## Purpose

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

## Prerequisites

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

- Nagios Log Server installation
- A separate Microsoft Windows-based AD infrastructure that is accessible to the Nagios Log Server machine
    - OR
- A separate LDAP infrastructure (like OpenLDAP) that is accessible to the Nagios Log Server machine

## Cluster Considerations

Nagios Log Server is a clustered application, it consists of one or more instances of Nagios Log Server. Being a clustered application, it does not matter which instance a user connects to when logging into the web interface. With this in mind, each instance of Nagios Log Server will need to be able to communicate with the AD or LDAP servers when authenticating user credentials.

## Nagios Log Server DNS Resolution

It is assumed that the DNS settings for each of your Nagios Log Server instances 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:

**RHEL| CentOS | Oracle Linux**

```
systemctl restart httpd.service
```

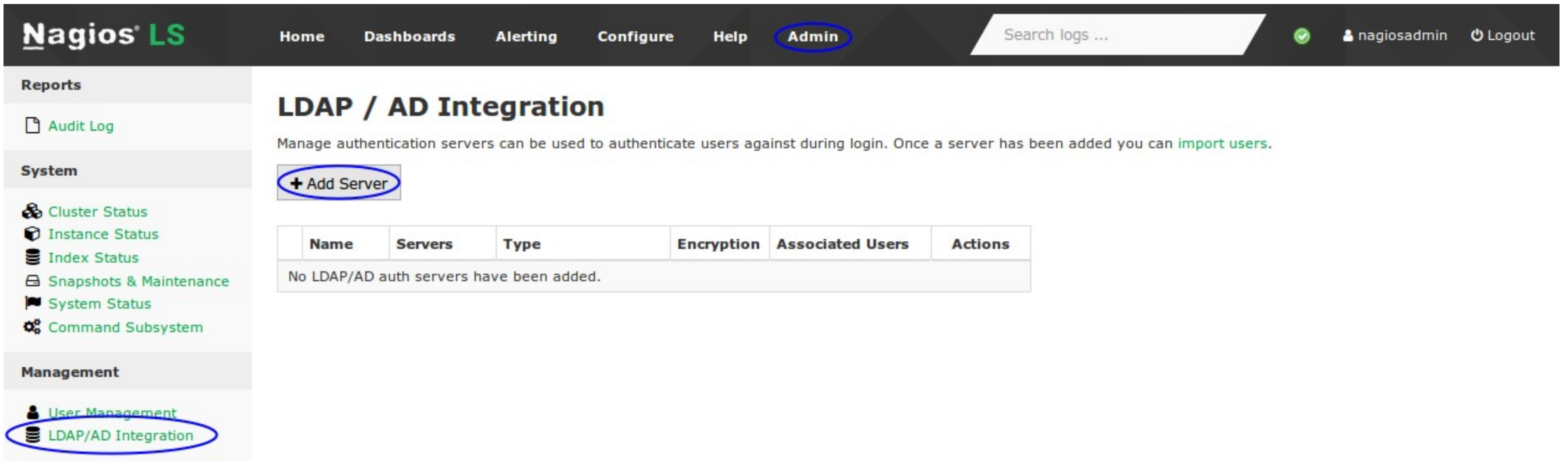
**Debian | Ubuntu**

```
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 Log Server will use. Navigate to **Admin** > **Management** > **LDAP/AD Integration**.



LDAP / AD Integration

Manage authentication servers can be used to authenticate users against during login. Once a server has been added you can import users.

| | Name | Servers | Type | Encryption | Associated Users | Actions |
|---|---|---|---|---|---|---|
| No LDAP/AD auth servers have been added. | | | | | | |

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

### Active Directory

You will need to provide the following details:

Server Type: **Active Directory**

Enabled: **Checked**

Server Name:

Provide a name to associate with this authentication method.

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 Log Server 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 the Nagios Log Server instance.

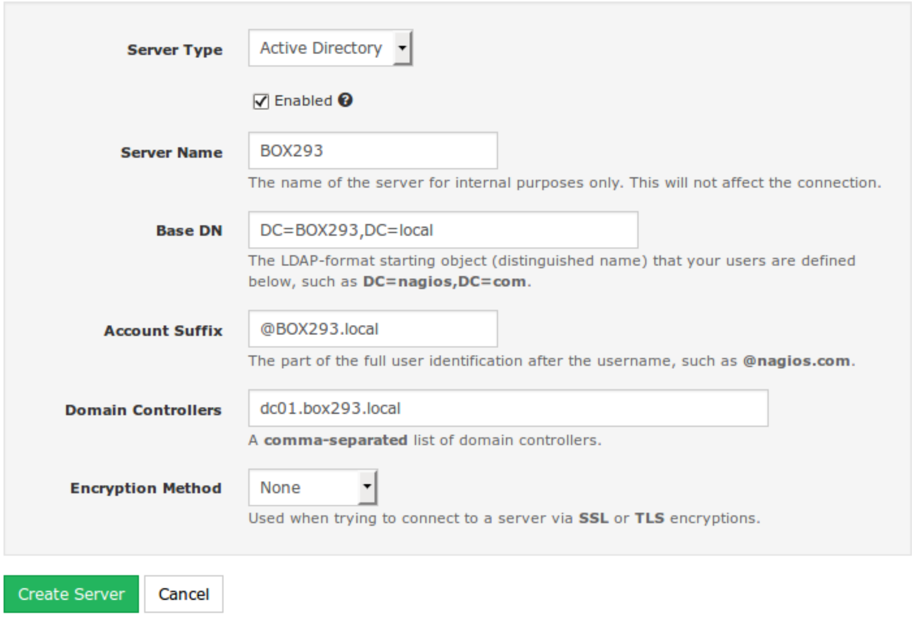
Example: `dc01.box293.local,dc02.box293.local`

Encryption Method:

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.



**Server Type** Active Directory

☑ Enabled

**Server Name** BOX293

The name of the server for internal purposes only. This will not affect the connection.

**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.

**Encryption Method** None

Used when trying to connect to a server via **SSL** or **TLS** encryptions.

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

You can now proceed to the Importing Users section.

## LDAP

You will need to provide the following details:

Server Type: **LDAP**

Enabled: **Checked**

Server Name:

Provide a name to associate with this authentication method.

Base DN:

An LDAP formatted string where the users are located.

Example: `dc=box293,dc=local`

LDAP Host:

The LDAP server that Nagios Log Server 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 the Nagios Log Server instance.

Example: `ldap01.box293.local`

LDAP Port:

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

Example: `389`

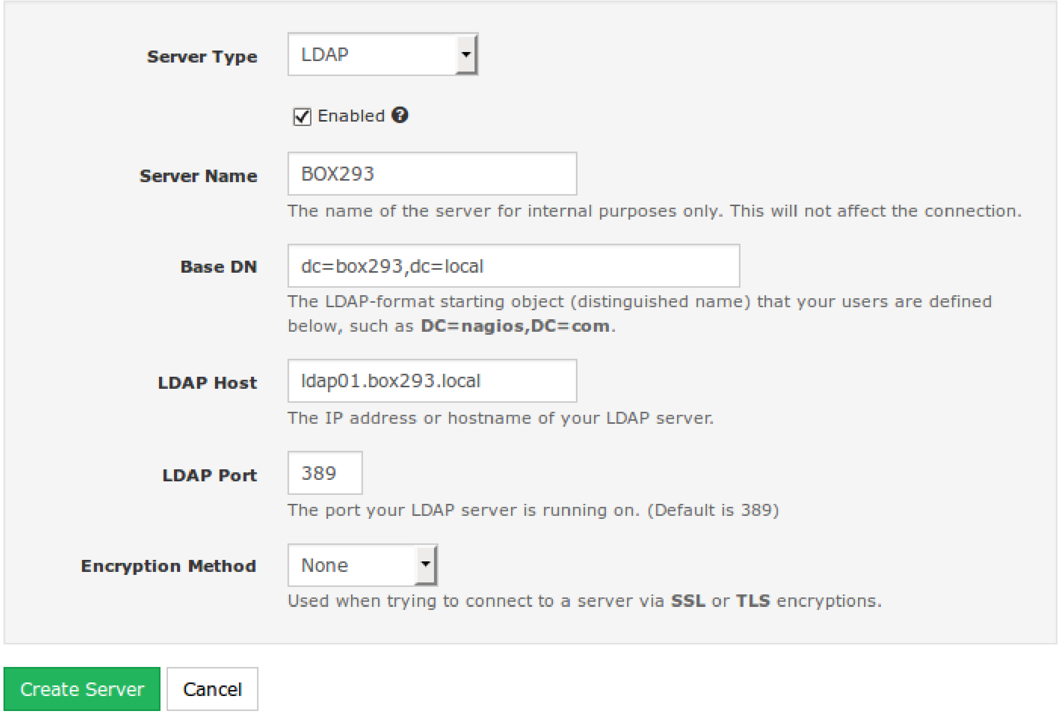
Encryption Method:

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 **Create Server** button.

You can now proceed to the Importing Users section.



Server Type: LDAP

☑ Enabled

Server Name: BOX293
The name of the server for internal purposes only. This will not affect the connection.

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.

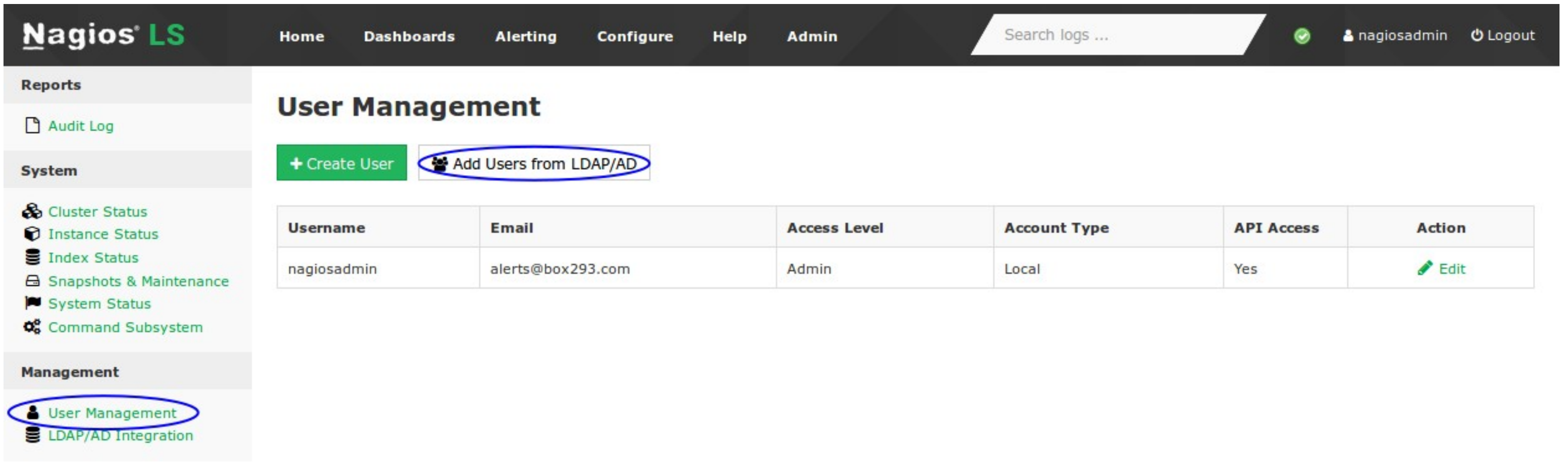
LDAP Port: 389
The port your LDAP server is running on. (Default is 389)

Encryption Method: None
Used when trying to connect to a server via **SSL** or **TLS** encryptions.

## Importing Users

The next step is to import users from Active Directory or LDAP. Once the user has been imported, Nagios Log Server 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** > **Management** > **User Management** and click the **Add Users from LDAP/AD** button.

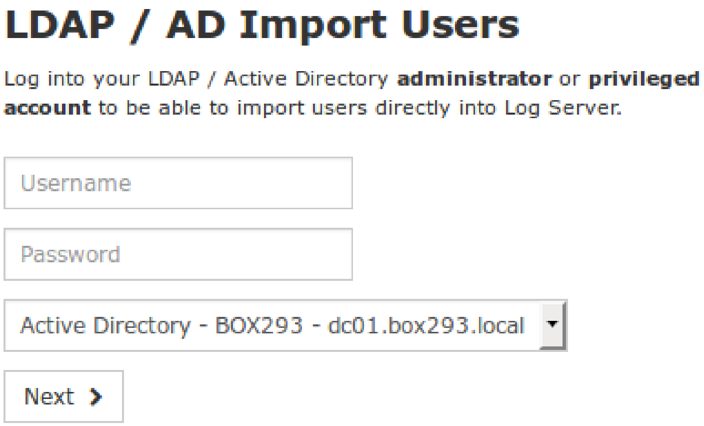


### User Management

| Username | Email | Access Level | Account Type | API Access | Action |
|---|---|---|---|---|---|
| nagiosadmin | alerts@box293.com | Admin | Local | Yes | Edit |

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.



LDAP / AD Import Users

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

Username

Password

Active Directory - BOX293 - dc01.box293.local

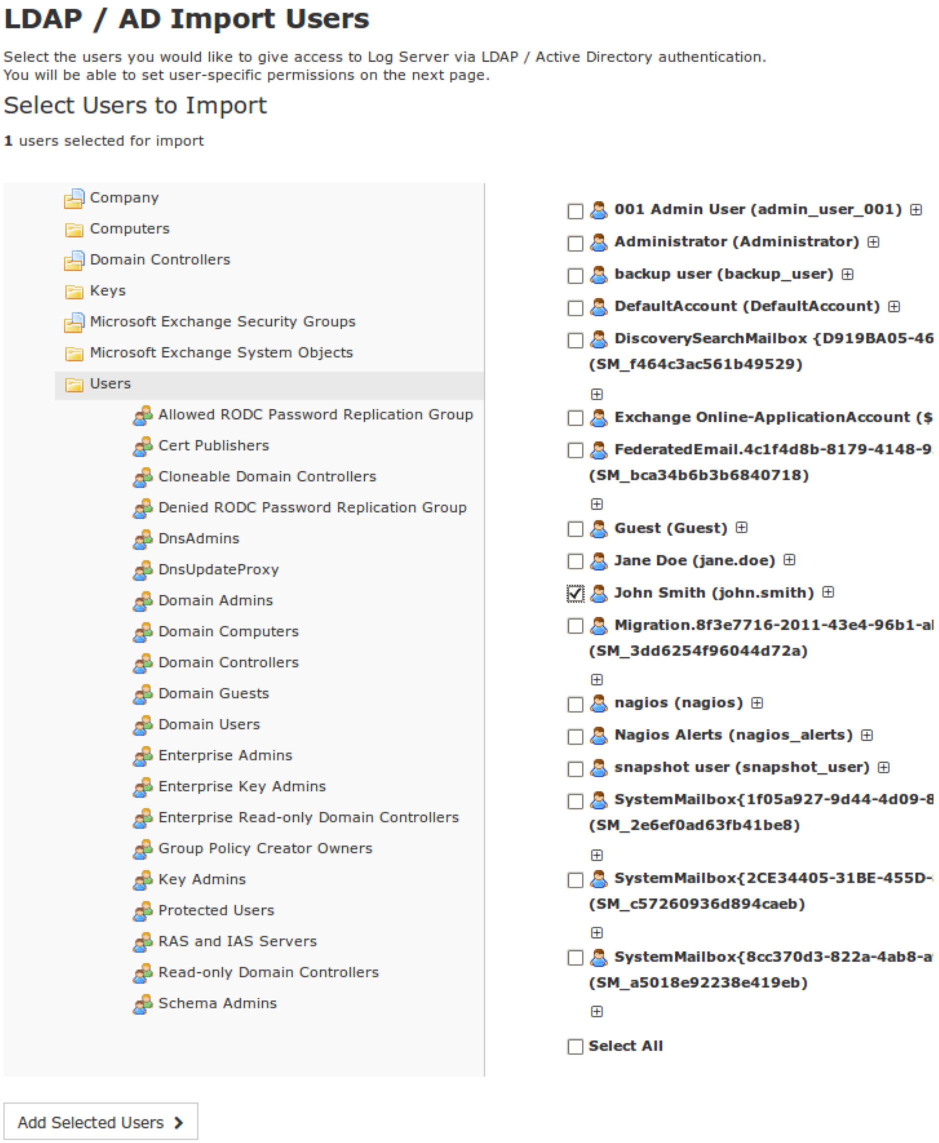
Click **Next**.

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 / AD Import Users

Select the users you would like to give access to Log Server via LDAP / Active Directory authentication.
You will be able to set user-specific permissions on the next page.

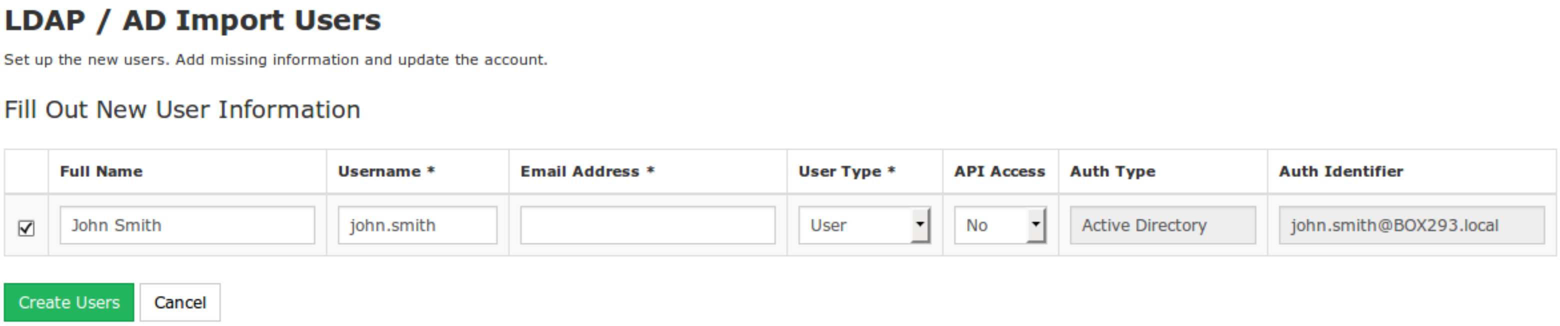
Select Users to Import

**1** users selected for import

- 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 {D919BA05-46 (SM_f464c3ac561b49529) ⊞
☐ Exchange Online-ApplicationAccount ($
☐ FederatedEmail.4c1f4d8b-8179-4148-9 (SM_bca34b6b3b6840718) ⊞
☐ Guest (Guest) ⊞
☐ Jane Doe (jane.doe) ⊞
☑ John Smith (john.smith) ⊞
☐ Migration.8f3e7716-2011-43e4-96b1-al (SM_3dd6254f96044d72a) ⊞
☐ nagios (nagios) ⊞
☐ Nagios Alerts (nagios_alerts) ⊞
☐ snapshot user (snapshot_user) ⊞
☐ SystemMailbox{1f05a927-9d44-4d09-8 (SM_2e6ef0ad63fb41be8) ⊞
☐ SystemMailbox{2CE34405-31BE-455D- (SM_c57260936d894caeb) ⊞
☐ SystemMailbox{8cc370d3-822a-4ab8-a (SM_a5018e92238e419eb) ⊞
☐ Select All

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 (see screenshot below).



## LDAP / AD Import Users

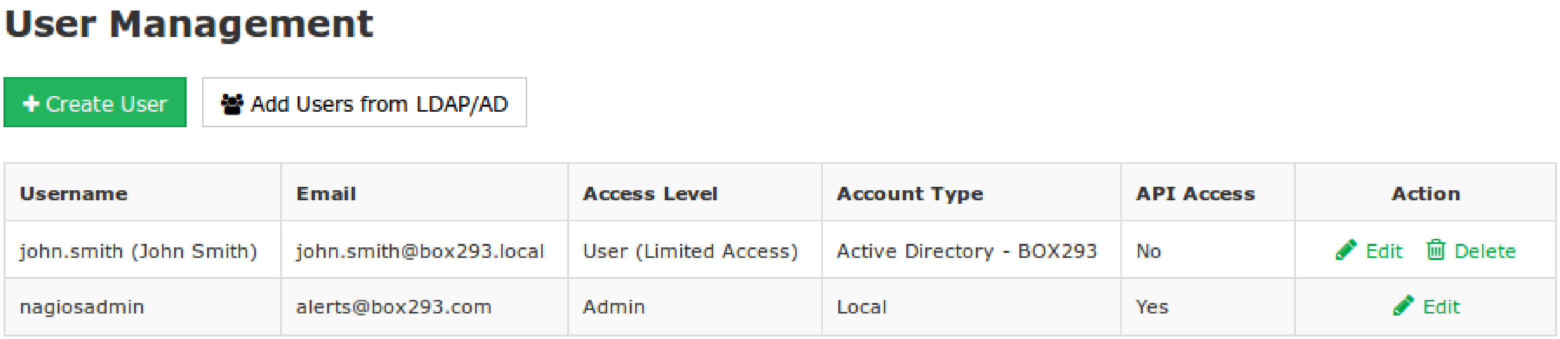
Set up the new users. Add missing information and update the account.

### Fill Out New User Information

| | Full Name | Username * | Email Address * | User Type * | API Access | Auth Type | Auth Identifier |
|---|---|---|---|---|---|---|---|
| ☑ | John Smith | john.smith | | User | No | Active Directory | john.smith@BOX293.local |

Every user will need the required fields (marked by an *) defined before you can click the Create Users button.

Click the **Create Users** button to continue. The user accounts will now be imported into Nagios Log Server. When finished you will be returned to the User Management screen.



## User Management

| Username | Email | Access Level | Account Type | API Access | Action |
|---|---|---|---|---|---|
| john.smith (John Smith) | john.smith@box293.local | User (Limited Access) | Active Directory - BOX293 | No | Edit Delete |
| nagiosadmin | alerts@box293.com | Admin | Local | Yes | Edit |

This completes importing users into Nagios Log Server from AD/LDAP.

## Linking Existing Nagios Log Server Users to Active Directory Users

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

Navigate to **Admin** > **Management** > **User Management**.

Click the **Edit** link for the user you want to update, the settings are on the **External Authentication** tab:

Auth Type: **Active Directory**

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

AD Username:

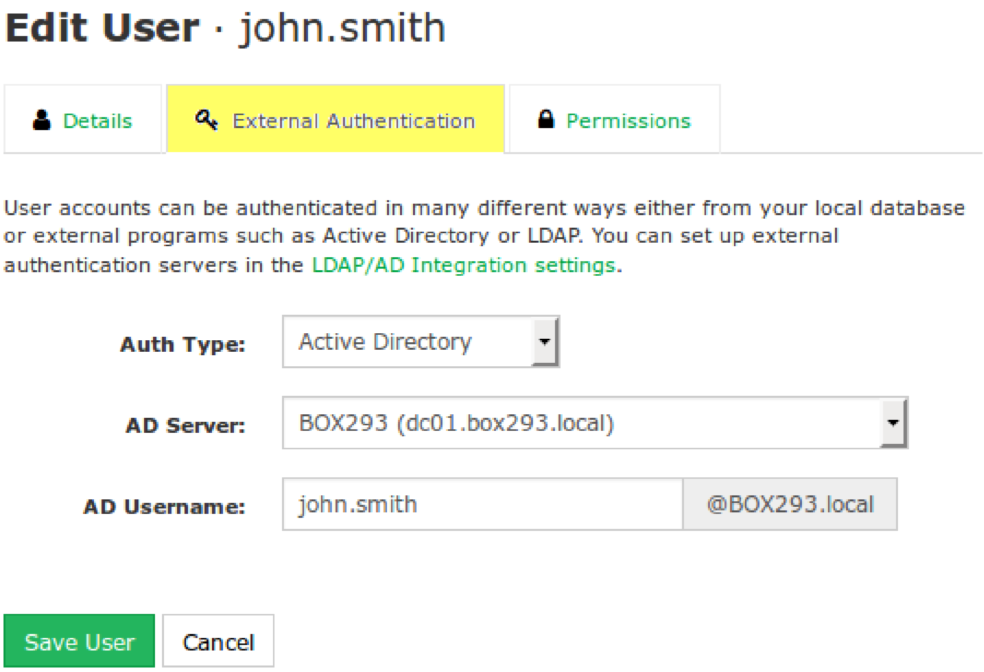
Type the username for this user as it is configured in Active Directory

Example: `jane.doe`

Click the **Save 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 Log Server user will be able to login using their Active Directory credentials.



**Edit User** · john.smith

User accounts can be authenticated in many different ways either from your local database or external programs such as Active Directory or LDAP. You can set up external authentication servers in the LDAP/AD Integration settings.

**Auth Type:** Active Directory

**AD Server:** BOX293 (dc01.box293.local)

**AD Username:** john.smith @BOX293.local

## Linking Existing Nagios Log Server Users to LDAP Users

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

Navigate to **Admin** > **Management** > **User Management**.

Click the **Edit** link for the user you want to update, the settings are on the **External Authentication** tab:

Auth Type: **LDAP**

LDAP Server: Select the authentication server you previously defined

Users Full DN:

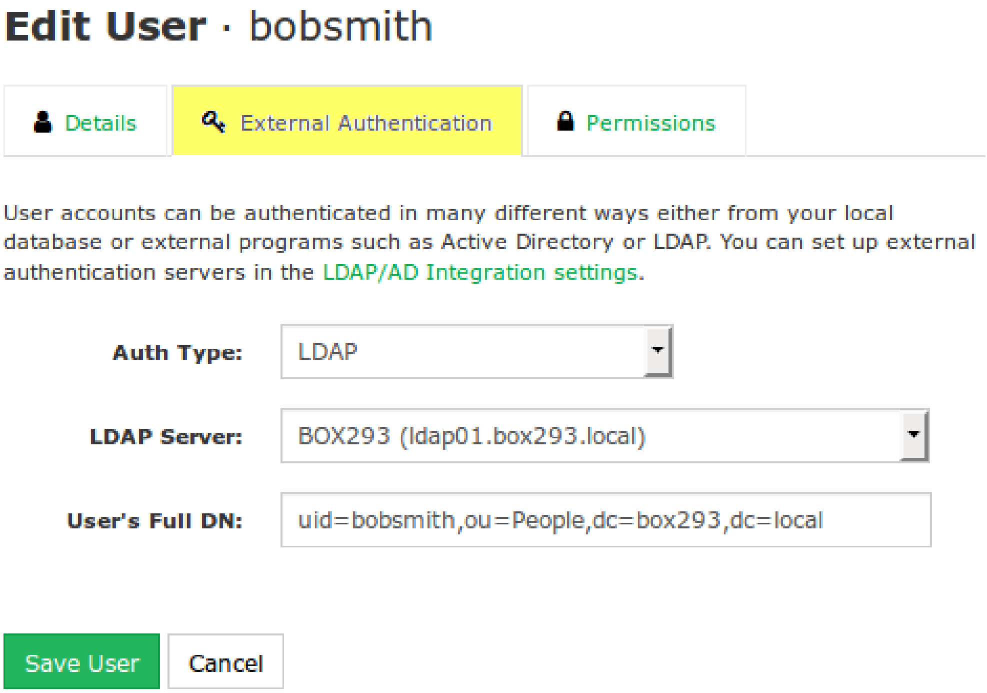
Type the full distinguished name (DN) for this user as it is defined in LDAP

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

Click the **Save 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 Log Server user will be able to login using their LDAP credentials.


**Edit User** · bobsmith

User accounts can be authenticated in many different ways either from your local database or external programs such as Active Directory or LDAP. You can set up external authentication servers in the LDAP/AD Integration settings.

|  |  |
|---|---|
| **Auth Type:** | LDAP |
| **LDAP Server:** | BOX293 (ldap01.box293.local) |
| **User's Full DN:** | uid=bobsmith,ou=People,dc=box293,dc=local |

## 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 to integrate Nagios Log Server with Active Directory or LDAP to allow user authentication and validation with the Nagios Log Server 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