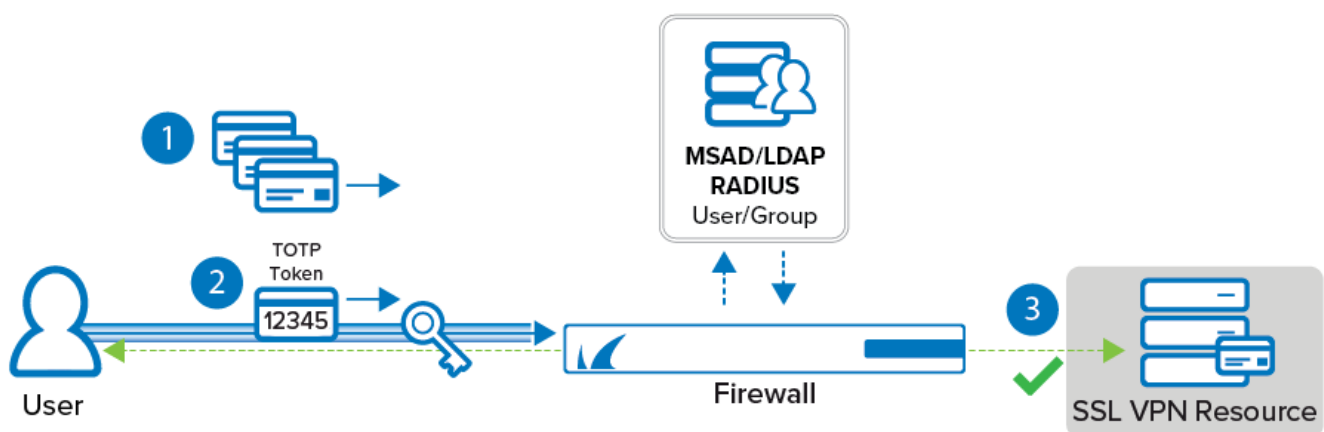


How to Configure Access Control Policies for One-Time Password Authentication

<https://campus.barracuda.com/doc/96026113/>

TOTP authenticators, such as Google Authenticator or Microsoft Authenticator, use Time-Based One-Time Passwords (TOTP) generated by an app on your mobile device to authenticate the user. The app generates temporary six-digit numbers calculated from a shared secret and the current time. To be able to use this on the CloudGen Firewall, the TOTP app must be enrolled by the user in a two-step process. To associate TOTP authentication with user and group information, a helper scheme such as MSAD or LDAP must be configured. TOTP authentication is supported for CudaLaunch, the SSL VPN web portal, and the Barracuda VPN Client. For SSL VPN users to be able to self-enroll, they must be able to access the SSL VPN through an Access Control Policy that is not using TOTP as an authentication method. After all users are enrolled, the admin can then switch to an Access Control Policy requiring TOTP authentication. To be able to share the linked accounts over managed firewalls in a single HA cluster, use a repository entry.



Enrolling Mobile Devices

- Create an SSL VPN Access Control Policy that allows users to log in without TOTP authentication.
- Instruct users to log into CudaLaunch or the SSL VPN web portal to enroll their devices. For more information, see [How to Self-Enroll for Time-Based One-Time Passwords \(TOTP\) Using CudaLaunch or the SSL VPN Web Portal](#).
- Deactivate the original Access Control Policy and enable an Access Control Policy using TOTP.

Before You Begin

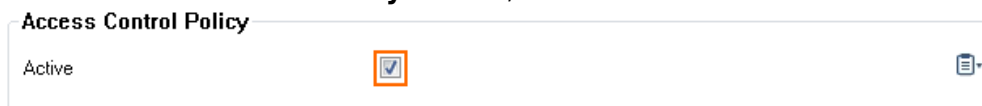
- Enable SSL VPN. For more information, see [How to Configure the SSL VPN Service](#).

- Configure an authentication scheme with user/group information such as MSAD or LDAP to be used as the **User Info Helper Scheme**. For more information, see [Authentication](#).
- Configure time-based OTP as authentication scheme and enable self-enrollment for Users and Groups. For more information, see [How to Configure Multi-Factor Authentication Using Time-based One-time Password \(TOTP\)](#).

Step 1. Configure an MFA Access Control Policy for TOTP Authentication

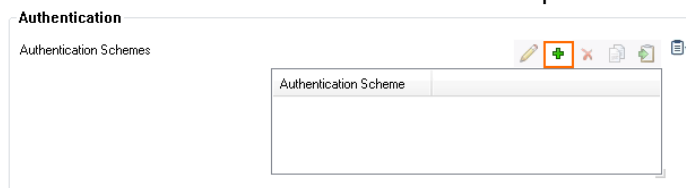
Configure an Access Control Policy using TOTP as the secondary authentication scheme.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu, click **Access Control Policies**.
3. Click **Lock**.
4. Click **+** to add an **Access Control Policy**. The **Access Control Policies** window opens.
5. Enter a **Name** and click **OK**.
6. In the **Access Control Policy** section, select the **Active** check box.



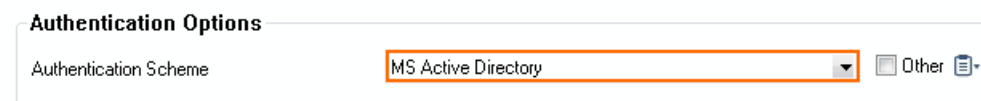
The screenshot shows the 'Access Control Policy' configuration window. It has a title bar 'Access Control Policy' and a checkbox labeled 'Active' which is checked. There is a small icon on the right side of the window.

7. (optional) Add **Allowed Groups** and **Blocked Groups**.
8. (optional) To use multi-factor authentication, add the primary authentication scheme:
 1. Click **+** to add the primary authentication scheme to the **Authentication Scheme** table. The **Authentication Scheme** window opens.



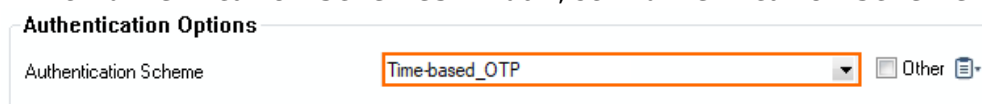
The screenshot shows the 'Authentication Scheme' configuration window. It has a title bar 'Authentication' and a subtitle 'Authentication Schemes'. There is a table with one column 'Authentication Scheme'. There are icons for adding, editing, deleting, and saving.

2. From the **Authentication Scheme** drop-down list, select the primary authentication scheme. E.g., **MS Active Directory**, or **LDAP**



The screenshot shows the 'Authentication Options' configuration window. It has a title bar 'Authentication Options' and a subtitle 'Authentication Scheme'. There is a dropdown menu with 'MS Active Directory' selected. There is a checkbox labeled 'Other' which is unchecked.

3. Click **OK**.
9. Click **+** to add TOTP to the **Authentication Scheme** table. The **Authentication Scheme** window opens.
10. In the **Authentication Schemes** window, set **Authentication Scheme** to **Time-based_OTP**.




The screenshot shows the 'Authentication Options' configuration window. It has a title bar 'Authentication Options' and a subtitle 'Authentication Scheme'. There is a dropdown menu with 'Time-based_OTP' selected. There is a checkbox labeled 'Other' which is unchecked.

11. Click **OK**.
12. (optional) Click **+** to add Network Access Control criteria to the **NAC Criteria** table.

13. Click **OK**.
14. Click **Send Changes** and **Activate**.

Step 2. Activate the Access Control Policy for TOTP Authentication

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu pane, click **SSL VPN Settings**.
3. Click **Lock**.
4. In the **Access** section, click **+** and select the Access Control Policy created in Step 2.

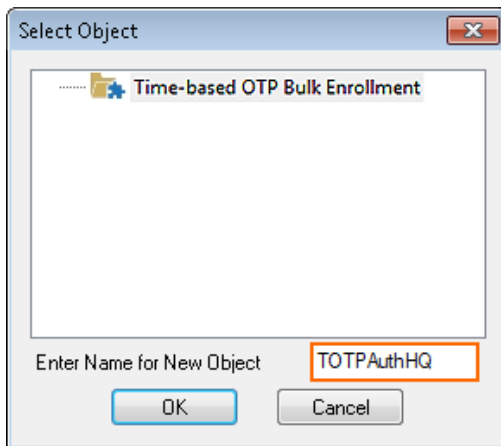


5. Click **Send Changes** and **Activate**.

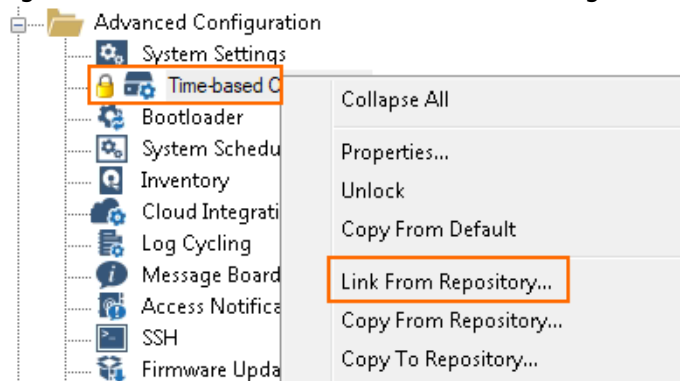
Step 3. (Single HA Cluster Only) Create a Repository Entry and Link

To be able to share the linked TOTP authentication accounts over managed firewalls in a high availability cluster, use a repository entry and create repository links. The primary and secondary firewall must use the repository entry.

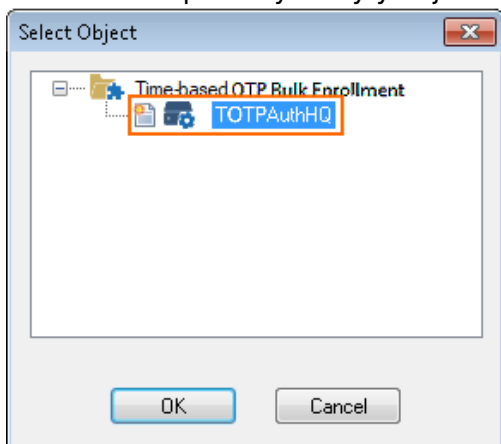
1. Log into the Control Center.
2. Go to **Your Managed Firewall > Infrastructure Services**.
3. Expand the configuration node, right-click **Time-based OTP Bulk Enrollment** and click **Copy To Repository**. The **Select Object** window opens.
4. Enter a **Name** for the new object.



5. Click **OK**.
6. Right-click **Time-based OTP Bulk Enrollment** again and click **Lock**.
7. Right-click **Time-based Bulk Enrollment** again and click **Link From Repository**.

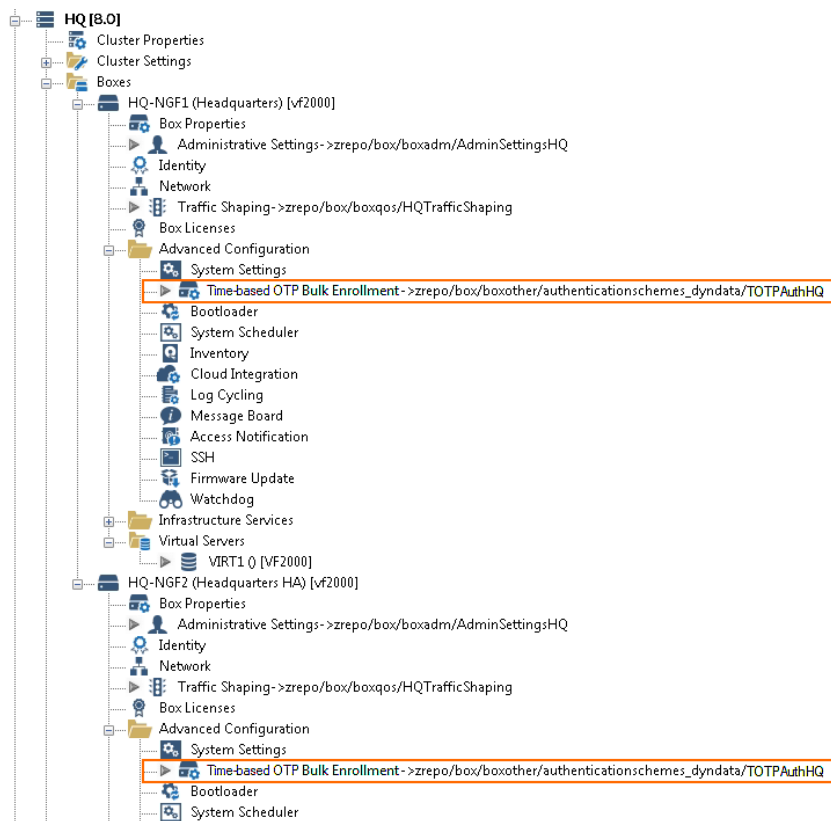


8. Select the Repository entry you just created.



9. Click **OK**.
10. Click **Activate**.

You can now link this repository entry to the secondary firewall in your HA cluster.



Figures

1. auth02.png
2. activate_auth_scheme_00.png
3. add_authentication_scheme_00.png
4. add_authentication_scheme01.png
5. set_auth_scheme_totp_00.png
6. add_authentication_scheme02.png
7. totp_auth_repository_01.png
8. totp_auth_repository_02.png
9. totp_auth_repository_03.png
10. totp_auth_repository_04.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.