



Manage services

SaaS Backup for Microsoft 365

NetApp

February 12, 2024

This PDF was generated from https://docs.netapp.com/us-en/saasbackupO365/task_activating_a_service.html on February 12, 2024. Always check docs.netapp.com for the latest.

Table of Contents


- Manage services 1
 - Activate a service 1
 - Deactivate a service 1
 - Activate support 1
 - Discover new mailboxes, sites, and groups 2
 - Purge a user, site collection, or Microsoft 365 group 3
 - Enable Modern Authentication 3

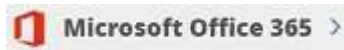
Manage services

Activate a service

If needed, you can activate one or more SaaS Backup for Microsoft 365 services. Microsoft Exchange Online or Microsoft SharePoint Online must be activated before you can activate Microsoft 365 Groups.

Steps

1. Click  from the left navigation pane.
2. Click the Microsoft 365 link.




3. Click **Activate** next to the service that you want to activate.
4. Click **Confirm**.


Deactivate a service

If needed, you can deactivate one or more of your SaaS Backup for Microsoft 365 services. If you deactivate a service, all of the schedules associated with that service are removed and no further backup is performed. You can still view the last backup that occurred before deactivation and you can still perform restores.

Steps

1. Click  from the left navigation pane.
2. Click the Microsoft 365 link.



3. Click  next to the service that you want to deactivate.
4. Click **Confirm**.

Activate support



If you purchased SaaS Backup through NetApp, support is activated by default. If you purchased SaaS Backup through a Cloud Marketplace such as AWS, you must activate support. Activating support enables you to access technical support over the phone, online chat, or web ticketing system.

If you are upgrading from a trial version of SaaS Backup, you can activate support either before or after you complete the upgrade process.

Before you begin

In order to activate support, you must have a NetApp SSO user ID and password. If you do not have a NetApp SSO account, go to <http://register.netapp.com> 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


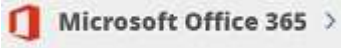
1. Click  **SERVICES** from the left navigation pane.
2. Click the settings icon .
3. In the **Activate Support** box, click **Activate**.
4. Enter your NetApp SSO username and password.
5. Click **Activate**.

The support status is now **Active**.

Discover new mailboxes, sites, and groups

A synchronization must occur between SaaS Backup and your Microsoft 365 account for new mailboxes (including shared and archive mailboxes), sites, groups, and teams to be discovered by SaaS Backup. By default, synchronization automatically occurs once every 24 hours. However, if you make changes and you want discovery to occur before the next scheduled **Auto Sync**, you can initiate an immediate synchronization.

Steps

1. Click  **SERVICES** from the left navigation pane.
2. Click the Microsoft 365 settings icon.

3. Click **Sync Now** next to the service that you want to synchronize.




New users, shared mailboxes, and archive mailboxes are discovered and added in an unprotected state. If you want newly discovered users, shared mailboxes, or archive mailboxes to be backed up, you must change the backup policy of the users from unprotected to one of the predefined tier groups.

4. Click **Confirm**.
5. Click **View the job progress** to monitor the progress.
When the job is complete, you can click the job under **Recent Completed Jobs** to view the number of users that were added or removed during the synchronization. Changes to user accounts are indicated as follows:
 - **Rediscovered** users indicates the number of unchanged user accounts.
 - **Deactivated** users indicates the number of deleted user accounts.
 - **Newly added** users indicates the number of new user accounts.


Purge a user, site collection, or Microsoft 365 group

You can completely remove all the data associated with a user, site collection, or Microsoft 365 group. Purged data is recoverable for seven days. After seven days, the data is permanently deleted and the user license is automatically released.

Steps

1. Click the configuration icon  next to your SaaS Backup user id in the top left corner.
2. Select **ACCOUNT SETTINGS**.
3. Click **RETAIN AND PURGE**.
4. Under **Purge Data**, select the **Type of Service** (Exchange, OneDrive, or SharePoint) from the dropdown menu.
5. Search for the user, site collection, or Microsoft 365 group that you want to purge.
For Microsoft Exchange Online or OneDrive for Business, enter the user or Microsoft 365 group name. For SharePoint Online, enter the site collection name.

NOTE: If the user has an archive mailbox, the username of the archive mailbox is prefixed by "In-Place Archive".

6. When the search result returns, click the  to select the user, site collection, or Microsoft 365 group.
7. Click **Save**.
8. Click **Yes** to confirm that you want purge the data.

Enable Modern Authentication

Microsoft 365 targets October 2021 to deprecate Basic Authentication in Exchange Online. After deprecation, discovery failures can occur for Microsoft 365 groups, and Shared and Archive mailboxes.

You can enable Modern Authentication at any time.

New customers don't need to take any action. Modern Authentication is enabled when you sign up.

Existing customers need to take action. Follow the instructions below to enable Modern Authentication.



To enable Modern Authentication, log in with your tenant account credentials; the account name can be found in Microsoft 365 Service Settings (see **Option 2 steps** below). Make sure the Global Administrator role is assigned to this account. After Modern Authentication is successfully enabled, you can remove the Global Administrator role from the admin user.

Option 1 steps

1. Sign in to SaaS Backup for Microsoft 365.
The following message pops up.
2. Select **Confirm** to enable Modern Authentication.
3. Accept all permissions.

Modern Authentication is now enabled.
The ZZZ config service account has been removed.

Option 2 steps

1. In SaaS Backup for Microsoft 365, go to Settings  > Service settings > Microsoft 365 service settings.



2. Select **Enable Modern Authentication**.



3. Accept all permissions.
Modern Authentication is now enabled.
The ZZZ config service account has been removed.

If you receive a failure notification, you can retry to enable Modern Authentication.

For support, email saasbackupsupport@netapp.com.

For more information, see [Basic Authentication and Exchange Online - September 2021 Update](#).

Copyright information

Copyright © 2024 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.