



# **Generating an HTTPS security certificate**

Active IQ Unified Manager 9.9

NetApp  
February 20, 2023

# Table of Contents

- Generating an HTTPS security certificate ..... 1
  - Before you begin ..... 1
  - About this task ..... 1
  - Steps ..... 1
  - After you finish ..... 2
- Restarting the Unified Manager virtual machine ..... 2

# Generating an HTTPS security certificate

When Active IQ Unified Manager is installed for the first time, a default HTTPS certificate is installed. You might generate a new HTTPS security certificate that replaces the existing certificate.

## Before you begin

You must have the Application Administrator role.

## About this task

There can be multiple reasons to regenerate the certificate such as if you want to have better values for Distinguished Name (DN) or if you want a higher key size, or longer expiry period or if the current certificate has expired.

If you do not have access to the Unified Manager web UI, you can regenerate the HTTPS certificate with the same values using the maintenance console. While regenerating certificates, you can define the key size and the validity duration of the key. If you use the `Reset Server Certificate` option from the maintenance console, then a new HTTPS certificate is created which is valid for 397 days. This certificate will have an RSA key of size 2048 bits.


## Steps

1. In the left navigation pane, click **General > HTTPS Certificate**.
2. Click **Regenerate HTTPS Certificate**.

The Regenerate HTTPS Certificate dialog box is displayed.

3. Select one of the following options depending on how you want to generate the certificate:

If you want to...	Do this...
Regenerate the certificate with the current values	Click the <b>Regenerate Using Current Certificate Attributes</b> option.

If you want to...	Do this...
Generate the certificate using different values	<p>Click the <b>Update the Current Certificate Attributes</b> option.</p> <p>The Common Name and Alternative Names fields will use the values from the existing certificate if you do not enter new values. The “Common Name” should be set to the FQDN of the host. The other fields do not require values, but you can enter values, for example, for the EMAIL, COMPANY, DEPARTMENT, City, State, and Country if you want those values to be populated in the certificate. You can also select from the available KEY SIZE (The key algorithm is “RSA”.) and VALIDITY PERIOD.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <ul style="list-style-type: none"> <li>The permitted values for key size are 2048, 3072 and 4096.</li> <li>The validity periods are minimum 1 day to maximum 36500 days.</li> </ul> <p>Even though a validity period of 36500 days is permitted, it is recommended you use a validity period of not more than 397 days or 13 months. Because if you select a validity period of more than 397 days and plan to export a CSR for this certificate and get it signed by a well known CA, the validity of the signed certificate returned to you by the CA will be reduced to 397 days.</p> <ul style="list-style-type: none"> <li>You can select the “Exclude local identifying information \\\(e.g. localhost\\)” checkbox if you want to remove the local identifying information from the Alternative Names field in the certificate. When this checkbox is selected, only what you enter in the field is used in the Alternative Names field. When left blank the resulting certificate will not have an Alternative Names field at all.</li> </ul> </div>

1. Click **Yes** to regenerate the certificate.
2. Restart the Unified Manager server so that the new certificate takes effect.

## After you finish

Verify the new certificate information by viewing the HTTPS certificate.

## Restarting the Unified Manager virtual machine

You can restart the virtual machine from the maintenance console of Unified Manager. You must restart after generating a new security certificate or if there is a problem with the virtual machine.

### Before you begin

The virtual appliance is powered on.

You are logged in to the maintenance console as the maintenance user.

## About this task

You can also restart the virtual machine from vSphere by using the **Restart Guest** option. See the VMware documentation for more information.

## Steps

1. Access the maintenance console.
2. Select **System Configuration > Reboot Virtual Machine**.

## Copyright information

Copyright © 2023 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.