

How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

Prerequisites

You will need the following prerequisites to follow the documentation:

- Nagios Log Server 2026R2
 - A separate Microsoft Windows-based AD infrastructure that is accessible to the Nagios Log Server machine
- or-
- A separate LDAP infrastructure (like OpenLDAP) that is accessible to the Nagios Log Server machine

Certificate Overview

A "brief" explanation of certificates is required to be able to explain which certificate needs to be uploaded to your Nagios Log Server instance 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 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 and it happens automatically.

Why did all of that need explaining? When Nagios Log Server connects to an LDAP / AD server to authenticate a user, the domain controller you are authenticating with provides the Nagios Log Server instance with a certificate to use for encryption and security. Nagios Log Server 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 Log Server so that Nagios Log Server can trust the certificate the domain controller provides.

How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

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 DC's 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 Log Server. The following documentation will walk you through the steps to obtain and then upload the CA certificate.

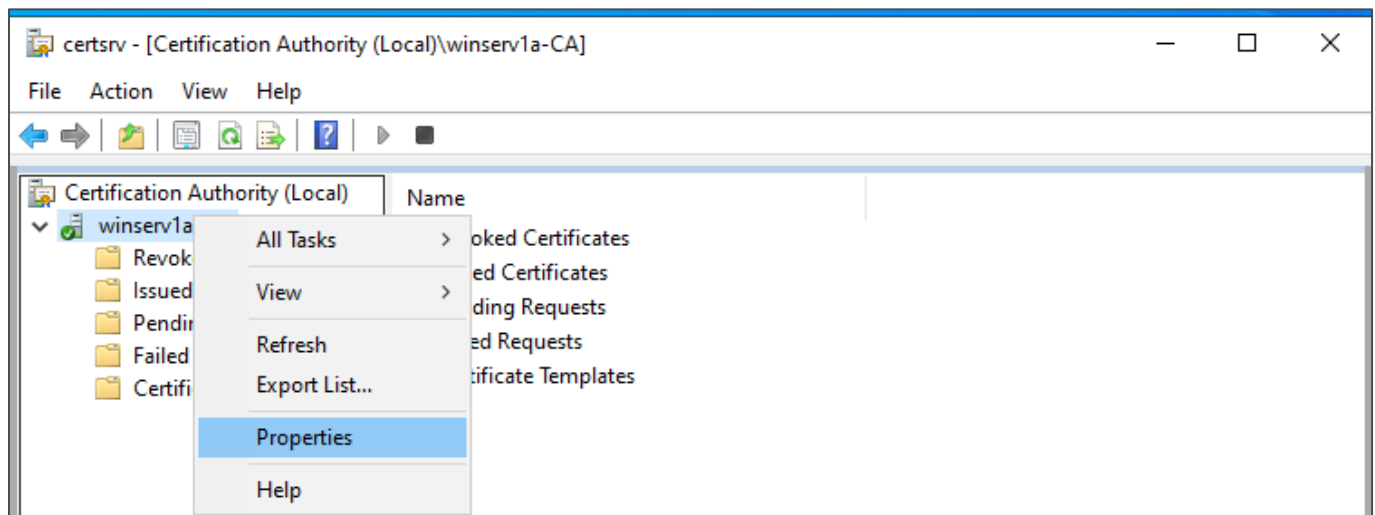
Obtaining The Certificate - Microsoft Windows

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

Method 1) Console / RDP Session To CA Server

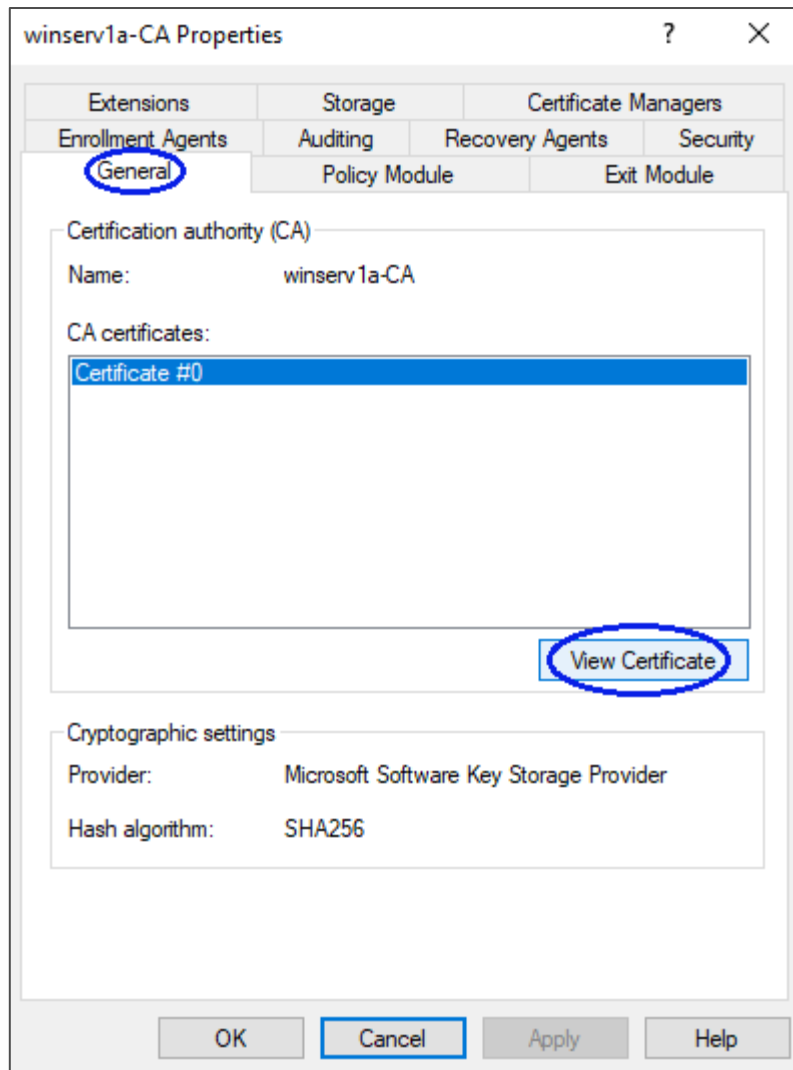
Using this method, you will need a console or RDP session to your CA server.

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**.



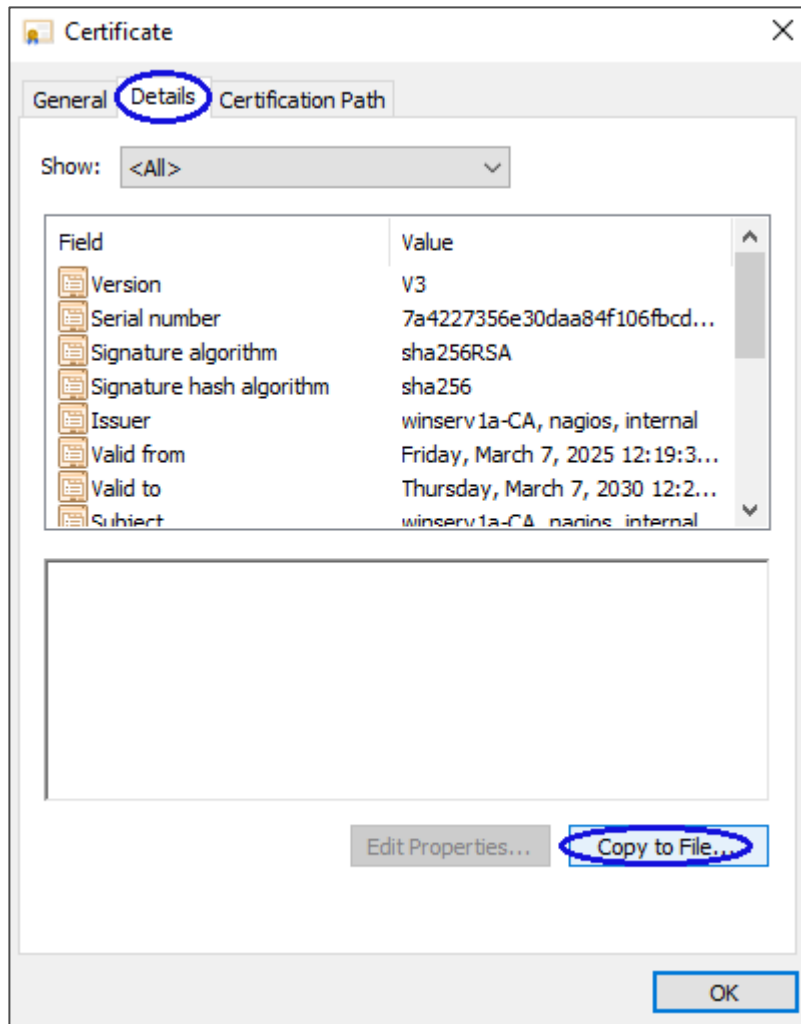
How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

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



How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

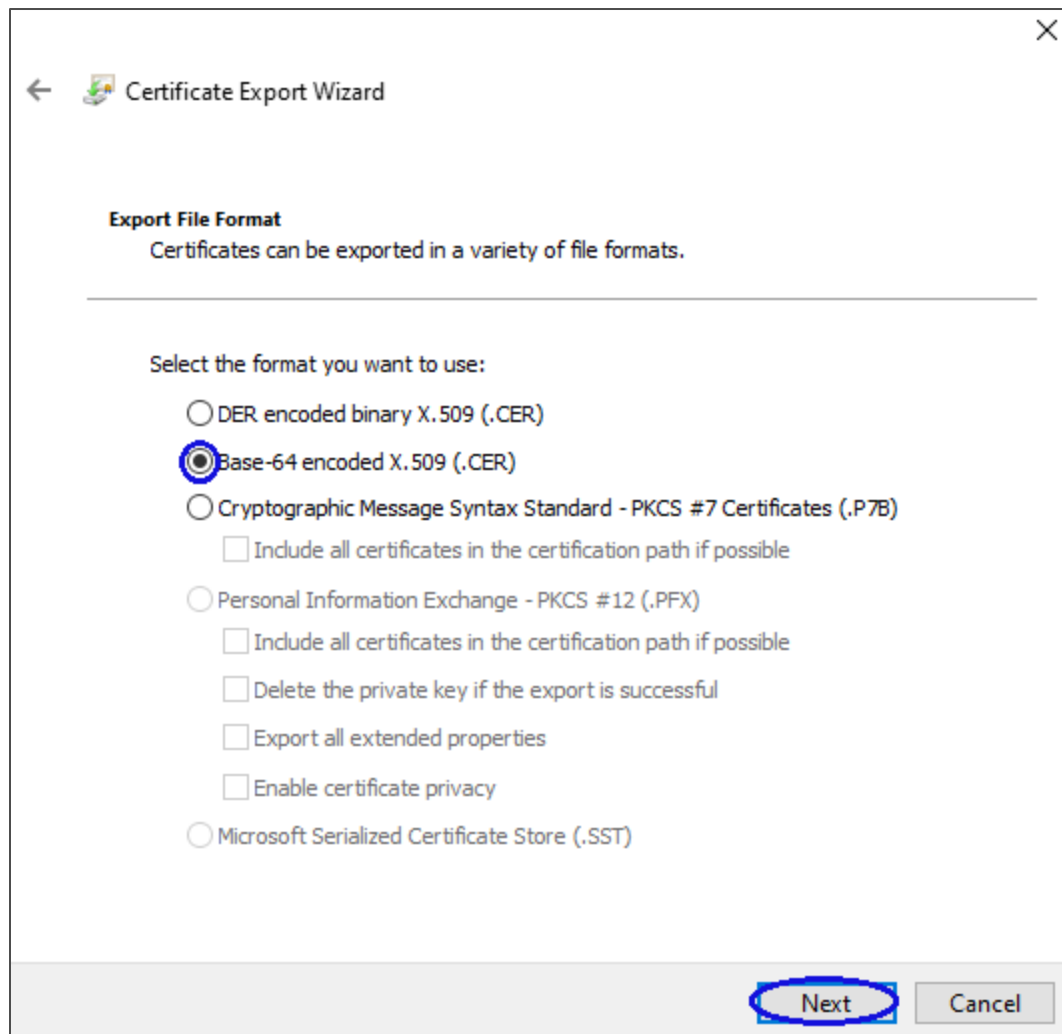
5. When the Certificate window appears, click on the **Details** tab.
6. Click the **Copy to File** button.



7. When the **Certificate Export Wizard** window appears, click **Next**.

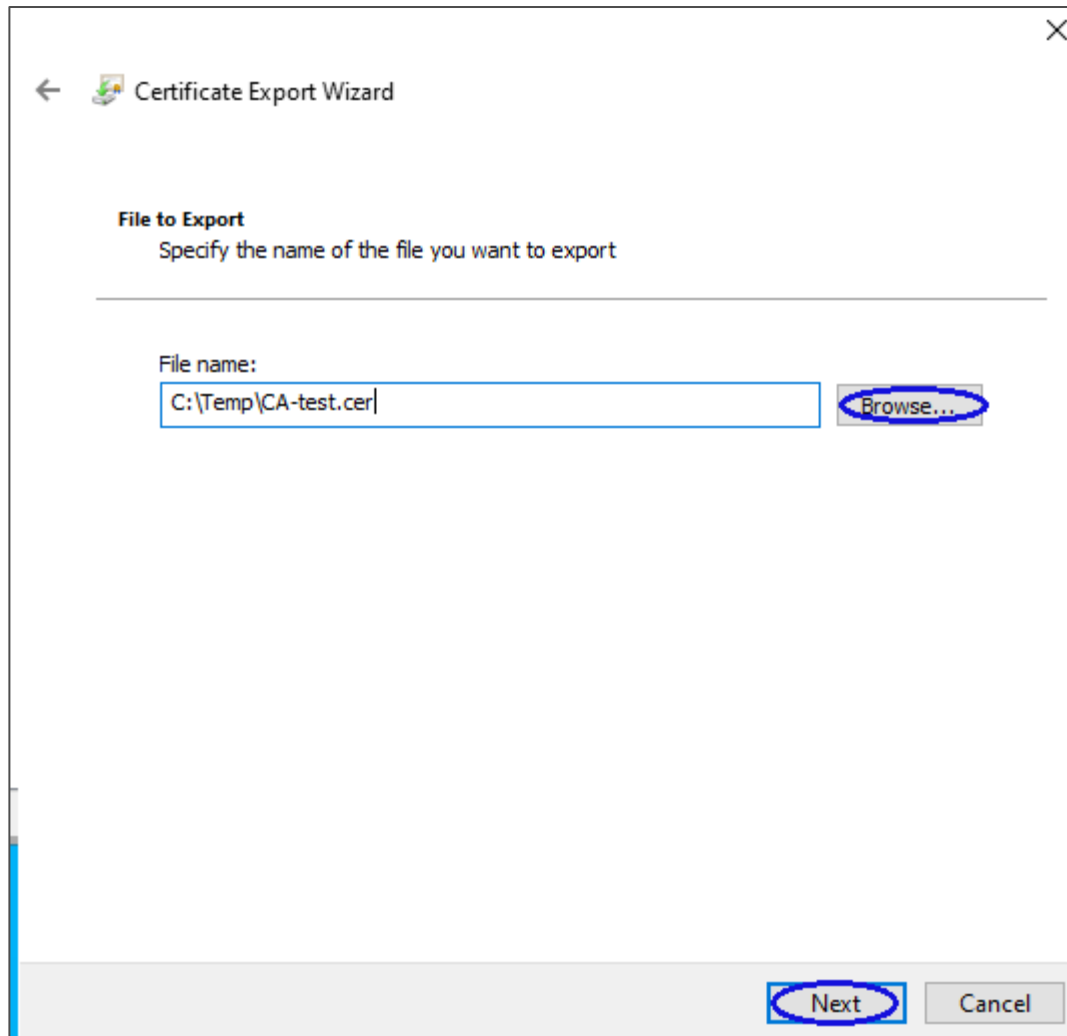
How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

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



How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

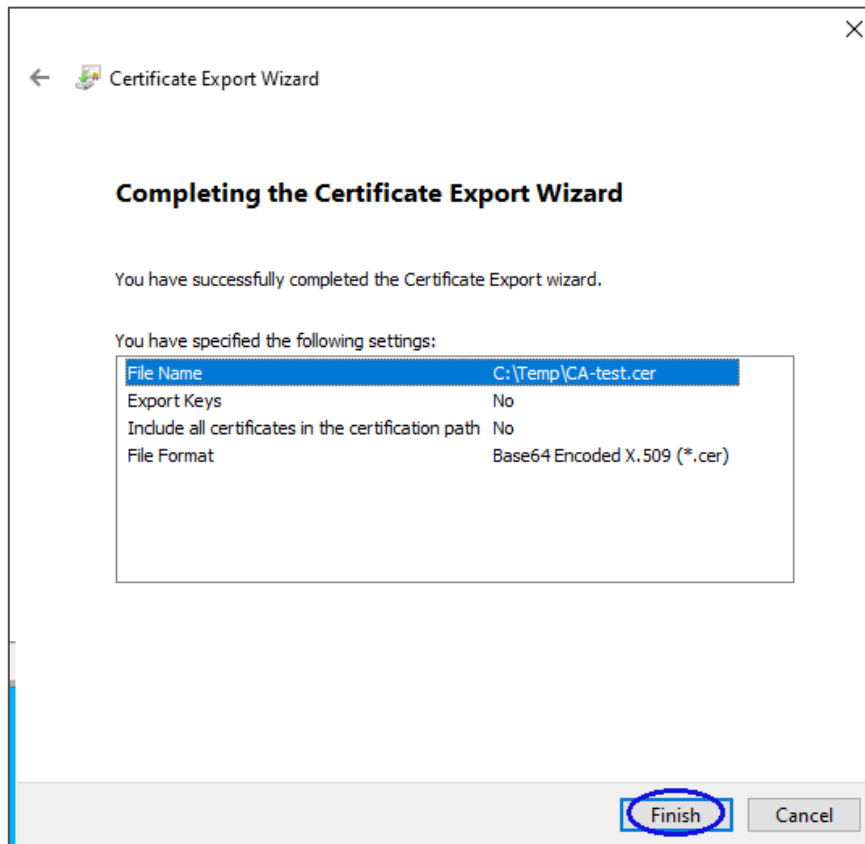
9. Use the **Browse** button to select a location to save the certificate file to, you will need to provide a name for the certificate.



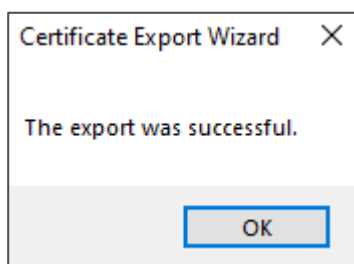
10. Click **Next** to continue.

How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

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



12. You will receive a message to confirm the certificate export was a success. Click **OK**.



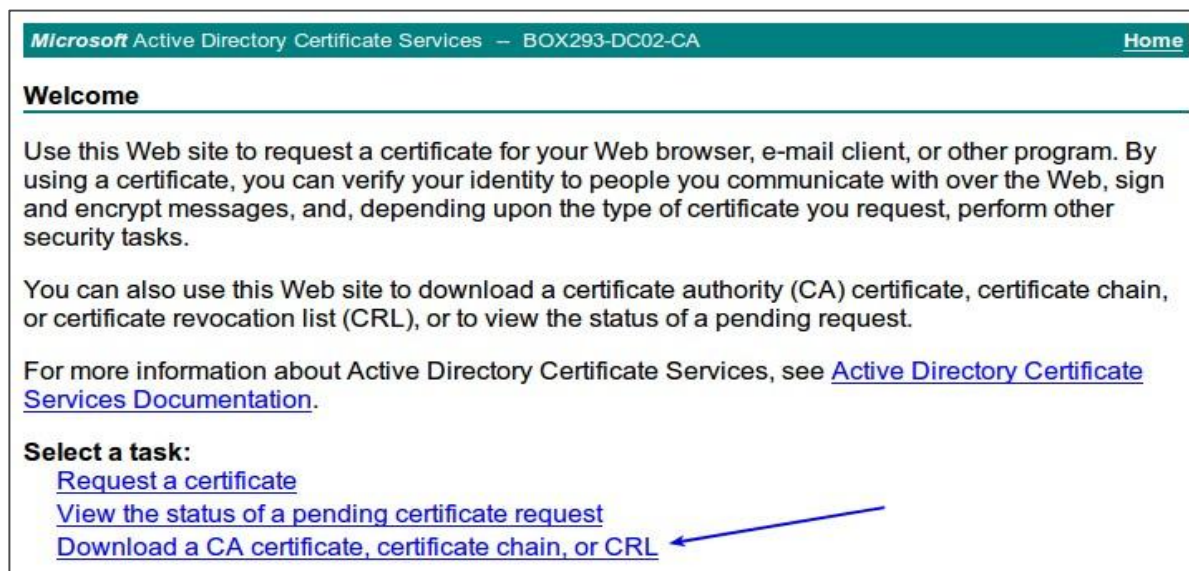
You can now close all the open windows and proceed to the [Upload Certificate](#) section of this document. Make sure you have access to the exported .cer file from the computer you will upload the certificate to Nagios Log Server from.

How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

Method 2) CA Server Web Interface

If the CA server publishes the Certificate Services web page you can download the CA certificate from this page.

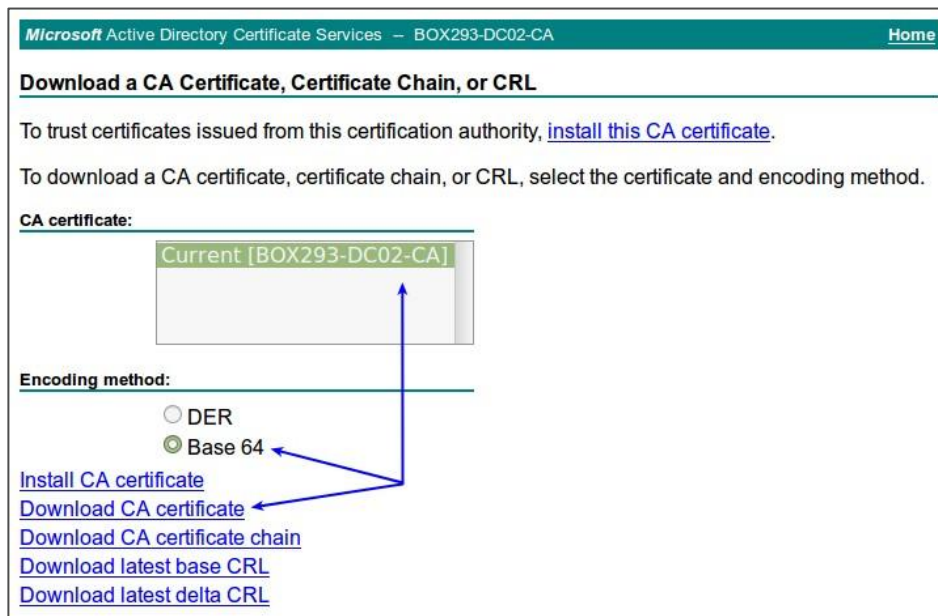
1. Navigate to `http://<CA_Server_Name>/certsrv` and provide valid credentials when prompted. Replace `<CA_Server_Name>` with the address of your CA server. You will be presented with a page like the screenshot below.
2. Click the **Download a CA certificate, certificate chain, or CRL link**.



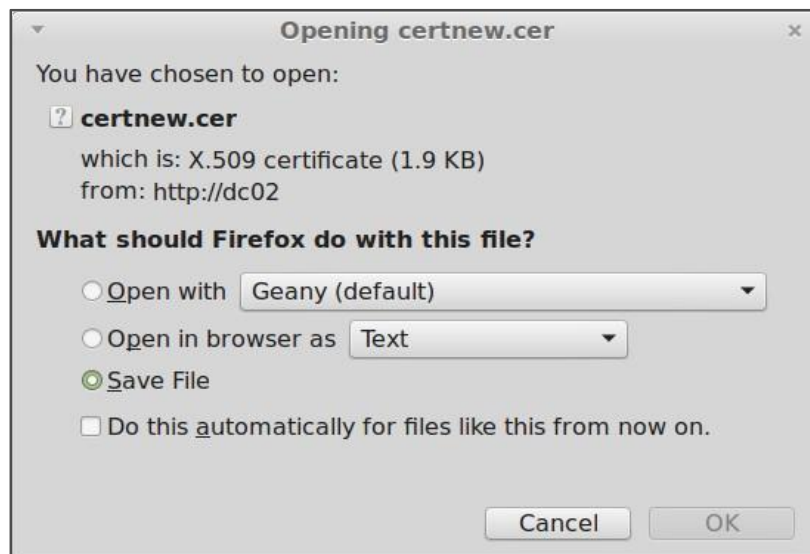
3. Select the **CA certificate** from the list of available certificates.

How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

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.



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 Log Server from.

How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

Obtaining the Certificate - LDAP Server

There are many implementations of LDAP servers, so it is hard to clearly document exactly where your CA certificate file exists.

Note: For Debian/Ubuntu systems, you will need to replace the `/etc/openssl/` directory in the following examples with `/etc/ldap/`

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/openssl/certs/ca_box293_cert.pem
```

You can see in the output the location of the CA certificate file. 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:

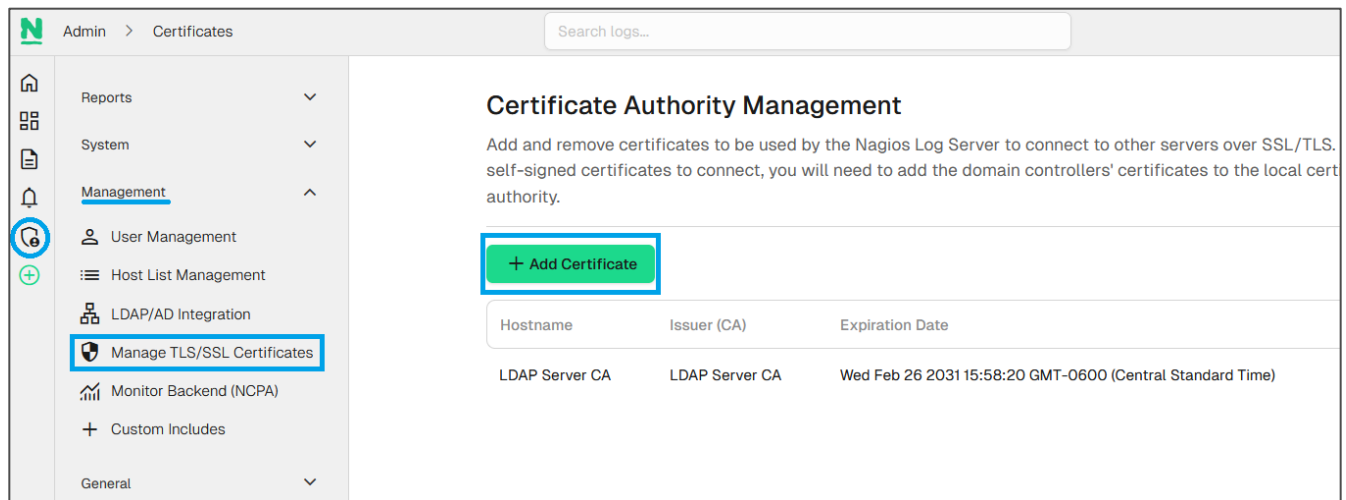
```
cat /etc/openssl/certs/ca_box293_cert.pem
```

You can now proceed to the [Upload Certificate](#) section of this document.

How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

Upload Certificate

7. In your browser, navigate to Nagios Log Server and log in with a user account with Administrator privileges.
8. Go to **Admin > Management > Manage TLS/SSL Certificates**, and click **+Add Certificate**.



(Note that if you are on a Log Server version prior to 2026R2, the certificate will be added in the **LDAP/AD Integration** menu, rather than in the **Manage TLS/SSL Certificates** menu).

9. Open the certificate you obtained in the last step with a text editor like Notepad. Copy and paste the certificate text into the **Add SSL / TLS Certificate** window, including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines.

The screenshot shows the 'Add SSL/TLS Certificate' dialog box. It has a text input field for the hostname, which contains 'openldap.nagios.com'. Below it is a large text area containing a certificate. The certificate text is as follows: -----BEGIN CERTIFICATE-----
Og63hITB5e1QegC/
BRv8D5mZdloeSUa4NdeH4b5oyusqANmUTyzelwVcLpTukHBn
9iICPBv1jxj15AtFi75OWRUfE8wWGE4arQ5sFQ5AMJTU/MdJNLEilt+0snlp0oQ
pMV84itCQ8/
IEWM8SwIDAQABMAOGCSqGSIb3DQEBBQUAA4IBAQC8JG5ZJ4Garn/
2djp3nbvVhgV6rFsLuYOpW7pshSFBeUDxwkVJSFsRVq6LA/
p6OXsQ71bPcpwSNX
R9wMjt9bObXZWE9Hhwy5w2hUkyRV30AvD34GNcTALoR0hUODOB2X9h62qZP
TrNOc
Jfs1BDcpEHYwdIzkzWQzXuoJ23ImMo+P4+cPpML9ij+HfCOvOs1IVEFJmLs+DE7q
D9Bb1ydCyzyItOmwdMGbG7jIE8vGweNVnH/
cSb54JXWotpNS1G8ocWQ2XbW5dJdL
INHwUtjyoPvsqyHPyJLKJShxGudFQZklqoLIAP4Bp1Q9jG4PWLWKhKHoenZs/SBG
at62JEVO
-----END CERTIFICATE-----
At the bottom of the dialog box, there are 'Submit' and 'Close' buttons.

How To Use TLS With AD And LDAP In Nagios Log Server 2026R2

Note: When done correctly, the Hostname field should fill itself out automatically using the information encoded in the certificate. This will also enable the **Submit** button.

10. Click **Submit** to finish uploading the certificate.

Repeat On All Nagios Log Server Instances

You will now need to repeat the above steps on all Nagios Log Server instances that participate in this cluster, so the CA certificate is available on every instance.

Configure Authentication Server

This guide does not explain how to add an Authentication Server to Nagios Log Server, 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 don't define which CA certificate is used. When Nagios Log Server is presented with a certificate from the LDAP / AD server, the Nagios Log Server checks its 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 and LDAP in Nagios Log Server 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](#)