How-To Guide

Configure Single Sign-On (SSO) in Netsurion Open XDR

Publication Date:

17 October 2023

Table of Contents

1   Overview

This document describes the configuration of Netsurion Open XDR's Single Sign-On (SSO) feature that facilitates to securely authenticate users using Microsoft Entra ID (formerly known as Azure AD) credentials.

*Azure Active Directory (AAD) is now Microsoft Entra ID.

2   Configuring Single Sign-On (SSO) in Netsurion Open XDR

Perform the following procedure to configure the SSO login in Netsurion Open XDR.

1. In the Netsurion Open XDR console, hover over **Admin** and go to **Manager** Configuration.

2. In the **Manager** interface, scroll down to the **Single Sign-On (SSO)** section, select the **Enable Sign in using Single Sign-On (SSO)** check box and click **Save** to enable the SSO feature.

   The details for the **Identifier** (Entity ID) and **Reply URL** (Assertion Consumer Service URL) fields will be retrieved automatically.
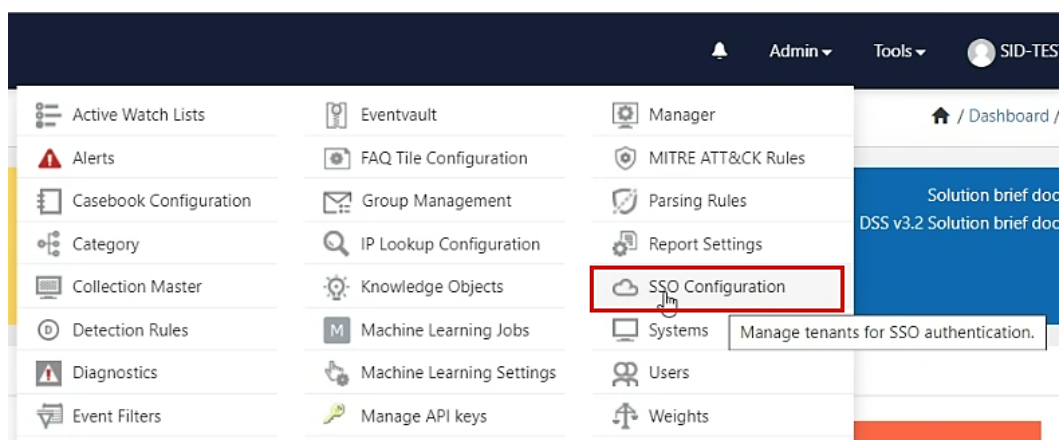

3. After enabling Single Sign-On (SSO), re-login to the Netsurion Open XDR console to view the SSO configuration option in the **Admin** menu.

3 Registering Netsurion Open XDR in Microsoft Entra ID (Azure Active Directory)
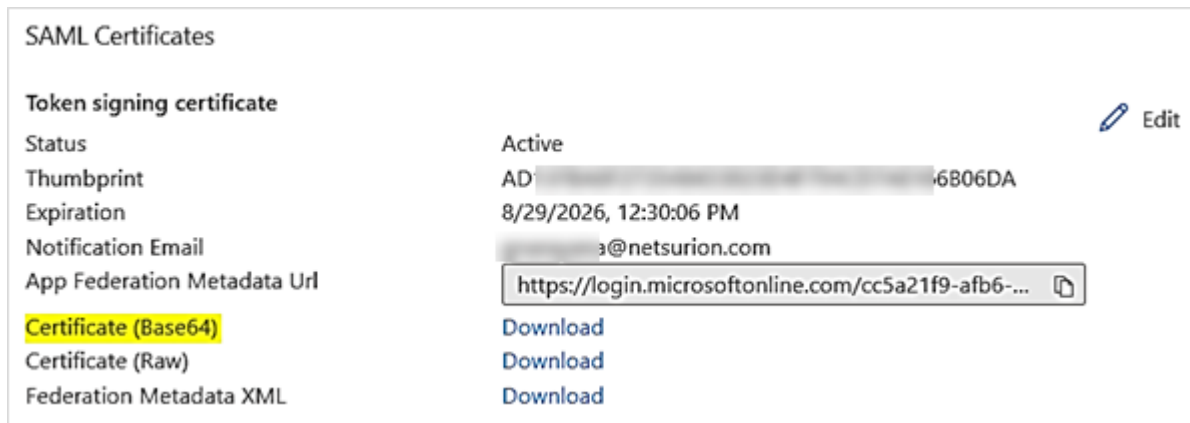
After setting the SSO configuration in the Netsurion Open XDR console, perform the following procedure to register Netsurion Open XDR in Microsoft Entra ID.

1. Log in to the [Azure](#) portal, and go to **Azure Services** > **Microsoft Entra ID** and go to **App registrations** to register Netsurion Open XDR.

2. In **App registrations**, click **+New registrations** and add the application (For e.g., **Netsurion Open XDR)** to the Microsoft AAD list.

3. Configure Single sign-on using Basic SAML by following Microsoft documented procedure. Use the Identifier and Reply URL obtained in [Chapter 2](#) (above) for SAML configuration.
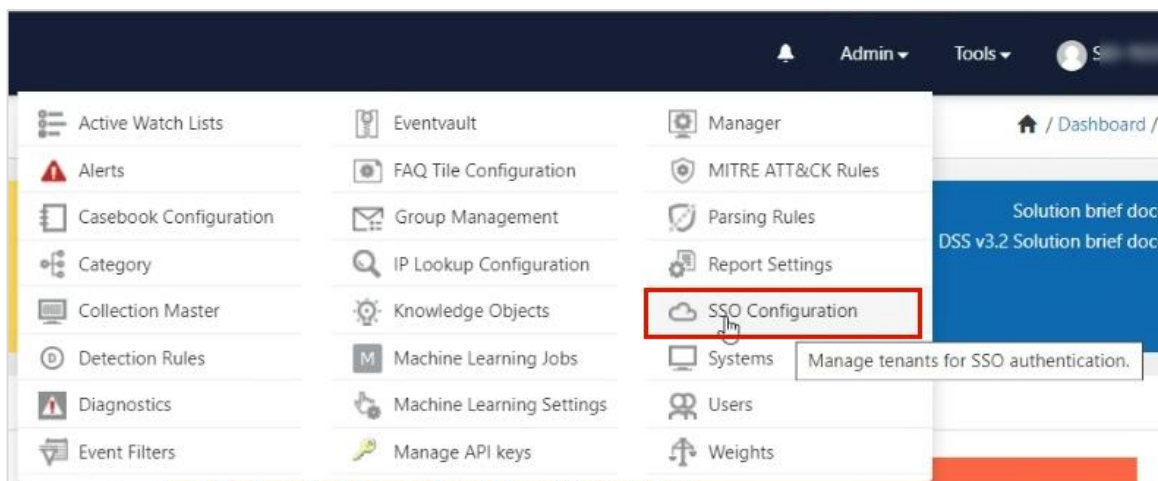
> **Note**:
>
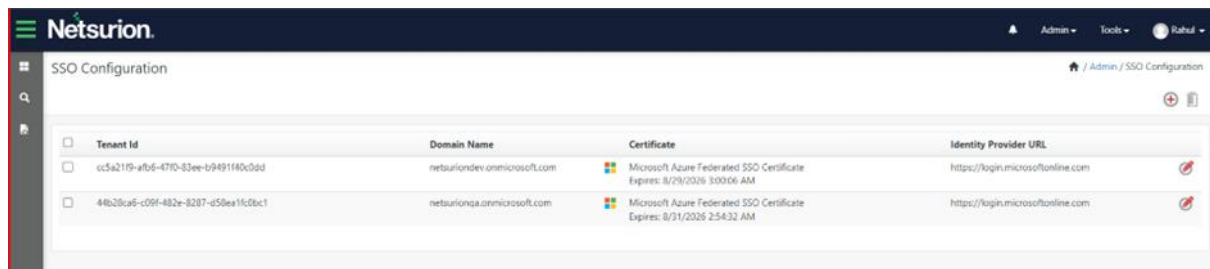> After configuring SSO, assign users and groups.

4. After setting the SSO, go to **SAML Certificates** and download **Certificate (Base64)**.

5. Next, login to the **Netsurion Open XDR** console, hover over the **Admin** menu and go to **SSO Configuration**.

6. In the **SSO Configuration** interface, click Add ⊕ to add the Tenant details.

7. In the **Add tenant details** window, specify the details for **Tenant Id**, **Domain Name**, **Certificate File** and click **Save** to add the tenant.

Note:

All the tenant information will be available in **Azure portal** > **App registrations**.
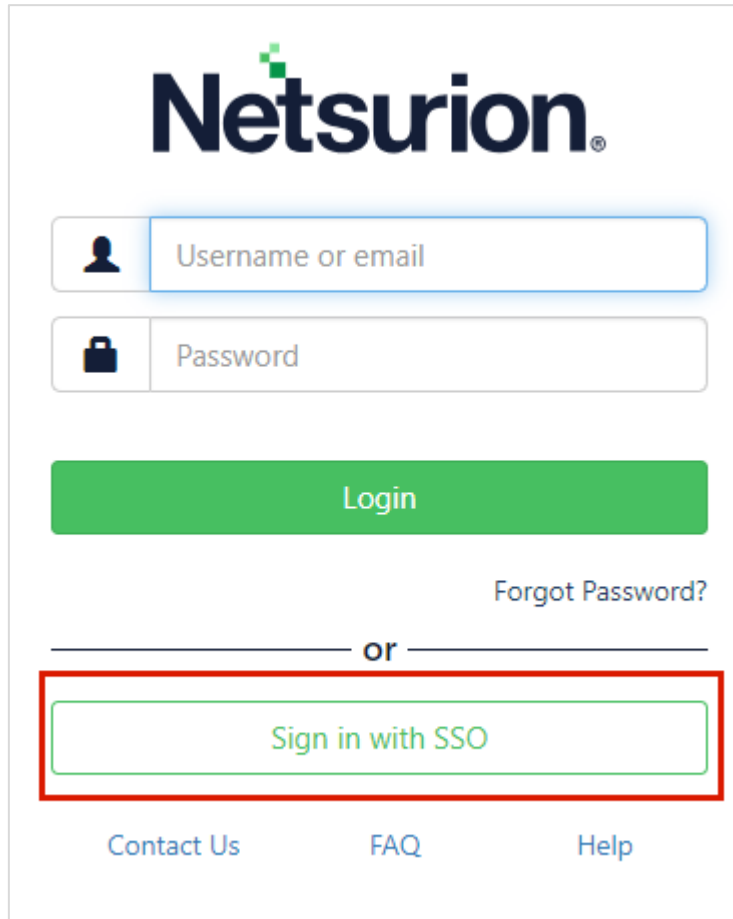
4 Logging into Netsurion Open XDR with Single Sign-On (SSO)

Once above configuration is configured successfully then Single Sign-On will be enabled for users.

1. In the **Netsurion Open XDR Login** page, click **Sign in with SSO**.

Netsurion®

2. In the **Single Sign-On** window, enter the appropriate email ID and click **Continue**.
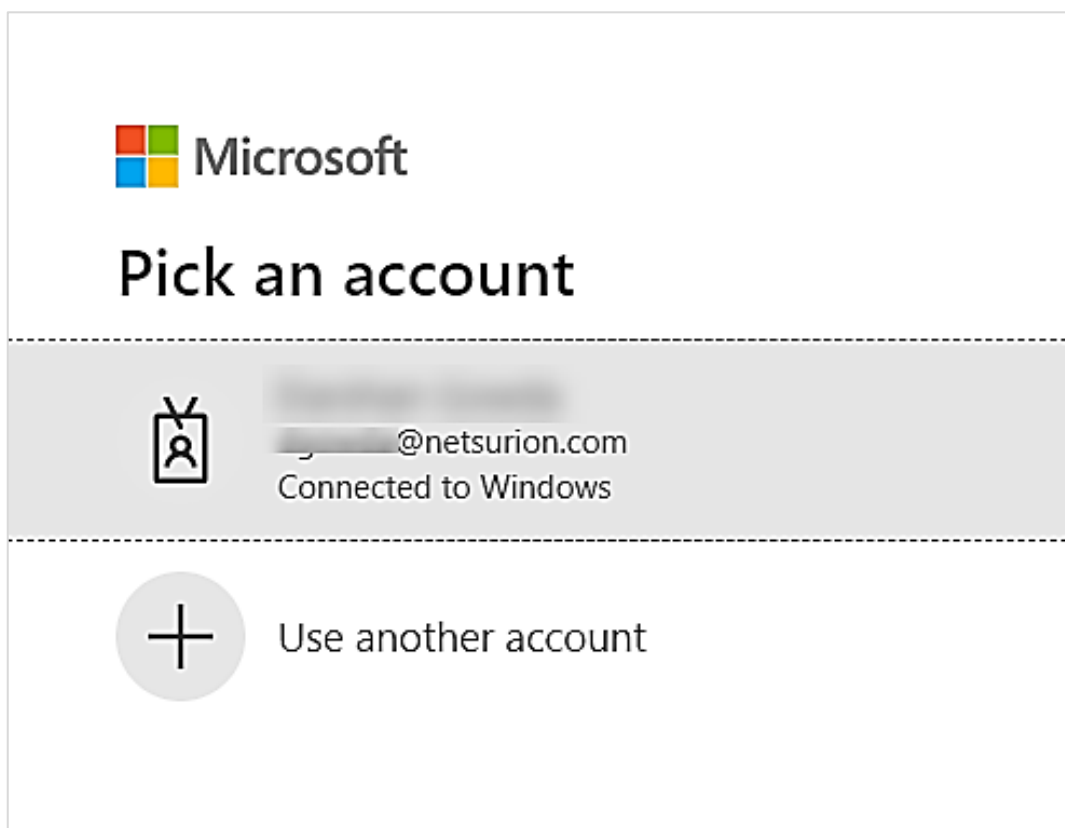
Netsurion®

IMPORTANT

It is important to add the users in the Netsurion Open XDR platform for SSO to work. In case, if a user is not registered in the Netsurion Open XDR platform, an error message appears stating *User is not found*.

In case, if a user is not assigned with SSO login permission in Microsoft Azure AD, an error message appears stating *Invalid email provided*.

In case, if an inactive user attempt logging in using SSO, an error message appears stating *Your login attempt was not successful. Please try again.*

3. The page will be redirected to Microsoft Authentication, select the appropriate ID to login using Azure credentials.

After the successful authentication, the user will be logged in to the Netsurion Open XDR console.

Points to Note

- Change password will not be available when user logged in through the SSO login.

- Modify or reset password done inside the Netsurion Open XDR platform will not affect the SSO login.

- The **Start In** Login feature functionality remains same.

- Users can Add or Modify or Delete multiple tenants in SSO Configuration.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support