Purpose

This document describes how to use SSL/TLS with Active Directory (AD) AND LDAP in Nagios Fusion 2024.

Prerequisites

You will need the following prerequisites to follow the documentation:

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

www.nagios.com



Page 1 of 12

Why did all of that need to be explained? 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 DCs; 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. This 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
- Method 2: CA Server Web Interface

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.



www.nagios.com



Page 2 of 12

- 3. When the **Properties** window appears, you will be on the **General** tab.
- 4. Click the View Certificate button.

inservia-CA Propertie	es			?	×
Extensions	Storage		Certificate I	Manager	s
Enrollment Agents	Auditing	Recover	y Agents	Sec	urity
General	Policy Ma	dule	Exit	Module	
Certification authority	(CA)				
Name:	winserv 1a-CA	λ			
CA certificates:					
Certificate #0					
			View C	ertificate	$\mathbf{\Sigma}$
			View C	ertificate	$\mathbf{\Sigma}$
Cryptographic setting	s		View C	ertificate	Σ
Cryptographic setting Provider:	s Microsoft Soft	tware Key St	View C orage Provi	iertificate	Σ
Cryptographic setting Provider: Hash algorithm:	s Microsoft Soft SHA256	tware Key St	View C orage Provi	iertificate	>
Cryptographic setting Provider: Hash algorithm:	s Microsoft Soft SHA256	tware Key St	View C orage Provi	ertificate ider	Σ
Cryptographic setting Provider: Hash algorithm:	s Microsoft Soft SHA256	tware Key St	View C orage Provi	iertificate	
Cryptographic setting Provider: Hash algorithm:	s Microsoft Soft SHA256	tware Key St	View C orage Provi	ertificate ider	Σ
Cryptographic setting Provider: Hash algorithm:	s Microsoft Soft SHA256	tware Key St	View C	ider	Σ



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

📃 Certificate		Х
General Details Certification Path	1	
Show: <all></all>	~	
Field	Value	^
Version	V3	
Serial number	7a4227356e30daa84f106fbcd	
Signature algorithm	sha256RSA	
Signature hash algorithm	sha256	
Issuer	winserv1a-CA, nagios, internal	
Valid from	Thursday, March 7, 2025 12:19:5	
	winserv1a-CA narios internal	-
E	dit Properties Copy to File	
	ОК	

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:	
	O 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	
	Enable certificate privacy	
	O Microsoft Serialized Certificate Store (.SST)	
	Next Canc	el

www.nagios.com



Page 5 of 12

- 9. Use the **Browse** button to select a location to save the certificate file to, and provide a name for the certificate.
- 10. Click **Next** to continue.

		Х
←	🐓 Certificate Export Wizard	
	File to Export	
	Specify the name of the file you want to export	
		-
	File name:	
	C:\Temp\CA-test.cer	
	(Next) Cance	

www.nagios.com



Page 6 of 12

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

← 🛛 & Certificate Export Wizard	×
Completing the Certificate E	xport Wizard
You have successfully completed the Certifica	ate Export wizard.
You have specified the following settings:	
File Name	C:\Temp\CA-test.cer
Export Keys	No
Include all certificates in the certification pa	th No
File Format	Base64 Encoded X.509 (*.cer)
	Finish Cancel

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 <u>Upload Certificate</u> 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	Х
The export was successful.	
ОК	



Method 2: CA Server Web Interface

If the CA server publishes the Certificate Services web page, you can download the CA certificate directly from there.

1. Navigate to http://<caservername>/certsrv. Replace <caservername> with the address of your CA server. Provide valid credentials when prompted. You will be presented with a page similar to this screenshot.



- 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.



www.nagios.com



Page 8 of 12

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.

v	Opening certnew.cer ×
You have ch	losen to open:
2 certnev	w.cer
which is from: ht	: X.509 certificate (1.9 KB) tp://dc02
What shou	Id Firefox do with this file?
○ <u>O</u> pen	with Geany (default)
○ O <u>p</u> en	in browser as Text 🔹
© <u>S</u> ave	File
🗆 Do thi	is <u>a</u> utomatically for files like this from now on.
	Cancel OK

Proceed to the <u>Upload Certificate</u> section of this document. Make sure you have access to the exported .cer file from the computer you will use to upload the certificate to Nagios Fusion.

Obtaining The Certificate - LDAP Server

There are many implementations of LDAP servers, making it difficult to document the exact location of your CA certificate file. 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 the location of the CA certificate file in the output. In the <u>Upload Certificate</u> 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

Proceed to the Upload Certificate section of this document.

www.nagios.com



Page 9 of 12

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 similar to this screenshot.
- 2. Select all of the text (**Ctrl** + **A**) and copy (**Ctrl** + **C**) it to your clipboard.

Make sure to include the

----BEGIN CERTIFICATE---- and

-----END CERTIFICATE----- lines.

MIIFazCCA10gAwIBAgIQRKee45LY7JtEa3Z9QmbKpjANBgkqhkiG9w0BAQUFADBI MRUWEWYKCZImiZPyLGQBGRYFbG9jYWwxFjAUBgoJkiaJk/IsZAEZFgZCT1gyOTMx FzAVBgNVBAMTDkJPWDI5My1EQzAyLUNBMB4XDTE2MDcwNjA5MzQyNFoXDT12MDcw NjA5NDQyM1owSDEVMBMGCgmSJomT8ixkARkWBWxvY2FsMRYwFAYKCZImiZPyLGQB GRYGQk9YMjkzMRcwFQYDVQQDEw5CT1gy0TMtREMwMi1DQTCCAiIwDQYJKoZIhvcN AQEBBQADqqIPADCCAqoCqqIBAMhqx1/3sYSB9LqcWiHG5fjQ9sd+wwlXYWPTqxAz 5F+CacNIIHvYDuwAOTzlZLCO8VvHymMOMRfF1/Vro6JZB2IXBMXuRfMrxoSErudq WniuFNdAp/cRHNHu6WDJ1h4UwAitNpmxIbGSK9DquSYzfQc1RzsGDDJVB05vmjg NcYtPX3N2EYd7fn2vn1GuxYfV9d+qg/PFJIw0kVuib3L4ifIG86naCEc3RrDz6k2 /6wbgf034+wziXTcEezvpxvvofDg2LhYbDA8+rFP5GJU0lH0khAWv45209VT3gsG PSQVP2td9opWf4mPxB0Dz7o1z6I8eGItdQoBwwOy+ki/Uu5/tGWQjcFd/5Nf/83L 0fmTahtGX80DvYfU5HXKtc4kggGVL4akjTaQrryNgd30RnioesBcdKrKes+6brAM w1HHQGp6EK8xoH/tfRbpef0DqP9NEFJHwzBxwHWRG7zT/ivkp/E/WBX0yISMdlJV lNPkf6ur2E2Zi1KtdokRtHIea0S38flnyNwApXwnikaQDhioOdgbjDHvwhf7KODQ 3hjDXBnCImHDNqDikv4NiJ94jVOyyOK3q6b/XCI19+hWNNqv6m3As/Wv12zUWeCY Wni93w9nzVTuKRSFlJqmKsKSAbu82HdVBHQKCM3Hm/3/cLq9+A+1ukYTcRm5/Ocb TkcrAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1Ud DaOWBBT0uvFW8isRFVa8Y6wx1Lbu0XhoVDA0BakrBaEEAYI3F0EEAwIBADANBaka hkiG9w0BAQUFAAOCAgEAcHY2bSjlHDVWxzt93rRGK/LfWvVPyZh/4gUKRmYyGrkV 2w2ARBulfd3Fch8nzaFsx+LVZtfJUZTjsKIMFGn09vHukMbCCoIMBn2GH2w30N9F SHSbrjvlMkClv0LeoJumTRx1mKYKhFFgLKD9Ma4T7XpICDURhH8W/RiAYA0IA9b3 F0e2qVhPXMBxv3/iK8qlicArfLoqNgha0GPcnDYEUvp5YPSUKu97cBH+ZVQfm40j VCkd0Z3vMtaEclhRSl+VfPlzVEjRhDjDzyf7VMC1jeTnGrbpkc2lDQJWeWcM25o VqyeBKnR9FaV0tJ+1wD0QozKzVmzf8DWpEGgEKL9ĺt3lMaT9la3ilPcvbobHD1Rl pyRlyZp7fmocz1X6i6xZldH9zd5oXjGEV4sBU/AkV6hiEZaZohXVR2xhnJt0rAZP co9kfXQaMQNE3cpnnKEvslfWxmTDoPf0+EeaqUYlPh0f8k0KF3iXZfo1i5kKCQk+ GE0jXeFo8KJyewq4yF0dq7vFlJzFRdf0Lb4z11BA88sPARUscdI2ooocxK/8nf3M TmYKLh/s+4i+3aaMRj0tpB9hIrk8C2gute4Rl+0/6mPDvUced0icqMI+Bh+Q688V /QxbAST1jfku+418VWbVNZVT0dxonuaxiCvqI+uAWHbAwZqXF21peJoKYctfNjE= -----END CERTIFICATE--

---BEGIN CERTIFICATE---

- 3. Open Nagios Fusion and navigate to Admin > Users > LDAP/AD Integration.
- 4. Click the Add Certificate button.

Authentication servers Once a server has bee	can be used to authenticate added you can import us	e users over on lagin. ers.		
Add Authentication	Server			
Server(s)	Туре	Encryption	Associated Users	Actions
There are currently n	o LDAP or AD servers to au	thenticate against.		
Certificate Authori	ty Management SL/TLS using self-signed cer	tificates you will need to add the	e certificate(s) of the	
Certificate Authori for connecting over SS fomain controller(s) to host other than itself Add Certificate	ty Management SL/TLS using self-signed cer o the local certificate author , that certificate authority/h	tificates you will need to add the ity so they are trusted. If any ce ost certificate needs to be added	e certificate(s) of the rtificate was signed by d.	

www.nagios.com



Page 10 of 12

- 5. The Add Certificate to Certificate Authority window will appear.
- 6. Paste the text in your clipboard into the **Certificate** field. The formatting may look different from the text editor, but this is expected.
- 7. Once pasted, the Hostname field will automatically populate with the CA name.
- 8. Click the Add Certificate button to finish uploading this certificate to Nagios Fusion.

certificate between, and in	icluding, the begin/end certificate sections.	
Hostname		
BOX293-DC02-CA		
Certificate		
F0e2qVhPXMBxv3 /iK8qlicArfLoqNgha0G VCkd0Z3vMtaEclhRSl+V M25os VqyeBKnR9FaV0tJ+1wD0 HD1Rl pyRlyZp7fmocz1X6i6xZ /AkV6hiEZaZohXVR2xhn co9kfXQaMQNE3cpnnKEv KC0k+ GE0jXeFo8KJyewq4yF0d /8nf3M TmYKLh/s+4i+3aaMRj0t /6mPDvUced0icqMI+Bh+ /0xbAST1jfku+418VWbV fNjE=	PcnDYEUvp5YPSUKu97cBH+ZVQfm40j fPlzVEjRhDjDzyf7VMCljeTnGrbpkc2lDQJWeWc QozKzVmzf8DWpEGgEkL9lt3lMaT9la3ilPcvbob ldH9zd5oXjGEV4sBU Jt0rAZP slfWxmTDoPf0+EeaqUYlPh0f8k0KF3iXZfoli5k q7vFlJzFRdf0Lb4z11BA88sPARUscdI2ooocxK pB9hIrk8C2gute4Rl+0 QG88V NZVT0dxonuaxiCvqI+uAWHbAwZqXF2lpeJoKYct	0

9. Once the certificate is uploaded, it will appear in the list of certificates in the **Certificate Authority Management** section.

Certificate Autho	ority 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 Apr 26 2027 10:10:03 GMT+1000 (AUS Eastern Standard Time)	×		

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 <u>Authenticating and Importing Users with AD and LDAP</u> documentation.

The following screenshot shows the Security setting that requires authentication to use SSL/TLS with certificates.



You do not actually define which CA certificate is used. When Nagios Fusion is presented with a certificate from the LDAP/AD server, 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 and LDAP in Nagios Fusion. 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

www.nagios.com



Page 12 of 12