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

Target Audience
This document is intended for use by Nagios XI Administrators that require secure LDAP / AD connectivity. You may already have the LDAP / AD Integration configured in Nagios XI, 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 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 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
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 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 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.

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 XI 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 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.
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 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.

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

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 XI.

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

This completes uploading the certificate to Nagios XI.
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, the Nagios XI 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 XI. If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

[https://support.nagios.com/forum](https://support.nagios.com/forum)

The Nagios Support Knowledgebase is also a great support resource:

[https://support.nagios.com/kb](https://support.nagios.com/kb)