How to Configure Risk Based Authentication

https://campus.barracuda.com/doc/41102818/

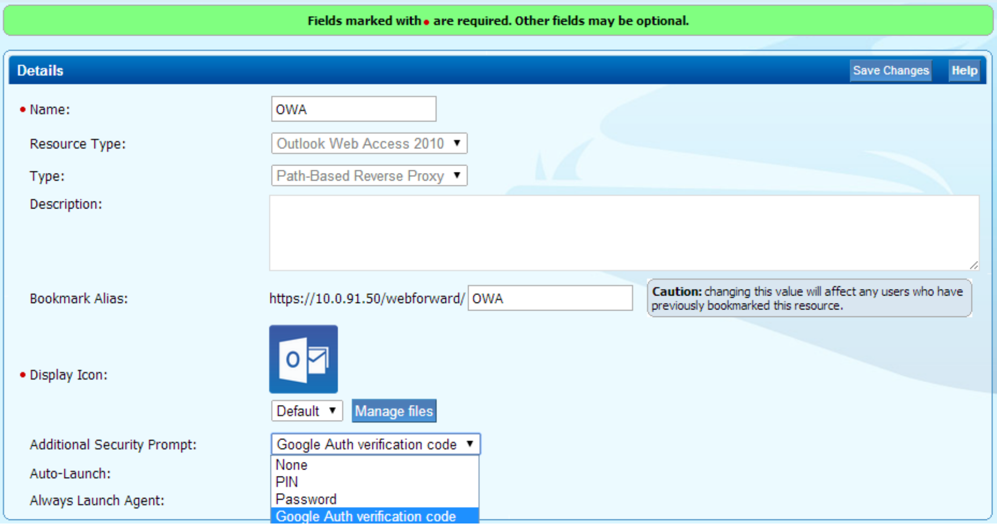
Some network environments might require additional security levels to authenticate users when they access specific high-risk SSL VPN resources. Barracuda SSL VPN provides risk based authentication for Web Forwards, applications and SSL tunnels. Each launch of these resource types can be protected by PIN, password or Google Authenticator authentication.

Step 1. Configure the additional security prompt

Configure risk based authentication for an existing Web Forward, application or SSL tunnel, depending on your requirements.

1. Open the **RESOURCES** tab.
2. Edit the resource you want to configure risk based authentication for.
3. In the **Details** section, select an option from the **Additional Security Prompt** list:
    - If you want users to enter a PIN, select **PIN**.
    - If you want users to enter a password, select **Password**.
    - If you want users to login via Google Authenticator, select **Google Auth verification code**.

      With **Google Auth verification code** selected, users will be prompted to enter the authentication code provided by Google.



Fields marked with • are required. Other fields may be optional.

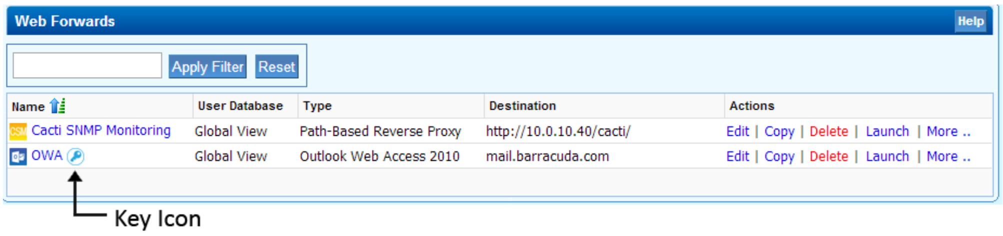
Details

• Name:	OWA
Resource Type:	Outlook Web Access 2010
Type:	Path-Based Reverse Proxy
Description:	
Bookmark Alias:	https://10.0.91.50/webforward/ OWA
• Display Icon:	Default
Additional Security Prompt:	Google Auth verification code
Auto-Launch:	
Always Launch Agent:	

Caution: changing this value will affect any users who have previously bookmarked this resource.

4. Click **Save Changes**.

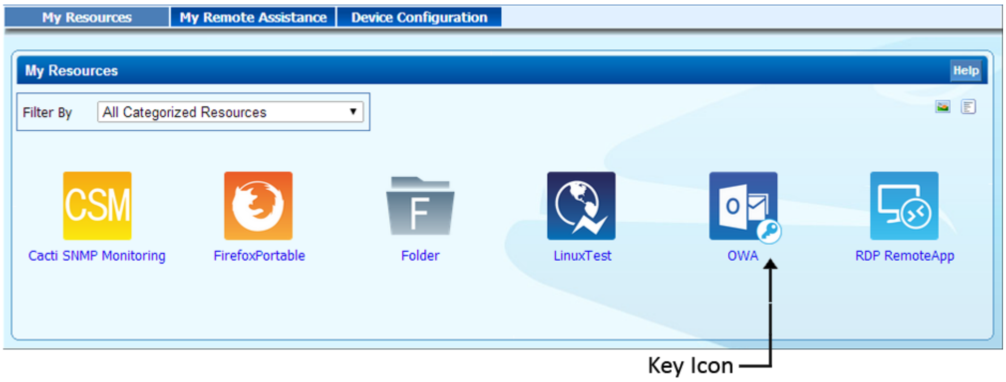
The configured resource is now protected by PIN, password or Google Authenticator authentication, which is indicated by a blue key icon next to the entry in the resource list.



Web Forwards

Name	User Database	Type	Destination	Actions
Cacti SNMP Monitoring	Global View	Path-Based Reverse Proxy	http://10.0.10.40/cacti/	Edit | Copy | Delete | Launch | More ..
OWA	Global View	Outlook Web Access 2010	mail.barracuda.com	Edit | Copy | Delete | Launch | More ..

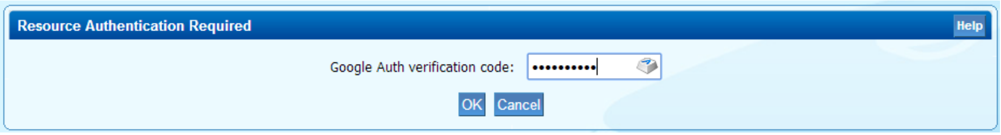
The protected resource is also marked with a blue key icon on the user´s **My Resources** page.



Step 2. Launch the protected resource

To use risk based authentication when logged into the Barracuda SSL VPN interface,

1. Log into the SSL VPN interface as the user.
2. Select the protected resource.
3. In the upcoming security prompt, enter the PIN, password or Google Auth verification code.



Resource Authentication Required

Google Auth verification code: ••••••••••

4. Launch the resource.

Figures