



**StorageGRID® Webscale 10.4**

# **Tenant Administrator Guide**

April 2017 | 215-11757\_A0  
[doccomments@netapp.com](mailto:doccomments@netapp.com)



# Contents

<b>Administering a StorageGRID Webscale tenant account .....</b>	<b>4</b>
<b>Understanding tenant accounts .....</b>	<b>5</b>
<b>Using the Tenant Management Interface .....</b>	<b>7</b>
Signing in for the first time .....	7
Web browser requirements .....	8
Understanding the Dashboard .....	8
Understanding the StorageGRID Webscale Tenant API .....	10
<b>Configuring identity federation .....</b>	<b>13</b>
Configuring a federated identity source .....	13
Guidelines for configuring an OpenLDAP server .....	15
Forcing synchronization with the identity source .....	16
Disabling identity federation .....	16
<b>Managing groups .....</b>	<b>18</b>
Creating groups for an S3 tenant .....	18
Creating groups for a Swift tenant .....	20
Tenant management permissions .....	21
Cloning a group .....	22
Editing a group .....	23
Removing a group .....	24
<b>Managing users .....</b>	<b>25</b>
Creating local users .....	25
Cloning local users .....	26
Editing local users .....	27
Changing a local user's password .....	28
Removing local users .....	28
Signing in as a tenant user .....	29
Managing S3 access keys .....	30
Creating your own S3 access keys .....	30
Removing your own S3 access keys .....	32
Creating another user's S3 access keys .....	33
Removing another user's S3 access keys .....	34
<b>Glossary .....</b>	<b>35</b>
<b>Copyright information .....</b>	<b>42</b>
<b>Trademark information .....</b>	<b>43</b>
<b>How to send comments about documentation and receive update notifications .....</b>	<b>44</b>
<b>Index .....</b>	<b>45</b>

## Administering a StorageGRID Webscale tenant account

---

As an administrator of a StorageGRID Webscale tenant account, you can use the Tenant Management Interface to monitor how much storage the tenant account is consuming, and you can manage access control by setting up groups and users.

The *StorageGRID Webscale Tenant Administrator Guide* contains information and instructions for managing and monitoring a StorageGRID Webscale tenant account on a day-to-day basis. This guide also includes instructions for setting up tenant users and groups.

This guide does not provide information about using the rest of the StorageGRID Webscale system and its functional areas. For additional information, see these publications:

- *Grid Primer*, which provides a general introduction to StorageGRID Webscale
- *Administrator Guide*, which provides detailed instructions and explanations for using the Grid Management Interface to manage the entire StorageGRID Webscale system
- *Simple Storage Service Implementation Guide*, which provides instructions for using the S3 client protocol with StorageGRID Webscale
- *Swift Implementation Guide*, which provides instructions for using the Swift client protocol with StorageGRID Webscale

### Related information

[\*StorageGRID Webscale 10.4 Grid Primer\*](#)

[\*StorageGRID Webscale 10.4 Administrator Guide\*](#)

[\*StorageGRID Webscale 10.4 S3 \(Simple Storage Service\) Implementation Guide\*](#)

[\*StorageGRID Webscale 10.4 Swift Implementation Guide\*](#)

## Understanding tenant accounts

---

A tenant account allows clients that use the Simple Storage Service (S3) protocol or the Swift protocol to store and retrieve objects on a StorageGRID Webscale system.

Each client protocol that will use the StorageGRID Webscale system requires its own tenant account. If both the Swift client protocol and the S3 client protocol will share a StorageGRID Webscale system to store and retrieve objects, there must be at least two tenant accounts: one for Swift containers and objects and one for S3 buckets and objects. Each tenant account has its own unique account ID, Tenant Management Interface, federated or local groups and users, and containers (buckets for S3) and objects.

Optionally, the StorageGRID Webscale system can use additional tenant accounts in order to segregate stored objects by different entities. For example, a StorageGRID Webscale system might use multiple tenant accounts in either of these use cases:

- **Enterprise use case:** If the StorageGRID Webscale system is being used in an enterprise application, the grid's object storage might be segregated by the different departments in the organization. For example, there might be tenant accounts for the Marketing department, the Customer Support department, the Human Resources department, and so on.

**Note:** If you use the S3 client protocol, you can simply use S3 buckets and bucket policies to segregate objects between the departments in an enterprise. You do not need to use tenant accounts. See the *StorageGRID Webscale Simple Storage Service Implementation Guide* for more information.

- **Service provider use case:** If the StorageGRID Webscale system is being used by a service provider, the grid's object storage might be segregated by the different entities that lease the storage. For example, there might be tenant accounts for Company A, Company B, Company C, and so on.

Storage tenant accounts are created by a StorageGRID Webscale grid administrator using the Grid Management Interface (either the user interface or the API). When creating a tenant account, the grid administrator specifies the following information:

- Display name for the tenant account (the tenant's account ID is assigned automatically and cannot be changed)
- Which client protocol will be used by the tenant account (S3 or Swift)
- Initial password for the tenant account's root user
- Whether the tenant account uses the identity source that was configured for the grid or its own identity source for identity federation
- Optionally, a storage quota for the tenant account—the maximum number of gigabytes, terabytes, or petabytes available for the tenant's objects

As soon as the tenant account has been created, you can sign into the Tenant Management Interface to monitor storage usage and to set up identity federation, groups, and users. After users have been set up, S3 client users will also use the Tenant Management Interface to create and manage the access keys needed to store and retrieve objects on the StorageGRID Webscale system.

This guide provides instructions for using the Tenant Management Interface. For information about creating storage tenant accounts, see the *Administrator Guide*.

### Related information

[\*StorageGRID Webscale 10.4 S3 \(Simple Storage Service\) Implementation Guide\*](#)



## Using the Tenant Management Interface

---

The Tenant Management Interface includes a Dashboard that shows the tenant's storage usage as well as settings for configuring identity federation, groups, users, and S3 keys.

### Signing in for the first time

When you sign into the StorageGRID Webscale Tenant Administration Interface for the first time, you sign in as the tenant's root user or as another tenant user created by the grid administrator.

#### Before you begin

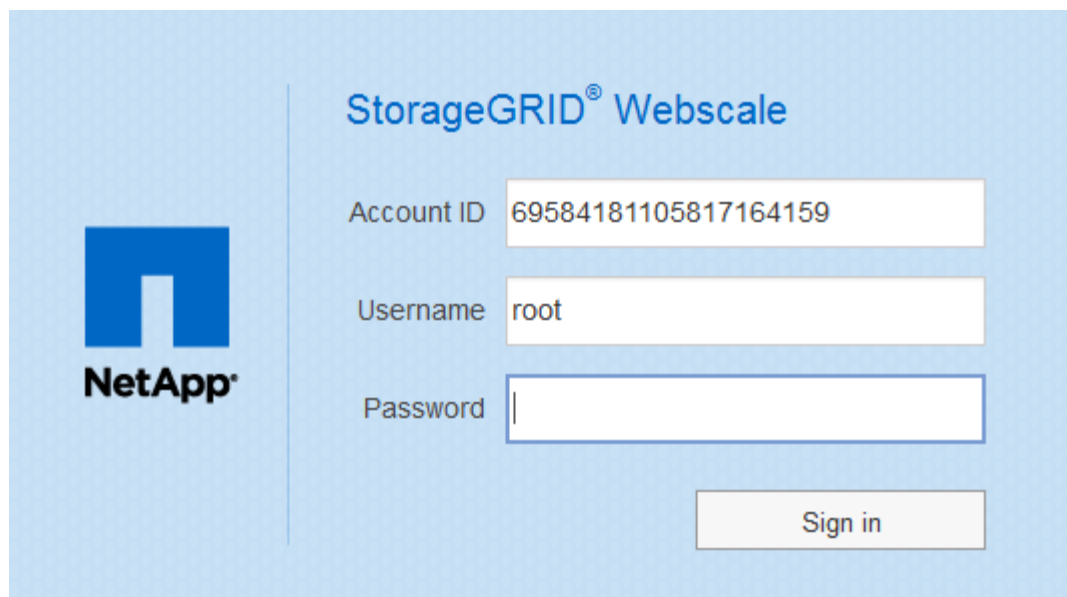
- You must know the password associated with the tenant user.
- You must be using a supported web browser.

#### Steps

1. Browse to the URL for your tenant account.

Grid administrators who know the tenant account's root user password can also sign using the **Sign In** link for the tenant in the Grid Management Interface.

The Sign in page appears, with the **Account ID** field completed.

The image shows the StorageGRID Webscale sign-in interface. On the left is the NetApp logo. To the right, the title "StorageGRID® Webscale" is displayed. Below the title are three input fields: "Account ID" with the value "69584181105817164159", "Username" with the value "root", and "Password" which is empty. A "Sign in" button is located at the bottom right of the form area.

StorageGRID® Webscale

Account ID 69584181105817164159

Username root

Password

Sign in

2. Type the username in the **Username** field.  
For example, if you are signing in as the root user, type "root".
3. Type the password for the user in the **Password** field, and click **Sign in**.  
The Tenant Administration Interface appears. You are now signed in.
4. If you signed in as the root user, and you received the password from someone at another company, such as a service provider, consider changing the password to ensure it is secure.

**Related tasks**

[Changing a local user's password](#) on page 28

**Related references**

[Web browser requirements](#) on page 8

## Web browser requirements

You must use a supported web browser.

Web browser	Minimum supported version
Google Chrome	54
Microsoft Internet Explorer	11 (Native Mode)
Mozilla Firefox	50

You should set the browser window to a recommended width.

Browser width	Pixels
Minimum	1024
Optimum	1280

## Understanding the Dashboard

When you first sign in to the Tenant Management Interface, the Dashboard shows how much storage the tenant account is using.

The Dashboard includes two panels:

- **Storage Usage** – This panel shows which containers (buckets for S3) are consuming the most storage. Up to eight containers can be shown. The Other segment combines all other containers, including any containers that consume less than 1% of the total storage.
- **Quota** – If the maximum number of gigabytes, terabytes, or petabytes available for the tenant was specified when the account was created, this panel shows how much of that quota has been used and how much is still available. If no quota was set, the tenant has an unlimited quota, and an informational message is displayed.

**Note:** If the quota is exceeded, the tenant account cannot create new objects.



NetApp® StorageGRID® Webscale

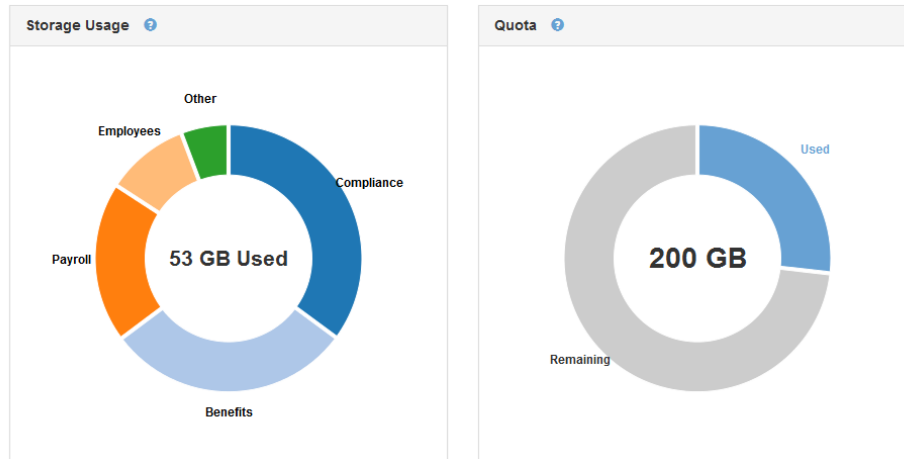
Help | Root @ Human Resources | Sign Out

Dashboard

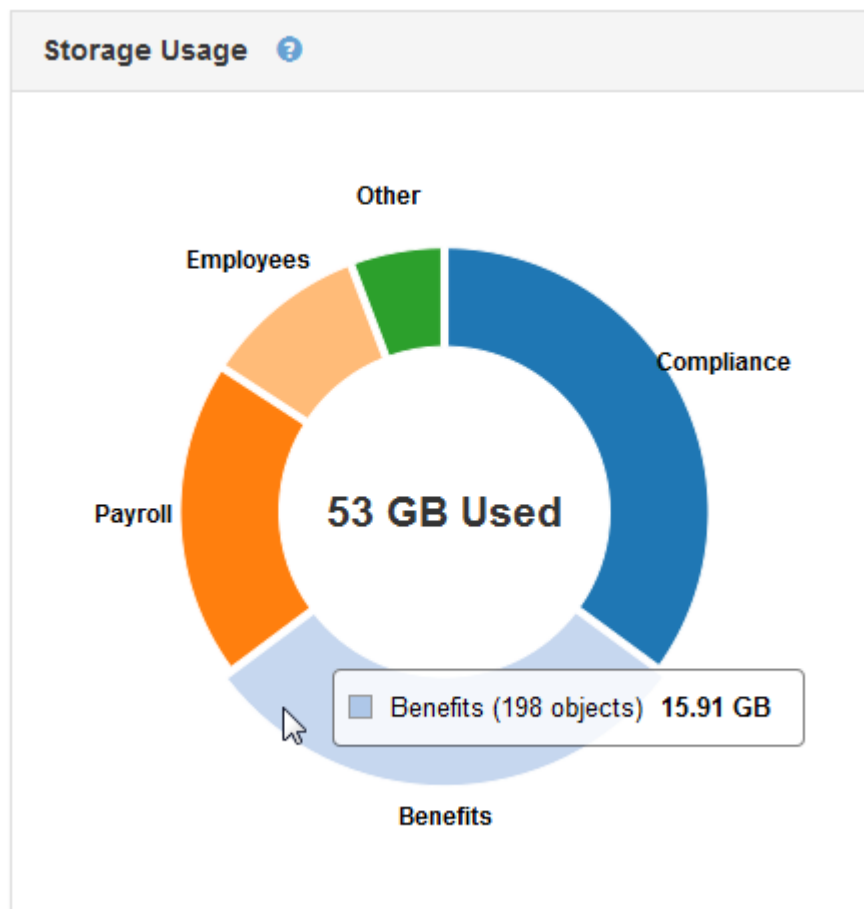
S3

Access Control

## Dashboard



You can place your cursor over any of the chart segments to obtain more information, including the number of stored objects and total bytes for each container or bucket.



## Understanding the StorageGRID Webscale Tenant API

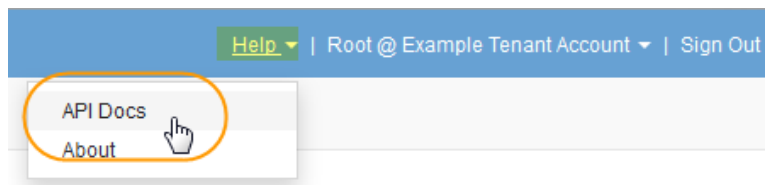
StorageGRID Webscale provides a REST API for managing the tenant account.

### StorageGRID Webscale Tenant API documentation

The StorageGRID Webscale Tenant API uses the Swagger open source API platform to provide the API documentation. Swagger allows both developers and non-developers to interact with the API in a user interface that illustrates how the API responds to parameters and options. This documentation assumes that you are familiar with standard web technologies and the JSON (JavaScript Object Notation) data format.

**Attention:** Any API operations you perform using the Swagger user interface are live operations. Be careful not to create, update, or delete configuration or other data by mistake.

You can access the Tenant API documentation by signing in to the Tenant Management Interface and selecting **Help > API Docs** in the web application header.



### API

Each REST API command includes the API's URL, an HTTP action, any required or optional URL parameters, and an expected API response.

The Swagger user interface provides complete details and documentation for each API operation, as in the following example. To get information about a local tenant user, you would enter that user's unique name as the value for the `shortName` parameter and click **Try it out**.

GET /org/users/user/{shortName} Retrieves a local Tenant User by unique name

Response Class (Status 200)

Model | Model Schema

```
{
  "responseTime": "2016-10-19T21:48:54.245Z",
  "status": "success",
  "apiVersion": "2.0",
  "deprecated": false,
  "data": {
    "fullName": "Test User",
    "memberOf": [
      "00000000-0000-0000-0000-000000000000"
    ]
  },
}
```

Response Content Type

Parameters

Parameter	Value	Description	Parameter Type	Data Type
shortName	<input type="text" value="(required)"/>	uniqueName minus prefix	path	string

Response Messages

HTTP Status Code	Reason	Response Model	Headers
default	General error	Model   Model Schema	

```
{
  "responseTime": "2016-10-19T21:48:54.249Z",
  "status": "success",
  "apiVersion": "2.0",
  "deprecated": false,
  "data": {},
  "code": 0,
  "message": {
    "text": "string",
    "key": "string",
    "context": "string",
  }
}
```

[Try it out!](#)

The StorageGRID Webscale Tenant API includes the following sections:

- **account** – Operations on the current tenant account, including getting storage usage information.
- **auth** – Operations to perform user session authentication.  
The Tenant API supports the Bearer Token Authentication Scheme. To login, you provide a username and password in the JSON body of the authentication request (that is, POST /api/v2/authorize). If the user is successfully authenticated, a security token is returned. This token must be provided in the header of subsequent API requests ("Authorization: Bearer *token*").
- **config** – Operations related to the product release and versions of the Tenant API. You can list the product release version and the major versions of the API supported by that release.
- **deactivated-features** – Operations to view features that might have been deactivated.
- **groups** – Operations to manage local tenant groups and to retrieve federated tenant groups from an external identity source.
- **identity-source** – Operations to configure an external identity source and to manually synchronize federated group and user information.
- **S3** – Operations to manage S3 access keys for tenant users.
- **users** – Operations to view and manage tenant users.

## Tenant API versioning

The Tenant API uses versioning to support non-disruptive upgrades. For example, this Request URL specifies version 2 of the API.

`https://hostname_or_ip_address/api/v2/authorize`

Changes in the Tenant API that are backward incompatible bump the major version of the API. For example, an incompatible API change would bump the version from 1.1 to 2.0. Changes in the Tenant API that are backward compatible bump the minor version instead. Backward-compatible changes include the addition of new endpoints or new properties. For example, a compatible API change would bump the version from 1.0 to 1.1.

When you install StorageGRID Webscale software for the first time, only the most recent version of the Tenant API is enabled. However, when you upgrade to a new major version of StorageGRID Webscale, you continue to have access to the older API version for at least one major release.

Outdated requests are marked as deprecated in the following ways:

- The response header is "Deprecated: true"
- The JSON response body includes "deprecated": true

### Determining which API versions are supported in the current release

Use the following API request to return a list of the supported API major versions:

```
GET https://{IP-Address}/api/versions
{
  "responseTime": "2016-10-03T14:49:16.587Z",
  "status": "success",
  "apiVersion": "2.0",
  "data": [
    1,
    2
  ]
}
```

### Specifying an API version for a request

You can specify the API version using a path parameter (/api/v2) or a header (Api-Version: 2). If you provide both values, the header value overrides the path value.

```
curl https://[IP-Address]/api/v2/org/config
```

```
curl -H "Api-Version: 2" https://[IP-Address]/api/org/config
```

## Configuring identity federation

---

You can use identity federation to import tenant groups and users. Using identity federation makes setting up tenant groups and users faster, and it allows tenant users to sign in to the tenant account using familiar credentials.

### Steps

1. [Configuring a federated identity source](#) on page 13
2. [Forcing synchronization with the identity source](#) on page 16
3. [Disabling identity federation](#) on page 16

## Configuring a federated identity source

You must configure a federated identity source (such as Active Directory or OpenLDAP) before you can assign management permissions to federated groups and users.

### Before you begin

- You must be signed in using a supported browser.
- You must have specific access permissions.
- The **Uses Own Identity Source** check box must have been selected when the tenant account was created. Contact the grid administrator for information or to change this setting.

**Note:** When using identity federation, be aware that users who only belong to a primary group on Active Directory are not allowed to sign in to the Tenant Management Interface. To allow these users to sign in, grant them membership in a user-created group.

### Steps

1. Select **Access Control > Identity Federation**.
2. Select **Enable Identity Federation**.  
LDAP service configuration information appears.
3. Select the type of LDAP service you want to configure from the **LDAP Service Type** drop-down list.  
You can select **Active Directory**, **OpenLDAP**, or **Other**.  
**Note:** If you select **OpenLDAP**, you must configure the OpenLDAP server. See “Guidelines for configuring an OpenLDAP server” in this guide.
4. If you selected **Other**, complete the fields in the **LDAP Attributes** section.
  - **Unique User Name:** The name of the attribute that contains the unique identifier of an LDAP user. This attribute is equivalent to `sAMAccountName` for Active Directory and `uid` for OpenLDAP.
  - **User UUID:** The name of the attribute that contains the permanent unique identifier of an LDAP user. This attribute is equivalent to `objectGUID` for Active Directory and `entryUUID` for OpenLDAP.

- **Group Unique Name:** The name of the attribute that contains the unique identifier of an LDAP group. This attribute is equivalent to `sAMAccountName` for Active Directory and `cn` for OpenLDAP.
  - **Group UUID:** The name of the attribute that contains the permanent unique identifier of an LDAP group. This attribute is equivalent to `objectGUID` for Active Directory and `entryUUID` for OpenLDAP.
5. Enter the required LDAP server and network connection information:
- **Hostname:** The hostname or IP address of the LDAP server.
  - **Port:** The port used to connect to the LDAP server. This is typically 389.
  - **Username:** The username used to access the LDAP server, including the domain.  
The specified user must have permission to list groups and users and to access the following attributes:
    - `cn`
    - `sAMAccountName` or `uid`
    - `objectGUID` or `entryUUID`
    - `memberOf`
  - **Password:** The password associated with the username.
  - **Group Base DN:** The fully qualified Distinguished Name (DN) of an LDAP subtree you want to search for groups. In the example, all groups whose Distinguished Name is relative to the base DN (`DC=storagegrid,DC=example,DC=com`) can be used as federated groups.
 

**Note:** The Unique Group Name values must be unique within the Group Base DN they belong to.
  - **User Base DN:** The fully qualified Distinguished Name (DN) of an LDAP subtree you want to search for users.
 

**Note:** The Unique User Name values must be unique within the User Base DN they belong to.
6. Select a security setting from the **Transport Layer Security (TLS)** drop-down list to specify if TLS is used to secure communications with the LDAP server.
- **Use operating system CA certificate:** Use the default CA certificate installed on the operating system to secure connections.
  - **Use custom CA certificate:** Use a custom security certificate.  
If you select this setting, copy and paste the custom security certificate in the CA Certificate text box.
  - **Do not use TLS:** The network traffic between the StorageGRID Webscale system and the LDAP server will not be secured.

### Example

The following screen shot shows example configuration values for an LDAP server that uses Active Directory.

## Identity Federation

Configure a federated identity source (such as Active Directory or OpenLDAP) to enable management permissions to be granted to federated groups.

Enable Identity Federation ☒

LDAP Service Type Active Directory

---

**LDAP Server**

Hostname my-active-directory.example.com

Port 389

Username MyDomain\Administrator

Password ••••••••

Group Base DN DC=storagegrid,DC=example,DC=com

User Base DN DC=storagegrid,DC=example,DC=com

Transport Layer Security (TLS) Use custom CA certificate

CA Certificate 

```
-----BEGIN CERTIFICATE-----
MIIFmzCCA4OgAwIBAgIJAM5MuRrbdKo/MA0GCSqGSIb3
DQEBDQUAMGMxCzAJBgNV
BAYTAiVTMRcwFQYDVQQIDA5Ob3J0aCBDYXJvGluYTE
MMAoGA1UEBwwDUiRQMw
DQYDVQQKDAZOZXRBcHAXHDAaBgNVBAsME1N0b3Jh
```

Test Connection Save

7. Optionally, click **Test Connection** to validate your connection settings for the LDAP server.

8. Click **Save**.

### Related concepts

[Tenant management permissions](#) on page 21

[Guidelines for configuring an OpenLDAP server](#) on page 15

## Guidelines for configuring an OpenLDAP server

If you want to use an OpenLDAP server for identity federation, you must configure specific settings on the OpenLDAP server.

### Memberof and refint overlays

The memberof and refint overlays should be enabled. For more information, see the “Reverse Group Membership Maintenance” section in the *OpenLDAP Software Administrator's Guide*.

### Indexing

You must configure the following OpenLDAP attributes with the specified index keywords:

```

olcDbIndex: objectClass eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: cn eq,pres,sub
olcDbIndex: entryUUID eq

```

In addition, ensure the fields mentioned in the help for Username are indexed for optimal performance.

For more information on the `olcDBIndex` directive used for indexing attributes, see the *OpenLDAP Software Administrator's Guide*.

#### Related information

[OpenLDAP documentation: Version 2.4 Administrator's Guide](#)

## Forcing synchronization with the identity source

The StorageGRID Webscale system periodically synchronizes federated groups and users from the identity source. You can force synchronization to start if you want to enable or restrict user permissions as quickly as possible.

#### Before you begin

- The identity source must be enabled.
- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

#### Steps

1. Select **Access Control > Identity Federation**.
2. Click **Synchronize**.

A confirmation message is displayed indicating that synchronization started successfully.

#### Related concepts

[Tenant management permissions](#) on page 21

## Disabling identity federation

You can temporarily or permanently disable identity federation for tenant groups and users. When identity federation is disabled, there is no communication between the StorageGRID Webscale system and the identity source. However, any settings you have configured are retained, allowing you to easily re-enable identity federation in the future.

#### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

#### About this task

Before you disable identity federation, you should be aware of the following:

- Federated users will be unable to sign in.



- Federated users who are currently signed in will retain access to the tenant account until their session expires, but they will be unable to sign in after their session expires.
- Synchronization between the StorageGRID Webscale system and the identity source will not occur.

**Steps**

1. Select **Access Control > Identity Federation**.
2. Deselect the **Enable Identity Federation** checkbox.
3. Click **Save**.

**Related concepts**

[\*Tenant management permissions\*](#) on page 21

# Managing groups

User groups allow you to control which tasks tenant users can perform. You can create local groups or import federated groups from an identity source, such as Active Directory or OpenLDAP.

**Steps**

- 1. [Creating groups for an S3 tenant](#) on page 18
- 2. [Creating groups for a Swift tenant](#) on page 20
- 3. [Tenant management permissions](#) on page 21
- 4. [Cloning a group](#) on page 22
- 5. [Editing a group](#) on page 23
- 6. [Removing a group](#) on page 24

## Creating groups for an S3 tenant

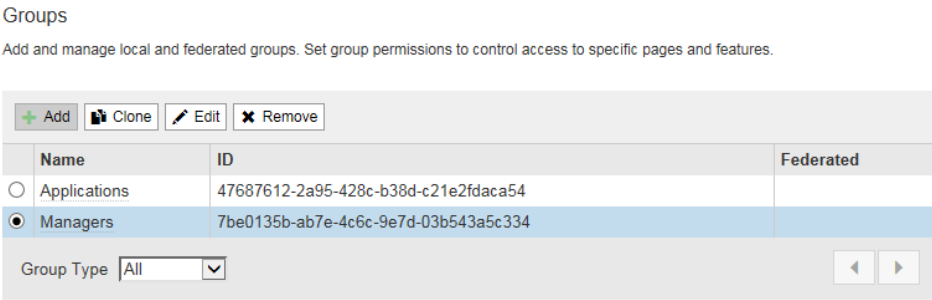
You can manage the access permissions for an S3 tenant account by creating local groups or by importing federated groups. As required, you can also specify S3 policies for each group.

**Before you begin**

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

**Steps**

- 1. Select **Access Control > Groups**.



- 2. Click **Add**.
- 3. Select **Local** to create a local group, or select **Federated** to import a group from the previously configured identity source.
- 4. Enter the group's name.

If you selected...	Enter...
Local	Both a display name and a unique name for this group. You can edit the display name later.

If you selected...	Enter...
Federated	The unique name of the federated group.  <b>Note:</b> For Active Directory, the unique name is the name associated with the <code>sAMAccountName</code> attribute. For OpenLDAP, the unique name is the name associated with the <code>uid</code> attribute.

5. In the **Management Permissions** section, select the tenant account permissions you want to assign to this group.
6. If you want to attach a group policy to this group, enter a JSON formatted string in the **S3 Policy** text box.

### Add Group

Create a new local group or import a group from the external LDAP server.

Type ☒ Local ☐ Federated

Display Name

Unique Name

#### Management Permissions

☐ Root Access ☒ Manage Your Own S3 Credentials

#### S3 Policy

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:sgws:s3::*"
    }
  ]
}
```

The JSON string is validated as it is entered, and you can only save group policy strings that are valid.

Each group policy has a size limit of 5,120 bytes.

Policy statements are built using this structure to specify permissions:

```
<Principal> is allowed/denied to perform <Action> to <Resource> when
<Condition> applies
```

For a group policy, you do not need to specify `<Principal>`. The principal is simply the group for which you are specifying the policy.

For example, the following group policy gives group members permission to perform all operations on all resources owned by the S3 tenant account:

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "urn:sgws:s3:::*"
    }
  ]
}
```

**Note:** See the *StorageGRID Webscale Simple Storage Service Implementation Guide* for detailed information about group policies, including language syntax and examples.

## 7. Click **Save**.

New group policies might take up to 15 minutes to take effect because of caching.

### Related concepts

[Tenant management permissions](#) on page 21

### Related information

[StorageGRID Webscale 10.4 S3 \(Simple Storage Service\) Implementation Guide](#)

## Creating groups for a Swift tenant

You can manage access permissions for a Swift tenant account by creating local groups or by importing federated groups.

### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

### Steps

#### 1. Select **Access Control > Groups**.

#### Groups

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

<a href="#">+ Add</a> <a href="#">📄 Clone</a> <a href="#">✎ Edit</a> <a href="#">✕ Remove</a>		
Name	ID	Federated
<input type="radio"/> Applications	47687612-2a95-428c-b38d-c21e2fdaca54	
<input checked="" type="radio"/> Managers	7be0135b-ab7e-4c6c-9e7d-03b543a5c334	

Group Type

#### 2. Click **Add**.

3. Select **Local** to create a local group, or select **Federated** to import a group from the previously configured identity source.
4. Enter the group's name.

If you selected...	Enter...
Local	Both a display name and a unique name for this group. You can edit the display name later.
Federated	The unique name of the federated group.  <b>Note:</b> For Active Directory, the unique name is the name associated with the <code>sAMAccountName</code> attribute. For OpenLDAP, the unique name is the name associated with the <code>uid</code> attribute.

5. In the **Management Permissions** section, select the tenant account permissions you want to assign to this group.
6. In the **Swift Permissions** section, select the **Administrator** check box if you want users in this group to be Swift Administrators.
7. Click **Save**.

New group policies might take up to 15 minutes to take effect because of caching.

#### Related concepts

[Tenant management permissions](#) on page 21

#### Related information

[StorageGRID Webscale 10.4 Swift Implementation Guide](#)

## Tenant management permissions

Tenant management permissions are assigned to groups and determine which tasks users can perform using the Tenant Management Interface or the Tenant API. A user can belong to one or more groups.

### Permissions

To sign in to the Tenant Management Interface or to use the Tenant API, users must belong to a group that has at least one permission. All users who can sign in can perform the following tasks:

- View the dashboard
- Change their own password

You can assign the following permissions to a group. Note that S3 tenants and Swift tenants have different group permissions.

Permission	Description
Root Access	Provides access to all tenant administration features. Allows users to perform these tasks: <ul style="list-style-type: none"> <li>• Configure an identity server</li> <li>• Create, edit, and remove groups</li> <li>• Create, edit, and remove users</li> <li>• Change user passwords</li> <li>• S3 tenants only. Create and remove S3 access keys for the S3 root user and other S3 users</li> </ul>
Manage Your Own S3 Credentials	S3 tenants only. Allows users to create and remove their own S3 access keys. Users who do not have this permission do not see the <b>S3 &gt; My Credentials</b> menu option.

## Cloning a group

You can create new groups more quickly by cloning an existing group.

### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

### Steps

1. Select **Access Control > Groups**.

#### Groups

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

+ Add
📄 Clone
✎ Edit
✕ Remove

	Name	ID	Federated
<input type="radio"/>	Applications	47687612-2a95-428c-b38d-c21e2fdaca54	
<input checked="" type="radio"/>	Managers	7be0135b-ab7e-4c6c-9e7d-03b543a5c334	

Group Type All
◀
▶

2. Select the group you want to clone.
3. Click **Clone**.
4. Select **Local** to create a local group, or select **Federated** to import a group from the previously configured identity source.
5. Enter the group's name.

If you selected...	Enter...
Local	Both a display name and a unique name for this group. You can edit the display name later.
Federated	The unique name of the federated group.  <b>Note:</b> For Active Directory, the unique name is the name associated with the <code>sAMAccountName</code> attribute. For OpenLDAP, the unique name is the name associated with the <code>uid</code> attribute.

- Assign permissions to this group.
- If you cloned a group for an S3 tenant, optionally update or enter the S3 policy you want to use for this group in the **S3 Policy** text box.
- Click **Save**.

New group policies might take up to 15 minutes to take effect because of caching.

#### Related concepts

[Tenant management permissions](#) on page 21

## Editing a group

You can edit a group to change the display name of a local group or to update permissions.

#### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

#### Steps

- Select **Access Control > Groups**.

#### Groups

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

	Name	ID	Federated
<input type="radio"/>	Applications	47687612-2a95-428c-b38d-c21e2fdaca54	
<input checked="" type="radio"/>	Managers	7be0135b-ab7e-4c6c-9e7d-03b543a5c334	

Group Type: All ▼ ◀ ▶

- Select the group you want to edit.
- Click **Edit**.
- If you are editing a local group, update the display name as needed.  
You cannot change a group's unique name. You cannot edit the display name for a federated group.
- Update the permissions as needed.

6. If you are editing a group for an S3 tenant, optionally update the JSON string for the S3 group policy.
7. Click **Save**.

Changes to group policies might take up to 15 minutes to take effect because of caching.

#### Related concepts

[Tenant management permissions](#) on page 21

## Removing a group

You can remove a group. Any users who belong only to that group will no longer be able to sign in to the Tenant Management Interface or use the tenant account.

#### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.


#### Steps


1. Select **Access Control > Groups**.


#### Groups

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

+ Add

 Clone

 Edit

 Remove

	Name	ID	Federated
<input type="radio"/>	Applications	47687612-2a95-428c-b38d-c21e2fdaca54	
<input checked="" type="radio"/>	Managers	7be0135b-ab7e-4c6c-9e7d-03b543a5c334	

Group Type 

All

2. Select the group you want to remove.
3. Click **Remove**.
4. Click **Close**.

Changes to access permissions might take up to 15 minutes to take effect because of caching.

#### Related concepts

[Tenant management permissions](#) on page 21



## Managing users

---

After you create local groups, you can create local users and assign them to the appropriate group or groups.

### Steps

1. [Creating local users](#) on page 25
2. [Cloning local users](#) on page 26
3. [Editing local users](#) on page 27
4. [Changing a local user's password](#) on page 28
5. [Removing local users](#) on page 28
6. [Signing in as a tenant user](#) on page 29
7. [Managing S3 access keys](#) on page 30

## Creating local users

After you create local groups, you can create local users and assign them to one or more groups to control their access permissions. Because local users must be assigned to local groups, you should create the groups before creating the users.

### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

### Steps

1. Select **Access Control > Users**.
2. Click **Create**.

Users

View local and federated users. Edit properties and group membership of local users.

<a href="#">+ Create</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Change Password</a> <a href="#">Remove</a>				
	Username	Full Name	Denied	Federated
<input type="radio"/>	root	Root		

User Type All ▼

◀ ▶

3. Complete the following fields.
  - **Full name:** The full name for this user, for example, the first name and last name of a person or the name of an application.
  - **Unique name:** A unique username, which is used when the user signs in.
  - **Deny access:** If selected, this user cannot sign in to the tenant account, even though the user might still belong to one or more groups.

**Note:** You can use this check box to temporarily suspend a user's ability to sign in.

- **Password:** A password, which is used when the user signs in.

Create User

Create a local user.

Full Name

Unique Name

Deny Access

☐

Password

Password

Confirm Password

Group Membership

	Group Name
<input type="checkbox"/>	Managers

Cancel

Save

4. In the **Group Membership** section, select one or more local groups.

Permissions are cumulative. Users will have all permissions for all groups they belong to.

5. Click **Save**.

#### Related concepts

[Tenant management permissions](#) on page 21

## Cloning local users

You can clone a local user to create a new user more quickly.

#### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

#### Steps

1. Select **Access Control > Users**.
2. Click **Clone**.
3. Complete the following fields.

- **Full name:** The full name for this user, for example, the first name and last name of a person or the name of an application.
- **Unique name:** A unique username, which is used when the user signs in.
- **Deny access:** If selected, this user cannot sign in to the tenant account, even though the user might still belong to one or more groups.

**Note:** You can use this check box to temporarily suspend a user's ability to sign in.

- **Password:** A password, which is used when the user signs in.

4. In the **Group Membership** section, select one or more local groups.

Permissions are cumulative. Users will have all permissions for all groups they belong to.

5. Click **Save**

**Related concepts**

[Tenant management permissions](#) on page 21

## Editing local users

You can edit local users to change names, deny access, or assign them to different groups.

**Before you begin**

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

**Steps**

1. Select **Access Control > Users**.

2. Click **Edit**.

3. Update the following fields as required:

- **Full name:** The full name for this user, for example, the first name and last name of a person or the name of an application.
- **Deny access:** If selected, this user cannot sign in to the tenant, even though the user might still belong to one or more groups.

**Note:** You can use this check box to temporarily suspend a user's ability to sign in.

4. In the **Group Membership** section, select one or more local groups.

Permissions are cumulative. Users will have all permissions for all groups they belong to.

5. Click **Save**

**Related concepts**

[Tenant management permissions](#) on page 21

## Changing a local user's password

A tenant administrator can change passwords for local tenant users.

### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

### Steps

1. Select **Access Control > Users**.
2. Select the user, and click **Change Password**.

Users

View local and federated users. Edit properties and group membership of local users.

	Username	Full Name	Denied	Federated
<input type="radio"/>	root	Root		
<input type="radio"/>	user1	Manager User 1		
<input checked="" type="radio"/>	user2	Manager User 2		

User Type: All

3. Enter the new password, and click **Save**.

Change Password - user2

New Password:

Confirm New Password:

### Related concepts

[Tenant management permissions](#) on page 21

## Removing local users

You can permanently remove local users who no longer need to access the StorageGRID Webscale tenant account.

### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

**Steps**

1. Select **Access Control > Users**.
2. Click **Remove**.  
A confirmation dialog appears.
3. Click **OK** to confirm you want to remove the user.

**Related concepts**

[Tenant management permissions](#) on page 21

## Signing in as a tenant user

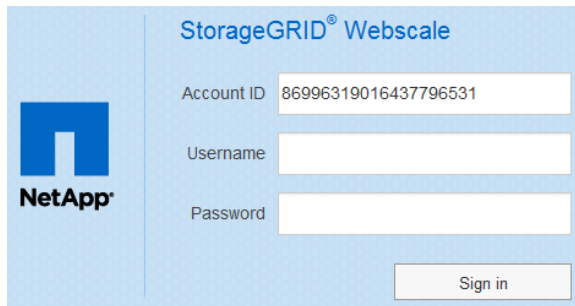
Tenant users can sign in as federated users or as local users.

**Before you begin**

- You must know your username and password.
- You must have specific access permissions.
- You must be using a supported web browser.

**Steps**

1. Browse to the URL for your tenant account.  
The sign-in page appears, with the **Account ID** field completed.



2. Type your username in the **Username** field.
3. Type your password in the **Password** field.
4. Click **Sign in**.  
The Tenant Administration Interface appears. You are now signed in.

**Related references**

[Web browser requirements](#) on page 8

## Managing S3 access keys

Each user of an S3 tenant account must have an access key to store and retrieve objects on the StorageGRID Webscale system. An access key consists of an access key ID and a secret access key.

### About this task

S3 access keys can be managed as follows:

- Users who have the **Manage Your Own S3 Credentials** permission can create or remove their own S3 access keys.
- Users who have appropriate access permissions can create and remove S3 access keys for other users.
- Users who have the **Root Access** permission can manage the access keys for the S3 root account. Root access keys provide full access to the tenant's buckets and objects unless explicitly disabled by a bucket policy.

StorageGRID Webscale supports Signature Version 2 and Signature Version 4 authentication. Cross-account access is not permitted unless explicitly enabled by a bucket policy.

### Related tasks

[Creating your own S3 access keys](#) on page 30

[Removing your own S3 access keys](#) on page 32

[Creating another user's S3 access keys](#) on page 33

[Removing another user's S3 access keys](#) on page 34

## Creating your own S3 access keys

If you are using an S3 tenant and you have the appropriate permission, you can create your own S3 access keys. You must have an access key to access your buckets and objects in the S3 tenant account.

### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

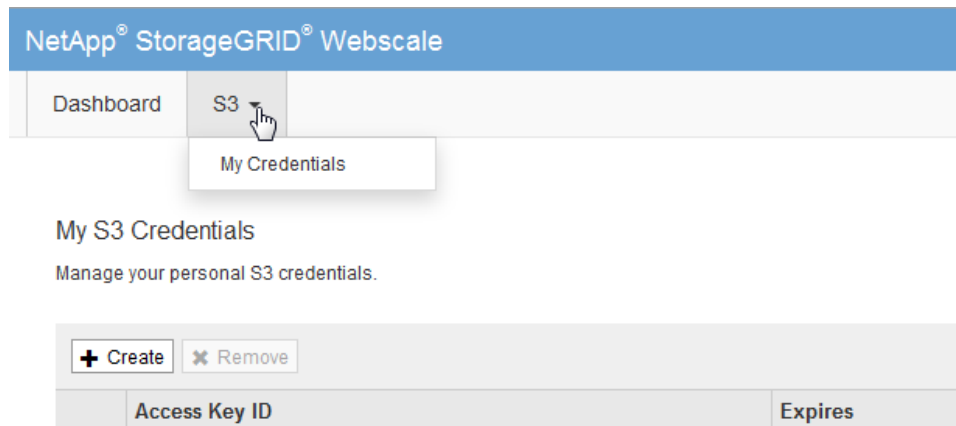
### About this task

You can create one or more S3 access keys. Multiple access keys allow you to begin using a new key without temporarily losing access to the objects in the account. You simply create the new access key, update the application with your new access key ID and secret key, and then remove the old access key from StorageGRID Webscale.

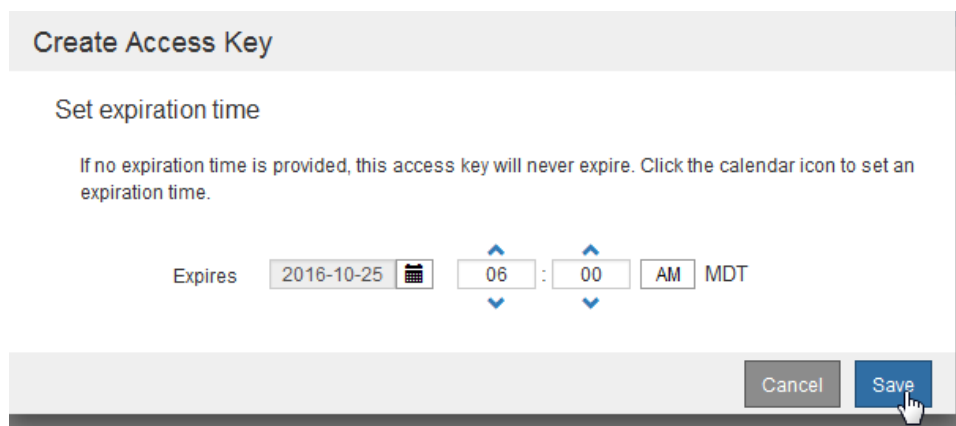
**Important:** The S3 account can be accessed using the Access Key ID and Secret Key for any currently displayed key. For this reason, protect your access keys as you would a password. Rotate access keys on a regular basis, remove any unused keys from your account, and never share them with other users.

### Steps

1. Click **S3 > My Credentials**.



2. Click **Create**.
3. Use the calendar control to select the expiration date and then set the time, or leave the default value of Never, and click **Save**.



You can set an expiration date and time to limit your access to a certain time period or to cause old keys to be removed automatically. Setting a short expiration time can help reduce your risk if your access key ID and secret key are accidentally exposed.

The Save Keys dialog box is displayed, listing your Access Key ID and Secret Access Key.

4. Copy the Access Key ID and the Secret Access Key to a safe location, or click **Download** to save a spreadsheet file (.csv) containing the Access Key ID and Secret Access Key.

### Save Keys

You will not be able to view the Access Key ID and Secret Access Key after you close this dialog. To save the keys for future reference, click the Download button or copy and paste the values to another location.

Access Key ID	9PELXW0KAZVP1QCNMWGC
Secret Access Key	F30BjSpVKSI9pt6FxGwKGJ1Q47AbxrTVh21qcuQY

Download

Finish

**Important:** Do not close this dialog until you have copied or downloaded this information.

5. Click **Finish**.

#### Related concepts

[Tenant management permissions](#) on page 21

## Removing your own S3 access keys

If you are using an S3 tenant and you have the appropriate permission, you can remove your own S3 access keys. After an access key is removed, it can no longer be used to access the objects and buckets in the tenant account.

#### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

#### About this task

You should remove any access keys from your StorageGRID Webscale user account that you are no longer using.

#### Steps

1. Click **S3 > My Credentials**.
2. Select the entry you want to remove.
3. Click **Remove**.
4. Click **OK**.

#### Related concepts

[Tenant management permissions](#) on page 21



## Creating another user's S3 access keys

If you are using an S3 tenant and you have the appropriate permission, you can create S3 access keys for other users.

### Before you begin

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

### About this task

If you have the appropriate permissions, you can create one or more S3 access keys for other users.

**Important:** The S3 account can be accessed using the Access Key ID and Secret Access Key for any currently displayed key. For this reason, protect access keys as you would a password. Rotate access keys on a regular basis, remove any unused keys from the account, and never share them with other users.

### Steps

1. Click **Access Control > Users**.
2. Select the user whose S3 access keys you want to manage, and click **Edit S3 Keys**.  
The Managing S3 Access Key dialog appears, showing any S3 access keys previously defined for the user.
3. Click **Create**.
4. Use the calendar control to select the expiration date and then set the time, or leave the default value of Never, and click **Save**.

**Create Access Key**

**Set expiration time**

If no expiration time is provided, this access key will never expire. Click the calendar icon to set an expiration time.

Expires 2016-10-25 [calendar icon] 06 : 00 AM MDT

Cancel Save

You can set an expiration date and time to limit the user's access to a certain time period or to cause old access keys to be removed automatically. Setting a short expiration time can help reduce the risk if the Access Key ID and Secret Access Key are accidentally exposed.

The Save Keys dialog box is displayed, listing the Access Key ID and Secret Access Key.

5. Copy the Access Key ID and the Secret Access Key to a safe location, or click **Download** to save a spreadsheet file (.csv) containing the Access Key ID and Secret Access Key.

### Save Keys

You will not be able to view the Access Key ID and Secret Access Key after you close this dialog. To save the keys for future reference, click the Download button or copy and paste the values to another location.

Access Key ID

9PELXW0KAZVP1QCNMWGC

Secret Access Key

F30BjSpVKSI9pt6FxGwKGJ1Q47AbxrTVh21qcuQY

Download

Finish

**Important:** Do not close this dialog until you have copied or downloaded this information.

6. Click **Finish**.

**Related concepts**

[Tenant management permissions](#) on page 21

## Removing another user's S3 access keys

If you are using an S3 tenant and you have appropriate permissions, you can remove another user's S3 access keys. After an access key is removed, it can no longer be used to access the objects and buckets in the tenant account.

**Before you begin**

- You must be signed in to the Tenant Management Interface using a supported browser.
- You must have specific access permissions.

**Steps**

1. Click **Access Control > Users**.
2. Select the user whose S3 access keys you want to manage, and click **Edit S3 Keys**.  
The Managing S3 Access Key dialog appears, showing any S3 access keys previously defined for the user.
3. Select the entry you want to remove.
4. Click **Remove**.
5. Click **OK**.

**Related concepts**

[Tenant management permissions](#) on page 21

# Glossary

---

**ACL**

Access control list. Specifies which users or groups of users are allowed to access an object and what operations are permitted, for example, read, write, and execute.

**active-backup mode**

A method for bonding two physical ports together for redundancy.

**ADC service**

Administrative Domain Controller. The ADC service maintains topology information, provides authentication services, and responds to queries from the LDR, CMN, and CLB services. The ADC service is present on each of the first three Storage Nodes installed at a site.

**ADE**

Asynchronous Distributed Environment. Proprietary development environment used as a framework for services within the StorageGRID Webscale system.

**Admin Node**

The Admin Node provides services for the web interface, system configuration, and audit logs. See also, *primary Admin Node*.

**Amazon S3**

Proprietary web service from Amazon for the storage and retrieval of data.

**AMS service**

Audit Management System. The AMS service monitors and logs all audited system events and transactions to a text log file. The AMS service is present on the Admin Node.

**API Gateway Node**

An API Gateway Node provides load balancing functionality to the StorageGRID Webscale system and is used to distribute the workload when multiple client applications are performing ingest and retrieval operations. API Gateway Nodes include a Connection Load Balancer (CLB) service.

**ARC service**

Archive. The ARC service provides the management interface with which you configure connections to external archival storage such as the cloud through an S3 interface or tape through TSM middleware. The ARC service is present on the Archive Node.

**Archive Node**

The Archive Node manages the archiving of object data to an external archival storage system.

**atom**

Atoms are the lowest level component of the container data structure, and generally encode a single piece of information.

**audit message**

Information about an event occurring in the StorageGRID Webscale system that is captured and logged to a file.

**Base64**

A standardized data encoding algorithm that enables 8-bit data to be converted into a format that uses a smaller character set, enabling it to safely pass through legacy systems

that can process only basic (low order) ASCII text excluding control characters. See RFC 2045 for more details.

#### **bundle**

A structured collection of configuration information used internally by various components of the StorageGRID Webscale system. Bundles are structured in container format.

#### **Cassandra**

An open-source database that is scalable and distributed, provides high availability, and handles large amounts of data across multiple servers.

#### **CBID**

Content Block Identifier. A unique internal identifier of a piece of content within the StorageGRID Webscale system.

#### **CDMI**

Cloud Data Management Interface. An industry-standard defined by SNIA that includes a RESTful interface for object storage. For more information, see [www.snia.org/cdm](http://www.snia.org/cdm).

#### **CIDR**

Classless Inter-Domain Routing. A notation used to compactly describe a subnet mask used to define a range of IP addresses. In CIDR notation, the subnet mask is expressed as an IP address in dotted decimal notation, followed by a slash and the number of bits in the subnet. For example, 192.0.2.0/24.

#### **CLB service**

Connection Load Balancer. The CLB service provides a gateway into the StorageGRID Webscale system for client applications connecting through HTTP. The CLB service is part of the API Gateway Node.

#### **Cloud Data Management Interface**

See *CDMI*.

#### **CMN service**

Configuration Management Node. The CMN service manages system-wide configurations and grid tasks. The CMN service is present on the primary Admin Node.

#### **CMS service**

Content Management System. The CMS service carries out the operations of the active ILM policy's ILM rules, determining how object data is protected over time. The CMS service is present on the Storage Node.

#### **command**

In HTTP, an instruction in the request header such as GET, HEAD, DELETE, OPTIONS, POST, or PUT. Also known as an HTTP method.

#### **container**

Created when an object is split into segments. A container object lists the header information for all segments of the split object and is used by the LDR service to assemble the segmented object when it is retrieved by a client application.

#### **content block ID**

See *CBID*.

#### **content handle**

See *UUID*.

#### **CSTR**

Null-terminated, variable-length string.

**DC**

Data Center site.

**DDS service**

Distributed Data Store. The DDS service interfaces with the distributed key-value store and manages object metadata. It distributes metadata copies to multiple instances of the distributed key-value store so that metadata is always protected against loss.

**distributed key value store**

Data storage and retrieval that unlike a traditional relational database manages data across grid nodes.

**DNS**

Domain Name System.

**enablement layer**

Used during installation to customize the Linux operating system installed on each grid node. Only the packages needed to support the services hosted on the grid node are retained, which minimizes the overall footprint occupied by the operating system and maximizes the security of each grid node.

**Fibre Channel**

A networking technology primarily used for storage.

**Grid ID signed text block**

A Base64 encoded block of cryptographically signed data that contains the grid ID. See also, *provisioning*.

**grid node**

The basic software building block for the StorageGRID Webscale system, for example, Admin Node or Storage Node. Each grid node type consists of a set of services that perform a specialized set of tasks.

**grid task**

System-wide scripts used to trigger various actions that implement specific changes to the StorageGRID Webscale system. For example, most maintenance and expansion procedures involve running grid tasks. Grid tasks are typically long-term operations that span many entities within the StorageGRID Webscale system. See also, *Task Signed Text Block*.

**ILM**

Information Lifecycle Management. A process of managing content storage location and duration based on content value, cost of storage, performance access, regulatory compliance, and other factors. See also, *Admin Node* and *storage pool*.

**LACP**

Link Aggregation Control Protocol. A method for bundling two or more physical ports together to form a single logical channel.

**LAN**

Local Area Network. A network of interconnected computers that is restricted to a small area, such as a building or campus. A LAN can be considered a node to the Internet or other wide area network.

**latency**

Time duration for processing a transaction or transmitting a unit of data from end to end. When evaluating system performance, both throughput and latency need to be considered. See also, *throughput*.

**LDR service**

Local Distribution Router. The LDR service manages the storage and transfer of content within the StorageGRID Webscale system. The LDR service is present on the Storage Node.

**LUN**

See *object store*.

**mDNS**

Multicast Domain Name System. A system for resolving IP addresses in a small network where no DNS server has been installed.

**metadata**

Information related to or describing an object stored in the StorageGRID Webscale system; for example, ingest time.

**MLAG**

Multi-Chassis Link Aggregation Group. A type of link aggregation group that uses two (and sometimes more) switches to provide redundancy in case one of the switches fails.

**MTU**

Maximum transmission unit. The largest size packet or frame that can be sent in any transmission.

**namespace**

A set whose elements are unique names. There is no guarantee that a name in one namespace is not repeated in a different namespace.

**nearline**

A term describing data storage that is neither “online” (implying that it is instantly available, like spinning disk) nor “offline” (which can include offsite storage media). An example of a nearline data storage location is a tape that is loaded in a tape library, but is not mounted.

**NFS**

Network File System. A protocol (developed by SUN Microsystems) that enables access to network files as if they were on local disks.

**NMS service**

Network Management System. The NMS service provides a web-based interface for managing and monitoring the StorageGRID Webscale system. The NMS service is present on the Admin Node. See also, *Admin Node*.

**node ID**

An identification number assigned to a service within the StorageGRID Webscale system. Each service (such as an NMS service or ADC service) must have a unique node ID. The number is set during system configuration and tied to authentication certificates.

**NTP**

Network Time Protocol. A protocol used to synchronize distributed clocks over a variable latency network, such as the Internet.

**object**

An artificial construct used to describe a system that divides content into data and metadata.

**object segmentation**

A StorageGRID Webscale process that splits a large object into a collection of small objects (segments) and creates a segment container to track the collection. The segment container contains the UUID for the collection of small objects as well as the header

information for each small object in the collection. All of the small objects in the collection are the same size. See also, *segment container*.

### **object storage**

An approach to storing data where the data is accessed by unique identifiers and not by a user-defined hierarchy of directories and files. Each object has both data (for example, a picture) and metadata (for example, the date the picture was taken). Object storage operations act on entire objects as opposed to reading and writing bytes as is commonly done with files, and provided via APIs or HTTP instead of NAS (CIFS/NFS) or block protocols (iSCSI/FC/FCOE).

### **object store**

A configured file system on a disk volume. The configuration includes a specific directory structure and resources initialized at system installation.

### **OID**

Object Identifier. The unique identifier of an object.

### **primary Admin Node**

Admin Node that hosts the CMN service. Each StorageGRID Webscale system has only one primary Admin Node. See also, *Admin Node*.

### **provisioning**

The process of generating a new or updated Recovery Package and GPT repository. See also, *SAID*.

### **quorum**

A simple majority:  $50\% + 1$ . Some system functionality requires a quorum of the total number of a particular service type.

### **Recovery Package**

A .zip file containing deployment-specific files and software needed to install, expand, upgrade, and maintain a StorageGRID Webscale system. The package also contains system-specific configuration and integration information, including server hostnames and IP addresses, and highly confidential passwords needed during system maintenance, upgrade, and expansion. See also, *SAID*.

### **SAID**

Software Activation and Integration Data. The component in the Recovery Package that includes the `Passwords.txt` file.

### **SATA**

Serial Advanced Technology Attachment. A connection technology used to connect server and storage devices.

### **SCSI**

Small Computer System Interface. A connection technology used to connect servers and peripheral devices, such as storage systems.

### **segment container**

An object created by the StorageGRID Webscale system during the segmentation process. Object segmentation splits a large object into a collection of small objects (segments) and creates a segment container to track the collection. A segment container contains the UUID for the collection of segmented objects as well as the header information for each segment in the collection. When assembled, the collection of segments creates the original object. See also, *object segmentation*.

### **server**

Used when specifically referring to hardware. Might also refer to a virtual machine.

**service**

A unit of the StorageGRID Webscale system, such as the ADC service, NMS service, or SSM service. Each service performs unique tasks critical to the normal operations of a StorageGRID Webscale system.

**SQL**

Structured Query Language. An industry-standard interface language for managing relational databases. An SQL database is one that supports the SQL interface.

**ssh**

Secure Shell. A UNIX shell program and supporting protocols used to log in to a remote computer and run commands over an authenticated and encrypted channel.

**SSL**

Secure Socket Layer. The original cryptographic protocol used to enable secure communications over the Internet. See also, *TLS*.

**SSM service**

Server Status Monitor. A component of the StorageGRID Webscale software that monitors hardware conditions and reports to the NMS service. Every grid node runs an instance of the SSM service.

**Storage Node**

The Storage Node provides storage capacity and services to store, move, verify, and retrieve objects stored on disks.

**storage pool**

The element of an ILM rule that determines the location where an object is stored.

**storage volume**

See *object store*

**StorageGRID**

A registered trademark of NetApp, Inc., used for an object storage grid architecture and software system.

**Task Signed Text Block**

A Base64 encoded block of cryptographically signed data that provides the set of instructions that define a grid task.

**TCP/IP**

Transmission Control Protocol/Internet Protocol. A process of encapsulating and transmitting packet data over a network. It includes positive acknowledgment of transmissions.

**throughput**

The amount of data that can be transmitted or the number of transactions that can be processed by a system or subsystem in a given period of time. See also, *latency*.

**Tivoli Storage Manager**

IBM storage middleware product that manages storage and retrieval of data from removable storage resources.

**TLS**

Transport Layer Security. A cryptographic protocol used to enable secure communications over the Internet. See RFC 2246 for more details.

**transfer syntax**

The parameters, such as the byte order and compression method, needed to exchange data between systems.



**URI**

Universal Resource Identifier. A generic set of all names or addresses used to refer to resources that can be served from a computer system. These addresses are represented as short text strings.

**UTC**

A language-independent international abbreviation, UTC is neither English nor French. It means both “Coordinated Universal Time” and “Temps Universel Coordonné.” UTC refers to the standard time common to every place in the world.

**UUID**

Universally Unique Identifier. Unique identifier for each piece of content in the StorageGRID Webscale system. UUIDs provide client applications with a content handle that permits them to access content in a way that does not interfere with the StorageGRID Webscale system’s management of that same content. A 128-bit number that is guaranteed to be unique. See RFC 4122 for more details.

**virtual machine (VM)**

A software platform that enables the installation of an operating system and software, substituting for a physical server and permitting the sharing of physical server resources among several virtual servers.

**VLAN**

Virtual local area network (or virtual LAN). A group of devices that are located on different LAN segments but are configured to communicate as if they were attached to the same network switch.

**WAN**

Wide area network. A network of interconnected computers that covers a large geographic area, such as a country.

**XFS**

A scalable, high-performance journaled file system originally developed by Silicon Graphics.

**XML**

Extensible Markup Language. A text format for the extensible representation of structured information; classified by type and managed like a database. XML has the advantages of being verifiable, human readable, and easily interchangeable between different systems.

## Copyright information

---

Copyright © 1994–2017 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.

**RESTRICTED RIGHTS LEGEND:** Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark information

---

Active IQ, AltaVault, Arch Design, ASUP, AutoSupport, Campaign Express, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Element, Fitness, Flash Accel, Flash Cache, Flash Pool, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, Fueled by SolidFire, GetSuccessful, Helix Design, LockVault, Manage ONTAP, MetroCluster, MultiStore, NetApp, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANscreen, SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, SolidFire Helix, StorageGRID, SyncMirror, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## How to send comments about documentation and receive update notifications

---

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

[\*doccomments@netapp.com\*](mailto:doccomments@netapp.com)

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

# Index

## A

- access keys
  - creating for other users [33](#)
  - creating own keys [30](#)
  - managing for S3 tenants [30](#)
  - removing [32](#)
  - removing S3 keys for other users [34](#)

## API

- Tenant [10](#)

## B

- browsers
  - supported [8](#)

## C

- cloning
  - local groups [22](#)
  - local users [26](#)
- comments
  - how to send feedback about documentation [44](#)
- configuring identity federation [13](#)
- creating
  - groups for S3 tenant [18](#)
  - groups for Swift tenant [20](#)
  - local users [25](#)

## D

- Dashboard
  - Tenant Management Interface [8](#)
- documentation
  - how to receive automatic notification of changes to [44](#)
  - how to send feedback about [44](#)

## F

- federated groups
  - importing for S3 tenants [18](#)
  - importing for Swift tenants [20](#)
- federated identity source
  - configuring [13](#)
- federated users
  - signing in [29](#)
- feedback
  - how to send comments about documentation [44](#)

## G

- group policies
  - specifying for S3 tenants [18](#)
- groups
  - cloning [22](#)
  - creating for S3 tenants [18](#)
  - creating for Swift tenants [20](#)

- disabling identity federation [16](#)
- editing [23](#)
- managing [18](#)
- permissions [21](#)
- removing [24](#)

## I

- identity federation
  - configuring [13](#)
  - configuring identity source for [13](#)
  - configuring OpenLDAP for [15](#)
  - disabling [16](#)
- identity source
  - forcing synchronization [16](#)
- information
  - how to send feedback about improving documentation [44](#)

## L

- local groups
  - editing [23](#)
- local users
  - changing password [28](#)
  - editing [27](#)
  - removing [28](#)
  - signing in [29](#)

## M

- Manage Your Own S3 Credentials permission
  - tenant account [21](#)

## O

- OpenLDAP
  - configuration guidelines for [15](#)

## P

- password
  - changing for local user [28](#)
  - root user [7](#)
- permissions
  - Manage Your Own S3 Credentials permission [21](#)
  - Root Access permission [21](#)

## Q

- quota
  - tenant account [8](#)

## R

- Root Access permission
  - tenant account [21](#)

root user  
password [7](#)  
permissions for [21](#)

## S

S3 access keys  
creating [30](#)  
creating for other users [33](#)  
managing [30](#)  
removing [32](#)  
removing for other users [34](#)

S3 clients  
relation to tenant [5](#)

S3 group policies  
specifying [18](#)

S3 tenants  
access keys for [30](#)  
cloning groups [22](#)  
creating groups [18](#)  
editing groups [23](#)  
removing groups [24](#)

signing in [7, 29](#)

storage usage  
tenant account [8](#)

suggestions  
how to send feedback about documentation [44](#)

Swift clients  
relation to tenant [5](#)

Swift tenants  
cloning groups [22](#)  
creating groups [20](#)  
editing groups [23](#)  
removing groups [24](#)

synchronizing  
identity source [16](#)

## T

tenant accounts

administering [4](#)  
creating S3 access keys [30, 33](#)  
managing S3 access keys [30](#)  
overview [5](#)  
quota for [8](#)  
removing S3 access keys [32, 34](#)  
signing in [7, 29](#)  
storage usage [8](#)

Tenant API

overview [10](#)

Tenant Management Interface

Dashboard [8](#)

using [7](#)

tenant users

creating S3 access keys [30, 33](#)  
removing S3 access keys [32, 34](#)  
signing in [7, 29](#)

Twitter

how to receive automatic notification of  
documentation changes [44](#)

## U

users

access keys for S3 tenants [30](#)  
changing password [28](#)  
cloning [26](#)  
creating [25](#)  
disabling identity federation [16](#)  
editing [27](#)  
managing [25](#)  
permissions for [21](#)  
removing [28](#)

## W

web browsers

supported [8](#)