



Getting Started with a Paid Subscription

SaaS Backup For Office 365

NetApp
March 22, 2021

This PDF was generated from https://docs.netapp.com/us-en/saasbackupO365/concept_paid_subscription_workflow.html on March 22, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Getting Started with a Paid Subscription 1
 - Workflow for getting started with a paid subscription to SaaS Backup for Microsoft 365 1
 - Creating a new Microsoft Office 365 service account 3
 - Configuring Impersonation for Microsoft Exchange Online 6
 - Signing up for a paid subscription of SaaS Backup for Microsoft 365 8
 - Scheduling your first backup 10
 - Performing an immediate backup of a specific backup policy 10
 - Paid subscription data deletion 11

Getting Started with a Paid Subscription

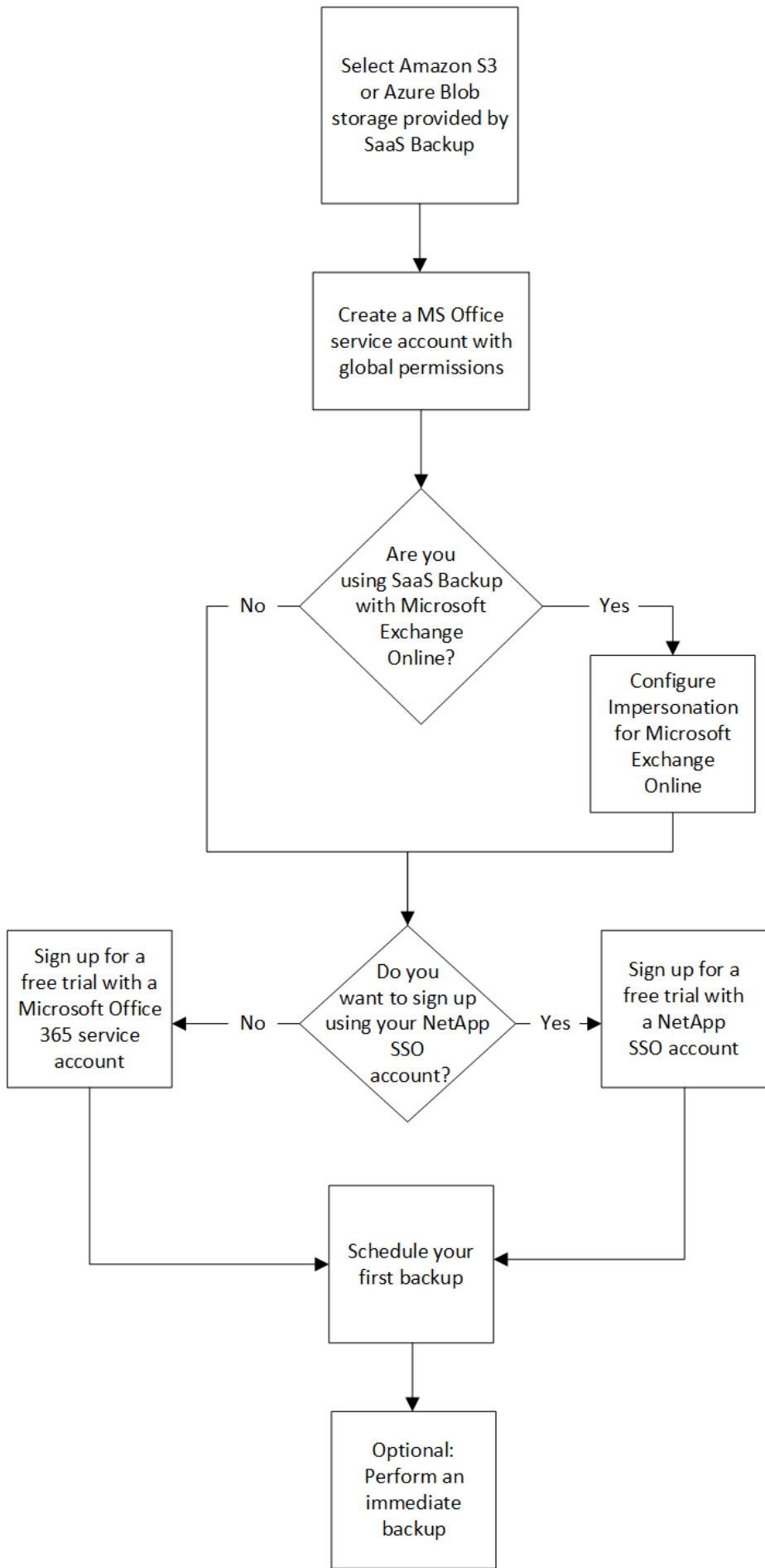
Workflow for getting started with a paid subscription to SaaS Backup for Microsoft 365

To get started with a paid subscription to SaaS Backup for Microsoft 365, you must do the following:

1. Decide if you will use Amazon S3 or Azure Blob storage provided by SaaS Backup.

[Storage types you can use with SaaS Backup.](#)

2. [Create a MS Office service account with global permissions.](#)
3. If needed, [configure Impersonation for Microsoft Exchange Online.](#)
4. [Sign up for SaaS Backup for Microsoft 365](#) using your Microsoft 365 account or your NetApp SSO account.
5. [Schedule your first backup](#)
6. [Optional: Immediately back up your data](#)

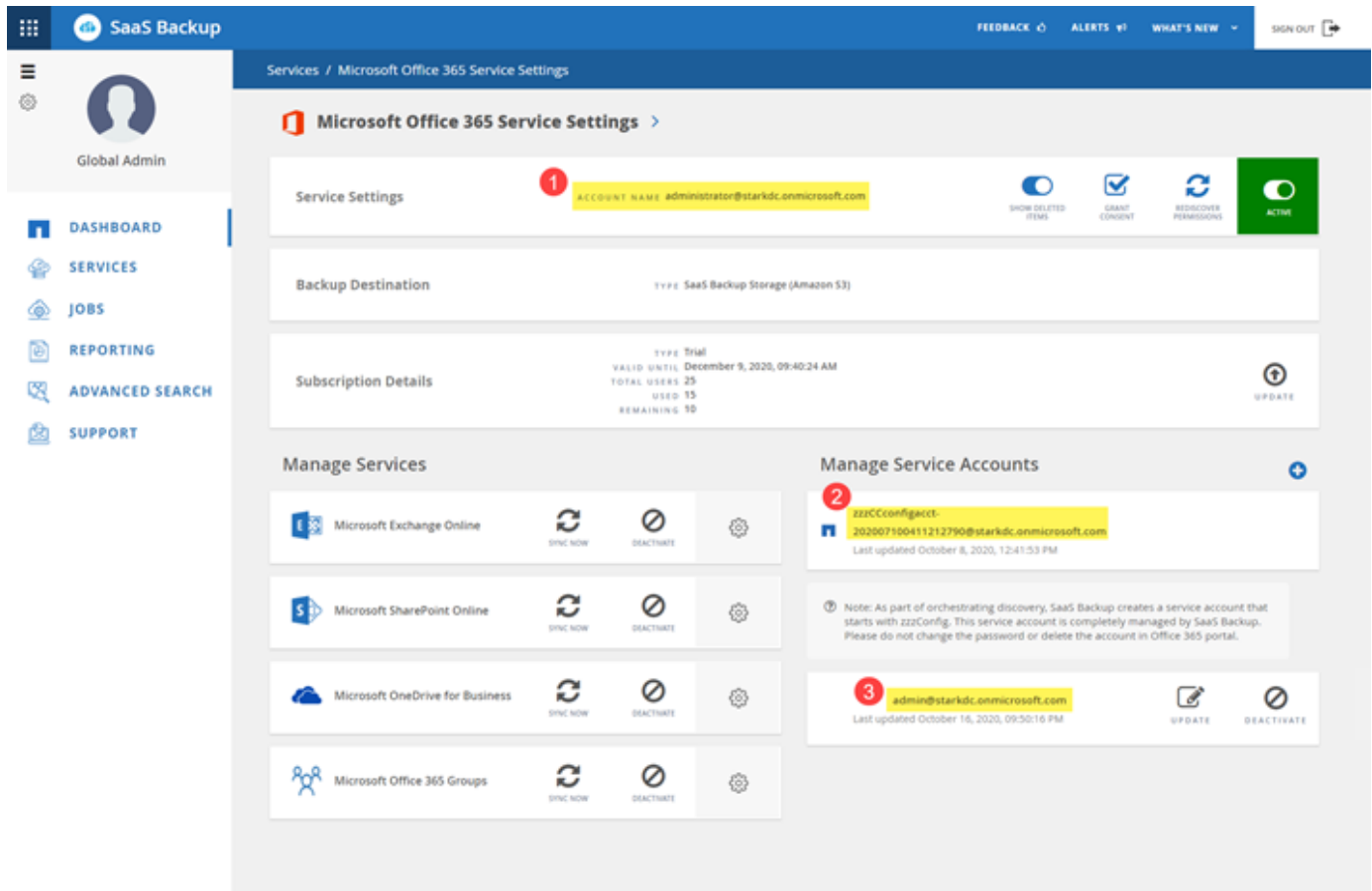


Creating a new Microsoft Office 365 service account

When you create your new Microsoft Office 365 account, this account must have global administration permissions with a valid and assigned Microsoft Office 365 license.

This is not the only service account used to manage SaaS Backup for Microsoft Office 365. The following image points out the different service account types with descriptions below.

Service account descriptions



- 1 The account used to sign up for SaaS Backup; it requires global administration permissions with a valid Microsoft Office 365 license during sign up. It can be used for backup and restore operations.
- 2 A **zzzCCconfigacct** is automatically created as a service account to discover Office 365 Groups.
- 3 An additional service account can be added to enhance performance of backup and restore operations.

Creating a new MS Office 365 service account with global administrator permissions

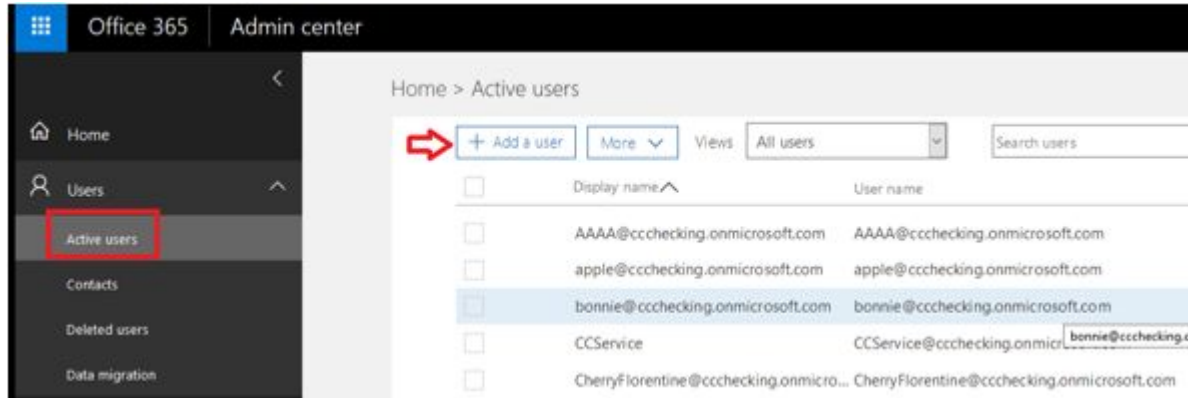
During sign up, create an account with global permissions and a valid Microsoft Office 365 license. You can remove the global administration permissions and the license from this account after you complete sign up.

Steps

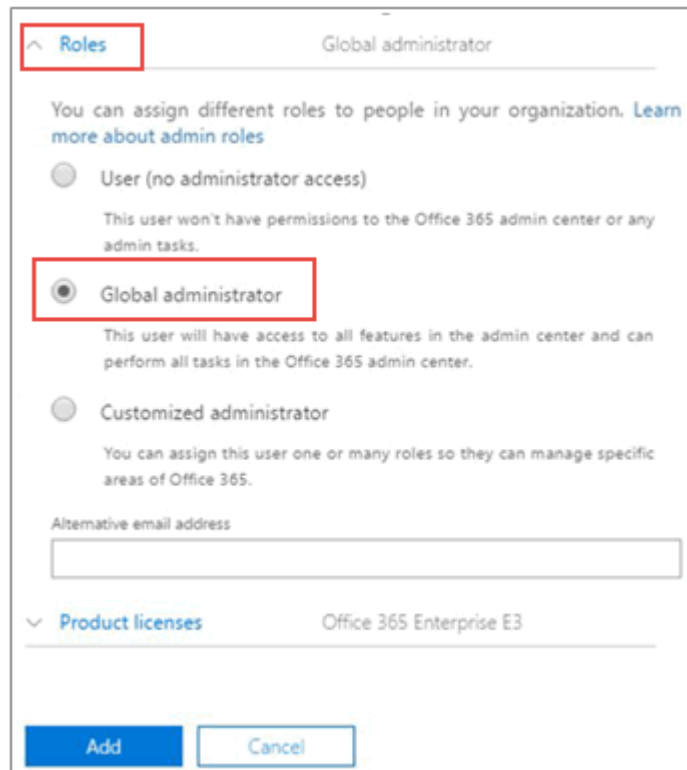
1. Log in to your Microsoft 365 Management portal using an account with administrative privileges.
2. Click **Users**.



3. Select **Active users**, and then click **Add a user**.



4. Enter the details of the new service account.
 - First name
 - Last name
 - Display name
 - User name
The user name is the name of the service account.
5. Expand **Roles**, select **Global administrator** as the role, and then click **Add**.



The service account details are sent to the administrator.

6. Log in to your Microsoft 365 Management Portal with the new account to activate it.
7. After signup, ensure this service account maintains three permissions:
 - Exchange Administrator
 - SharePoint Administrator
 - Application Impersonation Role

This is especially important if you restrict the individual licenses for the Global administrator role.

ZZZ Config account

As part of your SaaS Backup subscription, a new account is created with ZZZ CC Config [GUID].

This auto-created account is used for discovering Shared/Archive mailboxes and private groups. It should have Exchange and SharePoint permissions (customized administrator in O365). It is recommended that you exclude this account from MFA policies.

To avoid any discovery or backup failures, leave the account as is.

Creating additional service accounts

Service Accounts can be added in SaaS Backup for Microsoft Office 365 to improve the backup performance for a customer. A service account is a Microsoft Office 365 user account without a license; it is used for backup and restore operations.

This type of account requires 3 permissions:

- Exchange administrator
- SharePoint administrator
- Application impersonation role

To add an additional service account, the service account must already exist in your Microsoft Office 365 environment. If you do not have an existing account, then create one.



To optimize performance, it is recommended that you have 1 service account added per 1000 users in Office 365.

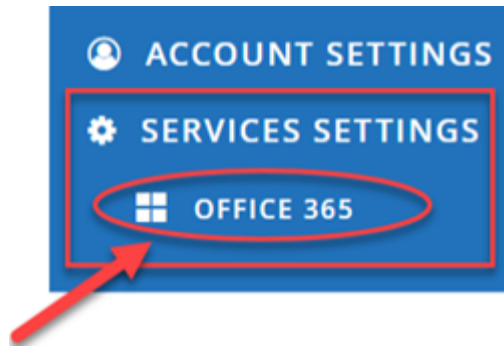
Steps

1. Log in to SaaS Backup for Microsoft Office 365.

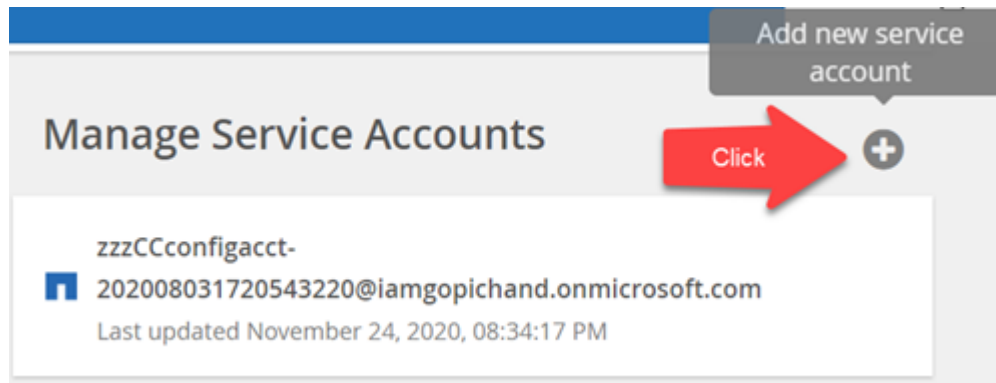
2.



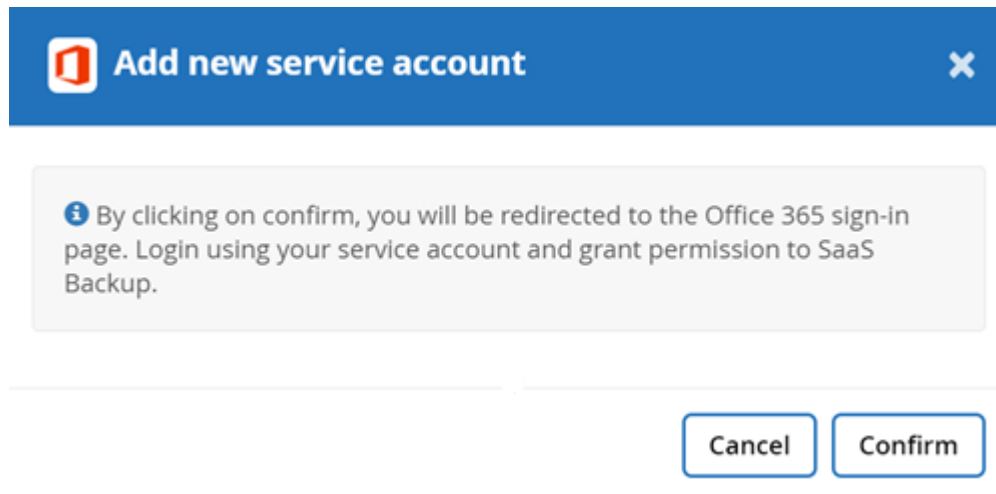
3. Click **Service Settings**.



4. To add a service account, click  under **Manage service accounts**.



A confirmation message pops up.



5. Click **Confirm**.
6. On the Microsoft Office 365 sign-in page, provide the credentials of the above mentioned service account to add it to SaaS Backup.

Configuring Impersonation for Microsoft Exchange Online

If you plan to use SaaS Backup with Microsoft Exchange Online, you must configure impersonation. Impersonation allows your Microsoft 365 service account to impersonate

user accounts and access associated permissions.

Automatically configuring impersonation

To automatically configure impersonation, run [MSDN PowerShell Commands](#).

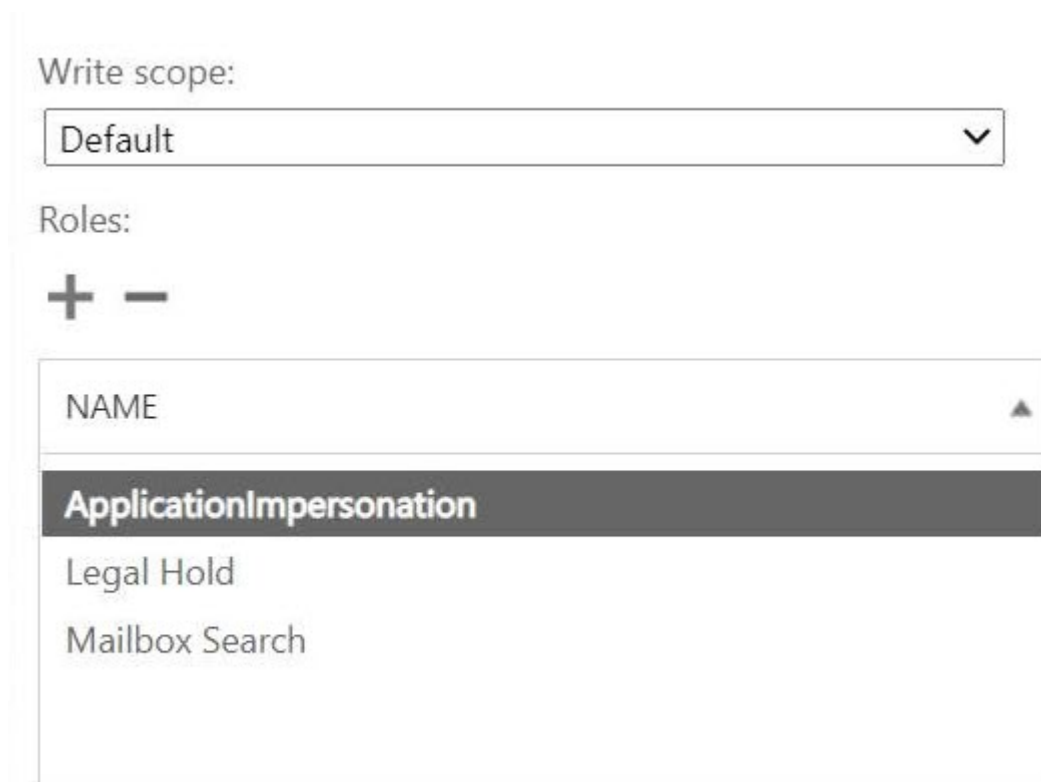
Manually configuring impersonation

You can manually configure impersonation with your Microsoft 365 administrator account as well as with added Microsoft 365 service accounts in SaaS Backup. For more information about Microsoft 365 service accounts, go to [creating a Microsoft 365 service account with global permissions](#).

To manually configure impersonation do the following:

Steps

1. Log in to your Microsoft 365 service account.
2. Select the **Exchange** tab.
3. On the left, under Dashboard, select **Permissions**.
4. Click **Admin roles**.
5. Double-click in the right pane to select **Discovery management**.
6. Under **Roles**, click the **+** symbol.



The screenshot shows a portion of the Microsoft 365 Admin Center interface. At the top, there is a 'Write scope:' label followed by a dropdown menu currently set to 'Default'. Below this is a 'Roles:' label with a plus sign (+) and a minus sign (-) icon. A list of roles is displayed below the icons, with 'ApplicationImpersonation' selected and highlighted in a dark grey bar. Other roles visible in the list are 'Legal Hold' and 'Mailbox Search'.

NAME
ApplicationImpersonation
Legal Hold
Mailbox Search

7. Select **ApplicationImpersonation** from the drop-down menu.
8. Click **Add**.
9. Click **OK**.

10. Verify that **ApplicationImpersonation** was added under **Roles**.
11. Under **Members**, click the **+** symbol.

Members:



NAME	DISPLAY NAME
AirBender	Air Bender

A new window appears

12. Choose the user name.
13. Click **Add**.
14. Click **OK**.
15. Verify that the user name appears in the **Members** section.
16. Click **Save**.

Signing up for a paid subscription of SaaS Backup for Microsoft 365

You can sign up for SaaS Backup for Microsoft 365 with your Microsoft 365 service account or with your NetApp SSO account.

Signing up for a paid subscription with a Microsoft 365 service account

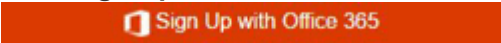
Users who sign up for a paid subscription with a Microsoft 365 service account need to enable Basic Authentication to use SaaS Backup. SaaS Backup supports Basic Authentication only. If your Microsoft 365 tenant was created beginning in October 2020, and it has no recorded usage, you may encounter authentication failures. Ensure that you disable Modern Authentication for your Microsoft 365 service account.

[Learn how to disable Modern Authentication](#)

Steps

1. Enter the SaaS Backup for Microsoft 365 URL into your web browser:
<https://saasbackup.netapp.com>
2. Select your region.
Your tenancy is created in the selected region. Your data will be stored in that datacenter location and

cannot be changed later.




3. Click **Sign up** at the bottom of the landing page.
4. Accept the End-User License Agreement.
5. Click **Sign Up with Office 365**.
A red button with a white icon of a person and the text "Sign Up with Office 365".
6. Enter the email address and password for your Microsoft 365 global administrator service account, and then click **Sign in**.
A list of the permissions requested by SaaS Backup for Microsoft 365 is displayed.
7. Click **Accept**.
8. Enter the requested user information.
9. Click **Sign up**.
Your user name and a list of permissions given to SaaS Backup for Microsoft 365 is displayed.
10. Click **Next**.
A list of the available Microsoft 365 services is displayed.
11. Select the Microsoft 365 services that you want to activate.
12. Click **Next**.
13. If you purchased your license through NetApp, your subscription types are displayed
Click [here](#) for additional steps.
14. If you purchased your license through a Cloud Marketplace, such as AWS, your license information is displayed.
Click [here](#) for additional steps.

Signing up for a paid subscription with a NetApp SSO account

Before you begin

To validate your subscription, you must have a NetApp SSO user ID and password. If you do not have a NetApp SSO account, go to <https://mysupport.netapp.com/eservice/public/now.do> to register for one. After your request has been processed, you will receive an email notification containing your NetApp SSO credentials. It will take approximately 24 hours to process the request and send the notification email.

Steps

1. Enter the SaaS Backup for Microsoft 365 URL into your web browser:
<https://saasbackup.netapp.com>
2. Click Sign up at the bottom of the landing page.
3. Accept the End-User License Agreement.
4. Click **Sign Up with NetApp SSO**.
A blue button with the text "Sign Up with NetApp SSO".
5. Enter your NetApp SSO and password, and then click **LOGIN**.
6. Enter the requested user information, and then click **Sign Up**.
7. Click the **Services**  icon.
The Services icon is a blue circle with a white plus sign.
8. Click the Microsoft 365  icon to select the SaaS service.
The Microsoft 365 icon is a red square with a white 'O' shape inside.

9. Click **Add Microsoft Office 365 Account**.
10. Enter the email address and password for your Microsoft 365 global administrator service account, and then click **Sign in**.
A list of the permissions requested by SaaS Backup for Microsoft 365 is displayed.
11. Click **Accept**.
12. Click **Next**.
A list of the available Microsoft 365 services is displayed.
13. Select the Microsoft 365 services that you want to activate.
14. Click **Next**.
15. Select **Licensed** for the subscription type.
16. Enter the requested information, and then validate the subscription.
17. Click **Next**.
18. Select your backup storage option.
 - a. Click **SaaS Backup Provided Storage**.
 - b. Select the **Amazon S3** or **Azure Blob** storage option.
 - c. Select the **AWS S3** or **Azure Blob** region for your backup.
You should select the region that is the closest to the physical location of the data you are backing up.
 - d. Click **Next**.
 - e. Review your configuration, and then click **Save**.

Scheduling your first backup

When you set up SaaS Backup for Microsoft 365, by default, your data is unprotected. You must move your data from the unprotected tier to one of the protected tiers to so that your data will be backed up during the next scheduled back up of the selected tier.

Steps

1. From the Dashboard, select the service containing the unprotected data.
2. Click **view** next to the number of unprotected mailboxes, MySites, sites or groups.
3. Select the items that you want to protect.
4. Click the **Groups** menu.



5. Select the **tier** for the backup policy that you want to assign.
See [Backup Policies](#) for a description of the backup policy tiers.
6. Click **Apply**.

Performing an immediate backup of a specific backup policy

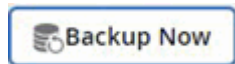
When you set up SaaS Backup for Microsoft 365, by default, all of your data is unprotected. After you move your data to a protected tier, you can perform an immediate

backup of the tier to which you moved your data. This prevents your data from being at risk until the first scheduled backup occurs. If you can wait for the first scheduled backup, performing an immediate backup is not necessary.

You can perform an immediate backup any time you deem necessary for data protection. If you are running a trial version of SaaS Backup for Microsoft 365, you can only perform three immediate backups per day, per service.

Steps

1. From the Dashboard, select the service for which you want to perform an immediate backup.
2. Under **Backup Policies**, click the tier that you want to back up.
3. Click Backup Now.



A message is displayed indicating that the services under the selected tier will be placed in the job queue for immediate backup.

4. Click **Confirm**.
A message is displayed indicating that the backup job was created.
5. Click **View the job progress** to monitor the progress of the backup.

Paid subscription data deletion

If you do not renew your licensed version of SaaS Backup for Microsoft 365, the data used during your subscription is deleted as follows:

If your SaaS Backup free trial is...	Number of days after paid subscription ends	Your data is...
Expired	1-30 days	Available: The administrator has normal access and can perform manual backups and restores. SaaS Backup continues to display alerts and send out notifications.
Disabled	31-60 days	Deactivated: The administrator does not have access to the SaaS Backup portal. If subscription is renewed during this period, data can be reactivated.
Deprovisioned	61 or more days	Deleted: All data is deleted and your tenant account is removed.

Copyright Information

Copyright © 2021 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

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.