

## The Industry Standard in IT Infrastructure Monitoring

### Purpose

This document describes how to integrate Nagios XI with Active Directory to allow user authentication and validation with an Active Directory (AD) infrastructure through the Nagios XI interface. This is helpful for system administrators by simplifying user management of large infrastructures and standardize credentials needed for Nagios XI by allowing users to authenticate with their Windows Active Directory credentials when logging into the system.

### Target Audience

This is intended for Nagios administrators who want to allow users to authenticate with their Windows Active Directory 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 Active Directory infrastructure 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 a domain controllers in your Active Directory domain. If you are having issues you can edit the `resolv.conf` file to use a DNS server within the Active Directory 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 run `service httpd restart` (on RHEL/CentOS 6) or `systemctl restart httpd.service` (on RHEL/CentOS 7) to restart Apache afterwards.

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 XI will use.

Navigate to **Admin > Users** and click **LDAP/AD Integration**.

Click the **Add Authentication Server** button, refer to the following screenshot.

**Nagios XI** Home Views Dashboards Reports Configure Tools Help Admin

System Information  
Users  
Manage Users  
LDAP/AD Integration  
Notification Management

### 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.				

#### 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,dc02.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).

**Save Server** Cancel

#### Certificate Authority Management

For connecting over SSL/TLS using self-signed certificates you will need to add the certificate(s) of the domain controller(s) to the local certificate authority so they are trusted. If any certificate was signed by a host other than itself, that certificate authority/host certificate needs to be added.

**Add Certificate**

Hostname	Issuer (CA)	Expires On	Actions
You have not added any CA certificates through the web interface			

To configure an authentication server you will need to provide the following details:

Enable this authentication server: **Checked**

Connection Method:

**Active Directory**

Base DN:

An LDAP formatted string to address your domain correctly

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 servers that Nagios XI can use to authenticate against. This can be both a combination of IP addresses, short names, and fully qualified domain names.

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

Security:

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

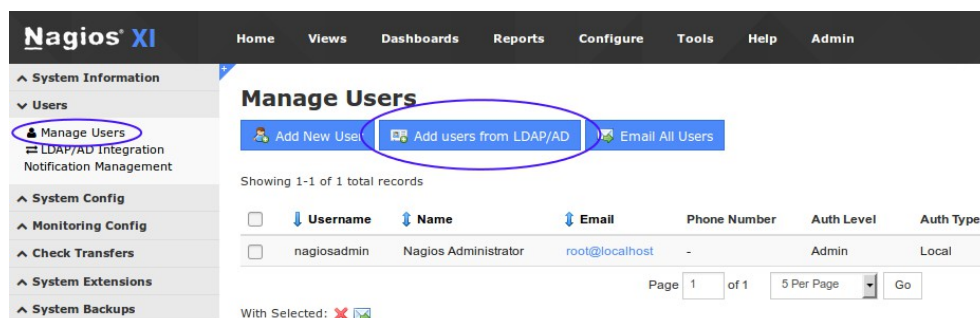
If you are in a domain forest that has been raised to a functional level of 2012, then TLS is needed along with additional steps in the following guide: [Using SSL with XI Active Directory Component directions](#).

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

## Importing Users From Active Directory into Nagios XI

The next step is to import users from Active Directory. Once the user has been imported, Nagios XI will query the domain controller each time the user logs in to validated credentials.

Navigate to **Admin > Users > Manage Users** and click **Add Users from LDAP/AD**



# Nagios XI – How to Authenticate and Import Users with Active Directory

The first step is to select the authentication servers you previously defined and to provide credentials to connect to the servers. This account is used to authenticate against Active Directory and list the contents.

## 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 >

Click Next.

Once you've successfully authenticated, you'll be presented with the root node of your active directory tree. In the following 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.

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**

Computers

Domain Controllers

Users

- Allowed RODC Password Replication Group
- Cert Publishers
- Denied RODC Password Replication Group
- DnsAdmins
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users
- Enterprise Admins
- Enterprise Read-only Domain Controllers
- Group Policy Creator Owners
- RAS and IAS Servers
- Read-only Domain Controllers
- Schema Admins

001 Admin User (admin\_user\_001)

Administrator (Administrator)

Guest (Guest)

John Smith (john.smith)

Select All

Add Selected Users

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.

## 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: English

XI User Interface Theme: Default

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

Number Format: 1,000.00

Save Cancel

### Security Settings

Authorization Level: User

Can see all hosts and services:

Can (re)configure hosts and services:

Can control all hosts and services:

Can see/control monitoring engine:

Can access advanced features:

Has read-only access:

Save Cancel

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 checkboxes 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 shown 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 [Nagios XI Users and Contacts](#).

ALL users being imported will require the Preferences and Security Settings to have a checkbox appear in the 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.

<input type="checkbox"/>	Username	Display Name	Email	Preferences	Security Settings
<input checked="" type="checkbox"/>	john.smith	John Smith	john.smith@box293.local	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Edit

Edit multiple ...

Cancel 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.

## 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.

nagiosadmin

.....

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

Next >

This completes importing users into Nagios XI from Active Directory.

## 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

### Authentications Setting section

Auth Type:

Change to **Active Directory**

AD Server:

Select the authentication servers you previously defined

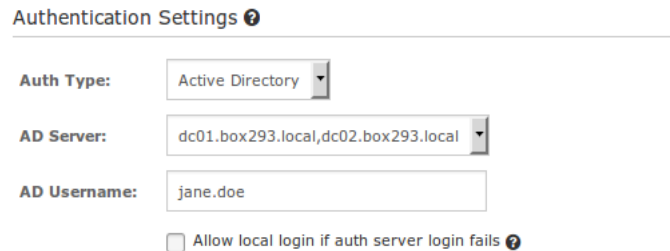
AD Username:

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

Example: **jane.doe**

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

Here is a screenshot of the user settings described above:



The screenshot shows the 'Authentication Settings' form in Nagios XI. It includes the following fields:

- Auth Type:** A dropdown menu set to 'Active Directory'.
- AD Server:** A dropdown menu set to 'dc01.box293.local,dc02.box293.local'.
- AD Username:** A text input field containing 'jane.doe'.
- Allow local login if auth server login fails:** An unchecked checkbox.

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

## Final Thoughts

If you have any issues with configuring the Active Directory integration or its use, please post your questions on the [Nagios Support Forums](#) at the following URL:

<http://support.nagios.com/>