Actions on Existing Scans and Web Applications

https://campus.barracuda.com/doc/53676684/

After you have created one or more web applications and/or scans, there are additional actions you can take with them. For example, after you have set up the original scan, you can create other related scans while impersonating different devices or different schedules.

Working with Scans

All of these actions are performed from the **Scanner > Web Applications** page.

Run an Existing Scan

You can manually start a scan from this screen.

Locate the desired scan in the **Web Applications** table. In the **Actions** column, click **Run Now**. The scan begins immediately.

Cancel a Scan in Progress

If a scan is currently running, a **Cancel** link displays first in the **Actions** column.

For the target scan, click **Cancel**. The scan will stop when it finishes the operation currently in progress.

Create a New Scan; Clone or Edit an Existing Scan

- **To create a new scan**, locate the desired web application to scan in the **Web Applications** table. In the **Actions** column, click **New Scan**.
- **To Edit an existing scan**, locate the desired scan in the **Web Applications** table. In the **Actions** column, click **Edit**.
- **To Clone an existing scan**, locate the desired scan in the **Web Applications** table. In the **Actions** column, click **Clone**.
    - Be sure to enter a new **Name** for this scan to distinguish it from the original scan.
    - Cloning a scan is faster than creating a new scan if you are making only minor changes. For example, you might choose to clone a scan to:
        - change the crawling method, to scan the same web application on the same schedule, for both the desktop and mobile sites.
        - change the schedule, to perform identical scans on both the 1st and 15th of each month.

In the **New/Edit/Clone Scan Configuration** window, select each tab, in turn, and complete the

information. When you have finished, click **Save**.

Select the General Tab

1. Type, or edit, the **Name** of the scan.
2. In the **Maximum Length of Scan (Hours)** field, you can specify a scan duration limit. For example, for a large site, limit the scan duration for faster results. If you shorten the time of the scan, you might not see results for the deeper levels of your web application.
3. Specify the **Scheduling** for this scan:
    1. **Run this scan manually** – When selected, you must manually start this scan. For configured scans, locate the desired scan on the **Scanner > Web Applications** page, and click **Run Now**.
    2. **Once** or **Recurring** – When selected, you specify the date and time that the scan is to start. Options for **Recurring** include **Daily**, **Weekly**, and **Monthly**.
    If the time zone shown is not correct, click its link. The **Barracuda Cloud Control Profile** page opens in a new browser tab. Set your time zone, then return to the **Barracuda Vulnerability Remediation Service** tab of your browser. Although the time zone update might not immediately display on the **Scanner Configuration** page, the correct time zone information will be used for the scan.
4. In the **WAF Bypass** section, specify whether to bypass the Web Application Firewall 's security policies to perform the scan. If you do not have a Web Application Firewall associated with the application, this option is disabled.
    - Select **Bypass the WAF to scan the application (recommended)** to enable the bypass. This increases the accuracy of your scan results.
    - Select **Scan without bypassing the WAF** to disable the bypass. Use this option only if you are running a compliance scan for audit purposes, because it might not find vulnerabilities that exist on your application.

Select the Crawling Tab

1. Select the type of scan you want:
    - **Scan Desktop Site –** Select **Firefox**, **Chrome**, **Safari**, or **Internet Explorer**.
    - **Scan Mobile Site –** Select **iPhone, iPad, or Android**.
    - **Scan using a custom browser** – To use a custom browser, specify the appropriate information in this field.
2. **Requests per second** – Specify the number of requests per second the scanner can make. Enter **0** (zero) to send the maximum requests your server can manage.

    A value of **0** (zero) is not recommended if you are setting up a scan on a *production server*.
    If you are running a scan on a *non-production server*, consider increasing the speed of the scan to as fast as the server can respond, so you will receive scan results more quickly.
    If Barracuda Vulnerability Remediation Service detects that it is starting to overwhelm your server, it will automatically throttle the number of requests per second. You cannot

disable this feature.

3. **Maximum crawl depth** – Specify the maximum link depth from the start page. A value of zero means only the home page will be scanned; the first layer of links is a value of 1, and so on.
4. Select the **Enable evasion techniques** check box if you want the scan to attempt to "confuse" sanitizing or filtering code in your web application during the scan.
   When **Enable evasion techniques** is activated, scanning takes approximately four times as long to complete as a normal scan.

Select the Scan Elements Tab

Select specific scan elements you want to include or exclude from the scan. Each scan element finds a certain set of vulnerabilities. For your first scans, select all of the elements for a thorough check of your web application. If there are certain vulnerabilities you are investigating, select only those elements.

Note: For the most thorough scans, select all scan elements.

Select the Authentication Tab

Do not enter administrator credentials when scanning a production site. See Avoiding Possible Scanning Side Effects for details.

Specify whether to scan the parts of your site accessible only by a user who has logged in. Select from the following three options:

1. **No authentication** – Select if you do not want to scan these areas of your website.
2. **HTTP authentication –** Select to scan areas of your website requiring login credentials. Click the HTTP authentication type used by your website, and then enter the associated **Username** and **Password**.
   Use this option for HTTP Basic authentication, HTTP Digest authentication, and NTLM authentication.
3. **HTML form-based authentication** – Select if your web application has a standard HTML login form that submits to the web server using HTTP POST.
   1. Enter the **Username** and **Password** for the site.
   2. Enter the **Login form URL**, along with your associated username and password. Then, click **Autodetect** to automatically complete the rest of the fields in the section. Alternatively, you can enter the information manually.
   3. Click **Test Authentication** to verify the information you entered is correct and the test will run as expected.

Select the Exclusions Tab

Use the **Exclusions** tab to define hostnames, IP addresses, URL patterns, and file extensions that you do not want the scanner to test for vulnerabilities.

Note that, by default, all images and videos are excluded.

- **To exclude a hostname, IP address, URL pattern, or file extension**:
  Enter the information into the correct segment of the page, then click **Add**.
- **To remove an exclusion**:
  - Click the X next to the exclusion you want to remove.
  - Click **Remove All** to remove all of the exclusions within a section of the page.

If you have unprotected forms that write data to a database or send emails based on form submissions, you might see a large number of database records or emails sent during the scan. You can safely ignore or delete these records and/or emails. They do not cause any damage.

Delete an Existing Scan

This action permanently deletes a scan from the Barracuda Vulnerability Remediation Server.

1. Locate the desired scan in the **Web Applications** table. In the **Actions** column, click **Delete**.
2. Confirm that you want to delete the selected scan. This will permanently delete the scan.

Note: If you think you might use a scan again in the future, you can keep it as a manually scheduled scan and run it when you need it.

Verify an Existing Scan

You must verify that you are the owner of the web application before you can scan it. If you created a scan, but it has not yet been verified, an orange triangle  and **Verify** link display in the **URL** column.

1. Click the **Verify** link.
2. In the **Verify** window, choose a method of verification, as described in How to Create a New Web Application Scan.
   - If you specified email, double-check the email address you entered, correct it if needed, then click **Resend Email**.

- For other methods, select the appropriate method and take the appropriate action on your web application. Then click **OK**.

Working with Web Applications

All of these actions are performed from the **Scanner > Web Applications** page.

Create a New Web Application

See How to Create a New Web Application Scan.

Clone or Edit an Existing Web Application

Goal	Steps
Edit an existing web application	1. Navigate to the **Scanner > Web Applications** page. 2. In the **Web Applications** table, locate the Web Application you want to edit. 3. In the **Actions** column, click **Edit**.
Clone an existing scan	1. Navigate to the **Scanner > Web Applications** page. 2. In the **Web Applications** table, locate the Web Application you want to clone. 3. In the **Actions** column, click **Clone**. • Be sure to enter a new **Name** for this Web Application to distinguish it from the original scan. • Cloning a Web Application is faster than creating a new scan, if you are making only minor changes. For example, you might choose to clone a Web Application to: ◦ use the same configuration to scan a different Web Application that you own. ◦ maintain all configured scans in a second copy of a site, for example, a staging copy.

In the **Edit/Clone Web Application** window, complete the required information. When you have finished, click **Save**.

Figures