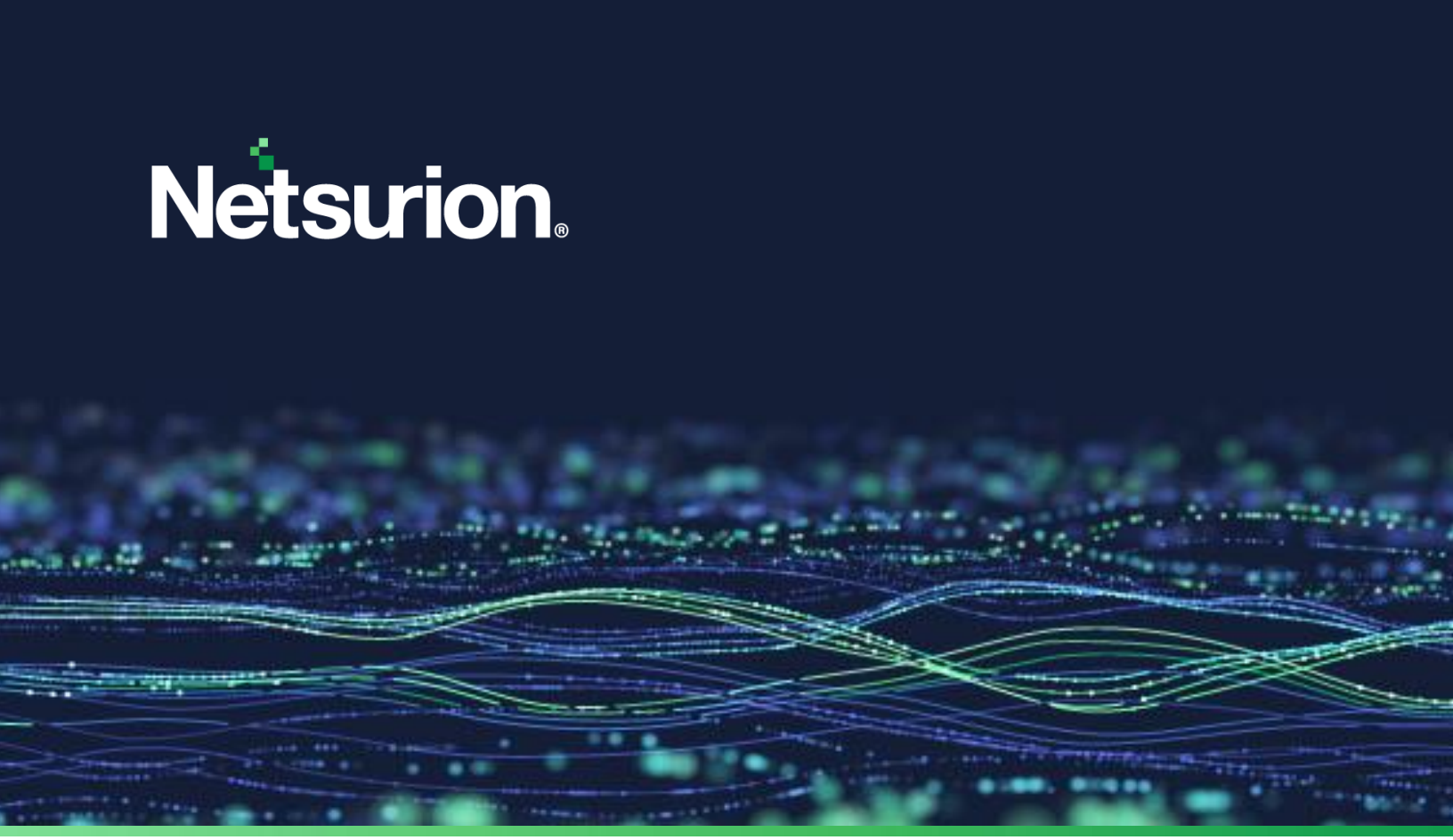


How-To Guide

Configure Two-Factor Authentication (2FA) using Authenticator App

Publication Date
March 06, 2024

Abstract

This document provides the steps to configure Two-Factor Authentication (2FA) on the user's mobile phone (Android and IOS) via the Authenticator App.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Netsurion Open XDR 9.4.

Audience

This guide is for the administrators responsible for configuring Two-Factor Authentication.

Table of Contents

1 Overview

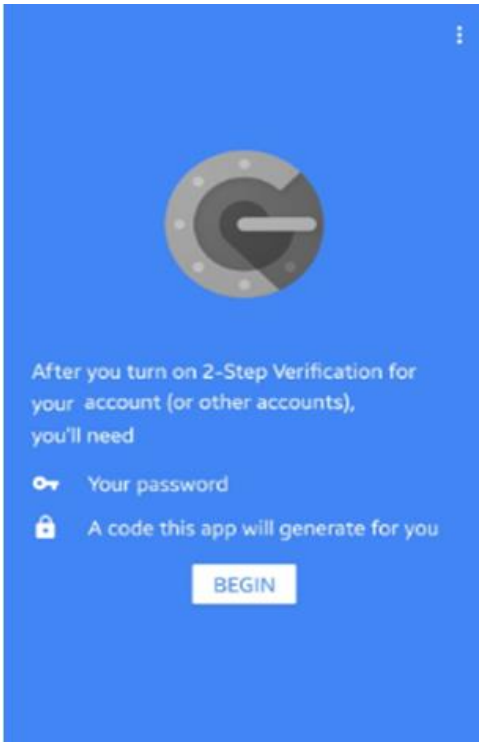
Netsurion Open XDR 9.4 supports Two-Factor Authentication using the Google Authenticator App or Microsoft Authenticator App. The Two-Factor Authentication, also known as 2-step verification helps to secure the Netsurion Open XDR account using a Password and an Authenticator PIN. The Authenticator configured on the phone provides an additional level of security to the account.

2 Configuring 2FA using the Authenticator App

1. Install the Authenticator App on your phone.

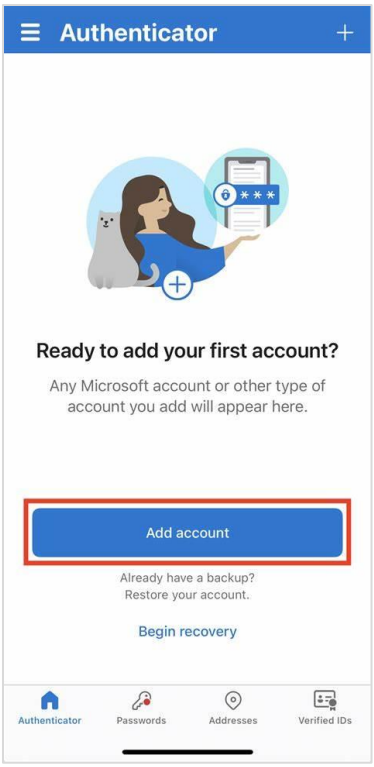
Note
The Authenticator screens vary according to the Authenticator apps and devices (Android or IOS).

2. Launch the Authenticator app. The following screen opens. Click **Begin** to proceed further.

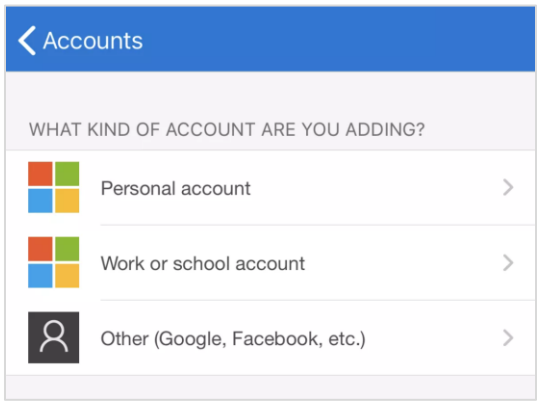


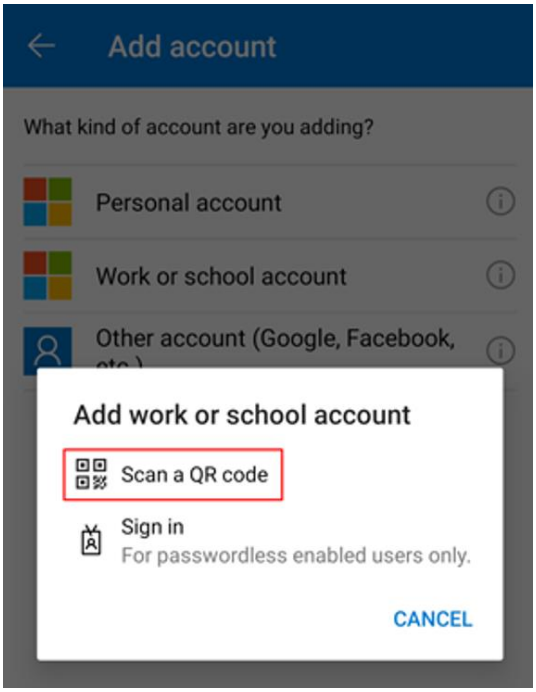
Note
If the Authenticator App is already installed on your phone and configured for any other application, this screen will not be displayed. Sample screenshots for the Google Authenticator and Microsoft Authenticator are provided below.

3. A screen to add an account will be displayed as shown below. Click **Add Account**.



4. On the next screen, select the type of account that you want to create.





5. An account can be added in two ways:
    a. Scan QR Code
    b. Enter Secret Key

The procedure is explained in the following sections.

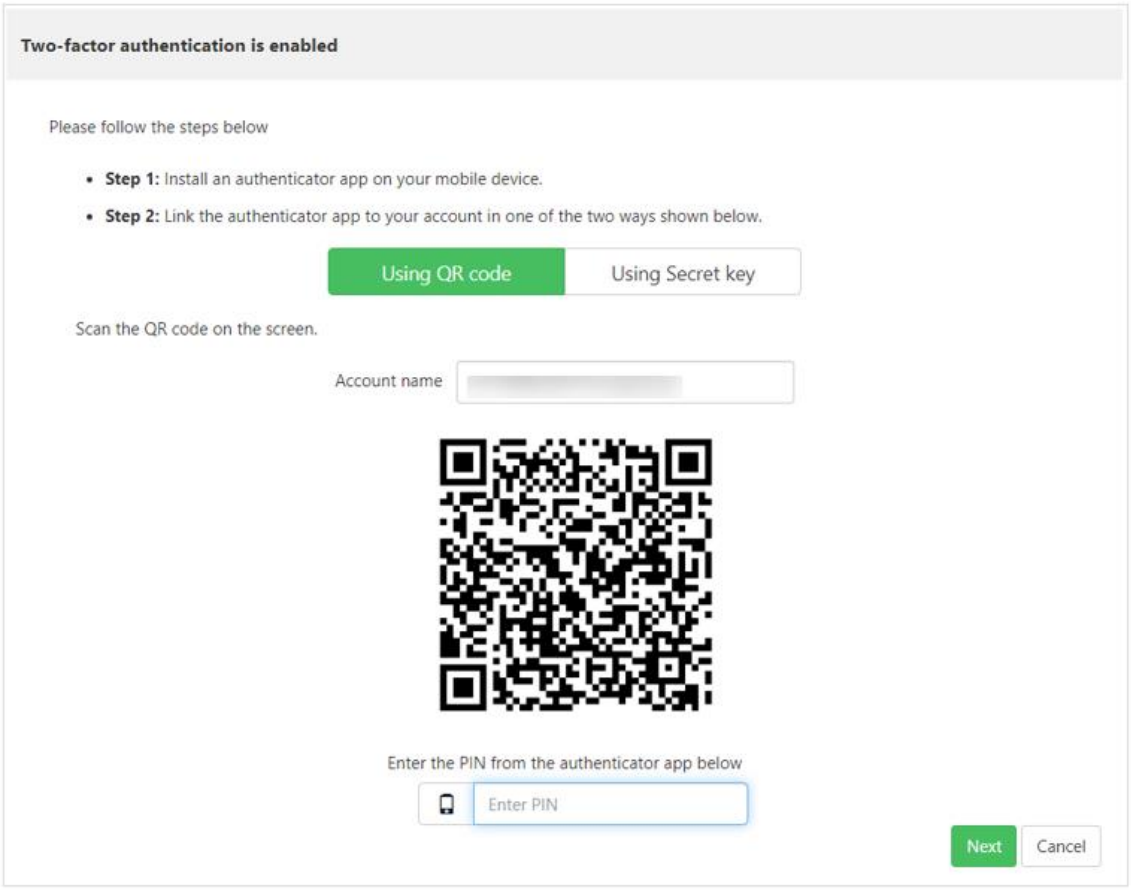
2.1 QR Code

1. Log in to the Netsurion Open XDR Web console from your system with the username and password. The **Two-factor Authentication using Authenticator page** opens. The **QR Code** option is selected by default.

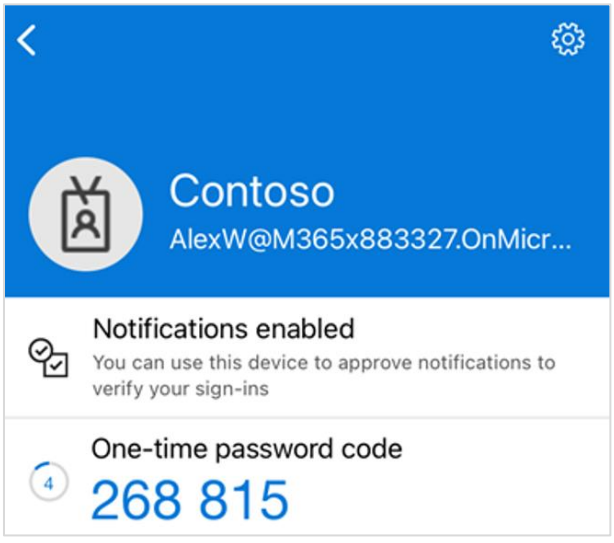
Note
This page is displayed only when your administrator has enabled 2FA for your account.

2. On the Authenticator App, select the **Scan QR Code** option and capture the QR code available on the screen.

Note
By default, the account name is captured as your Netsurion Open XDR domain. If you wish to change it, enter the name as per your requirement and reload the QR code. Scan the same to proceed further.



3. After the QR code is scanned successfully, the account will be added, and upon clicking that, a PIN will be generated.



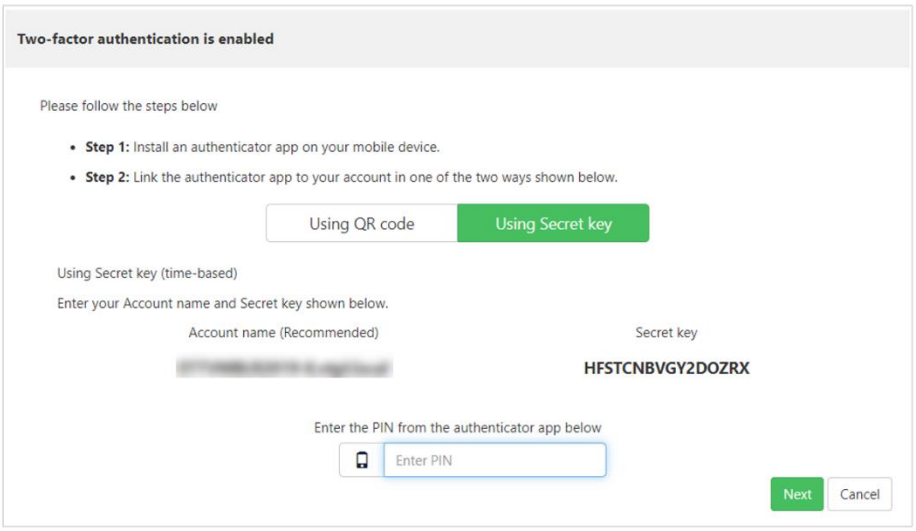
4. Enter the PIN on the Authenticator page and click **Next** to proceed further.

2.2 Secret Key

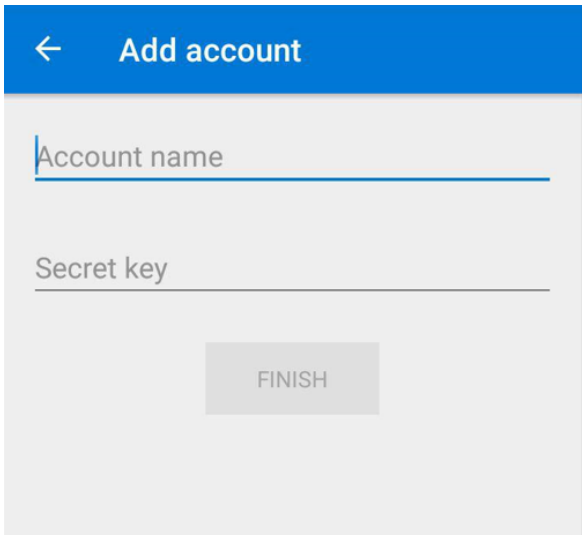
1. Log in to the Netsurion Open XDR Web console from your system with the username and password. The **Two-factor Authentication Using Authenticator page** opens.

Note
This page is displayed only when your administrator has enabled 2FA for your account.

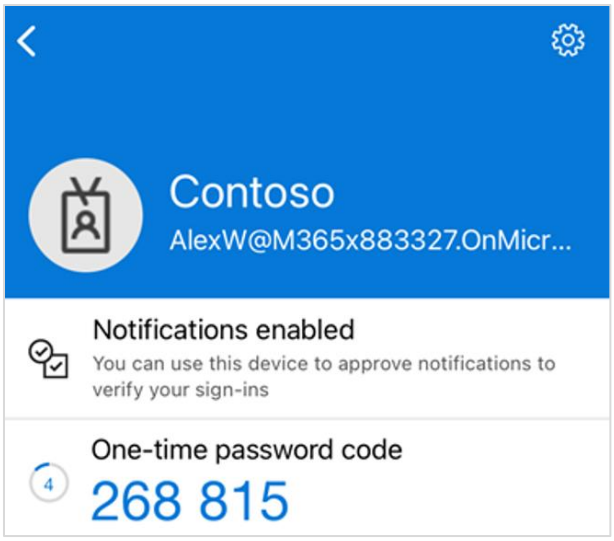
2. Select the **Using Secret key** button. A secret key will be generated as shown below:



3. On the Authenticator App, tap the **Other** option on your phone, then select **Or Enter Code Manually.**
4. A screen to enter the account details will open. Provide the account name and key.



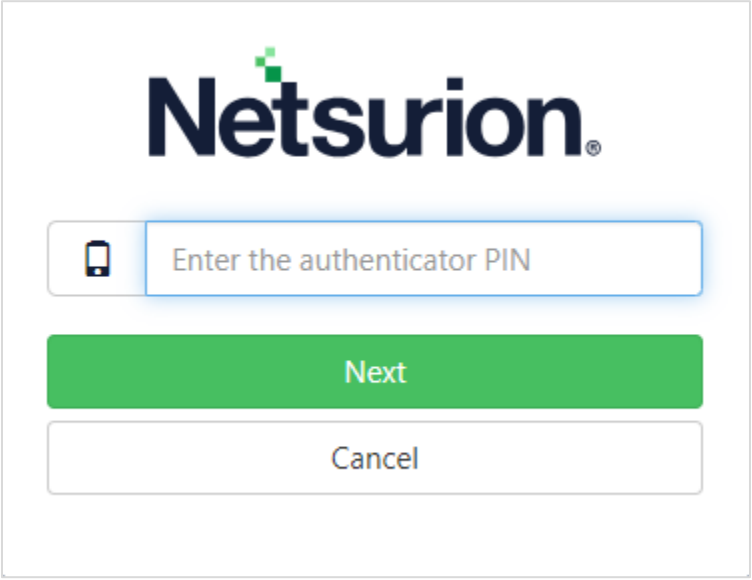
5. Click **Finish**.
6. A PIN will be generated as shown below:



7. Enter the PIN on the Authenticator page and click **Next** to proceed further.

3 Logging in to the Web Console after Configuring 2FA

Each time when you log in to the Netsurion Open XDR Web console with the username and password, you will be prompted to enter the authentication PIN generated in the Authenticator app.

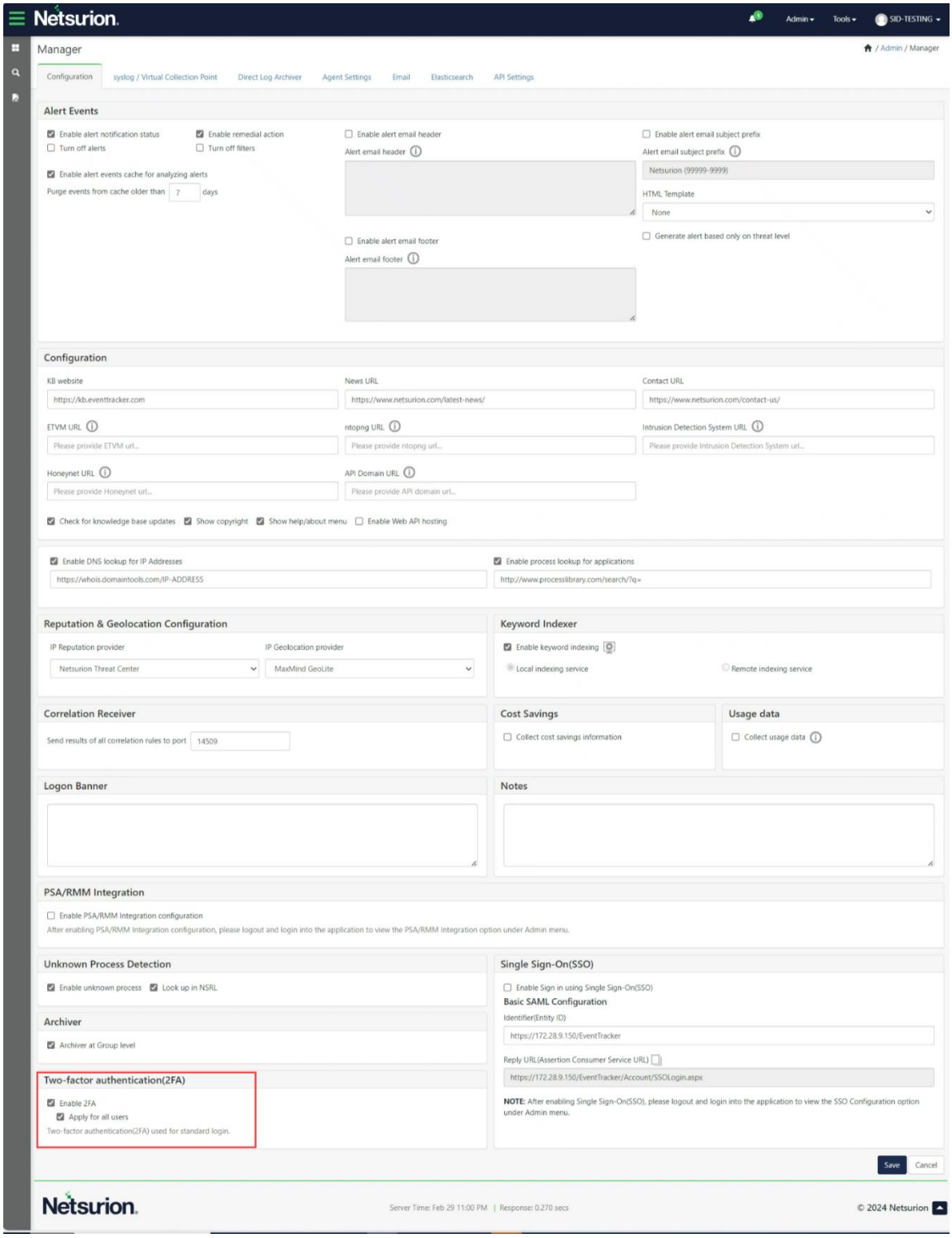


4 Enabling Two-Factor Authentication

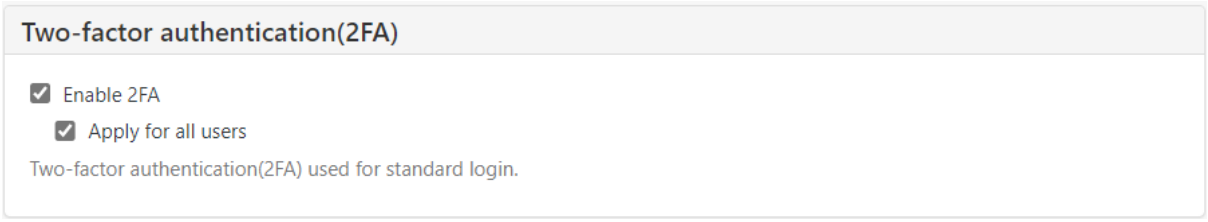
This section is for the Netsurion Open XDR admins and User Management admins who manage the user accounts in Netsurion Open XDR.

To enable the 2FA option in Netsurion Open XDR 9.4, perform the following steps:

1. Log into Netsurion Open XDR, click **Admin,** and then click **Manager.**
2. The **Manager screen** appears as shown below. Scroll down and enable **2FA Authentication**.



3. Enabling the 2FA option also enables the option **Apply for all users**. This will enable 2FA for all the users excluding the Netsurion Open XDR admins.

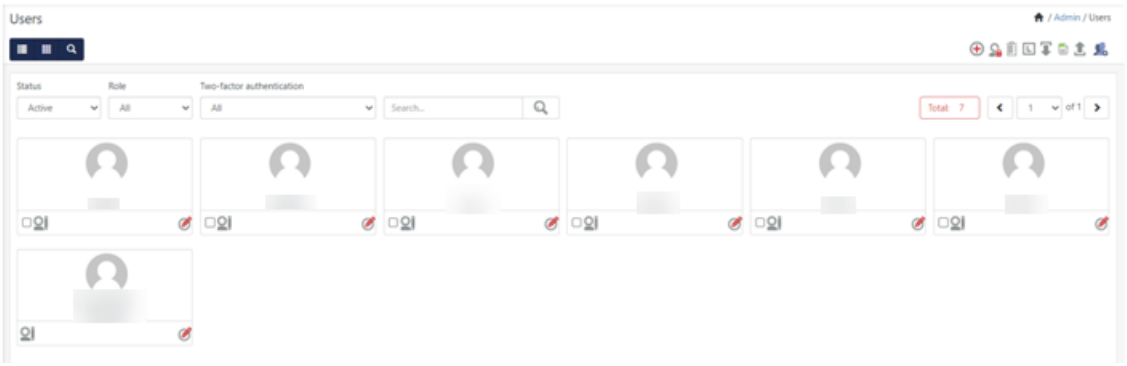


4. You can also disable the option if you decide not to apply 2FA for all the users.

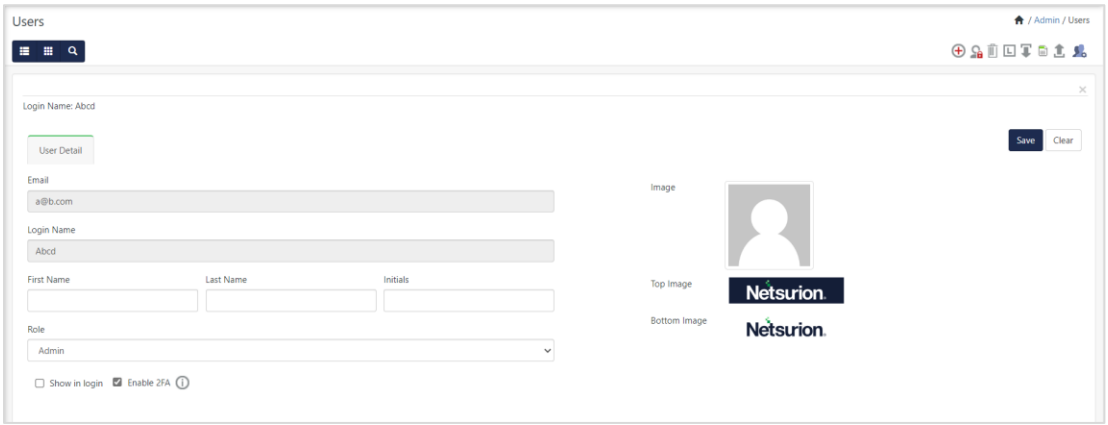
4.1 Enabling 2FA for Individual Users

This feature applies to Netsurion Open XDR admins, MSP admins, MMSP admins, and those who manage the user accounts.

1. Click **Admin** > **Users.** The user page appears as shown below:



2. To enable/disable the 2FA authentication option for the individual user level, click the **Edit** icon.



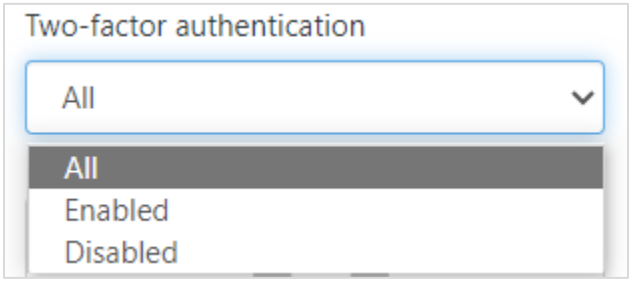
Note

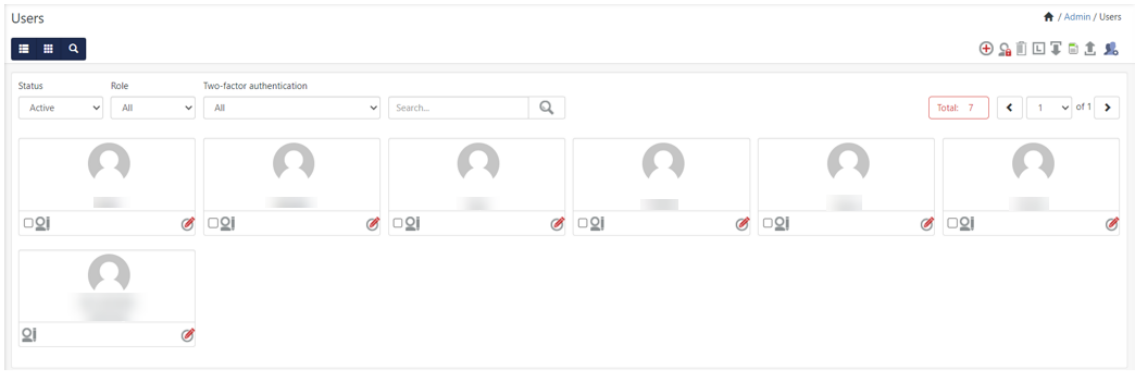
- 2FA can be either enabled or disabled based on the requirements.
- Disabling 2FA will allow the user to log into the Netsurion Open XDR Web console with just a username and password.

4.2 Enabling 2FA for All Users

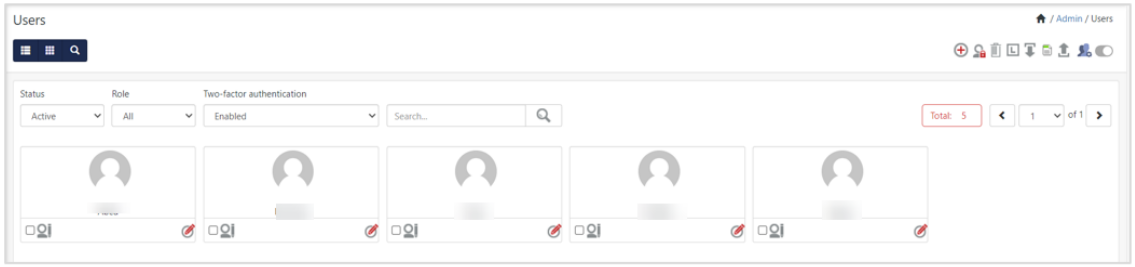
This feature applies to Netsurion Open XDR admins, MSP admins, MMSP admins, and those who manage the user accounts.

1. Click the **Two-factor authentication** drop-down and choose **All** to display all the users.

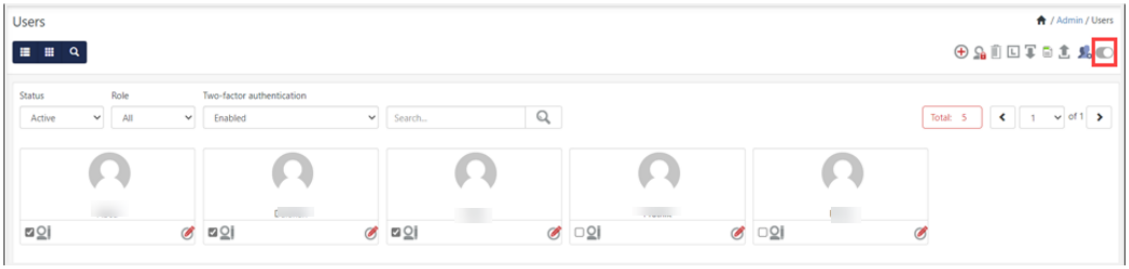




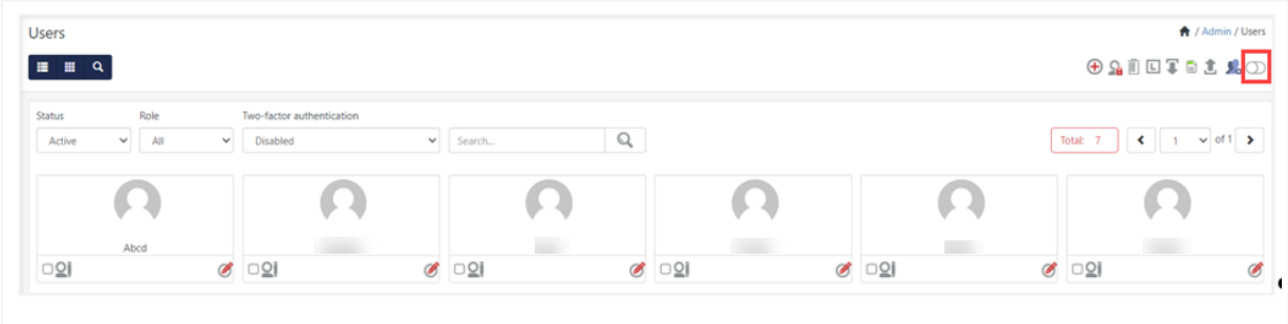
2. From the same drop-down, select **Enabled** and all the users for whom the Two-Factor authentication is enabled will be displayed.



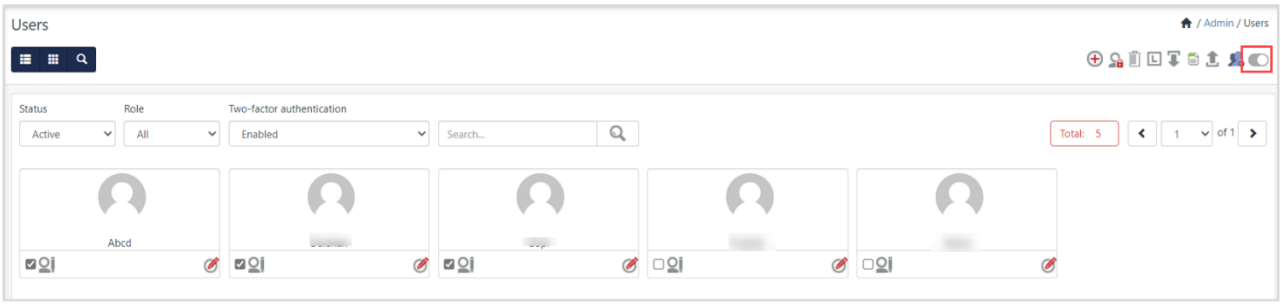
3. Select the users you wish to disable 2FA and click the toggle button on the top-right corner to disable 2FA.



4. Similarly, select **Disabled** from the drop-down, and all the users for whom the Two-Factor authentication is disabled will be displayed.



5. Select the users you wish to enable 2FA, and click the toggle button on the top right corner to enable 2FA.



5 FAQ's

1. **What shall I do if I have more than one Netsurion Open XDR Web console login?**

   You need to configure different accounts in the Authenticator App. By default, the account Name is set to the login URL domain. However, you can choose to select your account name at your convenience.

2. **What shall I do if I accidentally delete the account configured on the Authenticator App?**

   Please contact your Netsurion Open XDR Administrator to reset the 2FA for your account. Once reset, you will be presented with the 2FA configuration screen upon your login to the Netsurion Open XDR Web console.

3. **What shall I do if I lose my mobile or buy a new mobile?**

   Please contact your Netsurion Open XDR Administrator to reset the 2FA for your account. Once reset, you will be presented with the 2FA configuration screen upon your login to the Netsurion Open XDR Web console.

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