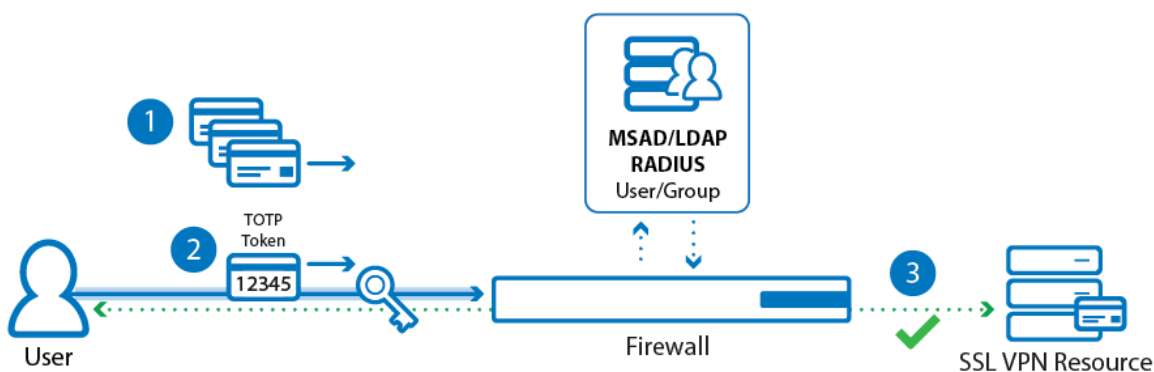


How to Configure Access Control Policies for One-Time Password Authentication

<https://campus.barracuda.com/doc/68359178/>

Google Authenticator or Microsoft Authenticator are authentication schemes using 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 Google Authenticator app must be enrolled by the user in a two-step process. To associate the Google/Microsoft Authenticator with a user and group information, a helper scheme such as MSAD or LDAP must be configured. Google/Microsoft Authenticator is supported for CudaLaunch and the SSL VPN web portal. For 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 Google/Microsoft Authenticator as an authentication method. After all users are enrolled, the admin can then switch to an Access Control Policy requiring Google/Microsoft Authenticator. 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 Google/Microsoft Authenticator.
- Instruct users to log into CudaLaunch or the SSL VPN web portal to enroll their devices. For more information, see [Enroll your Mobile Device for use Time-Based One-Time Passwords \(TOTP\)](#).
- Deactivate the original Access Control Policy and enable an Access Control Policy using Google/Microsoft Authenticator.

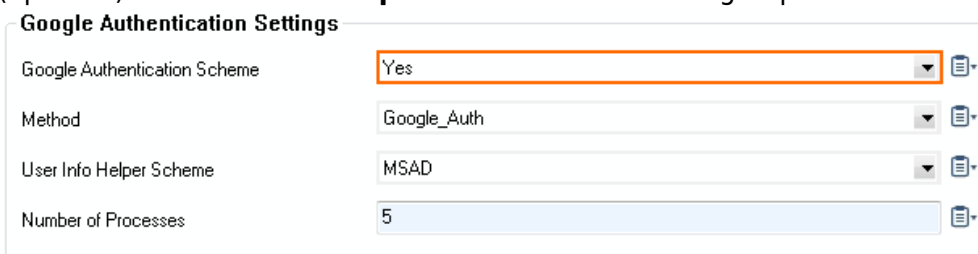
Before You Begin

- 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](#).

Step 1. Enable Google Authenticator

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left menu, click **Google Authentication**.
3. Click **Lock**.
4. From the **Google Authentication Scheme** drop-down list, select **Yes**.
5. (optional) Set **User Info Helper Scheme** to **MSAD** if group information is required.



The screenshot shows the 'Google Authentication Settings' configuration window. It contains four rows of settings, each with a label, a value, and a copy icon:

Setting	Value
Google Authentication Scheme	Yes
Method	Google_Auth
User Info Helper Scheme	MSAD
Number of Processes	5

6. Click **Send Changes** and **Activate**.

Step 2. Configure an MFA Access Control Policy for Google Authentication

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

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Service > VPN > 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 the **Name** and click **OK**.
6. In the **Access Control Policy** section, select the **Active** check box.



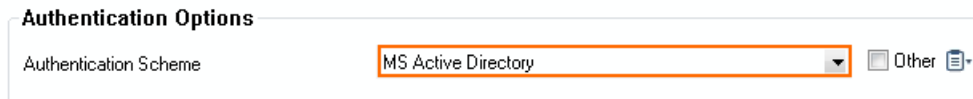
The screenshot shows the 'Access Control Policy' configuration window. It contains one row with the label 'Active' and a checked checkbox, followed by a copy icon:

Setting	Value
Active	<input checked="" type="checkbox"/>

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.



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



- Click **OK**.
- Click **+** to add Google Authentication to the **Authentication Scheme** table. The **Authentication Scheme** window opens.
- In the **Authentication Schemes** window, set **Authentication Scheme** to **GoogleAuth**.



- Click **OK**.
- (optional) Click **+** to add NAC criteria to the **Network Access Control Criteria** table.
- Click **OK**.
- Click **Send Changes** and **Activate**.

Step 3. Activate Access Control Policy for Google Authentication

- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN > SSL-VPN**.
- In the left menu pane, click **Login**.
- Click **Lock**.
- In the **Login** section, click **+** and select the Access Control Policy created in Step 2.



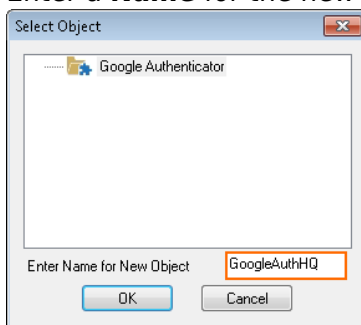
- Click **Send Changes** and **Activate**.

Step 4. (Single HA Cluster only) Create a Repository Entry and Link

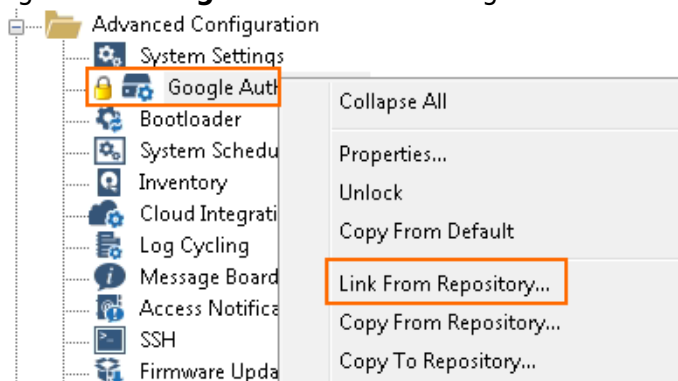
To be able to share the linked Google Authenticator accounts over managed firewalls in a high

availability cluster, use a repository entry and create repository links. The primary and secondary firewall must use the repository entry.

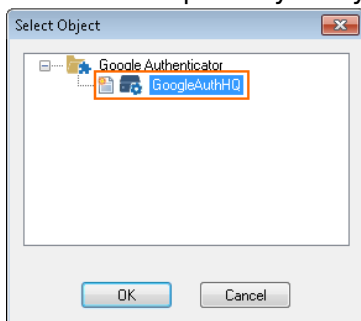
1. Log into the Control Center.
2. Go to **Your Managed Firewall > Infrastructure Services**.
3. Expand the configuration node, right-click **Google Authenticator** and click **Copy To Repository**. The **Select Object** window opens.
4. Enter a **Name** for the new object.



5. Click **OK**.
6. Right-click **Google Authenticator** again and click **Lock**
7. Right-click **Google Authenticator** again and click **Link From Repository**.

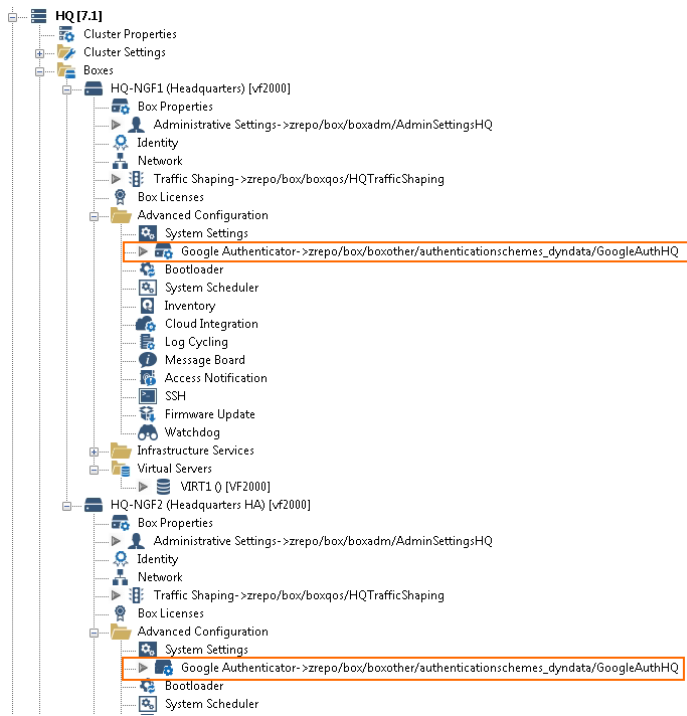


8. Select the Repository entry you just created.



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

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



Figures

1. auth_02.png
2. enable_google_auth.png
3. activate_auth_scheme_00.png
4. add_authentication_scheme_00.png
5. add_authentication_scheme01.png
6. set_auth_scheme_googleauth_00.png
7. add_authentication_scheme02.png
8. google_auth_repository_01.png
9. google_auth_repository_02.png
10. google_auth_repository_03.png
11. google_auth_repository_04.png

© Barracuda Networks Inc., 2020 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.