



## Purpose

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

## Target Audience

This document is intended for use by Nagios Fusion Administrators that require secure LDAP / AD connectivity. You may already have the LDAP / AD Integration configured in Nagios Fusion, this documentation will allow you to update your integration to use certificates.

## Prerequisites

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

- Nagios Fusion 4.1 or newer
- A separate Microsoft Windows-based AD infrastructure that is accessible to the Nagios Fusion machine
  - OR
- A 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 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 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 exist on your local computer. Computers that participate in a Windows domain automatically have a copy of this CA certificate, it happens automatically.

Why did all of that need explaining? 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 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 Fusion. The following documentation will walk you through the steps to obtain and then upload the CA certificate.

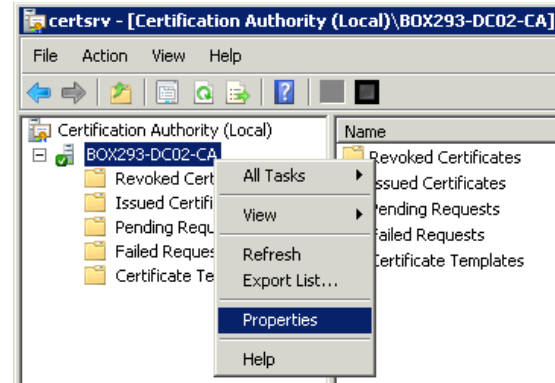
## Obtaining The Certificate - Microsoft Windows

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.

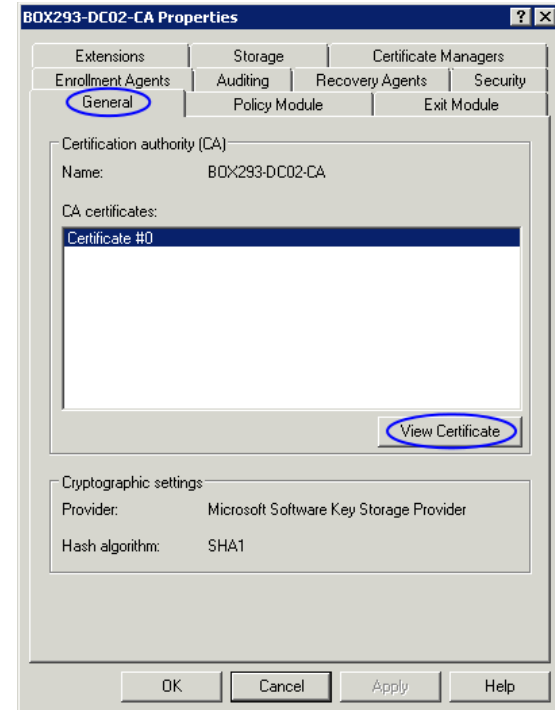
Navigate to **Administrative Tools** (commonly found in the control panel) and open **Certification Authority**.



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

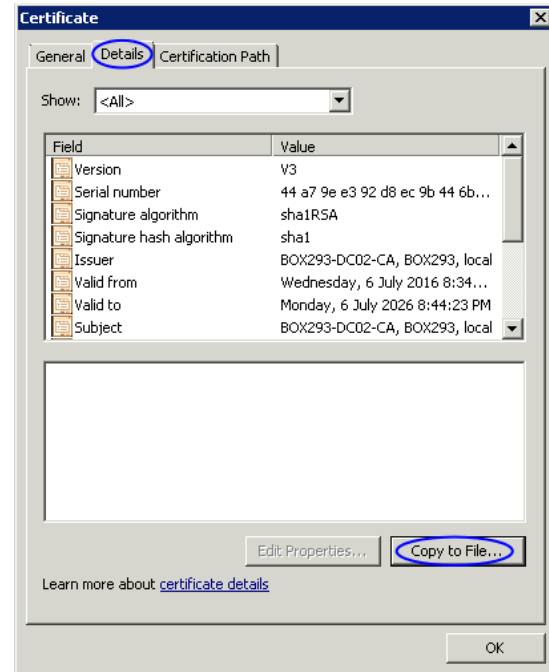
When the Properties window appears you will be on the **General** tab.

Click the **View Certificate** button.



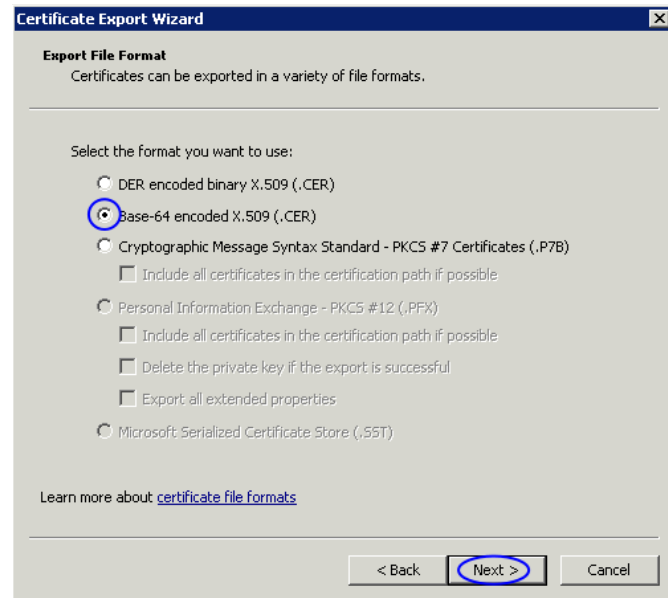
When the Certificate window appears, click on the **Details** tab.

Click the **Copy to File** button.



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

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

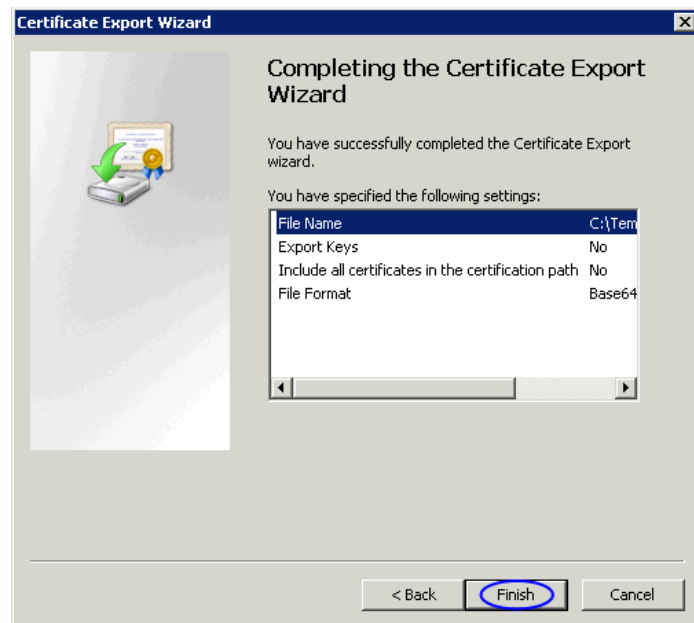
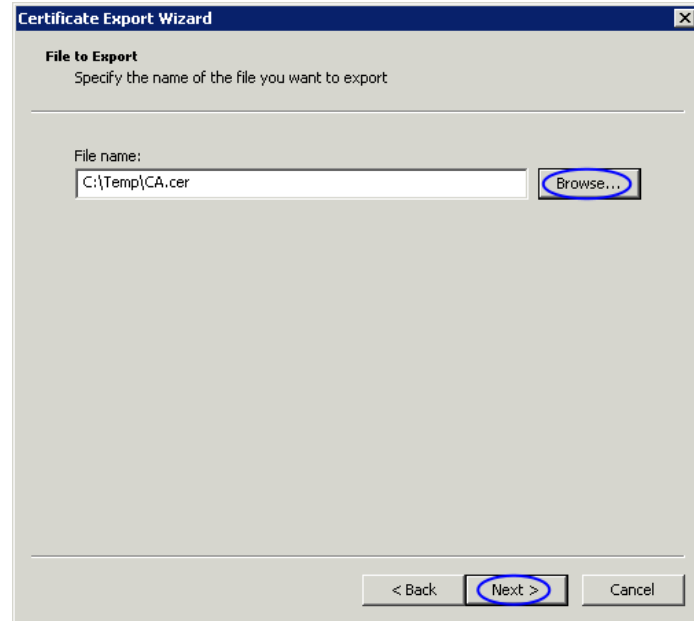


Use the **Browse** button to select a location to save the certificate file to, you will need to provide a name for the certificate.

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 Fusion from.



## 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.

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.

Select the CA certificate from the list of available certificates.

Select **Base 64**.

Click the **Download CA certificate** link.

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 Fusion from.

**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](#)

**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

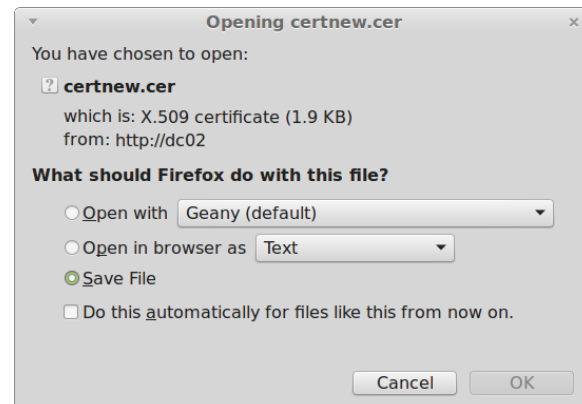
[Install CA certificate](#)

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)



## 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 Fusion server.

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

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.

```
-----BEGIN CERTIFICATE-----
MIIFazCCA10gAwIBAgIQRkee45LY7JtEa3Z9QmbKpJANBgkqhkiG9w0BAQUFADBI
MRUwEwYKCZImiZPyLGDQGRYFbg9jYWwxFjAUBgoJKiaJk/IsZAEZFGZCT1gy0TMx
FzAVBgNVBAMTDkJPWDI5My1EQzAylLUNBMB4XDTEmcWwNjA5MzQyNFoXDTI2MDcw
NjA5NDQyM1owSDEVMBMGCGmSj0mT8ixkARKwBwXvY2FsmRYwFAYKZImiZPyLGDQ
GRYGOk9YMjkzMRcwFQYDVQDEw5CT1gy0TMtREMwMi1DQTCACAIwDQYJKoZIhvcN
AQEBBQADggIPADCCAgCggIBAMhQxI/3sYSB9LqCwIHG5fj09sd+wwLXYWPTgxAz
5F+CacNIHvYDuwAOTzLZLC08VvHymMOMRFF1/Vro6JZB2IXBMXuRfMrxoSErudq
WniuFNdAp/cRHNHu6WDJ1h4UwAitNpmxIbGSK9DquSYzFqC1RzsGDDJVb05vmjg+
NcYtPXN32EYd7fn2vn1GuxYfV9d+qg/PfJIw0kVuib3L4ifI686naCeC3RDz6k2
/6wbgf034+wziXTcEezvpxvofDg2LHybDA8+rFP5GJU0LH0khAWv45209V73gsG
PSQVP2td9opWf4mPx80Dz7o1z6I8eGItdQoBwwOy+ki/Uu5/TGWQjCfD/5NF/83L
0fmTahtGX80DvYfU5HXKtc4kqg6VL4akjTaQrryNgd30RnioesBcdKrkEs+6brAM
w1HHQ6p6EK8xoh/tfRbpef0DqP9NEFJHwzBxwHWRG7zT/ivkp/E/WBx0yISMdLJV
LNpkf6ur2E2Zi1KtdokRtHlea0S38flnyNwApXwnikaQDhio0dgbjDhVwhf7K0DQ
3hjDXBnCIhHDNqDikv4NiJ94jV0yyOK3q6b/XCI19+hWNNq6m3As/Wv12zuWeCY
Wni93w9nzVTuKRSFLJqmKsKsABu82HdVBHQKCM3Hm/3/clq9+A+1ukYTcRm5/0cb
TkcrAgMBAAGjUTBPMASGA1UdDwQEAwIBhjAPBGNVHRMBAf8EBTADAQH/MB0GA1Ud
DgQWBBT0uyFw8jsrFVg8Y6wx1Lbu0XhoVDAQBgkrBgEEAYI3FQEEAwIBADANBgkq
hkiG9w0BAQUFAAOCAGEAChY2b5jLHDVWxz293rRGK/LfwvPpZh/4gUKRmYyGrkV
2w2ARBuLfd3Fch8nzaFsx+LVZtFJUJZTjSkIMFGn09vHukMbCCoIMBn2GH2w30N9P
SHSbrjvLMkClv0LeoJumTRx1mKYkhFFgLD9Ma4T7XpICDURhH8W/RiAYA0IA9b3
FOe2qVhPXMbxv3/iK8q1icArfLoqNgha0GpCndYUvP5YPSUKU97cBH+ZV0fm40j
VCkd0Z3vMtaEclhRSL+VfPLzVEjRhDjDzyf7VMC1jeTnGrbpc2LDQJWeWcM25os
VqyeBKnR9Fav0tJ+1wD0QozKzVzmf8DWPeggEkl9lt3lMaT9la3iLpCvbobHD1Rl
pyRlyZp7fmc0z1X6i6xZldH9zd50xjGEV4sBU/AkV6hiEzAzhXVR2xhnJt0rAZP
co9kfxQaMQNE3cpnnKEvslfwxmTDoPfo+EeaquYLPh0f8k0KF31XZfo115kKCKq+
GE0jXeFo8KJyewq4yF0dq7vFLJzFRdF0Lb4z11BA88sPARUscdI2ooccx/8nf3M
TmYKLh/s+4i+3aaMRj0tpB9hIrk8C2gute4Rl+0/6mPDvUced0icqMI+Bh+QG88V
/QxbAST1jfkU+418VwBVNzVT0dxonuaxiCvqI+uAWhbAwZqXF21peJoKycTfNJE=
-----END CERTIFICATE-----
```

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

**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](#).

[Add Authentication Server](#)

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 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
You have not added any CA certificates through the web interface			

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



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 Fusion.

### 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
/iK8q1lcArfLoqNgha0GPcnDYEUvp5YPSUKu97cBH+ZV0fm40j
VCkd0Z3vMtaEclhRSl+VfPlzVEjRhDjDzyf7VMC1jeTnGrbpc21DQJWeWc
M25os
VqyeBKnR9FaV0tJ+1wD0QozKzVmzf8DWpEGgEkL9lt3lMaT9la3ilPcvbob
HD1Rl
pyRlyZp7fmocz1X6i6xZldH9zd5oXjGEV4sBU
/AkV6h1EZaZohXVR2xhnJt0rAZP
co9kfXQaMQNE3cpnnKEvsLfWxmTDoPf0+EeaqUYlPh0f8k0KF3iXZfo1i5k
KCQk+
GE0jXeFo8KJyewq4yF0dq7vFLJzFRdf0Lb4z11BA88sPARUscdI2ooocxK
/8nf3M
TmYKLh/s+4i+3aaMRj0tpB9hIrk8C2gute4RL+0
/6mPDvUced0icMI+Bh+QG88V
/QxbAST1j fku+418VWbVNZVT0dxonuaxiCvqI+uAWHbAwZqXF21peJoKYct
fnjE=
-----END CERTIFICATE-----

```

[Add Certificate](#)

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.

[Add Certificate](#)

Hostname	Issuer (CA)	Expires On	Actions
BOX293-DC02-CA	BOX293-DC02-CA	Mon Apr 26 2027 10:10:03 GMT+1000 (AUS Eastern Standard Time)	<a href="#" style="color: #007bff; font-size: 1.2em;">✕</a>

This completes uploading the certificate to Nagios Fusion.

## Configure Authentication Server

This guide does not explain how to add an Authentication Server to Nagios Fusion, 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:



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

You don't actually define which CA certificate is used. When Nagios Fusion is presented with a certificate from the LDAP / AD server, the 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 how to use SSL/TLS with Active Directory / LDAP in Nagios Fusion. If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

<https://support.nagios.com/forum>

The Nagios Support Knowledgebase is also a great support resource:

<https://support.nagios.com/kb>