



Creating a tenant account

StorageGRID 11.5

NetApp

January 04, 2024

This PDF was generated from <https://docs.netapp.com/us-en/storagegrid-115/admin/creating-tenant-account-if-storagegrid-is-not-using-sso.html> on January 04, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Creating a tenant account 1
 - Creating a tenant account if StorageGRID is not using SSO..... 3
 - Creating a tenant account if SSO is enabled 6

Creating a tenant account

You must create at least one tenant account to control access to the storage in your StorageGRID system.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have specific access permissions.

Steps

1. Select **Tenants**.

The Tenant Accounts page appears and lists any existing tenant accounts.

Tenant Accounts

View information for each tenant account.

Note: Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant and select **View Details**.

The screenshot displays the 'Tenant Accounts' interface. At the top, there is a navigation bar with buttons: '+ Create', 'View details', 'Edit', 'Actions', and 'Export to CSV'. To the right of these buttons is a search bar labeled 'Search by Name/ID'. Below the navigation bar is a table header with columns: 'Display Name', 'Space Used', 'Quota Utilization', 'Quota', 'Object Count', and 'Sign in'. Each column has a small icon indicating sorting or filtering options. The table body is empty, showing the text 'No results found.' At the bottom right of the table, there is a pagination control that says 'Show 20 rows per page'.

2. Select **Create**.

The Create Tenant Account page appears. The fields included on the page depend on whether single sign-on (SSO) has been enabled for the StorageGRID system.

- If SSO is not being used, the Create Tenant Account page looks like this.

Create Tenant Account

Tenant Details

Display Name

Protocol ☐ S3 ☐ Swift

Storage Quota (optional) GB ▾

Authentication [?](#)

Configure how the tenant account will be accessed.

Uses Own Identity Source ☒

Specify a password for the tenant's local root user.

Username root

Password

Confirm Password

Cancel

Save

- If SSO is enabled, the Create Tenant Account page looks like this.

Create Tenant Account

Tenant Details

Display Name

Protocol ☒ S3 ☐ Swift

Allow Platform Services ☒

Storage Quota (optional)

Authentication

Because single sign-on is enabled, the tenant must use the Grid Manager's identity federation service, and no local users can sign in. You must select an existing federated group to have the initial Root Access permission for the tenant.

Uses Own Identity Source ☐

Single sign-on is enabled. The tenant cannot use its own identity source.

Root Access Group

Cancel

Save

Related information

[Using identity federation](#)

[Configuring single sign-on](#)

Creating a tenant account if StorageGRID is not using SSO

When you create a tenant account, you specify a name, a client protocol, and optionally a storage quota. If StorageGRID is not using single sign-on (SSO), you must also specify whether the tenant account will use its own identity source and configure the initial password for the tenant's local root user.

About this task

If the tenant account will use the identity source that was configured for the Grid Manager, and you want to grant Root Access permission for the tenant account to a federated group, you must have imported that federated group into the Grid Manager. You do not need to assign any Grid Manager permissions to this admin group. See the instructions for [managing admin groups](#).

Steps

1. In the **Display Name** text box, enter a display name for this tenant account.

Display names do not need to be unique. When the tenant account is created, it receives a unique, numeric Account ID.

2. Select the client protocol that will be used by this tenant account, either **S3** or **Swift**.
3. For S3 tenant accounts, keep the **Allow Platform Services** check box selected unless you do not want this tenant to use platform services for S3 buckets.

If platform services are enabled, a tenant can use features, such as CloudMirror replication, that access external services. You might want to disable the use of these features to limit the amount of network bandwidth or other resources a tenant consumes. See “Managing platform services.”

4. In the **Storage Quota** text box, optionally enter the maximum number of gigabytes, terabytes, or petabytes that you want to make available for this tenant’s objects. Then, select the units from the drop-down list.

Leave this field blank if you want this tenant to have an unlimited quota.



A tenant’s storage quota represents a logical amount (object size), not a physical amount (size on disk). ILM copies and erasure coding do not contribute to the amount of quota used. If the quota is exceeded, the tenant account cannot create new objects.



To monitor each tenant account’s storage usage, select **Usage**. Tenant accounts can also monitor their own storage usage from the Dashboard in the Tenant Manager or with the Tenant Management API. Note that a tenant’s storage usage values might become out of date if nodes are isolated from other nodes in the grid. The totals will be updated when network connectivity is restored.

5. If the tenant will manage its own groups and users, follow these steps.
 - a. Select the **Uses Own Identity Source** check box (default).



If this check box is selected and you want to use identity federation for tenant groups and users, the tenant must configure its own identity source. See the instructions for using tenant accounts.

- b. Specify a password for the tenant’s local root user.
6. If the tenant will use the groups and users configured for the Grid Manager, follow these steps.
 - a. Unselect the **Uses Own Identity Source** check box.
 - b. Do either or both of the following:
 - In the Root Access Group field, select an existing federated group from the Grid Manager that should have the initial Root Access permission for the tenant.



If you have adequate permissions, the existing federated groups from the Grid Manager are listed when you click the field. Otherwise, enter the group’s unique name.

- Specify a password for the tenant’s local root user.
7. Click **Save**.

The tenant account is created.


8. Optionally, access the new tenant. Otherwise, go to the step for [accessing the tenant later](#).

| If you are... | Do this... |
|---|--|
| Accessing the Grid Manager on a restricted port | <p>Click Restricted to learn more about accessing this tenant account.</p> <p>The URL for the Tenant Manager has this format:</p> <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> <ul style="list-style-type: none">• <i>FQDN_or_Admin_Node_IP</i> is a fully qualified domain name or the IP address of an Admin Node• <i>port</i> is the tenant-only port• <i>20-digit-account-id</i> is the tenant's unique account ID |
| Accessing the Grid Manager on port 443 but you did not set a password for the local root user | Click Sign In , and enter the credentials for a user in the Root Access federated group. |
| Accessing the Grid Manager on port 443 and you set a password for the local root user | Go to the next step to sign in as root . |

9. Sign in to the tenant as root:

a. From the Configure Tenant Account dialog box, click the **Sign in as root** button.

Configure Tenant Account

 Account **S3 tenant** created successfully.

If you are ready to configure this tenant account, sign in as the tenant's root user. Then, click the links below.

Sign in as root

- [Buckets](#) - Create and manage buckets.
- [Groups](#) - Manage user groups, and assign group permissions.
- [Users](#) - Manage local users, and assign users to groups.

Finish

A green check mark appears on the button, indicating that you are now signed in to the tenant account as the root user.

- b. Click the links to configure the tenant account.

Each link opens the corresponding page in the Tenant Manager. To complete the page, see the instructions for using tenant accounts.

- c. Click **Finish**.

10. To access the tenant later:

| If you are using... | Do one of these... |
|---------------------|---|
| Port 443 | <ul style="list-style-type: none">• From the Grid Manager, select Tenants, and click Sign in to the right of the tenant name.• Enter the tenant's URL in a web browser: <code>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</code><ul style="list-style-type: none">◦ <i>FQDN_or_Admin_Node_IP</i> is a fully qualified domain name or the IP address of an Admin Node◦ <i>20-digit-account-id</i> is the tenant's unique account ID |
| A restricted port | <ul style="list-style-type: none">• From the Grid Manager, select Tenants, and click Restricted.• Enter the tenant's URL in a web browser: <code>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</code><ul style="list-style-type: none">◦ <i>FQDN_or_Admin_Node_IP</i> is a fully qualified domain name or the IP address of an Admin Node◦ <i>port</i> is the tenant-only restricted port◦ <i>20-digit-account-id</i> is the tenant's unique account ID |

Related information

[Controlling access through firewalls](#)

[Managing platform services for S3 tenant accounts](#)

[Use a tenant account](#)

Creating a tenant account if SSO is enabled

When you create a tenant account, you specify a name, a client protocol, and optionally a storage quota. If single sign-on (SSO) is enabled for StorageGRID, you also specify which federated group has Root Access permission to configure the tenant account.

Steps

1. In the **Display Name** text box, enter a display name for this tenant account.

Display names do not need to be unique. When the tenant account is created, it receives a unique, numeric Account ID.

2. Select the client protocol that will be used by this tenant account, either **S3** or **Swift**.
3. For S3 tenant accounts, keep the **Allow Platform Services** check box selected unless you do not want this tenant to use platform services for S3 buckets.

If platform services are enabled, a tenant can use features, such as CloudMirror replication, that access external services. You might want to disable the use of these features to limit the amount of network bandwidth or other resources a tenant consumes. See “Managing platform services.”

4. In the **Storage Quota** text box, optionally enter the maximum number of gigabytes, terabytes, or petabytes that you want to make available for this tenant's objects. Then, select the units from the drop-down list.

Leave this field blank if you want this tenant to have an unlimited quota.



A tenant's storage quota represents a logical amount (object size), not a physical amount (size on disk). ILM copies and erasure coding do not contribute to the amount of quota used. If the quota is exceeded, the tenant account cannot create new objects.



To monitor each tenant account's storage usage, select **Usage**. Tenant accounts can also monitor their own storage usage from the Dashboard in the Tenant Manager or with the Tenant Management API. Note that a tenant's storage usage values might become out of date if nodes are isolated from other nodes in the grid. The totals will be updated when network connectivity is restored.

5. Notice that the **Uses Own Identity Source** check box is unchecked and disabled.

Because SSO is enabled, the tenant must use the identity source that was configured for the Grid Manager. No local users can sign in.

6. In the **Root Access Group** field, select an existing federated group from the Grid Manager to have the initial Root Access permission for the tenant.



If you have adequate permissions, the existing federated groups from the Grid Manager are listed when you click the field. Otherwise, enter the group's unique name.

7. Click **Save**.

The tenant account is created. The Tenant Accounts page appears, and it includes a row for the new tenant.

8. If you are a user in the Root Access group, optionally click the **Sign in** link for the new tenant to immediately access the Tenant Manager, where you can configure the tenant. Otherwise, provide the URL for the **Sign in** link to the tenant account's administrator. (The URL for a tenant is the fully qualified domain name or IP address of any Admin Node, followed by `/?accountId=20-digit-account-id`.)



An access denied message is displayed if you click **Sign in**, but you do not belong to the Root Access group for the tenant account.

Related information

[Configuring single sign-on](#)

[Managing platform services for S3 tenant accounts](#)

[Use a tenant account](#)

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.