How To Use SSL/TLS For AD And LDAP In Nagios Network Analyzer 2026

Purpose

This document describes how to use SSL/TLS with AD and LDAP in Nagios Network Analyzer 2026.

Prerequisites

You will need the following prerequisites in order to follow the documentation:

- Nagios Network Analyzer 2026R1 or newer
- A separate Microsoft Windows-based AD infrastructure that is accessible to the Nagios Network Analyzer machine
    - OR
- A separate LDAP infrastructure (like OpenLDAP) that is accessible to the Nagios Network Analyzer machine

Certificate Overview

A "brief" explanation of certificates is required to be able to explain which certificate needs to be uploaded to your Nagios Network Analyzer 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 actually 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) 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.

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Why did all of that need explaining? When Nagios Network Analyzer connects to an LDAP/AD server to authenticate a user, the domain controller you are authenticating with provides the Nagios Network Analyzer server with a certificate to use for encryption and security. Because Nagios Network Analyzer 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 Network Analyzer so that Nagios Network Analyzer 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 domain controllers; 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 Network Analyzer. This documentation will walk you through the steps to obtain and 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

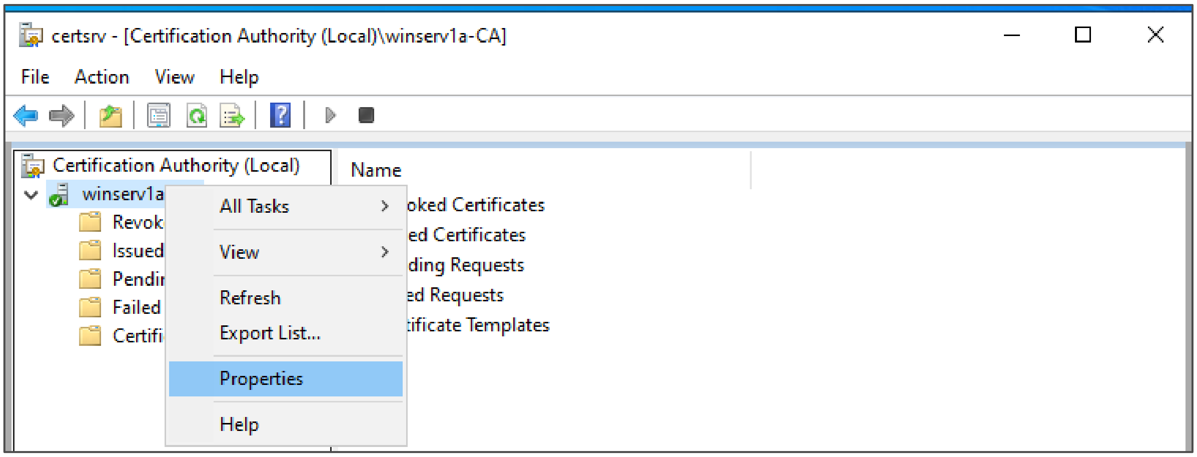
Method 1: Console / RDP Session To CA Server

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

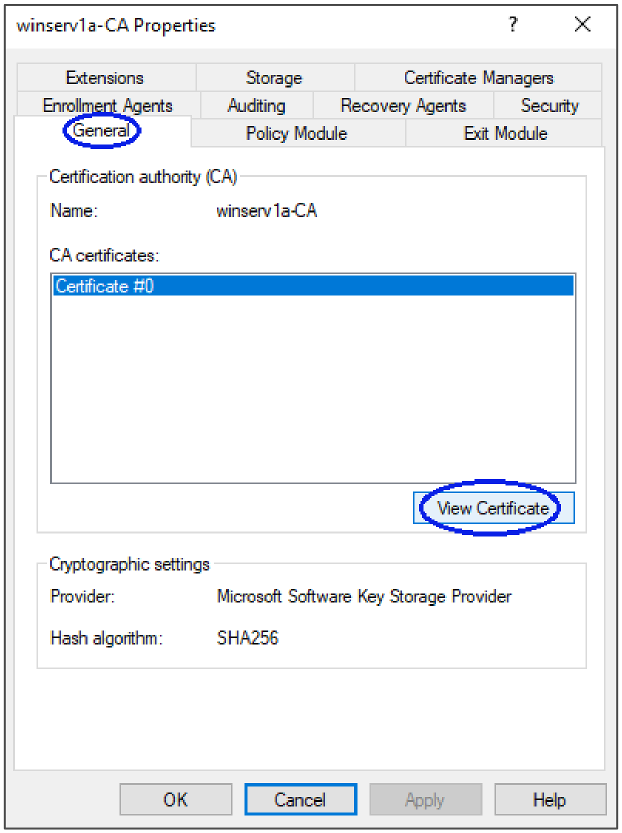
1. Navigate to **Administrative Tools** (commonly found in the Control Panel) and open **Certification Authority**.

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

2. When the **Certification Authority** opens, right click on the CA server and select **Properties**.



3. The **Properties** window will open to the **General** tab.
4. Click the **View Certificate** button.



Name: winserv1a-CA

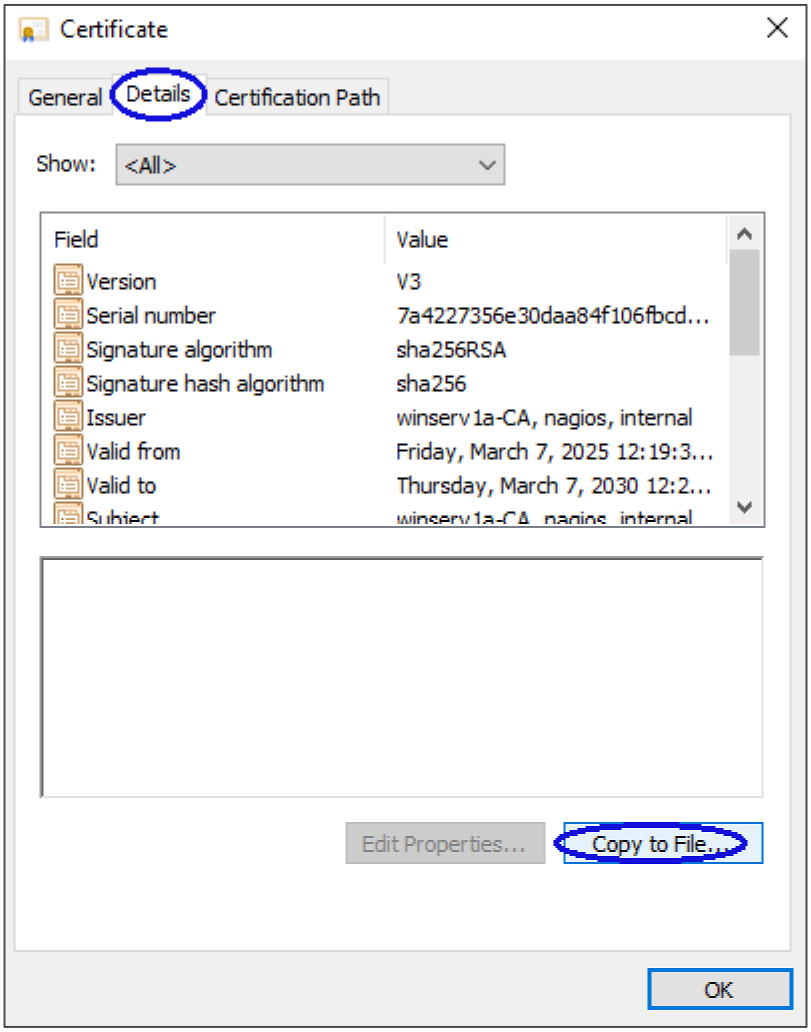
Certificate #0

Provider: Microsoft Software Key Storage Provider

Hash algorithm: SHA256

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

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



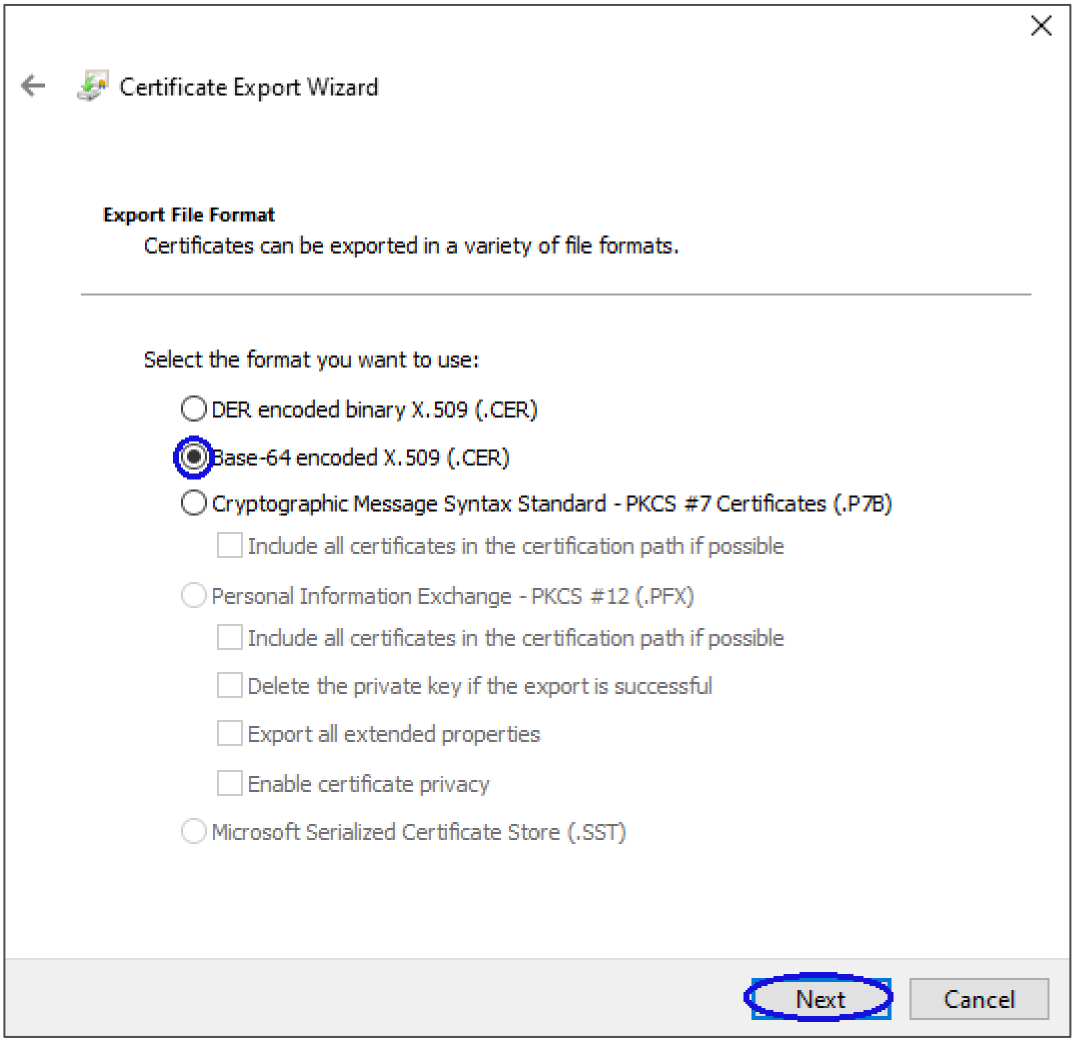
Certificate

Show: <All>

Field	Value
Version	V3
Serial number	7a4227356e30daa84f106fbcd...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	winserv1a-CA, nagios, internal
Valid from	Friday, March 7, 2025 12:19:3...
Valid to	Thursday, March 7, 2030 12:2...
Subject	winserv1a-CA, nagios, internal

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

7. When the **Certificate Export Wizard** window opens, click **Next**.
8. Select **Base-64 encoded X.509 (.CER)** and then click **Next**.



Certificate Export Wizard

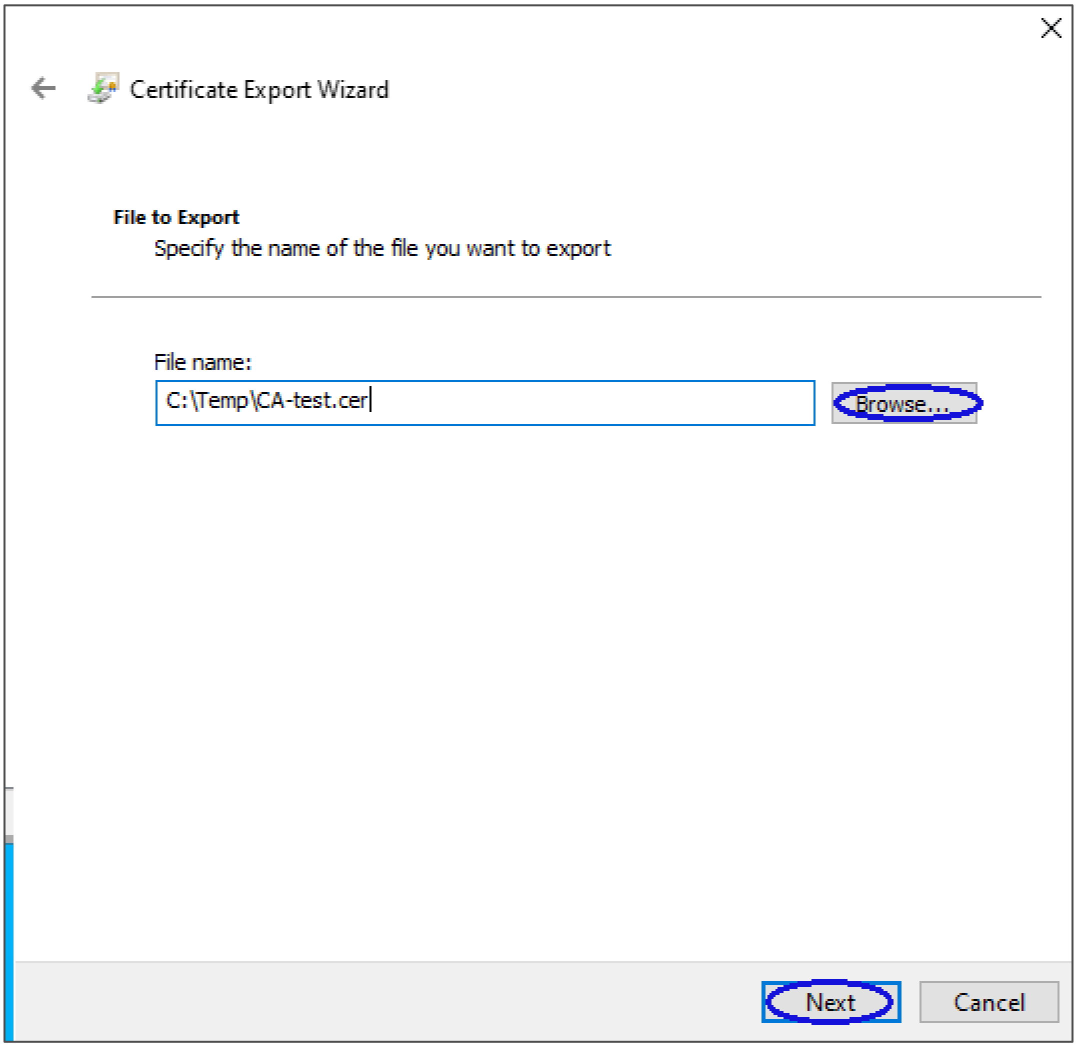
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
□ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

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.



Certificate Export Wizard

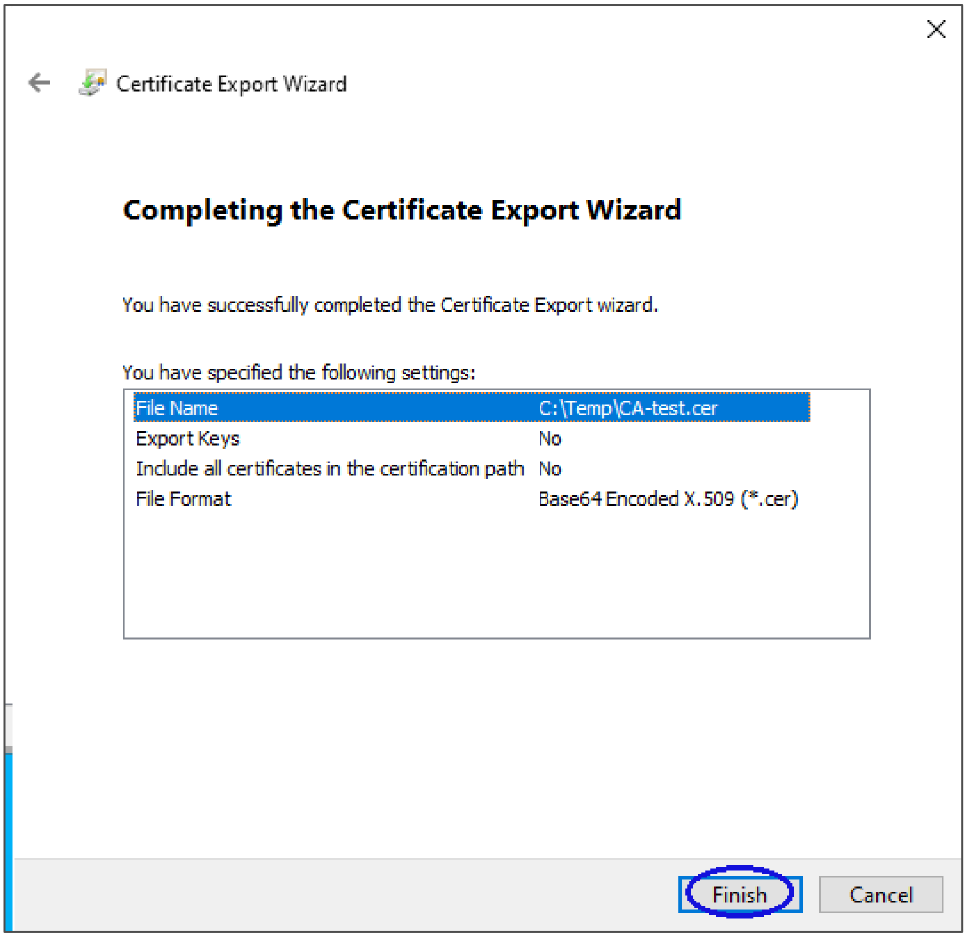
File to Export

Specify the name of the file you want to export

File name: C:\Temp\CA-test.cer

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

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



Certificate Export Wizard

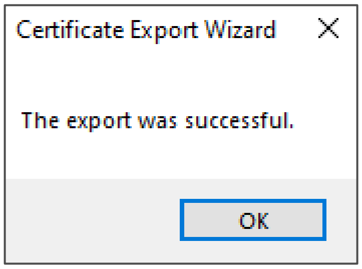
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Temp\CA-test.cer
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

12. You will receive a message to confirm the certificate export was a success. Click **OK**. Close all of the open windows and proceed to the [Upload Certificate]() section of this document. Make sure you have access to the exported `.cer` file on the computer you will use to upload the certificate to Nagios Network Analyzer.



Certificate Export Wizard

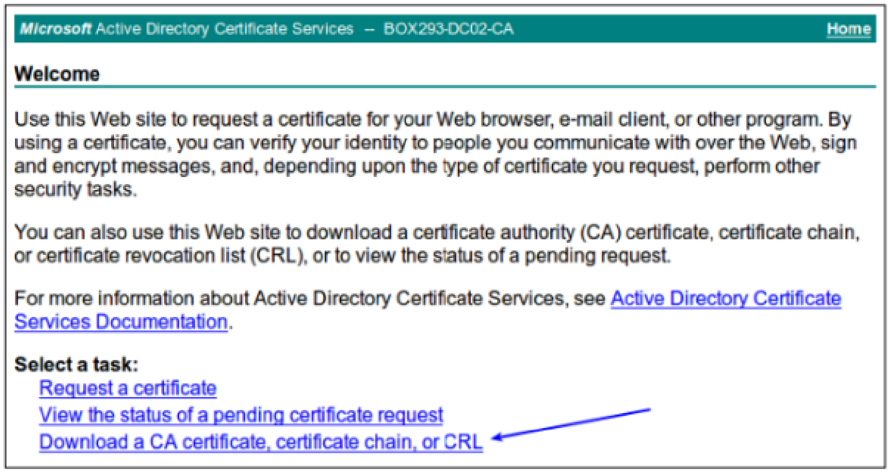
The export was successful.

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

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.



Microsoft Active Directory Certificate Services – BOX293-DC02-CA

Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

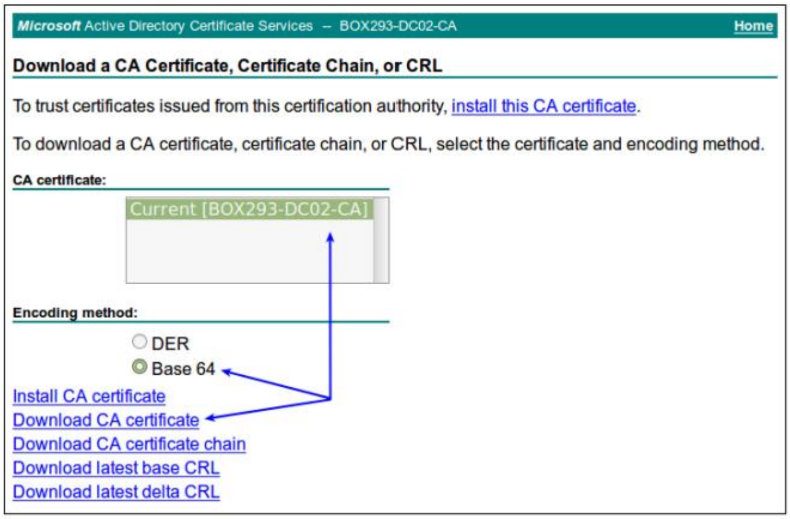
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

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.



Microsoft Active Directory Certificate Services – BOX293-DC02-CA

Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [BOX293-DC02-CA]

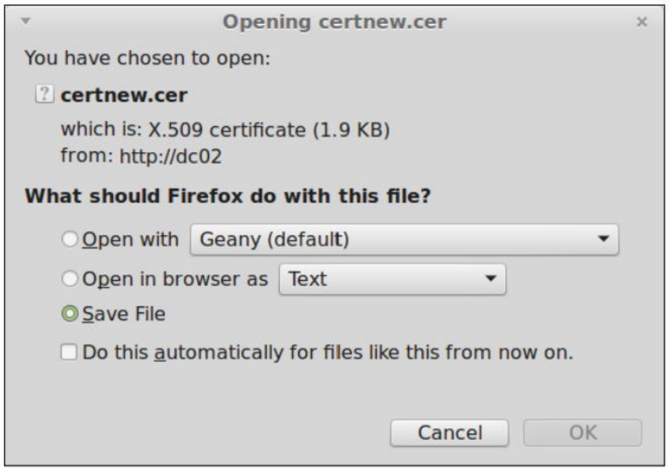
Encoding method:

○ DER
● Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

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.



Opening certnew.cer

You have chosen to open:

certnew.cer

which is: X.509 certificate (1.9 KB)
from: http://dc02

What should Firefox do with this file?

○ Open with Geany (default)
○ Open in browser as Text
● Save File
□ Do this automatically for files like this from now on.

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

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_contoso2_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_contoso2_cert.pem
```

Proceed to the Upload Certificate section of this document.

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Upload Certificate

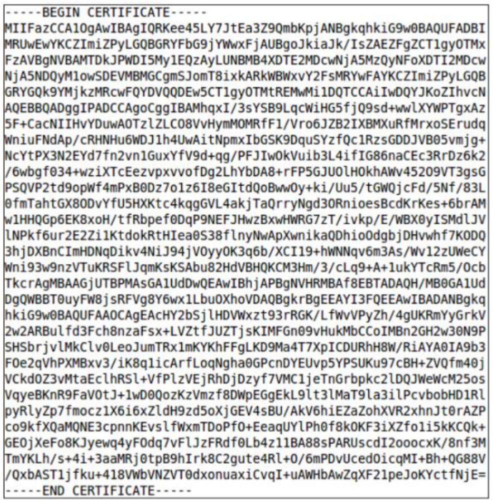
In this step you will upload the CA certificate to the Nagios Network Analyzer server.

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

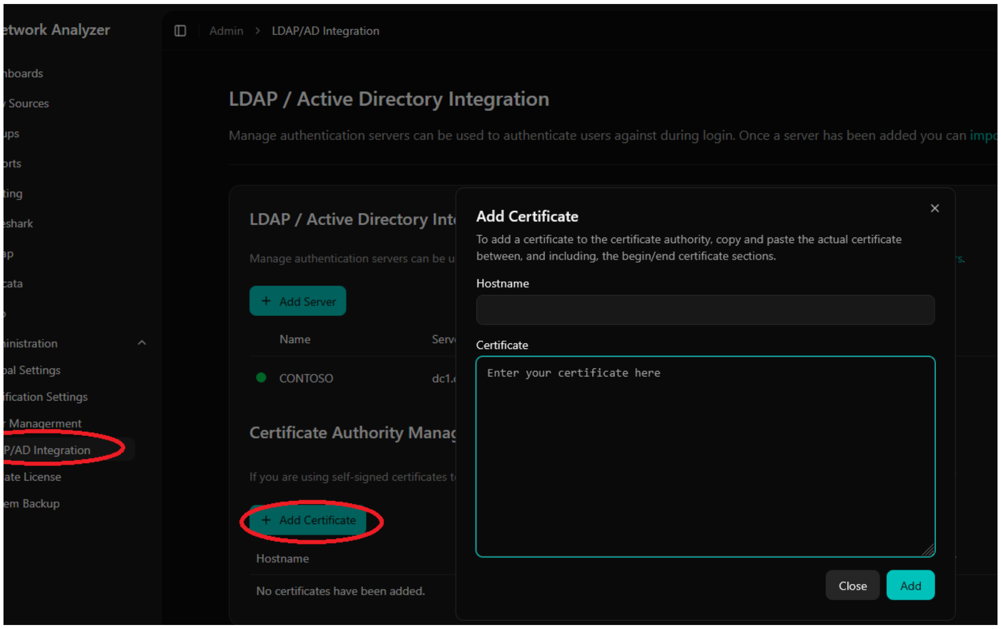
   `-----BEGIN CERTIFICATE-----` and

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



```
-----BEGIN CERTIFICATE-----
MIIFazCCA1OgAwIBAgIQRKee45LY7JtEa3Z9QmbKpjANBgkqhkiG9w0BAQUFADBI
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFjAUBgoJkiaJk/IsZAEZFgZCT1gyOTMx
FzAVBgNVBAMTDkJPWDI5My1EQzAyLUNBMB4XDTE2MDcwNjA5MzQyNFoXDTI2MDcw
NjA5NDQyM1owSDEVMBMGCgmSJomT8ixkARkWBWxvY2FsMRYwFAYKCZImiZPyLGQB
GRYGQk9YMjkzMRcwFQYDVQQDEw5CT1gyOTMtREMwMi1DQTCCAiIwDQYJKoZIhvcN
AQEBBQADggIPADCCAgoCggIBAMhqxI/3sYSB9LqcWiHG5fjQ9sd+wwlXYWPTgxAz
5F+CacNIIHvYDuwAOTzlZLCO8VvHymMOMRfF1/Vro6JZB2IXBMXuRfMrxoSErudq
WniuFNdAp/cRHNHu6WDJ1h4UwAitNpmxIbGSK9DquSYzfQc1RzsGDDJVB05vmjg+
NcYtPX3N2EYd7fn2vn1GuxYfV9d+qg/PFJIwOkVuib3L4ifIG86naCEc3RrDz6k2
/6wbgf034+wziXTcEezvpxvvofDg2LhYbDA8+rFP5GJUOlHOkhAWv452O9VT3gsG
PSQVP2td9opWf4mPxB0Dz7o1z6I8eGItdQoBwwOy+ki/Uu5/tGWQjcFd/5Nf/83L
0fmTahtGX8ODvYfU5HXKtc4kqgGVL4akjTaQrryNgd3ORnioesBcdKrKes+6brAM
w1HHQGp6EK8xoH/tfRbpef0DqP9NEFJHwzBxwHWRG7zT/ivkp/E/WBX0yISMdlJV
lNPkf6ur2E2Zi1KtdokRtHIea0S38flnyNwApXwnikaQDhioOdgbjDHvwhf7KODQ
3hjDXBnCImHDNqDikv4NiJ94jVOyyOK3q6b/XCI19+hWNNqv6m3As/Wv12zUWeCY
Wni93w9nzVTuKRSFlJqmKsKSAbu82HdVBHQKCM3Hm/3/cLq9+A+1ukYTcRm5/Ocb
TkcrAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1Ud
DgQWBBT0uyFW8jsRFVg8Y6wx1LbuOXhoVDAQBgkrBgEEAYI3FQEEAwIBADANBgkq
hkiG9w0BAQUFAAOCAgEAcHY2bSjlHDVWxzt93rRGK/LfWvVPyZh/4gUKRmYyGrkV
2w2ARBulfd3Fch8nzaFsx+LVZtfJUZTjsKIMFGn09vHukMbCCoIMBn2GH2w30N9P
SHSbrjvlMkClv0LeoJumTRx1mKYKhFFgLKD9Ma4T7XpICDURhH8W/RiAYA0IA9b3
FOe2qVhPXMBxv3/iK8q1icArfLoqNgha0GPcnDYEUvp5YPSUKu97cBH+ZVQfm40j
VCkdOZ3vMtaEclhRSl+VfPlzVEjRhDjDzyf7VMC1jeTnGrbpkc2lDQJWeWcM25os
VqyeBKnR9FaVOtJ+1wD0QozKzVmzf8DWpEGgEkL9lt3lMaT9la3ilPcvbobHD1Rl
pyRlyZp7fmocz1X6i6xZldH9zd5oXjGEV4sBU/AkV6hiEZaZohXVR2xhnJt0rAZP
co9kfXQaMQNE3cpnnKEvslfWxmTDoPfO+EeaqUYlPh0f8kOKF3iXZfo1i5kKCQk+
GEOjXeFo8KJyewq4yFOdq7vFlJzFRdf0Lb4z11BA88sPARUscdI2ooocxK/8nf3M
TmYKLh/s+4i+3aaMRj0tpB9hIrk8C2gute4Rl+O/6mPDvUcedOicqMI+Bh+QG88V
/QxbAST1jfku+418VWbVNZVT0dxonuaxiCvqI+uAWHbAwZqXF21peJoKYctfNjE=
-----END CERTIFICATE-----
```

3. Open Nagios Network Analyzer and navigate to **Administration > LDAP/AD Integration**.
4. Click the **Add Certificate** button.
5. The **Add Certificate** window will appear.



LDAP / Active Directory Integration

Manage authentication servers can be used to authenticate users against during login. Once a server has been added you can imp

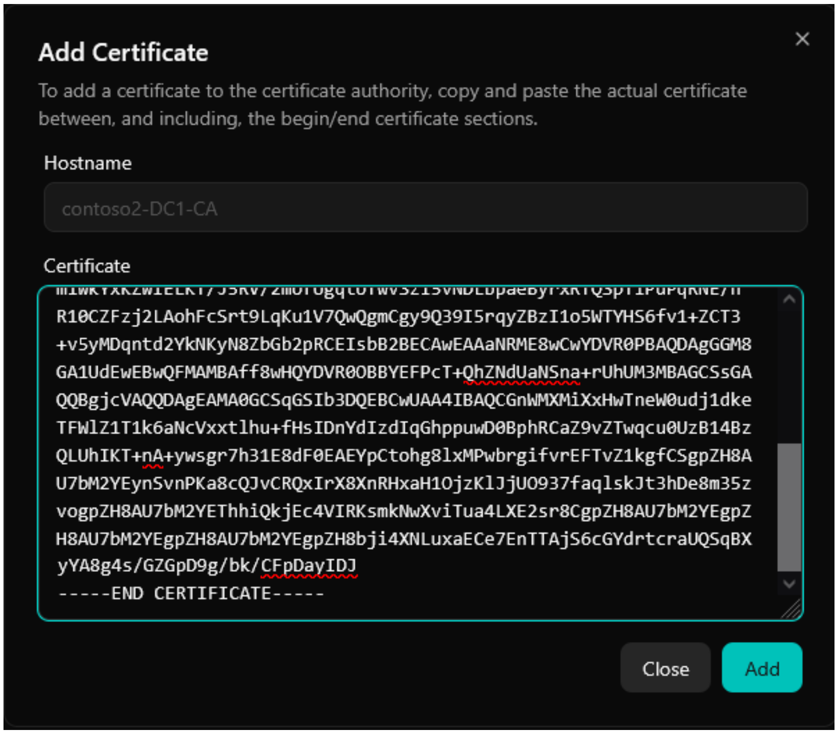
LDAP / Active Directory Int
Manage authentication servers can be u
+ Add Server
Name
Serv
CONTOSO
dc1.
Certificate Authority Manag
If you are using self-signed certificates t
+ Add Certificate
Hostname
No certificates have been added.

Add Certificate

To add a certificate to the certificate authority, copy and paste the actual certificate between, and including, the begin/end certificate sections.

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

6. Paste the text from 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** button to finish uploading this certificate to Nagios Network Analyzer.



Add Certificate

To add a certificate to the certificate authority, copy and paste the actual certificate between, and including, the begin/end certificate sections.

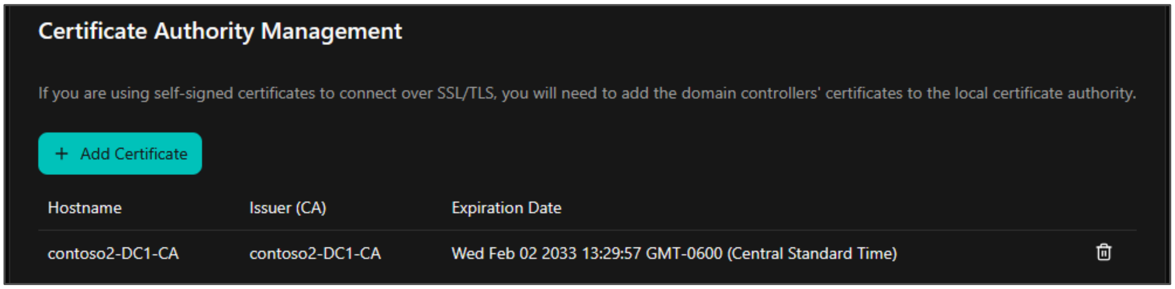
Hostname

contoso2-DC1-CA

Certificate

```
mIwkYXkZwIELKT/J5Kv/ZmUTUgqtUTWV3Z15VNDLDpaeByfXKTQ5pT1PuPqKNE/n
R10CZFzj2LAohFcSrt9LqKu1V7QwQgmCgy9Q39I5rqyZBzI1o5WTYHS6fv1+ZCT3
+v5yMDqntd2YkNKyN8ZbGb2pRCEIsbB2BECAwEAAaNRME8wCwYDVR0PBAQDAgGGM8
GA1UdEwEBwQFMAMBAff8wHQYDVR0OBBYEFPcT+QhZNdUaNSna+rUhUM3MBAGCSsGA
QQBgjcVAQQDAgEAMA0GCSqGSIb3DQEBCwUAA4IBAQCGnWMXMiXxHwTneW0udj1dke
TFWlZ1T1k6aNcVxxtlhu+fHsIDnYdIzdIqGhppuwD0BphRCaZ9vZTwqcu0UzB14Bz
QLUhIKT+nA+ywsgr7h31E8dF0EAEYpCtohg8lxMPwbrgifvrEFTvZ1kgfCSgpZH8A
U7bM2YEynSvnPKa8cQJvCRQxIrX8XnRHxaH1OjzKlJjUO937faqlskJt3hDe8m35z
vogpZH8AU7bM2YEThhiQkjEc4VIRKsmkNwXviTua4LXE2sr8CgpZH8AU7bM2YEgpZ
H8AU7bM2YEgpZH8AU7bM2YEgpZH8bji4XNLuxaECe7EnTTAjS6cGYdrtcraUQSqBX
yYA8g4s/GZGpD9g/bk/CFpDayIDJ
-----END CERTIFICATE-----
```

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



Certificate Authority Management

If you are using self-signed certificates to connect over SSL/TLS, you will need to add the domain controllers' certificates to the local certificate authority.

Hostname	Issuer (CA)	Expiration Date	
contoso2-DC1-CA	contoso2-DC1-CA	Wed Feb 02 2033 13:29:57 GMT-0600 (Central Standard Time)	🗑

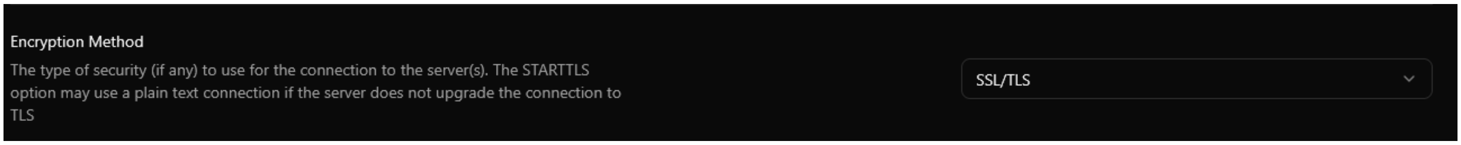
This completes uploading the certificate to Nagios Network Analyzer.

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Configure Authentication Server

This guide does not explain how to add an Authentication Server to Nagios Network Analyzer, 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.



Encryption Method

The type of security (if any) to use for the connection to the server(s). The STARTTLS option may use a plain text connection if the server does not upgrade the connection to TLS

SSL/TLS

You do not actually define which CA certificate is used. When Nagios Network Analyzer is presented with a certificate from the LDAP/AD server, the Nagios Network Analyzer 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 AD and LDAP in Nagios Network Analyzer. 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

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.