

# Using SSL/TLS With Active Directory And LDAP In Nagios Fusion 2026R2

## Purpose

This document describes how to use SSL/TLS with Active Directory (AD) AND LDAP in Nagios Fusion 2026R2.

## Prerequisites

You will need the following prerequisites to follow the documentation:

- Nagios Fusion 2026R2 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.

# Using SSL/TLS With Active Directory And LDAP In Nagios Fusion 2026R2

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

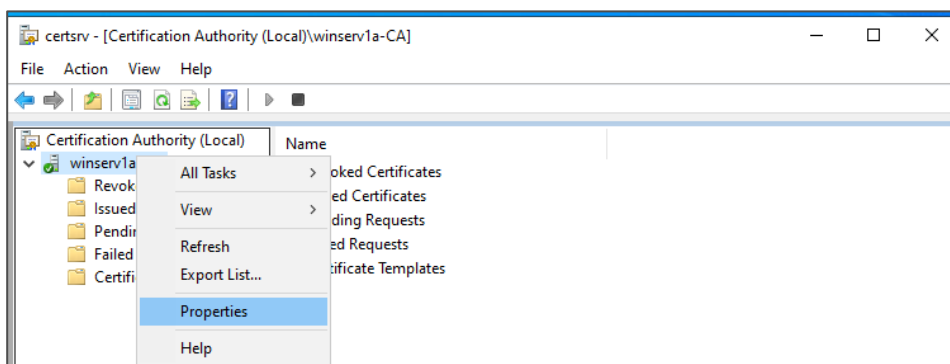
These steps are based on obtaining the CA certificate from your Microsoft Windows CA server. There are two methods explained here:

- [Method 1: Console / RDP Session To CA Server](#)
- [Method 2: CA Server Web Interface](#)

### Method 1: Console/RDP Session to CA Server

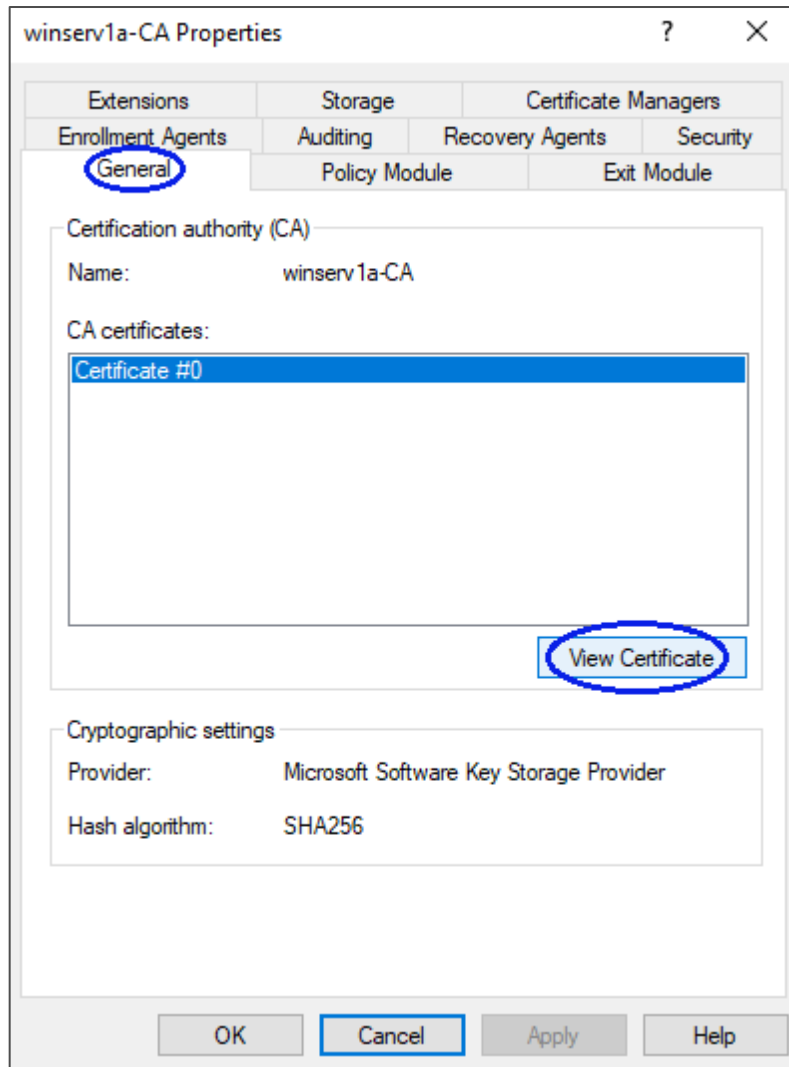
Using this method, you will need a console or RDP session to your CA server.

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**.



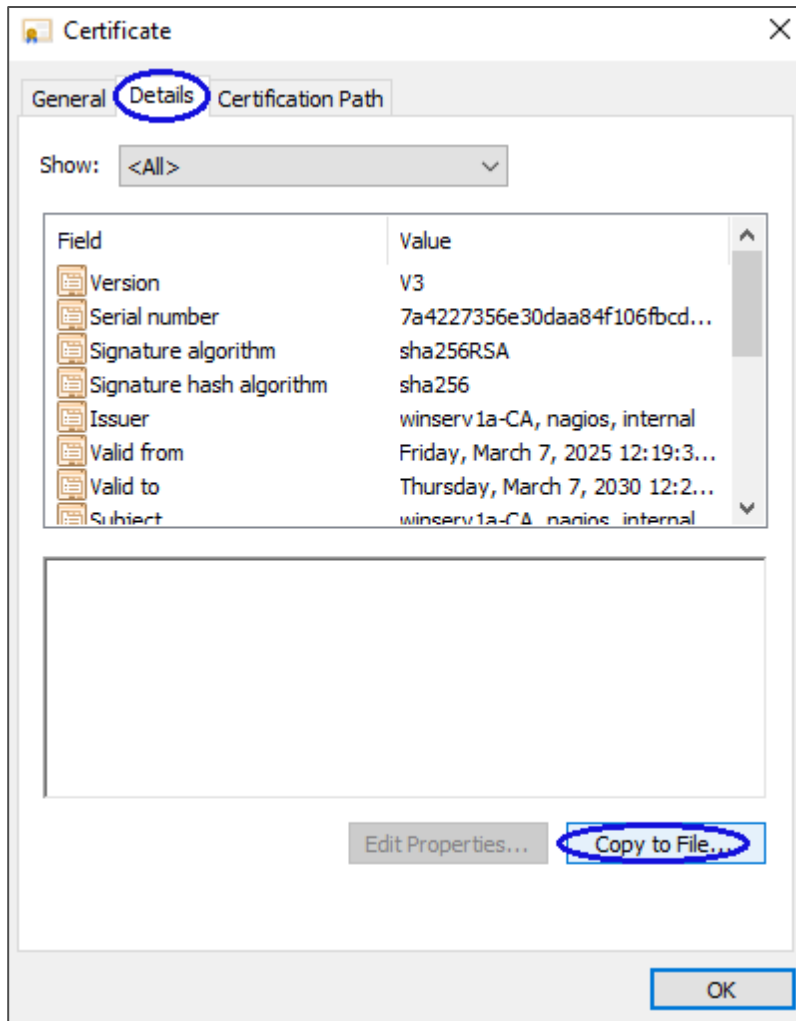
# Using SSL/TLS With Active Directory And LDAP In Nagios Fusion 2026R2

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



# Using SSL/TLS With Active Directory And LDAP In Nagios Fusion 2026R2

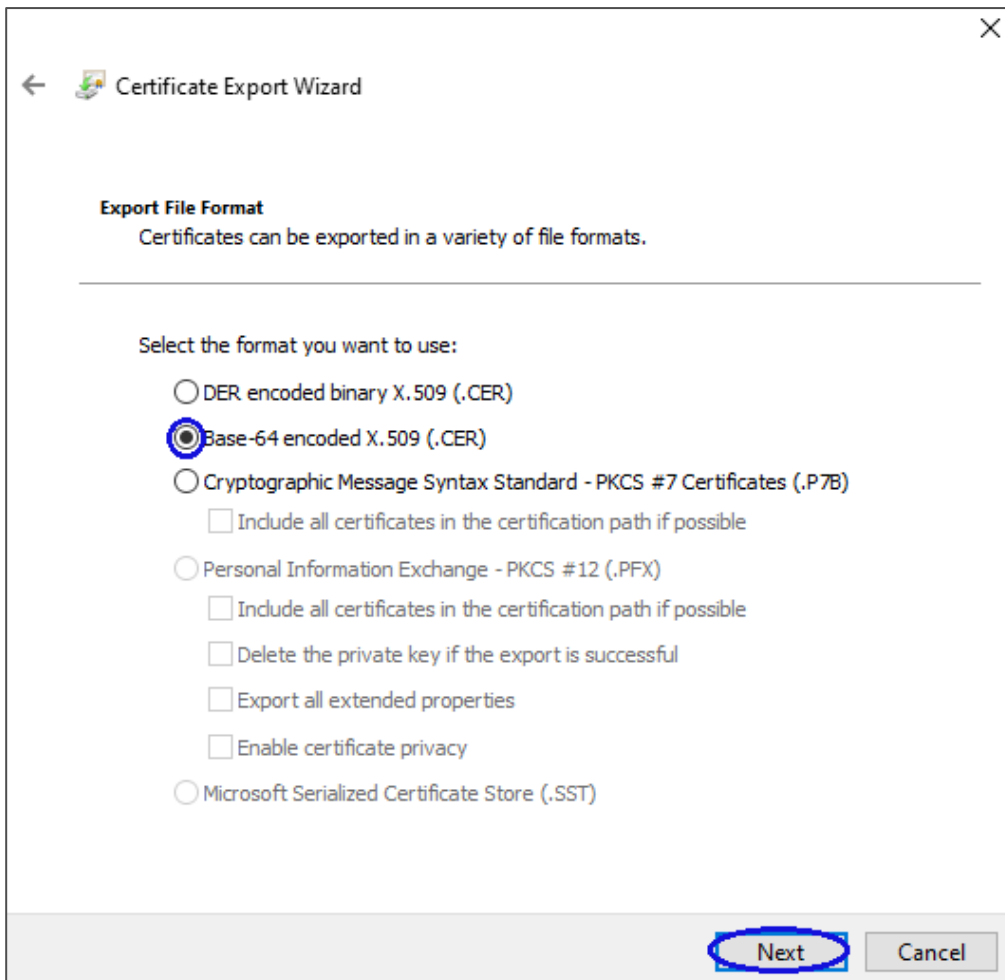
5. When the Certificate window appears, click on the **Details** tab.
6. Click the **Copy to File** button.



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

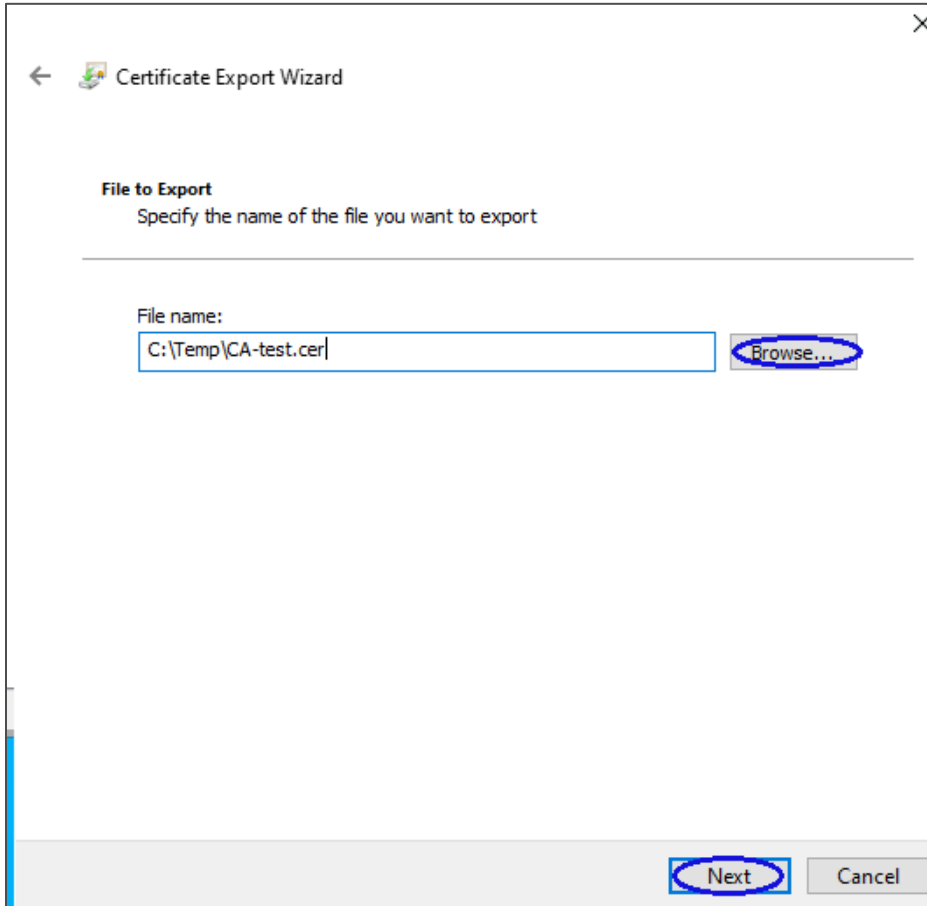
# Using SSL/TLS With Active Directory And LDAP In Nagios Fusion 2026R2

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



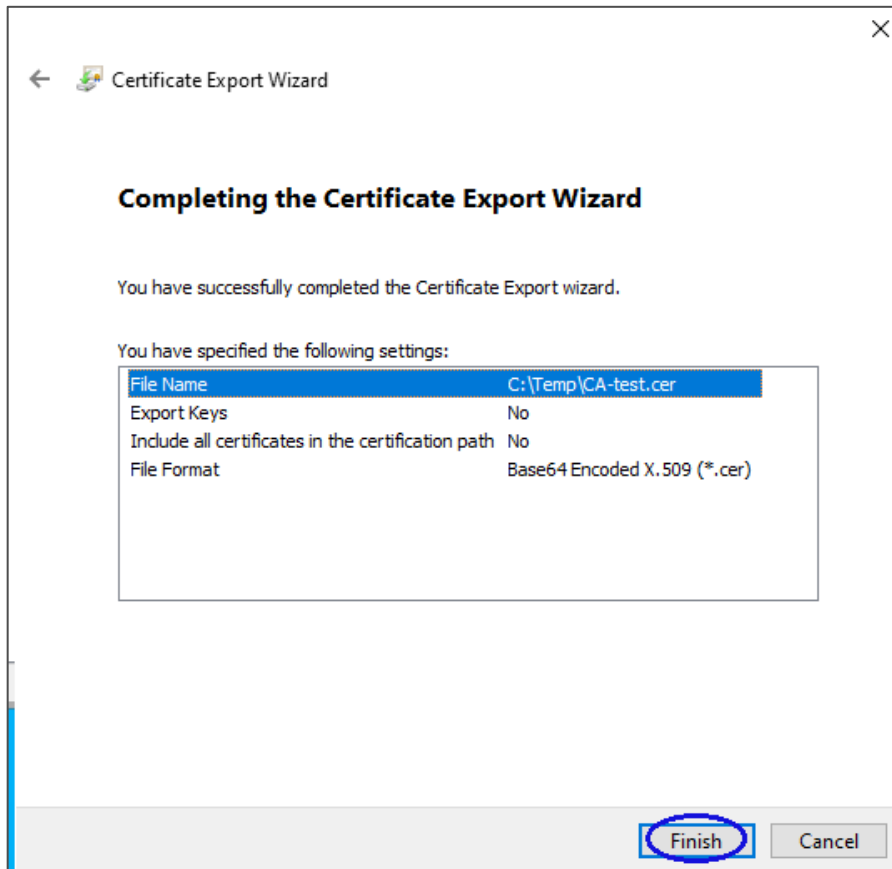
# Using SSL/TLS With Active Directory And LDAP In Nagios Fusion 2026R2

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.

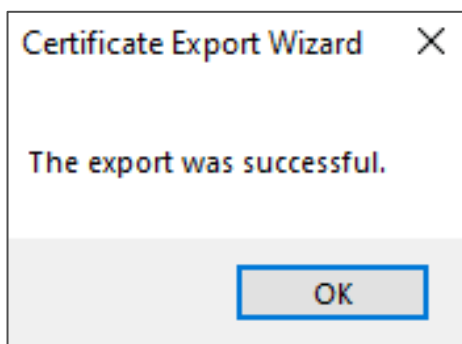


# Using SSL/TLS With Active Directory And LDAP In Nagios Fusion 2026R2

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

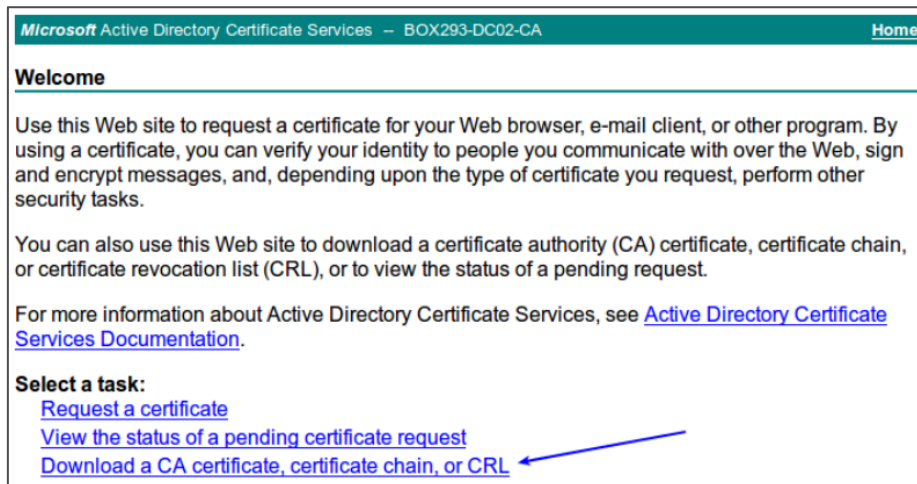


# Using SSL/TLS With Active Directory And LDAP In Nagios Fusion 2026R2

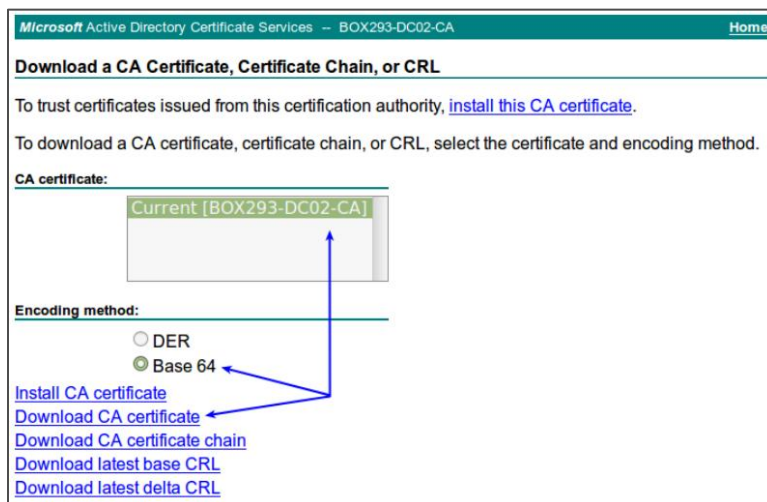
## Method 2: CA Server Web Interface

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.

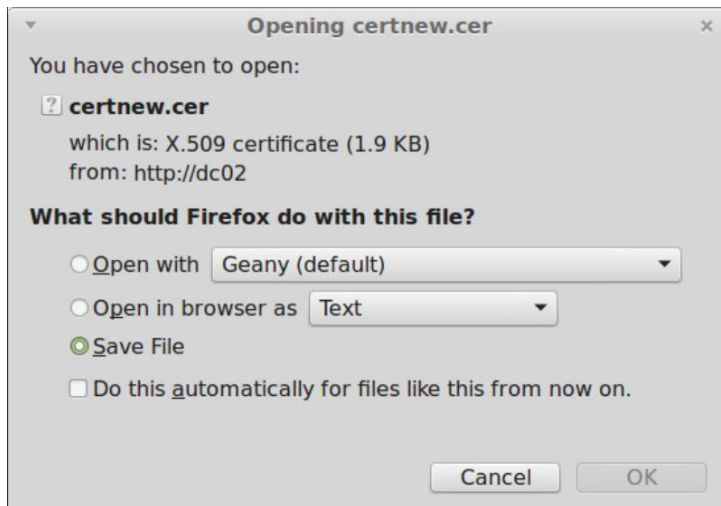


2. Click the **Download a CA certificate, certificate chain, or CRL** link.
3. Select the CA certificate from the list of available certificates.
4. Select **Base 64**.
5. Click the **Download CA certificate** link.



# Using SSL/TLS With Active Directory And LDAP In Nagios Fusion 2026R2

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

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

Make sure to include the

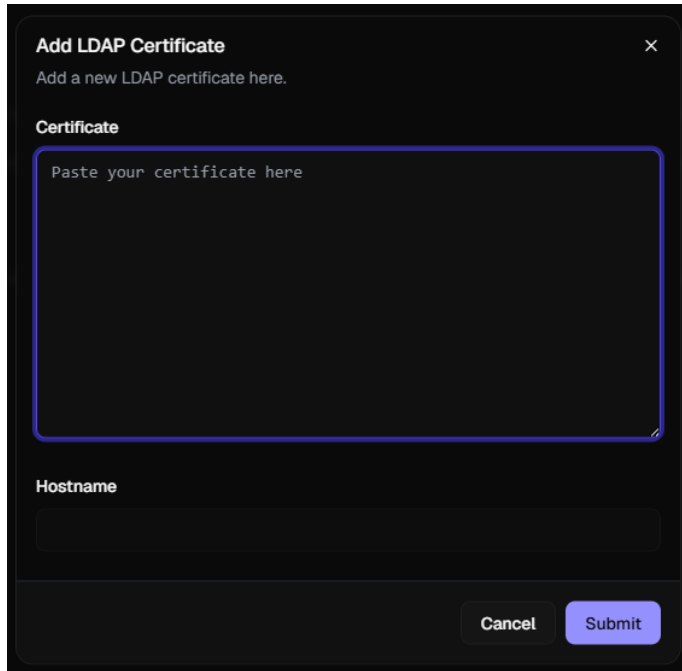
-----BEGIN CERTIFICATE----- and  
-----END CERTIFICATE----- lines.

- Open Nagios Fusion and navigate to **Administration > User Management > AD/LDAP**.
- Click the **Add Certificate** button.



# Using SSL/TLS With Active Directory And LDAP In Nagios Fusion 2026R2

11. The **Add Certificate** window will appear.



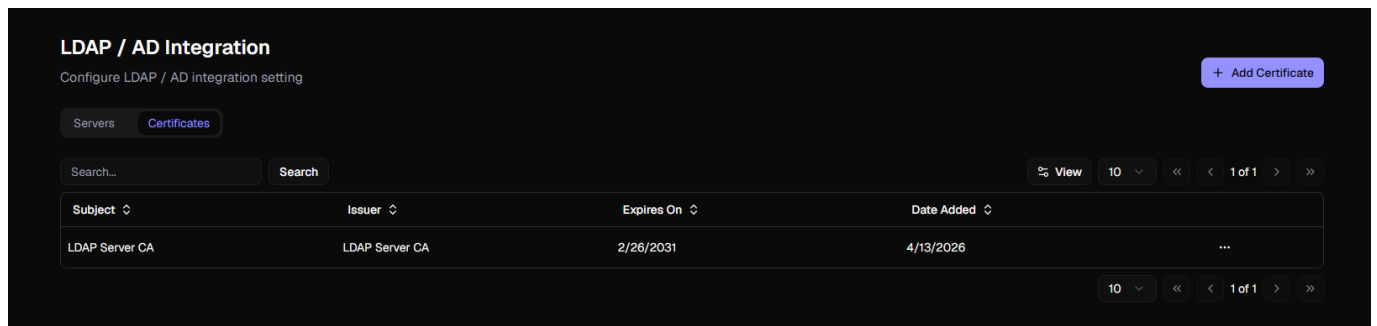
The image shows a dialog box titled "Add LDAP Certificate" with a close button (X) in the top right corner. Below the title is the instruction "Add a new LDAP certificate here." The dialog contains two main fields: "Certificate" and "Hostname". The "Certificate" field is a large text area with the placeholder text "Paste your certificate here". The "Hostname" field is a smaller text input. At the bottom right of the dialog are two buttons: "Cancel" and "Submit".

12. Paste the text in your clipboard into the **Certificate** field. The formatting may look different from the text editor, but this is expected.

13. Once pasted, the **Hostname** field will automatically populate with the CA name.

14. Click the **Submit** button to finish uploading this certificate to Nagios Fusion.

15. Once the certificate is uploaded, it will appear in the list of certificates in the **Certificates** section.



The image shows the "LDAP / AD Integration" section of the Nagios Fusion interface. It has a sub-header "Configure LDAP / AD integration setting" and a "+ Add Certificate" button. Below this are two tabs: "Servers" and "Certificates", with "Certificates" being the active tab. There is a search bar with the placeholder "Search..." and a "Search" button. To the right of the search bar are "View" and "10" dropdown menus, and navigation arrows. Below the search bar is a table with the following columns: "Subject", "Issuer", "Expires On", and "Date Added". The table contains one row with the following data: "LDAP Server CA", "LDAP Server CA", "2/26/2031", and "4/13/2026". At the bottom right of the table are "10", "1 of 1", and navigation arrows.

| Subject        | Issuer         | Expires On | Date Added |
|----------------|----------------|------------|------------|
| LDAP Server CA | LDAP Server CA | 2/26/2031  | 4/13/2026  |

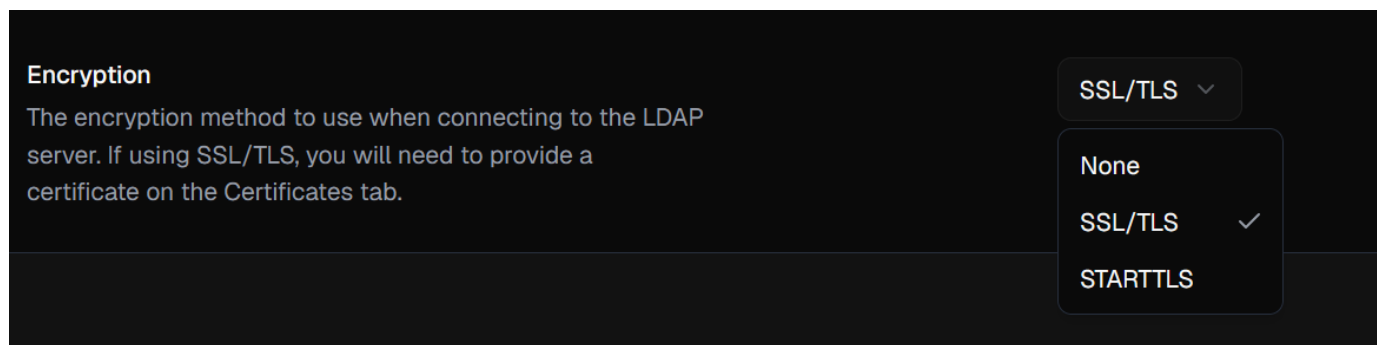
This completes uploading the certificate to Nagios Fusion.

# Using SSL/TLS With Active Directory And LDAP In Nagios Fusion 2026R2

## Configure Authentication Server and Users

This guide does not explain how to add an Authentication Server and add users to Nagios Fusion. Please refer to the [Authenticating and Importing Users with AD and LDAP](#) documentation for details.

The following screenshot shows the **Encryption** setting that requires authentication to use SSL/TLS with certificates:



The screenshot shows a configuration interface for the 'Encryption' setting. On the left, there is a text description: 'The encryption method to use when connecting to the LDAP server. If using SSL/TLS, you will need to provide a certificate on the Certificates tab.' To the right of this text is a dropdown menu. The dropdown is currently open, showing three options: 'None', 'SSL/TLS' (which is selected and marked with a checkmark), and 'STARTTLS'. The dropdown menu has a small 'x' icon in the top right corner.

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 Using TLS with AD & LDAP in Nagios Fusion 2026R2. If you have additional questions or other support-related questions, please visit the Nagios Support Forum, Nagios Documentation Hub, or Nagios Library:

[Visit Nagios Support Forum](#)

[Visit Documentation Hub](#)

[Visit Nagios Library](#)