



# **Manage multi-admin verification**

## **ONTAP 9**

NetApp  
June 04, 2024

# Table of Contents

- Manage multi-admin verification . . . . . 1
  - Multi-admin verification overview . . . . . 1
  - Manage administrator approval groups . . . . . 9
  - Enable and disable multi-admin verification . . . . . 12
  - Manage protected operation rules . . . . . 15
  - Request execution of protected operations . . . . . 17
  - Manage protected operation requests . . . . . 21

# Manage multi-admin verification

## Multi-admin verification overview

Beginning with ONTAP 9.11.1, you can use multi-admin verification (MAV) to ensure that certain operations, such as deleting volumes or Snapshot copies, can be executed only after approvals from designated administrators. This prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data.

Configuring multi-admin verification consists of:

- [Creating one or more administrator approval groups.](#)
- [Enabling multi-admin verification functionality.](#)
- [Adding or modifying rules.](#)

After initial configuration, these elements can be modified only by administrators in a MAV approval group (MAV administrators).

When multi-admin verification is enabled, the completion of every protected operation requires these steps:

1. When a user initiates the operation, a [request is generated](#).
2. Before it can be executed, at least one [MAV administrator must approve](#).
3. Upon approval, the user completes the operation.



If you need to disable multi-admin verification functionality without MAV administrator approval, contact NetApp Support and mention the following Knowledge Base article: [How to disable Multi-Admin Verification if MAV admin is unavailable](#).

Multi-admin verification is not intended for use with volumes or workflows that involve heavy automation, because each automated task would require approval before the operation could be completed. If you want to use automation and MAV together, it's recommended to use queries for specific MAV operations. For example, you could apply `volume delete` MAV rules only to volumes where automation is not involved, and you could designate those volumes with a particular naming scheme.



Multi-admin verification is not available with Cloud Volumes ONTAP.

## How multi-admin verification works

Multi-admin verification consists of:

- A group of one or more administrators with approval and veto powers.
- A set of protected operations or commands in a *rules table*.
- A *rules engine* to identify and control execution of protected operations.

MAV rules are evaluated after role-based access control (RBAC) rules. Therefore, administrators who execute or approve protected operations must already possess the minimum RBAC privileges for those operations.

[Learn more about RBAC.](#)

## System-defined rules

When multi-admin verification is enabled, system-defined rules (also known as *guard-rail* rules) establish a set of MAV operations to contain the risk of circumventing the MAV process itself. These operations cannot be removed from the rules table. Once MAV is enabled, operations designated by an asterisk ( \* ) require approval by one or more administrators before execution, except for **show** commands.

- `security multi-admin-verify modify operation *`

Controls the configuration of multi-admin verification functionality.

- `security multi-admin-verify approval-group operations *`

Control membership in the set of administrators with multi-admin verification credentials.

- `security multi-admin-verify rule operations *`

Control the set of commands requiring multi-admin verification.

- `security multi-admin-verify request operations`

Control the approval process.

## Rule-protected commands

In addition to system-defined operations, the following commands are protected by default when multi-admin verification is enabled, but you can modify the rules to remove protection for these commands.

- `security login password`
- `security login unlock`
- `set`

Each ONTAP version provides more commands you can choose to protect with multi-admin verification rules. Choose your ONTAP release for the full list of commands available for protection.

### 9.15.1

- cluster date modify<sup>3</sup>
- cluster log-forwarding create<sup>3</sup>
- cluster log-forwarding delete<sup>3</sup>
- cluster log-forwarding modify<sup>3</sup>
- cluster peer delete
- cluster time-service ntp server create<sup>3</sup>
- cluster time-service ntp server delete<sup>3</sup>
- cluster time-service ntp server key create<sup>3</sup>
- cluster time-service ntp server key delete<sup>3</sup>
- cluster time-service ntp server key modify<sup>3</sup>
- cluster time-service ntp server modify<sup>3</sup>
- event config modify
- lun delete<sup>3</sup>
- security anti-ransomware volume attack clear-suspect<sup>1</sup>
- security anti-ransomware volume disable<sup>1</sup>
- security anti-ransomware volume pause<sup>1</sup>
- security audit modify<sup>3</sup>
- security ipsec config modify<sup>3</sup>
- security ipsec policy create<sup>3</sup>
- security ipsec policy delete<sup>3</sup>
- security ipsec policy modify<sup>3</sup>
- security login create
- security login delete
- security login modify
- security saml-sp create<sup>3</sup>
- security saml-sp delete<sup>3</sup>
- security saml-sp modify<sup>3</sup>
- snaplock legal-hold end<sup>3</sup>
- storage aggregate delete<sup>3</sup>
- storage encryption disk destroy<sup>3</sup>
- storage encryption disk modify<sup>3</sup>
- storage encryption disk revert-to-original-state<sup>3</sup>

- storage encryption disk sanitize<sup>3</sup>
- system bridge run-cli<sup>3</sup>
- system controller flash-cache secure-erase run<sup>3</sup>
- system controller service-event delete<sup>3</sup>
- system health alert delete<sup>3</sup>
- system health alert modify<sup>3</sup>
- system health policy definition modify<sup>3</sup>
- system node autosupport modify<sup>3</sup>
- system node autosupport trigger modify<sup>3</sup>
- system node coredump delete<sup>3</sup>
- system node coredump delete-all<sup>3</sup>
- system node hardware nvram-encryption modify<sup>3</sup>
- system node run
- system node systemshell
- system script delete<sup>3</sup>
- system service-processor ssh add-allowed-addresses<sup>3</sup>
- system service-processor ssh remove-allowed-addresses<sup>3</sup>
- system smtape restore<sup>3</sup>
- system switch ethernet log disable-collection<sup>3</sup>
- system switch ethernet log modify<sup>3</sup>
- timezone<sup>3</sup>
- volume create<sup>3</sup>
- volume delete
- volume encryption conversion start<sup>3</sup>
- volume encryption rekey start<sup>3</sup>
- volume file privileged-delete<sup>3</sup>
- volume flexcache delete
- volume modify<sup>3</sup>
- volume recovery-queue modify<sup>2</sup>
- volume recovery-queue purge<sup>2</sup>
- volume recovery-queue purge-all<sup>2</sup>
- volume snaplock modify<sup>1</sup>
- volume snapshot autodelete modify
- volume snapshot create<sup>3</sup>

- volume snapshot delete
- volume snapshot modify<sup>3</sup>
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename<sup>3</sup>
- volume snapshot restore
- vservice audit create<sup>3</sup>
- vservice audit delete<sup>3</sup>
- vservice audit disable<sup>3</sup>
- vservice audit modify<sup>3</sup>
- vservice audit rotate-log<sup>3</sup>
- vservice delete<sup>3</sup>
- vservice modify<sup>2</sup>
- vservice object-store-server audit create<sup>3</sup>
- vservice object-store-server audit delete<sup>3</sup>
- vservice object-store-server audit disable<sup>3</sup>
- vservice object-store-server audit modify<sup>3</sup>
- vservice object-store-server audit rotate-log<sup>3</sup>
- vservice options<sup>3</sup>
- vservice peer delete
- vservice security file-directory apply<sup>3</sup>
- vservice security file-directory remove-slag<sup>3</sup>
- vservice vscan disable<sup>3</sup>
- vservice vscan on-access-policy create<sup>3</sup>
- vservice vscan on-access-policy delete<sup>3</sup>
- vservice vscan on-access-policy disable<sup>3</sup>
- vservice vscan on-access-policy modify<sup>3</sup>
- vservice vscan scanner-pool create<sup>3</sup>
- vservice vscan scanner-pool delete<sup>3</sup>
- vservice vscan scanner-pool modify<sup>3</sup>

#### 9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect<sup>1</sup>
- security anti-ransomware volume disable<sup>1</sup>
- security anti-ransomware volume pause<sup>1</sup>
- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify<sup>2</sup>
- volume recovery-queue purge<sup>2</sup>
- volume recovery-queue purge-all<sup>2</sup>
- volume snaplock modify<sup>1</sup>
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver modify<sup>2</sup>
- vserver peer delete

#### 9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect<sup>1</sup>
- security anti-ransomware volume disable<sup>1</sup>
- security anti-ransomware volume pause<sup>1</sup>



- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify<sup>1</sup>
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vservice peer delete

#### **9.12.1/9.11.1**

- cluster peer delete
- event config modify
- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete

- `volume snapshot policy modify`
- `volume snapshot policy modify-schedule`
- `volume snapshot policy remove-schedule`
- `volume snapshot restore`
- `vserver peer delete`

1. New rule-protected command for 9.13.1
2. New rule-protected command for 9.14.1
3. New rule-protected command for 9.15.1

## How multi-admin approval works

Any time a protected operation is entered on a MAV-protected cluster, an operation execution request is sent to the designated MAV administrator group.

You can configure:

- The names, contact information, and number of administrators in the MAV group.  
A MAV administrator should have an RBAC role with cluster administrator privileges.
- The number of MAV administrator groups.
  - A MAV group is assigned for each protected operation rule.
  - For multiple MAV groups, you can configure which MAV group approves a given rule.
- The number of MAV approvals required to execute a protected operation.
- An *approval expiry* period within which a MAV administrator must respond to an approval request.
- An *execution expiry* period within which the requesting administrator must complete the operation.

Once these parameters are configured, MAV approval is required to modify them.

MAV administrators cannot approve their own requests to execute protected operations. Therefore:

- MAV should not be enabled on clusters with only one administrator.
- If there is only one person in the MAV group, that MAV administrator cannot initiate protected operations; regular administrators must initiate protected operations, and the MAV administrator can only approve.
- If you want MAV administrators to be able to execute protected operations, the number of MAV administrators must be one greater than the number of approvals required. For example, if two approvals are required for a protected operation, and you want MAV administrators to execute them, there must be three people in the MAV administrators group.

MAV administrators can receive approval requests in email alerts (using EMS) or they can query the request queue. When they receive a request, they can take one of three actions:

- Approve
- Reject (veto)
- Ignore (no action)

Email notifications are sent to all approvers associated with a MAV rule when:

- A request is created.
- A request is approved or vetoed.
- An approved request is executed.

If the requestor is in the same approval group for the operation, they will receive an email when their request is approved.



A requestor can't approve their own requests even if they are in the approval group. They can get email notifications. Requestors who are not in approval groups (that is, who are not MAV administrators) don't receive email notifications.

## How protected operation execution works

If execution is approved for a protected operation, the requesting user continues with the operation when prompted. If the operation is vetoed, the requesting user must delete the request before proceeding.

MAV rules are evaluated after RBAC permissions. As a result, a user without sufficient RBAC permissions for operation execution cannot initiate the MAV request process.

## Manage administrator approval groups

Before enabling multi-admin verification (MAV), you must create an admin approval group containing one or more administrators to be granted approve or veto authority. Once you have enabled multi-admin verification, any modifications to approval group membership requires approval from one of the existing qualified administrators.

### About this task

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


MAV functionality honors existing role-based access control (RBAC) settings. Potential MAV administrators must have sufficient privilege to execute protected operations before they are added to MAV administrator groups. [Learn more about RBAC.](#)

You can configure MAV to alert MAV administrators that approval requests are pending. To do so, you must configure email notifications—in particular, the `Mail From` and `Mail Server` parameters—or you can clear these parameters to disable notification. Without email alerts, MAV administrators must check the approval queue manually.

## System Manager procedure

If you want to create a MAV approval group for the first time, see the System Manager procedure to [enable multi-admin verification](#).


To modify an existing approval group or create an additional approval group:

1. Identify administrators to receive multi-admin verification.
  - a. Click **Cluster > Settings**.
  - b. Click  next to **Users and Roles**.

- c. Click **+ Add** under **Users**.
- d. Modify the roster as needed.

For more information, see [Control administrator access](#).

## 2. Create or modify the MAV approval group:

- a. Click **Cluster > Settings**.
- b. Click **→** next to **Multi-Admin Approval** in the **Security** section. (You will see the  icon if MAV is not yet configured.)
  - Name: enter a group name.
  - Approvers: select approvers from a list of users.
  - Email address: enter email address(es).
  - Default group: select a group.

MAV approval is required to edit an existing configuration once MAV is enabled.

## CLI procedure

### 1. Verify that values have been set for the Mail From and Mail Server parameters. Enter:

```
event config show
```

The display should be similar to the following:

```
cluster01::> event config show
                        Mail From:  admin@localhost
                        Mail Server: localhost
                        Proxy URL:   -
                        Proxy User:  -
                        Publish/Subscribe Messaging Enabled: true
```

To configure these parameters, enter:

```
event config modify -mail-from email_address -mail-server server_name
```

### 2. Identify administrators to receive multi-admin verification

If you want to...	Enter this command
Display current administrators	<code>security login show</code>
Modify credentials of current administrators	<code>security login modify &lt;parameters&gt;</code>
Create new administrator accounts	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

### 3. Create the MAV approval group:

```
security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name -approvers approver1[,approver2...] [[-email address1], address1...]
```

- -vserver - Only the admin SVM is supported in this release.
- -name - The MAV group name, up to 64 characters.
- -approvers - The list of one or more approvers.
- -email - One or more email addresses that are notified when a request is created, approved, vetoed, or executed.

**Example:** The following command creates a MAV group with two members and associated email addresses.

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email
pavan@myfirm.com,julia@myfirm.com
```

### 4. Verify group creation and membership:

```
security multi-admin-verify approval-group show
```

**Example:**

```
cluster-1::> security multi-admin-verify approval-group show
Vserver   Name           Approvers      Email
-----
svm-1     mav-grp1      pavan,julia    email
pavan@myfirm.com,julia@myfirm.com
```

Use these commands to modify your initial MAV group configuration.

**Note:** All require MAV administrator approval before execution.

If you want to...	Enter this command
Modify the group characteristics or modify existing member information	<code>security multi-admin-verify approval-group modify [<i>parameters</i>]</code>
Add or remove members	<code>security multi-admin-verify approval-group replace [-vserver <i>svm_name</i>] -name <i>group_name</i> [-approvers-to-add <i>approver1[,approver2...]</i>] [-approvers-to-remove <i>approver1[,approver2...]</i>]</code>

If you want to...	Enter this command
Delete a group	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

## Enable and disable multi-admin verification

Multi-admin verification (MAV) must be enabled explicitly. Once you have enabled multi-admin verification, approval by administrators in a MAV approval group (MAV administrators) is required to delete it.

### About this task

Once MAV is enabled, modifying or disabling MAV requires MAV administrator approval.



If you need to disable multi-admin verification functionality without MAV administrator approval, contact NetApp Support and mention the following Knowledge Base article: [How to disable Multi-Admin Verification if MAV admin is unavailable](#).

When you enable MAV, you can specify the following parameters globally.

### Approval groups

A list of global approval groups. At least one group is required to enable MAV functionality.



If you are using MAV with Autonomous Ransomware Protection (ARP), define a new or existing approval group that is responsible for approving ARP pause, disable, and clear suspect requests.

### Required approvers

The number of approvers required to execute a protected operation. The default and minimum number is 1.



The required number of approvers must be less than the total number of unique approvers in the default approval groups.

### Approval expiry (hours, minutes, seconds)

The period within which a MAV administrator must respond to an approval request. The default value is one hour (1h), the minimum supported value is one second (1s), and the maximum supported value is 14 days (14d).



### Execution expiry (hours, minutes, seconds)

The period within which the requesting administrator must complete the operation. The default value is one hour (1h), the minimum supported value is one second (1s), and the maximum supported value is 14 days (14d).

You can also override any of these parameters for specific [operation rules](#).



## System Manager procedure

1. Identify administrators to receive multi-admin verification.

- a. Click **Cluster > Settings**.
- b. Click  next to **Users and Roles**.
- c. Click  **Add** under **Users**.
- d. Modify the roster as needed.

For more information, see [Control administrator access](#).

2. Enable multi-admin verification by creating at least one approval group and adding at least one rule.


- a. Click **Cluster > Settings**.
- b. Click  next to **Multi-Admin Approval** in the **Security** section.
- c. Click  **Add** to add at least one approval group.
  - Name – Enter a group name.
  - Approvers – Select approvers from a list of users.
  - Email address – Enter email address(es).
  - Default group – Select a group.
- d. Add at least one rule.
  - Operation – Select a supported command from the list.
  - Query – Enter any desired command options and values.
  - Optional parameters; leave blank to apply global settings, or assign a different value for specific rules to override the global settings.
    - Required number of approvers
    - Approval groups
- e. Click **Advanced Settings** to view or modify defaults.
  - Required number of approvers (default: 1)
  - Execution request expiry (default: 1 hour)
  - Approval request expiry (default: 1hour)
  - Mail server\*
  - From email address\*

\*These update the email settings managed under "Notification Management". You are prompted to set them if they have not yet been configured.


- f. Click **Enable** to complete MAV initial configuration.

After initial configuration, the current MAV status is displayed in the **Multi-Admin Approval** tile.

- Status (enabled or not)
- Active operations for which approvals are required
- Number of open requests in pending state

You can display an existing configuration by clicking . MAV approval is required to edit an existing configuration.

To disable multi-admin verification:

1. Click **Cluster > Settings**.
2. Click  next to **Multi-Admin Approval** in the **Security** section.
3. Click the Enabled toggle button.

MAV approval is required to complete this operation.

## CLI procedure

Before enabling MAV functionality at the CLI, at least one [MAV administrator group](#) must have been created.

If you want to...	Enter this command
Enable MAV functionality	<pre>security multi-admin-verify modify   -approval-groups <i>group1</i> [, <i>group2</i>...] [-   required-approvers <i>nn</i> ] -enabled true [   -execution-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]] [   -approval-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]]</pre> <p><b>Example :</b> the following command enables MAV with 1 approval group, 2 required approvers, and default expiry periods.</p> <pre>cluster-1::&gt; security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> <p>Complete initial configuration by adding at least one <a href="#">operation rule</a>.</p>
Modify a MAV configuration (requires MAV approval)	<pre>security multi-admin-verify approval- group modify [-approval-groups <i>group1</i> [, <i>group2</i>...]] [-required-approvers <i>nn</i> ] [ -execution-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]] [ -approval-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]]</pre>



If you want to...	Enter this command
Verify MAV functionality	<pre>security multi-admin-verify show</pre> <p><b>Example:</b></p> <pre>cluster-1::&gt; security multi-admin-verify show Is          Required  Execution Approval Approval Enabled Approvers Expiry      Expiry Groups ----- true        2          1h         1h mav-grp1</pre>
Disable MAV functionality (requires MAV approval)	<pre>security multi-admin-verify modify -enabled false</pre>

## Manage protected operation rules

You create multi-admin verification (MAV) rules to designate operations requiring approval. Whenever an operation is initiated, protected operations are intercepted and a request for approval is generated.

Rules can be created before enabling MAV by any administrator with appropriate RBAC capabilities, but once MAV is enabled, any modification to the rule set requires MAV approval.

Only one MAV rule can be created per operation; for example, you cannot make multiple `volume-snapshot-delete` rules. Any desired rule constraints must be contained within one rule.

You can create rules to protect [these commands](#). You can protect each command beginning with the ONTAP version in which protection capability for the command first became available.

The rules for MAV system-default commands, the `security multi-admin-verify` [commands](#), cannot be altered.

In addition to system-defined operations, the following commands are protected by default when multi-admin verification is enabled, but you can modify the rules to remove protection for these commands.

- `security login password`
- `security login unlock`
- `set`

## Rule constraints

When you create a rule, you can optionally specify the `-query` option to limit the request to a subset of the command functionality. The `-query` option can also be used to limit configuration elements, such as the SVM, the volume, and Snapshot names.

For example, in the `volume snapshot delete` command, `-query` can be set to `-snapshot !hourly*,!daily*,!weekly*`, meaning that volume Snapshots prefixed with hourly, daily, or weekly attributes are excluded from MAV protections.

```
smci-vsimg20::> security multi-admin-verify rule show
```

Vserver	Operation	Required Approvers	Approval Groups
vs01	volume snapshot delete	-	-
	Query: -snapshot !hourly*,!daily*,!weekly*		



Any excluded configuration elements would not be protected by MAV, and any administrator could delete or rename them.

By default, rules specify that a corresponding `security multi-admin-verify request create "protected_operation"` command is generated automatically when a protected operation is entered. You can modify this default to require that the `request create` command be entered separately.



By default, rules inherit the following global MAV settings, although you can specify rule-specific exceptions:

- Required Number of Approvers
- Approval Groups
- Approval Expiry period
- Execution Expiry period

## System Manager procedure

If you want to add a protected operation rule for the first time, see the System Manager procedure to [enable multi-admin verification](#).

To modify the existing rule set:

1. Select **Cluster > Settings**.
2. Select  next to **Multi-Admin Approval** in the **Security** section.
3. Select  **Add** to add at least one rule; you can also modify or delete existing rules.
  - Operation – Select a supported command from the list.
  - Query – Enter any desired command options and values.
  - Optional parameters – Leave blank to apply global settings, or assign a different value for specific rules to override the global settings.
    - Required number of approvers

- Approval groups

## CLI procedure



All `security multi-admin-verify rule` commands require MAV administrator approval before execution except `security multi-admin-verify rule show`.

If you want to...	Enter this command
Create a rule	<code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code>
Modify credentials of current administrators	<code>security login modify &lt;parameters&gt;</code>  <b>Example:</b> the following rule requires approval to delete the root volume.  <code>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</code>
Modify a rule	<code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code>
Delete a rule	<code>security multi-admin-verify rule delete -operation "protected_operation"</code>
Show rules	<code>security multi-admin-verify rule show</code>

For command syntax details, see the `security multi-admin-verify rule` man pages.

## Request execution of protected operations

When you initiate a protected operation or command on a cluster enabled for multi-admin verification (MAV), ONTAP automatically intercepts the operation and asks to generate a request, which must be approved by one or more administrators in a MAV approval group (MAV administrators). Alternatively, you can create a MAV request without the dialog.

If approved, you must then respond to the query to complete the operation within the request expiry period. If vetoed, or if the request or expiry periods are exceeded, you must delete the request and resubmit.

MAV functionality honors existing RBAC settings. That is, your administrator role must have sufficient privilege to execute a protected operation without regard to MAV settings. [Learn more about RBAC](#).

If you are a MAV administrator, your requests to execute protected operations must also be approved by a MAV administrator.

## System Manager procedure

When a user clicks on a menu item to initiate an operation and the operation is protected, a request for approval is generated and the user receives a notification similar to the following:

```
Approval request to delete the volume was sent.  
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

The **Multi-Admin Requests** window is available when MAV is enabled, showing pending requests based on the user's login ID and MAV role (approver or not). For each pending request, the following fields are displayed:

- Operation
- Index (number)
- Status (Pending, Approved, Rejected, Executed, or Expired)

If a request is rejected by one approver, no further actions are possible.

- Query (any parameters or values for the requested operation)
- Requesting User
- Request Expires On
- (Number of) Pending Approvers
- (Number of) Potential Approvers

When the request is approved, the requesting user can retry the operation within the expiry period.

If the user retries the operation without approval, a notification is displayed similar to the following:

```
Request to perform delete operation is pending approval.  
Retry the operation after request is approved.
```

## CLI procedure

1. Enter the protected operation directly or using the MAV request command.

**Examples – to delete a volume, enter one of the following commands:**

```
° volume delete
```

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

```
Warning: This operation requires multi-admin verification. To create a
```

```
verification request use "security multi-admin-verify request create".
```

```
Would you like to create a request for this operation?  
{y|n}: y
```

```
Error: command failed: The security multi-admin-verify request (index 3) is  
auto-generated and requires approval.
```

```
° security multi-admin-verify request create "volume delete"
```

```
Error: command failed: The security multi-admin-verify request (index 3)  
requires approval.
```

2. Check the status of the request and respond to the MAV notice.
  - a. If the request is approved, respond to the CLI message to complete the operation.

**Example:**

```
cluster-1::> security multi-admin-verify request show 3
```

```
    Request Index: 3
      Operation: volume delete
        Query: -vserver vs0 -volume voll
        State: approved
Required Approvers: 1
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: admin2
    User Vetoed: -
      Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
    Comment: -
  Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

Info: Volume "voll" in Vserver "vs0" will be marked as deleted and placed in the volume recovery queue. The space used by the volume will be recovered only after the retention period of 12 hours has completed. To recover the space immediately, get the volume name using (privilege:advanced) "volume recovery-queue show voll\_\*" and then "volume recovery-queue purge -vserver vs0 -volume <volume\_name>" command. To recover the volume use the (privilege:advanced) "volume recovery-queue recover -vserver vs0 -volume <volume\_name>" command.

Warning: Are you sure you want to delete volume "voll" in Vserver "vs0" ?  
{y|n}: y

- b. If the request is vetoed, or the expiry period has passed, delete the request, and either resubmit or contact the MAV administrator.

**Example:**

```
cluster-1::> security multi-admin-verify request show 3
```

```
    Request Index: 3
      Operation: volume delete
        Query: -vserver vs0 -volume voll
        State: vetoed
Required Approvers: 1
Pending Approvers: 1
  Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
    Approvals: -
    User Vetoed: admin2
      Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:38:47
  Time Approved: -
    Comment: -
  Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

```
Error: command failed: The security multi-admin-verify request (index
3) hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

## Manage protected operation requests

When administrators in a MAV approval group (MAV administrators) are notified of a pending operation execution request, they must respond with an approve or veto message within a fixed time period (approval expiry). If a sufficient number of approvals are not received, the requester must delete the request and make another.

### About this task

Approval requests are identified with index numbers, which are included in email messages and displays of the request queue.

The following information from the request queue can be displayed:

### Operation

The protected operation for which the request is created.

### Query

The object (or objects) upon which the user wants to apply the operation.

**State**

The current state of the request; pending, approved, rejected, expired, executed. If a request is rejected by one approver, no further actions are possible.

**Required approvers**

The number of MAV administrators that are required to approve the request. A user can set the required-approvers parameter for the operation rule. If a user does not set the required-approvers to the rule, then the required-approvers from the global setting is applied.

**Pending approvers**

The number of MAV administrators that are still required to approve the request for the request to be marked as approved.

**Approval expiry**

The period within which a MAV administrator must respond to an approval request. Any authorized user can set the approval-expiry for an operation rule. If approval-expiry is not set for the rule, then the approval-expiry from the global setting is applied.

**Execution expiry**

The period within which the requesting administrator must complete the operation. Any authorized user can set the execution-expiry for an operation rule. If execution-expiry is not set for the rule, then the execution-expiry from the global setting is applied.

**Users approved**

The MAV administrators who have approved the request.

**User vetoed**

The MAV administrators who have vetoed the request.

**Storage VM (vserver)**

The SVM with which the request is associated with. Only the admin SVM is supported in this release.

**User requested**

The username of the user who created the request.

**Time created**

The time when the request is created.

**Time approved**

The time when the request state changed to approved.

**Comment**

Any comments that are associated with the request.

**Users permitted**

The list of users permitted to perform the protected operation for which the request is approved. If `users-permitted` is empty, then any user with appropriate permissions can perform the operation.

All expired or executed requests are deleted when a limit of 1000 requests is reached, or when the expired time is greater than 8hrs for expired requests. Vetoed requests are deleted once they are marked as expired.



## System Manager procedure

MAV administrators receive email messages with details of the approval request, request expiry period, and a link to approve or reject the request. They can access an approval dialog by clicking the link in the email or navigate to **Events & Jobs>Requests** in System Manager.

The **Requests** window is available when multi-admin verification is enabled, showing pending requests based on the user's login ID and MAV role (approver or not).

- Operation
- Index (number)
- Status (Pending, Approved, Rejected, Executed, or Expired)

If a request is rejected by one approver, no further actions are possible.

- Query (any parameters or values for the requested operation)
- Requesting User
- Request Expires On
- (Number of) Pending Approvers
- (Number of) Potential Approvers

MAV administrators have additional controls in this window; they can approve, reject, or delete individual operations, or selected groups of operations. However, if the MAV administrator is the Requesting User, they cannot approve, reject or delete their own requests.

## CLI procedure

1. When notified of pending requests by email, note the request's index number and approval expiry period. The index number can also be displayed using the **show** or **show-pending** options mentioned below.
2. Approve or veto the request.

If you want to...	Enter this command
Approve a request	<code>security multi-admin-verify request approve nn</code>
Veto a request	<code>security multi-admin-verify request veto nn</code>
Show all requests, pending requests, or a single request	<code>security multi-admin-verify request { show   show-pending } [nn] { -fields field1[,field2...]   [-instance ] }</code>  You can show all requests in the queue or only pending requests. If you enter the index number, only information for that is displayed. You can display information about specific fields (by using the <code>-fields</code> parameter) or about all fields (by using the <code>-instance</code> parameter).

If you want to...	Enter this command
Delete a request	security multi-admin-verify request delete nn

### Example:

The following sequence approves a request after the MAV administrator has received the request email with index number 3, which already has one approval.

```

cluster1::> security multi-admin-verify request show-pending
Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete -    pending 1      julia

cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
Operation: volume delete
Query: -
State: approved
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
Approvals: mav-admin2
User Vetoed: -
Vserver: cluster-1
User Requested: julia
Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
Comment: -
Users Permitted: -

```

### Example:

The following sequence vetoes a request after the MAV administrator has received the request email with index number 3, which already has one approval.

```
cluster1::> security multi-admin-verify request show-pending
```

Index	Operation	Query	State	Approvers	Requestor
3	volume delete	-	pending	1	pavan

```
cluster-1::> security multi-admin-verify request veto 3
```

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
```

```
Operation: volume delete
```

```
Query: -
```

```
State: vetoed
```

```
Required Approvers: 2
```

```
Pending Approvers: 0
```

```
Approval Expiry: 2/25/2022 14:32:03
```

```
Execution Expiry: 2/25/2022 14:35:36
```

```
Approvals: mav-admin1
```

```
User Vetoed: mav-admin2
```

```
Vserver: cluster-1
```

```
User Requested: pavan
```

```
Time Created: 2/25/2022 13:32:03
```

```
Time Approved: 2/25/2022 13:35:36
```

```
Comment: -
```

```
Users Permitted: -
```

## 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.