CATO NETWORKS

Cato Client User Portal

USER GUIDE

Version 1.0

1. Overview of the User Portal

Admins and VPN users can use the Cato User Portal to easily manage the Cato Clients. Users can:

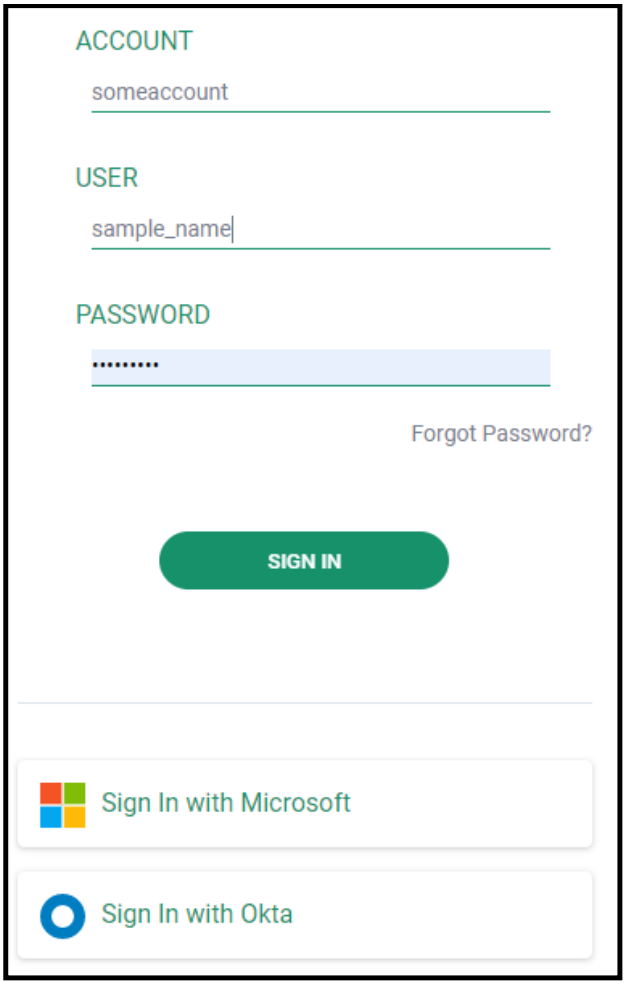
- Change the password for the Cato Client
- Show the trusted devices which only require MFA once during the set time period
- Download the most recent version of the Cato Client
- Download the Cato Certificate
- Change their MFA settings

1.1 Logging in to the User Portal

Log in to the User Portal (myvpn.catonetworks.com) using one of the following authentication methods. The same password is used for the Cato Client and the User Portal.

- Cato Client account name (only lower-case letters), username, and password
- SSO with Microsoft credentials
- SSO with Okta credentials

This screenshot is an example of logging in to the User portal with account, username, and password:

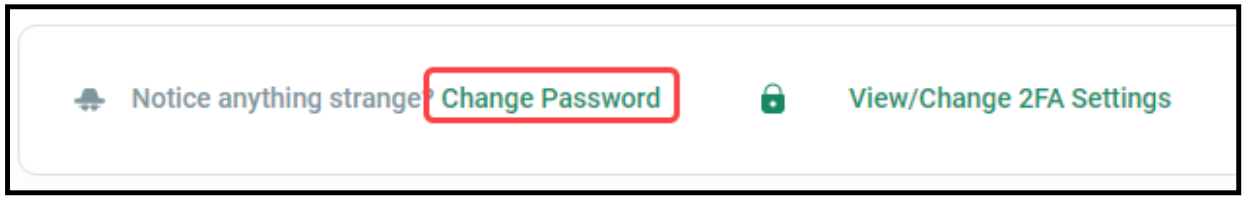


1.2 Changing the Password for the User Portal and Cato Clients

When you are logged in to the User Portal, you can change the password for the portal and the Cato Client. The same password is used for the Cato Client and the User Portal.

To change the User Portal and Cato Client password:

1. From the bottom of the **My Devices** window, click **Change Password**.



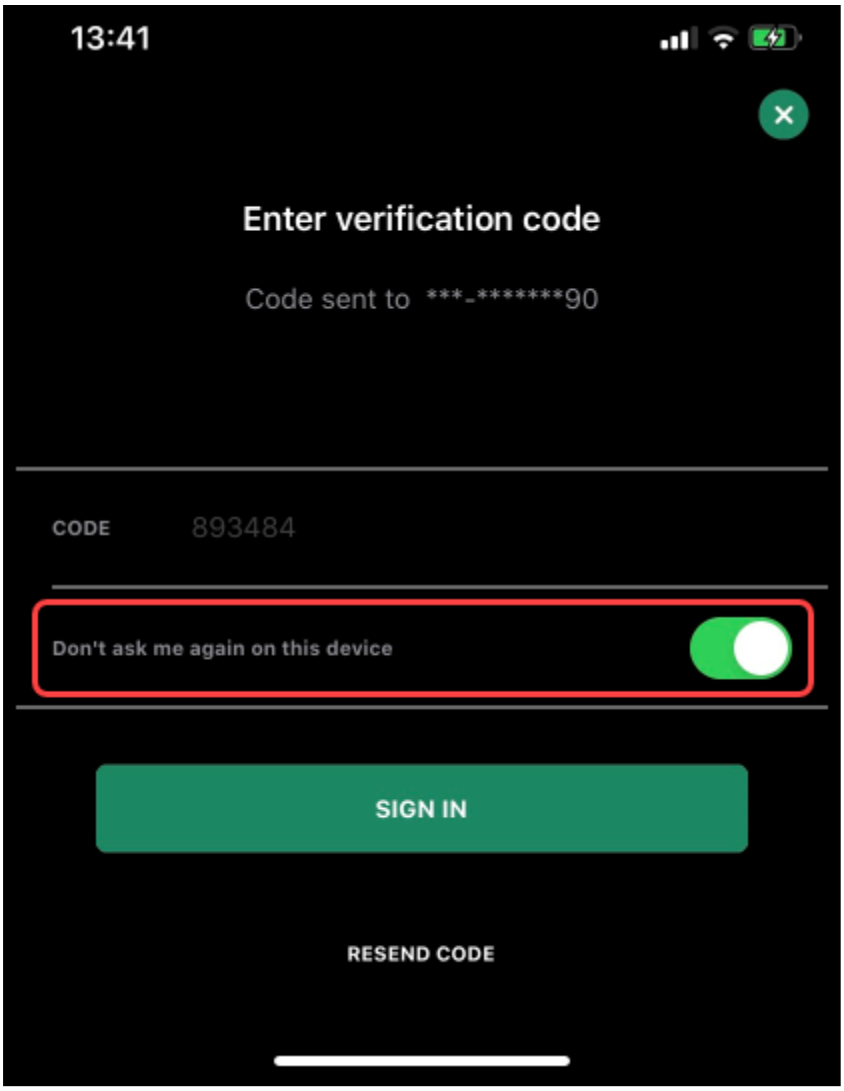
2. Enter your Cato Client **Current Password** and the new **Password**.
3. Click **Save**.

2. Working with Trusted Devices

For accounts or individual users that use Multi-Factor Authentication (MFA) for the Cato Client, the default behavior is to enter the extra authentication code each time they connect to the VPN. IT admins can choose to set the time period that the MFA token is valid, during this time the user doesn't require MFA. Users select the **Don't ask me again on this device/computer** option on the Client to designate that device or computer as trusted.

To configure a VPN client for a trusted device:

1. Log in to the Cato Client with the username and password.
2. On the MFA screen, select **Don't ask me again on this device**.



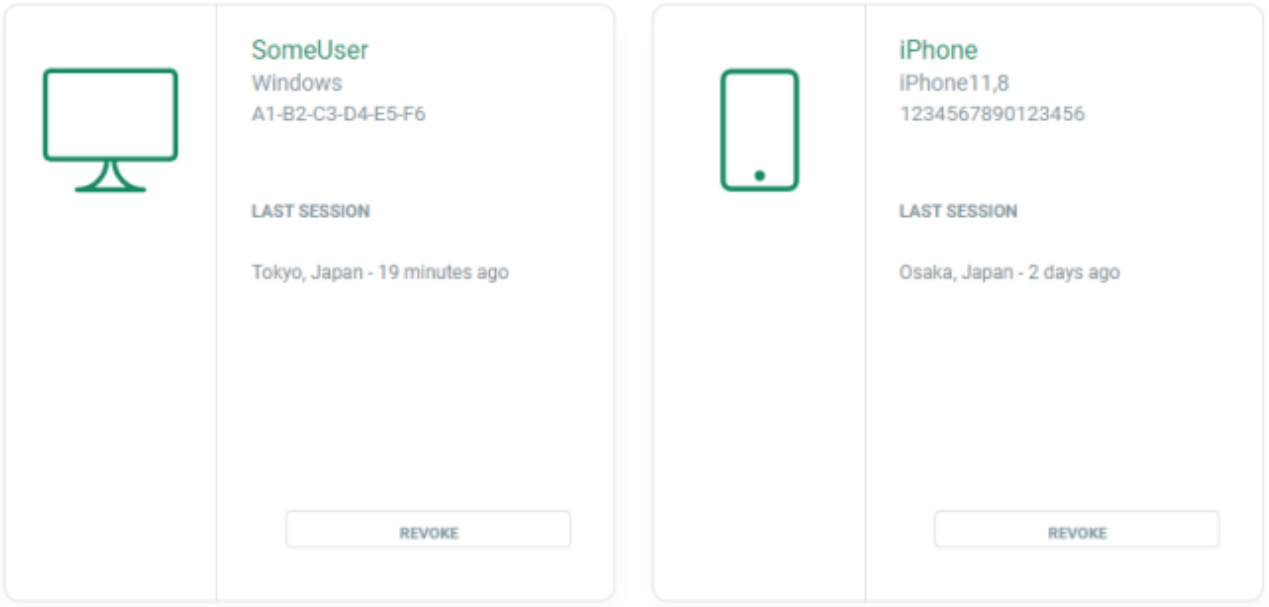
3. Enter the MFA code and click **Sign In**. After you are connected to the VPN, the device is trusted and MFA isn't required for the duration of the **Token Validity** setting.

2.1 Showing the Trusted Devices

The User Portal shows all the devices and hosts for a user that are defined as trusted devices.

To show the trusted devices for a user:

1. Log in to the User Portal (myvpn.catonetworks.com).
2. The **My Devices** window shows the trusted devices.



3. Downloading the Cato Clients

You can download the newest version of these Cato Clients from the User Portal:

- Windows
- Linux distributions:
  - Ubuntu (14, 16, 18)
  - Fedora (also RPM)
  - Debian
  - Centos

You can download the newest versions of these Clients from the respective app store:

- MacOS
- iOS
- Android

The User Portal has links to the above Cato Clients in their respective stores.

To download the newest version of the Cato Client:

1. From the User Portal, click **Download Cato Client**.
2. Click the tab for your operating system.
3. Click **Download VPN Client**.

4. Downloading the Cato Certificates

Install the Cato certificate on a device or host to define it as a root CA. This is necessary to let TLS inspection decrypt and then inspect traffic to provide the best threat protection for these endpoints.

When you install the Windows Cato Client on a host, the Cato certificate is installed automatically. For all other hosts and devices, you need to download and manually install the certificate.

You can also download the Cato certificate without logging in to the User Portal from here: https://myvpn.catonetworks.com/certificates

To download the Cato certificate:

1. From the User Portal, click **Download Cato Certificates**.
2. Click the tab for your operating system.
3. Click **Download Certificate**.

   For more about installing the certificate on the device or host, click **More info**.

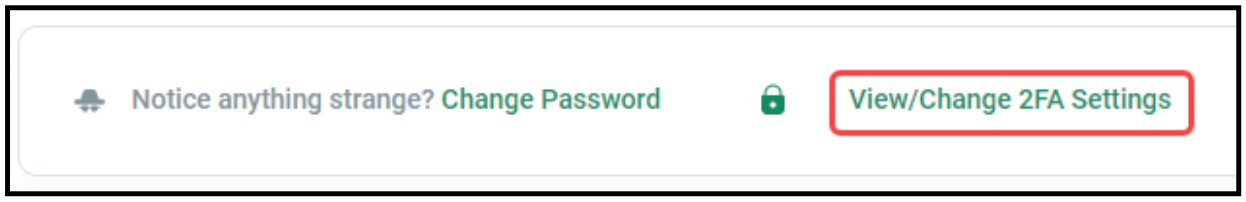
5. Changing the MFA Settings

The Cato Portal lets users make changes to the MFA settings for the Cato Client and the same settings are applied to the User Portal. For accounts that are configured for VPN users to use **Any Authentication Method** (MFA or SMS), they can change the MFA method that they are using. For example, someone who is using SMS to receive the MFA code can choose to use the Google authenticator app instead.

Note: The **View/Change 2FA Settings** link is only shown for accounts that let VPN users choose any MFA option.

To change the MFA settings:

1. From the bottom of the **My Devices** window, click **View/Change 2FA Settings**.



   The **My Account** window opens.

2. Click **Change Settings**.
3. In the pop-up window, enter the Cato Client password and click **Send**.

   The **Secure your account window** opens and helps you change the MFA settings

4. Follow the steps in the **Secure your account window** to make the changes to the MFA settings.
5. Click **OK**.