CDO Login Issues - To Reset Passwords and 2-Factor Authentication Token (OTP)

Contents

Introduction
Background Information
How to Reset Login Password for CDO Portal?
How to Reset Your OTP or 2-FA token?
How to Reset OTP or 2-FA if You Don't Have Access to Old Authentication Application?
Related Information

Introduction

This document describes solutions to three common login issues that you might encounter when you attempt to log into Cisco Defense Orchestrator (CDO) Portal:

1. To reset lost login password.
2. To reset One Time Password (OTP) or Two-factor authentication (2-FA) token.
3. To reset OTP or 2-FA token, but have no access to old authentication application or device.

Background Information

CDO uses OneLogin as its identity provider, which facilitates both basic user management and 2-FA. In order to log into CDO, you first have to activate your account on OneLogin. Once confirmed, you are prompted to configure your second factor OTP. If you do not face any of the above three issues and simply want to learn how to log into the CDO UI, visit this link and click on visual walkthrough.

How to Reset Login Password for CDO Portal?

Note: This process to reset the main password (first factor authentication) can be done by yourself without the need to open a TAC case.

Here are the Step-by-step instructions to reset initial login password:


Enter your Email Address and Click CONTINUE as shown in the image.
Step 2. Once you receive the message as shown in the image, navigate to the email inbox that you would have entered in Step 1. Ensure that you also check your Spam filter if you do not receive an email within a few minutes.
Step 3. You then receive an email from OneLogin <noreply@onelogin.com> as shown in the image.

**Click** on the link within the email to reset your password.

If you have requested a new password for your OneLogin account, please click on the link below to select a new password.

If you did not request a new password, please ignore this email.

https://cdo.onelogin.com/password/reset?token=ef051e100e587d3cfa6bdf2158317030a9606777

Step 4. Enter a new password and click **SUBMIT**.

Ensure that you meet the minimum password policy criteria and requirements listed, as
That's it! You're set to log in with your new password at this point.

**How to Reset Your OTP or 2-FA token?**

*Note:* This type of reset is only really necessary if you want to transfer the authentication application to a new device such as a new cellphone, etc.

This can be done by you, provided you have access to your 2-FA application in your old cellphone, tablet, etc. CDO currently supports these authentication applications on mobile devices:

- Symantec VIP Access
- Google Authenticator
- OneLogin OTP

Here are the step-by-step instructions to reset OTP or 2-FA token:

Step 1. Navigate to [https://cdo.onelogin.com/client/apps](https://cdo.onelogin.com/client/apps). Log in to the portal with your existing password and OTP from the authentication app from your old device (cellphone, etc). Hover over
your name on the top right hand corner and click Profile as shown in the image.

Step 2. Under your profile, scroll down to 2-Factor Authentication section and click Revoke next to the old authentication app name. You can see that the authentication application is Google Authenticator but it might be different in your case, as shown in the image.

Step 3. Click Revoke again to revoke the OTP or authentication token, as shown in the image.

You can now setup your new device (cellphone, etc) with an authentication application. The procedure is the same as you would when you configure 2-FA for the first time and is listed here for reference.

How to Reset OTP or 2-FA if You Don't Have Access to Old
Authentication Application?

In this scenario, open a case with CDO TAC. CDO TAC would assist you to reset your 2-FA token and setup a new authentication application on your new device (if necessary).

Related Information

- [Cisco Defense Orchestrator Documentation](#)
- [Technical Support & Documentation - Cisco Systems](#)