Using SSL/TLS With Active Directory AND LDAP In Nagios Fusion 2024

Purpose

This document describes how to use SSL/TLS with Active Directory (AD) AND LDAP in Nagios Fusion 2024.

Prerequisites

You will need the following prerequisites to follow the documentation:

- Nagios Fusion 4.1 or newer
- Either of the following:
    - A separate Microsoft Windows-based AD infrastructure that is accessible to the Nagios Fusion machine
    - Separate LDAP infrastructure (like OpenLDAP) that is accessible to the Nagios Fusion machine

Certificate Overview

A "brief" explanation of certificates is required to be able to explain which certificate needs to be uploaded to your Nagios Fusion server and why.

You will be familiar with certificates when shopping online using your web browser. When you connect to a server using SSL/TLS, the server you are connecting to will provide a certificate to use for encryption and security. Your computer will verify that the certificate provided is valid, but how does it do this? The certificate you are presented with is generated by a trusted source, a certificate authority (CA). Your computer has a copy of the CA certificate and can validate that the certificate you are being provided with is actually a valid certificate. Your computer's operating system keeps the public list of CA certificates up to date, it's not something that you need to worry about.

Certificates are also used for user authentication on private networks, such as communicating with an AD/LDAP server. If you have a Windows computer that is joined to an AD, certificates are used by the domain controller(s) (DC) to securely transmit username and password information. In this scenario the domain controller(s) have certificates that are issued by a private CA in the Windows domain. For all of this to work, the CA certificate of the Windows domain needs to exist on your local computer. Computers that participate in a Windows domain automatically have a copy of this CA certificate, it happens automatically.

Why did all of that need to be explained? When Nagios Fusion connects to an LDAP/AD server to authenticate a user, the domain controller you are authenticating with provides the Nagios Fusion server with a certificate to use for encryption and security. Nagios Fusion is running on a Linux server, there is no way that it would have a copy of your Windows domain CA certificate, so it will not be able to verify the certificate of the domain controller you are authenticating against. The purpose of this documentation is to upload the CA certificate onto your Nagios Fusion so that Nagios Fusion can trust the certificate the domain controller provides.

It does need to be made clear that it is the CA certificate that is required. Even in simple single-server AD domains (like Windows Server Essentials), the CA certificate is a different certificate to the certificate of the server itself. This might be clearer in a larger AD domain. You might have three separate DCs; however, they all have certificates issued to them by the CA. To be able to authenticate against all three servers you need to upload the CA to your Nagios Fusion. This documentation will walk you through the steps to obtain and then upload the CA certificate.

Obtaining The Certificate - Microsoft Windows

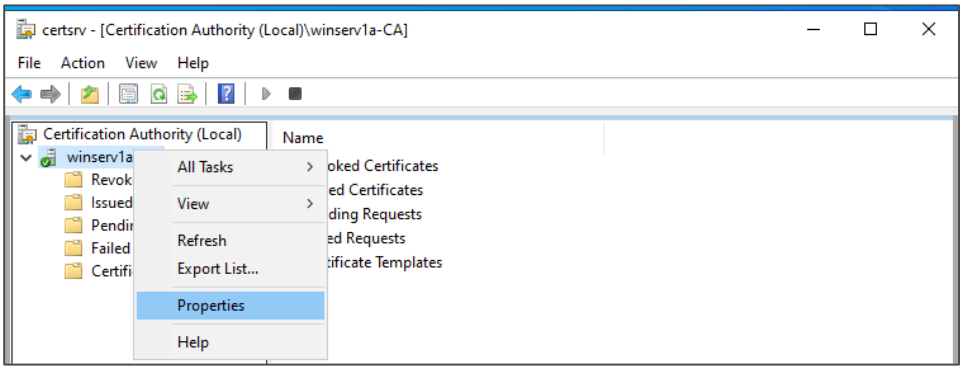
These steps are based on obtaining the CA certificate from your Microsoft Windows CA server. There are two methods explained here:

- Method 1: Console / RDP Session To CA Server
- Method 2: CA Server Web Interface

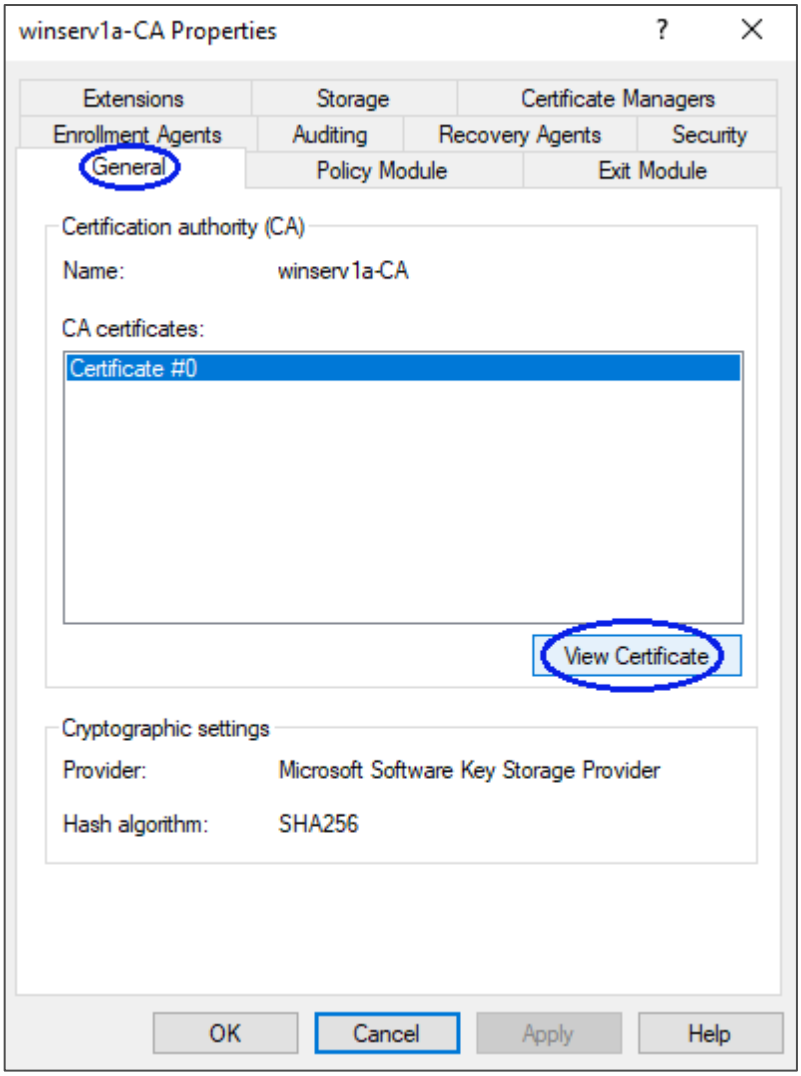
Method 1: Console/RDP Session to CA Server

Using this method, you will need a console or RDP session to your CA server.

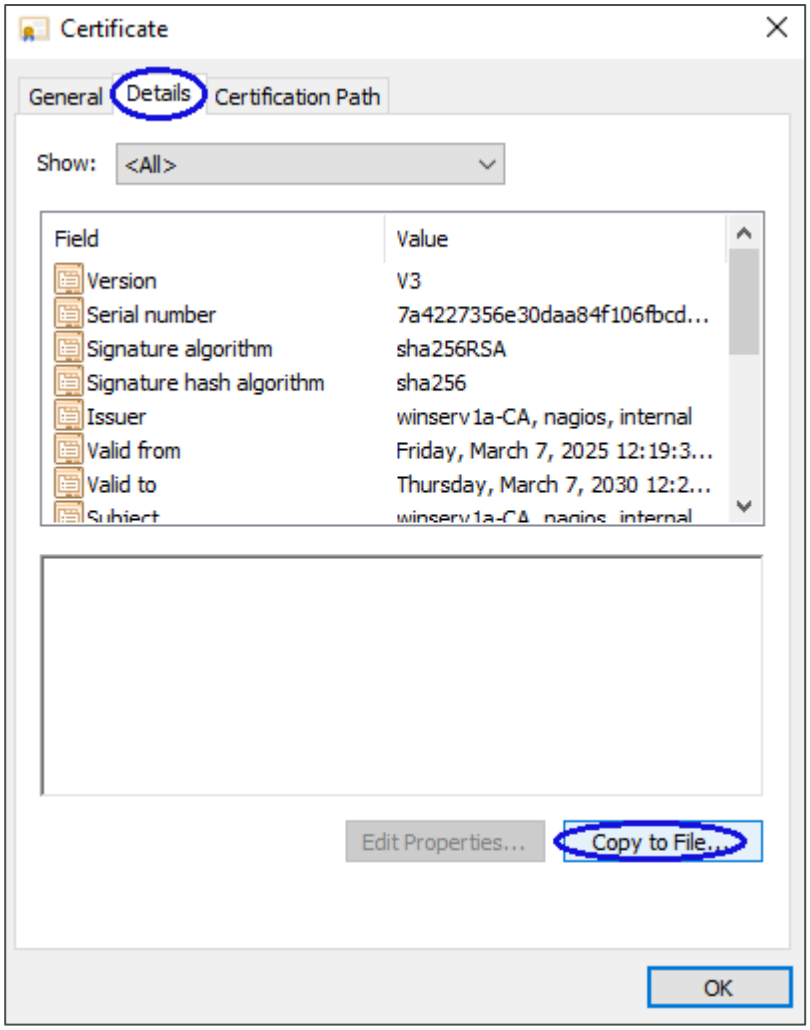
1. Navigate to **Administrative Tools** (commonly found in the control panel) and open **Certification Authority**.
2. When the **Certification Authority** opens right click on the **CA server** and select **Properties**.



3. When the **Properties** window appears, you will be on the **General** tab.
4. Click the **View Certificate** button.

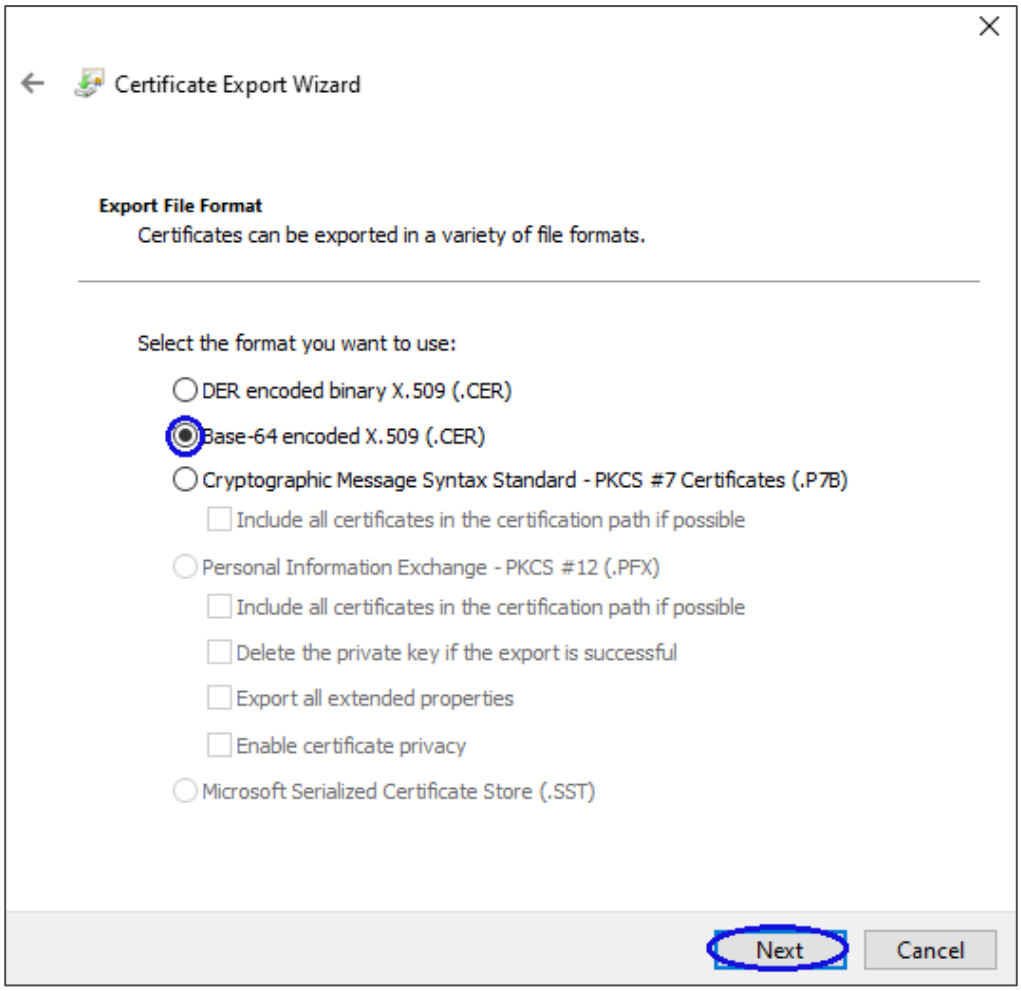


5. When the Certificate window appears, click on the **Details** tab.
6. Click the **Copy to File** button.

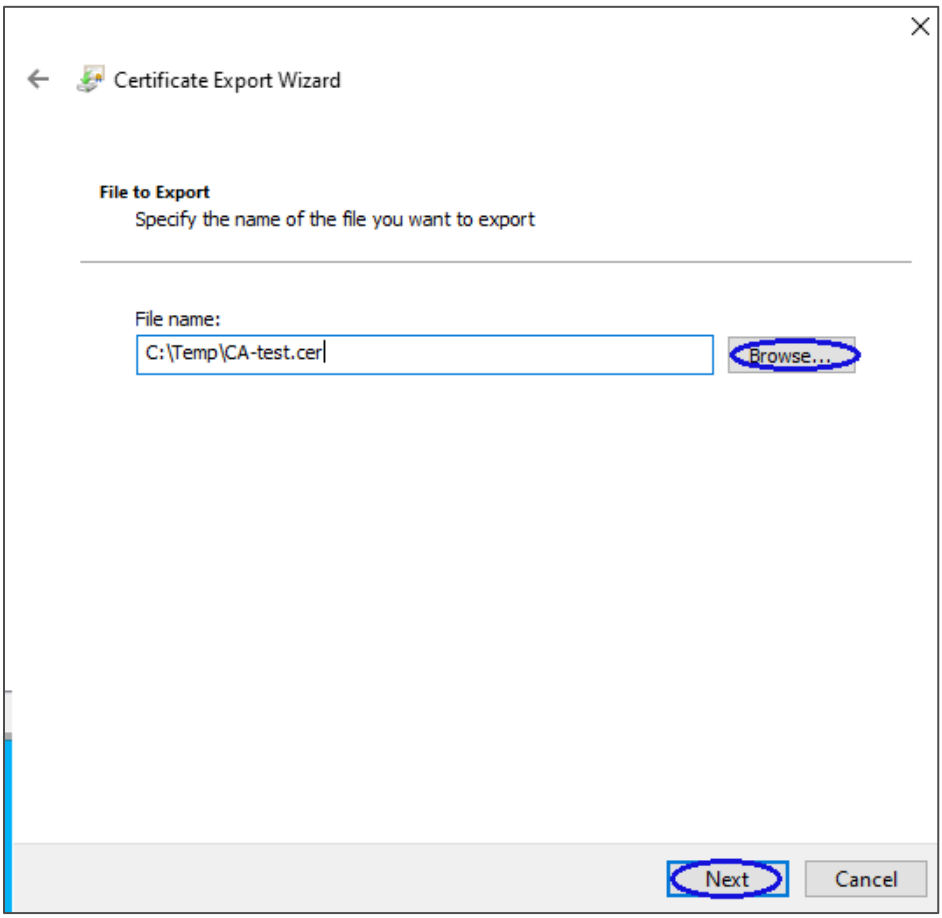


7. The Certificate Export Wizard window appears, click **Next**.

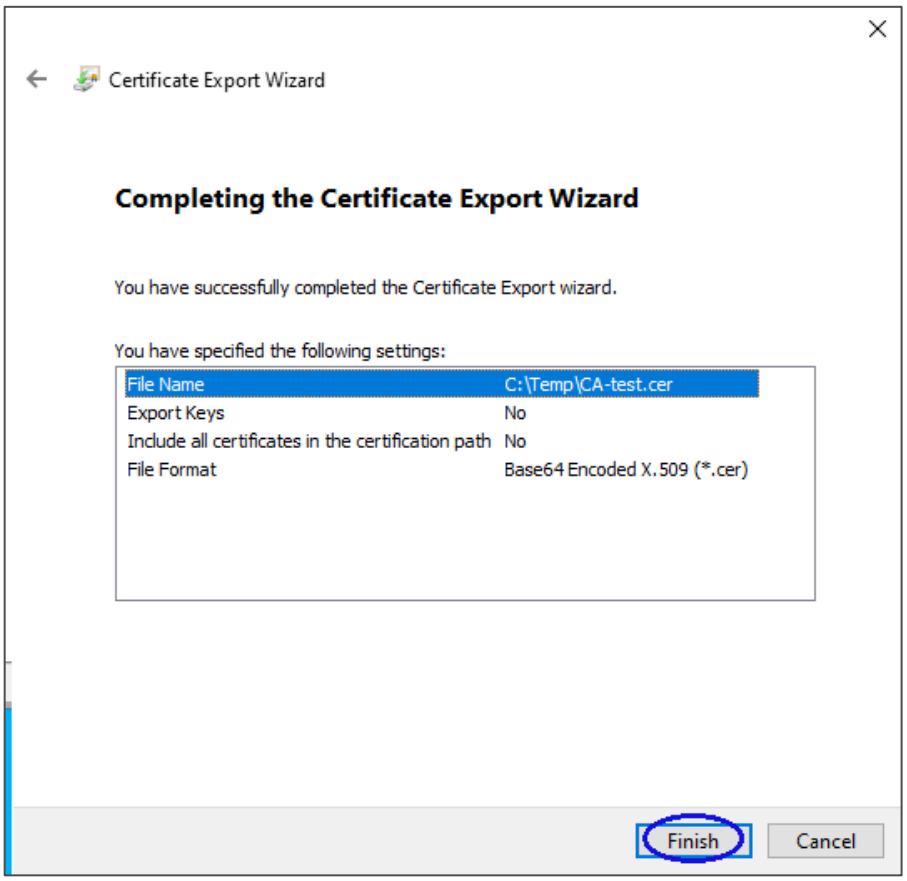
8. Select **Base-64 encoded X.509 (.CER)** and then click **Next**.



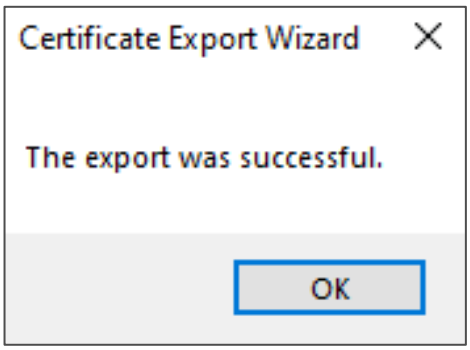
9. Use the **Browse** button to select a location to save the certificate file to, and provide a name for the certificate.
10. Click **Next** to continue.



11. Click the **Finish** button to export the certificate.



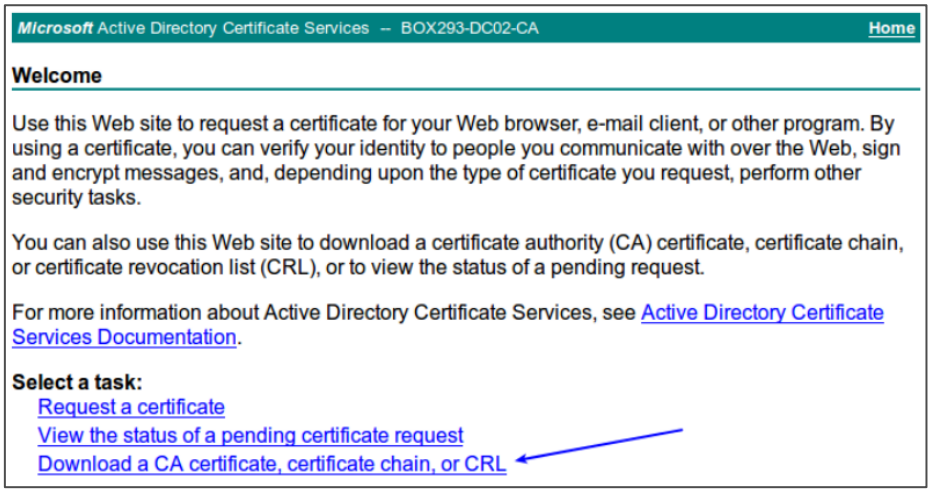
You will receive a message to confirm the certificate export was a success. Click **OK**. You can now close all the open windows. You can now proceed to the Upload Certificate section of this document. Make sure you have access to the exported .cer file from the computer you will upload the certificate to Nagios XI from



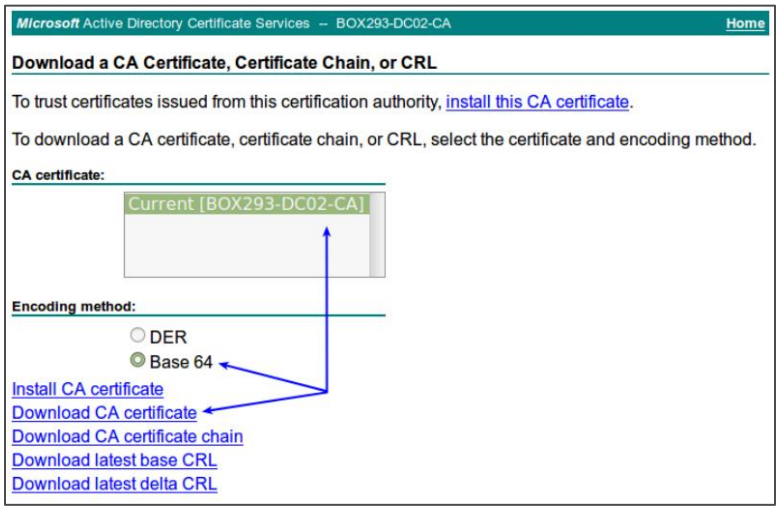
Method 2: CA Server Web Interface

If the CA server publishes the Certificate Services web page, you can download the CA certificate directly from there.

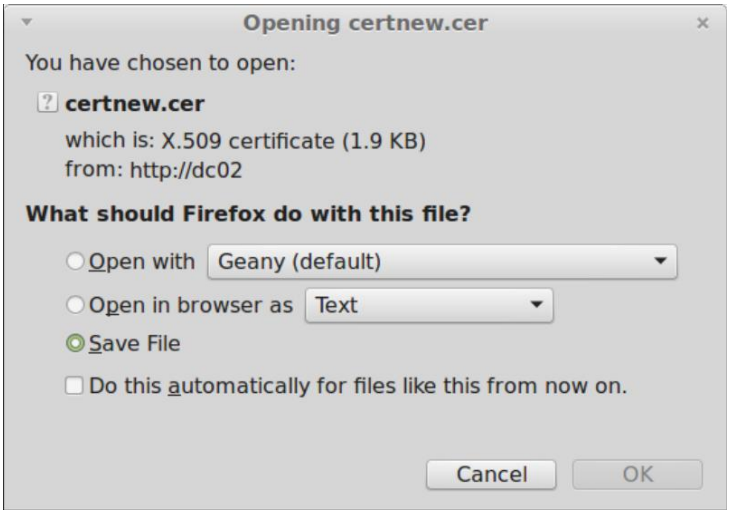
1. Navigate to `http://<caservername>/certsrv`. Replace `<caservername>` with the address of your CA server. Provide valid credentials when prompted. You will be presented with a page similar to this screenshot.



2. Click the **Download a CA certificate, certificate chain, or CRL** link.
3. Select the CA certificate from the list of available certificates.
4. Select **Base 64**.
5. Click the **Download CA certificate** link.



6. You will be prompted by your web browser to save the file; it should be named `certnew.cer`. This will vary depending on the web browser you are using.



Proceed to the Upload Certificate section of this document. Make sure you have access to the exported `.cer` file from the computer you will use to upload the certificate to Nagios Fusion.

Obtaining The Certificate - LDAP Server

There are many implementations of LDAP servers, making it difficult to document the exact location of your CA certificate file. One method is to search the `cn=config` for the `olcTLSCACertificateFile` attribute. Execute the following command on your LDAP server:

```
slapcat -b cn=config | grep olcTLSCACertificateFile
```

An example of the output is as follows:

```
olcTLSCACertificateFile: /etc/openldap/certs/ca_box293_cert.pem
```

You can see the location of the CA certificate file in the output. In the Upload Certificate section of this document, you will be required to copy and paste the contents of this file. To view the contents, execute the following command:

```
cat /etc/openldap/certs/ca_box293_cert.pem
```

Proceed to the Upload Certificate section of this document.

Upload Certificate

In this step you will upload the CA certificate to the Nagios Fusion server.

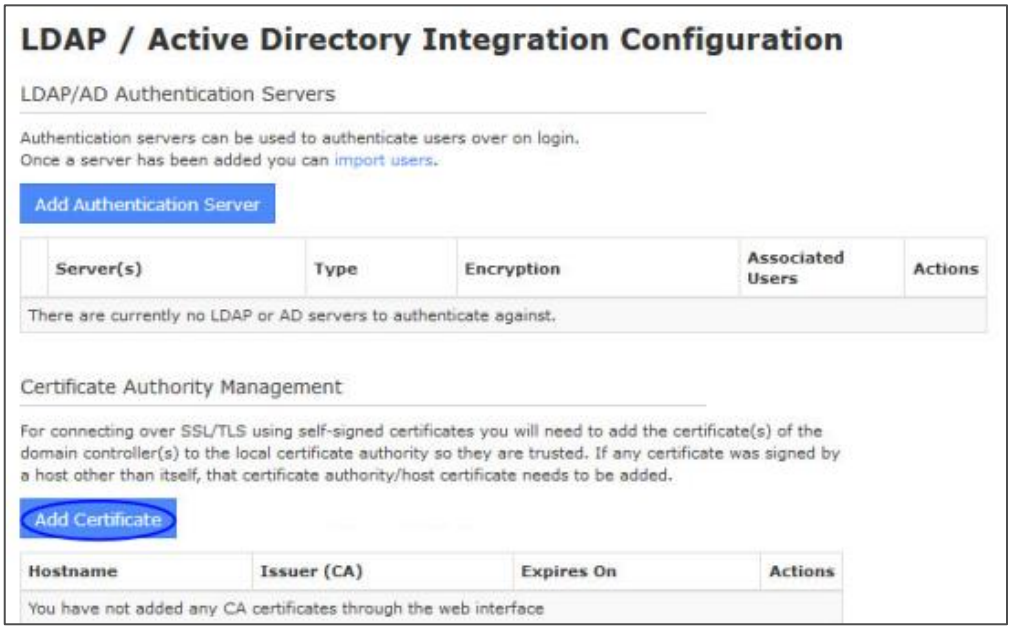
1. Open the certificate you exported in a text editor such as Notepad, it will appear similar to this screenshot.
2. Select all of the text (**Ctrl** + **A**) and copy (**Ctrl** + **C**) it to your clipboard.

   Make sure to include the

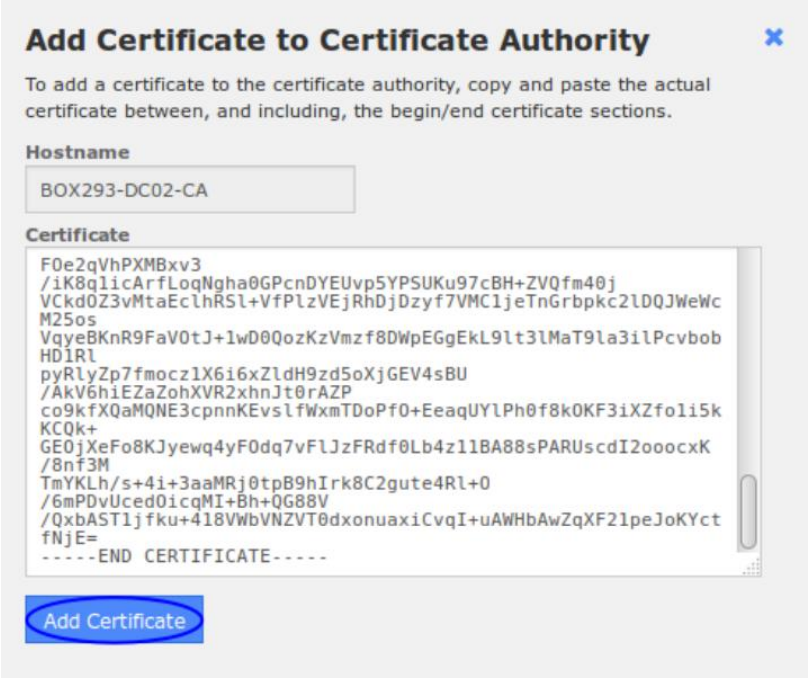
   `-----BEGIN CERTIFICATE-----` and

   `-----END CERTIFICATE-----` lines.

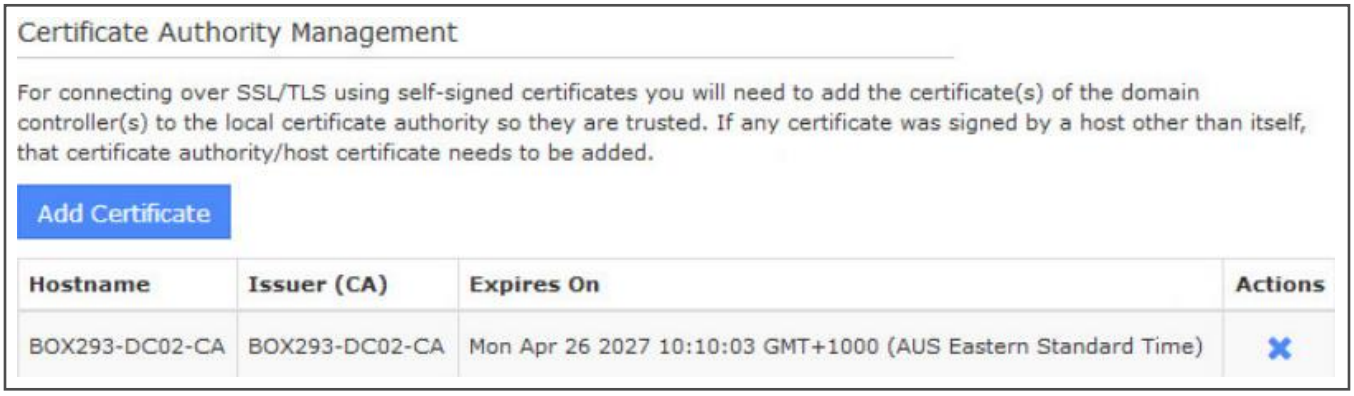
3. Open Nagios Fusion and navigate to **Admin > Users > LDAP/AD Integration**.
4. Click the **Add Certificate** button.



5. The **Add Certificate to Certificate Authority** window will appear.
6. Paste the text in your clipboard into the **Certificate** field. The formatting may look different from the text editor, but this is expected.
7. Once pasted, the **Hostname** field will automatically populate with the CA name.
8. Click the **Add Certificate** button to finish uploading this certificate to Nagios Fusion.



9. Once the certificate is uploaded, it will appear in the list of certificates in the **Certificate Authority Management** section.

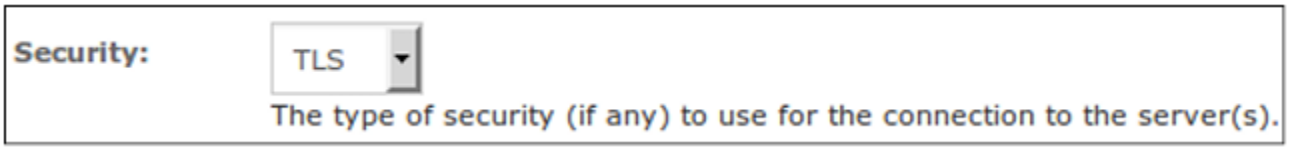


This completes uploading the certificate to Nagios Fusion.

Configure Authentication Server

This guide does not explain how to add an Authentication Server to Nagios Fusion, please refer to the Authenticating and Importing Users with AD and LDAP documentation.

The following screenshot shows the Security setting that requires authentication to use SSL/TLS with certificates.



You do not actually define which CA certificate is used. When Nagios Fusion is presented with a certificate from the LDAP/AD server, Nagios Fusion checks it's local CA store for the CA certificate to validate the certificate provided by the LDAP/AD server.

Finishing Up

This completes the documentation on how to use SSL/TLS with Active Directory and LDAP in Nagios Fusion. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library