



# **Verwalten von Gruppen**

StorageGRID

NetApp

October 03, 2025

This PDF was generated from <https://docs.netapp.com/de-de/storagegrid-115/tenant/creating-groups-for-s3-tenant.html> on October 03, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Inhalt

|  |    |
|--|----|
| Verwalten von Gruppen .....                            | 1  |
| Mandantenmanagement-Berechtigungen .....               | 1  |
| Erstellen von Gruppen für einen S3-Mandanten .....     | 2  |
| Erstellen von Gruppen für einen Swift Mandanten .....  | 5  |
| Anzeigen und Bearbeiten von Gruppendetails .....       | 7  |
| Hinzufügen von Benutzern zu einer lokalen Gruppe ..... | 10 |
| Gruppennamen bearbeiten .....                          | 12 |
| Duplizieren einer Gruppe .....                         | 13 |
| Löschen einer Gruppe .....                             | 14 |

# Verwalten von Gruppen

Sie weisen Benutzergruppen Berechtigungen zu, um zu steuern, welche Aufgaben Mandantenbenutzer durchführen können. Sie können föderierte Gruppen aus einer Identitätsquelle importieren, z. B. Active Directory oder OpenLDAP, oder Sie können lokale Gruppen erstellen.



Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich lokale Benutzer nicht beim Mandanten-Manager anmelden, obwohl sie auf Basis der Gruppenberechtigungen auf S3- und Swift-Ressourcen zugreifen können.

## Mandantenmanagement-Berechtigungen

Bevor Sie eine Mandantengruppe erstellen, überlegen Sie, welche Berechtigungen Sie dieser Gruppe zuweisen möchten. Über die Mandantenmanagement-Berechtigungen wird festgelegt, welche Aufgaben Benutzer mit dem Tenant Manager oder der Mandantenmanagement-API durchführen können. Ein Benutzer kann einer oder mehreren Gruppen angehören. Berechtigungen werden kumulativ, wenn ein Benutzer zu mehreren Gruppen gehört.

Um sich beim Tenant Manager anzumelden oder die Mandantenmanagement-API zu verwenden, müssen Benutzer einer Gruppe mit mindestens einer Berechtigung angehören. Alle Benutzer, die sich anmelden können, können die folgenden Aufgaben ausführen:

- Dashboard anzeigen
- Eigenes Kennwort ändern (für lokale Benutzer)

Für alle Berechtigungen legt die Einstellung Zugriffsmodus der Gruppe fest, ob Benutzer Einstellungen ändern und Vorgänge ausführen können oder ob sie nur die zugehörigen Einstellungen und Funktionen anzeigen können.



Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.

Sie können einer Gruppe die folgenden Berechtigungen zuweisen. Beachten Sie, dass S3-Mandanten und Swift-Mandanten unterschiedliche Gruppenberechtigungen haben. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

| Berechtigung | Beschreibung   |
|--------------|--|
| Root-Zugriff | Bietet vollständigen Zugriff auf den Tenant Manager und die Mandanten-Management-API.<br><br><b>Hinweis:</b> Swift-Benutzer müssen Root Access-Berechtigung haben, um sich beim Mandantenkonto anzumelden. |

| Berechtigung                            | Beschreibung   |
|---|--|
| Verwalter                               | <p>Nur Swift Mandanten. Bietet vollständigen Zugriff auf die Swift Container und Objekte für dieses Mandantenkonto</p> <p><b>Hinweis:</b> Swift-Benutzer müssen über die Swift-Administrator-Berechtigung verfügen, um alle Operationen mit der Swift REST-API auszuführen.</p>  |
| Management Ihrer eigenen S3 Credentials | <p>Nur S3-Mandanten. Benutzer können ihre eigenen S3-Zugriffsschlüssel erstellen und entfernen. Benutzer, die diese Berechtigung nicht besitzen, sehen nicht die Menüoption <b>STORAGE (S3) &gt; Meine S3-Zugriffstasten</b>.</p>  |
| Alle Buckets Verwalten                  | <ul style="list-style-type: none"> <li>S3-Mandanten: Ermöglicht Benutzern die Nutzung des Mandanten-Manager und der Mandanten-Management-API, um S3-Buckets zu erstellen und zu löschen sowie die Einstellungen für alle S3-Buckets im Mandantenkonto zu managen, unabhängig von S3-Bucket- oder Gruppenrichtlinien.</li> </ul> <p>Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption <b>Buckets</b> nicht.</p> <ul style="list-style-type: none"> <li>Swift Mandanten: Ermöglicht Swift Benutzern die Kontrolle der Konsistenzstufe für Swift Container mithilfe der Mandanten-Management-API.</li> </ul> <p><b>Hinweis:</b> Sie können Swift-Gruppen nur die Berechtigung Alle Buckets verwalten aus der Mandantenmanagement-API zuweisen. Sie können diese Berechtigung nicht Swift-Gruppen mit dem Tenant Manager zuweisen.</p> |
| Endpunkte Managen                       | <p>Nur S3-Mandanten. Ermöglicht Benutzern, Endpunkte mithilfe des Mandanten-Managers oder der Mandanten-Management-API zu erstellen oder zu bearbeiten, die als Ziel für StorageGRID-Plattformservices verwendet werden.</p> <p>Benutzer, die diese Berechtigung nicht besitzen, sehen nicht die Menüoption <b>Platform Services Endpunkte</b>.</p>  |

#### Verwandte Informationen

["S3 verwenden"](#)

["Verwenden Sie Swift"](#)

## Erstellen von Gruppen für einen S3-Mandanten

Sie können Berechtigungen für S3-Benutzergruppen managen, indem Sie föderierte Gruppen importieren oder lokale Gruppen erstellen.

#### Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie einen Identitätsverbund konfiguriert, und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

## Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.

The screenshot shows the 'Groups' page in the StorageGRID WebUI. At the top, it says 'Create and manage local and federated groups. Set group permissions to control access to specific pages and features.' Below this, there is a header with '2 groups' and a 'Create group' button. A dropdown menu labeled 'Actions' is open. The main area contains a table with columns: 'Name', 'ID', 'Type', and 'Access mode'. Two groups are listed:

| Name         | ID                                   | Type  | Access mode |
|--------------|--------------------------------------|-------|-------------|
| Applications | 22cc2e27-88ee-4461-a8c6-30b550beec0  | Local | Read-write  |
| Managers     | 8b15b131-1d21-4539-93ad-f2298347c4d8 | Local | Read-write  |

At the bottom, there are navigation links: 'Previous' and 'Next'.

2. Wählen Sie **Gruppe erstellen**.

3. Wählen Sie die Registerkarte **Lokale Gruppe** aus, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Federated Group** aus, um eine Gruppe aus der zuvor konfigurierten Identitätsquelle zu importieren.

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich Benutzer, die zu lokalen Gruppen gehören, nicht beim Mandanten-Manager anmelden, obwohl sie sich mithilfe von Client-Applikationen die Ressourcen des Mandanten basierend auf Gruppenberechtigungen managen können.

4. Geben Sie den Namen der Gruppe ein.

- **Lokale Gruppe:** Geben Sie einen Anzeigenamen und einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.
- **Federated Group:** Geben Sie den eindeutigen Namen ein. Bei Active Directory ist der eindeutige Name der dem zugeordneten Name sAMAccountName Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der dem zugeordnet ist uid Attribut.

5. Wählen Sie **Weiter**.

6. Wählen Sie einen Zugriffsmodus aus. Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.

- **Lesen-Schreiben** (Standard): Benutzer können sich bei Tenant Manager anmelden und die Mandantenkonfiguration verwalten.
- **Schreibgeschützt**: Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder Vorgänge in der Mandanten-Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.

7. Wählen Sie die Gruppenberechtigungen für diese Gruppe aus.

Weitere Informationen zu Berechtigungen für die Mandantenverwaltung finden Sie unter.

8. Wählen Sie **Weiter**.
9. Wählen Sie eine Gruppenrichtlinie aus, um zu bestimmen, über welche S3-Zugriffsrechte die Mitglieder dieser Gruppe verfügen.
  - **Kein S3-Zugriff:** Standard. Benutzer in dieser Gruppe haben keinen Zugriff auf S3-Ressourcen, es sei denn, der Zugriff wird mit einer Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat nur der Root-Benutzer standardmäßig Zugriff auf S3-Ressourcen.
  - **Schreibgeschützter Zugriff:** Benutzer in dieser Gruppe haben schreibgeschützten Zugriff auf S3-Ressourcen. Benutzer in dieser Gruppe können beispielsweise Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine schreibgeschützte Gruppenrichtlinie angezeigt. Sie können diesen String nicht bearbeiten.
  - **Vollzugriff:** Benutzer in dieser Gruppe haben vollen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine Richtlinie mit vollem Zugriff angezeigt. Sie können diesen String nicht bearbeiten.
  - **Benutzerdefiniert:** Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben. Anweisungen zur Implementierung einer S3-Client-Applikation finden Sie in den detaillierten Informationen zu Gruppenrichtlinien, einschließlich Sprachsyntax und Beispielen.

10. Wenn Sie **Benutzerdefiniert** ausgewählt haben, geben Sie die Gruppenrichtlinie ein. Jede Gruppenrichtlinie hat eine Größenbeschränkung von 5,120 Byte. Sie müssen einen gültigen JSON-formatierten String eingeben.

In diesem Beispiel dürfen Mitglieder der Gruppe nur einen Ordner auflisten und darauf zugreifen, der ihrem Benutzernamen (Schlüsselpräfix) im angegebenen Bucket entspricht. Beachten Sie, dass bei der Festlegung der Privatsphäre dieser Ordner Zugriffsberechtigungen aus anderen Gruppenrichtlinien und der Bucket-Richtlinie berücksichtigt werden sollten.

The screenshot shows the AWS IAM Groups configuration interface. On the left, there is a list of access options: 'No S3 Access', 'Read Only Access', 'Full Access', and 'Custom'. The 'Custom' option is selected and highlighted with a blue circle. Below it, a note says '(Must be a valid JSON formatted string.)'. To the right, there is a large text area containing a JSON policy document. The JSON code is as follows:

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3>ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

11. Wählen Sie die Schaltfläche aus, die angezeigt wird, je nachdem, ob Sie eine föderierte Gruppe oder eine

lokale Gruppe erstellen:

- Verbundgruppe: **Gruppe erstellen**
- Lokale Gruppe: **Weiter**

Wenn Sie eine lokale Gruppe erstellen, wird Schritt 4 (Benutzer hinzufügen) angezeigt, nachdem Sie **Weiter** ausgewählt haben. Dieser Schritt wird nicht für föderierte Gruppen angezeigt.

12. Aktivieren Sie das Kontrollkästchen für jeden Benutzer, den Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Gruppe erstellen**.

Optional können Sie die Gruppe speichern, ohne Benutzer hinzuzufügen. Sie können der Gruppe später Benutzer hinzufügen oder die Gruppe auswählen, wenn Sie neue Benutzer hinzufügen.

13. Wählen Sie **Fertig**.

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

#### Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

["S3 verwenden"](#)

## Erstellen von Gruppen für einen Swift Mandanten

Sie können Zugriffsberechtigungen für ein Swift-Mandantenkonto verwalten, indem Sie föderierte Gruppen importieren oder lokale Gruppen erstellen. Mindestens eine Gruppe muss über die Swift-Administratorberechtigung verfügen, die zur Verwaltung der Container und Objekte für ein Swift-Mandantenkonto erforderlich ist.

#### Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie einen Identitätsverbund konfiguriert, und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

#### Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.

# Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups

Create group

Actions

| <input type="checkbox"/> | Name         | ID                                   | Type  | Access mode |
|--------------------------|--------------|--------------------------------------|-------|-------------|
| <input type="checkbox"/> | Applications | 22cc2e27-88ee-4461-a8c6-30b550beec0  | Local | Read-write  |
| <input type="checkbox"/> | Managers     | 8b15b131-1d21-4539-93ad-f2298347c4d8 | Local | Read-write  |

← Previous 1 Next →

## 2. Wählen Sie Gruppe erstellen.

3. Wählen Sie die Registerkarte **Lokale Gruppe** aus, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Federated Group** aus, um eine Gruppe aus der zuvor konfigurierten Identitätsquelle zu importieren.

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich Benutzer, die zu lokalen Gruppen gehören, nicht beim Mandanten-Manager anmelden, obwohl sie sich mithilfe von Client-Applikationen die Ressourcen des Mandanten basierend auf Gruppenberechtigungen managen können.

## 4. Geben Sie den Namen der Gruppe ein.

- **Lokale Gruppe:** Geben Sie einen Anzeigenamen und einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.
- **Federated Group:** Geben Sie den eindeutigen Namen ein. Bei Active Directory ist der eindeutige Name der dem zugeordneten Name `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der dem zugeordnet ist `uid` Attribut.

## 5. Wählen Sie Weiter.

6. Wählen Sie einen Zugriffsmodus aus. Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.

- **Lesen-Schreiben** (Standard): Benutzer können sich bei Tenant Manager anmelden und die Mandantenkonfiguration verwalten.
- **Schreibgeschützt**: Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder Vorgänge in der Mandanten-Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.

## 7. Legen Sie die Gruppenberechtigung fest.

- Aktivieren Sie das Kontrollkästchen **Root Access**, wenn sich Benutzer bei der Tenant Manager- oder Mandantenmanagement-API anmelden müssen. (Standard)
- Deaktivieren Sie das Kontrollkästchen **Root Access**, wenn Benutzer keinen Zugriff auf die Tenant Manager- oder Mandantenmanagement-API benötigen. Deaktivieren Sie beispielsweise das

Kontrollkästchen für Anwendungen, die nicht auf den Mandanten zugreifen müssen. Weisen Sie dann die **Swift Administrator**-Berechtigung zu, damit diese Benutzer Container und Objekte verwalten können.

8. Wählen Sie **Weiter**.
9. Aktivieren Sie das Kontrollkästchen **Swift Administrator**, wenn der Benutzer die Swift REST API verwenden muss.

Swift-Benutzer müssen über die Root-Zugriffsberechtigung für den Zugriff auf den Mandanten-Manager verfügen. Die Root-Zugriffsberechtigung ermöglicht Benutzern jedoch nicht, sich in der Swift REST-API zu authentifizieren, um Container zu erstellen und Objekte aufzunehmen. Benutzer müssen über die Swift-Administratorberechtigung verfügen, um sich bei der Swift-REST-API zu authentifizieren.

10. Wählen Sie die Schaltfläche aus, die angezeigt wird, je nachdem, ob Sie eine föderierte Gruppe oder eine lokale Gruppe erstellen:

- Verbundgruppe: **Gruppe erstellen**
- Lokale Gruppe: **Weiter**

Wenn Sie eine lokale Gruppe erstellen, wird Schritt 4 (Benutzer hinzufügen) angezeigt, nachdem Sie **Weiter** ausgewählt haben. Dieser Schritt wird nicht für föderierte Gruppen angezeigt.

11. Aktivieren Sie das Kontrollkästchen für jeden Benutzer, den Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Gruppe erstellen**.

Optional können Sie die Gruppe speichern, ohne Benutzer hinzuzufügen. Sie können die Gruppe später Benutzer hinzufügen oder die Gruppe auswählen, wenn Sie neue Benutzer erstellen.

12. Wählen Sie **Fertig**.

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

#### Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

["Verwenden Sie Swift"](#)

## Anzeigen und Bearbeiten von Gruppendetails

Wenn Sie die Details für eine Gruppe anzeigen, können Sie den Anzeigennamen, Berechtigungen, Richtlinien und die Benutzer, die zu der Gruppe gehören, ändern.

#### Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

#### Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Wählen Sie den Namen der Gruppe aus, deren Details Sie anzeigen oder bearbeiten möchten.

Alternativ können Sie **Aktionen > Gruppendetails anzeigen** wählen.

Die Seite Gruppendetails wird angezeigt. Im folgenden Beispiel wird die Seite mit den S3-Gruppendetails angezeigt.

## Overview

|                                |                              |
|--------------------------------|------------------------------|
| Display name:                  | <a href="#">Applications</a> |
| Unique name:                   | group/Applications           |
| Type:                          | Local                        |
| Access mode:                   | Read-write                   |
| Permissions:                   | Root Access                  |
| S3 Policy:                     | None                         |
| Number of users in this group: | 0                            |

[Group permissions](#)[S3 group policy](#)[Users](#)

### Manage group permissions

Select an access mode for this group and select one or more permissions.

#### Access mode [?](#)

Select whether users can change settings and perform operations or whether they can only view settings and features.

 Read-write  Read-only

#### Group permissions [?](#)

Select the tenant account permissions you want to assign to this group.

 **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

 **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

 **Manage Endpoints**

Allows users to configure endpoints for platform services.

 **Manage Your Own S3 Credentials**

Allows users to create and delete their own S3 access keys.

[Save changes](#)

### 3. Nehmen Sie bei Bedarf Änderungen an den Gruppeneinstellungen vor.



Um sicherzustellen, dass Ihre Änderungen gespeichert werden, wählen Sie **Änderungen speichern** aus, nachdem Sie Änderungen in jedem Abschnitt vorgenommen haben. Wenn Ihre Änderungen gespeichert sind, wird oben rechts auf der Seite eine Bestätigungsmeldung angezeigt.

- a. Wählen Sie optional den Anzeigenamen oder das Bearbeitungssymbol aus Um den Anzeigenamen zu aktualisieren.

Sie können den eindeutigen Namen einer Gruppe nicht ändern. Sie können den Anzeigenamen für eine föderierte Gruppe nicht bearbeiten.

- b. Optional können Sie die Berechtigungen aktualisieren.
- c. Nehmen Sie für die Gruppenrichtlinie die entsprechenden Änderungen für Ihren S3- oder Swift-Mandanten vor.

- Wenn Sie eine Gruppe für einen S3-Mandanten bearbeiten, wählen Sie optional eine andere S3-Gruppenrichtlinie aus. Wenn Sie eine benutzerdefinierte S3-Richtlinie auswählen, aktualisieren Sie den JSON-String wie erforderlich.
- Wenn Sie eine Gruppe für einen Swift-Mandanten bearbeiten, aktivieren oder deaktivieren Sie das Kontrollkästchen **Swift Administrator**.

Weitere Informationen zum Swift Administrator erhalten Sie in den Anweisungen zum Erstellen von Gruppen für einen Swift-Mandanten.

- d. Optional können Benutzer hinzugefügt oder entfernt werden.
4. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt **Änderungen speichern** ausgewählt haben.

Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

#### Verwandte Informationen

["Erstellen von Gruppen für einen S3-Mandanten"](#)

["Erstellen von Gruppen für einen Swift Mandanten"](#)

## Hinzufügen von Benutzern zu einer lokalen Gruppe

Sie können bei Bedarf Benutzer zu einer lokalen Gruppe hinzufügen.

#### Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

#### Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Wählen Sie den Namen der lokalen Gruppe aus, der Sie Benutzer hinzufügen möchten.

Alternativ können Sie **Aktionen > Gruppendetails anzeigen** wählen.

Die Seite Gruppendetails wird angezeigt.

## Overview

|                                |                              |
|--------------------------------|------------------------------|
| Display name:                  | <a href="#">Applications</a> |
| Unique name:                   | group/Applications           |
| Type:                          | Local                        |
| Access mode:                   | Read-write                   |
| Permissions:                   | Root Access                  |
| S3 Policy:                     | None                         |
| Number of users in this group: | 0                            |

[Group permissions](#)[S3 group policy](#)[Users](#)

### Manage group permissions

Select an access mode for this group and select one or more permissions.

#### Access mode [?](#)

Select whether users can change settings and perform operations or whether they can only view settings and features.

 Read-write  Read-only

#### Group permissions [?](#)

Select the tenant account permissions you want to assign to this group.

 **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

 **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

 **Manage Endpoints**

Allows users to configure endpoints for platform services.

 **Manage Your Own S3 Credentials**

Allows users to create and delete their own S3 access keys.

[Save changes](#)

3. Wählen Sie **Benutzer verwalten** und dann **Benutzer hinzufügen**.

The screenshot shows a 'Manage users' interface. At the top, there are buttons for 'Add users' (blue) and 'Remove Users' (red). Below them is a search bar labeled 'Search Groups...' with a magnifying glass icon. To the right, it says 'Displaying 1 results'. The main area has three columns: 'Username', 'Full Name', and 'Denied'. A user named 'User\_02' is listed with the full name 'User\_02\_Managers' and a 'Denied' status.

4. Wählen Sie die Benutzer aus, die Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Benutzer hinzufügen**.

The screenshot shows an 'Add users' dialog. It says 'Select local users to add to the group **Applications**'. There is a search bar for 'Search Groups...' with a magnifying glass icon. Below it, it says 'Displaying 1 results'. A table lists a single user 'User\_01' with the full name 'User\_01\_Applications'. A checkbox next to the user's name is checked. The table has columns for 'Username', 'Full Name', and 'Denied'. At the bottom left is a 'Cancel' button, and at the bottom right is a blue 'Add users' button.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

## Gruppennamen bearbeiten

Sie können den Anzeigenamen für eine Gruppe bearbeiten. Sie können den eindeutigen Namen für eine Gruppe nicht bearbeiten.

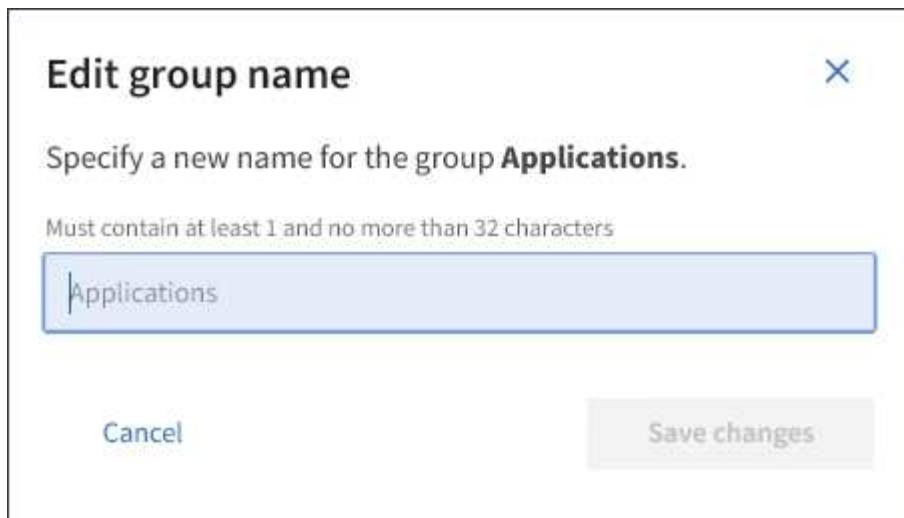
### Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

### Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für die Gruppe, deren Anzeigename Sie bearbeiten möchten.
3. Wählen Sie **Aktionen > Gruppenname bearbeiten**.

Das Dialogfeld Gruppenname bearbeiten wird angezeigt.



4. Wenn Sie eine lokale Gruppe bearbeiten, aktualisieren Sie den Anzeigenamen nach Bedarf.

Sie können den eindeutigen Namen einer Gruppe nicht ändern. Sie können den Anzeigenamen für eine föderierte Gruppe nicht bearbeiten.

5. Wählen Sie **Änderungen speichern**.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

#### Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

## Duplizieren einer Gruppe

Sie können neue Gruppen schneller erstellen, indem Sie eine vorhandene Gruppe duplizieren.

#### Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

#### Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für die Gruppe, die Sie duplizieren möchten.
3. Wählen Sie **Gruppe duplizieren**. Weitere Details zum Erstellen einer Gruppe finden Sie in den Anweisungen zum Erstellen von Gruppen für einen S3-Mandanten oder für einen Swift-Mandanten.
4. Wählen Sie die Registerkarte **Lokale Gruppe** aus, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Federated Group** aus, um eine Gruppe aus der zuvor konfigurierten Identitätsquelle zu importieren.

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich Benutzer, die zu lokalen Gruppen gehören, nicht beim Mandanten-Manager anmelden, obwohl sie sich mithilfe von Client-Applikationen die Ressourcen des Mandanten basierend auf Gruppenberechtigungen managen können.

5. Geben Sie den Namen der Gruppe ein.
  - **Lokale Gruppe:** Geben Sie einen Anzeigenamen und einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.
  - **Federated Group:** Geben Sie den eindeutigen Namen ein. Bei Active Directory ist der eindeutige Name dem zugeordneten Name `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der dem zugeordnet ist `uid` Attribut.
6. Wählen Sie **Weiter**.
7. Ändern Sie bei Bedarf die Berechtigungen für diese Gruppe.
8. Wählen Sie **Weiter**.
9. Wenn Sie eine Gruppe für einen S3-Mandanten duplizieren, wählen Sie bei Bedarf aus den Optionsfeldern **S3-Richtlinie hinzufügen** eine andere Richtlinie aus. Wenn Sie eine benutzerdefinierte Richtlinie ausgewählt haben, aktualisieren Sie den JSON-String wie erforderlich.
10. Wählen Sie **Gruppe erstellen**.

#### Verwandte Informationen

["Erstellen von Gruppen für einen S3-Mandanten"](#)

["Erstellen von Gruppen für einen Swift Mandanten"](#)

["Mandantenmanagement-Berechtigungen"](#)

## Löschen einer Gruppe

Sie können eine Gruppe aus dem System löschen. Benutzer, die nur zu dieser Gruppe gehören, können sich nicht mehr beim Mandantenmanager anmelden oder das Mandantenkonto verwenden.

#### Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

#### Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.

# Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups

[Create group](#)

Actions ▾

| <input type="checkbox"/> | Name         | ID                                   | Type  | Access mode |
|--------------------------|--------------|--------------------------------------|-------|-------------|
| <input type="checkbox"/> | Applications | 22cc2e27-88ee-4461-a8c6-30b550beec0  | Local | Read-write  |
| <input type="checkbox"/> | Managers     | 8b15b131-1d21-4539-93ad-f2298347c4d8 | Local | Read-write  |

[← Previous](#) **1** [Next →](#)

2. Aktivieren Sie die Kontrollkästchen für die Gruppen, die Sie löschen möchten.

3. Wählen Sie **Aktionen > Gruppe löschen**.

Eine Bestätigungsmeldung wird angezeigt.

4. Wählen Sie **Gruppe löschen**, um zu bestätigen, dass Sie die in der Bestätigungsmeldung angegebenen Gruppen löschen möchten.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

## Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

## **Copyright-Informationen**

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDERWEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

**ERLÄUTERUNG ZU „RESTRICTED RIGHTS“:** Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## **Markeninformationen**

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.