How to Configure Google Authenticator (TOTP) Authentication

https://campus.barracuda.com/doc/41102828/

Google Authenticator offers an easy way to use time based one time passwords (TOPT) using Google infrastructure and mobile apps. The authentication module can be used by itself or in combination with other authentication modules for multi-factor authentication. A new verification code is automatically generated every thirty seconds. The official Google Authenticator app is available for Android, iOS and Blackberry (version number 6 or lower) devices. Third-party apps are available for almost all other mobile operating systems.

Video

Watch the Techlib Video below to see Google Authenticator and Risk Based Authentication used and configured:

Before you begin

- Google Authenticator is time sensitive. Make sure your mobile device and Barracuda SSL VPN are set to the correct time.

Step 1. Create an authentication scheme using Google Authenticator

You need a new authentication scheme which uses the google authenticator as a secondary authentication module.

1. Log into the SSL VPN web interface.
2. Go to the **Manage System > ACCESS CONTROL > Authentication Schemes** page.
3. In the **Create Authentication Scheme** section:

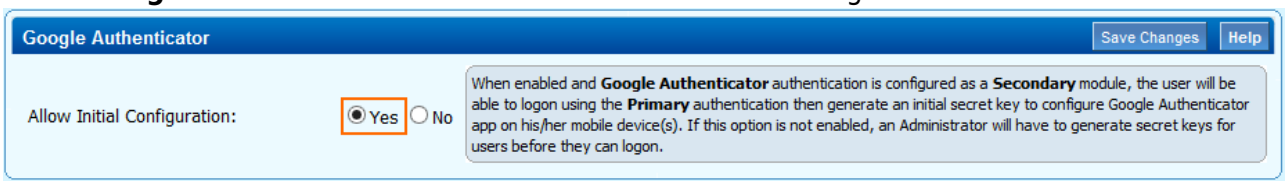
1. Enter a **Name** for the scheme (e.g., `Google Authenticator`).
2. From the **Available modules** list, select a **primary authentication module**. For more information, see Authentication Schemes.
3. From the **Available modules** list, select **Google Authenticator** and click **Add**. Google Authenticator is now listed second in the **Selected modules** list.
4. From the **Available Policies** list, select the policies that you want to apply this authentication scheme to and click **Add**. Selected policies are displayed in the **Selected Policies** list.
5. Click **Add**.

4. To make Google Authenticator the default authentication scheme, click the **More** link next to the entry in the **Authentication Schemes** section and then click **Increase Priority** until it is at the top of the list.

Step 2. Enable initial Google Authenticator configuration by users

Enable the user to configure Google Authenticator when logging in the first time.

1. Log into the SSL VPN web interface.
2. Go to the **Manage System > ACCESS CONTROL > Security Settings** page.
3. In the **Google Authenticator** section enable Allow Initial Configuration.



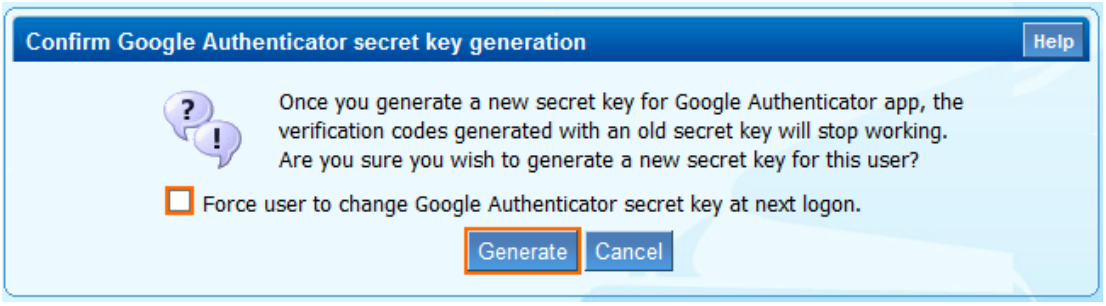
4. Click **Save Changes**.

Step 3. (optional) Create Google Authenticator secret keys for specific users

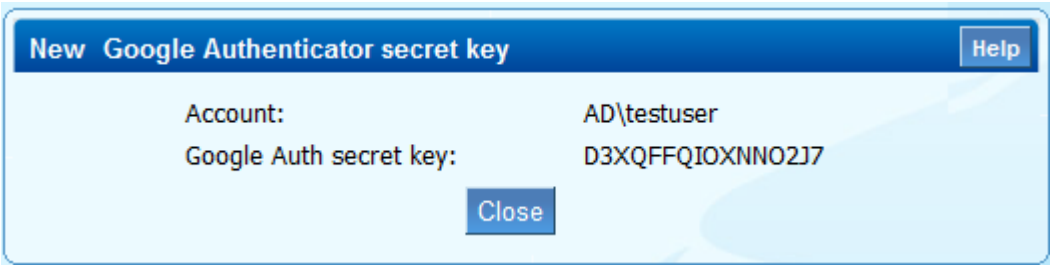
If a user looses access to the configured Google Authenticator app the administrator can generate a new secret key. This key will invalidate the old secret key and the user can log in again, once the new Google Authenticator account has been set up using the new key.

1. Log into the SSL VPN web interface.
2. Go to the **Manage Systems > ACCESS CONTROLS > Accounts** page.
3. For every user you want to generate the Google Authenticator secret keys for:
   1. In the **Accounts** section click on the **More** link for the user.
   2. Click **Generate Google Auth secret key**. The **Confirm Google Authenticator secret key generation** window opens.
   3. (optional) For additional security you can force the user to generate a new key after the first login by ticking the **Force user to change ... at next login** checkbox.

4. Click **Generate**.



4. Use the **Google Auth secret key** to configure the Google Authenticator account on the mobile device of the user.



Next steps

Every user must install the Google Authenticator app and complete the Google Authenticator User Guide to configure the app to work with the Barracuda SSL VPN.

Figures