Using SSL with AD and LDAP in Nagios Network Analyzer 2024

Prerequisites

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

- Nagios Network Analyzer 2.4 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 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.

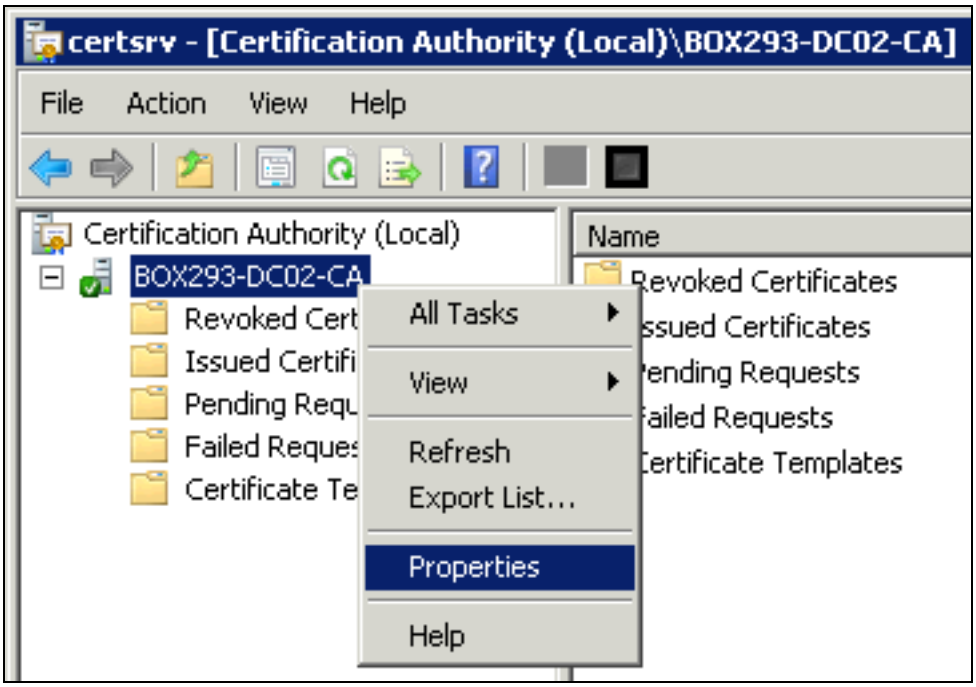
Certificates are also used for user authentication on private networks, such as communicating with an AD / LDAP server. If you have a Windows computer that is joined to an AD, certificates are used by the domain controller(s) (DC) to securely transmit username and password information. In this scenario 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 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. 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 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 Network Analyzer. 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.

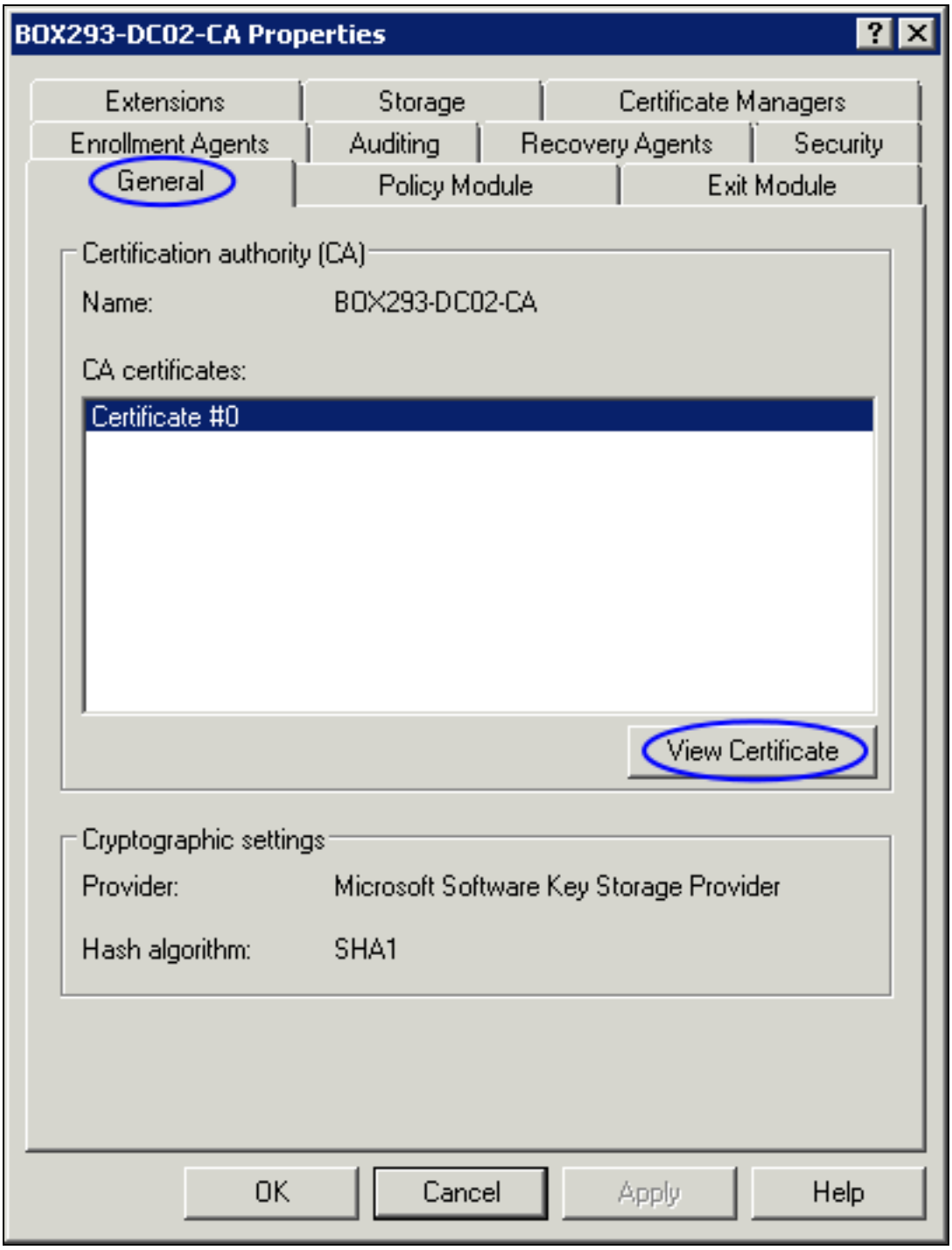


Method 1) Console / RDP Session To CA Server

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

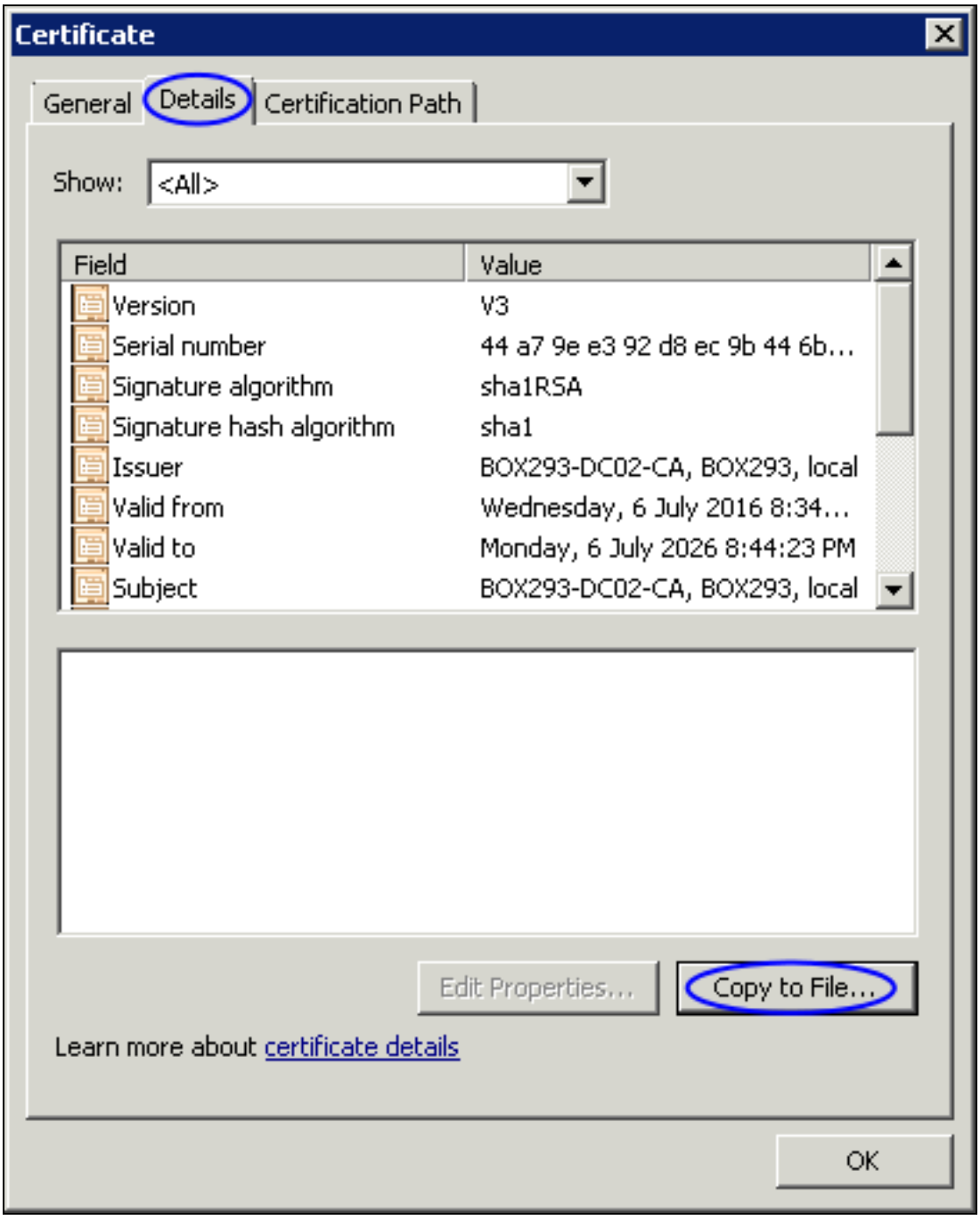
1. Navigate to Administrative Tools (commonly found in the control panel) and open Certification Authority.

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



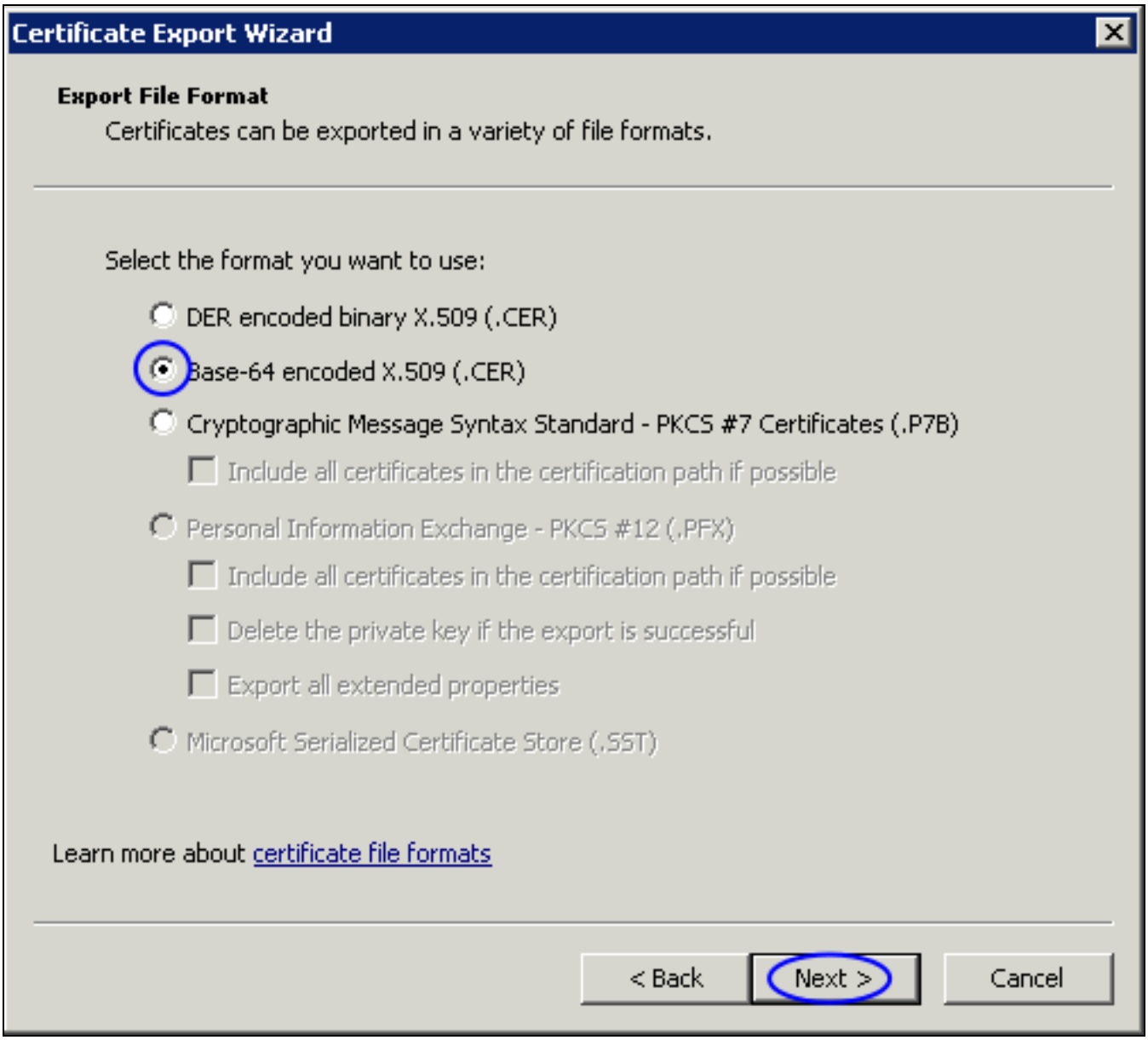
3. When the Properties window appears you will be on the General tab.

4. Click the View Certificate button.



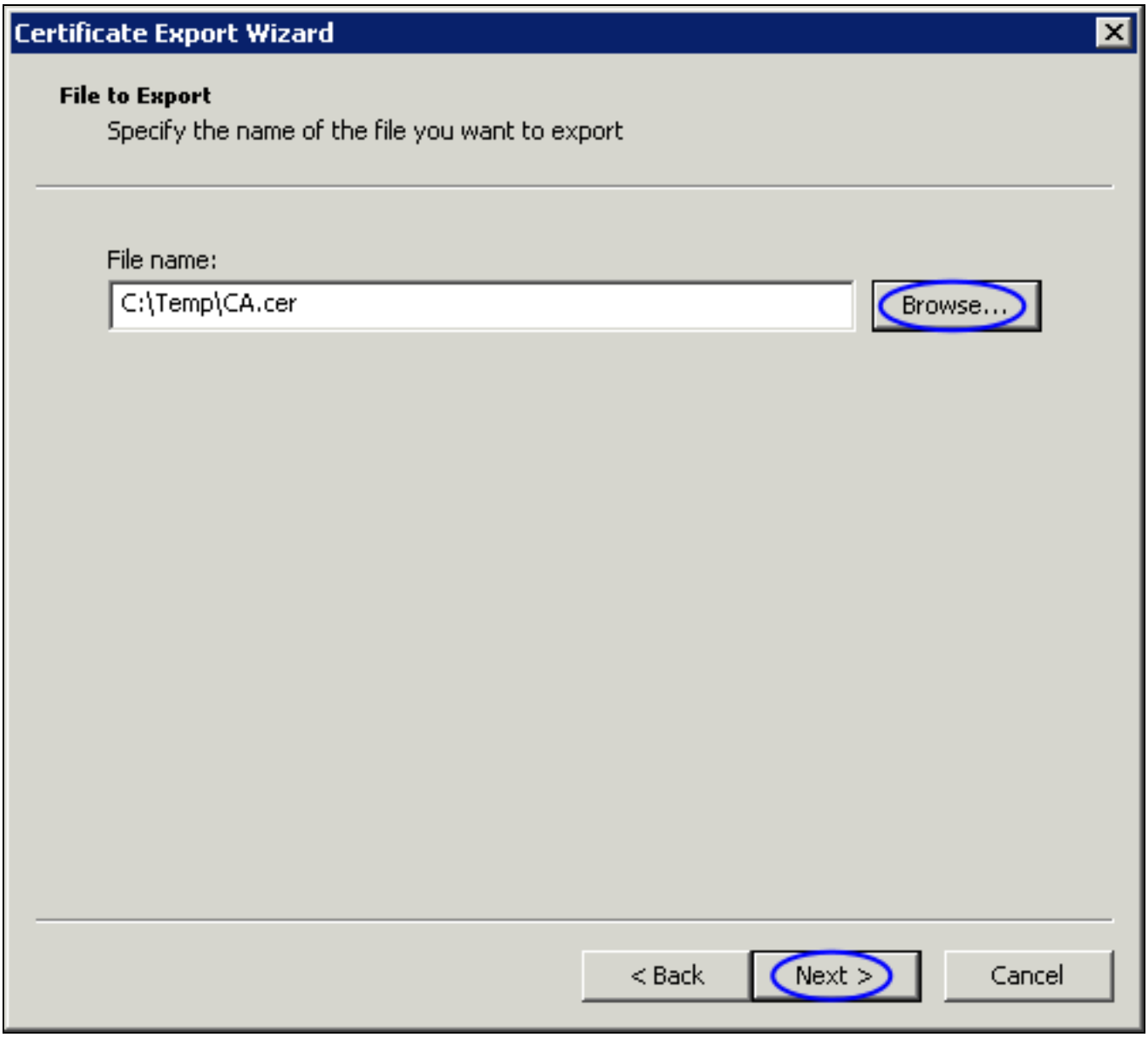
5. When the Certificate window appears, click on the Details tab.

6. Click the Copy to File button.



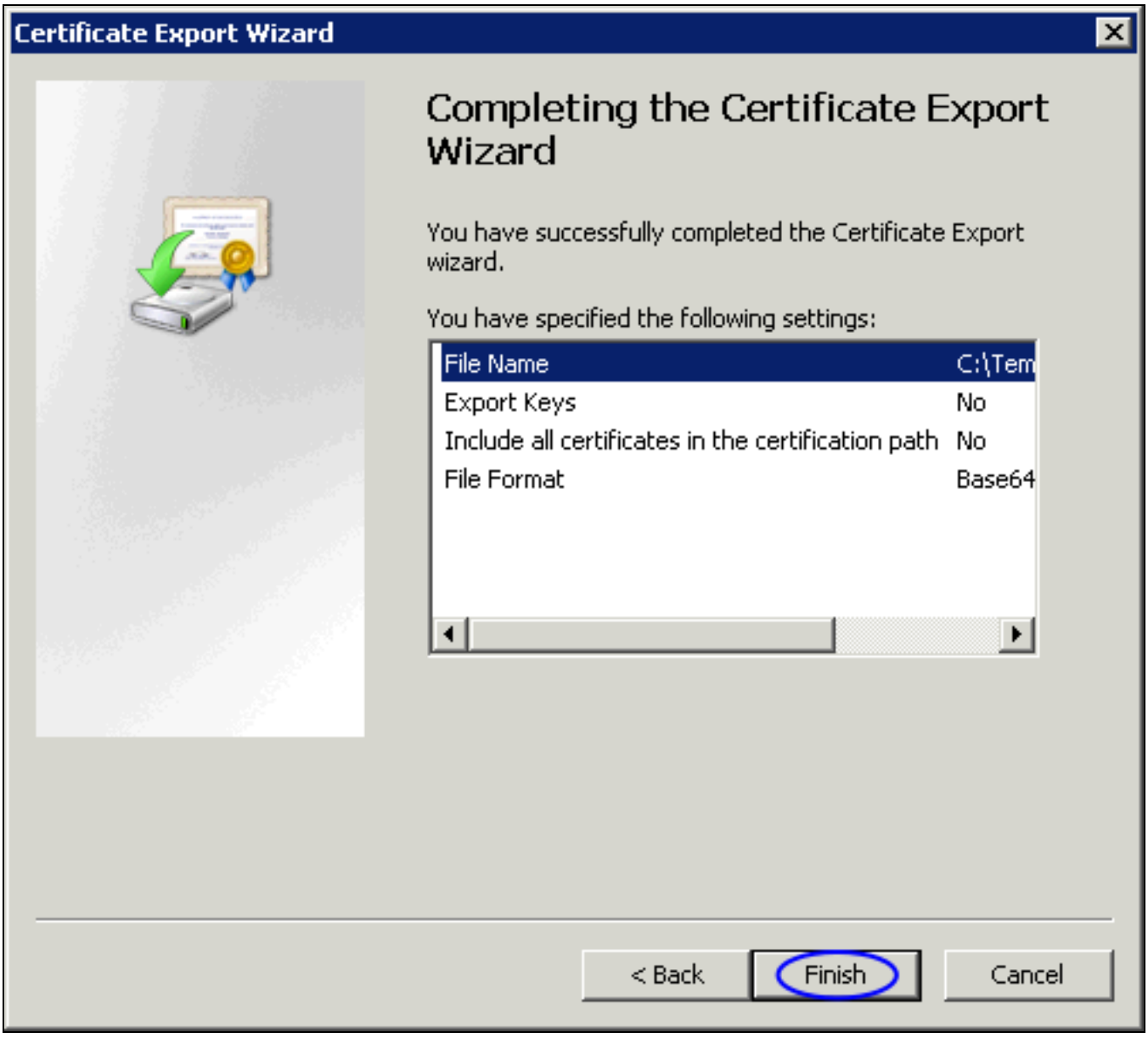
7. The Certificate Export Wizard window appears, click Next.

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



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.

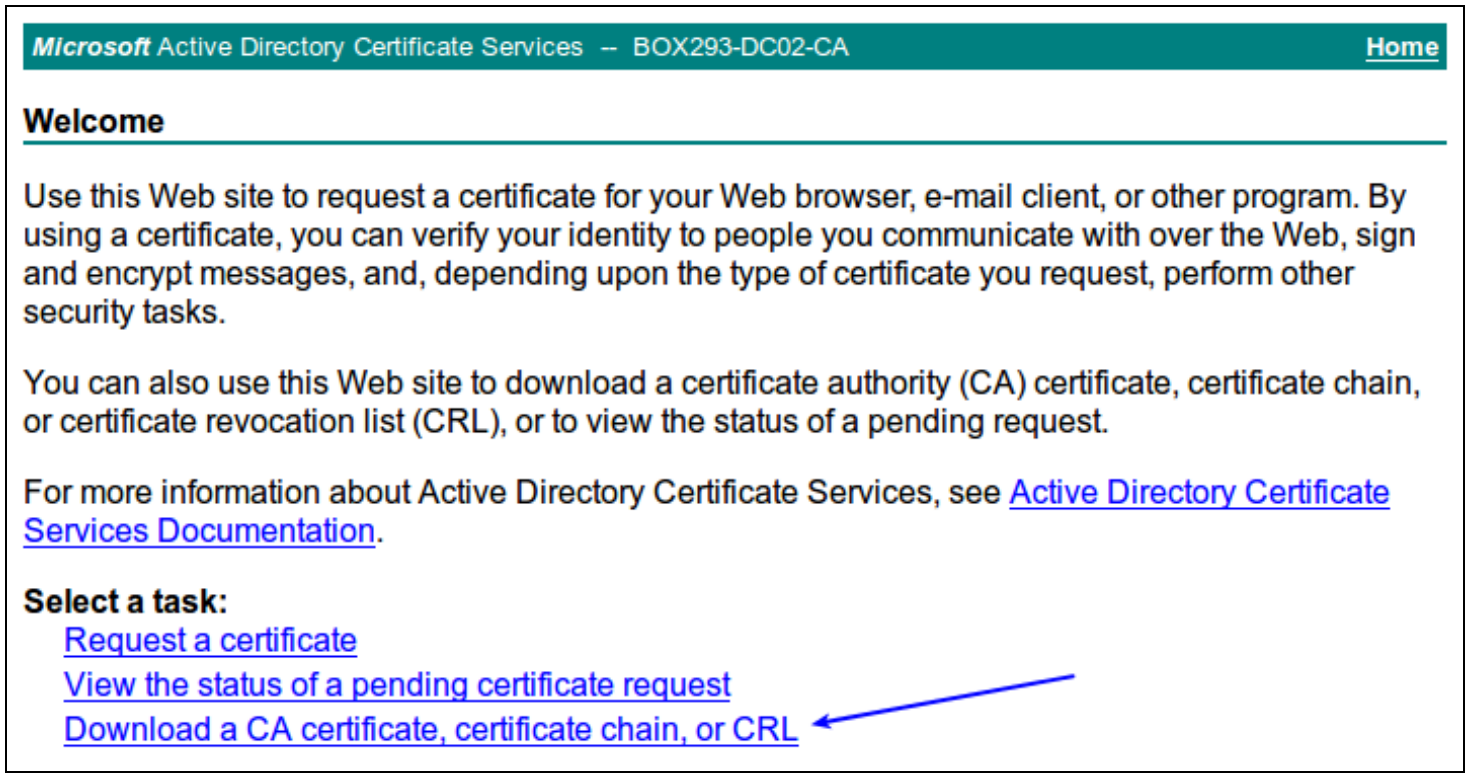
10. Click Next to continue.



11. Click the Finish button to export the certificate.

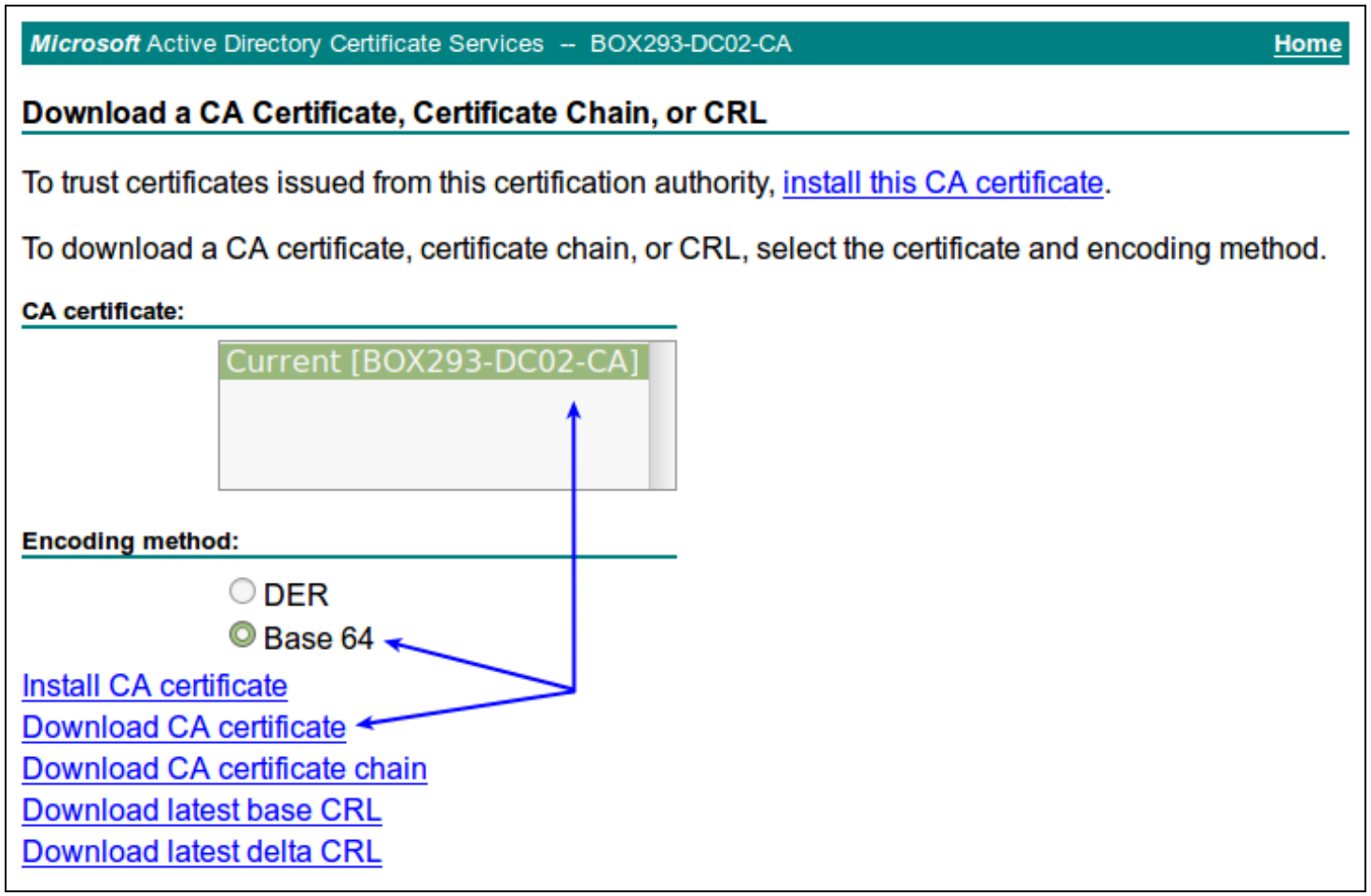
12. You will receive a message to confirm the certificate export was a success. Click OK. You can now close all the open windows. You can now proceed to the Upload Certificate section of this document. Make sure you have access to the exported .cer file from the computer you will upload the certificate to Nagios Network Analyzer 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.

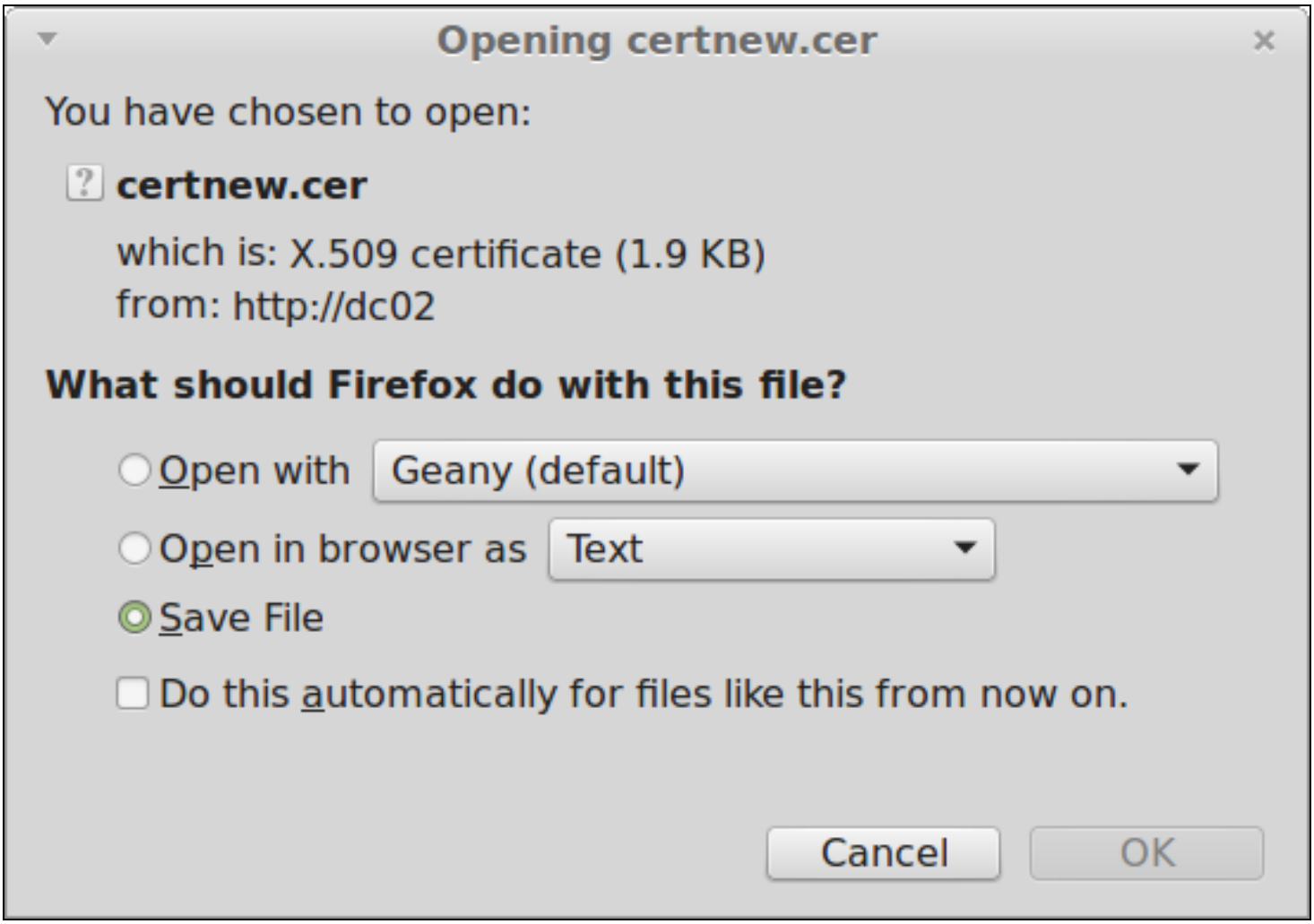


2. Click the Download a CA certificate, certificate chain, or CRL link.

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 Network Analyzer 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

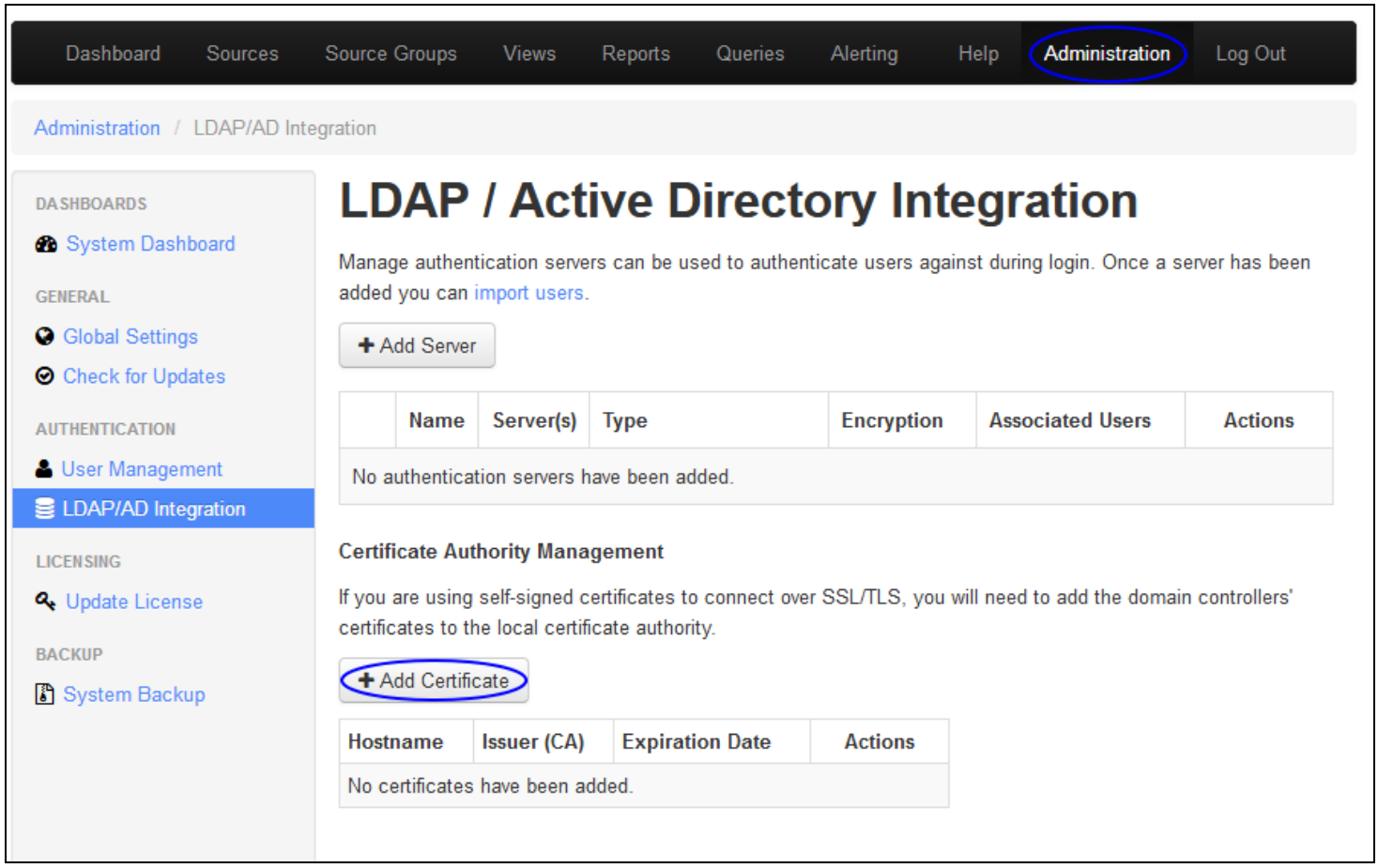
```
-----BEGIN CERTIFICATE-----
MIIFazCCA1OgAwIBAgIQRKee45LY7JtEa3Z9QmbKpjANBgkqhkiG9w0BAQUFADBI
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFjAUBgoJkiaJk/IsZAEZFgZCT1gyOTMx
FzAVBgNVBAMTDkJPWDI5My1EQzAyLUNBMB4XDTE2MDcwNjA5MzQyNFoXDTI2MDcw
NjA5NDQyM1owSDEVMBMGCgmSJomT8ixkARkWBWxvY2FsMRYwFAYKCZImiZPyLGQB
GRYGQk9YMjkzMRcwFQYDVQQDEw5CT1gyOTMtREMwMi1DQTCCAiIwDQYJKoZIhvcN
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-----
```

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

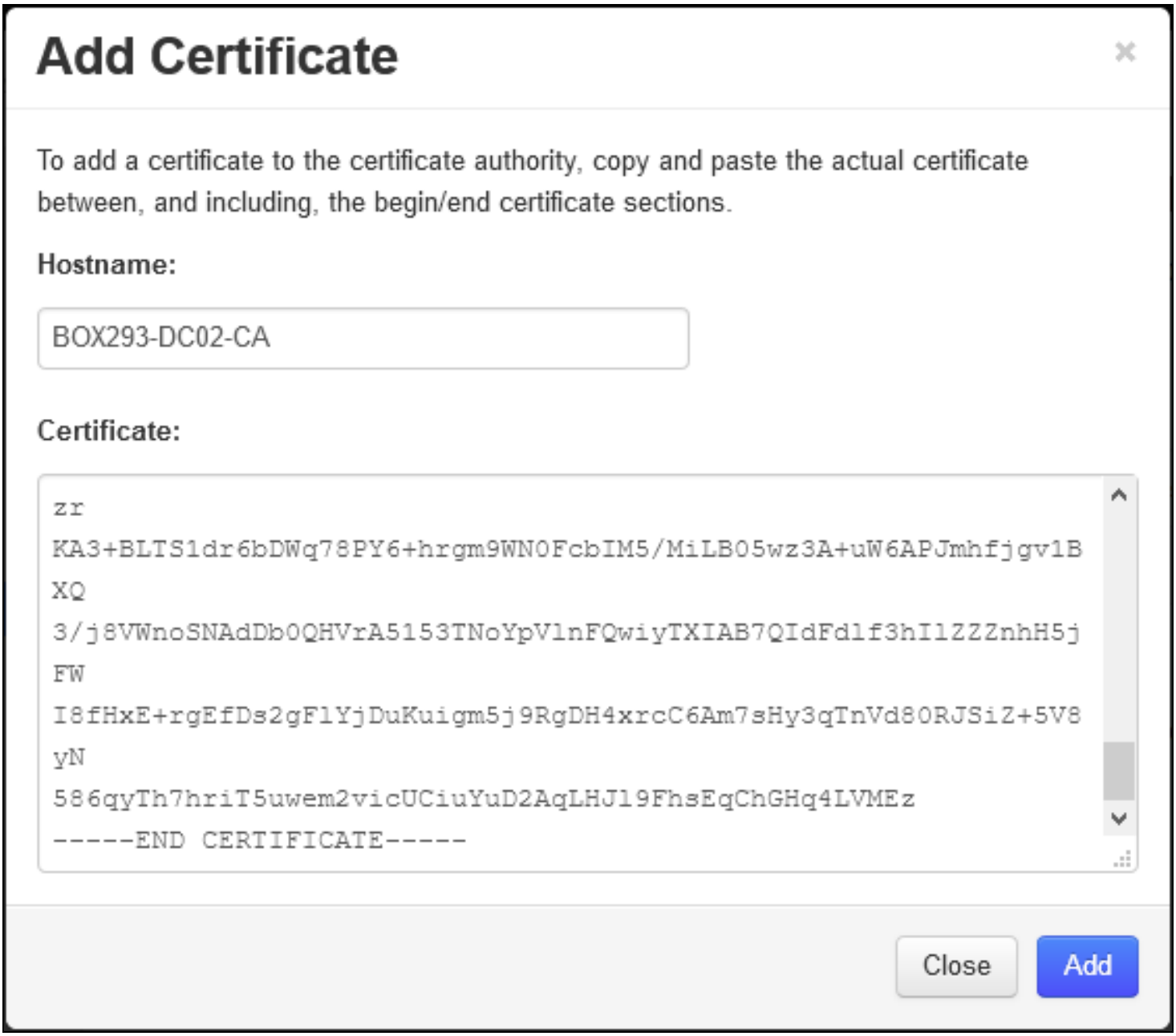
1. Open the certificate you exported in a text editor such as Notepad, it will appear something like the screenshot to the right.

2. 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.

3. Open Nagios Network Analyzer and navigate to Administration > Authentication > LDAP/AD Integration.



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

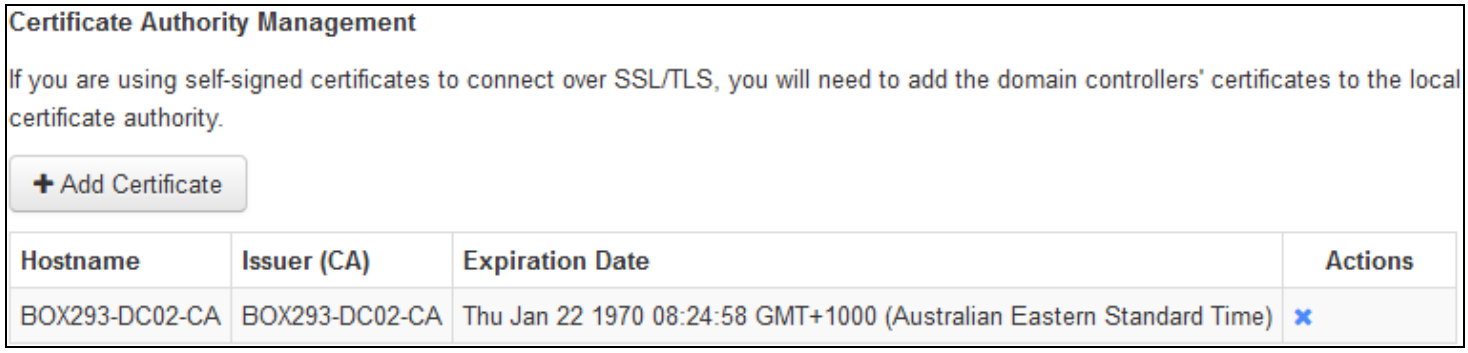


5. Paste the text in your clipboard into the certificate field. Don't worry that the text is not formatted the same as it is in the text editor you copied it from.

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

7. Click the Add Certificate button to finish uploading this certificate to Nagios Network Analyzer.

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

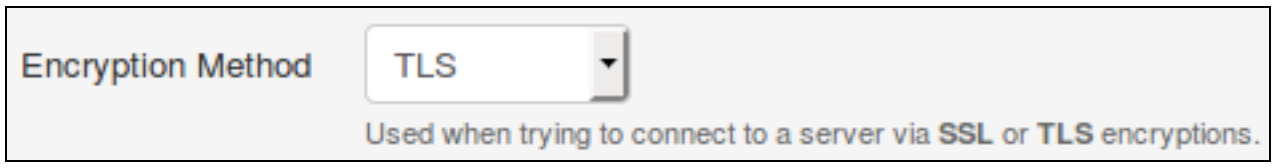


This completes uploading the certificate to Nagios Network Analyzer.

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 the Security setting that requires authentication to use SSL / TLS with certificates.

You don't 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.