



Page descriptions for certificate management

Active IQ Unified Manager 9.13

NetApp
February 12, 2024

Table of Contents

- Page descriptions for certificate management 1
- HTTPS Certificate page 1
- Regenerate HTTPS Certificate dialog box 1

Page descriptions for certificate management

You can use the HTTPS Certificate page to view the current security certificates and to generate new HTTPS certificates.

HTTPS Certificate page

The HTTPS Certificate page enables you to view the current security certificate, download a certificate signing request, generate a new self-signed HTTPS certificate, or install a new HTTPS certificate.

If you have not generated a new self-signed HTTPS certificate, the certificate that appears on this page is the certificate that was generated during installation.

Command buttons

The command buttons enable you to perform the following operations:

- **Download HTTPS Certificate Signing Request**

Downloads a certification request for the currently installed HTTPS certificate. Your browser prompts you to save the <hostname>.csr file so that you can provide the file to a Certificate Authority to sign.

- **Install HTTPS Certificate**

Enables you to upload and install a security certificate after a Certificate Authority has signed and returned it. The new certificate is in effect after you restart the management server.

- **Regenerate HTTPS Certificate**

Enables you to generate a new self-signed HTTPS certificate, which replaces the current security certificate. The new certificate is in effect after you restart Unified Manager.

Regenerate HTTPS Certificate dialog box

The Regenerate HTTPS Certificate dialog box enables you to customize the security information and then generate a new HTTPS certificate with that information.

The current certificate information appears on this page.

The “Regenerate Using Current Certificate Attributes” and “Update the Current Certificate Attributes” selection enables you to regenerate the certificate with the current information or generate a certificate with new information.

- **Common Name**

Required. The fully qualified domain name (FQDN) that you wish to secure.

In Unified Manager high availability configurations, use the virtual IP address.

- **Email**

Optional. An email address to contact your organization; typically the email address of the certificate administrator or IT department.

- **Company**

Optional. Typically the incorporated name of your company.

- **Department**

Optional. The name of the department in your company.

- **City**

Optional. The city location of your company.

- **State**

Optional. The state or province location, not abbreviated, of your company.

- **Country**

Optional. The country location of your company. This is typically a two-letter ISO code of the country.

- **Alternative Names**

Required. Additional, non-primary domain names that can be used to access this server in addition to the existing localhost or other network addresses. Separate each alternate name with a comma.

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.

- **KEY SIZE (KEY ALGORITHM: RSA)**

The key algorithm is set to RSA. You can select from one of the key sizes: 2048, 3072 or 4096 bits. The default key size is set to 2048 bits.

- **VALIDITY PERIOD**

The default validity period is 397 days. If you have upgraded from a previous version, you might see the previous certificate validity unchanged.

For more information, see [Generating HTTPS certificates](#).

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.