Get started

SaaS Backup for Microsoft 365

NetApp
February 12, 2024

Table of Contents

Get started

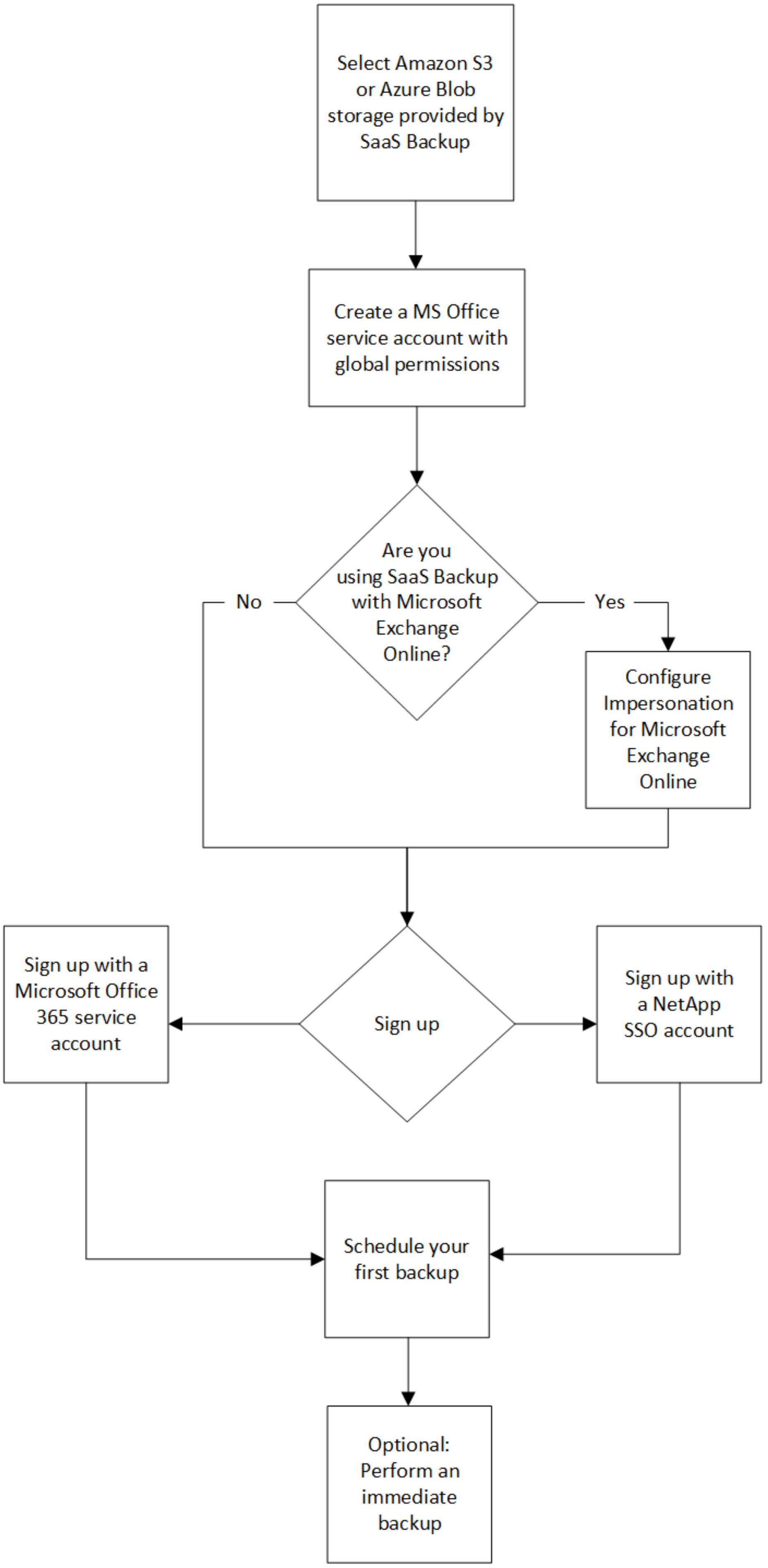
Workflow for getting started

To get started with 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

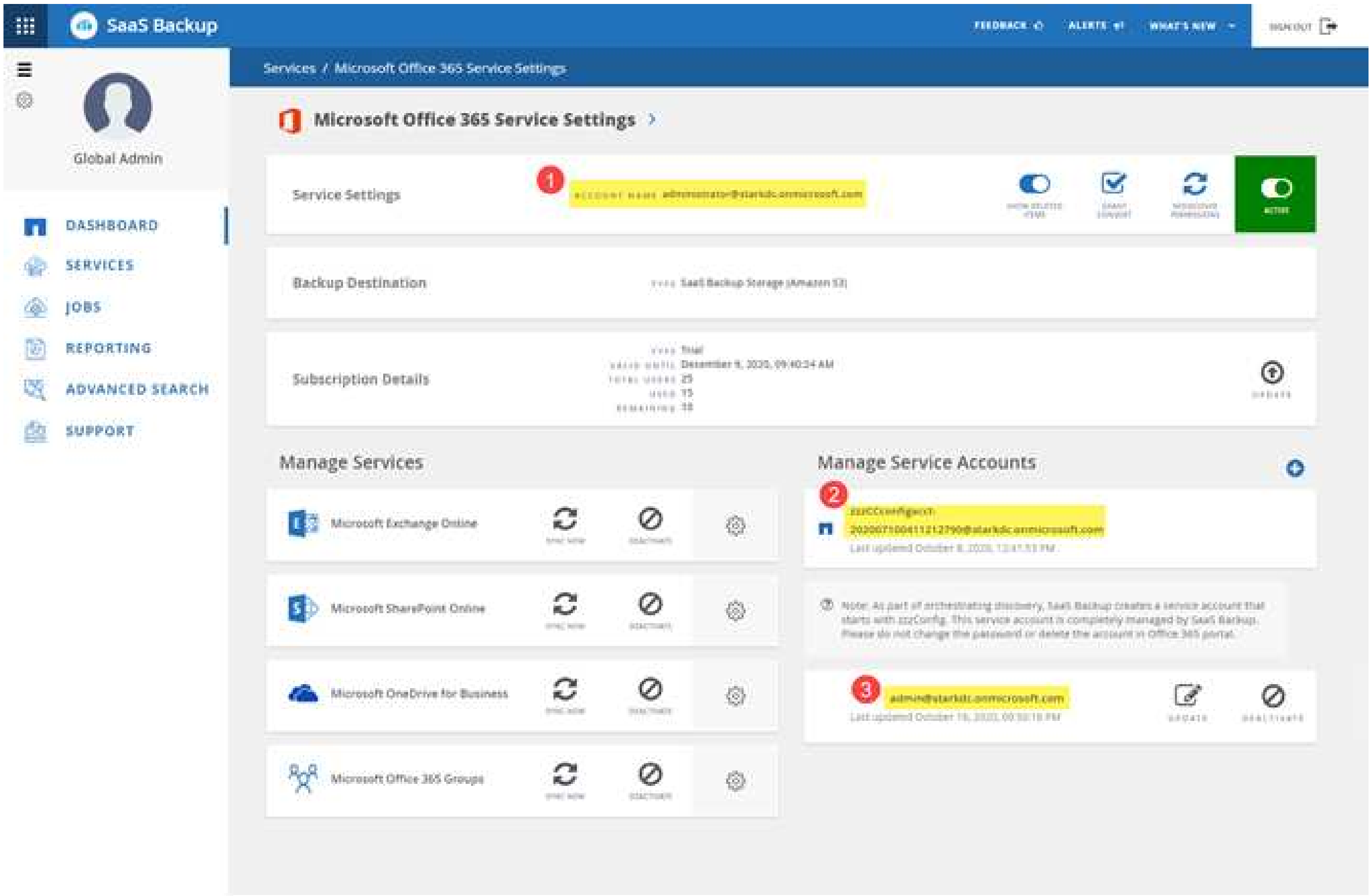

Select Amazon S3 or Azure Blob storage provided by SaaS Backup
Create a MS Office service account with global permissions
Are you using SaaS Backup with Microsoft Exchange Online?
No
Yes
Configure Impersonation for Microsoft Exchange Online
Sign up
Sign up with a Microsoft Office 365 service account
Sign up with a NetApp SSO account
Schedule your first backup
Optional: Perform an immediate backup

Create a new Microsoft 365 service account

When you create your new Microsoft 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 365. The following image points out the different service account types with descriptions below.

Service account descriptions



Service Settings — ACCOUNT NAME administrator@starkdc.onmicrosoft.com

Backup Destination — TYPE SaaS Backup Storage (Amazon S3)

Subscription Details — TYPE Trial; VALID UNTIL December 9, 2020, 09:40:34 AM; TOTAL USERS 25; USED 15; REMAINING 10

zzzCCconfigacct-202007100411212790@starkdc.onmicrosoft.com
Last updated October 8, 2020, 12:41:53 PM

Note: As part of orchestrating discovery, SaaS Backup creates a service account that starts with zzzConfig. This service account is completely managed by SaaS Backup. Please do not change the password or delete the account in Office 365 portal.

admin@starkdc.onmicrosoft.com
Last updated October 16, 2020, 00:50:18 PM

1 The account used to sign up for SaaS Backup; it requires global administration permissions with a valid Microsoft 365 license during signup. It can be used for backup and restore operations.

2 A **zzzCCconfigacct** is automatically created as a service account to discover Microsoft 365 Groups. When Modern Authentication is enabled, you do not have a ZZZ Config service account.

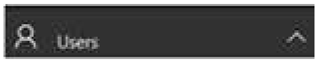
3 An additional service account can be added to enhance performance of backup and restore operations.

Create a new MS 365 service account with global administrator permissions

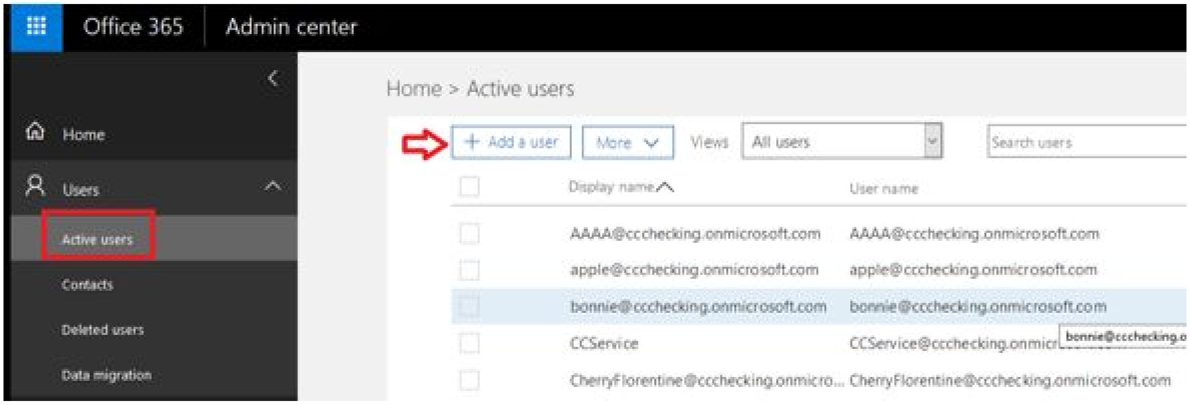
During signup, create an account with global permissions and a valid Microsoft 365 license. You can remove the global administration permissions and the license from this account after you complete signup.

Steps

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

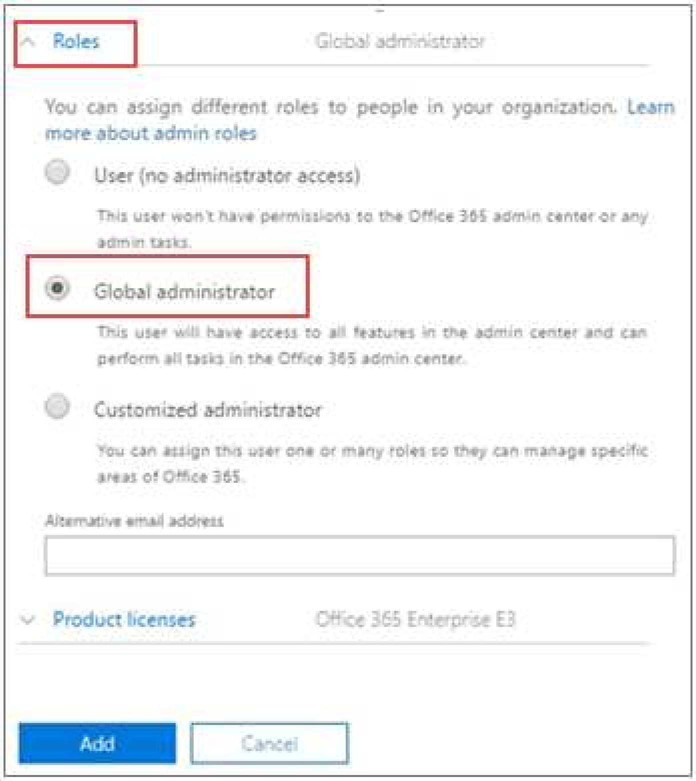


3. Select **Active users**, and then click **Add a user**.



Display name	User name
AAAA@ccchecking.onmicrosoft.com	AAAA@ccchecking.onmicrosoft.com
apple@ccchecking.onmicrosoft.com	apple@ccchecking.onmicrosoft.com
bonnie@ccchecking.onmicrosoft.com	bonnie@ccchecking.onmicrosoft.com
CCService	CCService@ccchecking.onmicr bonnie@ccchecking.o
CherryFlorentine@ccchecking.onmicro...	CherryFlorentine@ccchecking.onmicrosoft.com

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**.



You can assign different roles to people in your organization. Learn more about admin roles

○ User (no administrator access)

This user won't have permissions to the Office 365 admin center or any admin tasks.

● Global administrator

This user will have access to all features in the admin center and can perform all tasks in the Office 365 admin center.

○ Customized administrator

You can assign this user one or many roles so they can manage specific areas of Office 365.

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 service account

ZZZ Config service account is an auto-created account used for discovering Shared/Archive mailboxes and private groups if you use Basic Authentication. It should have Exchange and SharePoint permissions (customized administrator in M365). It is recommended that you exclude this account from MFA policies. To avoid any discovery or backup failures, leave the account as is.

If you enable Modern Authentication, the ZZZ Config service account is removed.

New customers do not have a ZZZ Config service account.

Create additional service accounts

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

This type of account requires 3 permissions:

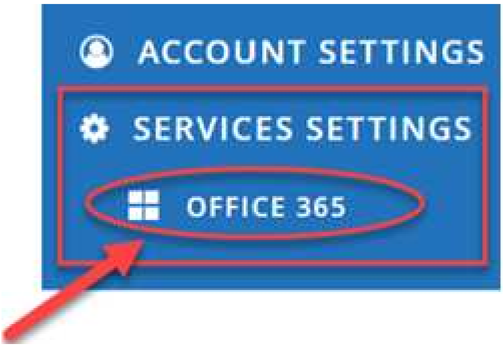
- Exchange administrator
- SharePoint administrator
- Application impersonation role

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

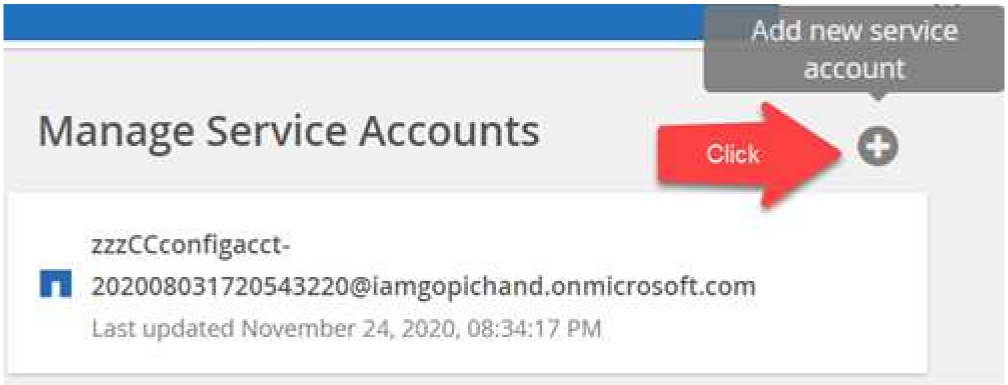
> To optimize performance, it is recommended that you have 1 service account added per 1000 users in Office 365.

Steps

1. Log in to SaaS Backup for Microsoft 365.
2. Click ⚙.
3. Click **Service Settings**.

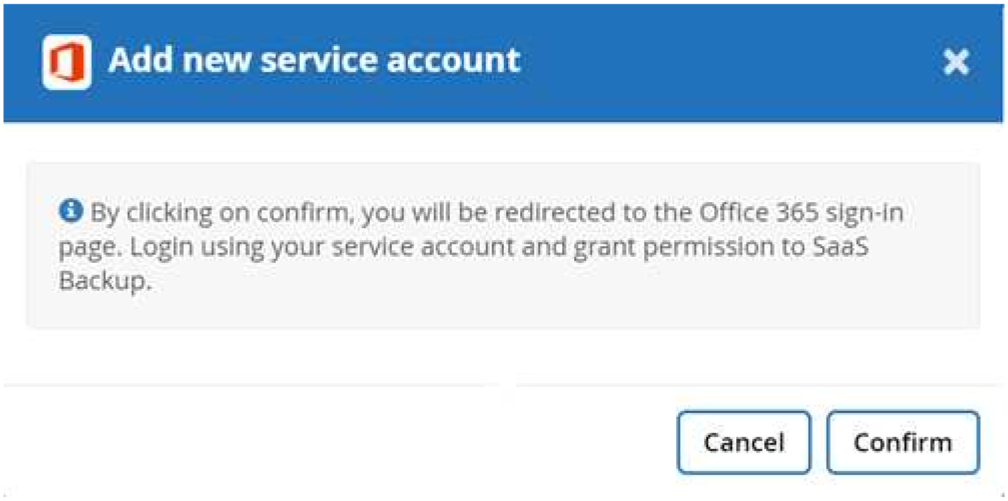


4. To add a service account, click ⊕ under **Manage service accounts**.



zzzCCconfigacct-20200831720543220@iamgopichand.onmicrosoft.com
Last updated November 24, 2020, 08:34:17 PM

A confirmation message pops up.



By clicking on confirm, you will be redirected to the Office 365 sign-in page. Login using your service account and grant permission to SaaS Backup.

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

Configure 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 configure impersonation

To automatically configure impersonation, run MSDN PowerShell Commands.

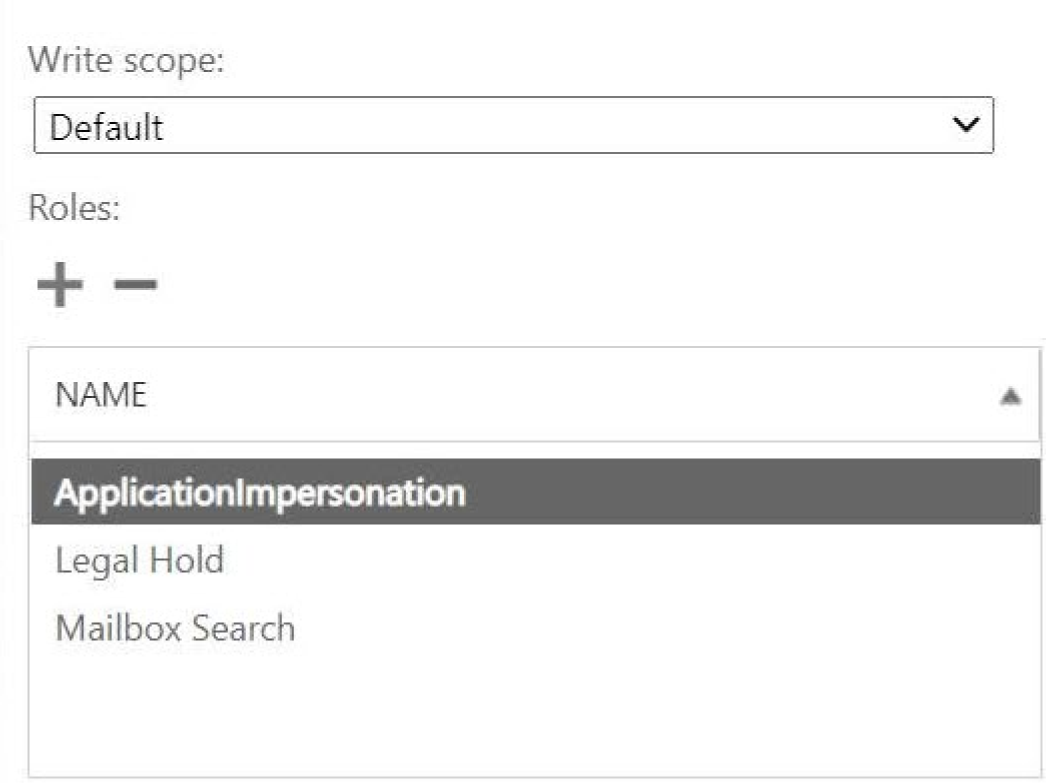
Manually configure impersonation

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.



Write scope:

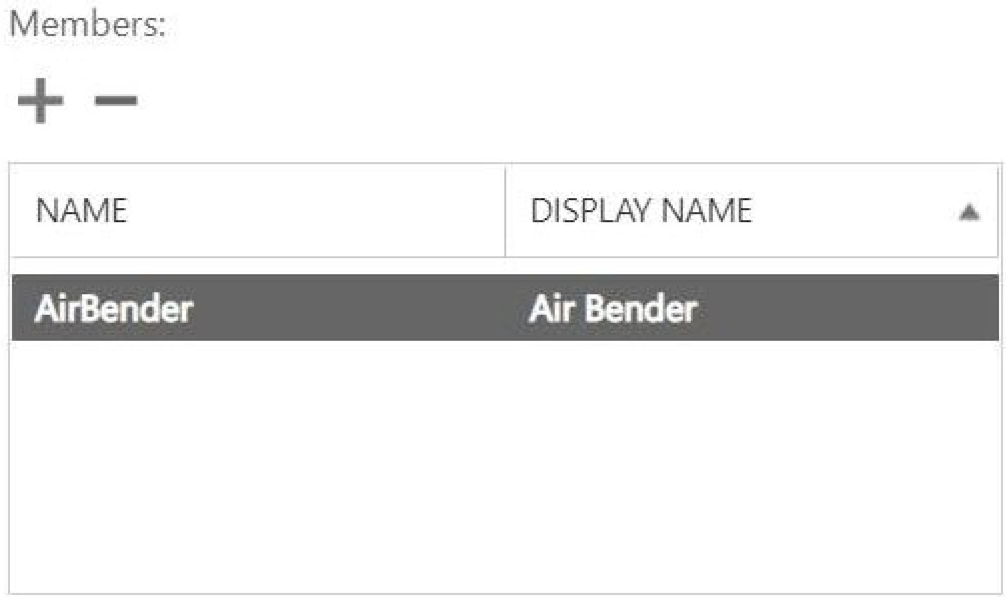
Default

Roles:

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**.

Sign up for 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.

Sign up with a Microsoft 365 service account

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.**

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.

Sign up 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**.

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.
8. Click the Microsoft 365 icon to select the SaaS service.
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**.

Schedule 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**.

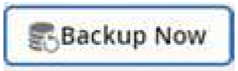
Perform an immediate backup of a specific backup policy

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.

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 paid subscription 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

Trademark information