

# Nagios XI – How to Use SSL with Active Directory / LDAP

## Purpose

This document describes how to use SSL with Active Directory / LDAP in Nagios XI 5.

**Note:** if you are using Nagios XI 2024, please refer to the [updated document](#).

## Prerequisites

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

- Nagios XI 5 or newer
- 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 to exist on your local computer. Computers that participate in a Windows domain automatically have a copy of this CA certificate as it happens automatically.

Why did all of that need explaining? When Nagios XI 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

# Nagios XI – How to Use SSL with Active Directory / LDAP

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. There are two methods explained here.

### Method 1) Console / RDP Session To CA Server

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

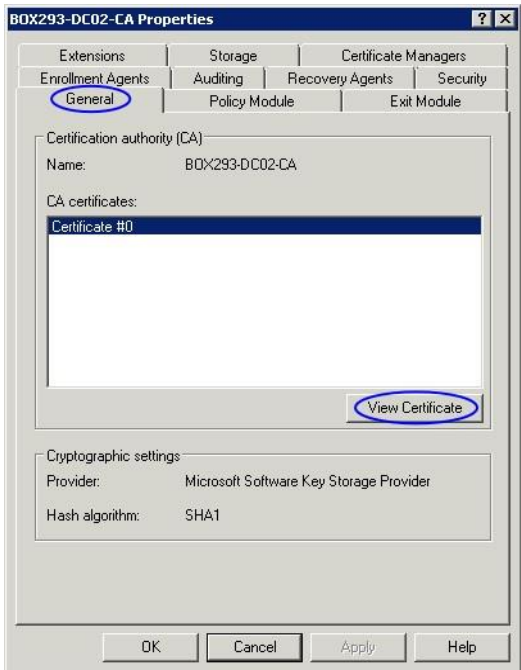
Navigate to **Administrative Tools** (commonly found in the control panel) and open **Certification Authority**.

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

When the **Properties** window appears, you will be on the **General** tab.



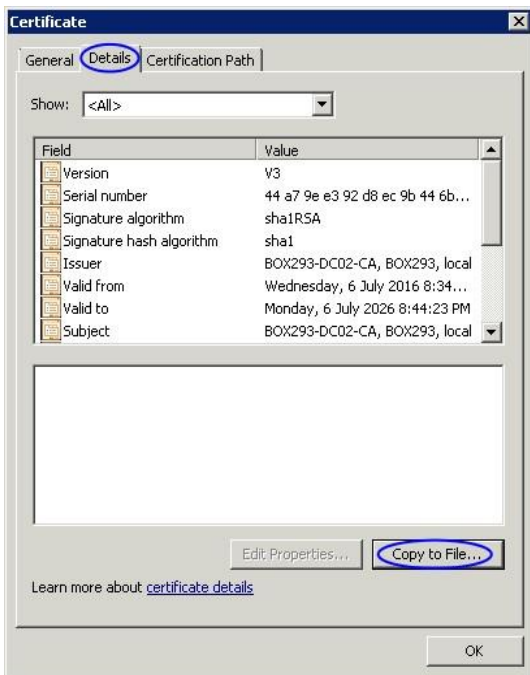
# Nagios XI – How to Use SSL with Active Directory / LDAP



Click the **View Certificate** button.

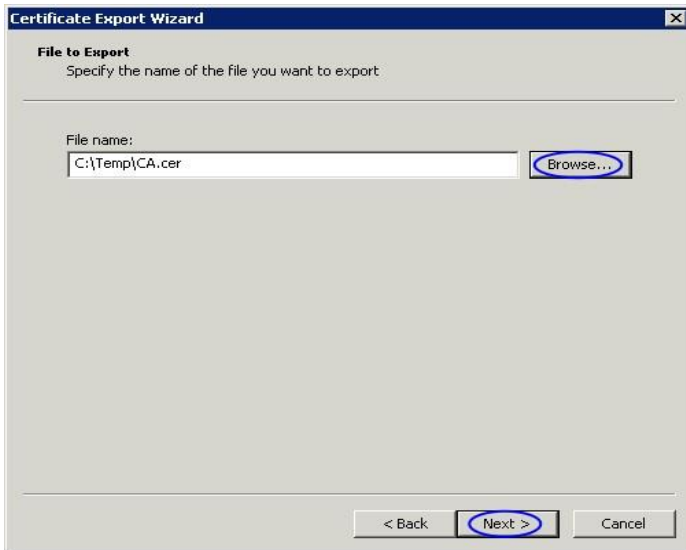
When the **Certificate** window appears, click on the **Details** tab.

Click the **Copy to File** button.

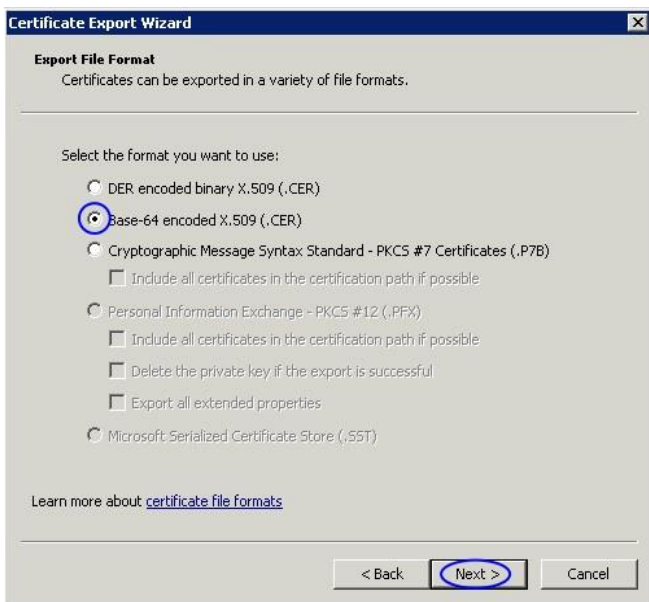


# Nagios XI – How to Use SSL with Active Directory / LDAP

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



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



# Nagios XI – How to Use SSL with Active Directory / LDAP

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

Click **Next** to continue.



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.

# Nagios XI – How to Use SSL with Active Directory / LDAP

## 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.

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](#)

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 similar to the screenshot to the right.

Click the **Download a CA certificate, certificate chain, or CRL** 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](#)

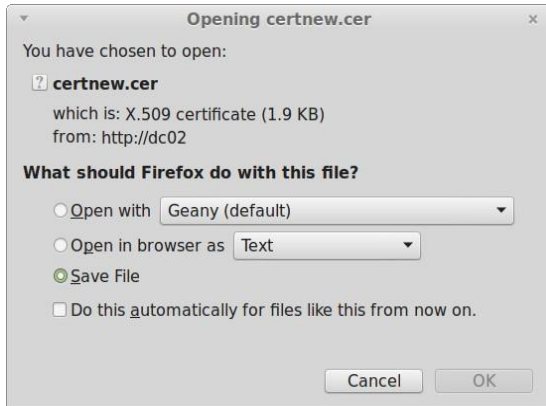
Select the CA certificate from the list of available certificates.

Select **Base 64**.

Click the **Download CA certificate** link.

# Nagios XI – How to Use SSL with Active Directory / LDAP

You will be prompted by your web browser to save the file, and 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 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.

# Nagios XI – How to Use SSL with Active Directory / LDAP

## Upload Certificate

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

Open the certificate you exported in a text editor such as

Notepad, it will appear something like the screenshot below.

```
-----BEGIN CERTIFICATE-----
MIIFAzCCA10gAwIBAgIQRKe45LY7JtEa3Z90mbKpjANBgkqhkiG9w0BAQUFADBI
MRUwEwYKCCImiZPyLGOBGRYFbG9jYWxfJAUBoGJkiaJk/IsZAEZFgZCT1gyOTMx
FzAVBgNVAAMTDkJPWDI5Hy1EQzAyLUNBMB4XDTE2MDcwNjA5MzQyNfoXDTI2MDcw
NjA5NDQyMjowSDEVMBMGcmSj0mT8ixkARKwBwxyY2F5MRYwFAYKCCImiZPyLGOB
GRYGOk9YmjkzMRcwFQYDVQQDEw5CT1gyOTMxREMEMi1DQ0TCCAiIwDQYJKoZIhvcN
AQEBBQADggIPADCCAgoCggIBAMhQXI/3sYSB9LqcWiHG5fj09sd+wwLYXWPTGxAz
5F+CacNIHvYDuWA0TzLZLCO8VvHymMOMRfF1/Vro6JZB2IXBMXURfMrxoseRudq
WniufNdAp/cRHNHu6WDJ1h4UwAitNpmxIBGSK9DquSyzfQc1RzsGDDJV805vmjg+
NcYtPX3N2EYd7fn2vn1GuxYfV9d+qg/PFJIwOkVuib3L4ifIG86naCEc3RrdZ6k2
/6wbgf634+wziXTcEezvpxvvoFDg2LhYbDA8+rFP5GJU0lH0khAWv45209VT3G5G
PSQVP2td9opWf4mPxB0Dz7o1z6I8eGItDQoBww0y+ki/Uu5/tGwQjcfD/5Nf/83L
0FmTahTGX80DvYfU5HXKtC4kqgVL4akJTaQrNyNgd30RnioesBcdKrkKs+6brAM
w1HHQGP6EK8xoh/tfRbpef0DqP9NEFJHwzBxwWRG7zT/ivkp/E/WBX0yISMdLJV
lNPKf6ur2E2Zi1KtdokRtHEa0S38flNyNwApXwnikaQDhio0dgbjDHvwhf7K0DQ
3hjDXBncImHDNqDiKv4NiJ94jV0yyOK3q6b/XCI19+hWNNqv6m3As/Wv12zUweCY
Wni93w9nzVTuKRSLJqmKsKSAbu82HdVBHQKCM3Hm/3/cLq9+A+1ukYtCRm5/Ocb
TKc rAgMBAAGjUTBPMAsGA1UdDwQEAwIBhJAPBgNVHRMBAf8EBTADAQH/MB0GA1Ud
DgQWBTT0uyFw8jsRFVg8Y6wx1Lbu0XhoVDAQBgrBgeEAYI3FQEEAwIBADANBgkq
hkiG9w0BAQUFAA0CAgEACHY2b5jLHDVwxzt93rRGK/LfwVPyZh/4gUKRmYyGrkv
2w2ARbuLfd3Fch8nzaFsx+LVZtFJUzTjSkiMFgn09vHukMbCcoIMBn2GH2w30N9P
SHSbrjvLMkClv0LeoJumTRx1mKYKhFFgLD9Ma4T7XpICDURhH8W/RiAYA0IA9b3
F0e2VhPXMbxv3/ik8q1iCArfLoqNga0GPcndYEUvp5YPSUKu97cBH+ZV0fm40j
Vckd0Z3vMtaEclhRSL+VfPlzVEjRhdjDzyf7VMC1jeTnGrbpc2LDQJewcM25os
VqyeBKnR9FaV0tJ+1wD0QozKzVmzf8DWPegGekL9lt3LmaT9la3ilPcvbobHD1Rl
pyRlyZp7fMoccz1X6i6xZldH9zd5oXjGEV4sBU/AkV6hiEzaZohXVR2xhnJt0rAZP
co9kfXQaMqNE3cpnnKEvsLfwxmTDOPf0+EeaqUYLPh0f8kOKF3iXZfo1i5kKQk+
GE0jXeFo8KJyewq4yF0dq7vFLzFRdf0Lb4z1BA88sPARUscdI2000cxK/8nf3M
TmYKlh/s+4i+3aaMRj0tpB9hIrk8C2gute4Rl+0/6mPDvUced0icqMI+Bh+QG88V
/QxbAST1jfkU+418VwbVNZVT0dxonuaxiCvqi+uAWHbAwZqXF21peJokYctfNjE=
-----END CERTIFICATE-----
```

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

Open Nagios XI and navigate to **Admin > Users > LDAP/AD Integration**.

The screenshot shows the Nagios XI Admin interface. The top navigation bar includes 'Home', 'Views', 'Dashboards', 'Reports', 'Configure', 'Tools', 'Help', and 'Admin' (highlighted). The left sidebar shows a tree view with 'System Information', 'Users', 'Manage Users', 'LDAP/AD Integration' (highlighted), and 'Notification Management'. The main content area is titled 'LDAP / Active Directory Integration Configuration'. It contains a section for 'LDAP/AD Authentication Servers' with an 'Add Authentication Server' button. Below this is a table with columns 'Server(s)', 'Type', 'Encryption', 'Associated Users', and 'Actions'. A message states: 'There are currently no LDAP or AD servers to authenticate against.' The next section is 'Certificate Authority Management' with an 'Add Certificate' button. Below this is another table with columns 'Hostname', 'Issuer (CA)', 'Expires On', and 'Actions'. A message states: 'You have not added any CA certificates through the web interface.'



# Nagios XI – How to Use SSL with Active Directory / LDAP

Click the **Add Certificate** button and the **Add Certificate to Certificate Authority** window will appear.

### 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**

  
**Certificate**

```
F0e2qVhPXMBxv3
/1K8q11cArfLoqNga0GPcnDYEUvp5YPSUKu97cBH+ZVQfm40j
VCkd0Z3vMtaEclhR5l+VfPlzVEjRhDjDzyf7VMCljeTnGrbpkc2LDQJWeWc
M25os
VeyEBKnR9FaV0tJ+1wD0QozKzVmzf8DWPegGekL9lt3lMaT9la3ilPcvbob
HD1Rl
pyRlyZp7fmocz1X6i6xZldH9zd5oXjGEV4sBU
/AkV6h1EZaZohXVR2xhnJt0rAZP
co9kfXQaMQNE3cpnnKEvslfWxmTDoPf0+EeaqUYlPh0f8k0KF3iXZfo1i5k
KCQk+
GE0jXeFo8KJyewq4yF0dq7vFlJzFRdf0Lb4z11BA88sPARUscdI2oocxK
/8nf3M
TmYKlh/s+4i+3aaMRj0tpB9hIrk8C2gute4Rl+0
/6mPDvUced0icqMI+Bh+QG88V
/QxbAST1j fku+418VWbVNZVT0dxonuaxiCvqI+uAWHbAwZqXF21peJoKYct
fNjE=
-----END CERTIFICATE-----
```

**Add Certificate**

Paste the text in your clipboard into the certificate field.

Don't worry that the text is not formatted the same as it is in the text editor you copied it from.

Once you've pasted the text, the **Hostname** field will be automatically populated with the name of the CA.

Click the **Add Certificate** button to finish uploading this certificate to Nagios XI.

## 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.

**Add Certificate**

Hostname	Issuer (CA)	Expires On	Actions
BOX293-DC02-CA	BOX293-DC02-CA	Mon Jul 06 2026 19:44:23 GMT+1000 (AEST)	<span>✕</span>

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

This completes uploading the certificate to Nagios XI.

# Nagios XI – How to Use SSL with Active Directory / LDAP

## 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.



You don't actually define which CA certificate is used. When Nagios XI is presented with a certificate from the LDAP / AD server, 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 with Active Directory / 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](#)