Managing security certificates

Active IQ Unified Manager 9.8

NetApp
February 20, 2023

Table of Contents

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.

Before you begin

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

About this task

Viewing the certificate enables you to verify the content of a regenerated certificate, or to view alternate URL names from which you can access Unified Manager.

Steps

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

   The HTTPS certificate is displayed at the top of the page

After you finish

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.

Generating an HTTPS security certificate

You might generate a new HTTPS security certificate for multiple reasons, including if you want to sign with a different Certificate Authority or if the current security certificate has expired. The new certificate replaces the existing certificate.

Before you begin

You must have the Application Administrator role.

About this task

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.

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.
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 other fields do not require values, but you can enter values, for example, for the City, State, and Country if you want those values to be populated in the certificate. ⓘ 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.

4. Click **Yes** to regenerate the certificate.
5. 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**.

Downloading an HTTPS certificate signing request

You can download a certification 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.

Before you begin

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.

After you finish

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

Installing an HTTPS security 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.

Before you begin

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.

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.

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-----
```

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.

Copyright information

Trademark information