

Purpose

This document describes how to integrate Nagios XI with Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) to allow user authentication and validation with an AD or LDAP infrastructure through the Nagios XI interface. This is helpful for system administrators

by simplifying user management of large infrastructures and standardizing credentials needed for XI by allowing users to authenticate with their AD or LDAP credentials.

Target Audience

This is intended for Nagios administrators who want to allow users to authenticate with their Windows AD or LDAP credentials when logging into Nagios XI.

Prerequisites

- You will need the following prerequisites in order to follow the documentation:
 Nagios XI 5
 - Nagios XI 2014 supports AD integration however is configured differently using the Active Directory
 component, which is not covered in this guide.
- A separate Microsoft Windows-based AD infrastructure that is accessible to the Nagios XI machine
 - o OR
- A separate LDAP infrastructure (like OpenLDAP) that is accessible to the Nagios XI machine

Nagios XI Server DNS Resolution

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

- Domain Controllers (DC) in your AD domain
 - o 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:
 - o vi /etc/resolv.conf
- Before all other lines starting with nameserver, enter the following:
 - o 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 7.x +:

```
systemctl restart httpd.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 define the Authentication Server(s) that Nagios XI will use. Navigate to **Admin > Users** and click **LDAP/AD Integration**.

How to Authenticate and Import Users with Active Directory or LDAP



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:

Authentication Server Settings			
	✓ Enable this authentication server		
Connection	Active Directory 🔻		
Method:	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	dc01.box293.local,dc02.box293.local		
Controllers:	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).		

Enable this authentication server: Checked

Connection Method: Active Directory

Base DN:

How to Authenticate and Import Users with Active Directory or LDAP

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 XI 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 XI server.

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: <u>Using SSL with XI Active Directory Component</u>. 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 <u>Importing Users</u> section.

LDAP

You will need to provide the following details:

Enable this authentication server: Checked

Connection Method: LDAP



How to Authenticate and Import Users with Active Directory or LDAP

Base DN:

An LDAP formatted string where the users are located.

Example: dc=box293, dc=local

LDAP Host:

The LDAP server that Nagios XI 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 XI server.

Example: ldap01.box293.local

LDAP Port:

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

Example: 389

Security:

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

If SSL or TLS is required then please refer to the <u>Using SSL with XI Active Directory Component</u> documentation.

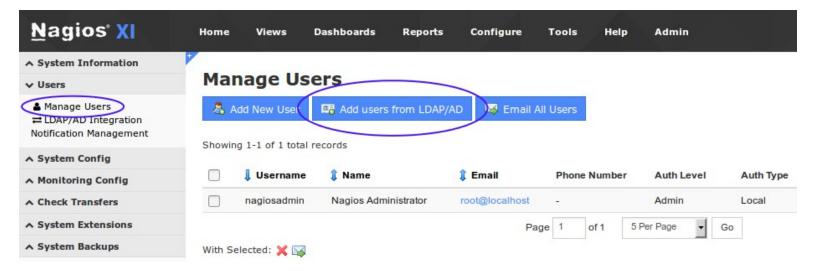
Authentication Server Settings ✓ Enable this authentication server Connection LDAP Method: Use either LDAP or Active Directory settings to connect. Base DN: dc=box293,dc=local The LDAP-format starting object (distinguished name) that your users are defined below, such as DC=nagios,DC=com. LDAP Host: Idap01.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 <u>Importing Users</u> section.

Importing Users

The next step is to import users from Active Directory or LDAP. Once the user has been imported, Nagios XI will query the DCs or LDAP server 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 **Add Users from LDAP/AD**.



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.

Administrator	

Active Directory - dc01.box293.local,dc02.box293.local	
Next >	

How to Authenticate and Import Users with Active Directory or LDAP

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.

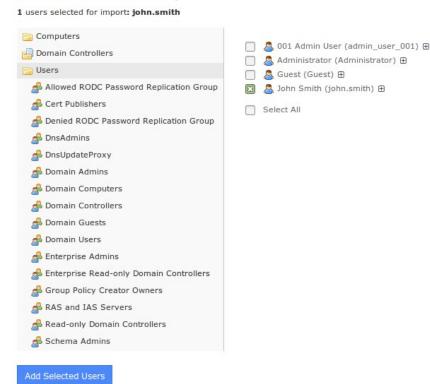
When you've chosen all the users to import, click the **Add Selected Users** button.

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 / 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



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.

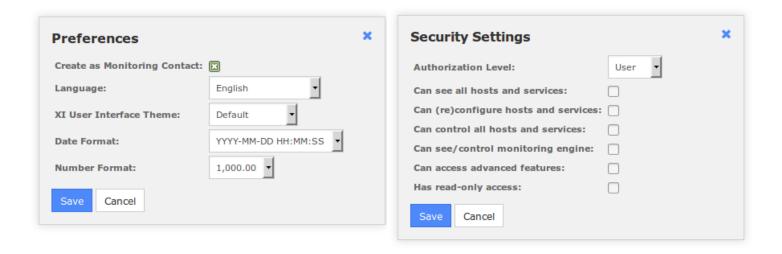
In order to finish importing you *must select the preferences and security settings for all users*. For quicker creation, select users with checkboxes and use the dropdown to set the preferences and security settings for multiple users at once.





How to Authenticate and Import Users with Active Directory or LDAP

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



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

In the Preferences screen there is the option **Create as Monitoring Contact**. It is strongly recommended that you check this box as the monitoring contact is required for users to receive notifications. For more information about contacts please refer to this documentation link <u>Nagios XI Users and Contacts</u>.

How to Authenticate and Import Users with Active Directory or LDAP

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.

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.

	Username	Display Name	Email	Preferences	Security Settings
×	john.smith	John Smith	john.smith@box293.local	E dit	• Edit
Edit	multiple				
Can	cel Import >				

Click **Import** to continue.

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

This completes importing users into Nagios XI from Active Directory or LDAP.

LDAP / Active Directory Import Users

Successfully added 1 users.		
Log into your LDAP / Active Directory administrator or	privileged ac	count to be able to import use
nagiosadmin		
•••••		
Active Directory - dc01.box293.local,dc02.box293.lo	cal	
Next >		

Linking Existing Nagios XI Users to Active Directory Users

If you already have Nagios XI 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** icon for the user you want to update, the settings are under the **Authentications Setting** 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:

Auth Type:	Active Directory
AD Server:	dc01.box293.local,dc02.box293.local
	_
AD Username:	jane.doe

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

Linking Existing Nagios XI Users to LDAP Users

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

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

Click the **Edit** icon for the user you want to update, the settings are under the **Authentications Setting** 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:	Idap01.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 XI 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 to integrate Nagios XI with Active Directory or LDAP to allow user authentication and validation with the Nagios XI 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