

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.

DetailsSave ChangesHelp

Name:

OWA

Resource Type:

Outlook Web Access 2010

Type:

Path-Based Reverse Proxy


Description:

Bookmark Alias:

https://10.0.91.50/webforward/ OWA

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

Display Icon:



Default

Manage files

Additional Security Prompt:

Google Auth verification code

Auto-Launch:

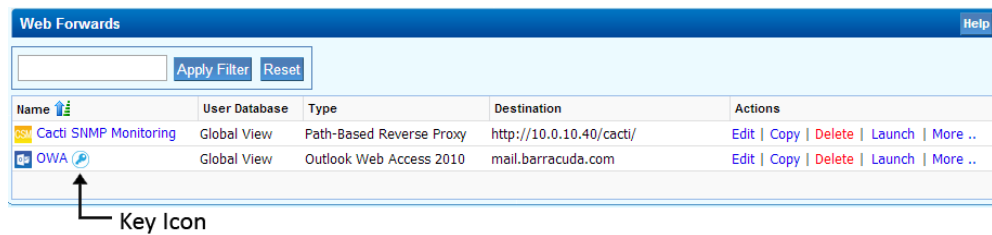
None

Always Launch Agent:

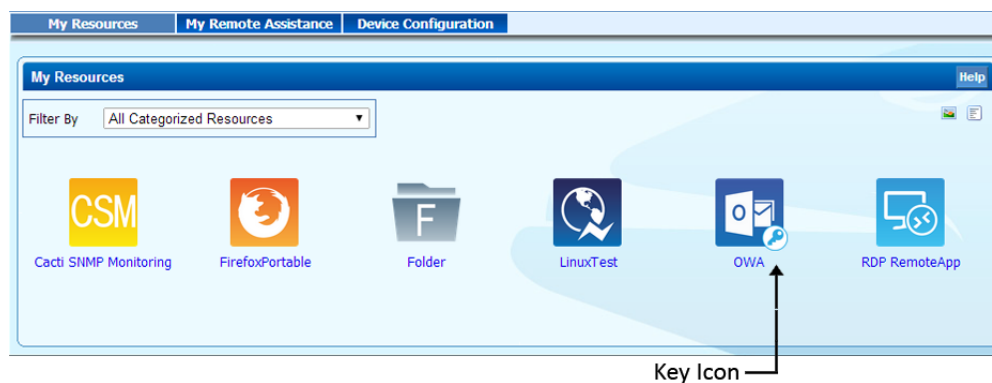
PIN

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.



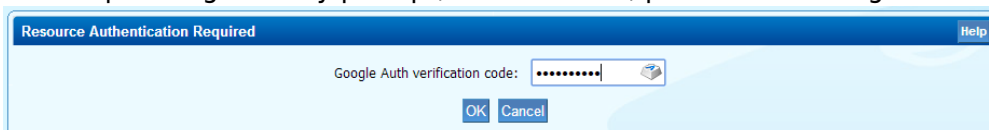
The protected resource is also marked with a blue key icon on the user's **My Resources** page.



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.



4. Launch the resource.

Figures

1. risk_based_conf.png
2. key_icon.png
3. key_user.png
4. risk_based_auth.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.