How to Configure Single Sign-On (SSO) in Nagios XI

Purpose

This document guides Nagios XI administrators through configuring Single-Sign-On (SSO) with Microsoft Azure Active Directory (AAD) for their Nagios XI users.

Important Note: SSO is one of Nagios XI's Premium features, so requires active support and maintenance benefits to function. For questions about renewing your benefits if they have lapsed, please email sales@nagios.com so we can assist you further.

Requirements

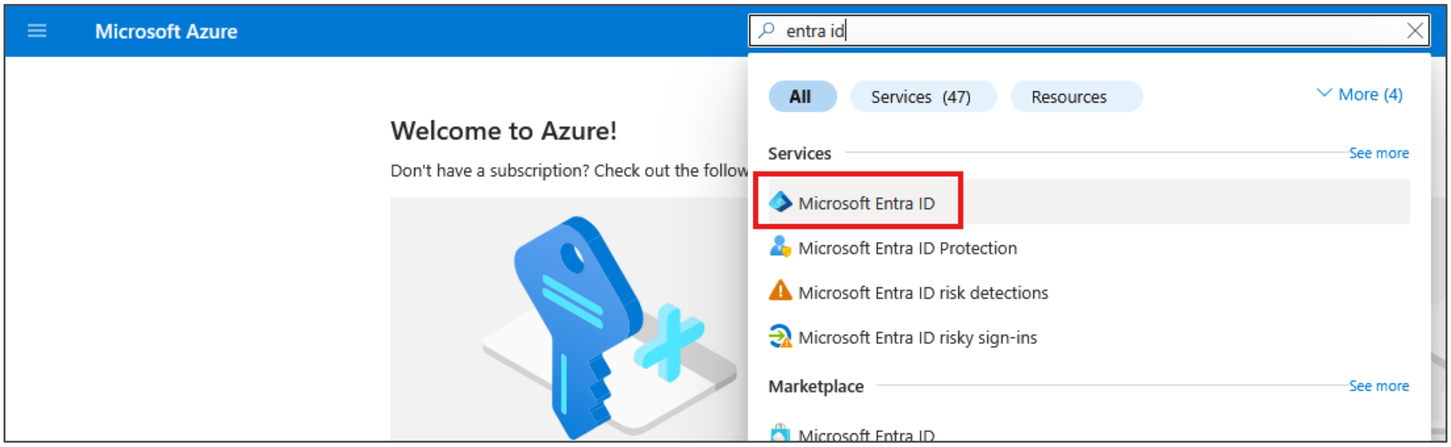
- Nagios XI 2024R2 or later
    - Nagios XI Administrator Account
    - TLS/SSL enabled – Configure TLS/SSL for Nagios XI

      You MUST configure TLS/SSL for Nagios XI before using SSO. If you do not, you will expose your credentials to anyone who intercepts your packets!
- Azure Active Directory (AAD)
    - Global Administrator account for your AAD tenant

Contents

Configure Your Azure AD Registration for SSO

1. Log in to the Azure Portal and navigate to **Microsoft Entra ID.**

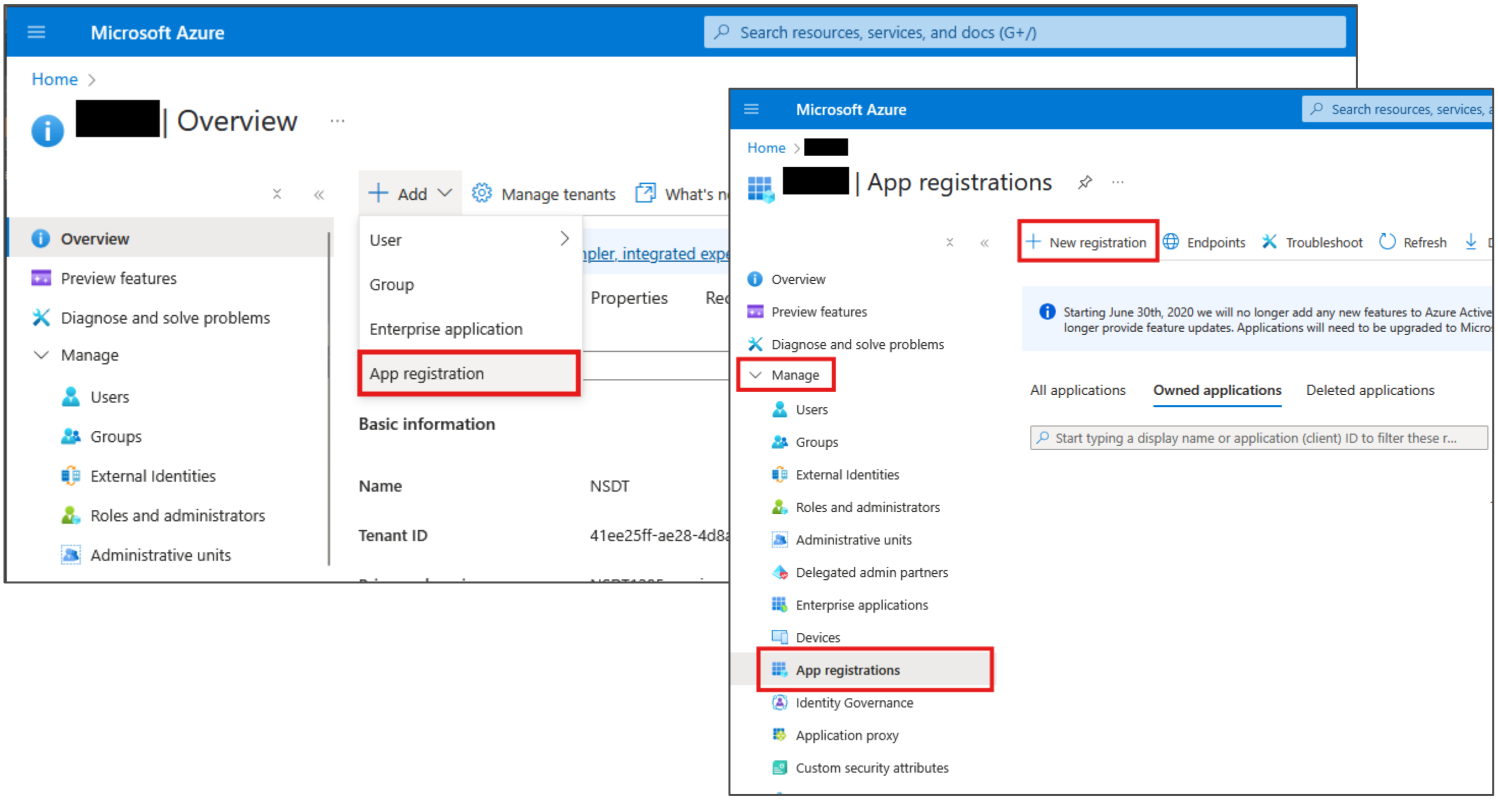


Welcome to Azure!

Don't have a subscription? Check out the follow

entra id

2. You can either select **+Add > App registration** from the **Overview** page, or navigate to **Microsoft Entra ID > Manage > App Registrations**, then click **+ New registration**.



[redacted] | Overview

Basic information

Name NSDT

Tenant ID 41ee25ff-ae28-4d8

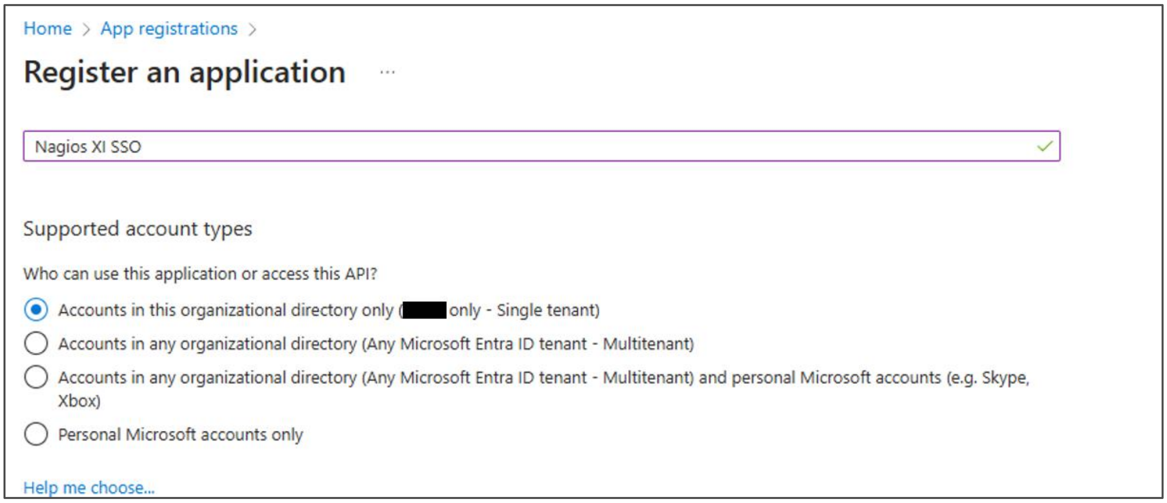
Home > [redacted]

[redacted] | App registrations

Starting June 30th, 2020 we will no longer add any new features to Azure Active longer provide feature updates. Applications will need to be upgraded to Micro

Start typing a display name or application (client) ID to filter these r...

3. Select **Accounts in this organizational directory only (<my_tenant_name> only - Single tenant)**. Currently, Nagios XI only supports single-tenant SSO. If you need to use SSO with multiple tenants, these tenants must be added separately.



Register an application ···

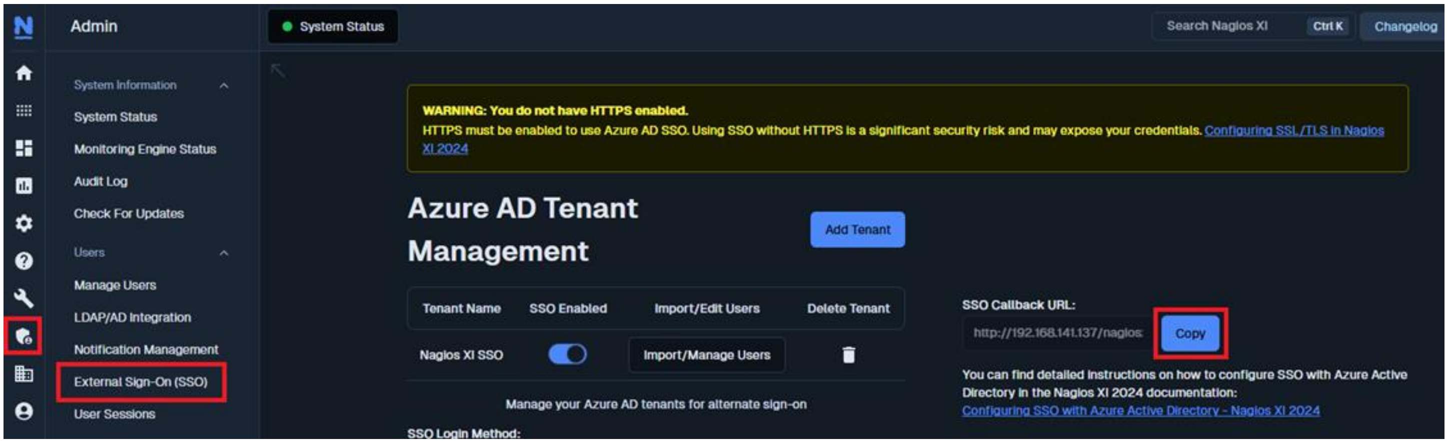
Nagios XI SSO

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only ([redacted] only - Single tenant)
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

4. Copy the callback URL from Nagios XI by navigating to **Admin** > **Users** > **External Sign-On (SSO)**



WARNING: You do not have HTTPS enabled.
HTTPS must be enabled to use Azure AD SSO. Using SSO without HTTPS is a significant security risk and may expose your credentials. Configuring SSL/TLS in Nagios XI 2024

Azure AD Tenant Management

Tenant Name	SSO Enabled	Import/Edit Users	Delete Tenant
Nagios XI SSO	●	Import/Manage Users	🗑

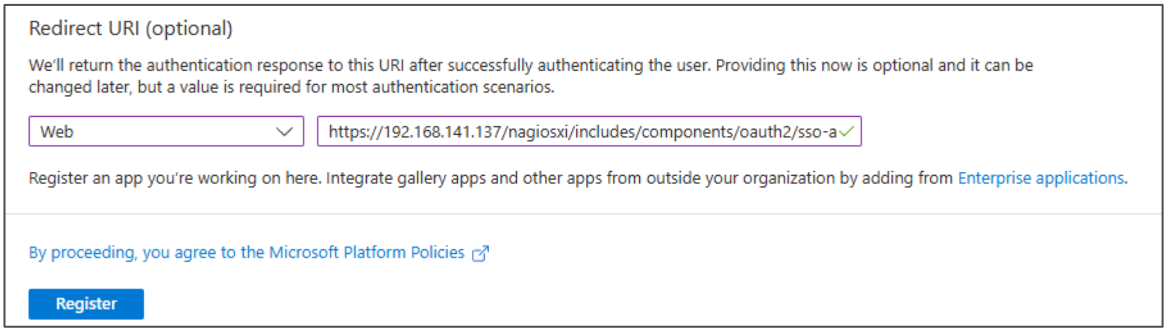
Manage your Azure AD tenants for alternate sign-on

SSO Login Method:

SSO Callback URL:
http://192.168.141.137/nagios

You can find detailed instructions on how to configure SSO with Azure Active Directory in the Nagios XI 2024 documentation:
Configuring SSO with Azure Active Directory - Nagios XI 2024

5. Paste the callback URL in the **Redirect URI** section of your application registration. Select **Web** from the dropdown menu and click **Register**.



Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

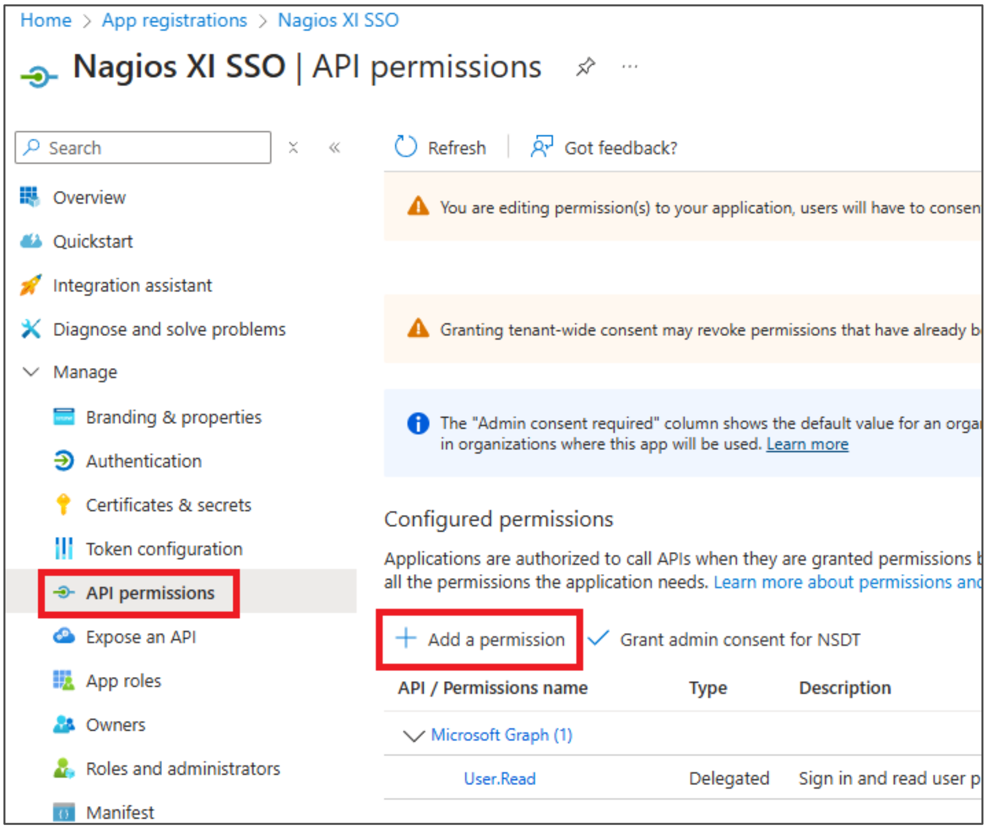
Web | https://192.168.141.137/nagiosxi/includes/components/oauth2/sso-a

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

Set Your App Registration's API Permissions

6. Navigate to **App Registrations >** your app registration's **API permissions** tab and select **Add a permission.**



You are editing permission(s) to your application, users will have to consen

Granting tenant-wide consent may revoke permissions that have already b

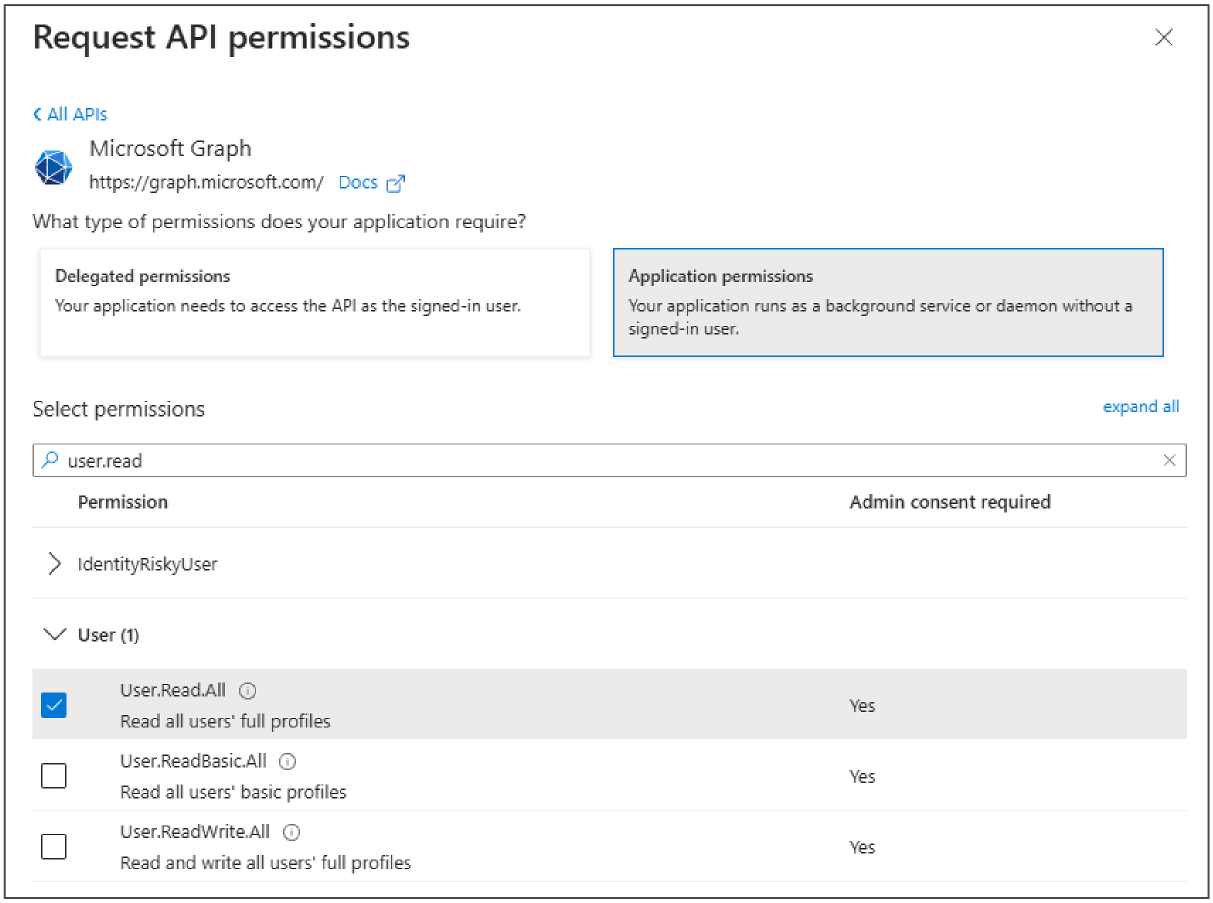
The "Admin consent required" column shows the default value for an orga in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions b all the permissions the application needs. Learn more about permissions and

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user p

7. Select **Microsoft Graph > Application permissions > User > User.Read.All**



Request API permissions

‹ All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

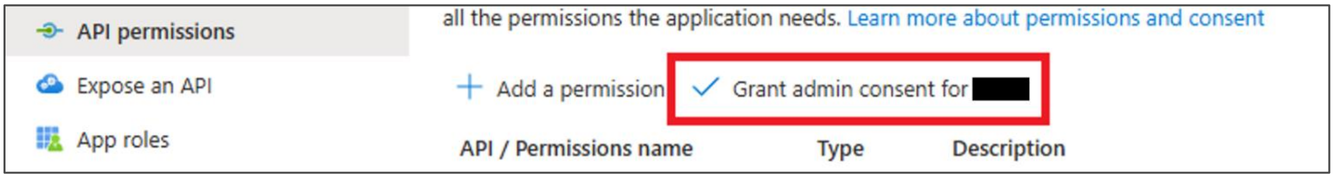
Select permissions

expand all

user.read

	Permission	Admin consent required
	› IdentityRiskyUser	
	⌄ User (1)	
☑	User.Read.All Read all users' full profiles	Yes
□	User.ReadBasic.All Read all users' basic profiles	Yes
□	User.ReadWrite.All Read and write all users' full profiles	Yes

8. Select **Grant admin consent for <my_tenant_name>.**

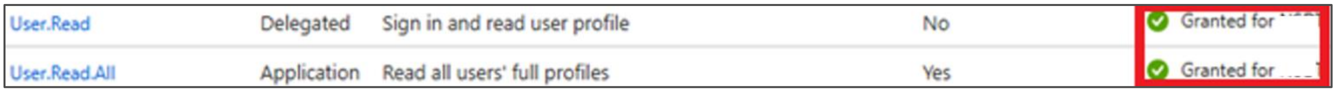


all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for [redacted]

API / Permissions name Type Description

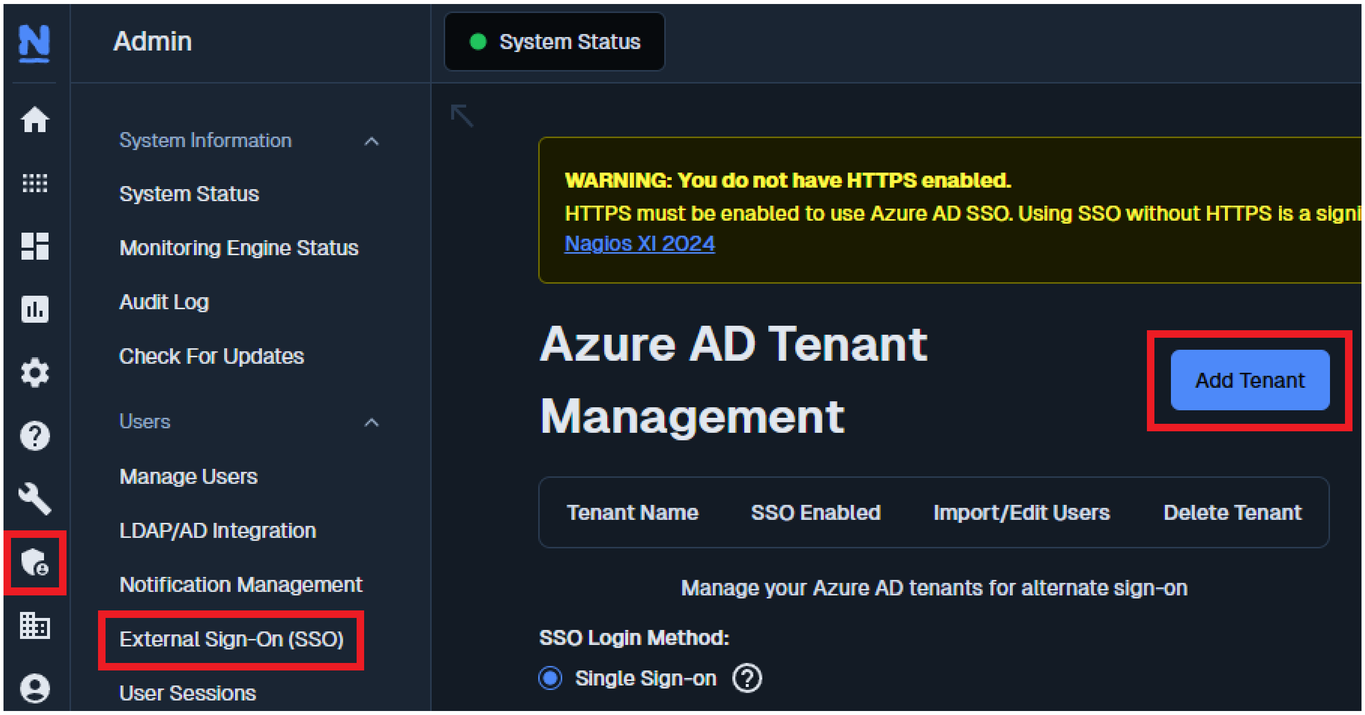
9. A green checkmark will appear in the right column confirming the selection.



User.Read	Delegated	Sign in and read user profile	No	✓ Granted for
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for

Add Your Tenant to Nagios XI

1. In Nagios XI, navigate to **Admin > Users > External Sign-On (SSO) > Add Tenant**.



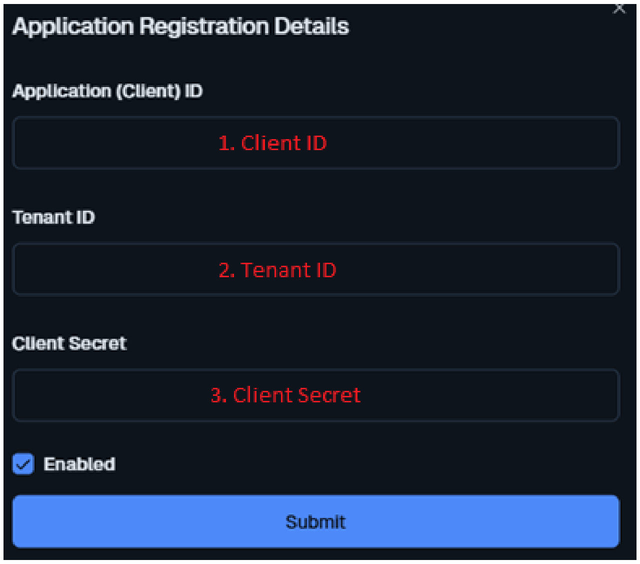
WARNING: You do not have HTTPS enabled.
HTTPS must be enabled to use Azure AD SSO. Using SSO without HTTPS is a signi
Nagios XI 2024

Azure AD Tenant Management

Manage your Azure AD tenants for alternate sign-on

SSO Login Method:
● Single Sign-on

2. The **Application Registration Details** screen will appear. You will need to copy your Client ID, Tenant ID, and Client Secret from Azure.



Application Registration Details

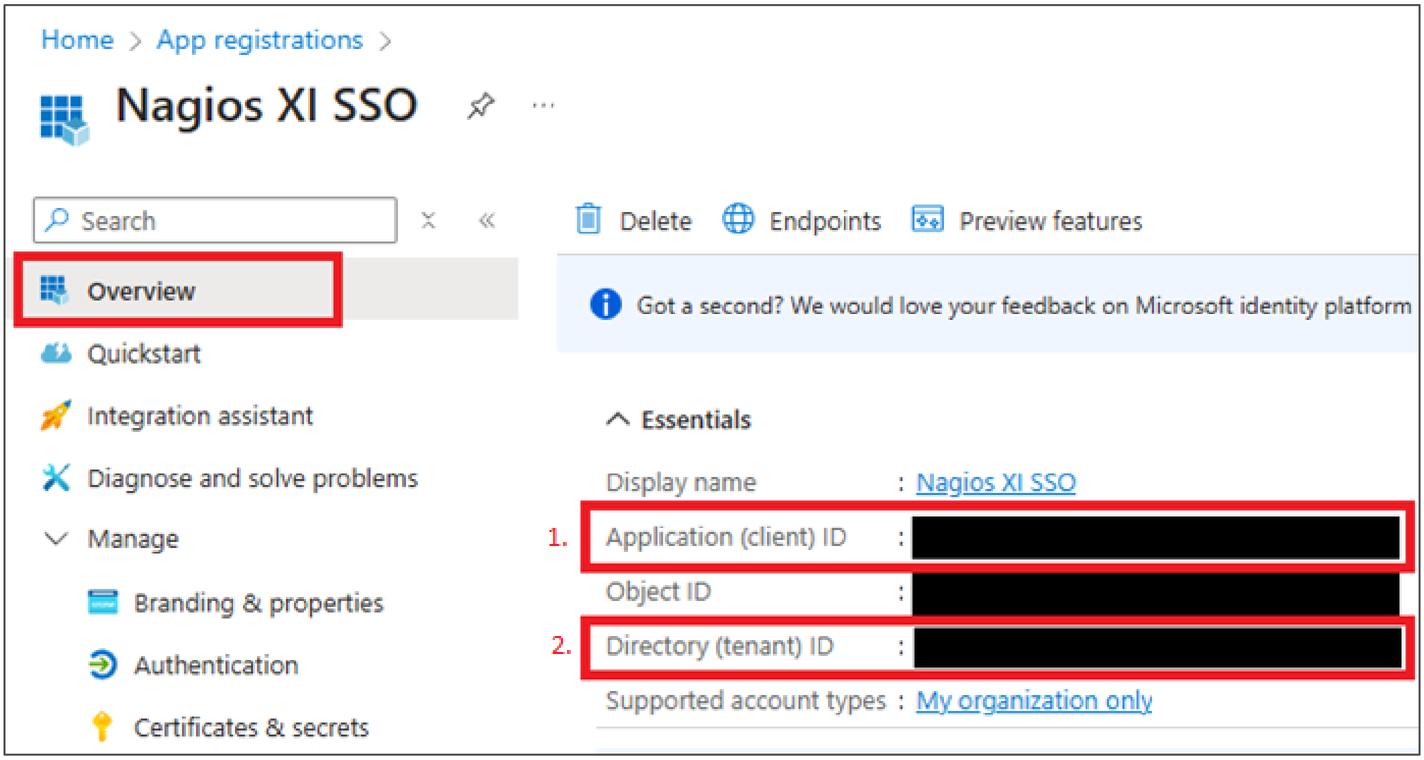
Application (Client) ID: 1. Client ID

Tenant ID: 2. Tenant ID

Client Secret: 3. Client Secret

☑ Enabled

3. In Azure, navigate to **Overview > Essentials** and copy the **Application (client) ID** and **Directory (tenant) ID**. Paste these into their respective fields in the **Application Registration Details** in Nagios XI.



Got a second? We would love your feedback on Microsoft identity platform

Display name : Nagios XI SSO

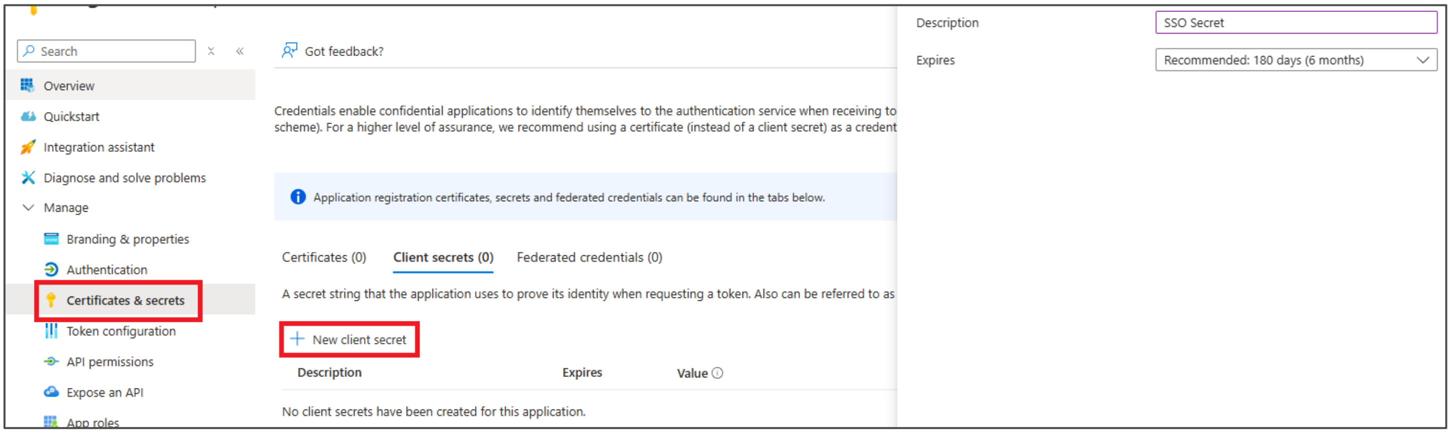
Application (client) ID : [redacted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : My organization only

4. Navigate to **Certificates & secrets > New client secret**.



Credentials enable confidential applications to identify themselves to the authentication service when receiving to
scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credent

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as

Description	Expires	Value ⓘ

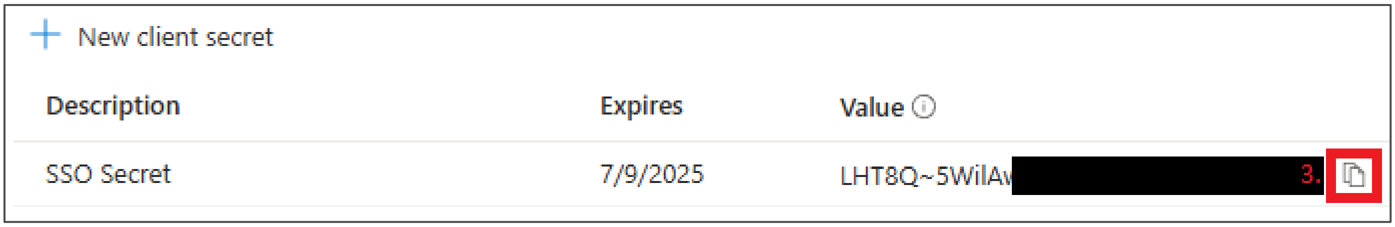
No client secrets have been created for this application.

Description: SSO Secret

Expires: Recommended: 180 days (6 months)

5. Be sure to copy the Value of your client secret, not the Secret ID. Paste it into its respective field in the Application Registration Details in Nagios XI.

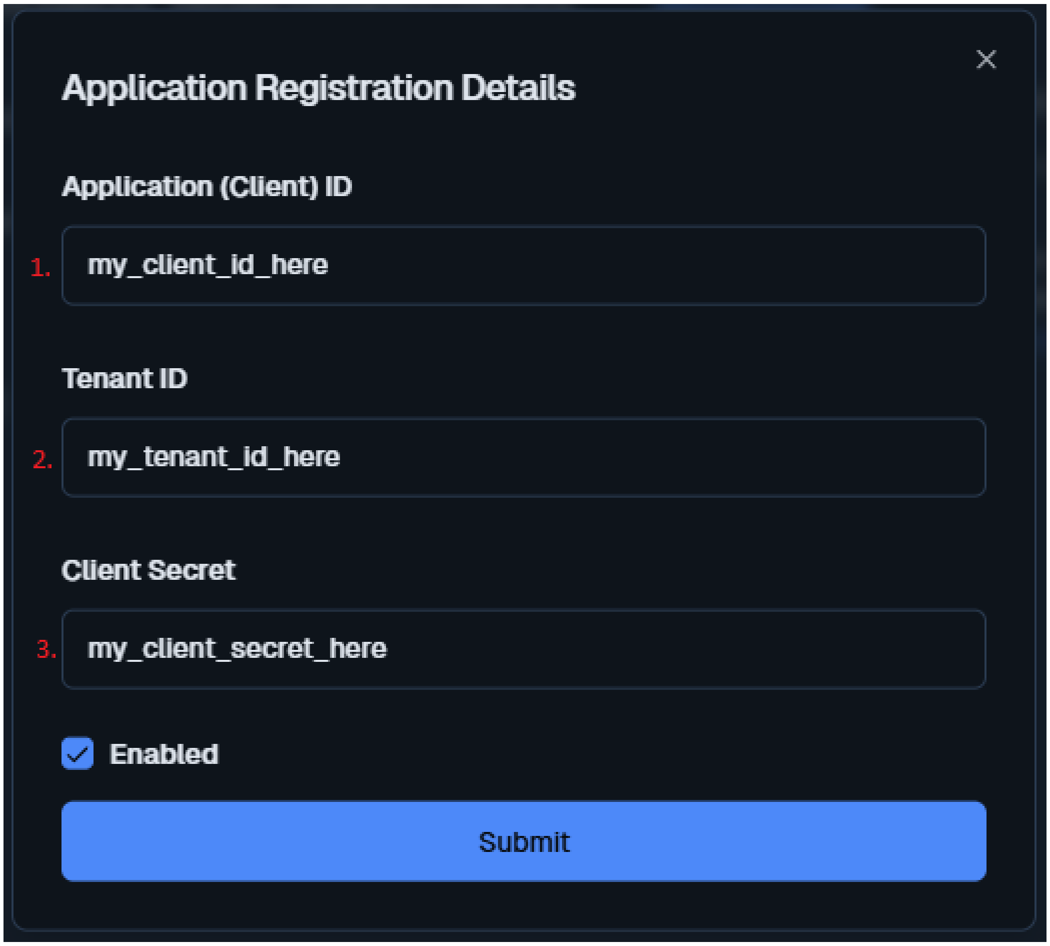
   Note that upon navigating away, you will no longer be able to read or copy your client secret, so be sure to store it in a secure place.



+ New client secret

Description	Expires	Value ⓘ
SSO Secret	7/9/2025	LHT8Q~5WilA[redacted]

6. After you have copied and pasted these values into the Application Registration Details form in Nagios XI, click Submit.



Application Registration Details

Application (Client) ID

1. my_client_id_here

Tenant ID

2. my_tenant_id_here

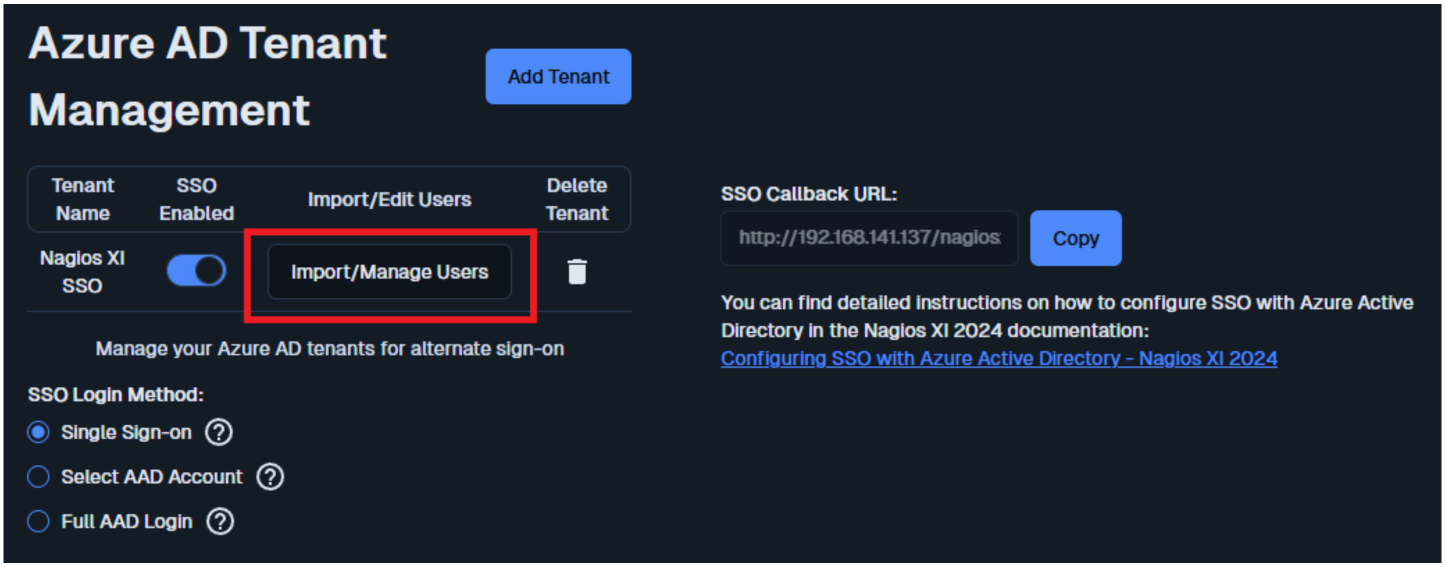
Client Secret

3. my_client_secret_here

☑ Enabled

Import/Configure Users

Navigate to **Admin** > **Users** > **Single Sign-On (SSO)**. Select **Import/Manage Users**.



Azure AD Tenant Management

Add Tenant

Tenant Name	SSO Enabled	Import/Edit Users	Delete Tenant
Nagios XI SSO	●	Import/Manage Users	🗑

Manage your Azure AD tenants for alternate sign-on

SSO Login Method:

● Single Sign-on ?

○ Select AAD Account ?

○ Full AAD Login ?

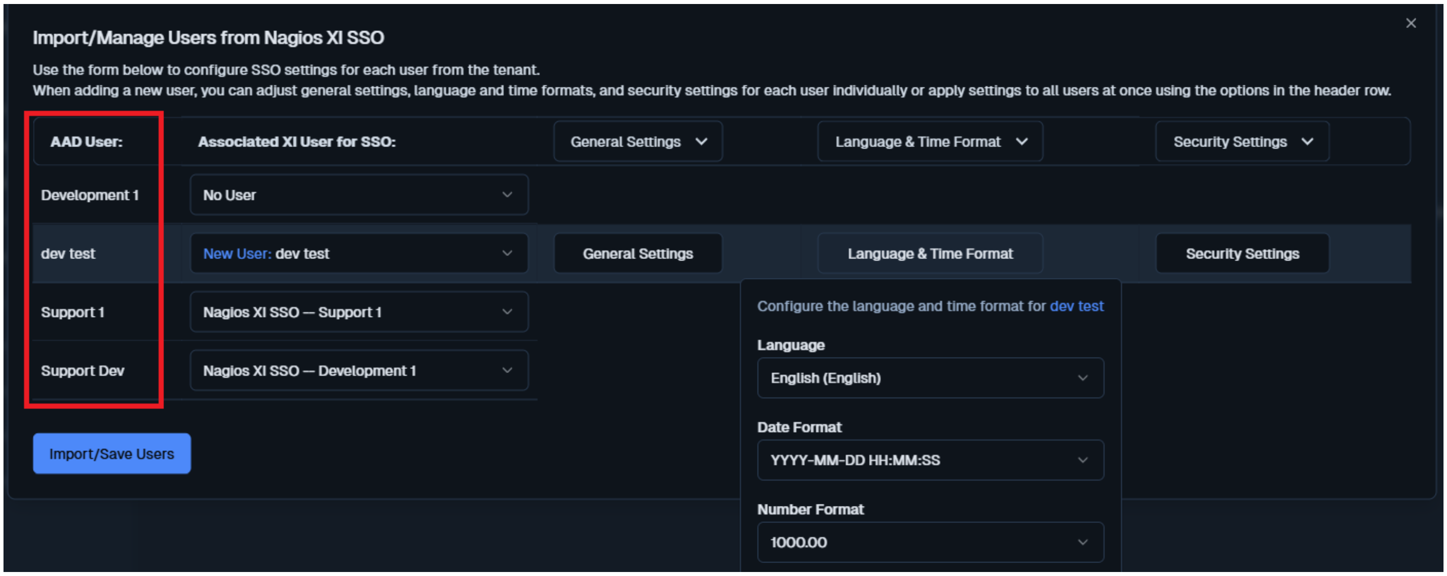
SSO Callback URL:

http://192.168.141.137/nagios

Copy

You can find detailed instructions on how to configure SSO with Azure Active Directory in the Nagios XI 2024 documentation:
Configuring SSO with Azure Active Directory - Nagios XI 2024

AAD Users available to be assigned to Nagios XI users are listed on the left under **AAD User**.



Import/Manage Users from Nagios XI SSO

Use the form below to configure SSO settings for each user from the tenant.
When adding a new user, you can adjust general settings, language and time formats, and security settings for each user individually or apply settings to all users at once using the options in the header row.

AAD User:	Associated XI User for SSO:	General Settings	Language & Time Format	Security Settings
Development 1	No User			
dev test	New User: dev test	General Settings	Language & Time Format	Security Settings
Support 1	Nagios XI SSO — Support 1			
Support Dev	Nagios XI SSO — Development 1			

Import/Save Users

Configure the language and time format for dev test

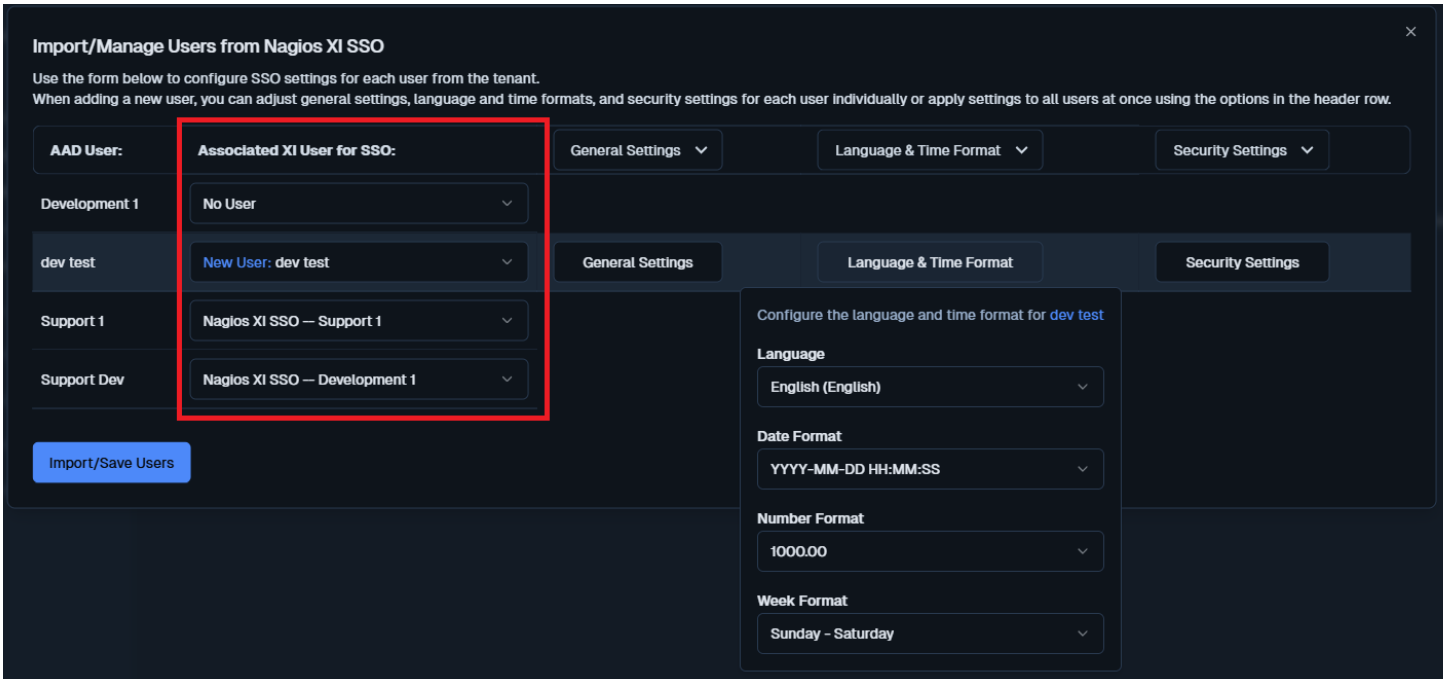
Language: English (English)

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

Number Format: 1000.00

Under **Associated XI User for SSO**, you can select which Nagios XI accounts each Azure AD user can log in to through Azure.

- **No User** indicates that the AAD User will not be assigned to a user in Nagios XI and thus will not be able to log in to Nagios XI with that AAD User.
- **New User: username** will create a new Nagios XI user with the given username and that AAD User's email. Upon selecting this option, you will be able to configure the various user settings to the right. In the screenshot below, this option is displayed as "New User: dev test".
  - As with the users **Nagios XI SSO – Support 1** and **Nagios XI SSO – Development 1** in the screenshot below, users created with this SSO integration will have their usernames prepended with the name of your AAD App Registration.
- Selecting an existing Nagios XI user's **Username** will assign the given AAD account to the specified existing Nagios XI user. These XI users will be able to log in to Nagios XI via their Username/Password or via SSO by logging in with the Microsoft AAD credentials of the given AAD user.



Import/Manage Users from Nagios XI SSO

Use the form below to configure SSO settings for each user from the tenant.
When adding a new user, you can adjust general settings, language and time formats, and security settings for each user individually or apply settings to all users at once using the options in the header row.

AAD User:	Associated XI User for SSO:	General Settings	Language & Time Format	Security Settings
Development 1	No User			
dev test	New User: dev test	General Settings	Language & Time Format	Security Settings
Support 1	Nagios XI SSO — Support 1			
Support Dev	Nagios XI SSO — Development 1			

Configure the language and time format for dev test

Language: English (English)

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

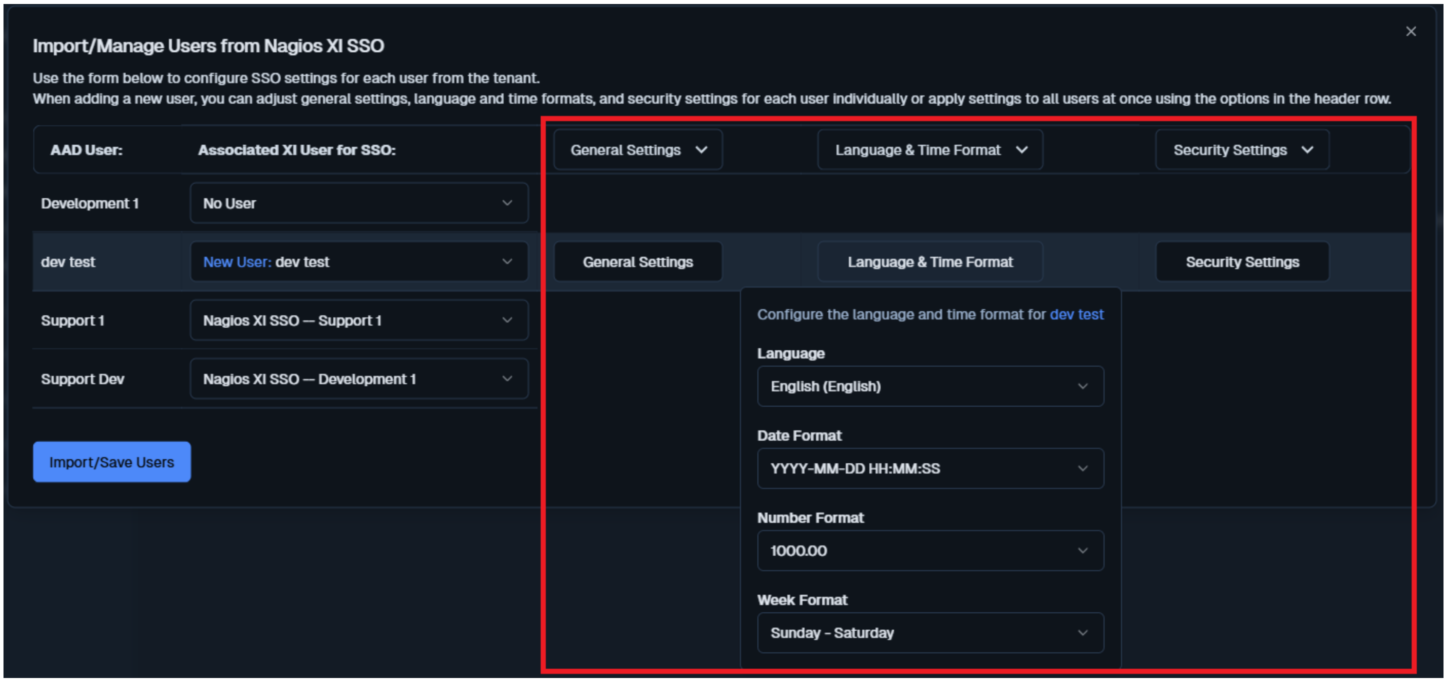
Number Format: 1000.00

Week Format: Sunday - Saturday

Newly created users can have their account settings configured in the given dropdown menus.

- The dropdown menus in the header above the table will apply settings to all newly created users.
- The dropdown menus to the right of AAD users assigned to create new XI user accounts will only modify the setting for that specific Nagios XI user.

When you are satisfied with your configuration, click **Import/Save Users**.



Import/Manage Users from Nagios XI SSO

Use the form below to configure SSO settings for each user from the tenant.
When adding a new user, you can adjust general settings, language and time formats, and security settings for each user individually or apply settings to all users at once using the options in the header row.

AAD User:	Associated XI User for SSO:	General Settings	Language & Time Format	Security Settings
Development 1	No User			
dev test	New User: dev test	General Settings	Language & Time Format	Security Settings
Support 1	Nagios XI SSO — Support 1			
Support Dev	Nagios XI SSO — Development 1			

Configure the language and time format for dev test

Language: English (English)

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

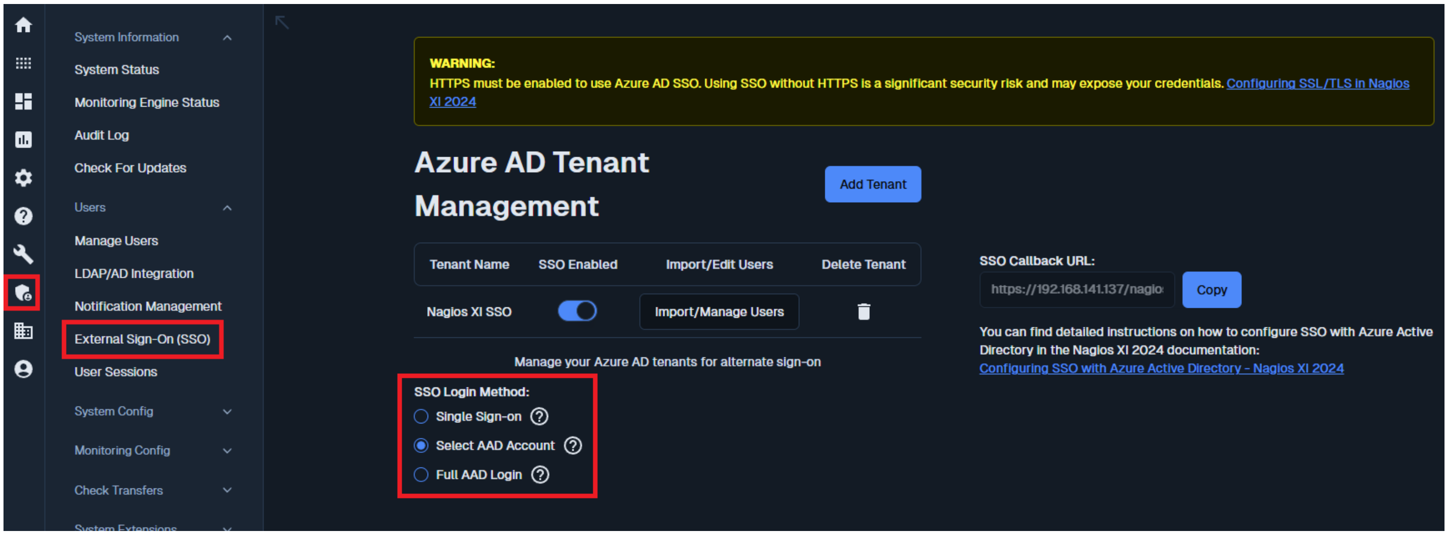
Number Format: 1000.00

Week Format: Sunday - Saturday

Login Methods

There are three options for login methods using Azure AD:

- **Single Sign-on** – Single Sign-on will only make the user log in once and so long as Microsoft continues to recognize them as logged in on their browser, they can log back in to Nagios XI by clicking the Sign in with Microsoft button on the login screen.
- **Select AAD Account** – Upon selecting the Sign in with Microsoft button, Select AAD Account will present the user with a list of their previously used logins with Microsoft and if they need to log in, it will present them with a password prompt.
- **Full AAD Login** – This will force the user to enter their Microsoft email and password to log in.



WARNING:
HTTPS must be enabled to use Azure AD SSO. Using SSO without HTTPS is a significant security risk and may expose your credentials. Configuring SSL/TLS in Nagios XI 2024

Azure AD Tenant Management

Tenant Name	SSO Enabled	Import/Edit Users	Delete Tenant
Nagios XI SSO	●	Import/Manage Users	🗑

Manage your Azure AD tenants for alternate sign-on

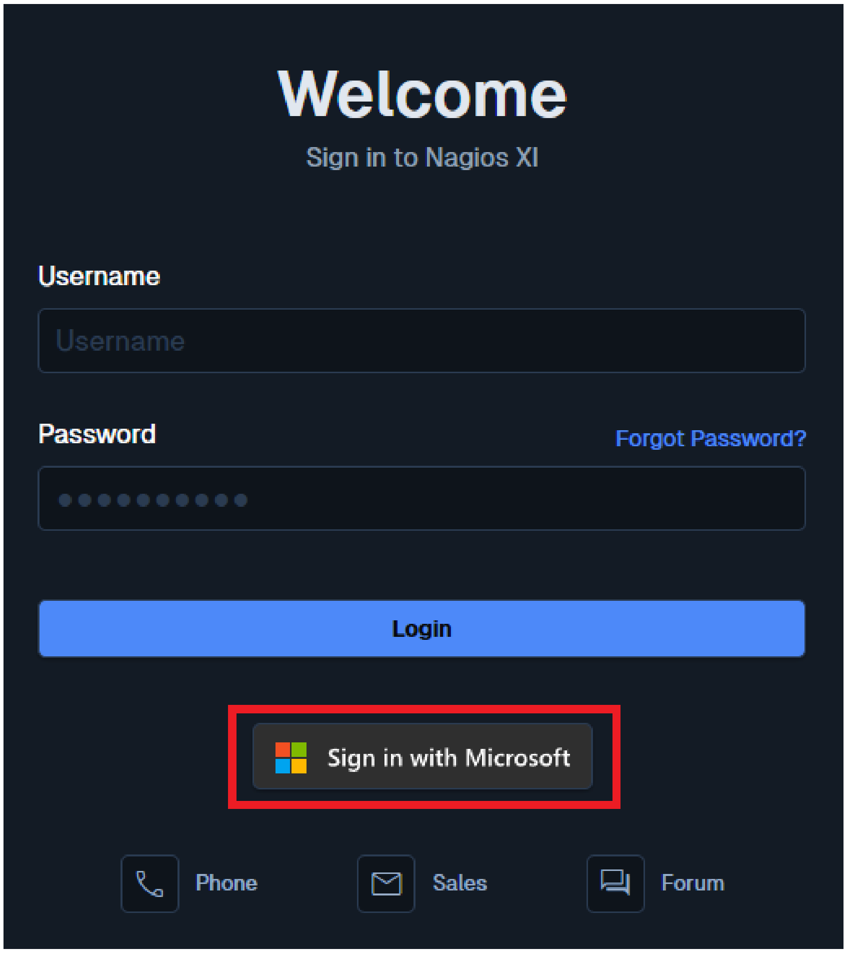
SSO Login Method:
○ Single Sign-on
● Select AAD Account
○ Full AAD Login

SSO Callback URL: https://192.168.141.137/naglo

You can find detailed instructions on how to configure SSO with Azure Active Directory in the Nagios XI 2024 documentation:
Configuring SSO with Azure Active Directory - Nagios XI 2024

Logging in to Nagios XI with SSO through Azure AD

Once configured, you will be able to log in to Nagios XI via SSO using the **Sign in with Microsoft** button on the Nagios XI login screen.



You will then be redirected to Microsoft to log in. Upon logging in, if your login is verified, you will be automatically logged in to Nagios XI.

Finishing Up

This completes the documentation on configuring Single Sign-On with Microsoft Azure Active Directory (AAD) for Nagios XI. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forums or Nagios Knowledge Base:

Visit Nagios Support Forum

Visit Nagios Knowledge Base