



Changing the Unified Manager virtual appliance host name

Active IQ Unified Manager

NetApp
February 21, 2022

This PDF was generated from https://docs.netapp.com/us-en/active-iq-unified-manager/config/task_generate_an_https_security_certificate_ocf.html on February 21, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- Changing the Unified Manager virtual appliance host name 1
 - Generating an HTTPS security certificate 1
 - Restarting the Unified Manager virtual machine 4

Changing the Unified Manager virtual appliance host name

The network host is assigned a name when the Unified Manager virtual appliance is first deployed. You can change the host name after deployment. If you change the host name, you must also regenerate the HTTPS certificate.

What you'll need

You must be logged in to Unified Manager as the maintenance user, or have the Application Administrator role assigned to you to perform these tasks.

You can use the host name (or the host IP address) to access the Unified Manager web UI. If you configured a static IP address for your network during deployment, then you would have designated a name for the network host. If you configured the network using DHCP, the host name should be taken from the DNS. If DHCP or DNS is not properly configured, the host name "Unified Manager" is automatically assigned and associated with the security certificate.

Regardless of how the host name was assigned, if you change the host name, and intend to use the new host name to access the Unified Manager web UI, you must generate a new security certificate.

If you access the web UI by using the server's IP address instead of the host name, you do not have to generate a new certificate if you change the host name. However, it is the best practice to update the certificate so that the host name in the certificate matches the actual host name.

If you change the host name in Unified Manager, you must manually update the host name in OnCommand Workflow Automation (WFA). The host name is not updated automatically in WFA.

The new certificate does not take effect until the Unified Manager virtual machine is restarted.

Steps

1. [Generate an HTTPS security certificate](#)

If you want to use the new host name to access the Unified Manager web UI, you must regenerate the HTTPS certificate to associate it with the new host name.

2. [Restart the Unified Manager virtual machine](#)

After you regenerate the HTTPS certificate, you must restart the Unified Manager virtual machine.

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.

What you'll need

You must have the Application Administrator role.

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 Regenerate Using Current Certificate Attributes option.

If you want to...	Do this...
Generate the certificate using different values	<p data-bbox="841 159 1354 226">Click the Update the Current Certificate Attributes option.</p> <p data-bbox="841 260 1481 600">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 data-bbox="873 642 1451 1682">  <ul style="list-style-type: none"> <li data-bbox="1016 642 1451 709">• The permitted values for key size are 2048, 3072 and 4096. <li data-bbox="1016 730 1451 798">• The validity periods are minimum 1 day to maximum 36500 days. <p data-bbox="1036 831 1451 1241">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 data-bbox="1016 1274 1451 1682">• 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. </div>

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

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.

What you'll need

The virtual appliance is powered on.

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

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 © 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.