Using SSL with AD and LDAP with Nagios Log 2024

Prerequisites

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

- Nagios Log Server 1.5 or newer
- 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 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 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.

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 here.
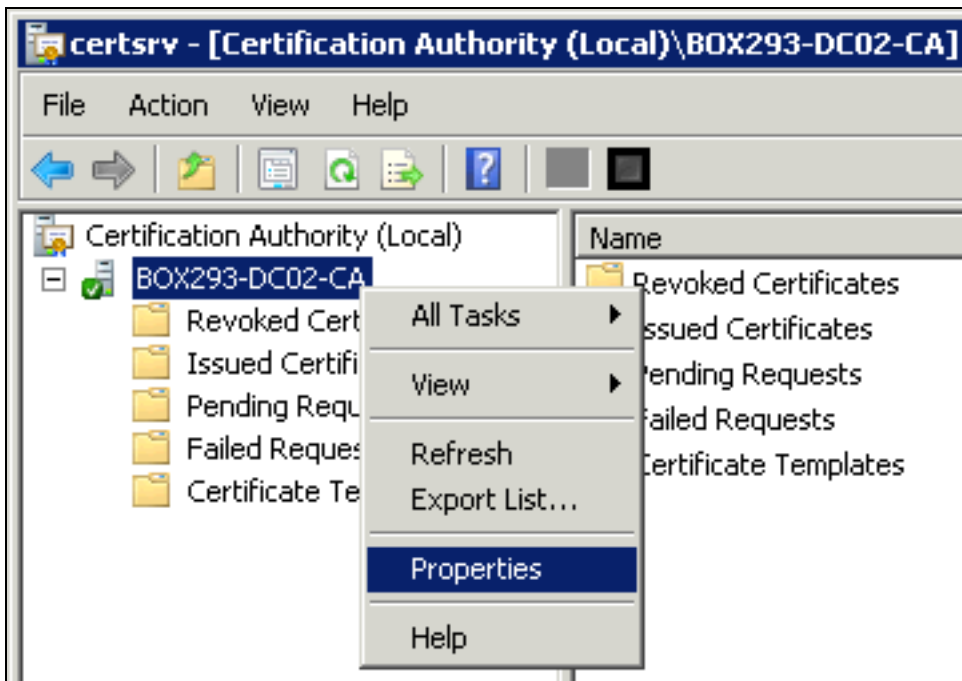
Method 1) Console / RDP Session To CA Server

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.

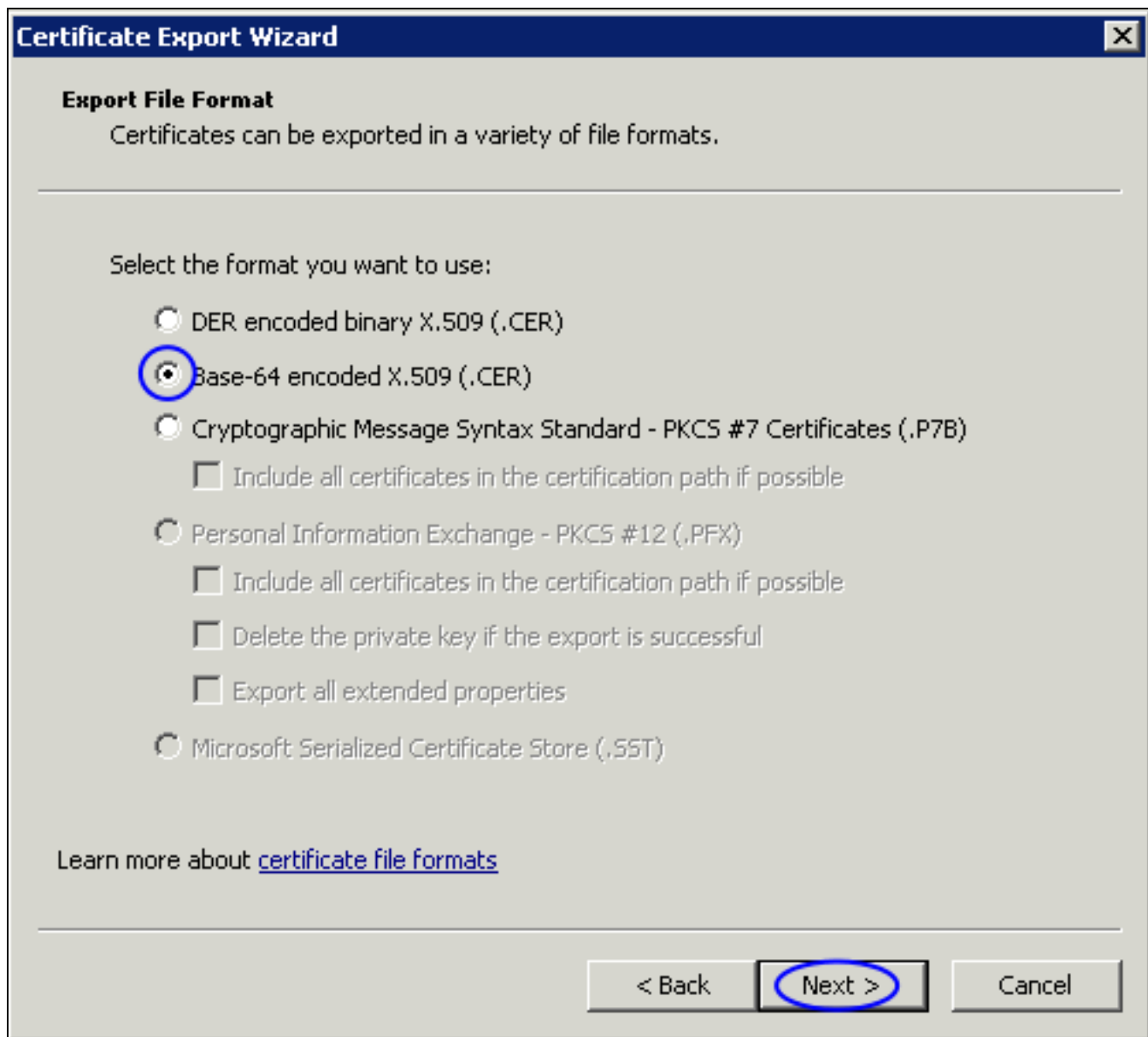2. When the Certification Authority opens right click on the CA server and select Properties.
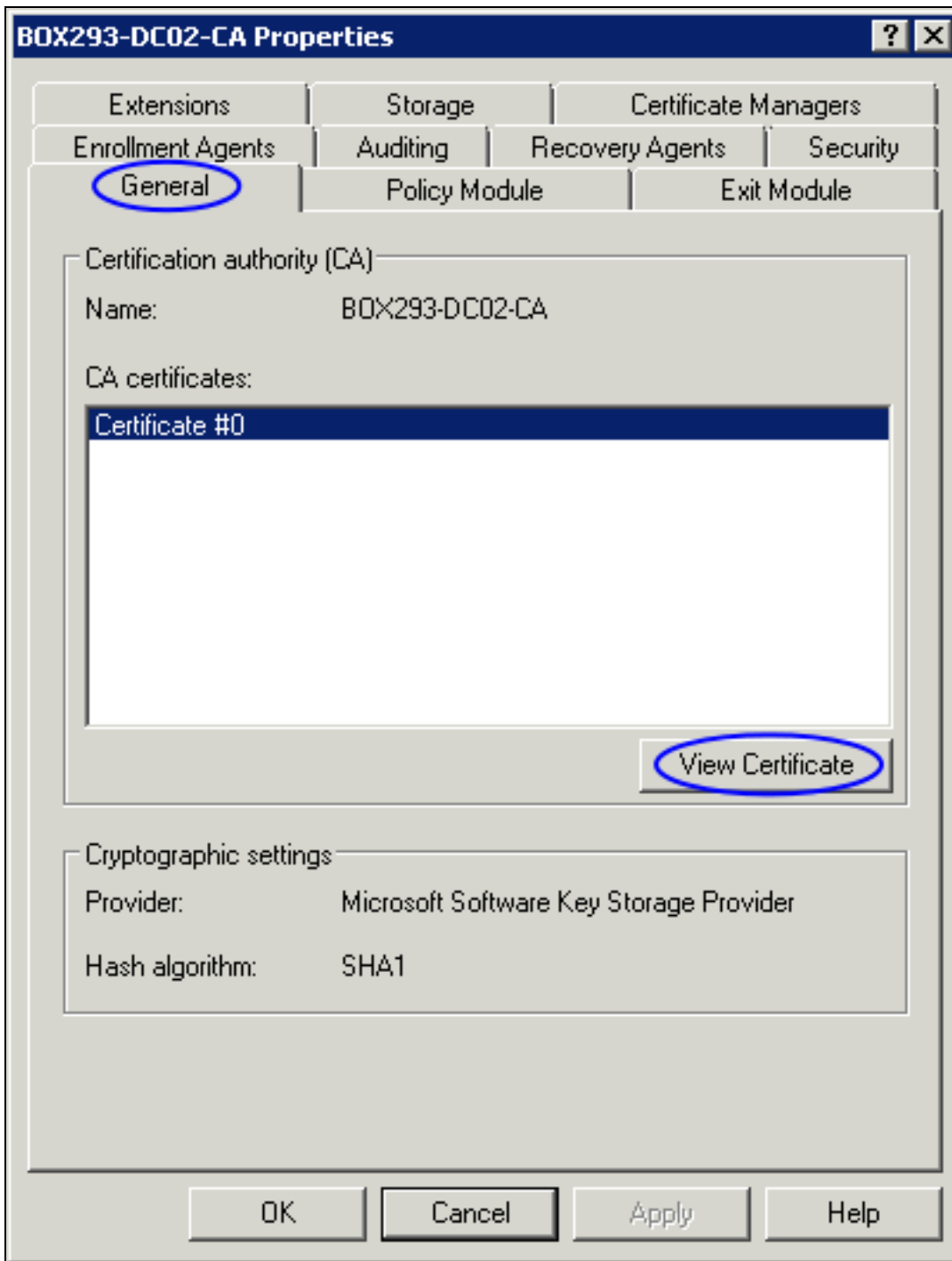
3. When the Properties window appears you will be on the General tab.
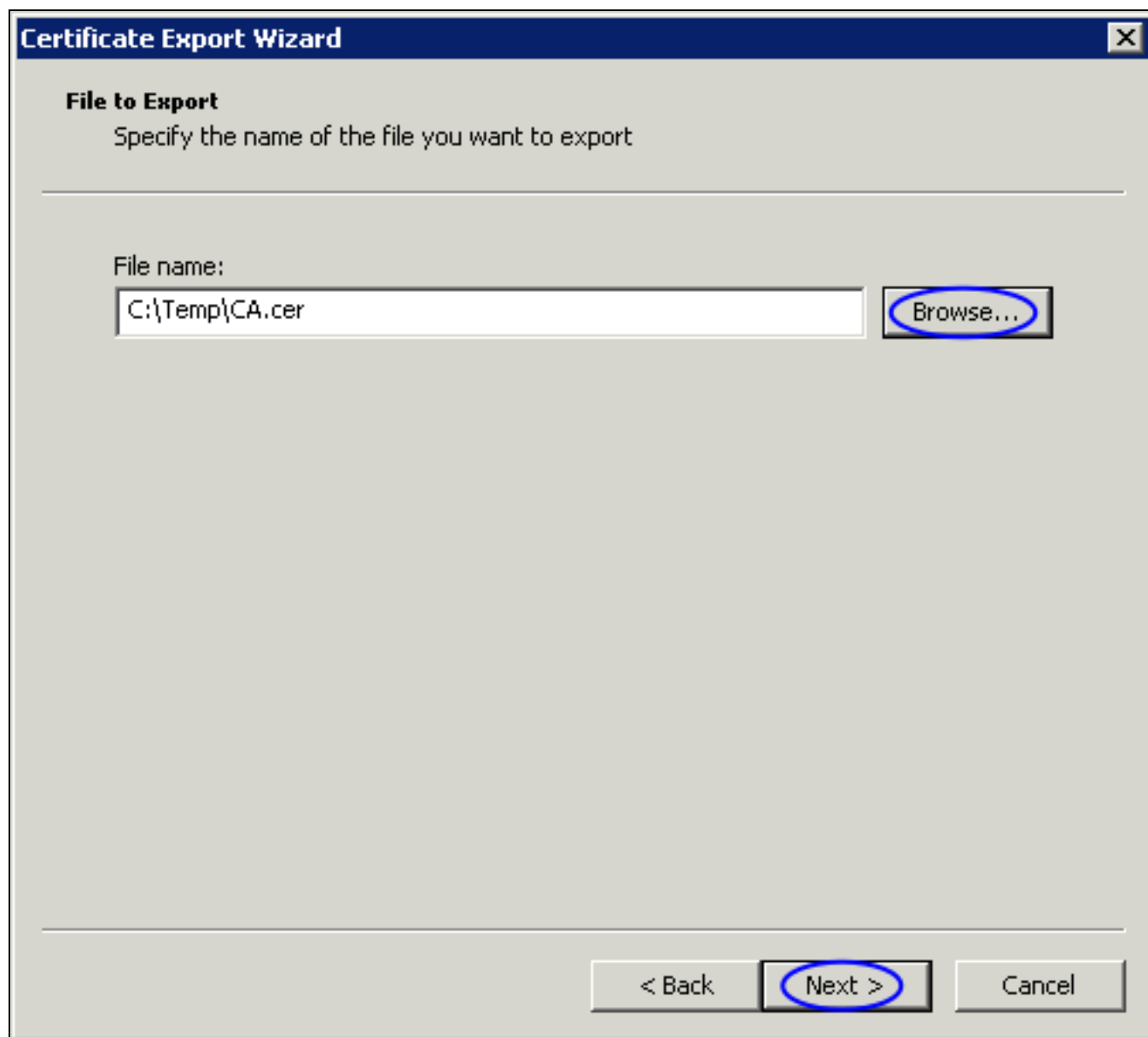
4. Click the View Certificate button.
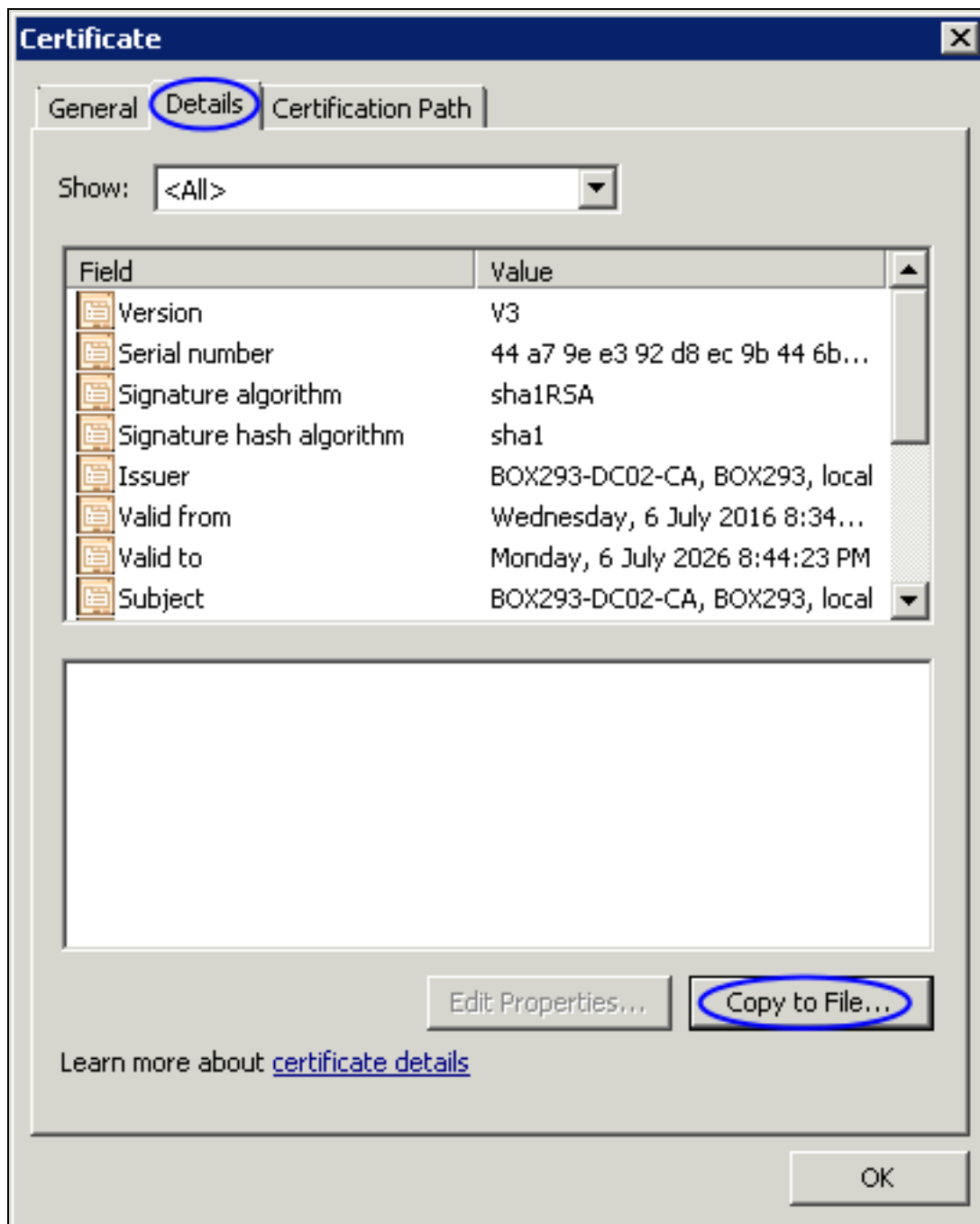
5. When the Certificate window appears, click on the Details tab.
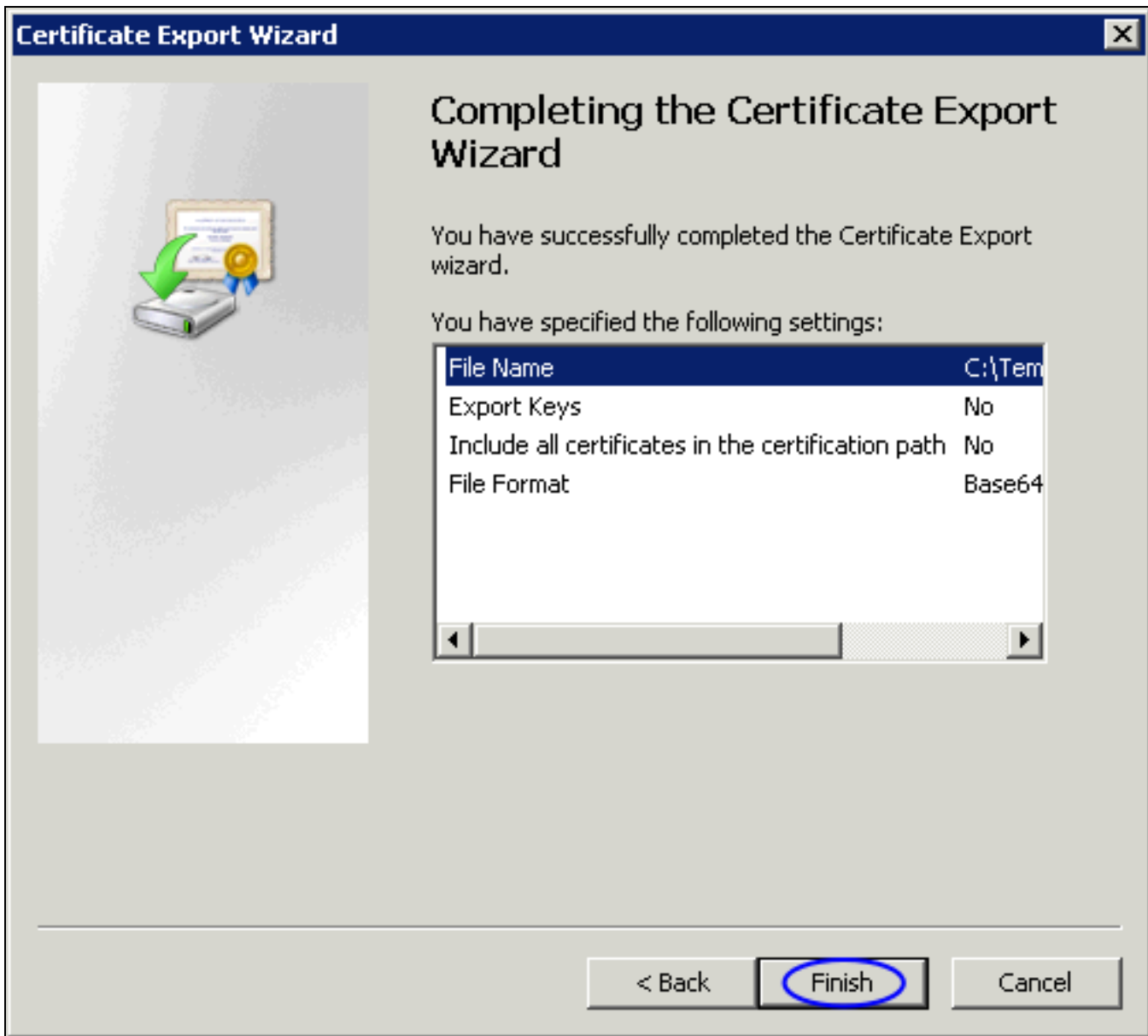
6. Click the Copy to File button.

Nagios

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

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

Nagios

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.

Nagios

11. 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 Log Server 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.

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 similar to the screenshot to the right.

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.
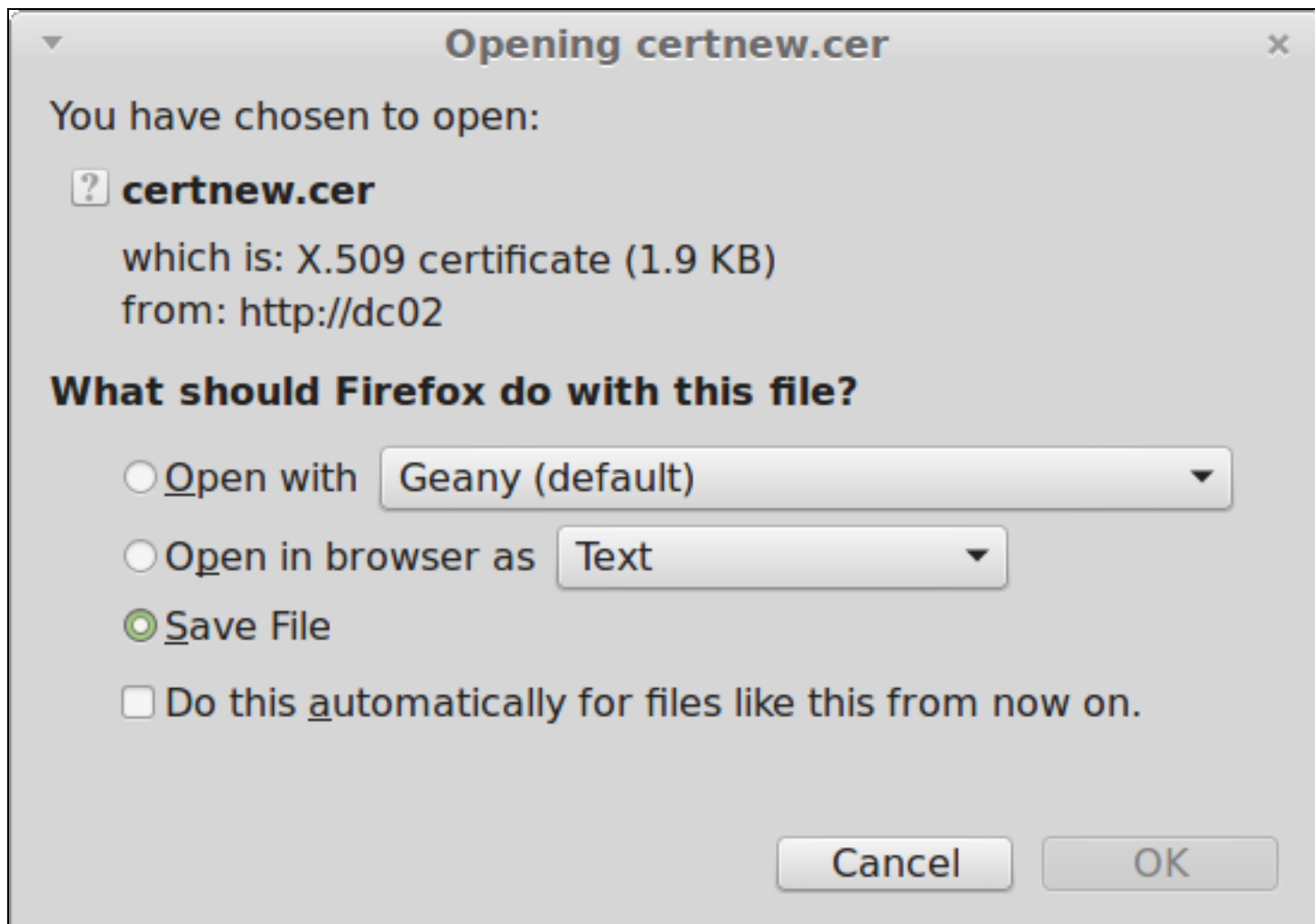
6. You will be prompted by your web browser to save the file, it should be named certnew.cer. This will vary depending on the web browser you are using.

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.

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.

Nagios

> 📝 **Debian/Ubuntu systems**: You will need to replace the /etc/openldap/ 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/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

Establish a terminal session to your Nagios Log Server. The next command has a value that need changing:

- ca_box293.crt

  - This is the name of file you are storing the CA certificate in

  - It can be named whatever you want as long as it ends in .crt

> 📝 **Debian/Ubuntu systems**: You will need to replace the /etc/openldap/ directory in the following examples with /etc/ldap/

Execute the following commands to create a new file (using the name above):

```
cd /etc/openldap
```

```
vi certs/ca_box293.crt
```

When using the vi editor, to make changes press i on the keyboard first to enter insert mode. Press Esc to exit insert mode.

Open the certificate you obtained in the last step with a text editor like Notepad. Copy and paste the certificate text into the new file, including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines.

> When you paste the certificate into vi, it's possible that blank lines are added between each line. You will need to remove these blank lines as they will cause the certificate file to break.

When you have finished, save the changes in vi by typing:

```
:wq
```

and press Enter.

The next step is to convert the certificate to the correct format.

Convert Certificate

Execute the following command to convert the CA certificate to a .pem file. The file will have the same name as the .crt file you are converting.

```
openssl x509 -text -in certs/ca_box293.crt > certs/ca_box293.pem
```

The next step is to create a directory and create a symbolic link to the .pem file into the new directory.

```
mkdir cacerts
```

```
hash=$(openssl x509 -in certs/ca_box293.pem -hash -noout)
```

```
ln -s /etc/openldap/certs/ca_box293.pem cacerts/$hash.0
```

On my server the symbolic file created was /etc/openldap/cacerts/467b6a1d.0 but on your server it will be different. It's very important that the file has this specific hash generated name otherwise OpenLDAP will simply ignore the CA .pem file it is linked to.

The next step will be to configure OpenLDAP to use this certificate.

Configure OpenLDAP/LDAP

You need to make a change to the OpenLDAP/LDAP configuration file so that it uses any certificate in the /etc/openldap/cacerts/ directory. The change is made to the /etc/openldap/ldap.conf file and the line in the file needs to look like this:

TLS_CACERTDIR /etc/openldap/cacerts

The following command will make that change:

```
sed -i 's/^TLS_CACERTDIR.*/TLS_CACERTDIR \/etc\/openldap\/cacerts/g' ldap.-
conf
```

Nagios

Restart Apache

The last step requires you to restart the Apache Web Server so it knows about the CA certificate.

RHEL | CentOS | Oracle Linux

```
systemctl restart httpd.service
```

Debian

```
systemctl restart apache2.service
```

Ubuntu

```
cp root.crt /usr/local/share/ca-certificates/
```

```
sudo update-ca-certificates
```
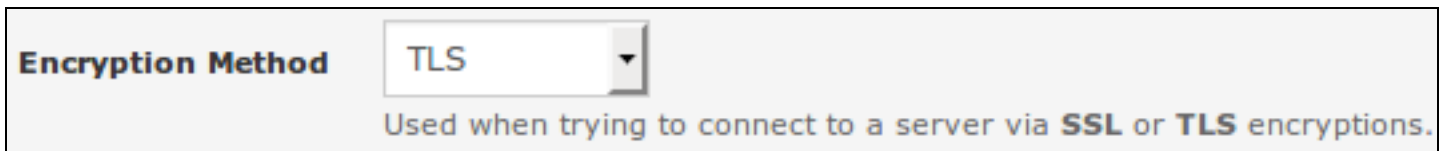
```
systemctl restart apache2.service
```

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.

Encryption Method TLS ▼

*Used when trying to connect to a server via **SSL** or **TLS** encryptions.*

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 Log Server is presented with a certificate from the LDAP / AD server, the Nagios Log Server checks it's local CA store for the CA certificate to validate the certificate provided by the LDAP / AD server.