Scanning OneDrive accounts

Cloud Manager

Tom Onacki
February 05, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/task_scanning_onedrive.html on February 28, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Scanning OneDrive accounts . . . 1
- Quick start . . . 1
- Reviewing prerequisites . . . 1
- Adding the OneDrive account . . . 1
- Adding OneDrive users to compliance scans . . . 2
- Removing OneDrive users from compliance scans . . . 3

Scanning OneDrive accounts

Complete a few steps to start scanning files in your user's OneDrive folders with Cloud Compliance.

Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

Review OneDrive prerequisites

Ensure that you have the Admin credentials to log into the OneDrive account.

Deploy the Cloud Compliance instance

Deploy Cloud Compliance if there isn't already an instance deployed.

Add the OneDrive account

Using Admin user credentials, log into the OneDrive account that you want to access so that it is added as a new working environment.

Add the users

Add the list of users from the OneDrive account that you want to scan. You can add up to 100 users at time.

Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you enable Cloud Compliance.

OneDrive requirements

You must have the Admin login credentials for the OneDrive for Business account that provides read access to all user files.

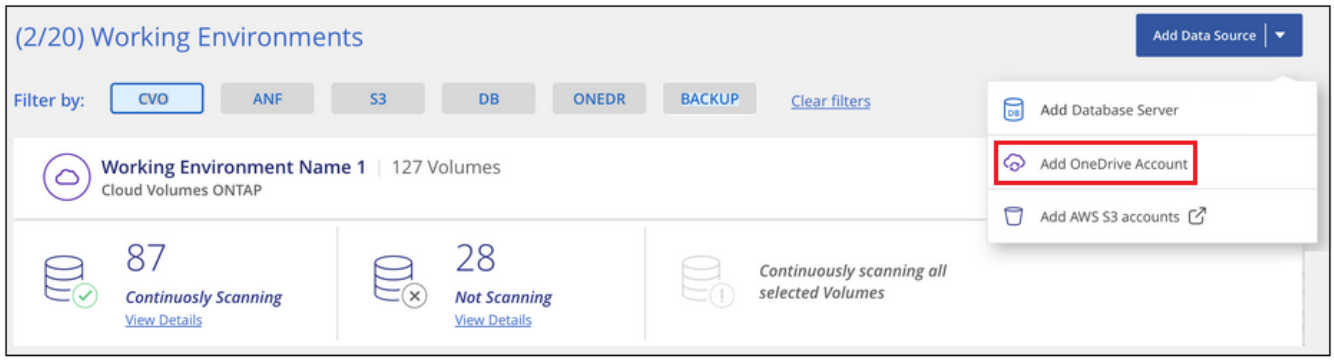
You will need a line-separated list of the email addresses for all the users whose OneDrive folders you want to scan.

Adding the OneDrive account

You must have deployed an instance of Cloud Compliance in Cloud Manager already.

Add the OneDrive account where the user files reside.

1. From the Working Environments Configuration page, click **Add Data Source** > **Add OneDrive Account**.



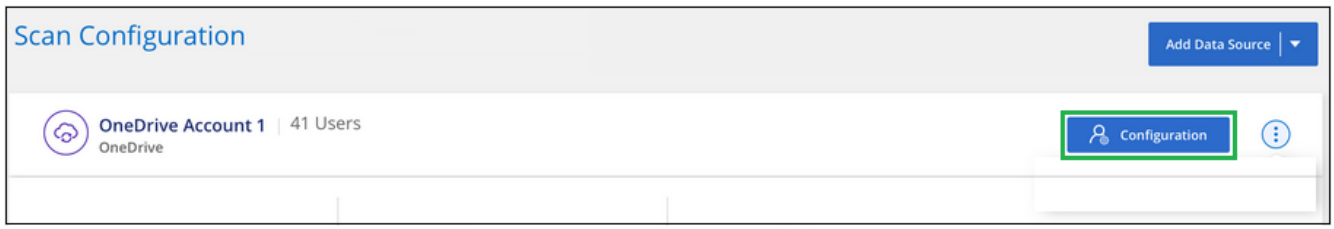
2. In the Add a OneDrive account dialog, click **Sign in to OneDrive**.
3. In the Microsoft page that appears, select the OneDrive account and enter the required Admin user and password, then click **Accept** to allow Cloud Compliance to read data from this account.

The OneDrive account is added to the list of working environments.

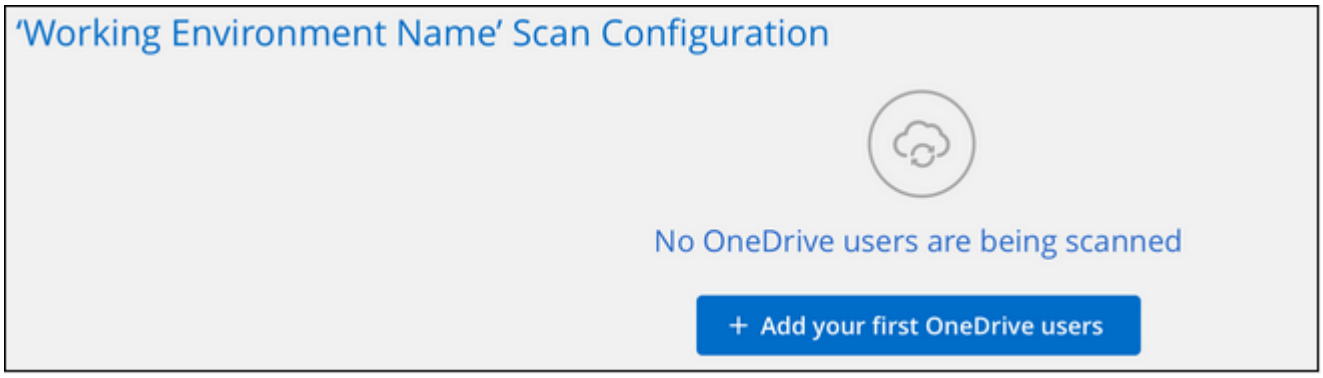
Adding OneDrive users to compliance scans

You can add individual OneDrive users, or all of your OneDrive users, so that their files will be scanned by Cloud Compliance.

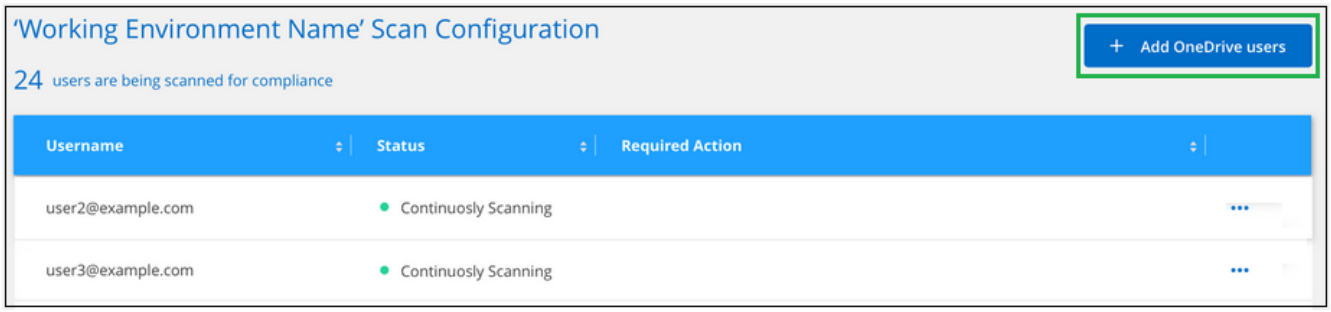
1. From the *Scan Configuration* page, click the **Configuration** button for the OneDrive account.



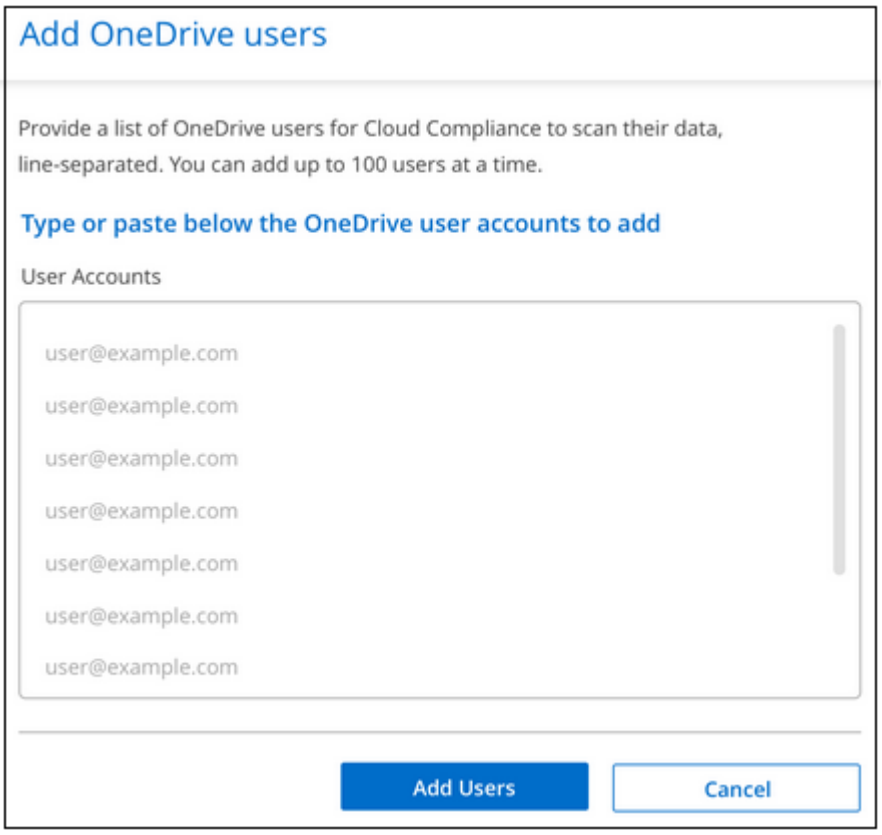
2. If this is the first time adding users for this OneDrive account, click **Add your first OneDrive users**.



If you are adding additional users, click **Add OneDrive users**.



3. Add the email addresses for the users whose files you want to scan - one email address per line (up to 100 maximum per session) - and click **Add Users**.



A confirmation dialog displays the number of users who were added.

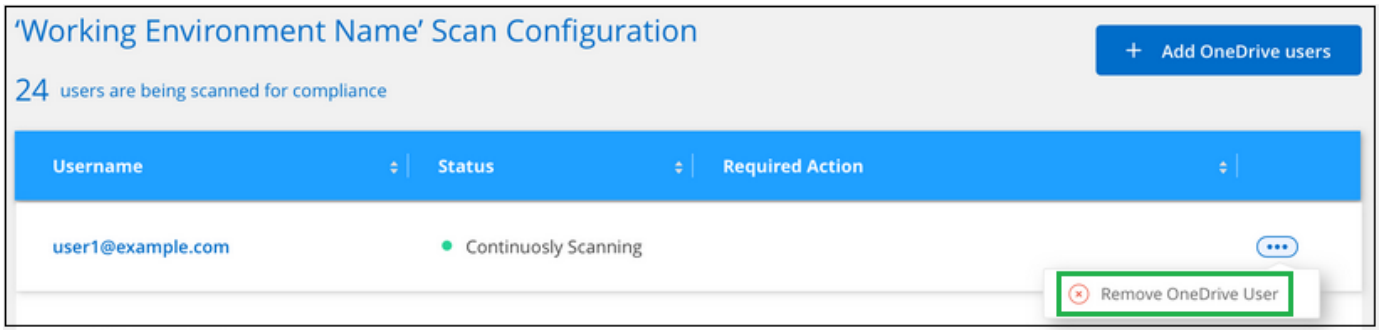
If the dialog lists any users who could not be added, capture this information so that you can resolve the issue. In some cases you can re-add the user with a corrected email address.

Result

Cloud Compliance starts scanning the files for the users you added, and the results are displayed in the Dashboard and in other locations.

Removing OneDrive users from compliance scans

If users leave the company or if their email address changes, you can remove individual OneDrive users from having their files scanned at any time. Just click **Remove OneDrive User** from the Configuration page.


'Working Environment Name' Scan Configuration
24 users are being scanned for compliance
+ Add OneDrive users
Username
Status
Required Action
user1@example.com
Continuosly Scanning
Remove OneDrive User

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.