Authenticating and Importing Users with AD and LDAP in Nagios Fusion 2024

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

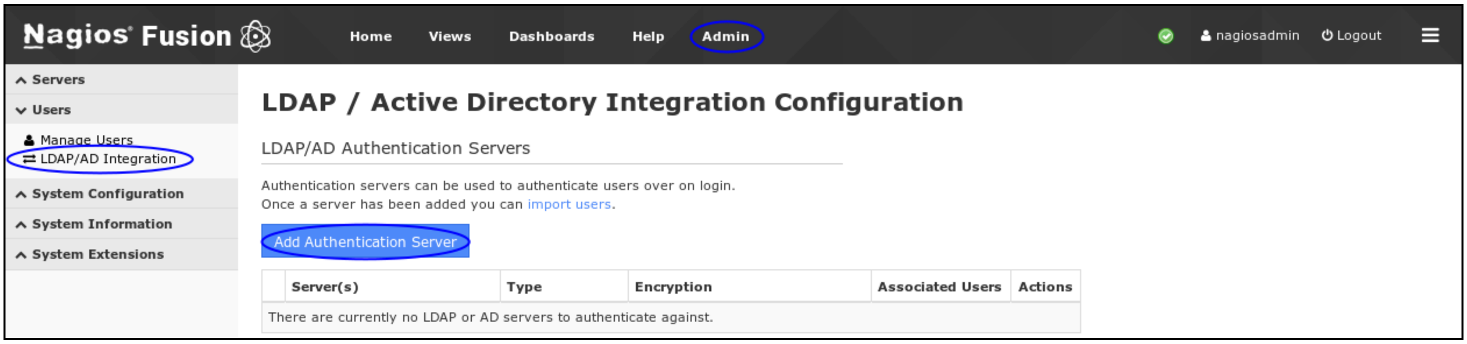
Debian | Ubuntu 20/22

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.



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.

> 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

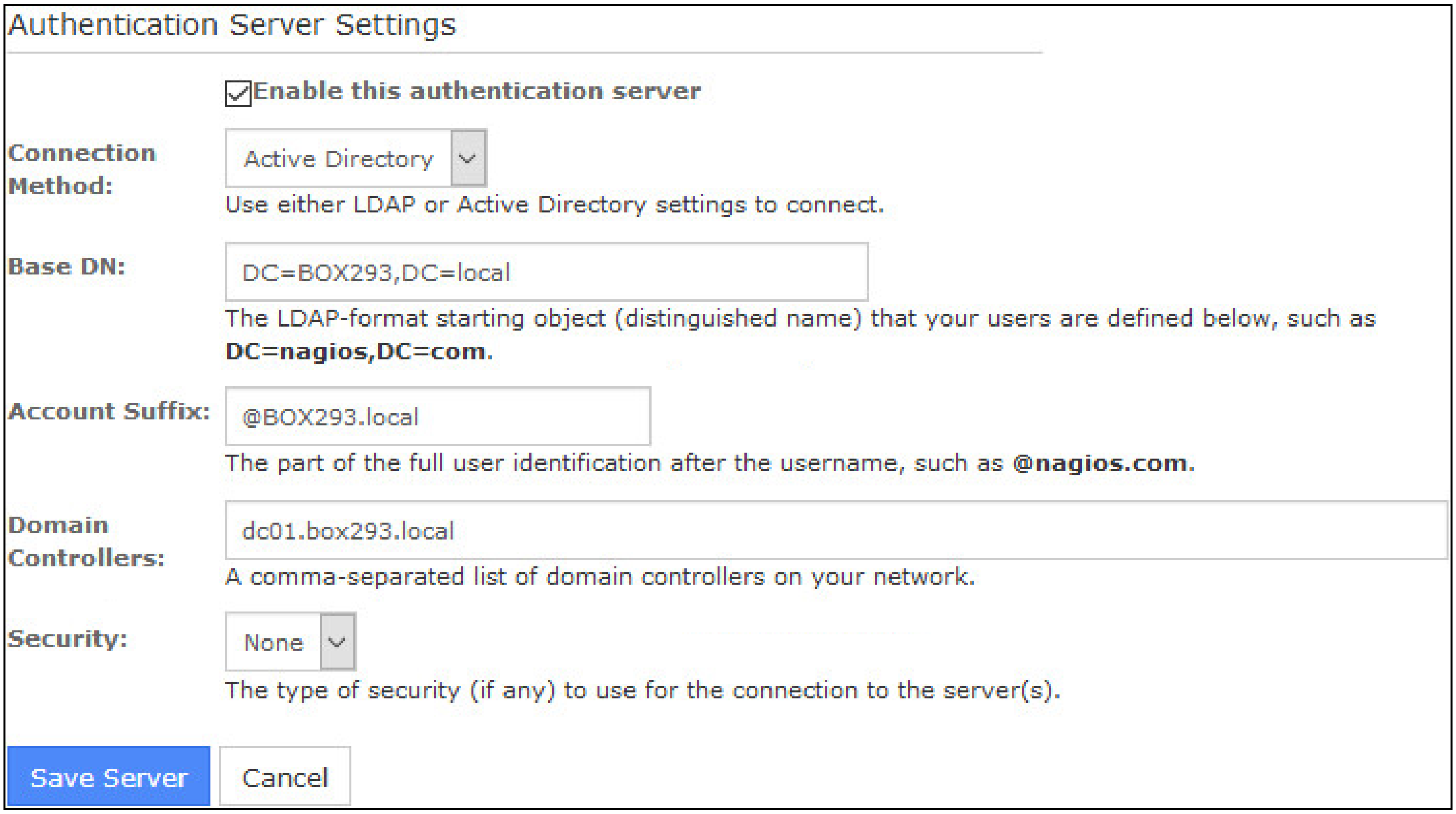
Security:

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.



Authentication Server Settings

☑ Enable this authentication server

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

Base DN: DC=BOX293,DC=local
The LDAP-format starting object (distinguished name) that your users are defined below, such as **DC=nagios,DC=com.**

Account Suffix: @BOX293.local
The part of the full user identification after the username, such as **@nagios.com.**

Domain Controllers: dc01.box293.local
A comma-separated list of domain controllers on your network.

Security: None
The type of security (if any) to use for the connection to the server(s).

Once completed click the Save Server button.

You can now proceed to the Importing Users section.

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.

> 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.

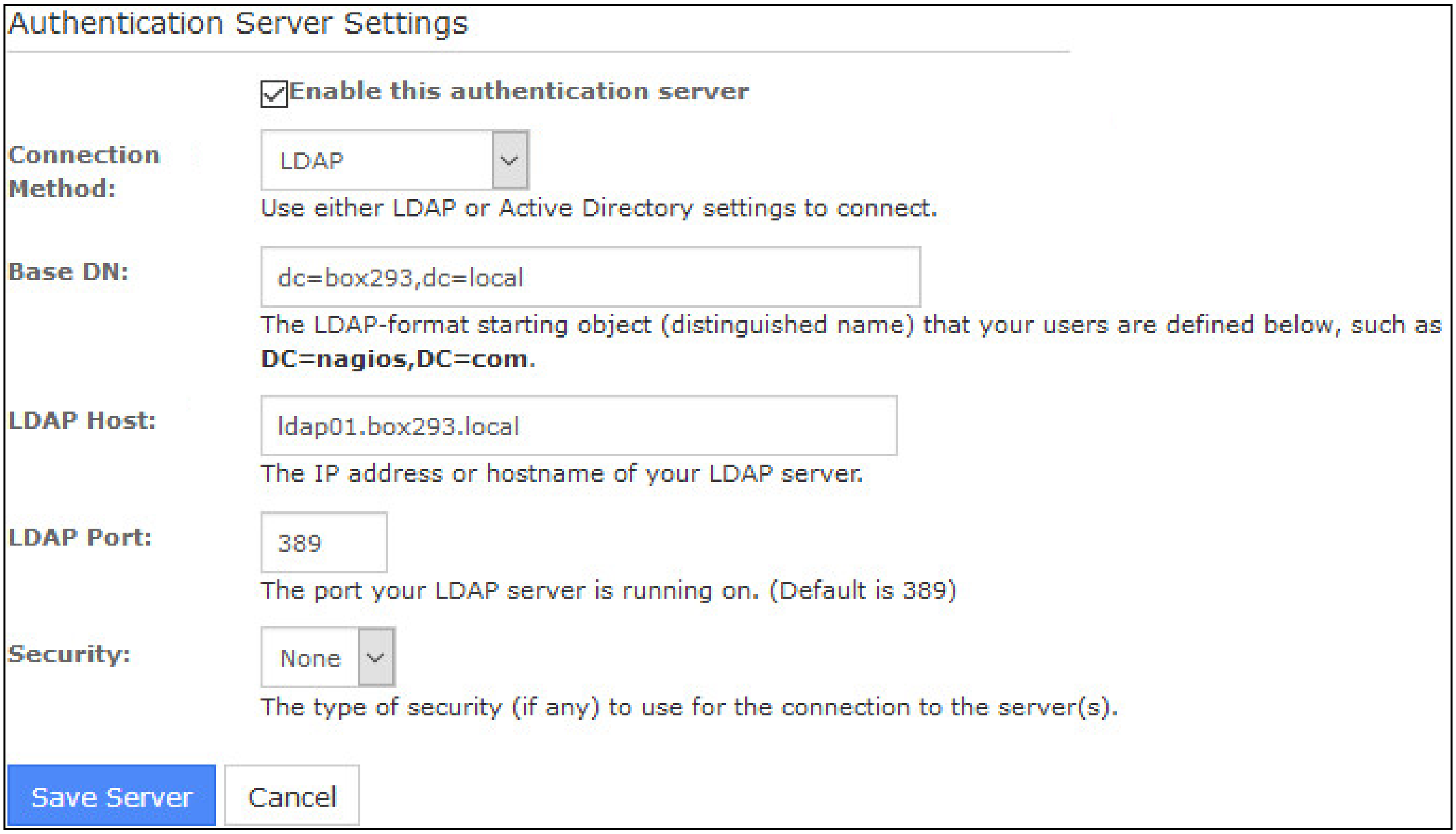
Example: 389

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.



Authentication Server Settings

☑ Enable this authentication server

Connection Method:	LDAP Use either LDAP or Active Directory settings to connect.
Base DN:	dc=box293,dc=local The LDAP-format starting object (distinguished name) that your users are defined below, such as **DC=nagios,DC=com**.
LDAP Host:	ldap01.box293.local The IP address or hostname of your LDAP server.
LDAP Port:	389 The port your LDAP server is running on. (Default is 389)
Security:	None The type of security (if any) to use for the connection to the server(s).

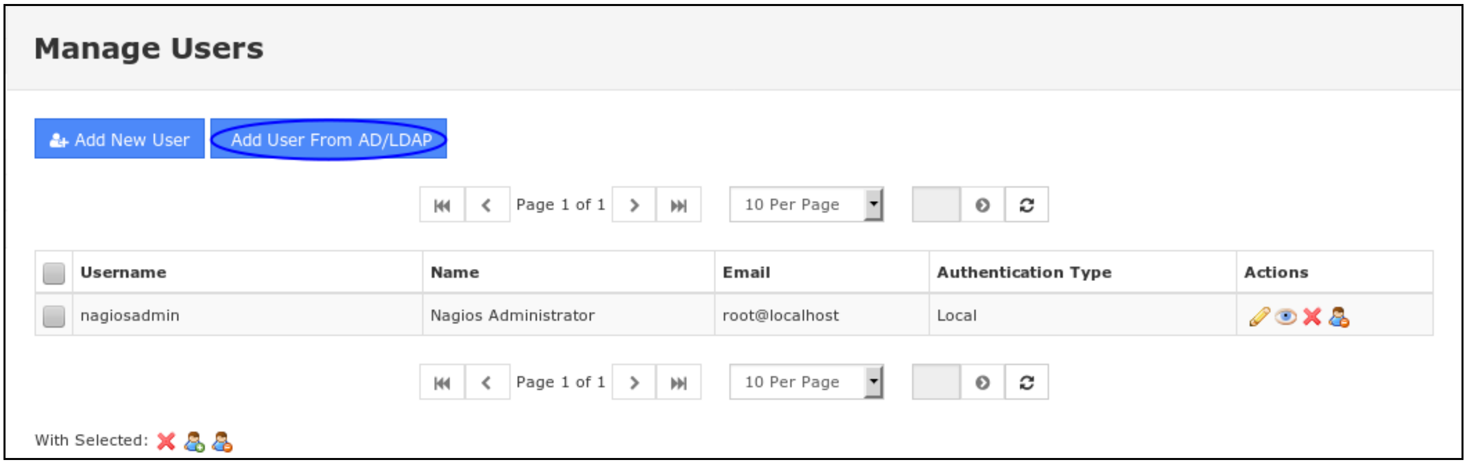
Once completed click the Save Server button.

You can now proceed to the Importing Users section.

Importing Users

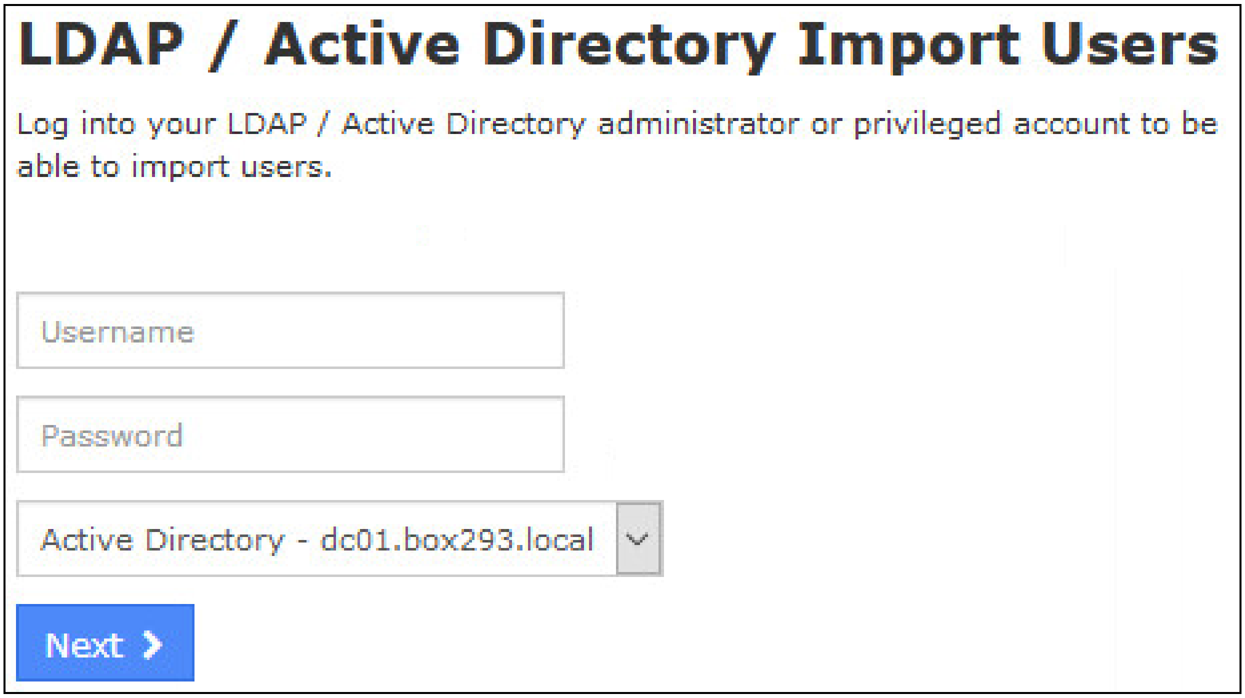
The next step is to import users from Active Directory or LDAP. Once the user has been imported, Nagios Fusion will query the DCs or LDAP server each each time the user logs in to validate credentials. The following steps are the same for Active Directory or LDAP.

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



Manage Users

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



LDAP / Active Directory Import Users

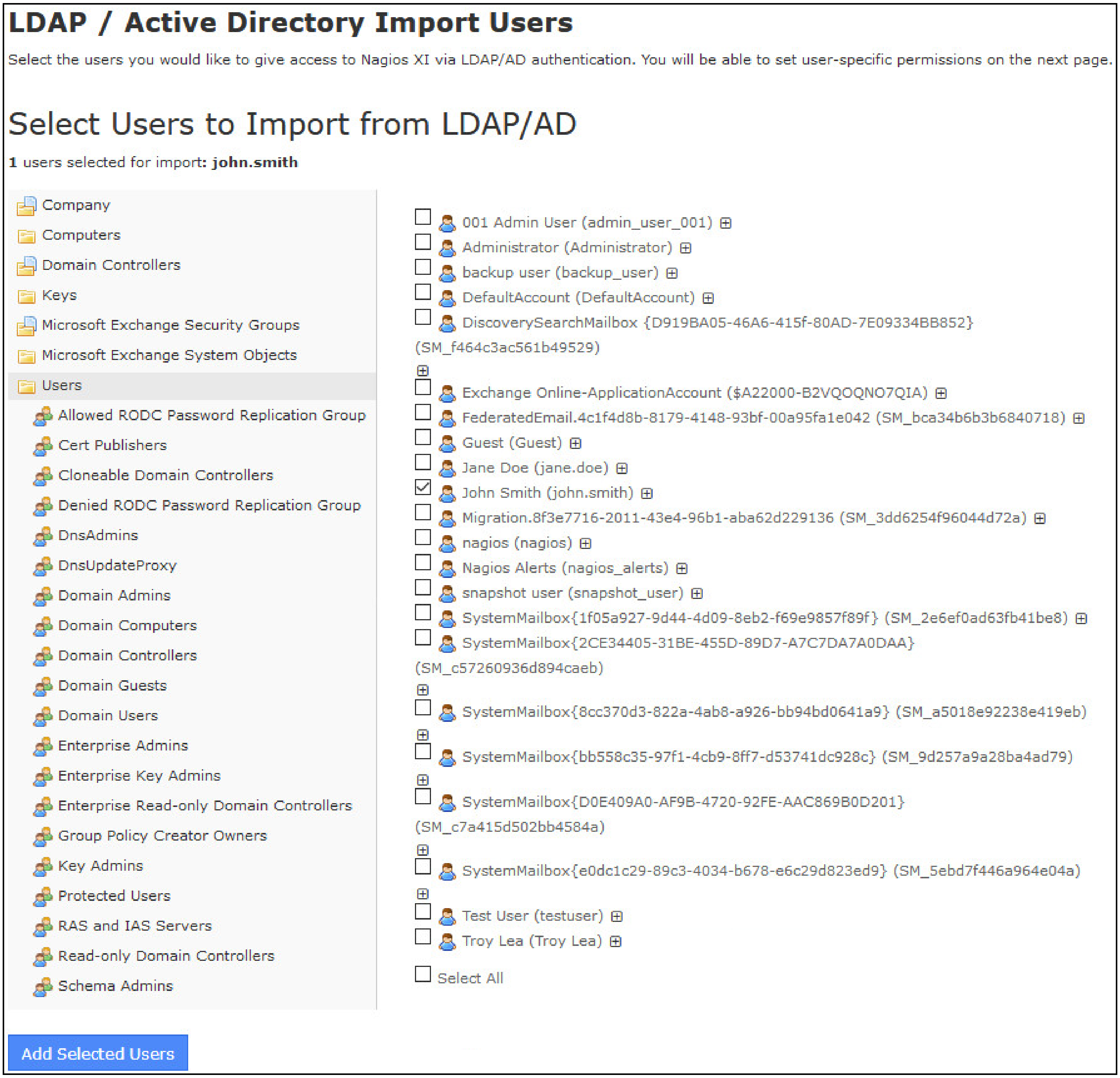
Log into your LDAP / Active Directory administrator or privileged account to be able to import users.

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

3. 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.

4. Click Next.

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



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**

- Company
- Computers
- Domain Controllers
- Keys
- Microsoft Exchange Security Groups
- Microsoft Exchange System Objects
- Users
  - Allowed RODC Password Replication Group
  - Cert Publishers
  - Cloneable Domain Controllers
  - Denied RODC Password Replication Group
  - DnsAdmins
  - DnsUpdateProxy
  - Domain Admins
  - Domain Computers
  - Domain Controllers
  - Domain Guests
  - Domain Users
  - Enterprise Admins
  - Enterprise Key Admins
  - Enterprise Read-only Domain Controllers
  - Group Policy Creator Owners
  - Key Admins
  - Protected Users
  - RAS and IAS Servers
  - Read-only Domain Controllers
  - Schema Admins

□ 001 Admin User (admin_user_001) ⊞

□ Administrator (Administrator) ⊞

□ backup user (backup_user) ⊞

□ DefaultAccount (DefaultAccount) ⊞

□ DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852} (SM_f464c3ac561b49529) ⊞

□ Exchange Online-ApplicationAccount ($A22000-B2VQOQNO7QIA) ⊞

□ FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042 (SM_bca34b6b3b6840718) ⊞

□ Guest (Guest) ⊞

□ Jane Doe (jane.doe) ⊞

☑ John Smith (john.smith) ⊞

□ Migration.8f3e7716-2011-43e4-96b1-aba62d229136 (SM_3dd6254f96044d72a) ⊞

□ nagios (nagios) ⊞

□ Nagios Alerts (nagios_alerts) ⊞

□ snapshot user (snapshot_user) ⊞

□ SystemMailbox{1f05a927-9d44-4d09-8eb2-f69e9857f89f} (SM_2e6ef0ad63fb41be8) ⊞

□ SystemMailbox{2CE34405-31BE-455D-89D7-A7C7DA7A0DAA} (SM_c57260936d894caeb) ⊞

□ SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9} (SM_a5018e92238e419eb) ⊞

□ SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c} (SM_9d257a9a28ba4ad79) ⊞

□ SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201} (SM_c7a415d502bb4584a) ⊞

□ SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9} (SM_5ebd7f446a964e04a) ⊞

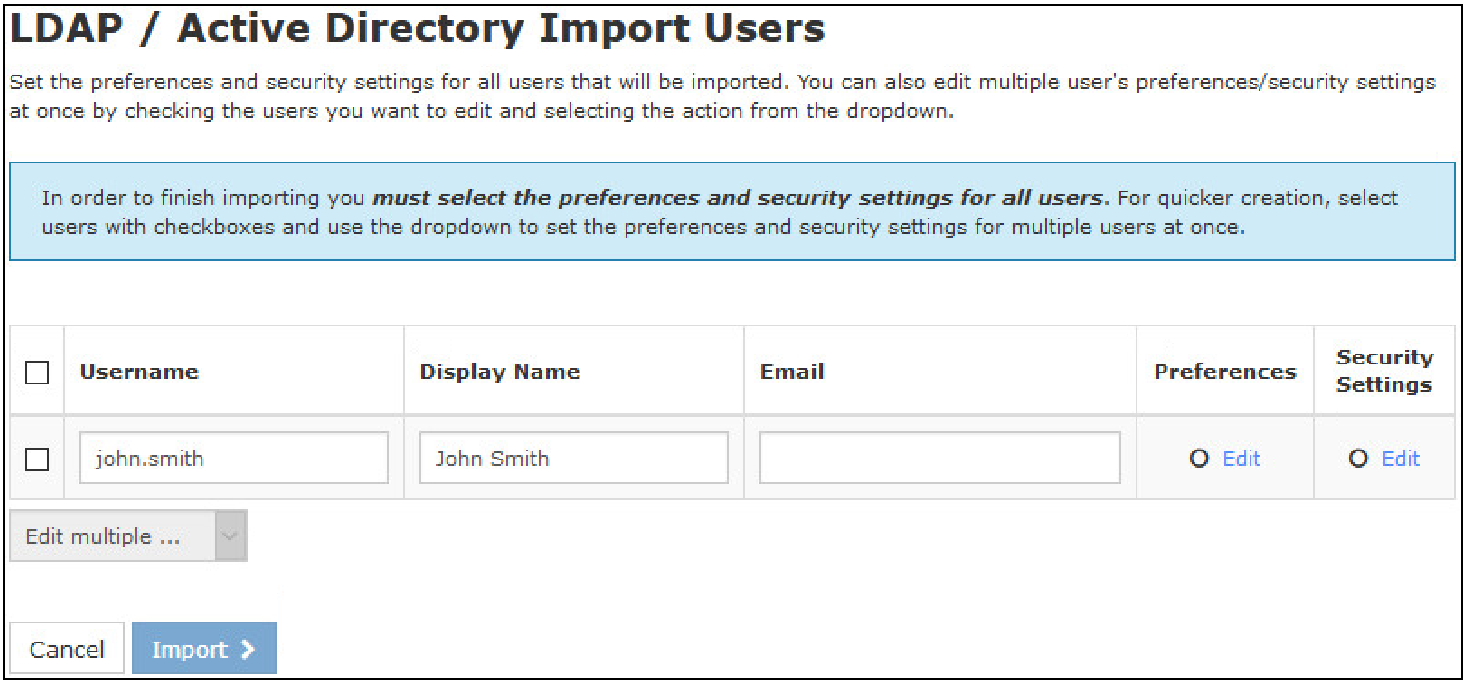
□ Test User (testuser) ⊞

□ Troy Lea (Troy Lea) ⊞

□ Select All

In the screenshot 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.

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



LDAP / Active Directory Import Users

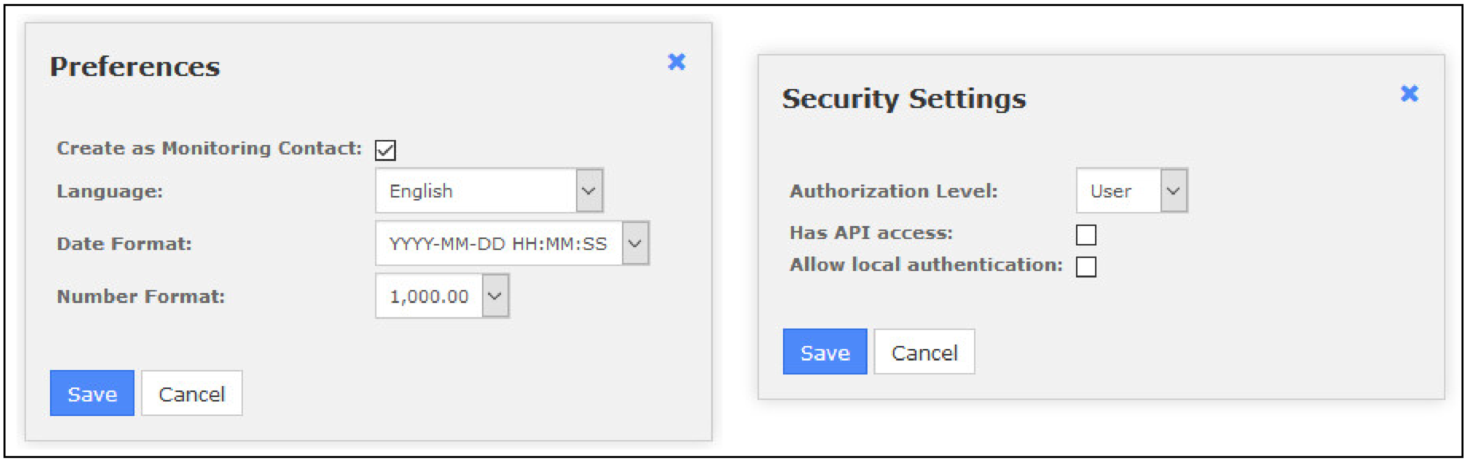
Set the preferences and security settings for all users that will be imported. You can also edit multiple user's preferences/security settings at once by checking the users you want to edit and selecting the action from the dropdown.

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.

□	Username	Display Name	Email	Preferences	Security Settings
□	john.smith	John Smith		○ Edit	○ Edit

7. On the next screen you are presented with a list of the users you are going to import and the summary of how they are going to be imported.

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



Preferences

Create as Monitoring Contact: ☑

Language: English

Date Format: YYYY-MM-DD HH:MM:SS

Number Format: 1,000.00

Security Settings

Authorization Level: User

Has API access: □

Allow local authentication: □

9. 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:

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

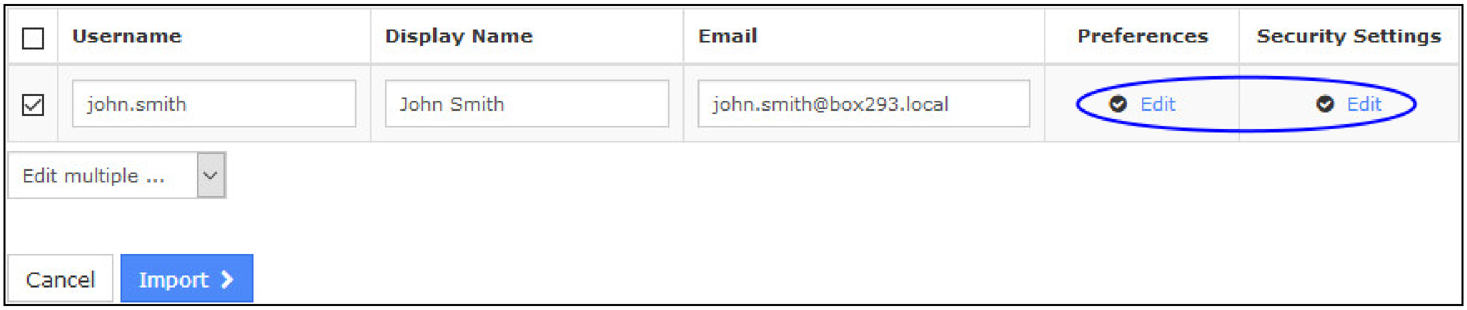
11. At the bottom of the user list there is a drop down list called Edit multiple …

12. Click the list and select Preferences or Security Settings

13. You will be presented with the appropriate popup window

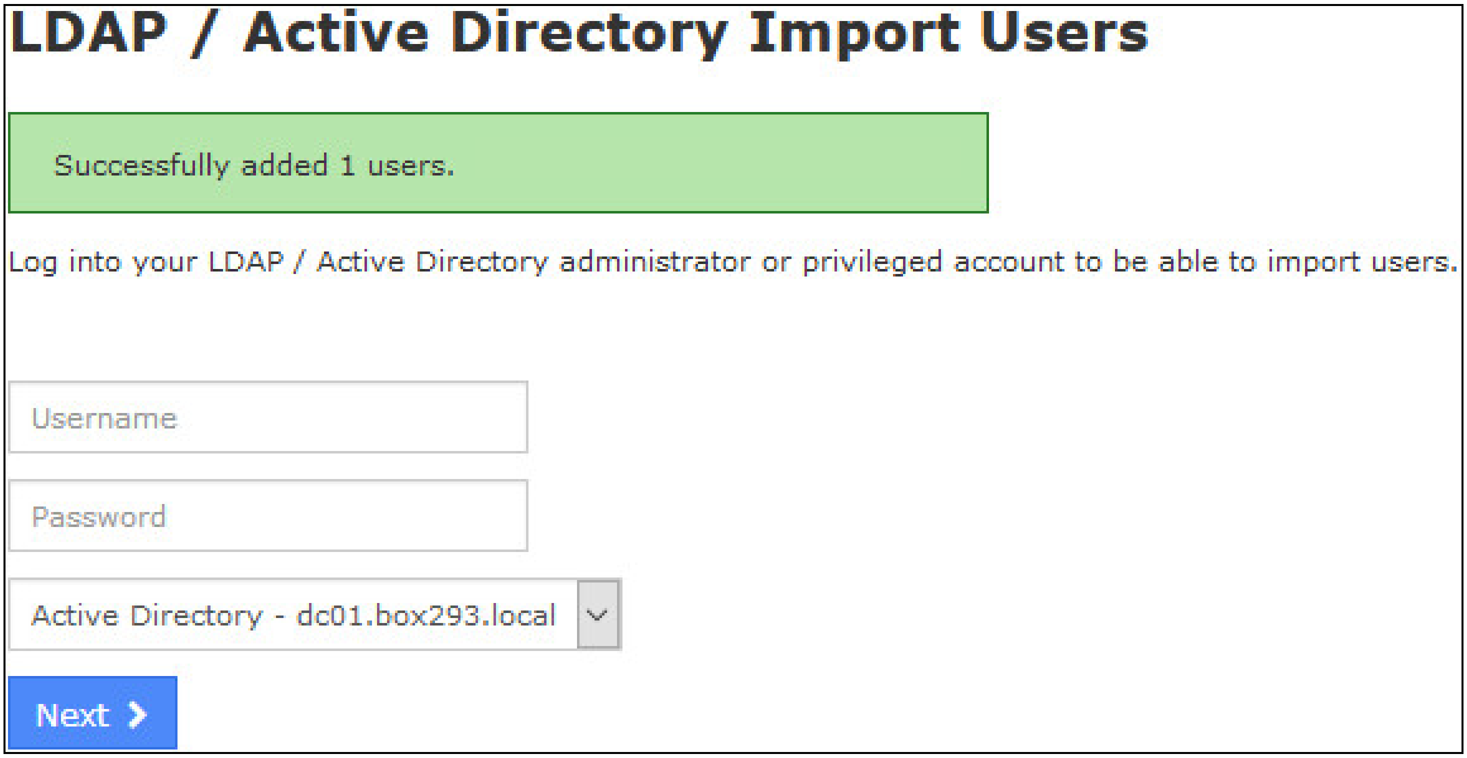
14. Define the required options and then click Save when done

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.



☐	Username	Display Name	Email	Preferences	Security Settings
☑	john.smith	John Smith	john.smith@box293.local	✓ Edit	✓ Edit

15. Click Import to continue.



LDAP / Active Directory Import Users

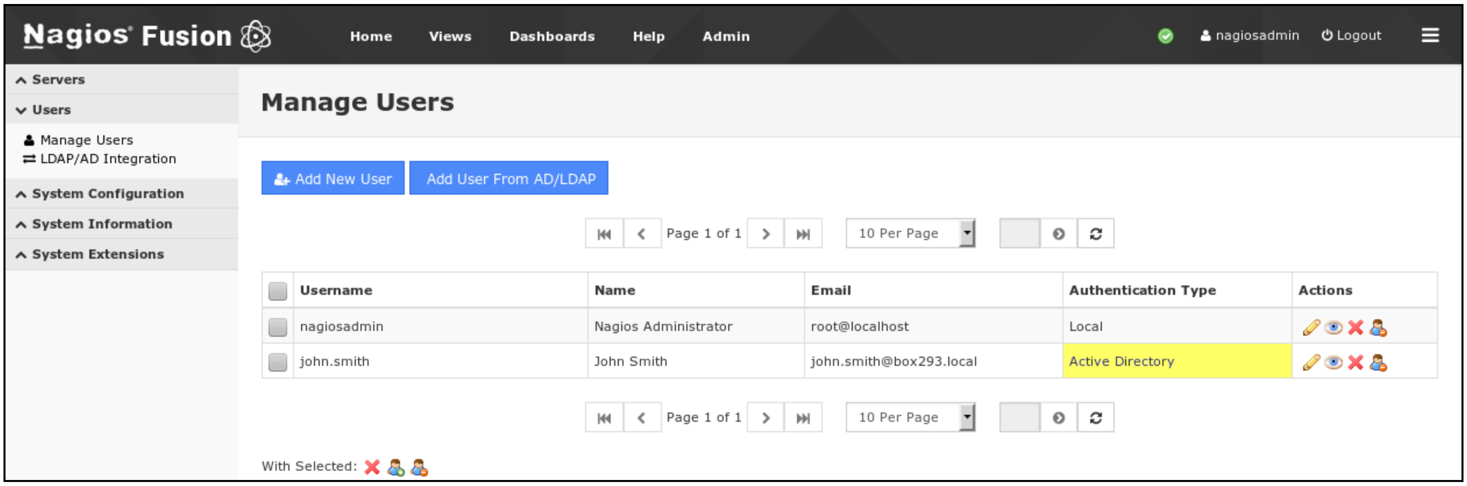
Successfully added 1 users.

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

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.

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



□	Username	Name	Email	Authentication Type	Actions
□	nagiosadmin	Nagios Administrator	root@localhost	Local	
□	john.smith	John Smith	john.smith@box293.local	Active Directory	

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.

1. Navigate to Admin > Users > Manage Users.

2. 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

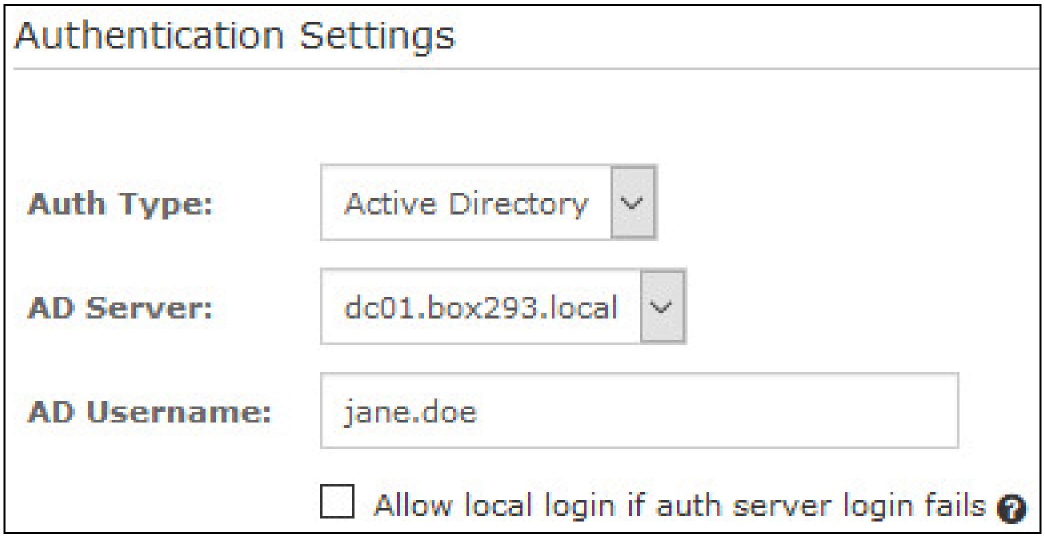
AD Username:

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.



Authentication Settings

Auth Type: Active Directory

AD Server: dc01.box293.local

AD Username: jane.doe

□ Allow local login if auth server login fails

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

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

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.

1. Navigate to Admin > Users > Manage Users.

2. 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

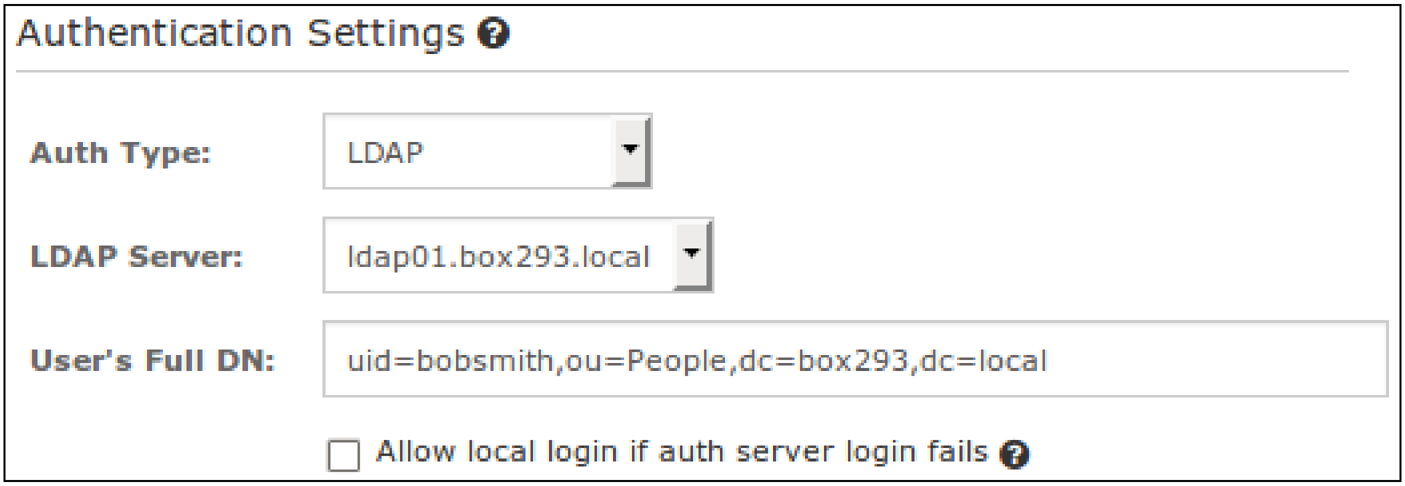
Users Full DN:

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.



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

3. 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 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
```