Managing security certificates

Active IQ Unified Manager

NetApp
May 05, 2022

This PDF was generated from https://docs.netapp.com/us-en/active-iq-unified-manager/config/task_view_https_security_certificate_ocf.html on May 05, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Managing security certificates . . . 1
Viewing the HTTPS security certificate . . . 1
Downloading an HTTPS certificate signing request . . . 1
Installing a CA signed and returned HTTPS certificate . . . 1
Installing a HTTPS certificate generated using external tools . . . 2
Page descriptions for certificate management . . . 5

Managing security certificates

You can configure HTTPS in the Unified Manager server to monitor and manage your clusters over a secure connection.

Viewing the HTTPS security certificate

You can compare the HTTPS certificate details to the retrieved certificate in your browser to ensure that your browser's encrypted connection to Unified Manager is not being intercepted.

What you'll need

You must have the Operator, Application Administrator, or Storage Administrator role.

Viewing the certificate enables you to verify the content of a regenerated certificate, or to view Subject Alt Names (SAN) from which you can access Unified Manager.

Step

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

   The HTTPS certificate is displayed at the top of the page

If you need to view more detailed information about the security certificate than what is displayed on the HTTPS Certificate page, you can view the connection certificate in your browser.

Downloading an HTTPS certificate signing request

You can download a certification signing request for the current HTTPS security certificate so that you can provide the file to a Certificate Authority to sign. A CA-signed certificate helps prevent man-in-the-middle attacks and provides better security protection than a self-signed certificate.

What you'll need

You must have the Application Administrator role.

Steps

1. In the left navigation pane, click **General** > **HTTPS Certificate**.
2. Click **Download HTTPS Certificate Signing Request**.
3. Save the `<hostname>.csr` file.

You can provide the file to a Certificate Authority to sign, and then install the signed certificate.

Installing a CA signed and returned HTTPS certificate

You can upload and install a security certificate after a Certificate Authority has signed and returned it. The file that you upload and install must be a signed version of the

existing self-signed certificate. A CA-signed certificate helps prevent man-in-the middle attacks and provides better security protection than a self-signed certificate.

What you'll need

You must have completed the following actions:

- Downloaded the Certificate Signing Request file and had it signed by a Certificate Authority
- Saved the certificate chain in PEM format
- Included all certificates in the chain, from the Unified Manager server certificate to the root signing certificate, including any intermediate certificates present

You must have the Application Administrator role.

If the validity of certificate for which a CSR was created is more than 397 days, then the validity will be reduced to 397 days by the CA before signing and returning the certificate

Steps

1. In the left navigation pane, click **General** > **HTTPS Certificate**.
2. Click **Install HTTPS Certificate**.
3. In the dialog box that is displayed, click **Choose file…** to locate the file to upload.
4. Select the file, and then click **Install** to install the file.

Installing a HTTPS certificate generated using external tools

Example certificate chain

The following example shows how the certificate chain file might appear:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Installing a HTTPS certificate generated using external tools

You can install certificates that are self signed or CA signed and are generated using an external tool like OpenSSL, BoringSSL, LetsEncrypt.

You should load the private key along with the certificate chain because these certificates are externally generated public-private key pair. The permitted key-pair algorithms are “RSA” and “EC”. The **Install HTTPS Certificate** option is available in the HTTPS Certificates page under the General section. The file you upload should be in the following input format.

1. Private Key of the server that belongs to the Active IQ UM host
2. Certificate of the server that matches with the private key
3. Certificate of the CAs in reverse till the root, which are used to sign the above certificate

Format for loading a certificate with an EC key pair

The permitted curves are “prime256v1” and “secp384r1”. Sample of certificate with an externally generated EC pair:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Format for loading a certificate with an RSA key pair

The allowed key sizes for the RSA key-pair belonging to the host certificate are 2048, 3072, and 4096. certificate with an externally generated **RSA key pair**:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

After the certificate is uploaded, you should restart the Active IQ Unified Manager instance for the changes to take effect.

Checks while uploading externally generated certificates

The system performs checks while uploading a certificate generated using external tools. If any of the checks fail, then the certificate is rejected. There are also validation included for the certificates that are generated from the CSR within the product and for certificates that are generated using external tools.

- The private key in the input is validated against the host certificate in the input.
- The Common Name (CN) in the host certificate is checked against the FQDN of the host.
- The Common Name (CN) of the host certificate should not be empty or blank and should not be set to localhost.
- The validity start date should not be in future and the validity expiry date of the certificate should not be in the past.
- If Intermediate CA or CA exists the validity start date of certificate should not be in future and the validity expiry date should not be in the past.

The private key in the input should not be encrypted. If there are any private keys that are encrypted, then they are rejected by the system.

Example 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Example 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Example 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

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 HTTPS certificate, or install a new HTTPS certificate.

If you have not generated a new 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 an 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.

Copyright Information

Copyright © 2022 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.