



Use multi-admin verification

StorageGRID software

NetApp
July 22, 2026

Table of Contents

- Use multi-admin verification 1
 - Learn about StorageGRID multi-admin verification 1
 - MAV configuration overview 1
 - How protected operations are handled under MAV 1
 - Configure StorageGRID multi-admin verification 1
 - Step 1: Create MAV administrator groups and users 1
 - Step 2: Enable or disable MAV 2
 - Step 3: Manage protected operations 2
 - Troubleshoot MAV email notifications 3
 - Request approval for MAV-protected operations in StorageGRID 3
 - Manage MAV-protected operations requests in StorageGRID 4

Use multi-admin verification

Learn about StorageGRID multi-admin verification

As a StorageGRID administrator, you can use multi-admin verification (MAV) to ensure that certain operations can be performed only after approvals from designated administrators. MAV helps prevent accidental or unauthorized changes to your StorageGRID system.

MAV is disabled by default.

MAV configuration overview

To configure MAV, you'll perform these tasks:

- Create one or more administrator groups. MAV administrators have approval and veto authority.
- Enable the multi-admin verification function.
- Select from a set of protected operations.

A user must have Root access permission to perform the initial configuration and make modifications later.

How protected operations are handled under MAV

When MAV is enabled, the completion of every protected operation requires these steps:

1. When a user initiates the operation, a request is generated.
2. Before the operation can be performed, at least one MAV administrator must approve.
3. When approved, the MAV-protected operation is performed automatically.

Configure StorageGRID multi-admin verification

Configuring a StorageGRID multi-admin verification (MAV) system involves creating and managing MAV administrator groups and users, enabling the MAV function, and selecting or configuring protected operations.

MAV administrators have approval and veto authority for protected operations.

Before you begin

- You have the [Root access permission](#).
- You're signed in to the Grid Manager from the primary Admin Node.

Step 1: Create MAV administrator groups and users

You can add existing administrators to a MAV group or create new administrators.

You can configure Active Directory (AD) users as MAV administrators. The AD user must be configured as a StorageGRID administrator.

Steps

1. To create a MAV administrator group, follow the steps to [create a local or federated group](#).
2. For Group permissions, select **Root access** or **Multi-admin verification requests**.
3. Add local or federated users to the group, or create new local users and add them to the group by following the steps to [create a local user](#).

Step 2: Enable or disable MAV

You must enable multi-admin verification (MAV) explicitly. If MAV is enabled and you decide to disable it when there are pending MAV requests, a notification states that pending requests will be deleted.

Steps

1. Select **Configuration > Access control > Multi-admin verification > MAV settings**.
2. Select the **Enable MAV** checkbox to enable multi-admin verification.
3. The Approver groups section lists the MAV admin groups and approvers.
4. In the Operations section, select the checkboxes for the operations you want to protect with MAV.
5. (Optional) If you want to use email notifications to alert MAV administrators of pending approval requests:
 - a. If you haven't configured an email server, follow the steps to [configure an email server](#).
 - b. Enter the email address of the sender.
 - c. Enter one or more recipients for the email notifications.
6. Select **Save** to save your changes.



If you decide not to configure email notifications, MAV administrators can view the Grid Manager dashboard or check the approval queue for pending approval requests. To check the approval queue, select **Other requests** on the Multi-admin verification page.

Step 3: Manage protected operations

After you enable multi-admin verification, you can manage the protected operations by selecting or clearing the checkboxes for the operations you want to protect with MAV.



For StorageGRID 12.1, the only protected operation is ILM policy activation. You must select the checkbox for ILM policy activation if you want to enable MAV.

A MAV request can have one of the following statuses:

- **Pending.** Request has been initiated.
- **Expired.** Request wasn't addressed within 30 days. Or a user with Root access permission disabled MAV, which means all pending requests are expired.
- **Withdrawn.** A user withdrew their request.
- **Approved.** A MAV administrator approved the pending request.
- **Rejected.** A MAV administrator rejected the pending request.

Troubleshoot MAV email notifications

If MAV administrators do not receive email notifications for pending requests, follow these steps to resolve the issue.

Before you begin

- You are signed in to the Grid Manager using a [supported web browser](#).
- You have the [Manage alerts](#) or [Root access permission](#).

Steps

1. Verify your settings.
 - a. Select **Configuration > Monitoring > Email server**.
 - b. Verify that the Email (SMTP) Server settings are correct.
 - c. Verify that you have specified valid email addresses for the recipients.
2. Check your spam filter, and make sure that the email was not sent to a junk folder.
3. Ask your email administrator to confirm that emails from the sender address aren't being blocked.
4. Collect a log file for the Admin Node, and then contact technical support.

Technical support can use the information in the logs to help determine what went wrong. For example, the `prometheus.log` file might show an error when connecting to the server you specified.

See [Collect log files and system data](#).

Request approval for MAV-protected operations in StorageGRID

As a StorageGRID administrator or user, when you initiate a MAV-protected operation in StorageGRID, a request is generated automatically. A message appears to inform you that the operation requires approval.

The StorageGRID system defines which operations are protected by MAV. When you initiate a MAV-protected operation, the request is sent to the MAV administrators for approval.

Steps

The StorageGRID system informs you that you've initiated a MAV-protected operation.

1. As needed, perform any of the following tasks:
 - a. Check the status of your request by selecting **Configuration > Access control > Multi-admin verification > My requests**.
 - **Pending**. Request has been initiated.
 - **Expired**. Request wasn't addressed within 30 days. Or a user with Root access permission disabled MAV, which means all pending requests are expired.
 - **Withdrawn**. A user withdrew their request.
 - **Approved**. A MAV administrator approved the pending request.
 - **Rejected**. A MAV administrator rejected the pending request.

- b. Check the pending requests of other users by selecting **Configuration > Access control > Multi-admin verification > Other requests**.
- c. To cancel an operation, select **My requests > *the request you want to cancel* > Withdraw**.

After a MAV administrator approves the request, the operation is performed automatically.

If your request is rejected, the operation isn't performed, and you can submit a new request if needed.

Manage MAV-protected operations requests in StorageGRID

As a MAV administrator, you can manage requests for MAV-protected operations in StorageGRID. You can view your own or others' pending requests, approve or reject requests, and view the history of past requests.

Before you begin

- You belong to a MAV administrator group and have the [Root access permission](#).
- You're signed in to the Grid Manager from the primary Admin Node.

Steps

1. If you receive an email notification about a MAV request, select **Configuration > Multi-admin verification > Other requests**.

Additionally, the Grid Manager dashboard displays a notification for pending MAV requests.

2. Select the radio button for each request you want to manage.
3. Select **Approve** or **Reject** to approve or reject the selected requests.
4. To view a history of past requests, select **History**.

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.