

## How to Configure Multi-Factor Authentication Using Time-based One-time Password (TOTP)

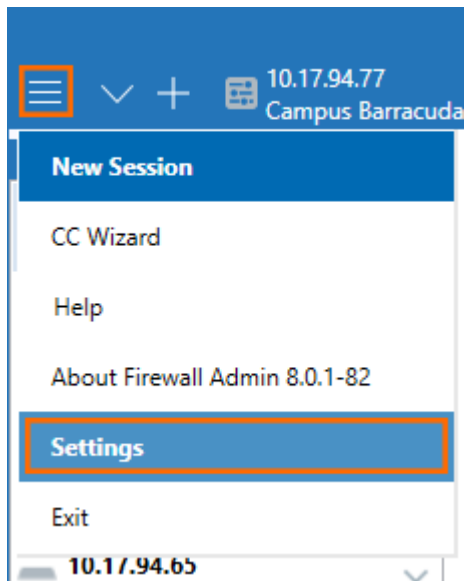
<https://campus.barracuda.com/doc/96026649/>

Some network environments require additional security levels to authenticate users when they access specific high-risk VPN or SSL VPN resources. For an additional level of security, multi-factor authentication can be enabled for accounts on an individual basis, using a Time-based One-time Password (TOTP) as a secondary authentication method. The Barracuda CloudGen Firewall supports multi-factor authentication for [client-to-site VPN](#) (TINA protocol only), [SSL VPN](#), [CudaLaunch](#), and the [Barracuda VPN Client](#) for Windows, macOS, and Linux. Time-based One-time Password authentication is not supported on iOS devices. Multi-Factor Authentication using TOTP requires an Advanced Remote Access subscription. For more information, see [Subscriptions](#).

- Like other time-based services, TOTP relies on a correct time system. Make sure the time settings on the client and the server are configured correctly. Time should be synced between all devices that are used for generating TOTP and authentication. Otherwise, authentication fails.
- For TOTP enrollment on a High Availability (HA) cluster, the primary CloudGen Firewall unit must be in active state.

### Before You Begin

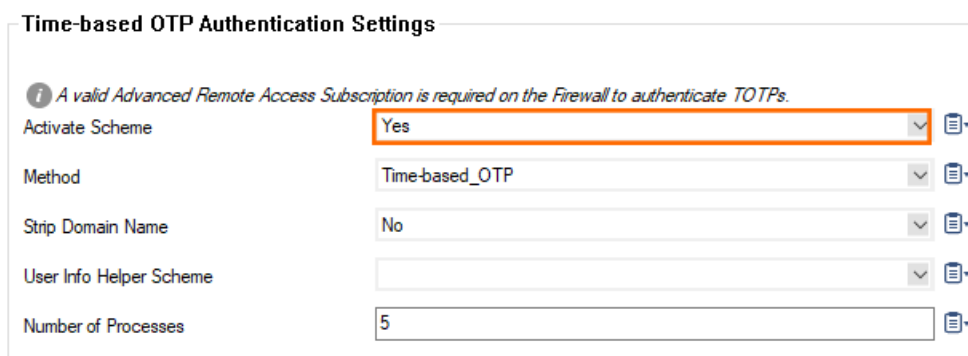
- Configure a primary authentication scheme, for example, MSAD. For more information, see [How to Configure MSAD Authentication](#).
  - In the **Authentication Service > Timeouts and Logging** configuration, set the **Request Timeout** to 30. For more information, see [How to Configure Authentication Service Timeouts and Logging](#).
- If you bulk enroll more than 20 users, you must temporarily increase the **Configuration Read Timeout**:
  1. In **Firewall Admin**, click the hamburger menu on the top left and select **Settings**.



2. Click **Client Settings**.
  3. In the **Connectivity Options** section, set **Configuration Read Timeout** to six times the number of users in seconds. For example, for 500 users, enter 30000.
  4. Restart Firewall Admin.
- If you bulk enroll, you must also set up a mail server so that the enrollment emails get sent out.

## Step 1. Enable Time-based OTP Authentication

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left navigation pane, select **TOTP Authentication**.
3. Click **Lock**.
4. Enable **Time-based OTP** as authentication scheme.

A screenshot of the 'Time-based OTP Authentication Settings' configuration page. At the top, there's a warning icon and text: 'A valid Advanced Remote Access Subscription is required on the Firewall to authenticate TOTP's.' Below this, there are several configuration fields:

- 'Activate Scheme' is a dropdown menu set to 'Yes' (highlighted with an orange rectangle).
- 'Method' is a dropdown menu set to 'Time-based\_OTP'.
- 'Strip Domain Name' is a dropdown menu set to 'No'.
- 'User Info Helper Scheme' is a dropdown menu.
- 'Number of Processes' is a text input field set to '5'.

Each field has a small document icon to its right.

5. (optional) To let users log in with domain and username (e.g., user@domain.com or domain/user), set **Strip Domain Name** to **Yes**.
6. If group information is queried from a different authentication scheme, select the scheme from the **User Info Helper Scheme** list. For example, select **LDAP** if group information must be queried from an LDAP directory.
7. Click **Send Changes** and **Activate**.

## Step 2. Enroll Users and Groups

The Barracuda CloudGen Firewall provides two options to enroll users and groups for TOTP authentication:

- **Bulk Enrollment** – Automatically enroll a group of users, e.g., from your authentication server.
- **Self Enrollment** – Configure self-enrollment for users to set up Time-based OTP. This option is available for the SSL VPN web portal, CudaLaunch, and the TOTP web portal.

### Bulk Enrollment

#### Step 2.1. (optional) Export Users from Active Directory

To simplify the TOTP enrollment procedure for MSAD users, export the users as a comma-separated list from Active Directory to Excel and then to a .csv file. While exporting the users, define the required fields to get the format: [user] | [empty\_password] | , [email] |.

1. On the PowerShell, type the command:
  - `Get-ADUser -SearchBase "OU= (your users),DC= (your domain)" -Filter * -properties mail | Format-Table -autosize -Property SamAccountName, mail > C:\bat\test.csv`For example:
  - `Get-ADUser -SearchBase "OU=EU Users,DC=eu,DC=ad,DC=cuda-inc,DC=com" -Filter * -properties mail | Format-Table -autosize -Property SamAccountName, mail > C:\bat\test.csv`
2. Export the output to an Excel file.
3. Add a column for [empty\_password]
4. Export the list into a .csv file.

You can now copy and paste the data from the .csv file into the **Time-based OTP Bulk Enrollment** configuration. Make sure to use the format: [username] | [password] | [email] |

#### Step 2.2. Enroll Users for TOTP Authentication

It is recommended to enroll one or two test users before launching the whole enrolling process in order to ensure that enrollment and email notifications are configured correctly.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Time-based OTP Bulk Enrollment**.
2. Click **Lock**.
3. Add the users that should be enrolled for TOTP authentication:
  - In the **User Bulk Enrollment** field, enter the users in the format

[username] | [password] | [email] | , or

- Copy and paste the data from the .csv file with the users from your authentication server.

4. Click **Send Changes**.

5. Click **Import**. The users are now listed in the **Enrolled Users** table.

Per default, all users in an imported VPN group are selected for TOTP authentication. You can delete users from the list, but not add them to it by entering a username.

6. Click **Activate**.

The TOTP token will be sent to each user per email during user bulk enrollment. Therefore, you must also configure email notifications. For more information, see [How to Configure System Email Notifications](#). Check the logs to verify that emails have been correctly sent.

When configuring TOTP bulk enrollment for CC-managed firewalls, enrollment emails are sent from the Control Center box IP address. However, the notification settings from the firewall (**Administrative Settings > Notifications**) are being used.

### Managing Enrolled Users

All users that have been enrolled are listed in the **Enrolled Users** table. If you want to overwrite the entries using an updated list, select the **Overwrite Users** check box and re-import your users. To replace all enrolled users, select the **Erase Users** check box before adding new users. You can also revoke users that have already been enrolled. To prevent users from authenticating via TOTP, simply remove their details from the **Enrolled Users** list and activate the changes. Users that have been deleted will have to re-enroll themselves.

### Self-Enrollment

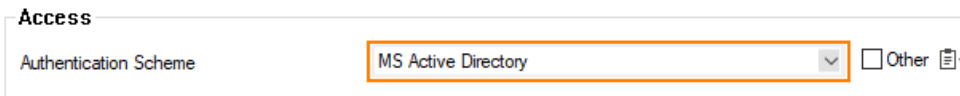
When using the SSL VPN web portal, CudaLaunch, or the TOTP web portal, enable self-enrollment for users to set up Time-based OTP via the web interface.

For HA setups, TOTP self-enrollment in the SSL VPN web portal only works when the primary firewall is the active unit. If the secondary box is active, an error is generated.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > SSL-VPN**.
2. Click **Lock**.
3. Select **yes** to **Enable the TOTP Self Service**.



4. In the left menu, click **Time-based OTP**.
5. From the **Authentication Scheme** drop-down list, select your authentication scheme. E.g., MS Active Directory.



6. In the **Self Enrollment** section:
  1. Select **yes** to **Enable Self Enrollment**.
  2. In the **Allowed User Groups** field, add the users that should be allowed to self-enroll for TOTP authentication. Delete the asterisk and enter the MSAD group name. E.g., CN=sales
  3. In the **Blocked User Groups** field, add the users that should be blocked from self-enrolling.
7. (optional) Import your company **Logo** and customize the **Login Message** for your users.
8. Click **Send Changes** and **Activate**.

Users can now use the SSL VPN web portal, CudaLaunch, or go to the dedicated TOTP web portal (URL [https://\(IP of the SSL VPN service\)/portal/totp.html](https://(IP of the SSL VPN service)/portal/totp.html)) and enroll themselves for TOTP authentication. For more information, see [How to Self-Enroll for Time-Based One-Time Passwords \(TOTP\) using the Simple TOTP Web Portal](#).

Users can also self-enroll via CudaLaunch or the SSL VPN web portal, using the **Time-based OTP** menu option found under **Settings** if the configured Access Control Policies are configured to allow access without using Time-based OTP.

### Step 3. Configure TOTP as Authentication Scheme

Enable TOTP authentication for client-to-site VPN, SSL VPN web portal, CudaLaunch, or the Barracuda VPN Client.

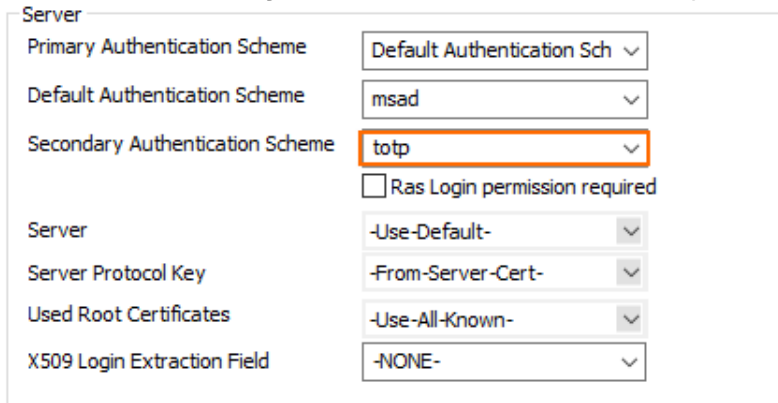
#### Enable TOTP for Client-to-Site VPN

Enable TOTP as the secondary authentication scheme:

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service**

**> Client to Site.**

2. Click **Lock**.
3. Click the **External CA** tab and then click the **Click here for options** link. The **Group VPN Settings** window opens.
4. Configure the settings for your VPN group. For more information, see [How to Configure a Client-to-Site VPN Group Policy](#).
5. From the **Secondary Authentication Scheme** drop-down list, select **totp**.



Primary Authentication Scheme	Default Authentication Sch
Default Authentication Scheme	msad
Secondary Authentication Scheme	totp
<input type="checkbox"/> Ras Login permission required	
Server	-Use-Default-
Server Protocol Key	-From-Server-Cert-
Used Root Certificates	-Use-All-Known-
X509 Login Extraction Field	-NONE-

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

Create a VPN group policy to enforce Time-based One-time Password (TOTP) authentication:

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Client to Site**.
2. Click **Lock**.
3. Click the **External CA** tab.
4. Create or edit a group policy. For more information, see [How to Configure a Client-to-Site VPN Group Policy](#).
5. In the **Edit Group Policy window**, right-click the **Group Policy Condition** field and select **New Rule**.
6. Configure the settings for your VPN group. For more information, see [How to Configure a Client-to-Site VPN Group Policy](#).
7. Select the **Enable One-Time Password** check box.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

When using more than one policy, make sure that you place this policy above the ones without Time-based One-time Password enforcement.

**Enable TOTP for SSL VPN and CudaLaunch**

To configure SSL VPN to use One-time Password authentication, create an Access Control Policy that requires TOTP authentication. For more information, see [How to Configure Access Control Policies for](#)

---

[One-Time Password Authentication](#) and [How to Self-Enroll for Time-Based One-Time Passwords \(TOTP\) using the Simple TOTP Web Portal](#).

## **Self-Enroll for TOTP**

To enroll a mobile device using CudaLaunch or SSL VPN, install a TOTP-compatible app and complete the 2-step enrollment process to link the app with Time-based One-time Password Authentication on the CloudGen Firewall. For more information, see [How to Self-Enroll for Time-Based One-Time Passwords \(TOTP\) Using CudaLaunch or the SSL VPN Web Portal](#).

## **Enable TOTP for the Barracuda VPN Client**

To use TOTP on the Barracuda VPN Client, create or edit a VPN profile and enable One-time Password (OTP) extensions. For more information, see [How to Create VPN Profiles](#).

## Figures

1. menu.png
2. totp01.png
3. enable\_ssl\_totp.png
4. enable\_ssl\_ad.png
5. totp\_sec.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.