Discover arrays

SANtricity software

NetApp
November 03, 2025

This PDF was generated from https://docs.netapp.com/us-en/e-series-santricity/um-manage/discover-multiple-arrays.html on November 03, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Discover arrays . . . 1
- Discover multiple storage arrays in SANtricity Unified Manager . . . 1
  - Step 1: Enter network address . . . 1
  - Step 2: Resolve self-signed certificates during discovery . . . 2
  - Step 3: Resolve untrusted certificates during discovery . . . 2
  - Step 4: Provide passwords . . . 2
- Discover a single array in SANtricity Unified Manager . . . 3

Discover arrays

Discover multiple storage arrays in SANtricity Unified Manager

You discover multiple arrays to detect all storage arrays across the subnet where the management server resides and to automatically add the discovered arrays to your management domain.

Before you begin

- You must be logged in with a user profile that includes Security Admin permissions.
- The storage array must be correctly set up and configured.
- Storage array passwords must be set up using System Manager's Access Management tile.
- To resolve untrusted certificates, you must have trusted certificate files from a Certificate Authority (CA), and the certificate files are available on your local system.

Discovering arrays is a multi-step procedure.

Step 1: Enter network address

You enter a network address range to search across the local sub-network. Any storage array successfully reached appears on the Discover page and might be added to your management domain.

If you need to stop the discovery operation for any reason, click **Stop Discovery**.

Steps

1. From the Manage page, select **Add/Discover**.

   The Add/Discover dialog box appears.

2. Select the **Discover all storage arrays within a network range** radio button.
3. Enter the starting network address and ending network address to search across your local sub-network, and then click **Start Discovery**.

   The discovery process starts. This discovery process can take several minutes to complete. The table on the Discover page is populated as the storage arrays are discovered.

   If no manageable arrays are discovered, verify that the storage arrays are properly connected to your network and their assigned addresses are within range. Click **New Discovery Parameters** to return to the Add/Discover page.

4. Review the list of discovered storage arrays.
5. Select the checkbox next to any storage array that you want to add to your management domain, and then click **Next**.

   Unified Manager performs a credential check on each array you are adding to the management domain. You might need to resolve any self-signed certificates and untrusted certificates associated with that array.

6. Click **Next** to proceed to the next step in the wizard.

Step 2: Resolve self-signed certificates during discovery

As part of the discovery process, the system verifies that the storage arrays are using certificates by a trusted source.

Steps

1. Do one of the following:
   - If you trust the connections to the discovered storage arrays, continue to the next card in the wizard. The self-signed certificates will be marked as trusted and the storage arrays will be added to Unified Manager.
   - If you do not trust the connections to the storage arrays, select **Cancel** and validate each storage array's security certificate strategy before adding any of them to Unified Manager.
2. Click **Next** to proceed to the next step in the wizard.

Step 3: Resolve untrusted certificates during discovery

Untrusted certificates occur when a storage array attempts to establish a secure connection to Unified Manager, but the connection fails to confirm as secure. During the array discovery process, you can resolve untrusted certificates by importing a certificate authority (CA) certificate (or CA-signed certificate) that has been issued by a trusted third party.

You may need to install additional trusted CA certificates if any of the following are true:

- You recently added a storage array.
- One or both certificates are expired.
- One or both certificates are revoked.
- One or both certificates are missing a root or intermediate certificate.

Steps

1. Select the check box next to any storage array that you want to resolve untrusted certificates for, and then select the **Import** button.

   A dialog box opens for importing the trusted certificate files.

2. Click **Browse** to select the certificate files for the storage arrays.

   The file names display in the dialog box.

3. Click **Import**.

   The files are uploaded and validated.

   Any storage array with untrusted certificate issues that are unresolved will not be added to Unified Manager.

4. Click **Next** to proceed to the next step in the wizard.

Step 4: Provide passwords

You must enter the passwords for the storage arrays that you want to add to your management domain.

Steps

1. Enter the password for each storage array you want to add to Unified Manager.
2. **Optional:** Associate storage arrays to a group: From the drop-down list, select the desired group to associate with the selected storage arrays.
3. Click **Finish**.

After you finish

The storage arrays are added to your management domain and associated with the selected group (if specified).

It can take several minutes for Unified Manager to connect to the specified storage arrays.

Discover a single array in SANtricity Unified Manager

Use the Add/Discover Single Storage Array option to manually discover and add a single storage array to your organization's network.

Before you begin

- The storage array must be correctly set up and configured.
- Storage array passwords must be set up using System Manager's Access Management tile.

Steps

1. From the Manage page, select **Add/Discover**.

   The Add/Discover dialog box appears.

2. Select the **Discover a single storage array** radio button.
3. Enter the IP address for one of the controllers in the storage array, and then click **Start Discovery**.

   It can take several minutes for Unified Manager to connect to the specified storage array.

   The Storage Array Not Accessible message appears when the connection to the IP address of the specified controller is unsuccessful.

4. If prompted, resolve any self-signed certificates.

   As part of the discovery process, the system verifies that the discovered storage arrays are using certificates by a trusted source. If it cannot locate a digital certificate for a storage array, it prompts you to resolve the certificate that is not signed by a recognized certificate authority (CA) by adding a security exception.

5. If prompted, resolve any untrusted certificates.

   Untrusted certificates occur when a storage array attempts to establish a secure connection to Unified Manager, but the connection fails to confirm as secure. Resolve untrusted certificates by importing a certificate authority (CA) certificate that has been issued by a trusted third party.

6. Click **Next**.
7. **Optional:** Associate the discovered storage array to a group: From the drop-down list, select the desired group to associate with the storage array.

The "All" group is selected by default.

8. Enter the administrator password for the storage array that you want to add to your management domain, and then click **OK**.

After you finish

The storage array is added to Unified Manager and, if specified, it is also added to the group you selected.

If automatic support data collection is enabled, support data is automatically collected for a storage array that you add.

Copyright information

Copyright © 2025 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.