



## **Los geht's**

### **SaaS Backup for Microsoft 365**

NetApp

December 20, 2023

This PDF was generated from [https://docs.netapp.com/de-de/saasbackupO365/concept\\_paid\\_subscription\\_workflow.html](https://docs.netapp.com/de-de/saasbackupO365/concept_paid_subscription_workflow.html) on December 20, 2023. Always check docs.netapp.com for the latest.

# Inhalt

- Los geht's ..... 1
  - Workflow für die ersten Schritte ..... 1
  - Erstellen Sie ein neues Microsoft 365-Servicekonto ..... 3
  - Impersonation für Microsoft Exchange Online konfigurieren ..... 7
  - Melden Sie sich für SaaS Backup für Microsoft 365 an ..... 9
  - Planen Sie Ihr erstes Backup ..... 10
  - Sofortiges Backup einer spezifischen Backup-Richtlinie durchführen ..... 11
  - Datenlöschung ..... 11

# Los geht's

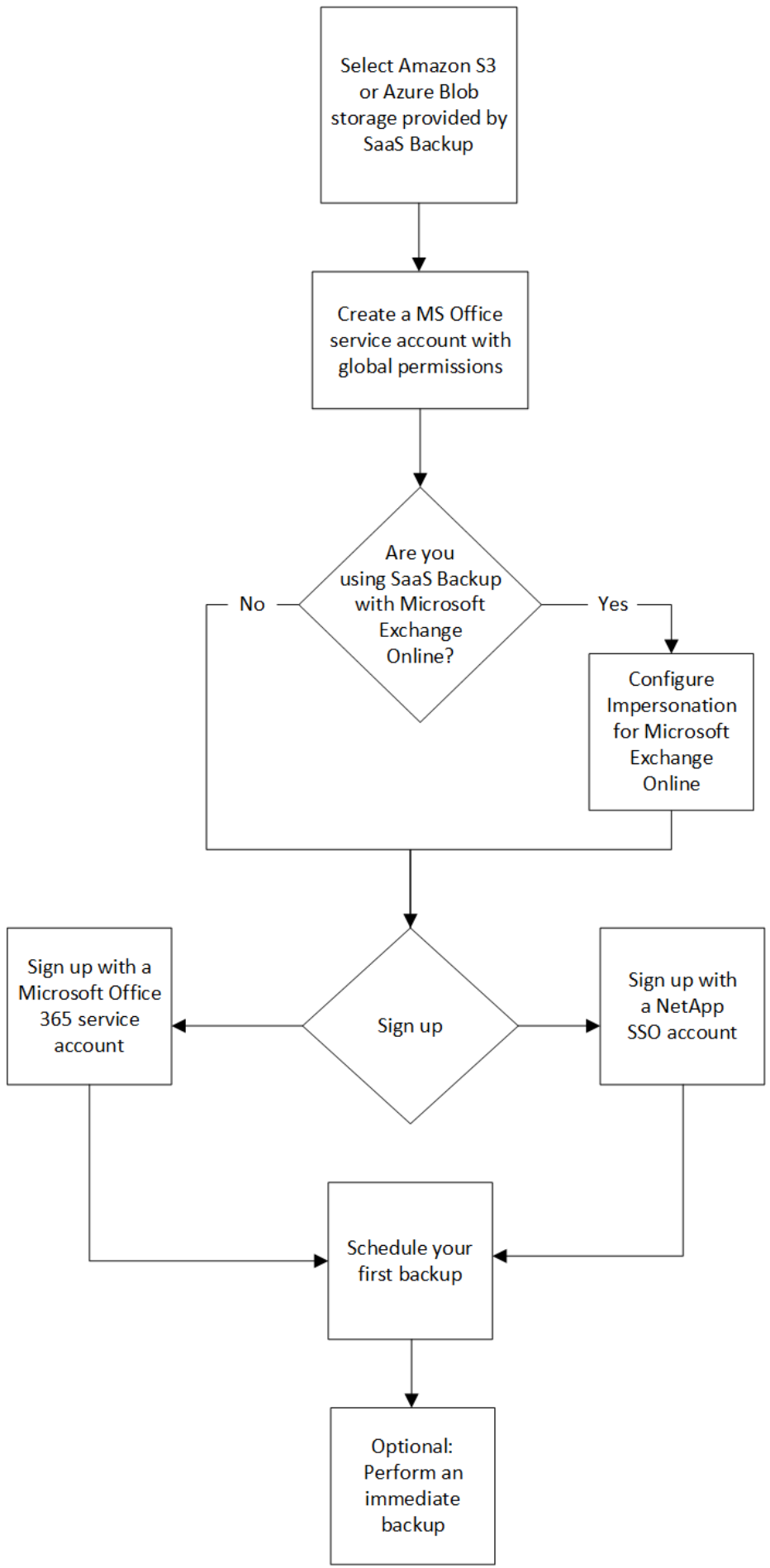
## Workflow für die ersten Schritte

Für den Einstieg in SaaS Backup für Microsoft 365 sind folgende Maßnahmen erforderlich:

1. Entscheiden Sie, ob Sie den von SaaS Backup bereitgestellten Amazon S3 oder Azure Blob Storage nutzen möchten.

["Storage-Typen, die Sie mit SaaS Backup verwenden können"](#).

2. ["Erstellen eines MS Office Servicekontos mit globalen Berechtigungen"](#).
3. Bei Bedarf ["Impersonation für Microsoft Exchange Online konfigurieren"](#).
4. ["Melden Sie sich für SaaS Backup für Microsoft 365 an"](#) Verwenden Ihres Microsoft 365 Kontos oder Ihres NetApp SSO-Kontos.
5. ["Planen Sie Ihr erstes Backup"](#)
6. ["Optional: Sichern Sie Ihre Daten sofort"](#)

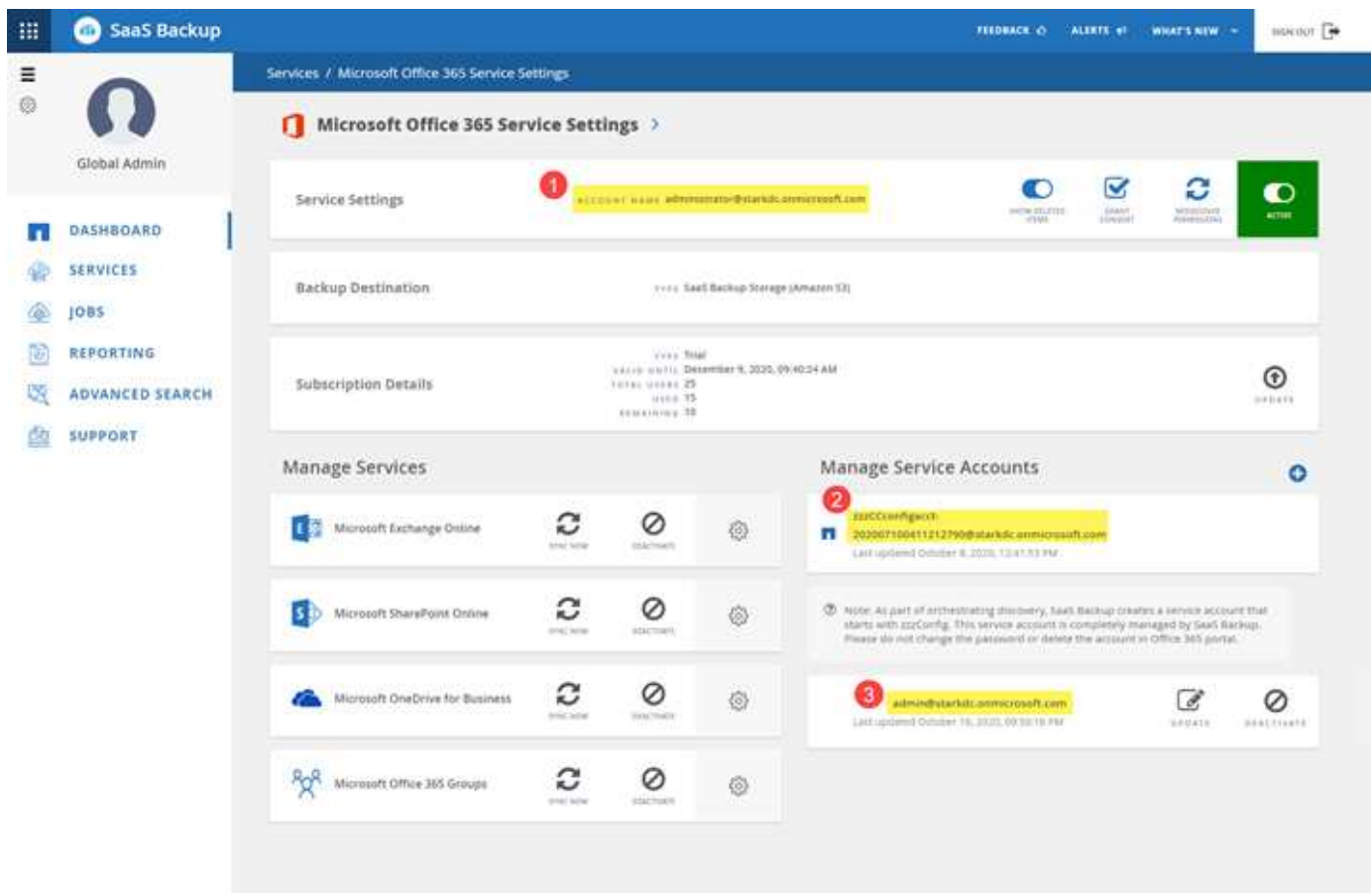


# Erstellen Sie ein neues Microsoft 365-Servicekonto

Wenn Sie Ihr neues Microsoft 365-Konto erstellen, muss dieses Konto über globale Administrationsberechtigungen mit einer gültigen und zugewiesenen Microsoft Office 365-Lizenz verfügen.

Dies ist nicht das einzige Servicekonto, mit dem SaaS Backup für Microsoft 365 verwaltet wird. Die folgende Abbildung zeigt die verschiedenen Service-Account-Typen mit den unten aufgeführten Beschreibungen.

## Service-Konto Beschreibung



1 Das Konto zur Anmeldung bei SaaS Backup; es erfordert globale Administrationsberechtigungen mit einer gültigen Microsoft 365-Lizenz während der Anmeldung. Sie kann für Backup- und Restore-Vorgänge

genutzt werden. 2 Ein **zzzCCconfigact** wird automatisch als Servicekonto erstellt, um Microsoft 365-Gruppen zu entdecken. Wenn die moderne Authentifizierung aktiviert ist, haben Sie kein ZZZ Config-

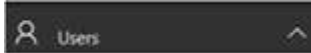
Dienstkonto. 3 Ein zusätzliches Servicekonto kann hinzugefügt werden, um die Performance von Backup- und Restore-Vorgängen zu verbessern.

# Erstellen Sie ein neues MS 365-Servicekonto mit globalen Administratorberechtigungen

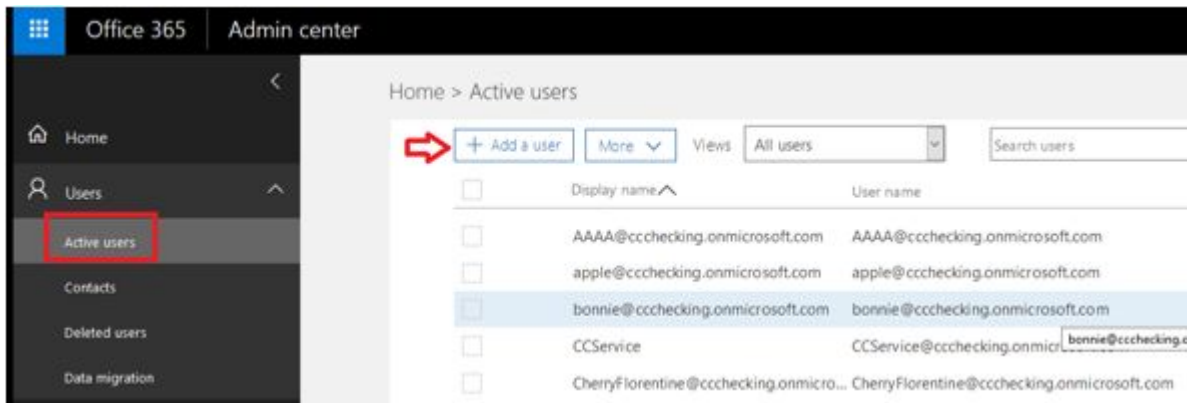
Erstellen Sie während der Anmeldung ein Konto mit globalen Berechtigungen und einer gültigen Microsoft 365-Lizenz. Sie können die globalen Administrationsberechtigungen und die Lizenz aus diesem Konto entfernen, nachdem Sie die Anmeldung abgeschlossen haben.

## Schritte

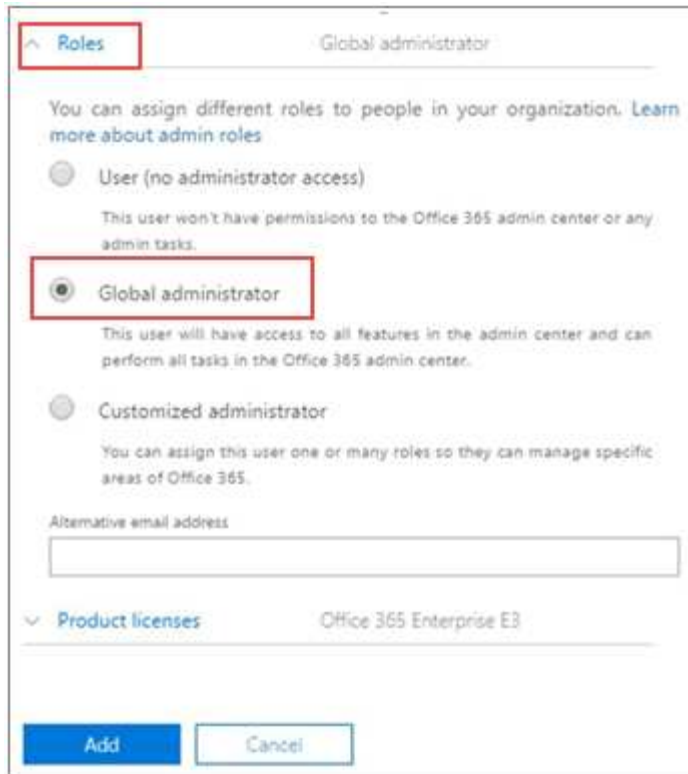
1. Melden Sie sich bei Ihrem Microsoft 365-Managementportal unter Verwendung eines Kontos mit Administratorrechten an.
2. Klicken Sie Auf **Benutzer**.



3. Wählen Sie **Aktive Benutzer** und klicken Sie dann auf **Benutzer hinzufügen**.



4. Geben Sie die Details für das neue Servicekonto ein.
  - Vorname
  - Nachname
  - Anzeigename
  - Benutzername der Benutzername ist der Name des Servicekontos.
5. Erweitern Sie **Rollen**, wählen Sie als Rolle **Global Administrator** aus und klicken Sie dann auf **Add**.



Die Details des Servicekontos werden an den Administrator gesendet.

6. Melden Sie sich mit dem neuen Konto bei Ihrem Microsoft 365 Management Portal an, um es zu aktivieren.
7. Stellen Sie nach der Anmeldung sicher, dass dieses Servicekonto drei Berechtigungen erhält:
  - Exchange Administrator
  - SharePoint Administrator
  - Rolle „Anwendungs-Impersonation“

Dies ist besonders wichtig, wenn Sie die einzelnen Lizenzen für die globale Administratorrolle einschränken.

## ZZZ Config Service-Konto

Das ZZZ Config-Dienstkonto ist ein automatisch erstelltes Konto, das zur Ermittlung von freigegebenen/Archiv-Mailboxen und privaten Gruppen verwendet wird, wenn Sie die Basisauthentifizierung verwenden. Es sollten Exchange- und SharePoint-Berechtigungen besitzen (benutzerdefinierter Administrator in M365). Es wird empfohlen, dieses Konto von den MFA-Richtlinien auszuschließen. Um Erkennungs- oder Backup-Fehler zu vermeiden, lassen Sie das Konto unverändert.

Wenn Sie die moderne Authentifizierung aktivieren, wird das ZZZ Config-Dienstkonto entfernt.

Neukunden haben kein ZZZ Config-Servicekonto.

## Erstellen Sie zusätzliche Servicekonten

In SaaS Backup für Microsoft 365 können Servicekonten hinzugefügt werden, um die Backup Performance für einen Kunden zu verbessern. Ein Servicekonto ist ein Microsoft 365-Benutzerkonto ohne Lizenz und wird für Backup- und Wiederherstellungsvorgänge verwendet.

Für diese Art von Konto sind 3 Berechtigungen erforderlich:

- Exchange-Administrator
- SharePoint-Administrator
- Rolle zur Imitation von Anwendungen

Um ein zusätzliches Servicekonto hinzuzufügen, muss das Servicekonto bereits in Ihrer Microsoft 365 Umgebung vorhanden sein. Wenn Sie kein Konto besitzen, erstellen Sie ein Konto.





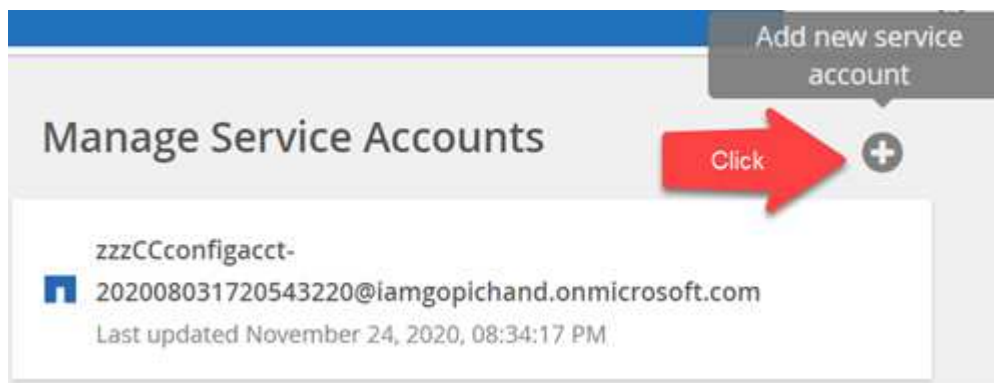
Um die Leistung zu optimieren, wird empfohlen, in Office 365 ein Servicekonto für 1000 Benutzer hinzuzufügen.

### Schritte

1. Melden Sie sich bei SaaS Backup für Microsoft 365 an.
2.  .  
Klicken Sie Auf  .
3. Klicken Sie Auf **Diensteinstellungen**.

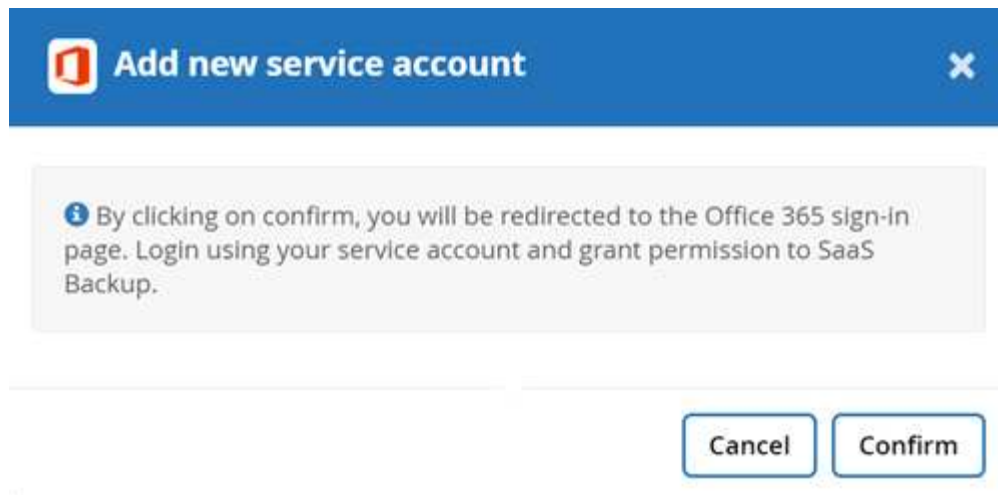


4.  .  
Klicken Sie auf, um ein Servicekonto hinzuzufügen  Unter \* Servicekonten verwalten\*.



Es wird eine Bestätigungsmeldung angezeigt.





5. Klicken Sie Auf **Bestätigen**.
6. Geben Sie auf der Anmeldeseite von Microsoft 365 die Anmeldeinformationen des oben genannten Servicekontos ein, um es zu SaaS Backup hinzuzufügen.

## Impersonation für Microsoft Exchange Online konfigurieren

Wenn Sie SaaS Backup mit Microsoft Exchange Online verwenden möchten, müssen Sie Impersonation konfigurieren. Mit der Impersonation kann Ihr Microsoft 365-Servicekonto Benutzerkonten imitieren und auf die zugehörigen Berechtigungen zugreifen.

### Impersonation automatisch konfigurieren

Um die Impersonation automatisch zu konfigurieren, führen Sie aus "[MSDN PowerShell-Befehle](#)".

### Impersonation manuell konfigurieren

Sie können Impersonation manuell mit Ihrem Microsoft 365-Administratorkonto konfigurieren sowie mit zusätzlichen Microsoft 365-Servicekonten in SaaS Backup. Weitere Informationen zu Servicekonten für Microsoft 365 finden Sie unter "[Erstellen eines Microsoft 365-Servicekontos mit globalen Berechtigungen](#)."

Um die Impersonation manuell zu konfigurieren, gehen Sie wie folgt vor:

#### Schritte

1. Melden Sie sich bei Ihrem Microsoft 365-Servicekonto an.
2. Wählen Sie die Registerkarte **Exchange** aus.
3. Wählen Sie links unter Dashboard die Option **Berechtigungen** aus.
4. Klicken Sie auf **Administratorrollen**.
5. Doppelklicken Sie im rechten Fensterbereich, um **Discovery Management** auszuwählen.
6. Klicken Sie unter **Rollen** auf das **+**-Symbol.

Write scope:

Default

Roles:



NAME
<b>ApplicationImpersonation</b>
Legal Hold
Mailbox Search

7. Wählen Sie im Dropdown-Menü die Option **ApplicationImpersonation** aus.
8. Klicken Sie Auf **Hinzufügen**.
9. Klicken Sie auf **OK**.
10. Überprüfen Sie, ob **ApplicationImpersonation** unter **Rollen** hinzugefügt wurde.
11. Klicken Sie unter Mitglieder auf das Symbol **+**.

Members:



NAME	DISPLAY NAME
<b>AirBender</b>	<b>Air Bender</b>

angezeigt

Ein neues Fenster wird

12. Wählen Sie den Benutzernamen aus.


13. Klicken Sie Auf **Hinzufügen**.
14. Klicken Sie auf **OK**.
15. Stellen Sie sicher, dass der Benutzername im Abschnitt **Mitglieder** angezeigt wird.
16. Klicken Sie Auf **Speichern**.

## Melden Sie sich für SaaS Backup für Microsoft 365 an

Sie können sich bei SaaS Backup für Microsoft 365 mit Ihrem Microsoft 365-Servicekonto oder mit Ihrem NetApp SSO-Konto anmelden.

### Melden Sie sich mit einem Microsoft 365-Servicekonto an

#### Schritte




1. Geben Sie die URL SaaS Backup für Microsoft 365 in Ihrem Webbrowser ein: <https://saasbackup.netapp.com>
2. Wählen Sie Ihre Region aus. Ihre Mandanten werden in der ausgewählten Region erstellt. Die Daten werden am Datacenter-Standort gespeichert und können später nicht mehr geändert werden.
3. Klicken Sie am Ende der Landing Page auf **Registrieren**.
4. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung.
5. Klicken Sie auf **Registrieren Sie sich mit Office 365**. 
6. Geben Sie die E-Mail-Adresse und das Kennwort für Ihr globales Administratorkonto von Microsoft 365 ein, und klicken Sie dann auf **Anmelden**. Eine Liste der von SaaS Backup für Microsoft 365 angeforderten Berechtigungen wird angezeigt.
7. Klicken Sie Auf **Akzeptieren**.
8. Geben Sie die angeforderten Benutzerinformationen ein.
9. Klicken Sie auf **Registrieren**. Ihr Benutzername und eine Liste der Berechtigungen für SaaS Backup für Microsoft 365 werden angezeigt.
10. Klicken Sie Auf **Weiter**. Eine Liste der verfügbaren Microsoft 365-Dienste wird angezeigt.
11. Wählen Sie die Microsoft 365-Dienste aus, die Sie aktivieren möchten.
12. Klicken Sie Auf **Weiter**.
13. Wenn Sie Ihre Lizenz über NetApp erworben haben, werden Ihre Abonnementtypen angezeigt. Klicken Sie auf "**Hier**" Für weitere Schritte.
14. Wenn Sie Ihre Lizenz über einen Cloud Marketplace, z. B. AWS, erworben haben, werden Ihre Lizenzinformationen angezeigt. Klicken Sie Auf "**Hier**" Für weitere Schritte.

### Melden Sie sich mit einem NetApp SSO Konto an

#### Bevor Sie beginnen

Zur Validierung Ihres Abonnements müssen Sie über eine NetApp SSO-Benutzer-ID und ein Passwort verfügen. Wenn Sie kein NetApp SSO-Konto besitzen, besuchen Sie <https://mysupport.netapp.com/eservice/public/now.do> Um sich für eine zu registrieren. Nach Bearbeitung Ihrer Anfrage erhalten Sie eine E-Mail-Benachrichtigung mit Ihren NetApp SSO-Anmeldedaten. Es dauert etwa 24 Stunden, die Anfrage zu bearbeiten und die E-Mail-Benachrichtigung zu senden.

#### Schritte

1. Geben Sie die URL SaaS Backup für Microsoft 365 in Ihrem Webbrowser ein: <https://saasbackup.netapp.com>
2. Klicken Sie unten auf der Landing Page auf „Sign Up“.
3. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung.
4. Klicken Sie auf **Registrieren Sie sich mit NetApp SSO**. 
5. Geben Sie Ihr NetApp SSO und Passwort ein und klicken Sie dann auf **LOGIN**.
6. Geben Sie die gewünschten Benutzerinformationen ein, und klicken Sie anschließend auf **Registrieren**.
7. Klicken Sie auf die Option **Services**  Symbol.
8. Klicken Sie auf Microsoft 365  Symbol, um den SaaS-Service auszuwählen.
9. Klicken Sie Auf **Microsoft Office 365 Konto Hinzufügen**.
10. Geben Sie die E-Mail-Adresse und das Kennwort für Ihr globales Administratorkonto von Microsoft 365 ein, und klicken Sie dann auf **Anmelden**. Eine Liste der von SaaS Backup für Microsoft 365 angeforderten Berechtigungen wird angezeigt.
11. Klicken Sie Auf **Akzeptieren**.
12. Klicken Sie Auf **Weiter**. Eine Liste der verfügbaren Microsoft 365-Dienste wird angezeigt.
13. Wählen Sie die Microsoft 365-Dienste aus, die Sie aktivieren möchten.
14. Klicken Sie Auf **Weiter**.
15. Wählen Sie für den Abonnementtyp \* licensed\* aus.
16. Geben Sie die angeforderten Informationen ein, und bestätigen Sie das Abonnement.
17. Klicken Sie Auf **Weiter**.
18. Wählen Sie Ihre Backup-Storage-Option aus.
  - a. Klicken Sie auf **SaaS Backup bereitgestellter Storage**.
  - b. Wählen Sie die Storage-Option **Amazon S3** oder **Azure Blob** aus.
  - c. Wählen Sie für Ihr Backup die Region **AWS S3** oder **Azure Blob** aus. Wählen Sie die Region aus, die dem physischen Standort der zu sichern Daten am nächsten ist.
  - d. Klicken Sie Auf **Weiter**.
  - e. Überprüfen Sie Ihre Konfiguration, und klicken Sie dann auf **Speichern**.

## Planen Sie Ihr erstes Backup

Wenn Sie SaaS Backup für Microsoft 365 einrichten, sind die Daten standardmäßig nicht geschützt. Sie müssen Ihre Daten von der ungeschützten Tier in eine der geschützten Tiers verschieben, sodass Ihre Daten während des nächsten geplanten Backups der ausgewählten Tier gesichert werden.

### Schritte

1. Wählen Sie im Dashboard den Service aus, der die nicht geschützten Daten enthält.
2. Klicken Sie auf **Ansicht** neben der Anzahl ungeschützter Mailboxen, MySites oder Gruppen.

3. Wählen Sie die Elemente aus, die Sie schützen möchten.

4.

Klicken Sie auf das Menü **Gruppen**.



5. Wählen Sie die **Tier** für die Sicherungsrichtlinie aus, die Sie zuweisen möchten. Siehe "[Backup-Richtlinien](#)"  
Eine Beschreibung der Backup Policy Tiers erhalten Sie hier.

6. Klicken Sie Auf **Anwenden**.

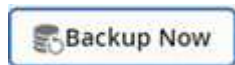
## Sofortiges Backup einer spezifischen Backup-Richtlinie durchführen

Wenn Sie SaaS Backup für Microsoft 365 einrichten, sind standardmäßig alle Daten nicht geschützt. Nachdem Sie Ihre Daten in eine geschützte Ebene verschoben haben, können Sie umgehend ein Backup der Ebene durchführen, auf die Sie Ihre Daten verschoben haben. Dadurch wird verhindert, dass Ihre Daten erst dann gefährdet werden, wenn das erste geplante Backup durchgeführt wird. Wenn Sie auf das erste geplante Backup warten können, ist es nicht erforderlich, ein sofortiges Backup durchzuführen.

Sie können jederzeit eine sofortige Sicherung durchführen, wenn Sie für die Datensicherheit erforderlich erachten. Wenn Sie eine Testversion von SaaS Backup für Microsoft 365 ausführen, können Sie nur drei sofortige Backups pro Tag und Service durchführen.

### Schritte

1. Wählen Sie im Dashboard den Dienst aus, für den Sie ein sofortiges Backup durchführen möchten.
2. Klicken Sie unter **Backup Policies** auf die Ebene, die Sie sichern möchten.
3. Klicken Sie Auf Jetzt Sichern.



Es wird eine Meldung angezeigt, die angibt, dass die Services unter der ausgewählten Ebene zur sofortigen Sicherung in die Jobwarteschlange verschoben werden.

4. Klicken Sie Auf **Bestätigen**. Es wird eine Meldung angezeigt, die angibt, dass der Backupjob erstellt wurde.
5. Klicken Sie auf **Auftragsfortschritt anzeigen**, um den Fortschritt des Backups zu überwachen.

## Datenlöschung

Wenn Sie Ihre lizenzierte Version von SaaS Backup für Microsoft 365 nicht erneuern, werden die während Ihres Abonnements verwendeten Daten wie folgt gelöscht:

<b>Wäre Ihr SaaS Backup-Abonnement kostenpflichtig?</b>	<b>Anzahl der Tage nach Ende des bezahlten Abonnements</b>	<b>Ihre Daten sind...</b>
Abgelaufen	1-30 Tage	Verfügbar: Der Administrator verfügt über normalen Zugriff und kann manuelle Backups und Restores durchführen. SaaS Backup zeigt weiterhin Warnungen an und sendet Benachrichtigungen.
Deaktiviert	31-60 Tage	Deaktiviert: Der Administrator hat keinen Zugriff auf das SaaS Backup Portal. Wenn das Abonnement während dieses Zeitraums verlängert wird, können Daten reaktiviert werden.
Deprovisioniert	61 oder mehr Tage	Gelöscht: Alle Daten werden gelöscht und Ihr Mandantenkonto wird entfernt.

## Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

## Markeninformationen

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