All Clusters View

SolidFire Active IQ

NetApp
October 02, 2025

Table of Contents

All Clusters View

All Clusters View

The **All Clusters View** is the landing page for SolidFire Active IQ.

Learn about what you can access from the **All Clusters View**:

- All Clusters View dashboard
- Alerts
- Capacity Licensing
- Term Capacity

Find more information

NetApp Product Documentation

All Clusters View Dashboard

All Clusters View dashboard

On the **Dashboard** page of the **All Clusters View**, you can view performance, capacity, and cluster statistic details about the clusters associated with your account.

Heading	Description
Company	Company name assigned to the cluster.
Cluster	Name assigned to the cluster.
Cluster ID	Assigned cluster number when the cluster is created.
Version	Version of the cluster master running on each node.
Nodes	Number of nodes in the cluster.
Volumes	Number of volumes in the cluster.
Efficiency	The amount of efficiency the system is seeing due to compression, deduplication, and thin provisioning.
Used Block Capacity	Current used capacity of the cluster block.
Faults	Number of currently unresolved faults detected on the cluster.
SVIP	Storage virtual IP address assigned to the cluster.
MVIP	Management Virtual IP address assigned to the cluster.
Last Update	Time and date that the most recent cluster update.
Actions	Options to request upgrade support for a cluster, archive a cluster, and suppress a cluster

ⓘ	If the cluster you are looking for is unavailable, be aware that clusters that have been inactive for 180 days or more are automatically archived. Contact support for further assistance.

Find more information

[NetApp Product Documentation](#)

Cluster Actions

On the **Dashboard** page of the **All Clusters View**, you can view the cluster support options about the clusters associated with your account.

Steps

1. Select **All Clusters View** > **Overview**.

2. In the **Actions** column, select the ⋮ icon for the cluster you want.

3. Select one of the following options:

    a. **Request Upgrade Support** sends a request for an upgrade of the cluster software. You can select element software, storage firmware, compute firmware, or the management node management services. You enter your contact information, any comments, and a callback time.

Request Support Upgrade Assistance for Cluster ❓ ✖

Current Cluster Version: **12.7.0.380**

Element Software ☐	Storage Firmware ☐	Compute Firmware ☐	mNode Management Services ☐

Contact Name *

Contact Email *

Contact Phone

Comments

Requested Callback Time *   `2025-09-18 14:18:00  ∨`

Submit   **Cancel**

---

b. **Archive Cluster** archives the cluster. A window opens providing warnings about the issues around archiving a cluster that might need to be unarchived at a later date.

Archive Cluster ✖

Are you sure you want to archive cluster SF_Cluster1 ?

Notice:
- Cluster Archival is *not* to be used to temporarially silence a noisy cluster.
- Restoring an archived cluster will have undefined ramifications.
- Future payloads from SF_Cluster1 will be ignored. Data will stop being ingested into Active IQ.
- Access to pages for SF_Cluster1 will be denied, and it will be removed from the All Cluster Dashboard View.
- Every effort will be made to stop and clear alerts for SF_Cluster1 . However, alerts may trigger while archival is being processed.
- The Active IQ development team reserves the right to delete data associated with archived clusters, at any time, and with no notice.

Are you sure you want to continue?

Archive Cluster   Cancel

c. **Suppress Cluster** stops repeated alerts. You choose alert type, start time, and duration. You can also see currently running alert suppression rules on this window.
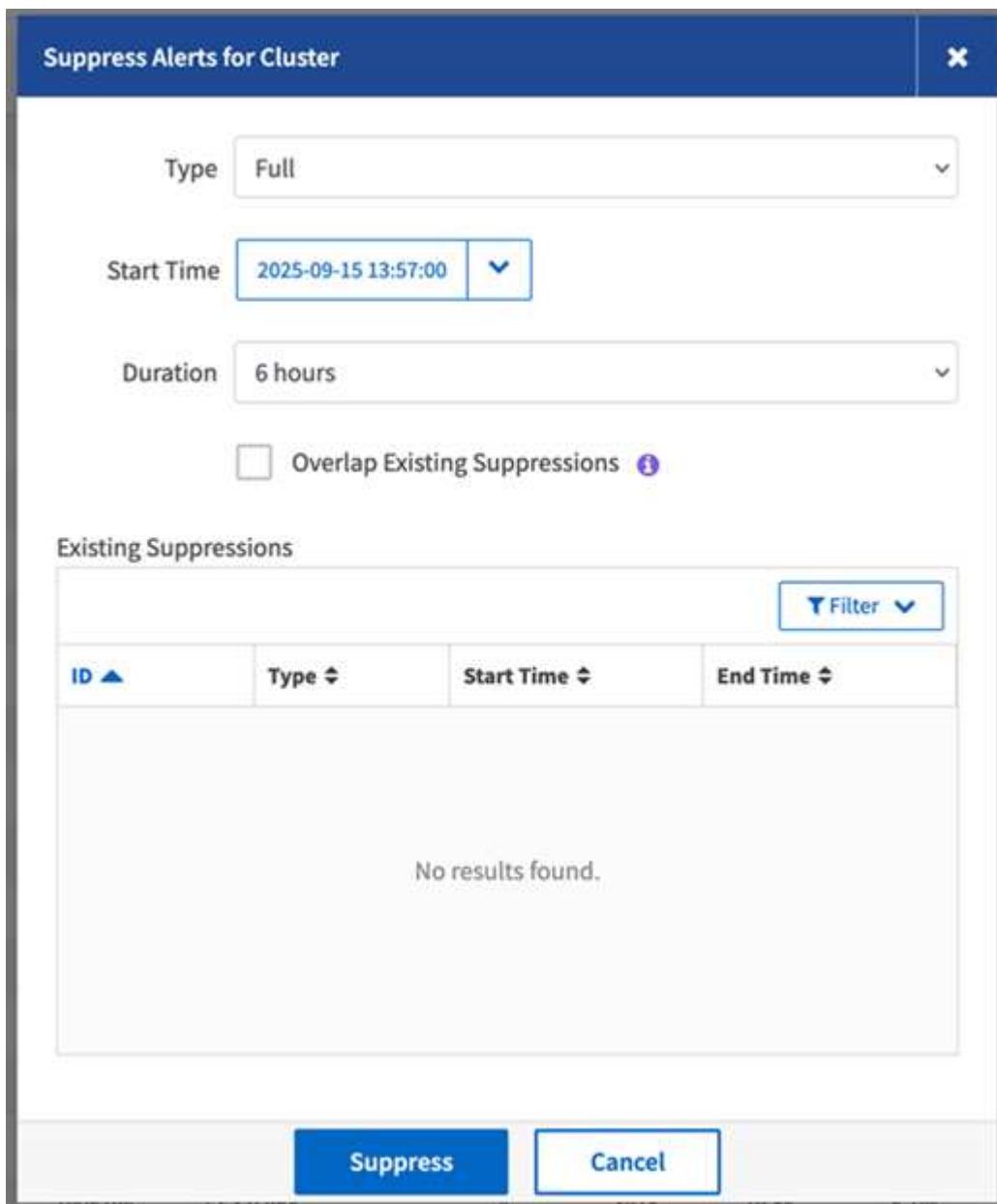
See Suppress Cluster Notifications for more information.

ⓘ   If the cluster you are looking for is unavailable, be aware that clusters that have been inactive for 180 days or more are automatically archived. Contact support for further assistance.

Find more information

NetApp Product Documentation

Alerts

From the **Alerts** drop-down menu within **All Clusters View**, you can view the alert

history, create and manage alert policies, and view and suppress cluster notifications.

Learn about or perform alerts-related tasks:

- View alerts history
- Alerts history details
- View alert policies
- Create an alert policy
- Alert policy types
- Edit an alert policy
- Delete an alert policy
- View suppressed clusters
- Suppress cluster notifications
- End cluster suppression from a cluster
- Alert notification email

View alerts history

You can view the history for either unresolved or resolved alerts.

Steps

1. Select **Alerts** > **History**.
2. Select either the **Unresolved** or **Resolved** tab to view the history of alerts for the cluster.
3. (Optional) Select the ![download icon] icon to export the data to a CSV file.

Alerts history details

The **History** page in the Alerts drop-down menu within All Clusters View shows up to 10000 entries of alert history, including all unresolved alerts and alerts resolved in the last 30 days.

The following list describes the details that are available to you:

Heading	Description
Alert ID	Unique ID for each alert.
Triggered	The time the alert was triggered in SolidFire Active IQ, not on the cluster itself.
Last Notified	The time the most recent alert email was sent.
Resolved	Shows if the cause of the alert has been resolved.
Resolution Time	The time an issue was resolved.
Policy	This is the user-defined alert policy name.
Severity	Severity assigned at the time the alert policy was created.
Destination	The email address or addresses selected to receive the alert email.
Company	Name of customer associated with the alert.

Heading	Description
Cluster	Displays the cluster name for which the alert policy was added.
Trigger	The user-defined setting that triggered the alert.

View alert policies

The **Policies** page in the Alerts drop-down menu within All Clusters View shows the following policy information for all clusters.

The following list describes the details that are available to you:

Heading	Description
Policy Name	User-defined alert policy name.
Destination	Email address defined in the alert policy.
Severity	Severity assigned in the alert policy.
Clusters	Number and name of each cluster defined in the alert policy. Select the information icon to reveal associated clusters.
Condition	User-defined setting for when an alert should be triggered.
Suppression Types	Determines which alerts and events are suppressed. The following types are possible: • **Full**: All alerts for the cluster are suppressed for the duration specified. No support cases or email alerts are generated. • **Upgrades**: Non-critical cluster alerts are suppressed for the duration specified. Critical alerts still generate support cases and emails. • **Compute**: Alerts that are triggered by VMware on the compute nodes are suppressed. • **NodeHardware**: Alerts associated with node maintenance are suppressed. For example, swapping out drives or taking nodes offline. • **Drive**: Alerts associated with drive health are suppressed. • **Network**: Alerts associated with network configuration and health are suppressed. • **Power**: Power redundancy alerts are suppressed. It does not suppress a *nodeOffline* alert which would occur in the event of a total power loss.
Actions	Select the vertical drop-down menu for edit and delete options for the selected policy.

Create an alert policy

You can create an alert policy to monitor information from the **All Clusters View** in SolidFire Active IQ. Alert policies allow you to be notified of a status or performance event with one or more clusters across an installation so that action can be taken in advance of, or in response to, a more serious event.

Steps

1. Select **Alerts** > **Policies**.
2. Select **Create Policy**.
3. Select an alert type from the **Policy Type** list. See Alert policy types.

   > ℹ️ There are additional policy-specific fields within the **Create Policy** dialog box depending on the policy type selected.

4. Enter a name for the new alert policy.

   > ℹ️ Alert policy names should describe the condition the alert is being created for. Descriptive titles help identify the alert easily. Alert policy names are displayed as a reference elsewhere in the system.

5. Select a severity level.

   > 💡 Alert policy severity levels are color coded and can be filtered easily from the **Alerts** > **History page**.

6. Determine the type of suppression for the alert policy by selecting a type from **Suppressible Types**. You can select more than one type.

   Confirm that the associations make sense. For example, you have selected **Network Suppression** for a network alert policy.

7. Select one or more clusters to include in the policy.

   > ⚠️ When you add a new cluster to your installation after you have created the policy, the cluster will not automatically be added to existing alert policies. You must edit an existing alert policy and select the new cluster you want to associate with the policy.

8. Enter one or more email addresses to which alert notifications will be sent. If you are entering multiple addresses, you must use a comma to separate each address.
9. Select **Save Alert Policy**.

Alert policy types

You can create alert policies based on available policy types listed in the **Create Policy** dialog box from **Alarms** > **Policies**.

Available policy alerts include the following types:

Policy Type	Description
Cluster Fault	Sends a notification when a specific type or any type of cluster fault occurs.
Event	Sends a notification when a specific event type occurs.
Failed Drive	Sends a notification when a drive failure occurs.
Available Drive	Sends a notification when a drive comes online in *Available* state.
Cluster Utilization	Sends a notification when the cluster capacity and performance being used is more than the specified percentage.

Policy Type	Description
Usable Space	Sends a notification when usable cluster space is less than a specified percentage.
Provisionable Space	Sends a notification when provisionable cluster space is less than a specified percentage.
Collector Not Reporting	Sends a notification when the collector for SolidFire Active IQ that runs on the management node fails to send data to SolidFire Active IQ for the duration specified.
Drive Wear	Sends a notification when a drive in a cluster has less than a specified percentage of wear or reserve space remaining.
iSCSI Sessions	Sends a notification when the number of active iSCSI sessions is greater than the value specified.
Chassis Resiliency	Sends a notification when the used space of a cluster is greater than a user-specified percentage. You should select a percentage that is sufficient to give early notice before reaching the cluster resiliency threshold. After reaching this threshold, a cluster can no longer automatically heal from a chassis-level failure.
VMware Alarm	Sends a notification when a VMware alarm is triggered and reported to SolidFire Active IQ.
Custom Protection Domain Resiliency	When used space increases beyond the specified percentage of custom protection domain resiliency threshold, the system sends a notification. If this percentage reaches 100, the storage cluster does not have enough free capacity to self-heal after a custom protection domain failure occurs.
Node Core/Crash Dump Files	When a service becomes unresponsive and must be restarted, the system creates a core file or crash dump file and sends a notification. This is not the expected behavior during regular operations.

Edit an alert policy

You can edit an alert policy to add or remove clusters from a policy or change additional policy settings.

Steps

1. Select **Alerts** > **Policies**.

2. Select the menu for more options under **Actions**.

3. Select **Edit Policy**.

   > The policy type and type-specific monitoring criteria are not editable.

4. (Optional) Enter a revised name for the new alert policy.

   > Alert policy names should describe the condition the alert is being created for. Descriptive titles help identify the alert easily. Alert policy names are displayed as a reference elsewhere in the system.

5. (Optional) Select a different severity level.

> 💡 Alert policy severity levels are color coded and can be filtered easily from the Alerts > History page.

6. Determine the type of suppression for the alert policy when it is active by selecting a type from **Suppressible Types**. You can select more than one type.

   Confirm that the associations make sense. For example, you have selected **Network Suppression** for a network alert policy.

7. (Optional) Select or remove cluster associations with the policy.

> ⚠️ When you add a new cluster to your installation after you have created the policy, the cluster is not automatically be added to existing alert policies. You must select the new cluster you want to associate with the policy.

8. (Optional) Modify one or more email addresses to which alert notifications will be sent. If you are entering multiple addresses, you must use a comma to separate each address.

9. Select **Save Alert Policy**.

Delete an alert policy

Deleting an alert policy removes it permanently from the system. Email notifications are no longer sent for that policy and cluster associations with the policy are removed.

Steps

1. Select **Alerts** > **Policies**.

2. Under **Actions**, select the menu for more options.

3. Select **Delete Policy**.

4. Confirm the action.

   The policy is permanently removed from the system.

View suppressed clusters

On the **Suppressed Clusters** page in the Alerts drop-down menu within the All Clusters View, you can view a list of clusters which have alert notifications suppressed.

NetApp Support or customers can suppress alert notifications for a cluster when performing maintenance. When notifications are suppressed for a cluster using upgrade suppression, common alerts that occur during upgrades are not sent. There is also a full alert suppression option that stops alert notification for a cluster for a specified duration. You can view any email alerts that are not sent when notifications are suppressed on the **History** page of the **Alerts** menu. Suppressed notifications resume automatically after the defined duration elapses. You can end suppression of notifications early by selecting "resume notifications" in the dropdown menu.

On the **Suppressed Clusters** page, you have the option to view the following information for **Past**, **Active**, and **Future** suppressions. The **Past** option shows the suppressions that ended in the last 90 days.

Heading	Description
Company	Company name assigned to the cluster.

Heading	Description
Cluster ID	Assigned cluster number when the cluster is created.
Cluster Name	Name assigned to the cluster.
Created By	The account username that created the suppression.
Created Time	The exact time that the suppression was created.
Updated Time	If the suppression was modified after it was created, this is the exact time that the suppression was last changed.
Start Time	The exact time that the suppression of notifications started or is scheduled to start.
End Time	The exact time that the suppression of notifications is scheduled to end.
Type	Determines which alerts and events are suppressed. The following types are possible: • **Full**: All alerts for the cluster are suppressed for the duration specified. No support cases or email alerts are generated. • **Upgrades**: Non-critical cluster alerts are suppressed for the duration specified. Critical alerts still generate support cases and emails. • **Compute**: Alerts that are triggered by VMware on the compute nodes are suppressed. • **NodeHardware**: Alerts associated with node maintenance are suppressed. For example, swapping out drives or taking nodes offline. • **Drive**: Alerts associated with drive health are suppressed. • **Network**: Alerts associated with network configuration and health are suppressed. • **Power**: Power redundancy alerts are suppressed. It does not suppress a *nodeOffline* alert which would occur in the event of a total power loss.
Status	Indicates the status of an alert notification: • **Active**: Suppression of alert notifications is active. • **Future**: Suppression of alert notifications is scheduled for a future date and time.
Scheduled	Indicates if the suppression was scheduled when it was created: • **True**: The Created Time and Start Time values are the same. • **False**: The Created Time and Start Time values are different.

Suppress cluster notifications

You can suppress alert notifications at the cluster level for a single cluster or multiple clusters for the current date and time or schedule to start at a future date and time.

Steps

1. Do one of the following:
   a. From the **Dashboard** overview, select the Actions menu for the cluster that you want to suppress.
   b. From **Alerts** > **Cluster Suppression**, select **Suppress Clusters**.
2. In the **Suppress Alerts for Cluster** dialog box, do the following:
   a. If you selected the **Suppress Clusters** button from the **Suppressed Clusters** page, select a cluster.
   b. Select an alert suppression type as either **Full**, **Upgrades**, **Compute**, **NodeHardware**, **Drive**, **Network** or **Power**. Learn about suppression types.

   > (i) A cluster can have multiple suppression types, which can include multiple selections of the same suppression type. When a suppression type already exists during a scheduled suppression window, it is greyed out. To select this suppression type again, select **Overlap Existing**. Multiple selections of the same suppression type can have overlapping times or, if scheduling future suppressions, be at different times. When two suppressions have overlapping time periods, the functionality is the same as having a single suppression with a start time starting at the earliest of the suppressions and an end time ending at the latest.

   c. Select the start date and time that you want the suppression of notifications to start.
   d. Select a common duration or enter a custom end date and time during which notifications should be suppressed.
3. Select **Suppress**.

   > (i) This action also suppresses certain or all notifications to NetApp Support. After cluster suppression is in effect, NetApp Support or any user that is entitled to view the cluster can update the suppression state.

End cluster suppression from a cluster

You can end cluster alert suppression on clusters that was applied using the Suppress Clusters feature. This enables clusters to resume their normal state of alert reporting.

Steps
1. From the **Dashboard** overview or **Alerts** > **Cluster Suppression**, end suppression for the single or multiple clusters that you want to resume normal alert reporting:
   a. For a single cluster, select the Actions menu for the cluster and select **End Suppression**.
   b. For multiple clusters, select the clusters and then select **End Selected Suppressions**.

Alert notification email

Subscribers to SolidFire Active IQ alerts receive status emails for any alert that triggers on the system. There are three types of status emails associated with alerts:

New Alert Email	This type of email is sent when an alert is triggered.
Reminder Alert Email	This type of email is sent once every 24 hours for as long as the alert remains active.
Alert Resolved Email	This type of email is sent when the issue is resolved.

After an alert policy is created, and if a new alert is generated for this policy, an email is sent to the designated email address (see Create an Alert Policy).

The alert email subject line uses one of the following formats depending on error type reported:

- Unresolved cluster fault: `[cluster fault code] fault on [cluster name] ([severity])`
- Resolved cluster fault: `Resolved: [cluster fault code] fault on [cluster name] ([severity])`
- Unresolved alert: `[policy name] alert on [cluster name] ([severity])`
- Resolved alert fault: `Resolved: [policy name] alert on [cluster name] ([severity])`

> ⓘ Multiple notifications are grouped into a single email with the most severe faults at the top of the email similar to the following example:
>
> Cluster Method Not Reporting detected 2 alert(s) on [SF_Cluster1, SF_Custer2]
> (1) SF_Cluster1
> (1) SF_Cluster2
> Alert: 1 of 2
> **Status: Alert Reminder Notification**
> Alert ID: 1a5a49b7-f0a1-4ca5-9aad-8047e40e6331
> Alert Policy: Cluster Method Not Reporting
> Severity: Error
> Cluster: SF_Cluster1
> Occurrence Time: 2025-05-10 01:13:28 UTC
> Notification Time: 2025-05-10 01:13:28 UTC
>
> - lastUpdate: 2025-05-10T00:17:18.362Z
> - methodName: ListSnapshots
> - expectedInterval: 300
>
> Additional Detail:
>
> - lastUpdate: 2025-05-10T00:17:18.362Z
> - methodName: ListSnapshots
> - expectedInterval: 300
>
> Historical Detail: This alert has occurred 34 times in the last 30 days.
> Alerts for this Cluster
> Alert: 2 of 2
> **Status: Alert Reminder Notification**
> Alert ID: ec463269-922c-4bcd-9622-12167f0950ae
> Alert Policy: Cluster Method Not Reporting
> Severity: Error
> Cluster: SF_Cluster2
> Occurrence Time: 2025-05-10 01:08:02 UTC
> Notification Time: 2025-05-10 01:08:02 UTC
>
> - lastUpdate: 2025-05-10T00:11:53.946Z
> - methodName: ListSnapshots
> - expectedInterval: 300
>
> Additional Detail:
>
> - lastUpdate: 2025-05-10T00:11:53.946Z
> - methodName: ListSnapshots
> - expectedInterval: 300
>
> Historical Detail: This alert has occurred 33 times in the last 30 days.
> Alerts for this Cluster

Find more information

NetApp Product Documentation

Capacity Licensing

On the **Capacity Licensing** page within the **All Clusters View**, you can view information about the NetApp Capacity Licensing model. Customers using standard SolidFire appliances should disregard this page.

To view a given capacity licensing pool, you must have permissions to view all clusters included in that pool. If there are parent and child company relationships involved, work with your account manager to confirm that this is correctly recorded. Failure to do so might cause the capacity licensing pool to become unavailable.

Capacity Licensing is an alternative licensing option available from NetApp. Learn about or perform capacity licensing related tasks:

Heading	Description
Pool Name	Name of the customer associated with the license.
Entitled Capacity	Sum of software capacity licenses purchased.
Provisioned Capacity	Amount of allocated provisioned capacity on all capacity licensed nodes in a customer environment.
Used Capacity	Current used capacity by all clusters in a cluster pool.
Clusters	Number of clusters and their IDs, which comprise a cluster pool for a license.

Find more information

NetApp Product Documentation

Term Capacity

On the **Term Capacity** page within the **All Clusters View**, you can view information about the NetApp term-capacity model.

Heading	Description
Company ID	Company ID associated with the license.
Company Name	Name of the company associated with the license.
Licenses	Number of licenses in a customer environment.
Clusters	Number of clusters and their IDs belonging to a customer.
Licensed Capacity	Amount of allocated capacity on the capacity licensed nodes in a customer environment.
Consumed Capacity	Current consumed capacity by all clusters belonging to a customer.

Find more information

NetApp Product Documentation