This page describes how to use Web Security Scanner to scan your Google Cloud applications. Web Security Scanner works with App Engine, Compute Engine, or Google Kubernetes Engine (GKE).

Before you scan, carefully audit your application for any feature that may affect data, users, or systems beyond the desired scope of your scan.

Because Web Security Scanner populates fields, pushes buttons, clicks links, and other interaction, you should use it with caution. Web Security Scanner might activate features that change the state of your data or system, with undesirable results. For example:

- In a blog application that allows public comments, Web Security Scanner might post test strings as comments on all your blog articles.
- In an email sign-up page, Web Security Scanner might generate large numbers of test emails.

For tips about how to minimize risk, see best practices (/security-scanner/docs/overview#best_practices) to prevent unintended consequences.

When you scan your app, it's best to use a test account that doesn't have access to sensitive data or harmful operations. Create a test account that can sign in to your app, and note the login credentials to provide for authentication when creating a scan. This enables you to use the test account to scan data.

1. Go to the Web Security Scanner (https://console.cloud.google.com/projectselector2/security/web-scanner/) page in the Cloud Console.

   Go to the Web Security Scanner page (https://console.cloud.google.com/projectselector2/security/web-scanner/)
2. Click **Select**, and then select a project that already has an App Engine, Compute Engine, or GKE application deployed.
3. To display the new scan form, click **Create scan** or **New scan**.

4. To add values to the new scan form, use the following table as a guide:

Field	Description
Starting URLs	A simple site usually requires only one starting URL, like the home, main, or landing page for the site, from which Web Security Scanner can find all other site pages. However, Web Security Scanner might not find all of the pages if a site has: • A lot of pages • Islands of unconnected pages • Navigation that requires complex JavaScript like a mouseover-driven multilevel menu In such cases, specify more starting URLs to increase scan coverage.
Excluded URLs	To reduce complexity, exclusions are defined using a simplified proto-language using one or more * wildcards, instead of requiring a valid regular expression. For details and sample valid patterns, see Excluding URLs in Scans (/security-scanner/docs/excluded-urls/)
Authentication > Google account	You can create a test account in Gmail and then use the account to scan your product. If you are a Google Apps customer, you can create test accounts within your domain, for example, `test-account@yourdomain.com`. In Web Security Scanner, these accounts work like Gmail accounts. Two factor authentication is not supported. Google enforces a real name policy on Google accounts. If the name on your test account doesn't look real, the account might be blocked.
Authentication > Identity-Aware Proxy alpha	To protect resources with Identity-Aware Proxy, see the IAP guide (/iap/docs/how-to). To use Web Security Scanner with an IAP-protected resource, first add the Web Security Scanner service account as an IAP member: a. Go to the IAP page (https://console.cloud.google.com/projectselector2/security/iap/) in the Cloud Console. b. Select the project that you want to use with Web Security Scanner. c. Select the application resource you want to scan, and then click **Add Member** on the **Info Panel**. d. In the **New members** box on the **Add members** panel, enter the Web Security Scanner service account in the form of `service-project-number@gcp-sa-websecurityscanner.iam.gserviceaccount.com`. e. On the **Select a role** drop-down list, select **Cloud IAP > IAP Secured Web App User**. f. When you're finished adding roles, click **Save**. Next, add the OAuth client ID to the scan. Web Security Scanner can only scan applications that are protected by a single OAuth Client ID. To add the OAuth client ID: a. Go to the IAP page (https://console.cloud.google.com/projectselector2/security/iap/) in the Cloud Console. b. Select the project that you want to use with Web Security Scanner. c. On the **Overflow menu**, select **Edit OAuth Client**.

	d. On the **Client ID for web application** window that appears, copy the **Client ID**. e. Go to the Web Security Scanner page (https://console.cloud.google.com/projectselector2/security/web-scanner/scanConfigs/) in the Cloud Console. f. Under **Authentication**, select **Identity-Aware Proxy alpha**. g. In the **OAuth2 Client ID** box, paste the OAuth client ID that you copied, and then click **Save**.
Authentication > Non-Google account	Select this option if you have created your own authentication system and you aren't using Google Account services. Specify the login form's URL, the username, and the password. These credentials are used to sign in to your application and scan it. Support for login forms is still in development, and might not work by default with your system.
Schedule	You can set the scan to run daily, weekly, every two weeks, or every four weeks. It's best to create a scheduled scan to ensure that future versions of your application are tested. Also, because we occasionally release new scanners that find new bug types, running a scheduled scan offers more coverage without manual effort.

5. When you're finished adding values, click **Create**. You can now run the new scan.

By default, Web Security Scanner uses randomly assigned IP addresses during each run, so it doesn't have a predictable IP address to use in your firewall configuration. To make Web Security Scanner IP addresses predictable, complete the guide to enable scans from static IPs (/security-scanner/docs/static-ip-scan).

To run a scan:

1. Sign in to the test account that you used to create the scan.
2. Go to the Web Security Scanner (https://console.cloud.google.com/projectselector2/security/web-scanner/) page in the Cloud Console.

   Go to the Web Security Scanner page (https://console.cloud.google.com/projectselector2/security/web-scanner/)
3. Click **Select**, and then select the project that you created the scan in.
4. Under **Scan configs**, click the name of the scan that you want to run.
5. On the scan details page, click **Run**.

The scan is placed in a queue, and there might be a delay before it runs. It can take several minutes or many hours to run, depending on the system load and features like:

- Site complexity
- Number of actionable elements per page
- Number of links

- The amount of JavaScript on the site, including navigation

You can set up and run up to 10 different scans before you need to delete or clean up previously saved results.

The status and results of a scan are displayed on the scan details page in the Cloud Console. To view scan results:

1. Sign in to the test account that you used to create the scan.
2. Go to the Web Security Scanner (https://console.cloud.google.com/projectselector2/security/web-scanner/) page in the Cloud Console.

   Go to the Web Security Scanner page (https://console.cloud.google.com/projectselector2/security/web-scanner/)
3. Click **Select**, and then select the project that contains the scan that you want to review.
4. Under **Scan configs**, click the name of the scan that you want to review.

The scan details page loads and displays results from the most recent scan. If a scan is in progress, the **Results** tab displays the current completion percent. To display results from previous scans, select the scan date and time from the drop-down list.

Details for completed scans include:

- The **Results** tab displays a list of vulnerabilities the scan found, if any.
- The **URLs crawled** tab displays a list of URLs that the scan checked.
- The **Details** tab includes:
  - Starting URLs
  - Authentication
  - User agent
  - Maximum scan speed as queries per second (QPS)

You can find more information about the scan in the project logs page (https://console.cloud.google.com/project/_/logs).

To edit a scan:

1. Sign in to the test account that you used to create the scan.
2. Go to the Web Security Scanner (https://console.cloud.google.com/projectselector2/security/web-scanner/) page in the Cloud Console.

   Go to the Web Security Scanner page (https://console.cloud.google.com/projectselector2/security/web-scanner/)
3. Click **Select**, and then select the project that contains the scan that you want to edit.
4. Under **Scan configs**, click the name of the scan that you want to edit.
5. On the scan details page that appears, click **Edit**.
6. On the **Editing [scan name]** page that appears, make the changes that you want, and then click **Save**.

The edited scan runs when it's next scheduled, or you can manually run it to get updated results.

To delete one or more scans:

1. Sign in to the test account that you used to create the scan.
2. Go to the Web Security Scanner (https://console.cloud.google.com/projectselector2/security/web-scanner/) page in the Cloud Console.

   Go to the Web Security Scanner page (https://console.cloud.google.com/projectselector2/security/web-scanner/)
3. Click **Select**, and then select the project that contains the scan that you want to edit.
4. Under **Scan configs** select the checkbox next to one or more scans that you want to delete.
5. Click **Delete**, and then click **Ok**.

All of the scans that you selected are deleted.

- Read about scan results (/security-scanner/docs/scan-result-details) and impact on logs.
- Learn how to exclude URLs from scans (/security-scanner/docs/excluded-urls).
- Learn how to remediate findings (/security-scanner/docs/remediate-findings).