How To Use SSL/TLS with AD/LDAP in Nagios XI 2024

Purpose

This document describes how to install the required certificate on Nagios XI for use with LDAP or Active Directory (AD) Integration in Nagios XI. This process is required if your LDAP / AD server has a self-signed certificate.

Prerequisites

You will need the following prerequisites to follow the documentation:

- A separate Microsoft Windows-based AD infrastructure that is accessible to the Nagios XI machine

  OR

- A separate LDAP infrastructure (like OpenLDAP) that is accessible to the Nagios XI machine

Certificate Overview

A "brief" explanation of certificates is required to be able to explain which certificate needs to be uploaded to your Nagios XI 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 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 exist on your local computer. Computers that participate in a Windows domain automatically have a copy of this CA certificate; it happens automatically.

When a Nagios XI server connects to an LDAP/AD server to authenticate a user, the domain controller you are authenticating with provides the Nagios XI server with a certificate to use for encryption and security. Nagios XI 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 XI so that Nagios XI 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 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 XI. The following documentation will walk you through the steps to obtain and then upload the CA certificate.

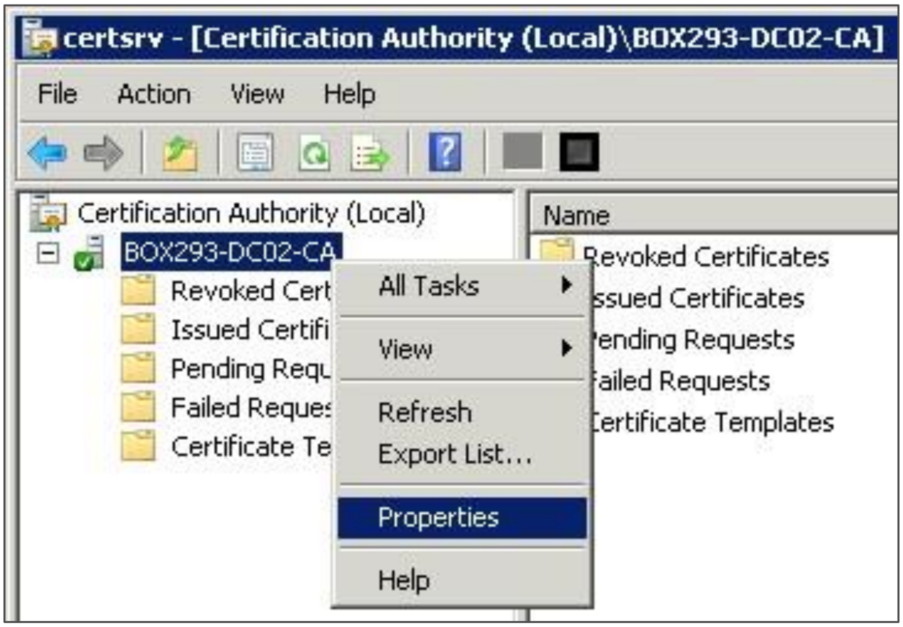
Obtaining The Certificate - Microsoft Windows

These steps are based on obtaining the CA certificate from your Microsoft Windows CA server. Two methods are explained in this document.

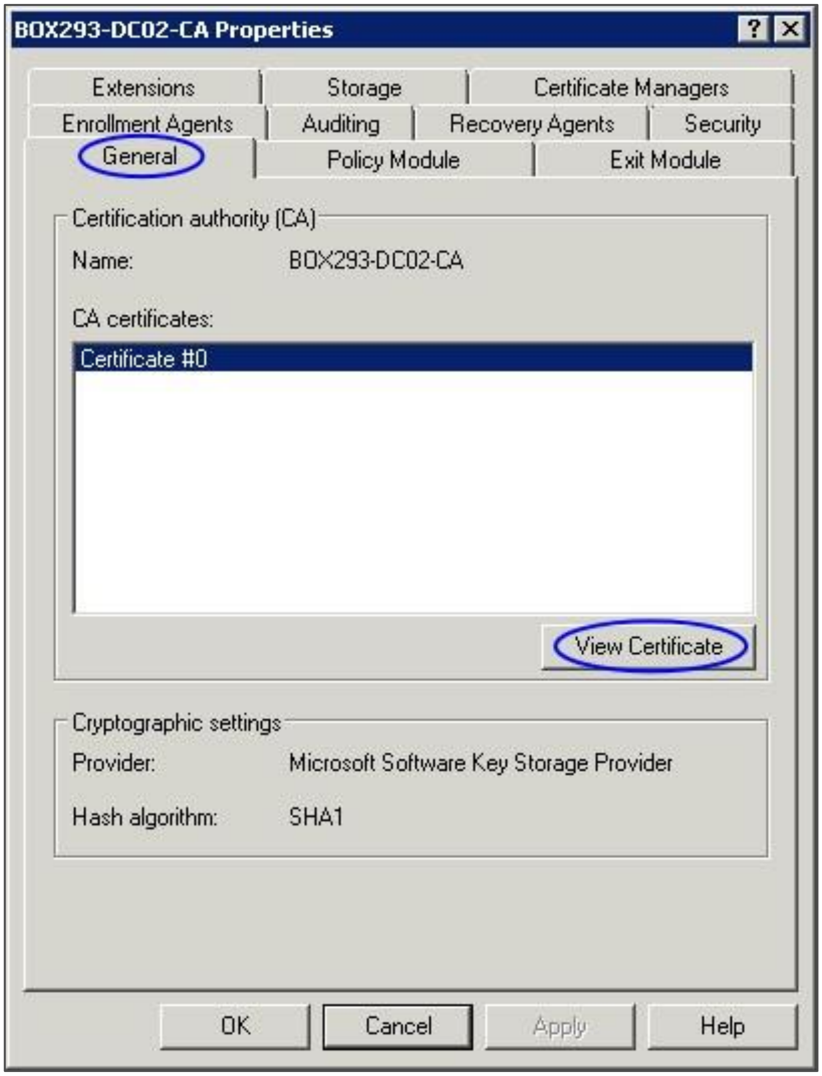
Method 1) Console/RDP Session to CA Server

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.



BOX293-DC02-CA Properties

Certification authority (CA)

Name: BOX293-DC02-CA

CA certificates:

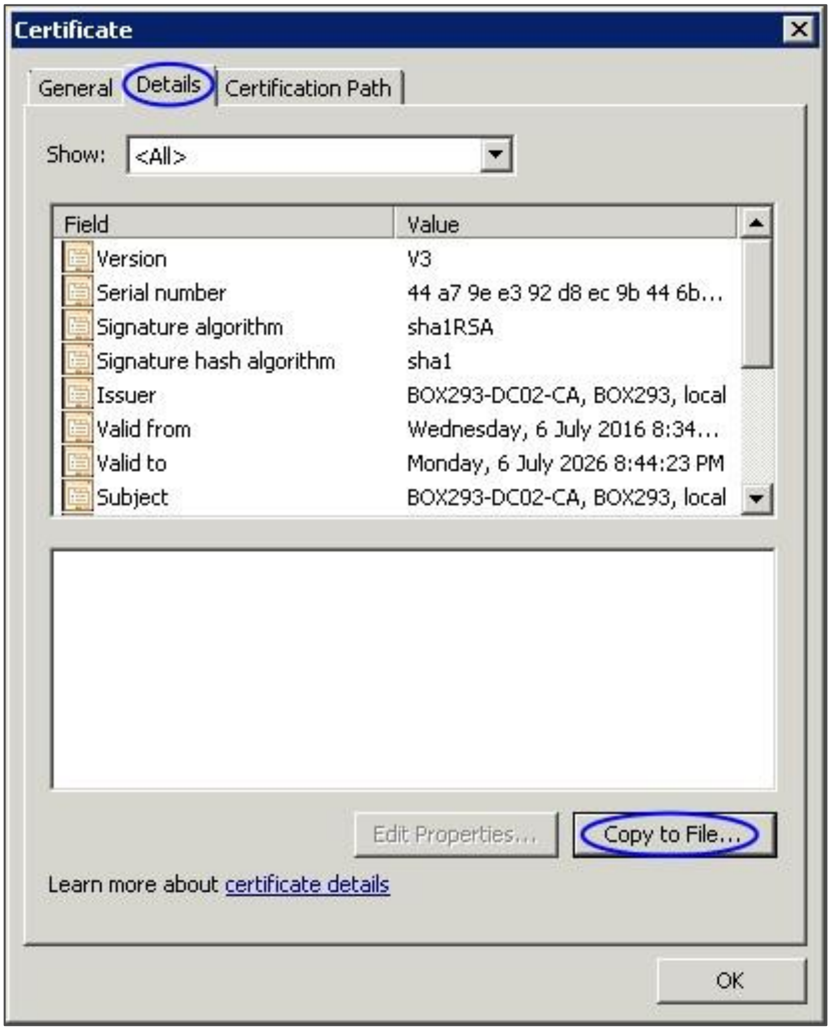
Certificate #0

Cryptographic settings

Provider: Microsoft Software Key Storage Provider

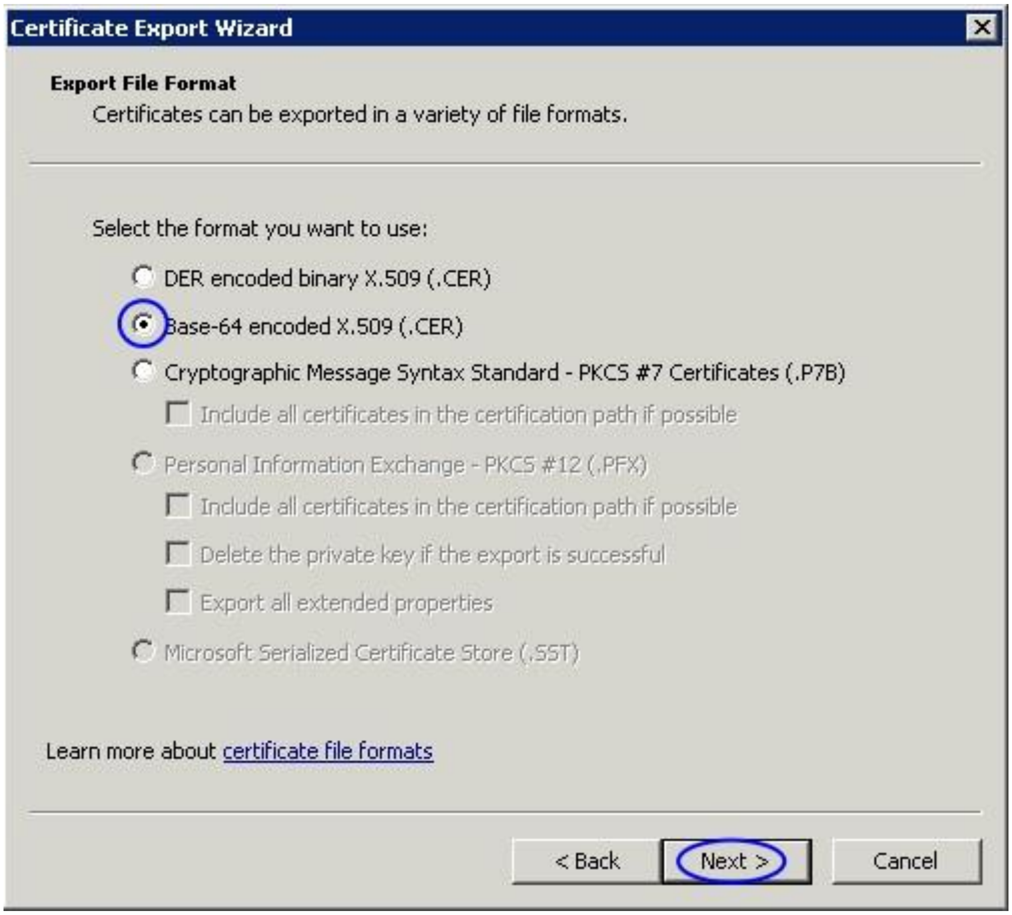
Hash algorithm: SHA1

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



Field	Value
Version	V3
Serial number	44 a7 9e e3 92 d8 ec 9b 44 6b...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	BOX293-DC02-CA, BOX293, local
Valid from	Wednesday, 6 July 2016 8:34...
Valid to	Monday, 6 July 2026 8:44:23 PM
Subject	BOX293-DC02-CA, BOX293, local

7. The Certificate Export Wizard window appears, 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

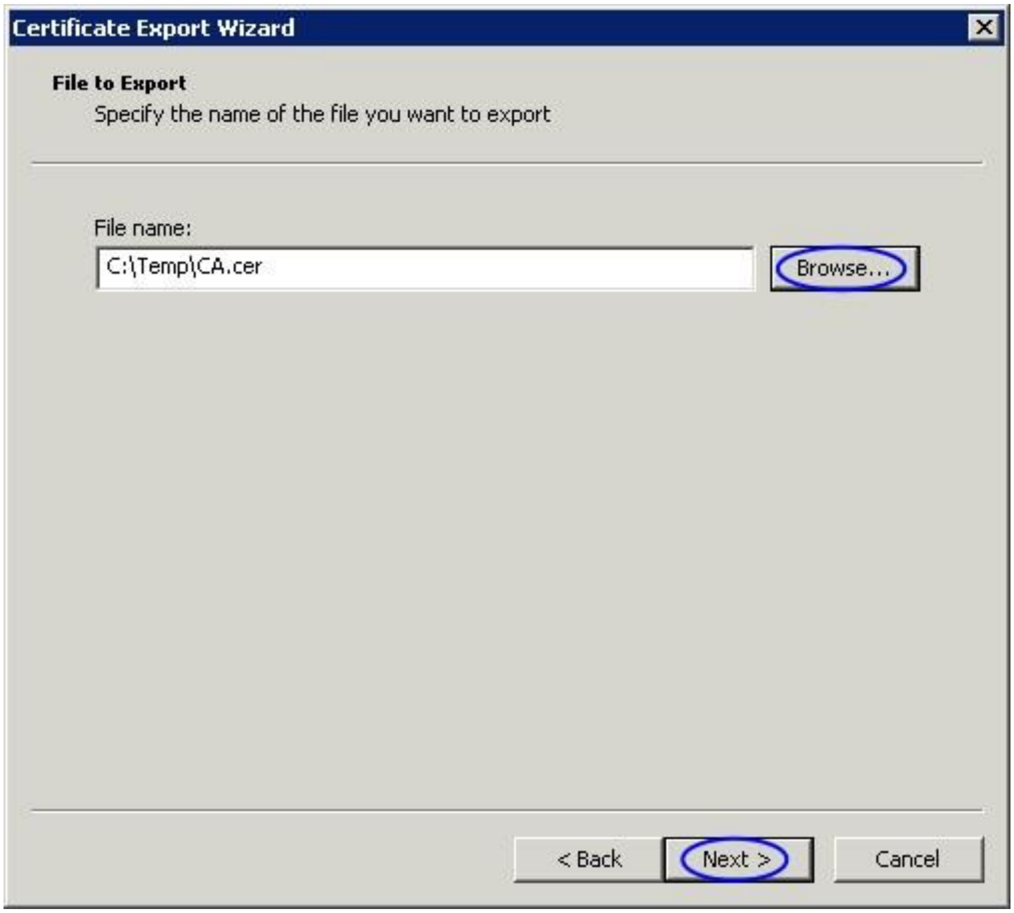
□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

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.



Certificate Export Wizard

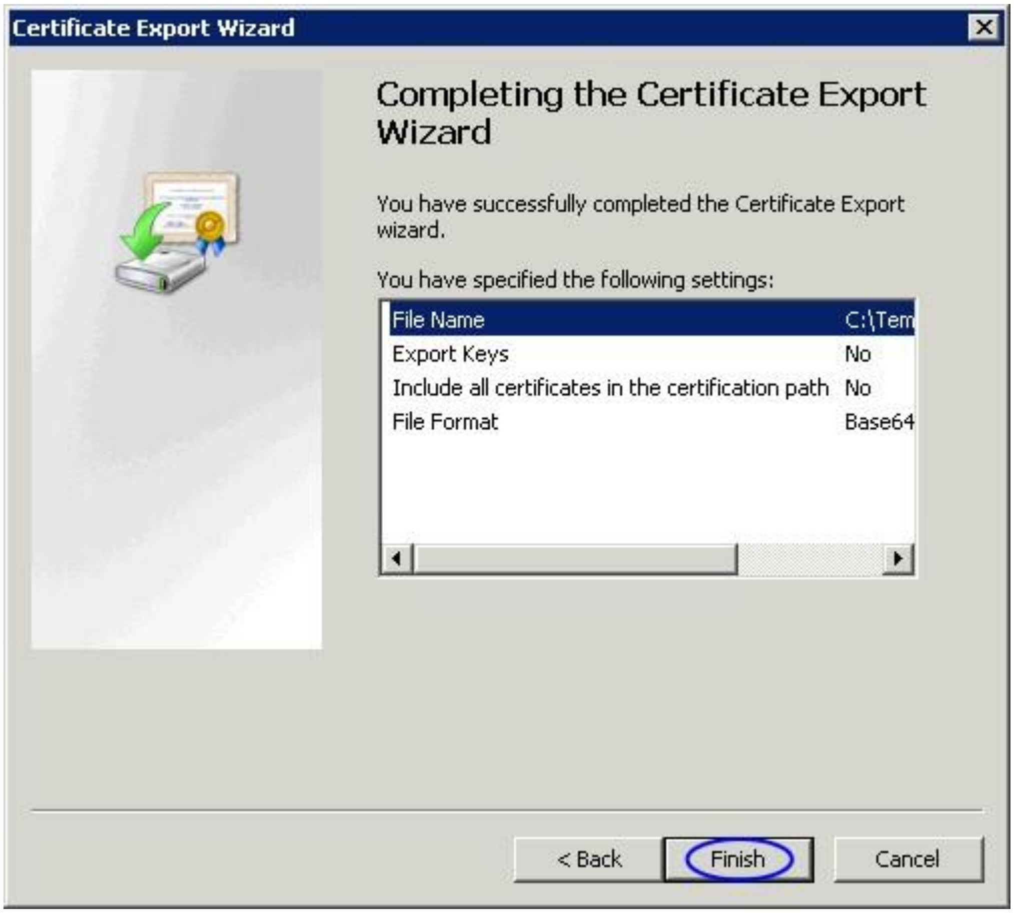
File to Export

Specify the name of the file you want to export

File name:

C:\Temp\CA.cer

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



Certificate Export Wizard

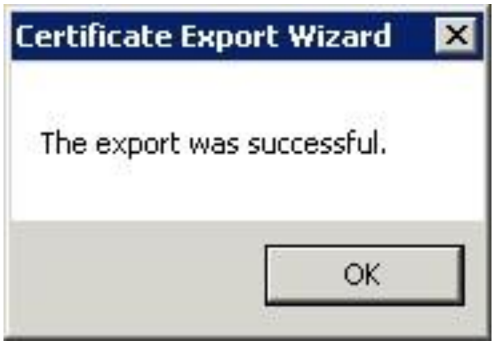
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Tem
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64

12. 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.



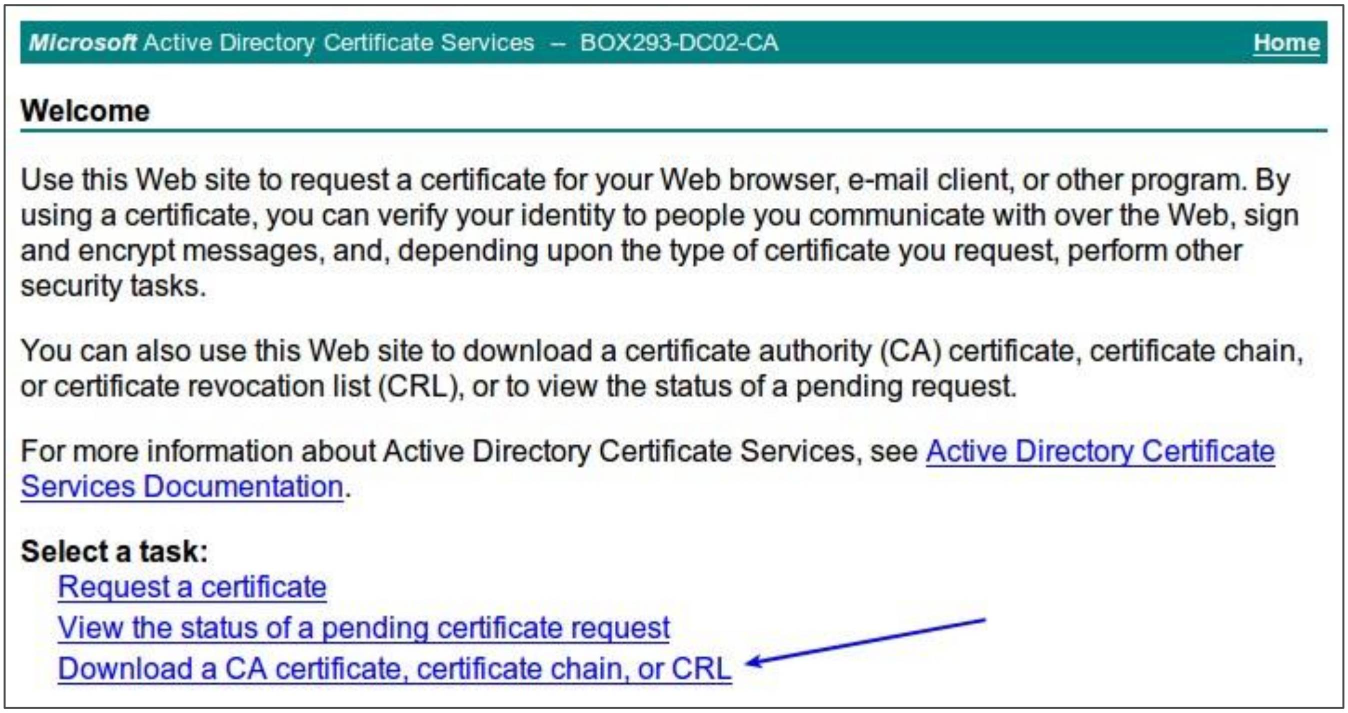
Certificate Export Wizard

The export was successful.

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



Microsoft Active Directory Certificate Services – BOX293-DC02-CA

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.

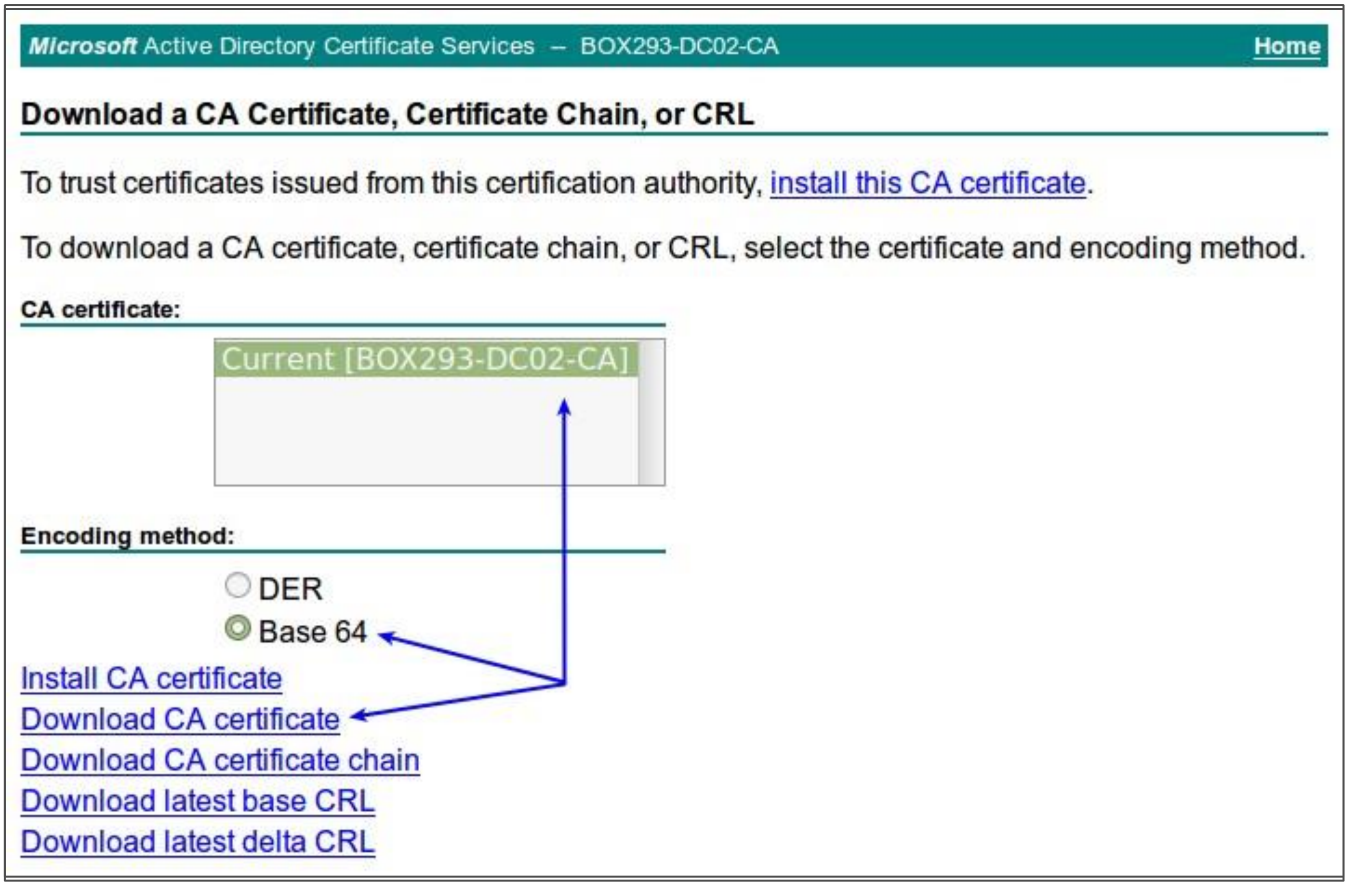
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

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

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:

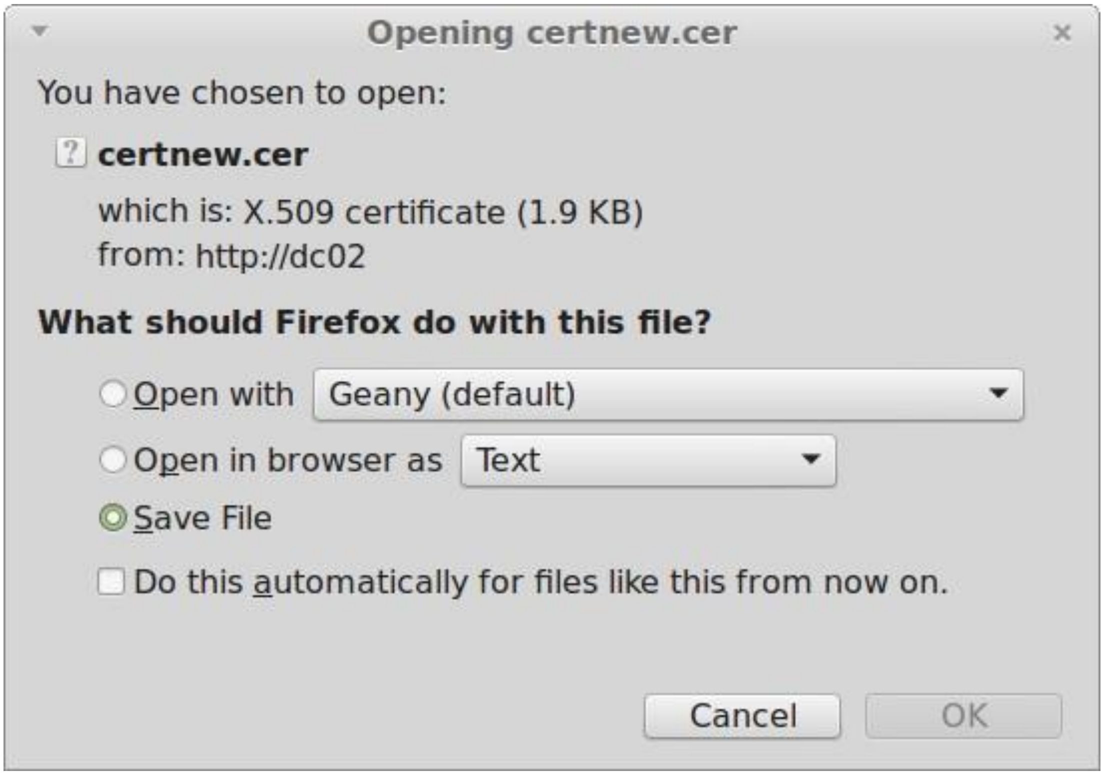
Current [BOX293-DC02-CA]

Encoding method:

○ DER
● Base 64

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

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.

7. 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.

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. 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 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:

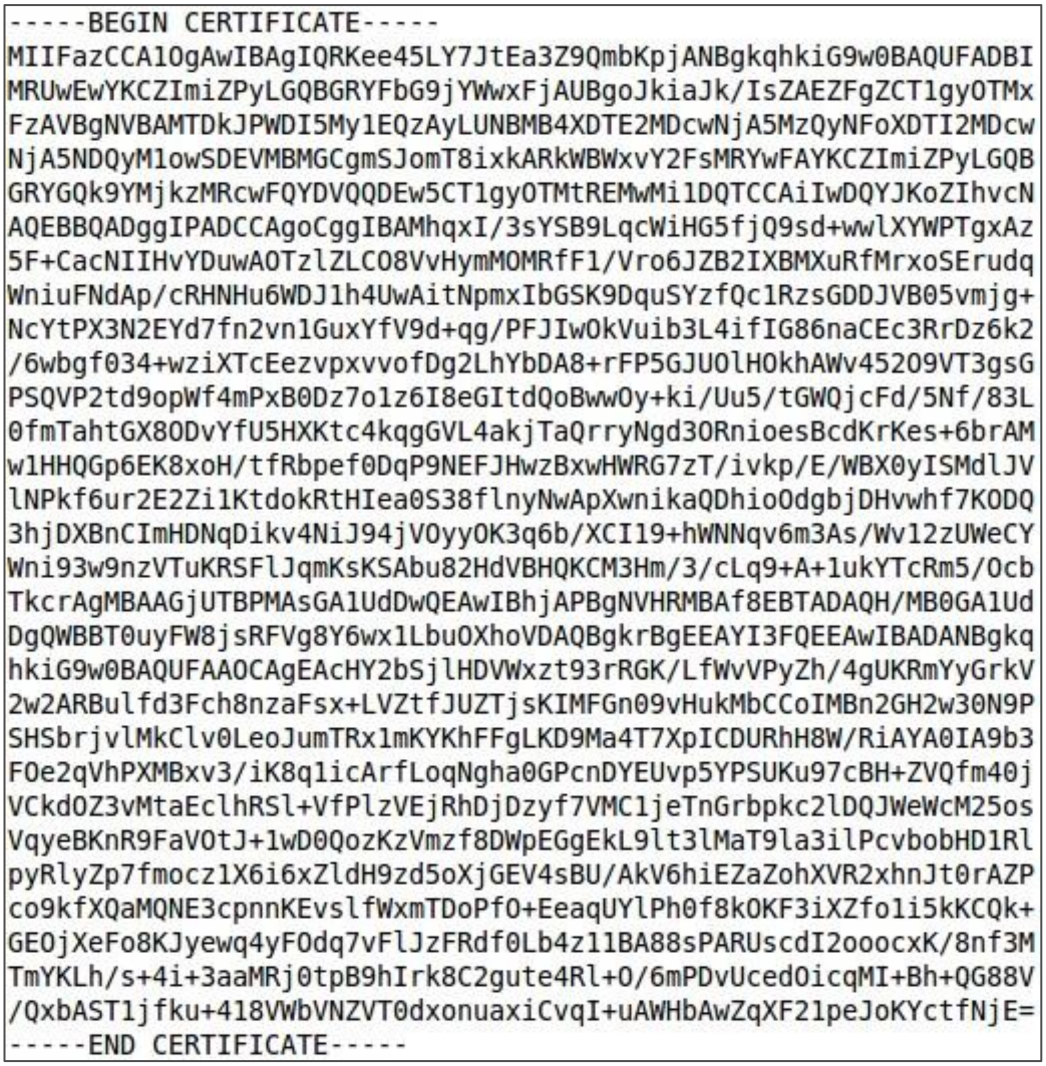
```
cat /etc/openldap/certs/ca_box293_cert.pem
```

You can now proceed to the Upload Certificate section of this document.

Upload Certificate

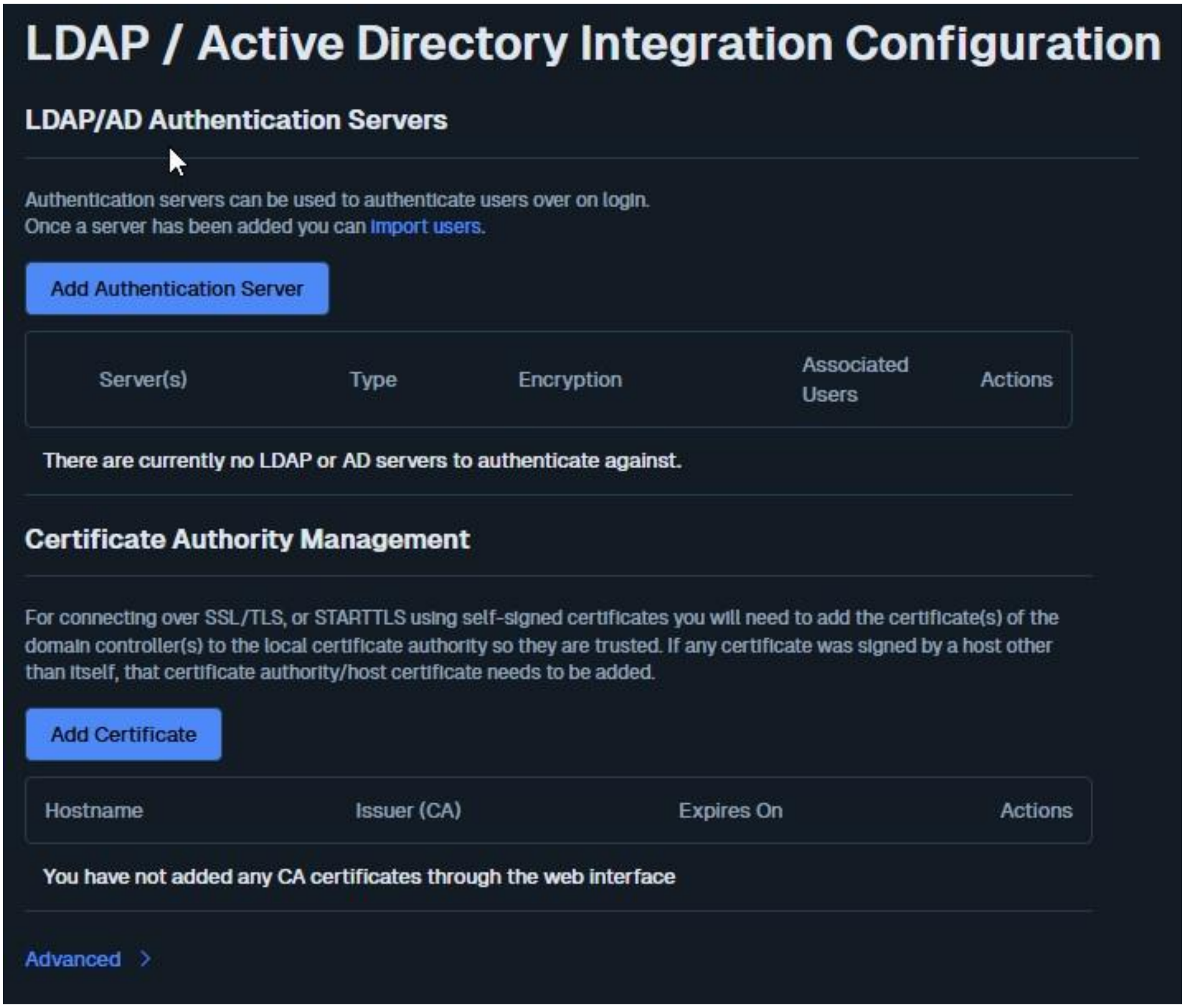
In this step you will upload the CA certificate to the Nagios XI server.

1. Open the certificate you exported in a text editor such as Notepad, it will appear something like the screenshot below.



```
-----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-----
```

2. Select all the text **(Ctrl + A**) and copy the text into your clipboard.
3. You will need to include the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE----` lines.



LDAP / Active Directory Integration Configuration

LDAP/AD Authentication Servers

Authentication servers can be used to authenticate users over on login.
Once a server has been added you can import users.

Server(s)	Type	Encryption	Associated Users	Actions

There are currently no LDAP or AD servers to authenticate against.

Certificate Authority Management

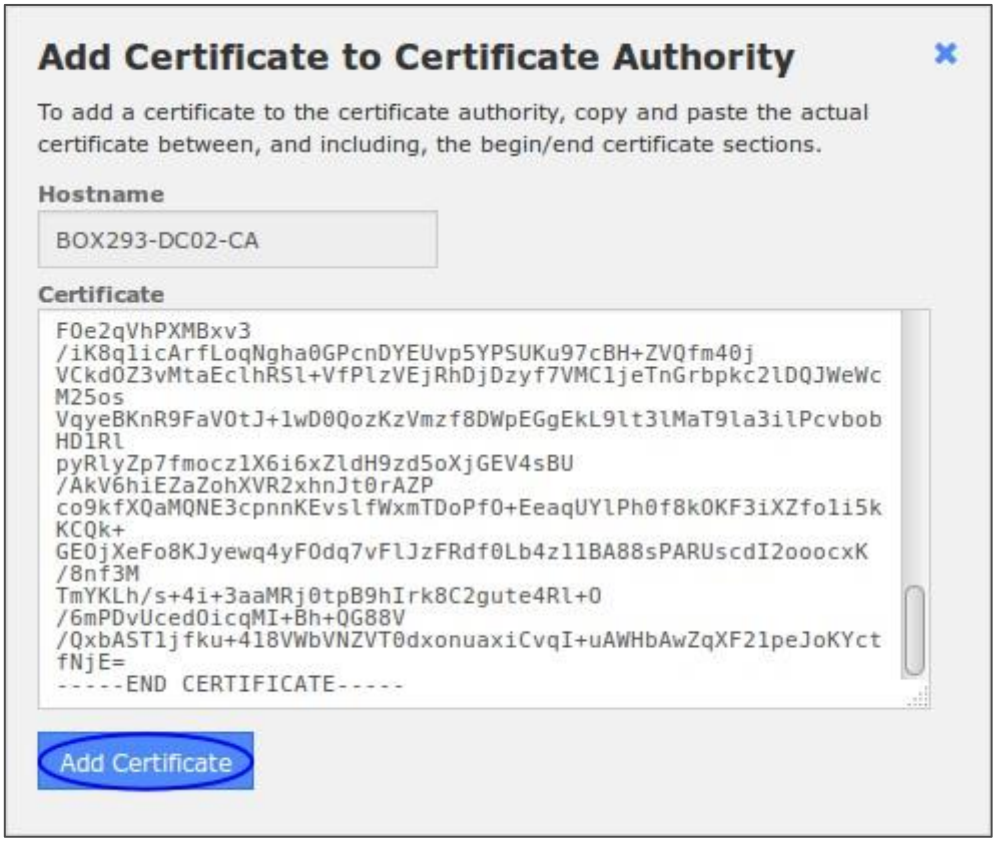
For connecting over SSL/TLS, or STARTTLS using self-signed certificates you will need to add the certificate(s) of the domain controller(s) to the local certificate authority so they are trusted. If any certificate was signed by a host other than itself, that certificate authority/host certificate needs to be added.

Hostname	Issuer (CA)	Expires On	Actions

You have not added any CA certificates through the web interface

4. Open Nagios XI and navigate to **Admin > Users > LDAP/AD** Integration.
5. Click the **Add Certificate** button and the **Add Certificate to Certificate Authority** window will appear.
6. Paste the text in your clipboard into the certificate field.

Note: The text copied from the text editor may not look the same once it is pasted into the certificate field.



Add Certificate to Certificate Authority

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

Hostname

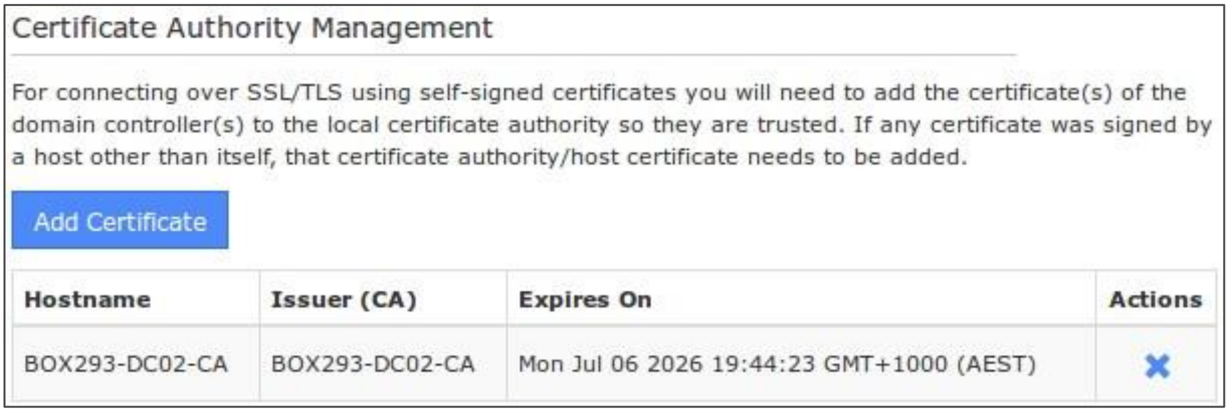
BOX293-DC02-CA

Certificate

```
FOe2qVhPXMBxv3
/iK8qlicArfLoqNgha0GPcnDYEUvp5YPSUKu97cBH+ZVQfm40j
VCkdOZ3vMtaEclhRSl+VfPlzVEjRhDjDzyf7VMC1jeTnGrbpkc2lDQJWeWc
M25os
VqyeBKnR9FaVOtJ+1wD0QozKzVmzf8DWpEGgEkL9lt3lMaT9la3ilPcvbob
HD1Rl
pyRlyZp7fmocz1X6i6xZldH9zd5oXjGEV4sBU
/AkV6hiEZaZohXVR2xhnJt0rAZP
co9kfXQaMQNE3cpnnKEvslfWxmTDoPfO+EeaqUYlPh0f8kOKF3iXZfoli5k
KCQk+
GEOjXeFo8KJyewq4yFOdq7vFlJzFRdf0Lb4z1lBA88sPARUscdI2ooocxK
/8nf3M
TmYKLh/s+4i+3aaMRj0tpB9hIrk8C2gute4Rl+O
/6mPDvUcedOicqMI+Bh+QG88V
/QxbAST1jfku+418VWbVNZVT0dxonuaxiCvqI+uAWHbAwZqXF21peJoKYct
fNjE=
-----END CERTIFICATE-----
```

7. Once you have pasted the text, the Hostname field will be automatically populated with the name of the CA.
8. Click the **Add Certificate** button to finish uploading this certificate to Nagios XI.

9. Once the certificate is uploaded it will appear under the list of certificates.



Certificate Authority Management

For connecting over SSL/TLS using self-signed certificates you will need to add the certificate(s) of the domain controller(s) to the local certificate authority so they are trusted. If any certificate was signed by a host other than itself, that certificate authority/host certificate needs to be added.

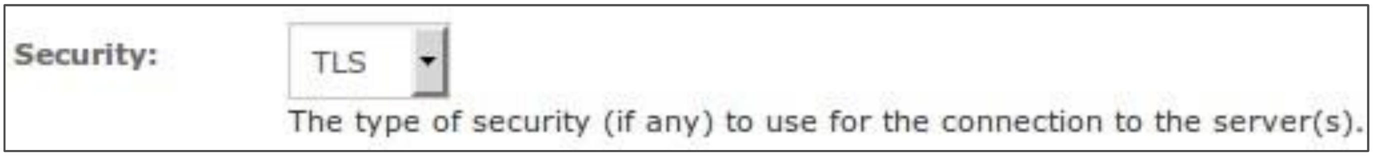
Hostname	Issuer (CA)	Expires On	Actions
BOX293-DC02-CA	BOX293-DC02-CA	Mon Jul 06 2026 19:44:23 GMT+1000 (AEST)	✖

This completes uploading the certificate to Nagios XI.

Configure Authentication Server

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



Security: TLS

The type of security (if any) to use for the connection to the server(s).

You do not actually define which CA certificate is used. When Nagios XI is presented with a certificate from the LDAP/AD server, the Nagios XI 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 how to use SSL/TLS Nagios XI and AD/LDAP. 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