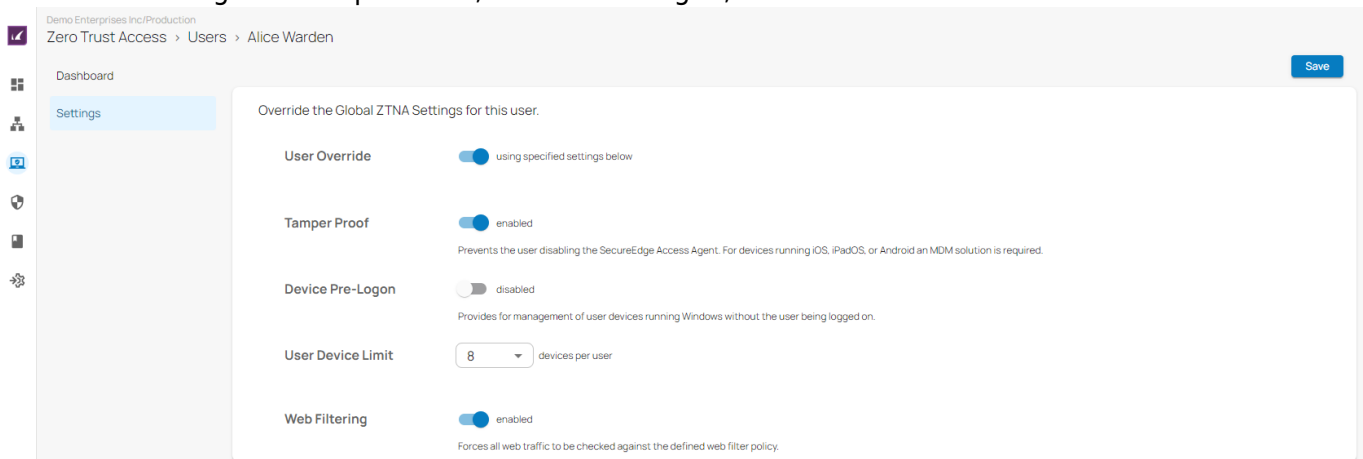


## How to Configure SecureEdge Access User Settings

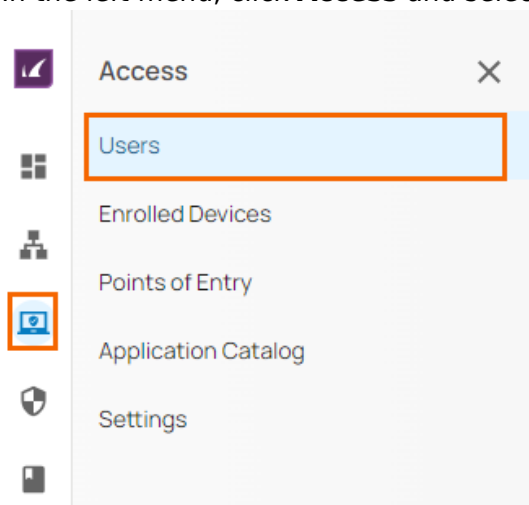
<https://campus.barracuda.com/doc/104381613/>

You can override the SecureEdge global Access/Default settings of the ZTNA features and create settings on a user level. You must first enable User Override for a specific user before configuring individual settings for Tamper Proof, Device Pre-Logon, and User Device Limit.



### Create an User Access Settings

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon.
3. From the drop-down menu, select the workspace your SecureEdge Access user should be configured for.
4. In the left menu, click **Access** and select **Users**.



5. The **Users** page opens. Select the user you want to edit.
6. To override the global SecureEdge Access settings for a specific user, click on the arrow icon next to the user.

Demo Enterprises Inc/Production  
Access > Users

Enroll users

Add filter Edit columns Download CSV

FULL NAME	EMAIL	USER OVERRIDE	TAMPER PROOF	DEVICE PRE-LOGON	DEVICE COUNT	ENROLLMENT COMPLETED	
Alice Warden	alice@companyazure.onmicr...				2 (8)		
Bob Smith	bob@companyazure.onmicro...				1 (8)		
Charlie Anderson	charlie@companyazure.onmi...				0 (2)		

7. The dashboard of the selected < **Name of User** > page opens. In the left menu, click **Settings**.


Demo Enterprises Inc/Production  
Zero Trust Access > Users > Alice Warden

Dashboard

Settings

Options Edit Dashboard

Device Map



Devices

USER	DEVICE BRAND	OPERATING SYSTEM	COUNTRY	ENROLLMENT DATE
Alice Warden	samsung	Android	United States of America	2024-05-14 08:10
Alice Warden	LENOVO	Windows	United Kingdom	2024-05-14 08:10

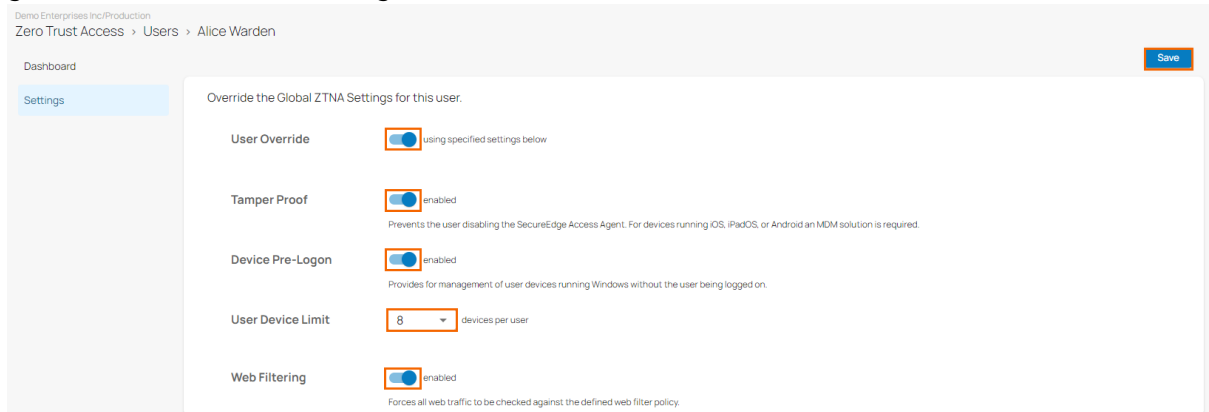
Summary Devices

Privacy Policy | Cookie Settings | © 2024 Barracuda Networks, Inc. All rights reserved. | Subscription serial: 123456789

Barracuda

8. The selected < **Name of User** > page opens. Specify values for the following:
- The individual user settings take precedence over the global Access/Default settings.
- User Override** – Click to enable/disable. By default, **User Override** is disabled.
- If **User Override** is enabled, specify the values for the following:
    - **Tamper Proof** – Click to enable/disable. By default, **Tamper Proof** is disabled.  
 Note: For devices running iOS, iPadOS, or Android, an MDM solution is required.
      - If **Tamper Proof** is enabled, the user will no longer be able to do the following:
        - Disable the SecureEdge Access Agent
        - Unenroll
        - The right-click **Quit** option for the SecureEdge Access Agent will not be available on the system tray.
      - If **Tamper Proof** is disabled, all of the above-mentioned features are available to the user.
    - **Device Pre-Logon** – Click to enable/disable. By default, **Device Pre-Logon** is disabled.
      - If **Device Pre-Logon** is enabled, administrators can manage user devices running Windows without the user being logged in. Note: This feature is available only for Windows.

- **User Device Limit** – Select a user device limit from the drop-down menu. You can choose between 1 to 10 devices per user. **User Device Limit** refers to the number of devices the user is allowed to enroll. By default, **User Device Limit** is 5.
- **Web Filtering** – Click to enable/disable DNS-based web filtering. By default, Web Filtering is enabled.
  - If **Web Filtering** is enabled, all web traffic will be checked against the defined Web Filter policy. You can enforce Web Filtering policies for the web traffic that the clients connect to via the SecureEdge Agent in order to establish a secure connection to access internal and external company resources. For more information, see [Web Filter Policies](#).
- If **User Override** is disabled, you are not allowed to set any of the ZTNA features. The global Access/Default settings will be used instead.



9. Click **Save**.

After configuration is complete, verify the user-level settings for a specific user on the SecureEdge Access Agent. The usage of ZTNA features is as follows:

- You can enable/disable Tamper Proof for a specific user if User Override is enabled
- You can enable/disable Device Pre-Logon for a specific user if User Override is enabled
- If User Override is enabled, you can increase/decrease the user device limit per user. By default, User Device Limit is 5. The range is between 1 and 10. You will get an enrollment error under the following circumstances:
  - If the user attempts to enroll more devices than the limit allows, an error message will be displayed.
  - Decreasing the number of devices in the global Access Settings is not allowed for a specific user when the user has already deployed the maximum number of devices. Attempting to do so will result in an error.

## Further Information

For more information how to set up ZTNA features on a global level, see [How to Configure SecureEdge Access Global Settings](#).

## Figures

1. settings\_user\_zta.png
2. goto\_access\_users.png
3. users\_page.png
4. zta\_dashboard.png
5. user\_level\_settings.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.