

## How to Enable Dual-Factor Authentication for the Barracuda Web Application Firewall Web Interface Access

<https://campus.barracuda.com/doc/95264429/>


To enable dual-factor authentication for Barracuda WAF web interface access, perform the following steps:

1. Log into the Barracuda Web Application Firewall web interface.
2. Go to the **ADVANCED > Admin Access Control** page.
3. In the **External Authentication Services** section:
  1. Select **LDAP** from the **Add Authentication Services** drop-down list. The **Add LDAP Service** page opens.
    1. On the **Add LDAP Service** page, enter your LDAP server details and click **Save**. For information about LDAP configuration, see [How to Configure Authentication and Access Control \(AAA\)](#).
  2. Select **RADIUS** from the **Add Authentication Services** drop-down list. The **Add RADIUS Service** page opens.
    1. On the **Add RADIUS Service** page, enter your RADIUS or RSA SecurID server details and click **Save**. For information about RADIUS configuration, see [How to Configure Authentication and Access Control \(AAA\)](#).
4. In the **Administrator Account Settings** section:
  1. Set **Dual Authentication** to **Enable**.
  2. Set **Use RSA SecureID** to **Yes** if you have specified RSA SecurID server details in the RADIUS service configuration. If not, keep the setting to **No**.
5. Click **Save**.

### Dual-Factor Authentication Flow with the Barracuda WAF Web Interface

When dual-factor authentication is enabled, the user is challenged to provide the username, password and passcode (RADIUS user password) to access the Barracuda Web Application Firewall.


**Login screen when dual-factor authentication is enabled with LDAP and RADIUS authentication services**



The image shows the login interface of the Barracuda Web Application Firewall. It features a dark blue header with the Barracuda logo and the text "Web Application Firewall". Below the header is a light gray login box with the instruction "Please enter your administrator login and password." Inside the box are three input fields labeled "Username", "Password", and "Passcode". A blue "Sign in" button is located at the bottom right of the login box.

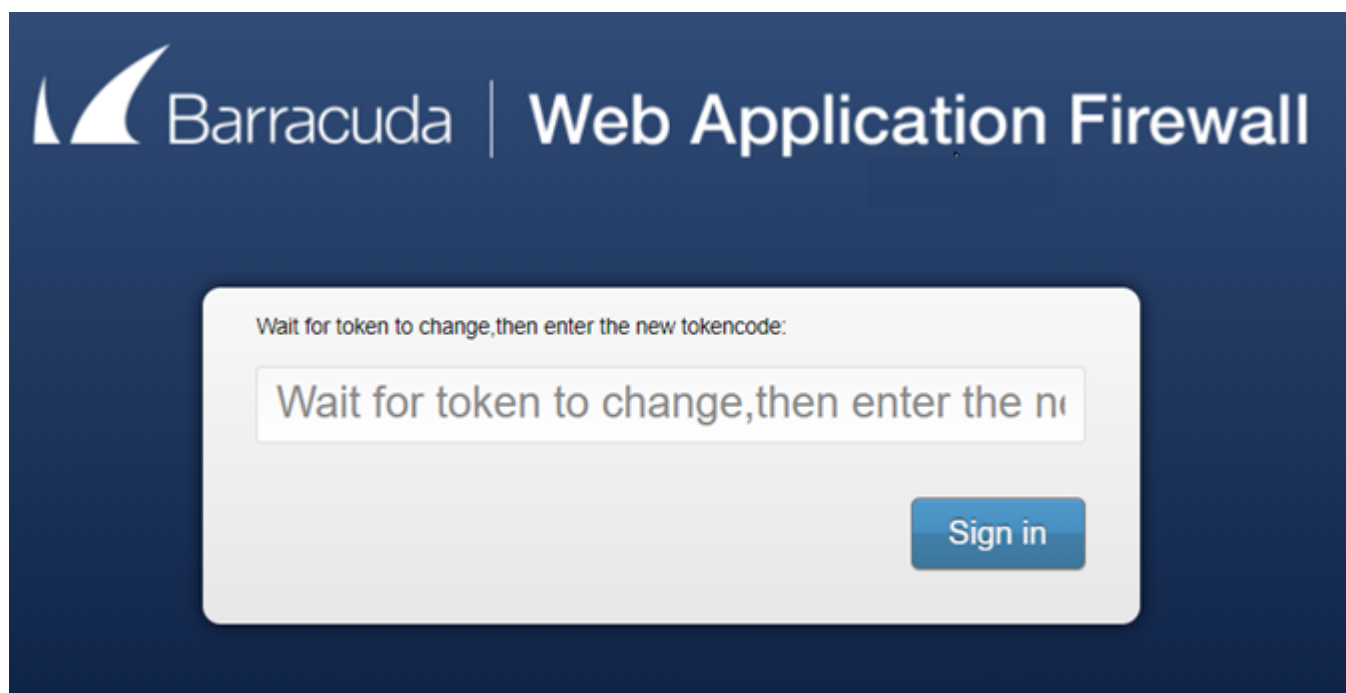
**Login screen when dual-factor authentication is enabled with LDAP and RSA SecurID authentication services**

The user is challenged to provide the username, password, and passcode (PIN followed by the RSA SecurID token code).



The image shows the login interface of the Barracuda Web Application Firewall. At the top, the Barracuda logo and the text "Web Application Firewall" are displayed. Below this, a light gray box contains the instruction "Please enter your administrator login and password." There are three input fields: the first contains the username "rsa\_user1", the second contains a masked password of seven dots, and the third contains a masked password of thirteen dots. A blue "Sign in" button is located at the bottom right of the input fields.

If the passcode is incorrect, the user is shown a challenge page to re-validate the passcode.



The image shows the challenge interface of the Barracuda Web Application Firewall. At the top, the Barracuda logo and the text "Web Application Firewall" are displayed. Below this, a light gray box contains the instruction "Wait for token to change, then enter the new tokencode:". There is a single input field containing the text "Wait for token to change, then enter the n". A blue "Sign in" button is located at the bottom right of the input field.

---

## API Calls Required to Get the Session Token

---

To get a token for API when dual-factor authentication is enabled with LDAP and RSA SecurID authentication services, perform the following steps:

Login Request:

Send a login request with the username, password, and passcode (if RSA SecurID is configured).

```
curl http://<IP:PORT>/restapi/v3/login -X POST -H Content-Type:application/json -d  
'{"username":"krbtest2","password":"35HJ2ab", "passcode":"63445348"}'
```

Response :

```
{"challenge":"b0a123456adxxxx52fab93f7xxxx12ee","message":"Enter a new PIN having from  
4 to 8 alphanumeric characters:\u0000"}
```

If you get a challenge back with a message, pass the challenge back as JSON along with the passcode to the login-dual-auth controller.

The passcode in the request must be provided according to the message you receive.

---

## Dual Auth Request

---

```
curl http://<IP:PORT>/restapi/v3/login-dual-auth -X POST -H Content-Type:application/json -d  
'{"challenge":"b0a123456ad23a523f6e93f7xxxxxxee", "passcode":"xyz35"}'
```

Response :

```
{"challenge":"b0a123456ad23a523f6e93f7xxxxxxee","message":"\r\nPlease re-enter new
```

PIN:\u0000"}

Re-enter the PIN and send the request again:

```
curl http://<IP:PORT>/restapi/v3/login-dual-auth -X POST -H Content-Type:application/json -d '{"challenge":"b0a123456ad23a523f6e93f7xxxxxxee", "passcode":"xyz35"}'
```

Response:

```
{"challenge":"b0a123456ad23a523f6e93f7xxxxxxee","message":"\r\nPIN Accepted.\r\nWait for the token code to change,\r\nthen enter the new passcode:\u0000"}
```

Request with the passcode:

```
curl http://<IP:PORT>/restapi/v3/login-dual-auth -X POST -H Content-Type:application/json -d '{"challenge":"b0a123456ad23a523f6e93f7xxxxxxee", "passcode":"xyz3545514106"}'
```

Response :

```
{"token":"eyJ1c2Vyljoia3JidGVzdDIiLCJldCI6Ixxxxxx3MzQwODliLXxxxxxxzd29yZCI6IjlkMzY0MzEx\nnZGE0NWMyNTA4xxxxxxU5MTNkYmU1MGQyIn0=\n"}
```

If the PIN is already set, send the request with the PIN and new token:

```
curl http://<IP:PORT>/restapi/v3/login -X POST -H Content-Type:application/json -d '{"username":"krbtest2","password":"35HJ2ab", "passcode":"xyz3513637390"}'
```

Response :

---

```
{"token":"eyJldCI6IjE1MjQ3MzQ4NjMxxxxxx2Vyljoia3JidGVzdDIiLCJxxxxxxXxyZCI6ImZhZDhiMzc1\nYnYTE1ODkwZjFhNjc0MDM4XxxxXXxxYml5In0=\n"}
```

## Figures

1. AuthLoginPage.png
2. Login\_RSA\_User.png
3. RSA\_Challenge\_Page.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.