



## Purpose

This document describes how to integrate Nagios Fusion with Active Directory (AD) or Lightweight Directory Access Protocol (LDAP). This allows user authentication and validation through the Nagios Fusion interface. This is helpful for system administrators by simplifying user management of large infrastructures and standardize credentials needed for Nagios Fusion by allowing users to authenticate with AD/LDAP credentials when logging into the system.

## Target Audience

This document is intended for use by Nagios Administrators who want to allow users to authenticate with their AD/LDAP credentials when logging into Nagios Fusion.

## 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

## Nagios Fusion DNS Resolution

It is assumed that the DNS settings for your Nagios Fusion server use DNS servers that are:

- Domain Controllers (DC) in your AD domain
  - OR
- Capable of resolving the DNS entries used to contact your LDAP server(s)

If you are having issues you can edit the `resolv.conf` file to use a DNS server within the AD infrastructure as the primary name server.

- Edit the `resolv.conf` file in a text editor:
  - `vi /etc/resolv.conf`
- Before all other lines starting with `nameserver`, enter the following:
  - `nameserver [IP address of DNS server]`

Caching options in PHP may prevent changes to the `resolv.conf` from taking effect and require restarting the Apache service. If you do edit the file, you will need to restart the Apache web server:

### RHEL7 | CentOS 7 | Oracle Linux 7

```
systemctl restart httpd.service
```

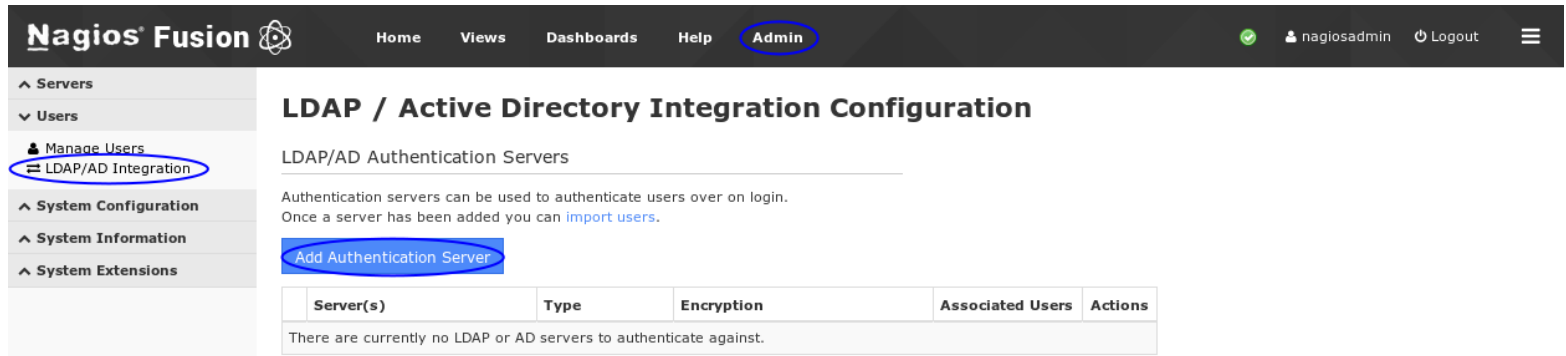
### Debian | Ubuntu 16/18

```
systemctl restart apache2.service
```

Be aware that the `/etc/resolv.conf` file can be automatically overwritten by the networking stack in RHEL / CentOS. Please consult the RHEL / CentOS documentation for more information on correctly configuring the DNS servers for Linux.

## Configuring The Authentication Servers

First you must configure the Authentication Server(s) that Nagios Fusion will use. Navigate to **Admin > Users > LDAP/AD Integration**.



**Nagios Fusion** Home Views Dashboards Help **Admin** 🟢 👤 nagiosadmin 🔌 Logout ☰

^ Servers  
v Users  
👤 Manage Users  
**LDAP/AD Integration**  
^ System Configuration  
^ System Information  
^ System Extensions

### 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.				

To add an Authentication Server click the **Add Authentication Server** button. There are different options for [Active Directory](#) and [LDAP](#).

### Active Directory

You will need to provide the following details:

Enable this authentication server: **Checked**

Connection Method: **Active Directory**

Base DN:

An LDAP formatted string where the users are located.

Example: `DC=BOX293,DC=local`

Account Suffix:

An `@your-domain.suffix` (the part of the full user identification after the username).

Example `@BOX293.local`

Domain Controllers:

A comma separated list of DC servers that Nagios Fusion can use to authenticate against. This can be a combination of IP addresses, short names, and fully qualified domain names.

**Note:** When using SSL or TLS for security, it is important that these entries match the Common

Name (CN) in the SSL/TLS certificate that these DCs will present to Nagios Fusion.

Example: `dc01.box293.local,dc02.box293.local`

Security:

Select the security method (or not) to use. This guide will choose **None**.

If you are in a domain forest that has been raised to a functional level of 2012, then TLS is needed along with additional steps in the following guide: [Using SSL with AD and LDAP](#).

If SSL or TLS is required then please refer to the same guide.

Once completed click the **Save Server** button.

You can now proceed to the [Importing Users](#) section.

Authentication Server Settings

Enable this authentication server

Connection Method:    
Use either LDAP or Active Directory settings to connect.

Base DN:    
The LDAP-format starting object (distinguished name) that your users are defined below, such as **DC=nagios,DC=com**.

Account Suffix:    
The part of the full user identification after the username, such as **@nagios.com**.

Domain Controllers:    
A comma-separated list of domain controllers on your network.

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

## LDAP

You will need to provide the following details:

Enable this authentication server: **Checked**

Connection Method: **LDAP**

Base DN:

An LDAP formatted string where the users are located.

Example: `dc=box293,dc=local`

LDAP Host:

The LDAP server that Nagios Fusion can use to authenticate against. This can be an IP address, short name or fully qualified domain name.

**Note:** When using SSL or TLS for security, it is important that this entry matches the Common Name (CN) in the SSL/TLS certificate that this LDAP server will present to Nagios Fusion.

Example: `ldap01.box293.local`

#### LDAP Port:

The TCP network port used to communicate with the LDAP server.

Example: `389`

#### Encryption Method:

Select the security method (or not) to use. This guide will choose **None**.

If SSL or TLS is required then please refer to the [Using SSL with AD and LDAP](#) documentation.

Once completed click the **Save Server** button.

You can now proceed to the [Importing Users](#) section.

#### Authentication Server Settings

Enable this authentication server

**Connection Method:**    
Use either LDAP or Active Directory settings to connect.

**Base DN:**    
The LDAP-format starting object (distinguished name) that your users are defined below, such as **DC=nagios,DC=com**.

**LDAP Host:**    
The IP address or hostname of your LDAP server.

**LDAP Port:**    
The port your LDAP server is running on. (Default is 389)

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

## Importing Users

The next step is to import users from Active Directory or LDAP. Once the user has been imported, Nagios Fusion will query the DCs or LDAP server each each time the user logs in to validate credentials. The following steps are the same for Active Directory or LDAP.

Navigate to **Admin > Users > Manage Users** and click the **Add User From AD/LDAP** button.

The screenshot shows the Nagios Fusion Admin interface. The top navigation bar includes Home, Views, Dashboards, Help, and Admin (circled in blue). The left sidebar shows a tree view with Servers, Users, Manage Users, LDAP/AD Integration (circled in blue), System Configuration, System Information, and System Extensions. The main content area is titled 'Manage Users' and contains two buttons: 'Add New User' and 'Add User From AD/LDAP' (circled in blue). Below the buttons is a table with one user entry:

Username	Name	Email	Authentication Type	Actions
nagiosadmin	Nagios Administrator	root@localhost	Local	

Below the table, there are pagination controls showing 'Page 1 of 1' and '10 Per Page'. At the bottom, it says 'With Selected: 

Select the authentication server(s) you previously defined and provide credentials to connect to the server(s).

The account credentials you are providing here are only required to authenticate against AD / LDAP to retrieve the directory contents. They are not saved or used in the actual user authentication.

Click **Next**.

### LDAP / Active Directory Import Users

Log into your LDAP / Active Directory administrator or privileged account to be able to import users.

Username

Password

Active Directory - dc01.box293.local

[Next >](#)



Once you've successfully authenticated, you'll be presented with the node of your directory tree (*relative to the Base DN that was defined*).

In the screenshot to the right you can see the Users node has been selected.

The user **John Smith** has been selected to import and you can see it summarizes this at the top of the screen.

When you've chosen all the users to import, click the **Add Selected Users** button.

### LDAP / Active Directory Import Users

Select the users you would like to give access to Nagios XI via LDAP/AD authentication. You will be able to set user-specific permissions on the next page.

#### Select Users to Import from LDAP/AD

1 users selected for import: **john.smith**

The screenshot shows the 'LDAP / Active Directory Import Users' interface. On the left, a directory tree is visible with 'Users' selected. The main area displays a list of users with checkboxes for selection. 'John Smith (john.smith)' is the only user selected. At the bottom, there is a blue button labeled 'Add Selected Users'.

### LDAP / Active Directory Import Users

Set the preferences and security settings for all users that will be imported. You can also edit multiple user's preferences/security settings at once by checking the users you want to edit and selecting the action from the dropdown.

In order to finish importing you **must select the preferences and security settings for all users**. For quicker creation, select users with checkboxes and use the dropdown to set the preferences and security settings for multiple users at once.

<input type="checkbox"/>	Username	Display Name	Email	Preferences	Security Settings
<input type="checkbox"/>	john.smith	John Smith		<input type="radio"/> Edit	<input type="radio"/> Edit

Edit multiple ...

Cancel Import >

Every user can have the following Preferences and Security Settings defined:

### Preferences ✕

**Create as Monitoring Contact:**

**Language:**

**Date Format:**

**Number Format:**

### Security Settings ✕

**Authorization Level:**

**Has API access:**

**Allow local authentication:**

Every user will need their preferences and security settings defined. When importing multiple users you can define the same settings for a selection of users following these steps:

In the left pane check the boxes for the users you want to define the same settings for

At the bottom of the user list there is a drop down list called **Edit multiple ...**

Click the list and select **Preferences** or **Security Settings**

You will be presented with the appropriate popup window

Define the required options and then click **Save** when done

ALL users being imported will require the Preferences and Security Settings to have a tick appear in the respective columns. Once all the required options have been defined the Import button will be able to be clicked.

Click **Import** to continue.

<input type="checkbox"/>	Username	Display Name	Email	Preferences	Security Settings
<input checked="" type="checkbox"/>	<input type="text" value="john.smith"/>	<input type="text" value="John Smith"/>	<input type="text" value="john.smith@box293.local"/>	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Edit
Edit multiple ... <input type="text"/>					
<input type="button" value="Cancel"/>		<input type="button" value="Import &gt;"/>			



The user accounts will now be imported into Nagios Fusion. When finished you will be informed that it was successful.

This completes importing users into Nagios Fusion from AD/LDAP.

## LDAP / Active Directory Import Users

Successfully added 1 users.

Log into your LDAP / Active Directory administrator or privileged account to be able to import users.





Once imported the users will appear on the **Admin > Users > Manage Users** page and their authentication method will be indicated in the **Authentication Type** column.

**Nagios Fusion** Home Views Dashboards Help Admin 🟢 nagiosadmin Logout

^ Servers  
v Users  
Manage Users  
LDAP/AD Integration  
^ System Configuration  
^ System Information  
^ System Extensions

### Manage Users

Page 1 of 1 10 Per Page

<input type="checkbox"/>	Username	Name	Email	Authentication Type	Actions
<input type="checkbox"/>	nagiosadmin	Nagios Administrator	root@localhost	Local	
<input type="checkbox"/>	john.smith	John Smith	john.smith@box293.local	Active Directory	

Page 1 of 1 10 Per Page

With Selected:

## Linking Existing Nagios Fusion Users to Active Directory Users

If you already have Nagios Fusion users that have been created, you can easily link these local accounts to Active Directory accounts.

Navigate to **Admin > Users > Manage Users**.

Click the **Edit** link for the user you want to update, the settings are under the **Authentication Settings** section:

Auth Type: **Active Directory**

AD Server: Select the authentication server(s) you previously defined

AD Username:

Type the username for this user as it is configured in Active Directory

Example: `jane.doe`

Allow local login if auth server login fails:


By checking this box you will allow the user to use the local password created for this user (if the password is not blank) when the authentication server cannot be connected to, times out, or the password provided is incorrect. This allows a secondary means of authentication in case the authentication server is unreachable.

Click the **Update User** button to save the changes.

Here is a screenshot of the user settings described above:

Once these changes have been made, the existing Nagios Fusion user will be able to login using their Active Directory credentials.

### Authentication Settings

<b>Auth Type:</b>	Active Directory <input type="text"/>
<b>AD Server:</b>	dc01.box293.local <input type="text"/>
<b>AD Username:</b>	jane.doe <input type="text"/>
	<input type="checkbox"/> Allow local login if auth server login fails 

## Linking Existing Nagios Fusion Users to LDAP Users

If you already have Nagios Fusion users that have been created, you can easily link these local accounts to LDAP accounts.

Navigate to **Admin > Users > Manage Users**.

Click the **Edit** link for the user you want to update, the settings are under the **Authentication Settings** section:

Auth Type: **LDAP**

LDAP Server: Select the authentication server you previously defined

Users Full DN:

Type the full distinguished name (DN) for this user as it is defined in LDAP

Example: `uid=bobsmith,ou=People,dc=box293,dc=local`

Allow local login if auth server login fails:

By checking this box you will allow the user to use the local password created for this user (if the password is not blank) when the authentication server cannot be connected to, times out, or the password provided is incorrect. This allows a secondary means of authentication in case the authentication server is unreachable.

Click the **Update User** button to save the changes.

Here is a screenshot of the user settings described above:

### Authentication Settings ?

Auth Type:

LDAP

LDAP Server:

ldap01.box293.local

User's Full DN:

uid=bobsmith,ou=People,dc=box293,dc=local

Allow local login if auth server login fails ?

Once these changes have been made, the existing Nagios Fusion user will be able to login using their LDAP credentials.

## LDAP Account Requirements

The following details demonstrate the required object classes and attributes that need to exist for an LDAP user. If these attributes do not exist it is likely that they will not appear in the list of users when performing an import from your LDAP server.

```
dn: uid=bobsmith,ou=People,dc=box293,dc=local
givenName: Bob
sn: Smith
cn: Bob Smith
uidNumber: 10004
gidNumber: 10004
mail: bobsmith@box293.local
homeDirectory: /home/bobsmith
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
```

## Finishing Up

This completes the documentation on how integrate Nagios Fusion with Active Directory or LDAP to allow user authentication and validation with the Nagios Fusion interface.

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>