 mode is enabled. When enabled, TLSv1 and SSLv3 are disabled and only TLSv1.1 and TLSv1.2 are allowed.	Enabled	Yes
Telnet	Whether Telnet access is enabled. SSH is the recommended secure remote access method.	Disabled	Yes
Insecure SSH settings	Whether SSH is configured with insecure ciphers, such as ciphers that begin with `cbc`.	No	Yes
Login banner	Whether a login banner is configured for system access.	Enabled	Yes
Cluster peering	Whether communication between peered clusters is encrypted. Encryption must be enabled on both source and destination clusters.	Encrypted	Yes
Network Time Protocol	Whether one or more NTP servers are configured for the cluster. NetApp recommends at least three NTP servers for resilience.	Configured	Yes
OCSP	Whether Online Certificate Status Protocol validation is enabled for SSL/TLS certificate validation.	Enabled	No

Category	What the category checks	Recommended value	Affects overall compliance
Remote audit logging	Whether log forwarding (syslog) is encrypted.	Encrypted	Yes
AutoSupport HTTPS transport	Whether HTTPS is used as the default transport protocol for AutoSupport messages.	Enabled	Yes
Default admin user	Whether the built-in default admin account is disabled.	Disabled	Yes
SAML users	Whether SAML is configured for single sign-on and MFA-capable authentication.	No	No
Active Directory users	Whether Active Directory authentication is configured for cluster access.	No	No
LDAP users	Whether LDAP authentication is configured for cluster access.	No	No
Certificate users	Whether certificate-based users are configured for cluster login.	No	No
Local users	Whether local users are configured for cluster login.	No	No
Remote shell	Whether RSH is enabled. SSH is preferred for secure remote access.	Disabled	Yes
MD5 in use	Whether ONTAP user accounts still use MD5 hashing instead of stronger hashes such as SHA-512.	No	Yes
Certificate issuer type	The certificate issuer type used by the cluster.	CA-Signed	No

Storage VM security compliance categories in NetApp Console local deployment

Use this reference to review the storage VM (SVM) security compliance categories shown in NetApp Console local deployment, including the recommended value and whether each category affects overall compliance status.

These categories are based on ONTAP security posture checks.

Category	What the category checks	Recommended value	Affects overall compliance
Audit log	Whether SVM audit logging is enabled.	Enabled	Yes
Insecure SSH settings	Whether SSH is configured with insecure ciphers, such as ciphers that begin with `cbc`.	No	Yes
Login banner	Whether a login banner is configured for users who access SVMs.	Enabled	Yes
LDAP encryption	Whether LDAP encryption is enabled.	Enabled	No
NTLM authentication	Whether NTLM authentication is enabled.	Enabled	No

Category	What the category checks	Recommended value	Affects overall compliance
LDAP payload signing	Whether LDAP payload signing is enabled.	Enabled	No
CHAP settings	Whether CHAP is enabled.	Enabled	No
Kerberos V5	Whether Kerberos V5 authentication is enabled.	Enabled	No
NIS authentication	Whether NIS authentication is configured.	Disabled	No
FPolicy status active	Whether FPolicy is created and active.	Yes	No
SMB encryption enabled	Whether SMB signing and sealing are enabled.	Yes	No
SMB signing enabled	Whether SMB signing is enabled.	Yes	No

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.