Generating an HTTPS security certificate

Active IQ Unified Manager 9.9

NetApp
February 20, 2023

Table of Contents

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 **Regenerate Using Current Certificate Attributes** option.

If you want to…	Do this…
Generate the certificate using different values	Click the **Update the Current Certificate Attributes** option. 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. • The permitted values for key size are `2048`, `3072` and `4096`. • The validity periods are minimum 1 day to maximum 36500 days. 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. • 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.

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

Trademark information