

USER MANUAL

Initializing an RSA Token on the Web Portal of the CTBTO

REVISION HISTORY

Version No	Date	Revised by	Description
1.0	07/05/2015	Jose GUERRERO	Created the first draft.
2.1	12/0452015	Efren Abaya	Added Scope and Definitions. General editing.

Initializing an RSA Token on the Web Portal of the CTBTO

Purpose

This document provides instructions for initializing a new RSA token on the Web Portal of the CTBTO and for recovering from a “Next Token Mode” condition.

Scope

This user manual covers the initialization and recovery from Next Token Mode on the Web Portal of the CTBTO. Other RSA token applications are covered in different user manuals.

Definitions and Acronyms

Passcode	During RSA token initialization, the password is the same as the token code. Otherwise, the password is the PIN followed by the 6-digit token code (without any space in between).
PIN	Personal Identification Number. The password used together with a token code to login. The PIN is selected by the user when an RSA token is initialized.
RSA token	An RSA SecurID hardware token that generates a new token code once every minute. Also called “VPN token.”
Token code	The 6-digit number displayed on an RSA token.

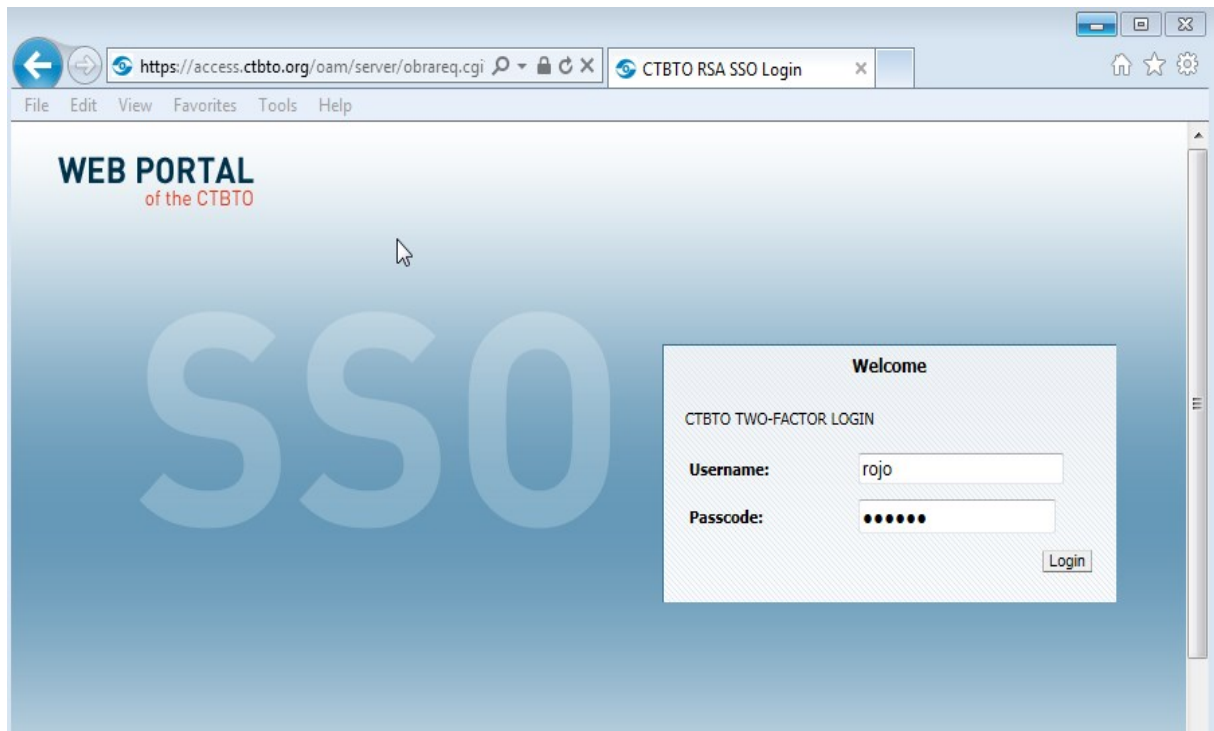
Initializing an RSA Token

Open this page of the Web Portal of the CTBTO with any web browser (figure below):

<https://access.ctbto.org/initrsa>.

If the Web Portal cannot be displayed, check that the computer has an Internet connection¹. It is also possible that there is a problem with the web browser.

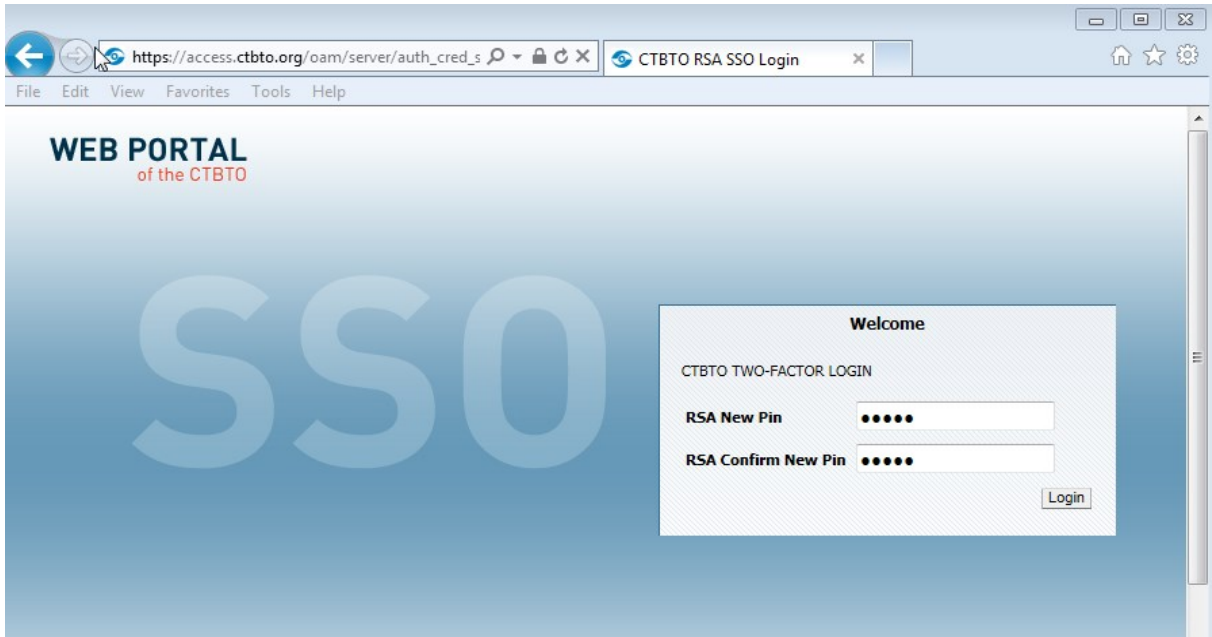
¹ For example, try to open <http://www.ctbto.org> or any other web site.



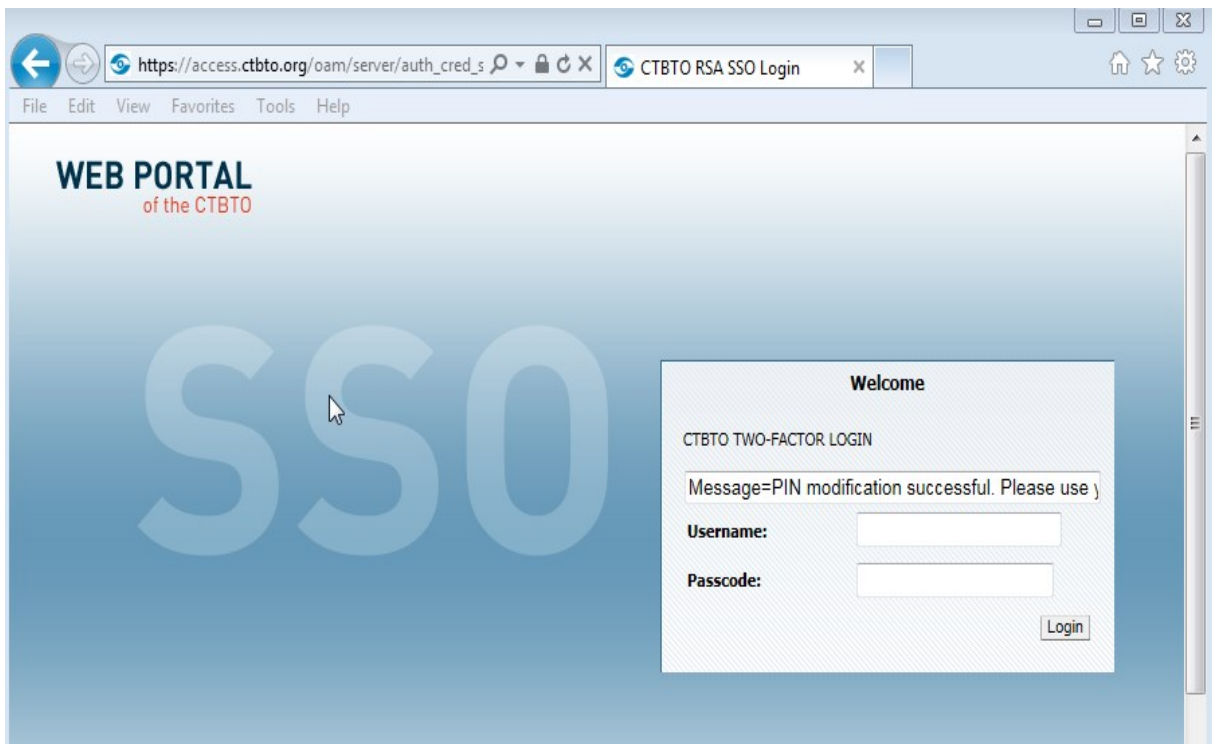
Enter in lower case the **Username** that is assigned to the RSA token. (The username is case sensitive.) Usually this is the last name or family name of the user. For example, for Ricardo Rojo the username shown in the above figure is “rojo”.

In the **Passcode** field enter the 6-digit number that appears in the RSA token. Make sure that there are at least 3 bars shown on the left side of the RSA token display so that the number does not change before the typing is completed.

After entering the **Username** and **Passcode**, click the **Login** button. A new screen (see below) will appear that asks for a new PIN. The PIN is needed to use the RSA token. Take some time to think about a PIN combination. Once the PIN has been entered, the user cannot change it. Choose a PIN having from 4 to 8 alphanumeric characters that is easy to remember. The PIN must not contain any special characters (like !, @ or #). Type the selected PIN two times in the dialog box below and click the **Logon** button.



The dialog box below confirms that token Initialization is successful. Be sure to remember this PIN! To read the whole message, place the cursor on the message field and press the left and right arrow keys to scroll left and right.



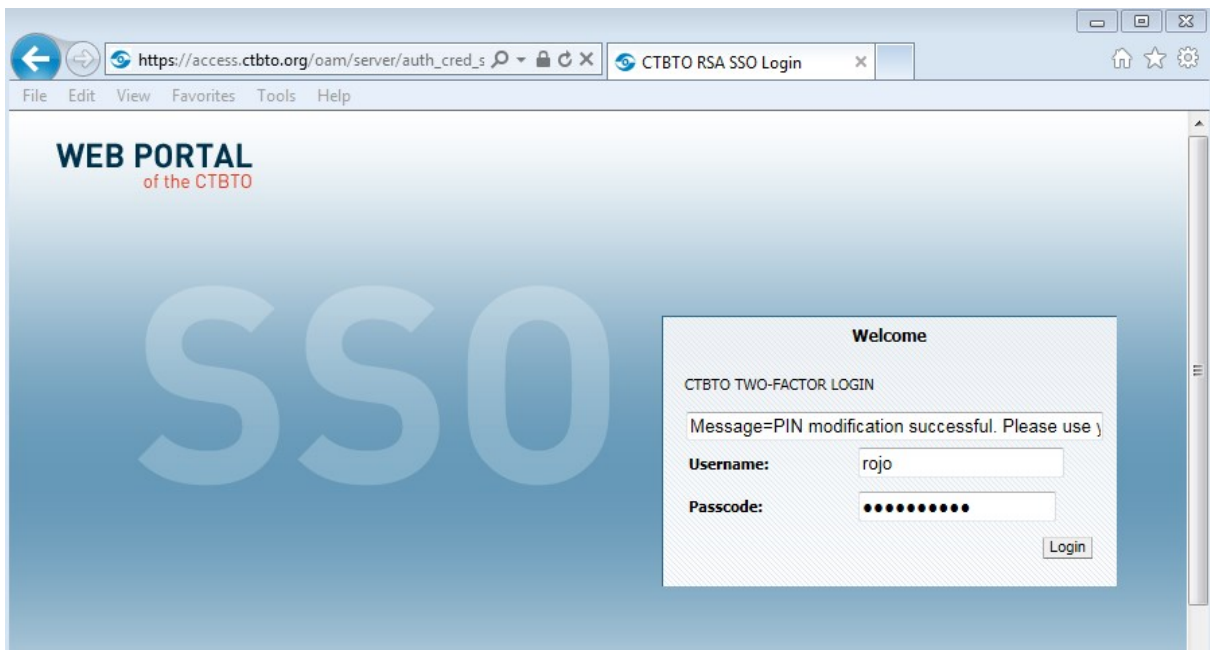
If the token initialization is not successful, wait for a new 6-digit token code to appear and try to initialize again. (The same token code cannot be used two times.) Check the spelling and

capitalization of the Username and the Passcode. Both are case sensitive. If this attempt fails again, send an email to support@ctbto.org².

Testing a newly initialized RSA token

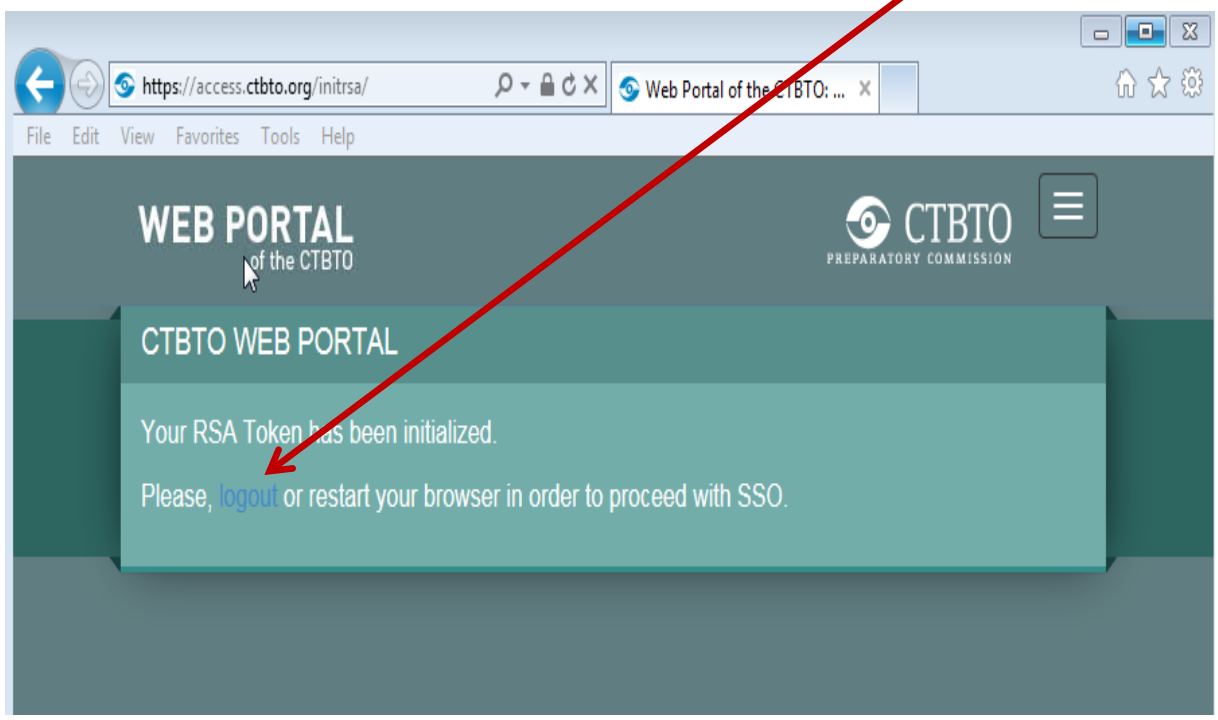
Continue with the last dialog box of the token initialization stage, or open the Two-Factor Login page in the Web Portal of the CTBTO: <https://access.ctbto.org/initrsa>. Enter the **Username** and the **Passcode** then click the **Login** button. For an initialized RSA token, the passcode is the PIN followed by the 6-digit token code (without any space in between).

Very important: The same token code cannot be used twice. Wait for a new 6-digit token code to appear before attempting to login.

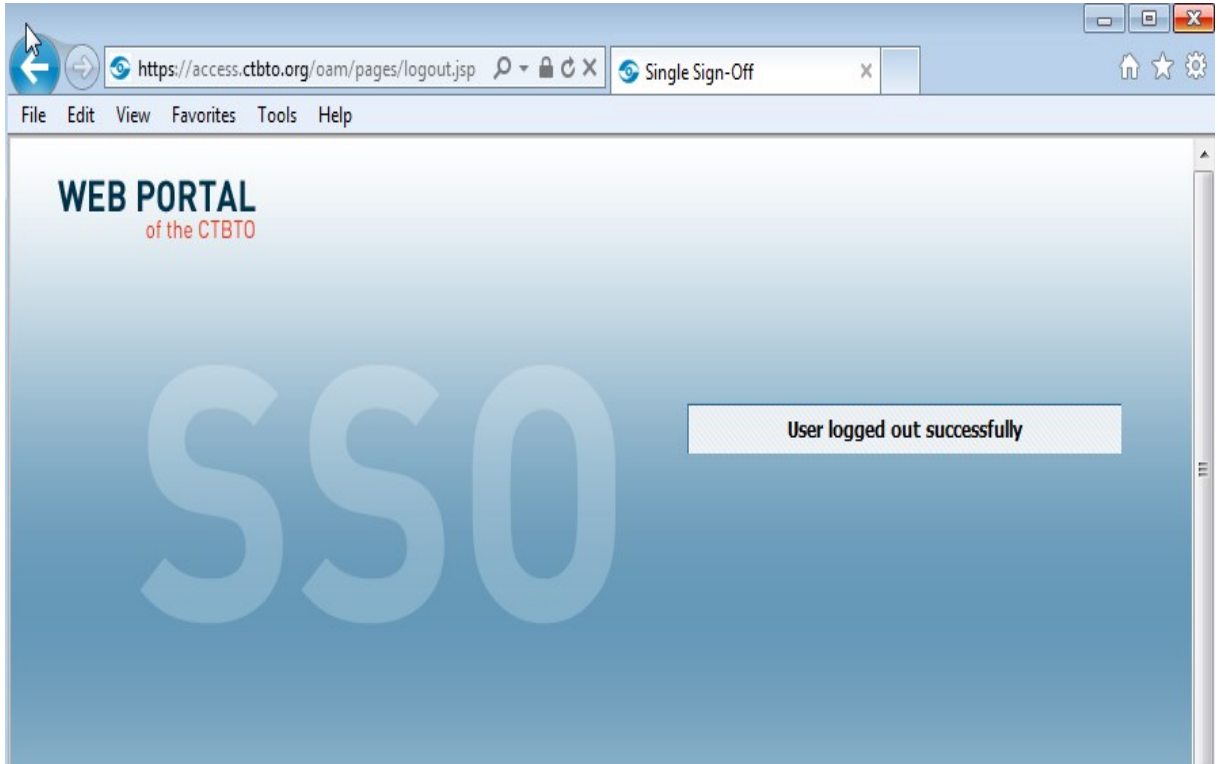


² CTBTO Staff should report to Computing Support Helpdesk.

The screen below confirms that the RSA Token has been initialized. Please don't forget to logout. Failure to do so a few times may bring the RSA token to the "Next Token Mode" (see next section) wherein the user will be unable to login. To logout, clicking on the word "logout."

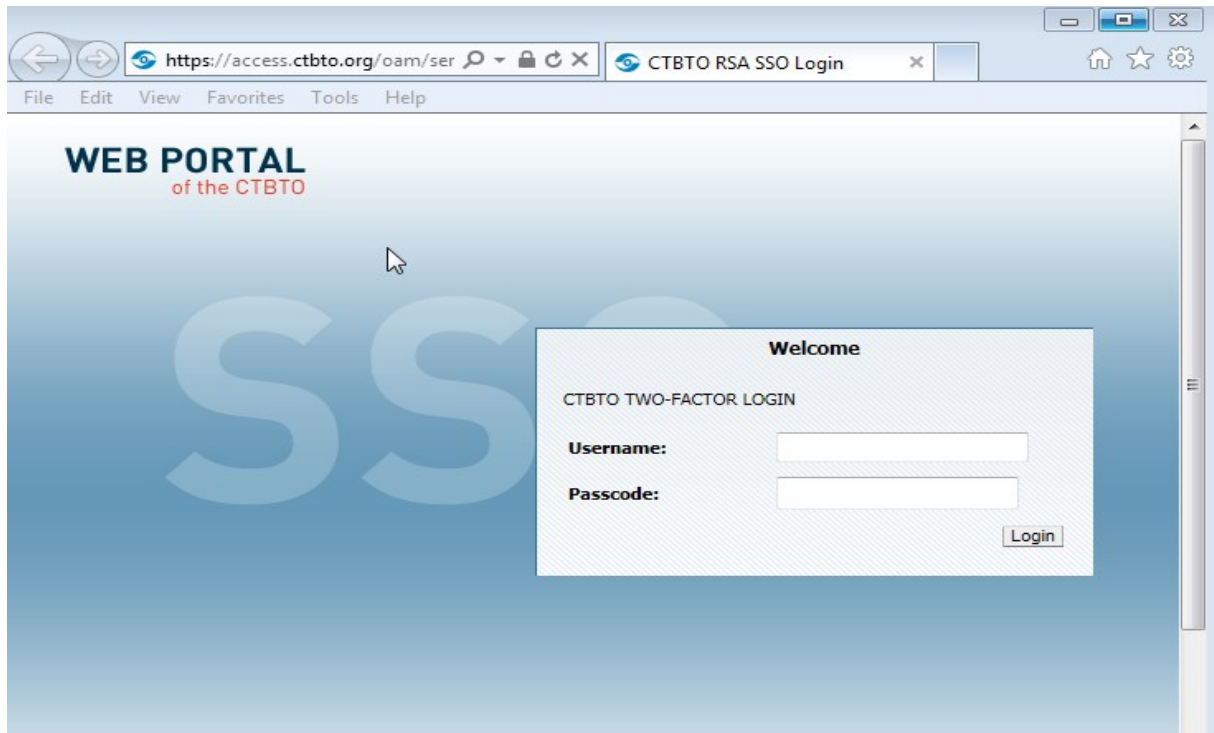


The next screen confirms successful logout.



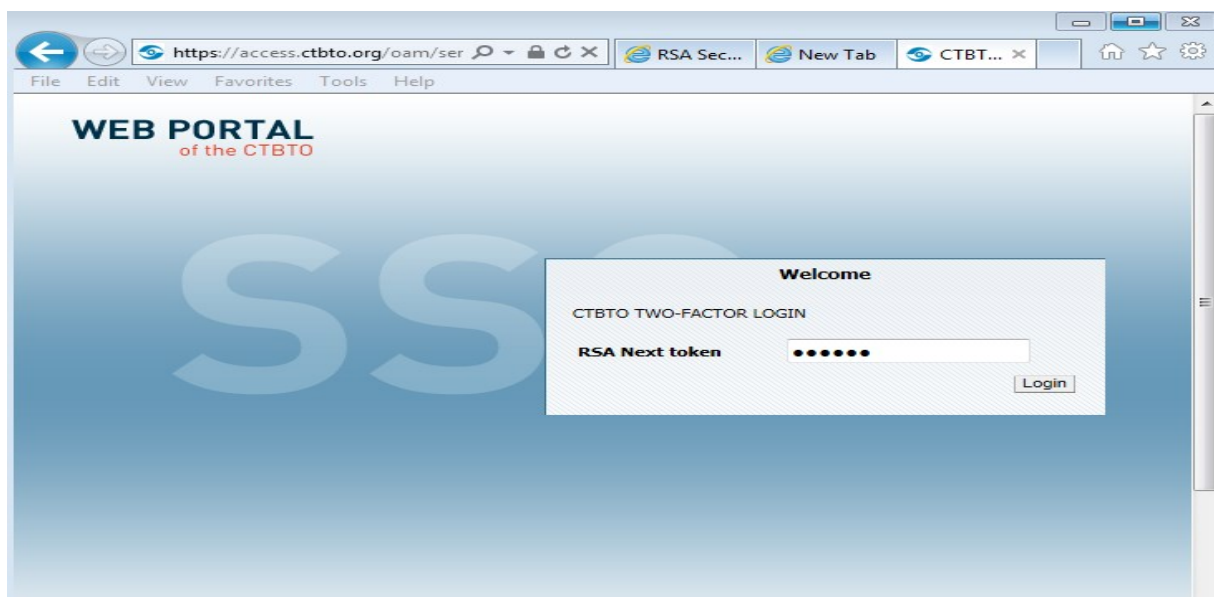
Next Token Mode

After a number of unsuccessful login attempts, the RSA Token will be in the so-called **Next Token Mode**. In this condition, the user will be unable to login anymore. To resolve this issue, open the Two-Factor Login page in the Web Portal of the CTBTO <https://access.ctbto.org/initrsa>.



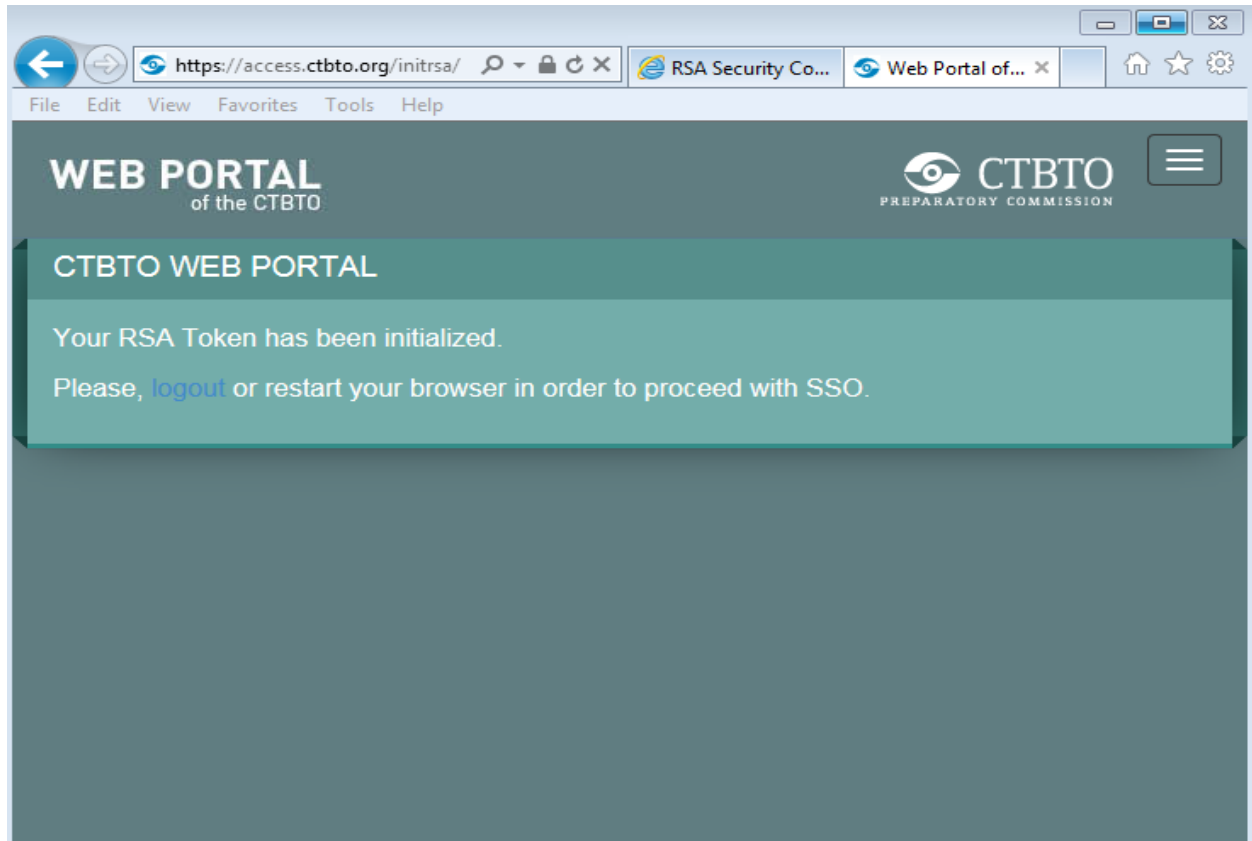
Enter the **Username** that is assigned to the RSA token Remember that this is case sensitive.

In the Passcode field, enter the PIN immediately followed by the 6-digit token code shown on the RSA Token (without any space in between). Click the **Login** button. The RSA Next Token dialog box shown below will appear.



Wait for the 6-digit number in the RSA token to change to make sure the number is not used twice (this is the so-called “Next token code”). Enter only the 6-digit number that appears in the RSA token. **DO NOT** type the PIN in this step. Click the **Login** button.

The screen below will confirm that the issue has been resolved and the RSA token can be used again.



Remember to logout by clicking on the word “logout.”