RAPID7

AppSpider Enterprise

Getting Started Guide

Contents

About AppSpider Enterprise

AppSpider Enterprise allows you to manage and coordinate multiple AppSpider, web application scan engine, installations across your organization.

This guide will provide an overview of the AppSpider Enterprise platform and features for:

- System Administrators
- Client Administrators
- Individual Users

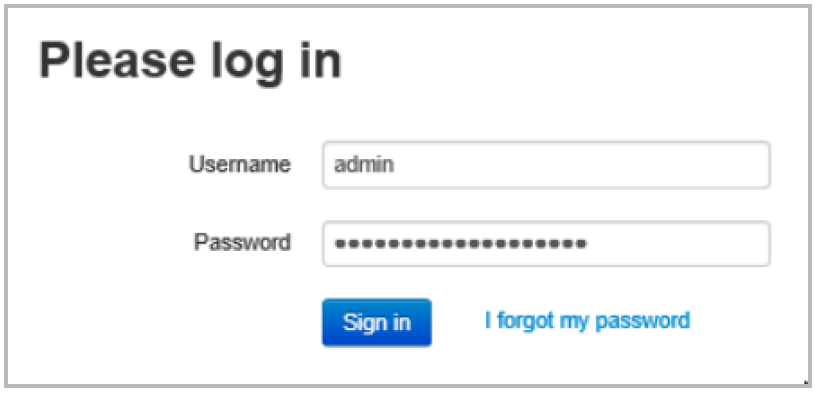
Tip: In order to run AppSpider Enterprise, a SQL Server Database as well as an AppSpider Pro scan engine must be configured. For installation and setup information, see the AppSpider Enterprise Installation Guide.

Getting Started (System Administrator)

AppSpider Enterprise system administrators have full permissions and can interact with multiple organizations across the platform.

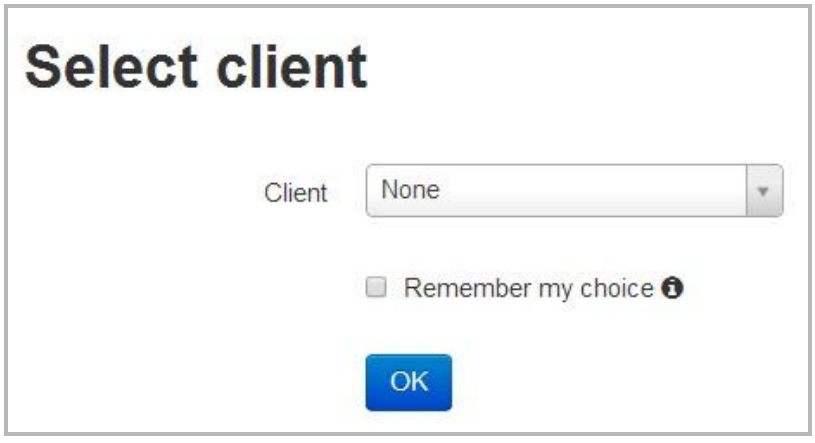
Login

To access the *Login* page, open a web browser and enter the IP address of the AppSpider installation in the navigation bar. The default path is localhost/AppSpiderEnterprise/



1. Provide your **Username** and **Password** then click the **Sign in** button.

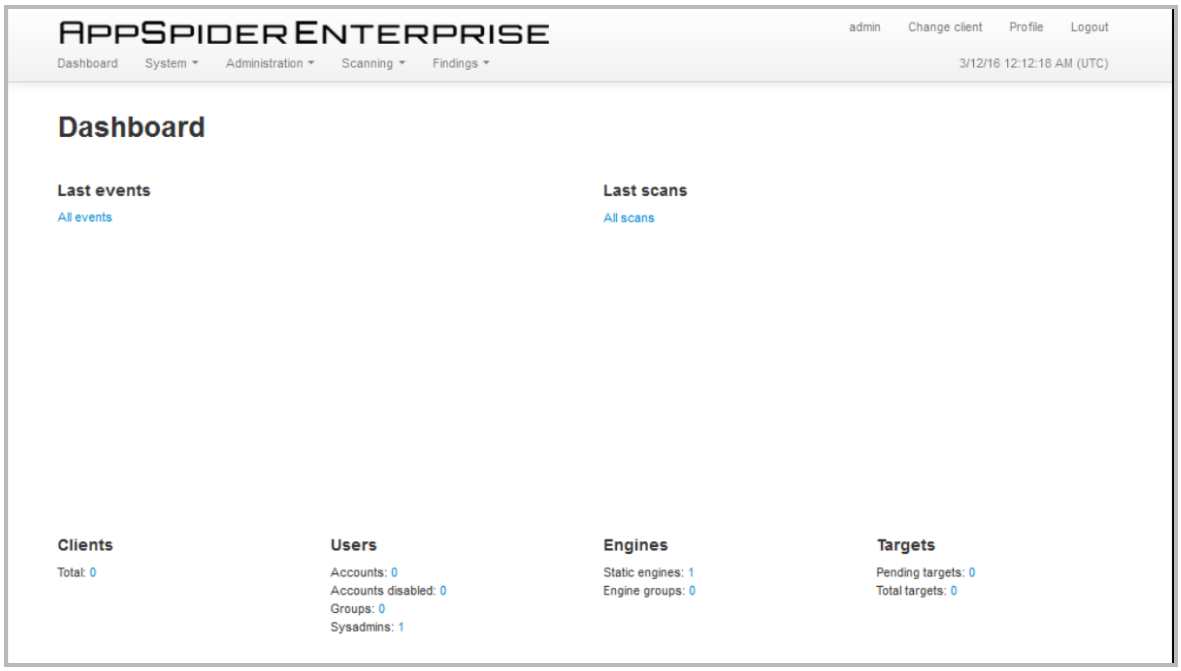
Once logged in as the system administrator, you will be presented with a **Client** drop down menu. The default *Client* is set to **None**.



2. Click the **OK** button to be authenticated as the system administrator.

   Tip: System administrators will have access to clients as they are introduced to the system.

Once authenticated as the system administrator, you will be taken to the *Dashboard*. From here, you can view recent **events** and **scans** as well as a summary of **Clients**, **Users**, **Scan Engines**, and **Targets**.

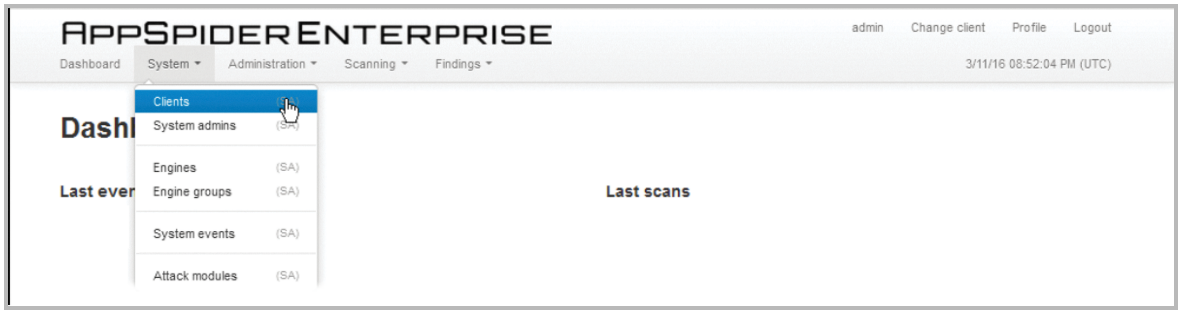


Client

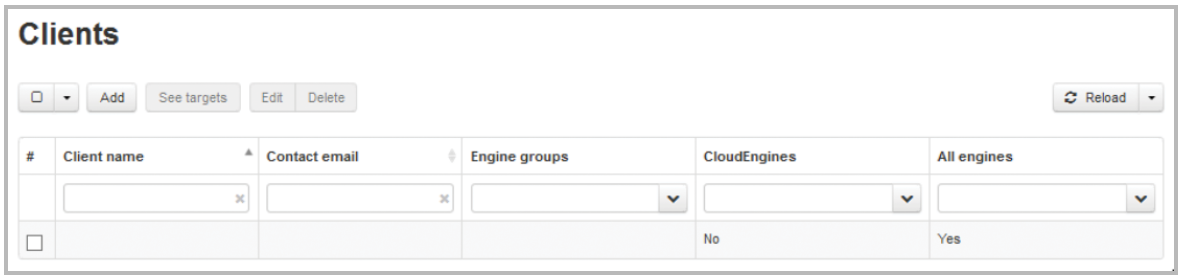
A client can be considered a company domain which contains a collection of users that interact with AppSpider Enterprise.

To add a client:

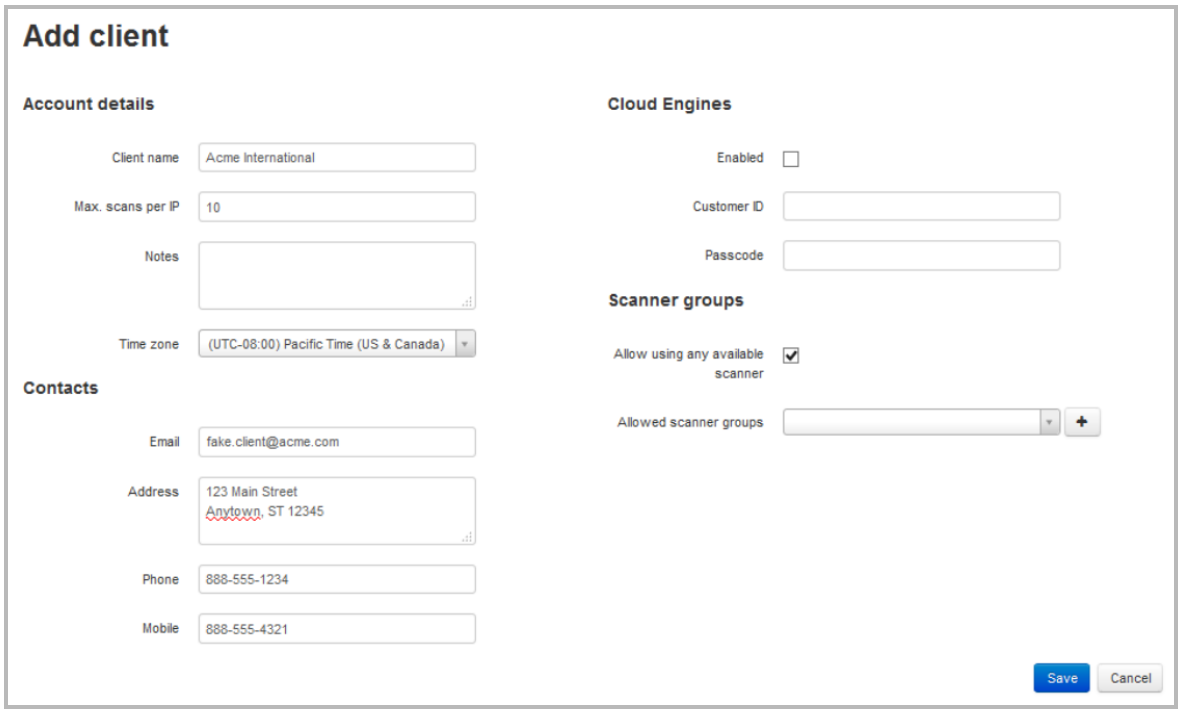
1. Select the **System** drop down menu.
2. Select **Clients**.



3. Click the **Add** button on the *Clients* page.



Add Client



1. Provide *Account details* including **Client name**, **Maximum scans per IP**, **Notes**, and **Time zone**.

   Tip: Max scans per IP can protect a scanned web application from DDoS. Scans against the same IP cannot exceed the value entered in this field.

2. Next, provide the *Contacts* information including **Email**, **Address**, and **Phone number(s)**.

   Tip: An SMTP server setup is required in order to handle outgoing email communication. AppSpider Enterprise can be configured to use an SMTP server during the installation process.

Cloud Engines

Cloud Engines are available to customers that have purchased the AppSpider On-Demand software as a service.

1. Select the **Enabled** check box.
2. Provide **Customer ID** and **Passcode**.
3. When you are finished, click the **Save** button.

Scanner Groups

Allow using any available scanner
You can enable the client to access any scan engine within the system.

1. Select the check box for **Allow using any available scanner**. If selected, AppSpider Enterprise will access the scan engine(s) added during the installation process.
2. When you are finished, click the **Save** button.

Allowed scanner groups
Scanner groups also known as engine groups can contain more than one scan engine. Engine groups are often assigned to different areas of your organization. Review the AppSpider Enterprise User's Guide for more information about creating engine groups.

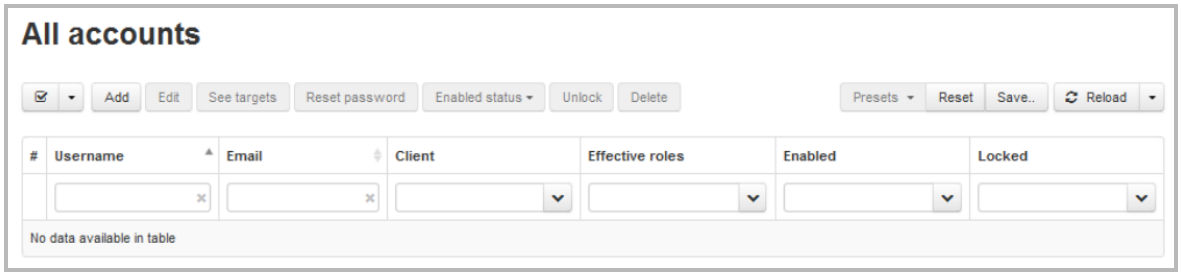
Account

Accounts are individual users of a client. System administrators and client administrators have the ability to create accounts and assign permissions that determine what they can access and which actions they can perform. It is not required but we recommend adding a client administrator.

To add a client administrator account:

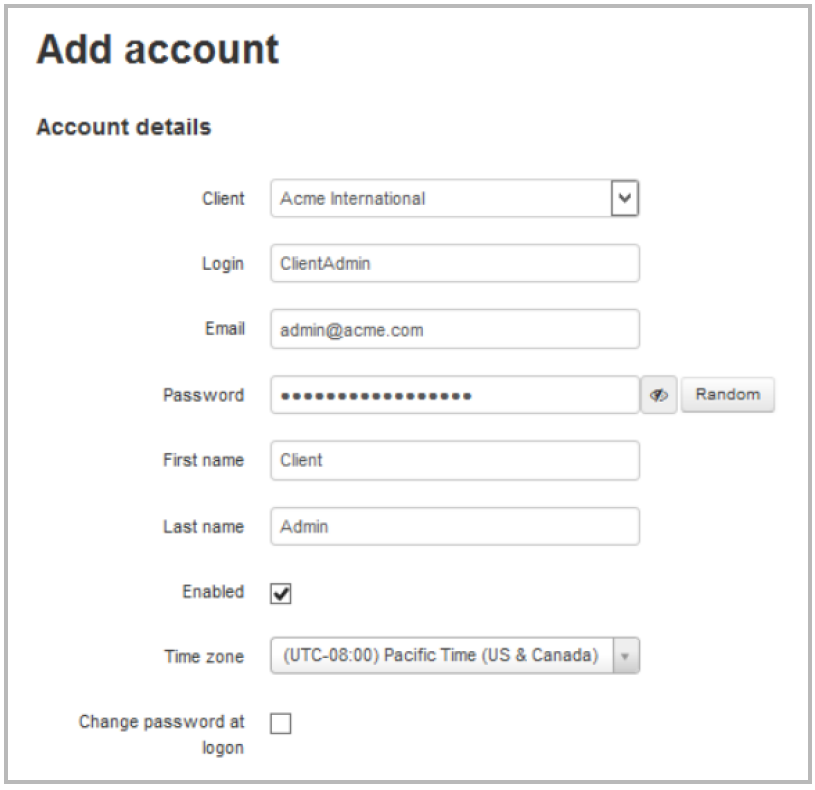
1. Select the **Administration** drop down menu.
2. Select **All Accounts**.

3. Click the **Add** button on the *All accounts* page.



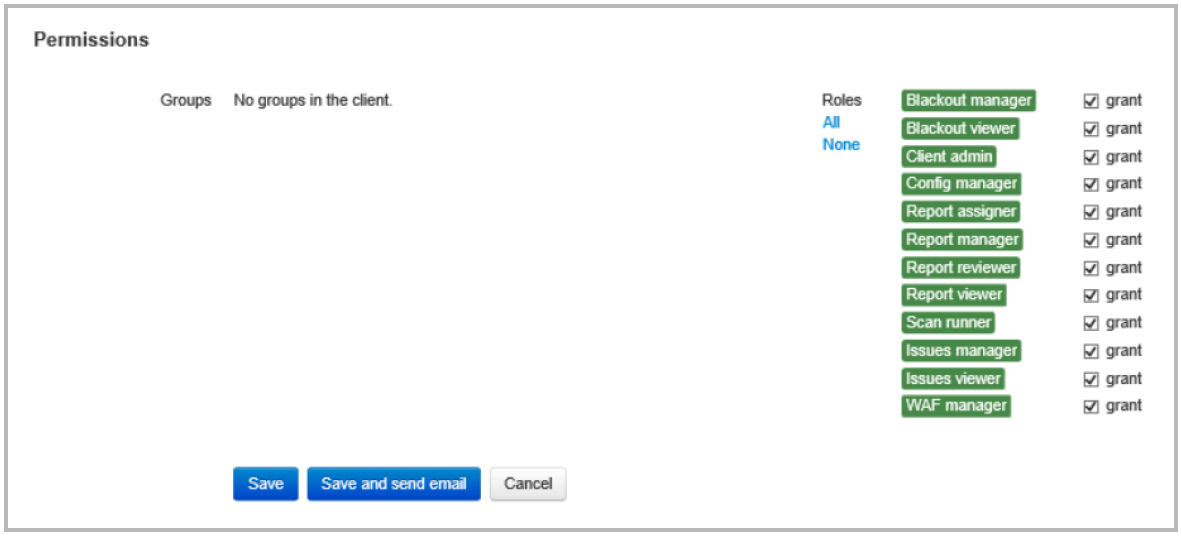
Add account

1. Provide *Account details* including **Client**, **Login**, **Email**, **Password**, **First name**, **Last name**, and **Time zone**.



Permissions

2. Select the *Roles* for the account.
3. When you are finished, click the **Save** button.

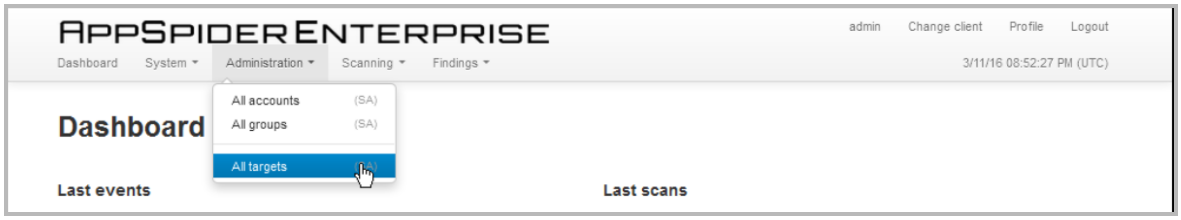


Target

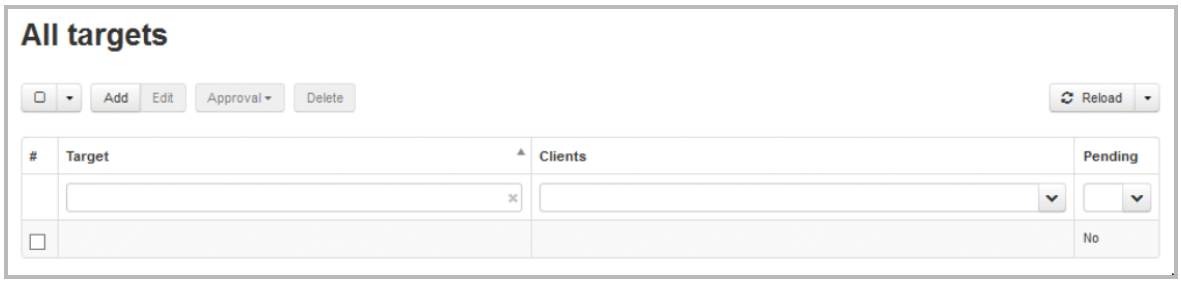
A target is a web application that you intend to scan.

To add a target:

1. Select the **Adminstration** drop down menu.
2. Select **All targets**.

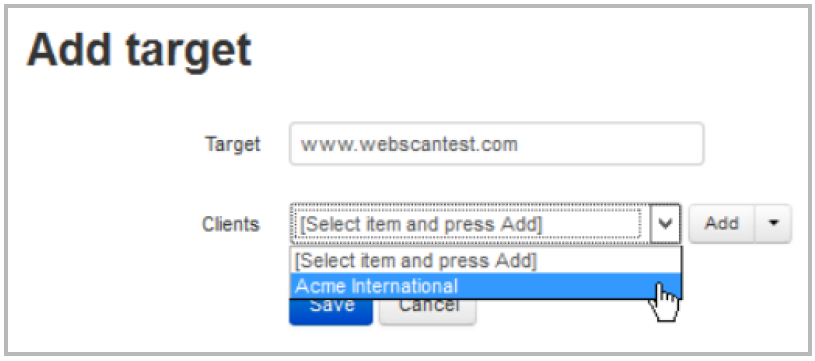


3. Click the **Add** button on the *All targets* page.

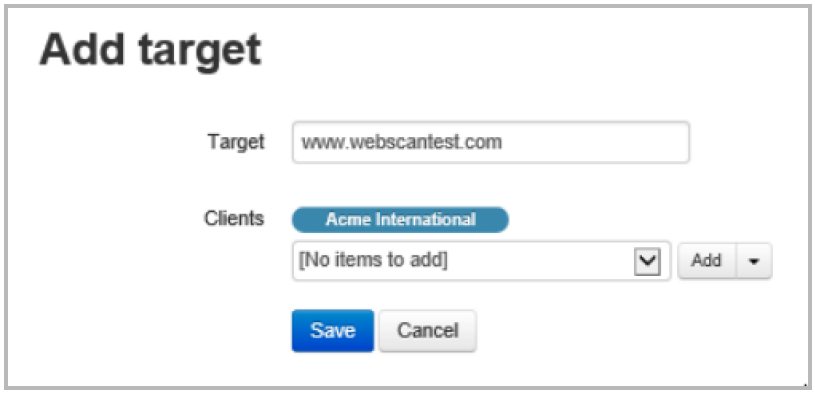


Add Target

To help you learn how to set up a target to be used with a scan, you can use www.webscantest.com. Webscantest.com is our test web application that is loaded with vulnerabilities. Once you are familiar with the interface, you can move on to scanning your organization's own applications.



1. Provide the *Target* url of the web application that you intend to target.
2. Next, locate the *Client* from the drop down menu and click the **Add** button. Repeat this step to associate additional clients with the target url.



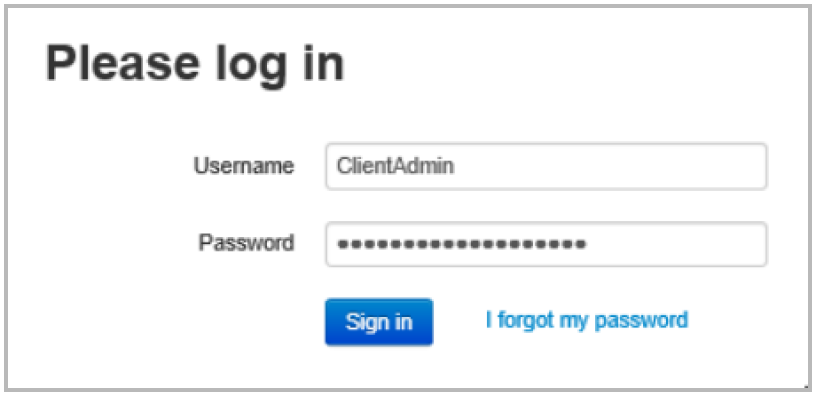
3. When you are finished, click the **Save** button.

Getting Started (Client Administrator)

AppSpider Enterprise client administrators have a wide range of privileges and can assign department specific permissions for individual users within a client.

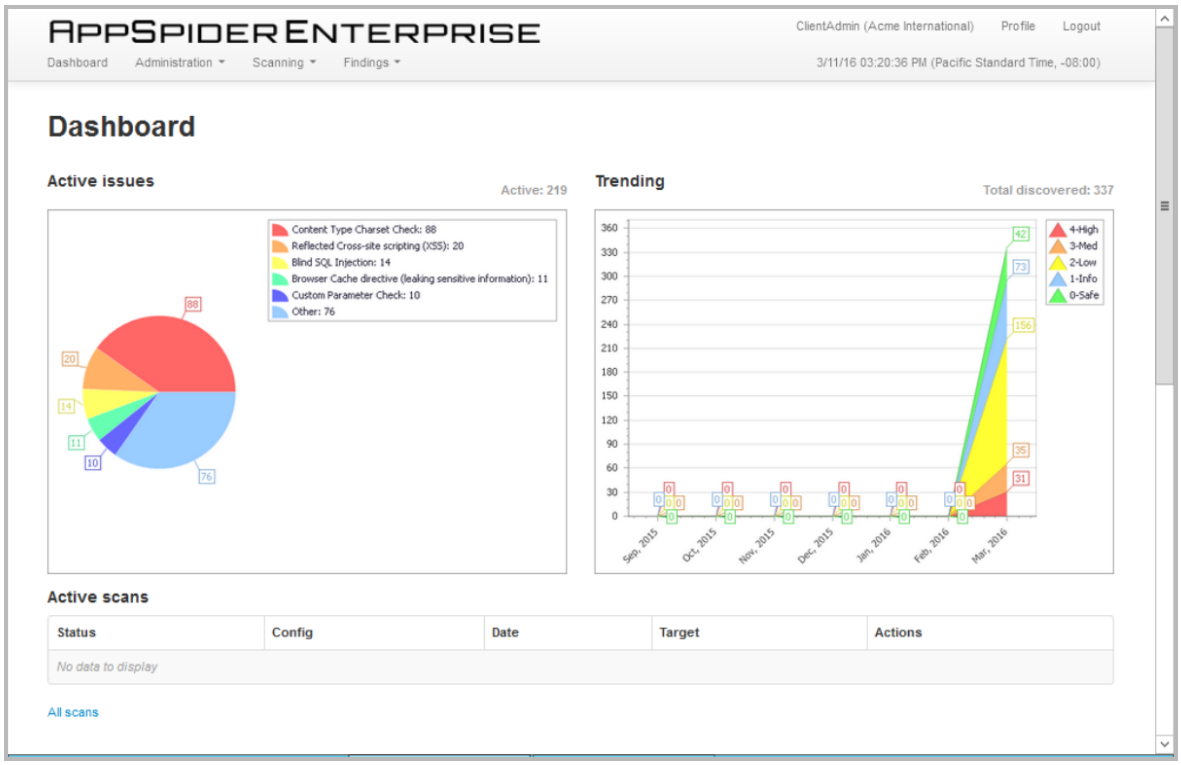
Login

To access the *Login* page, open a web browser and enter the IP address of the AppSpider installation in the navigation bar. The default path is localhost/AppSpiderEnterprise/



1. Provide your **Username** and **Password** then click the **Sign in** button.

Once logged in as a client administrator, you will be taken to the Dashboard where you can view **Active issues**, **Trending** vulnerabilities, and **Active scans** within the client.

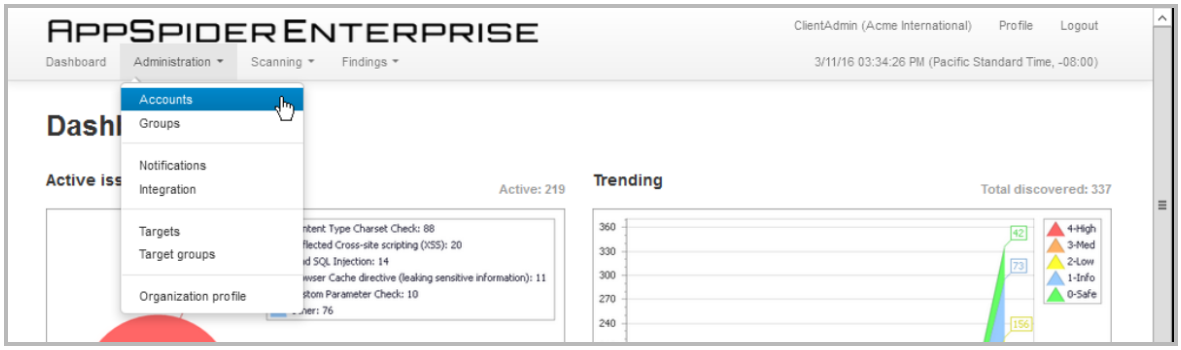


Account

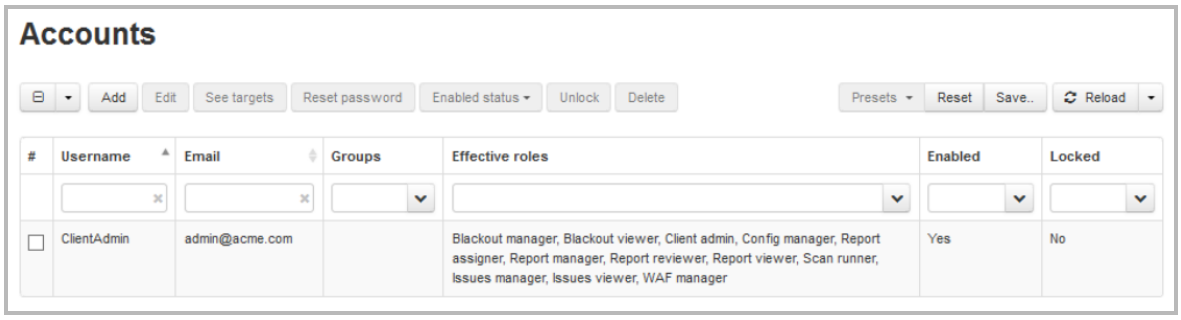
As client administrator, you can create user accounts and assign permissions that determine what they can access and which actions they can perform.

To add an account:

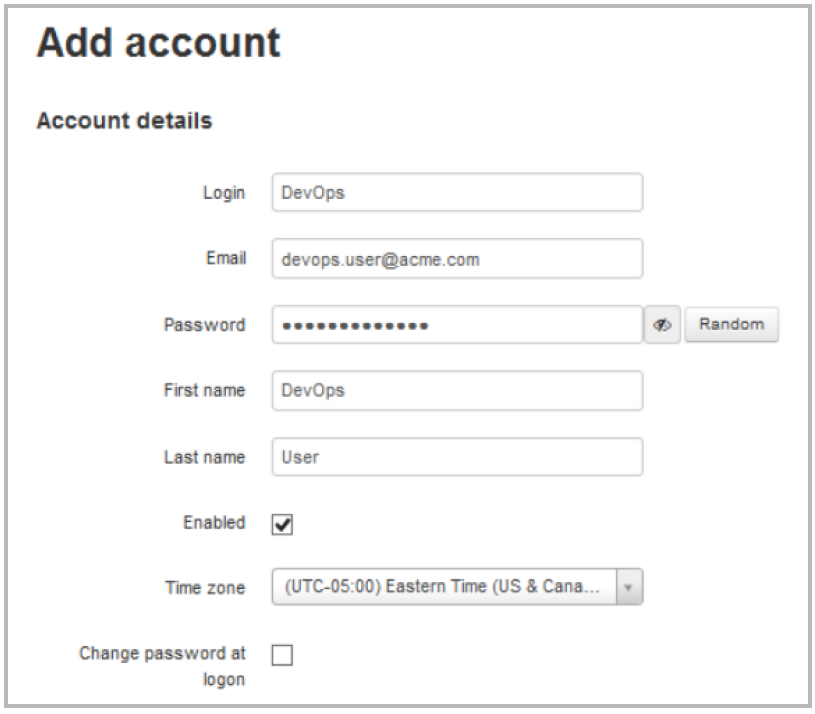
1. Select the **Administration** drop down menu.
2. Select **Accounts**.



3. Click the **Add** button on the *Accounts* page.

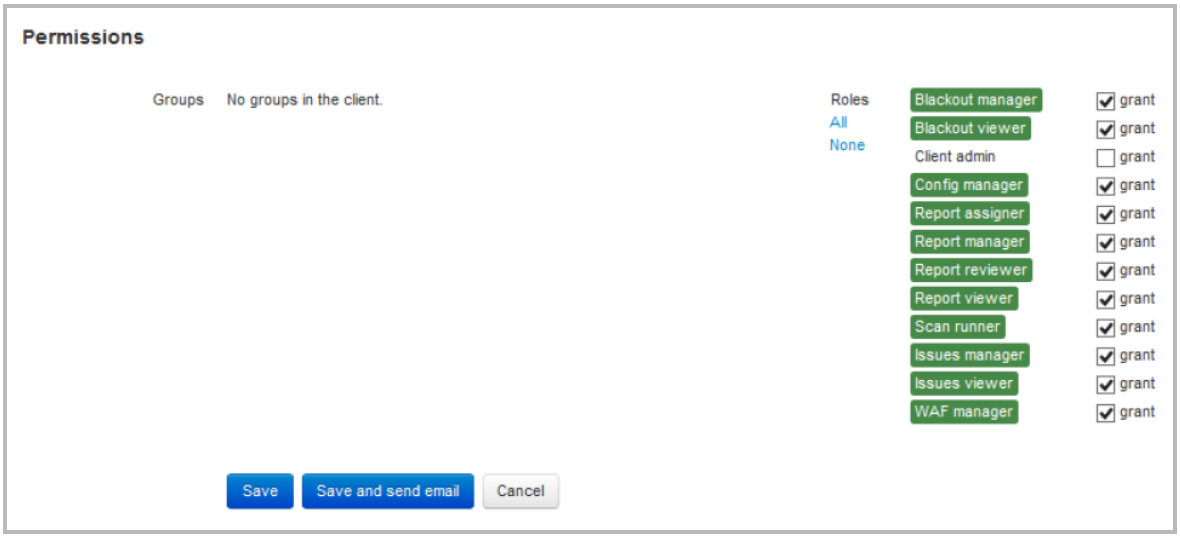


Add account



1. Provide *Account details* including **Login**, **Email**, **Password**, **First name**, **Last name**, and **Time zone**.

Permissions



2. Select the *Roles* for the user.
3. When you are finished, click the **Save** button.

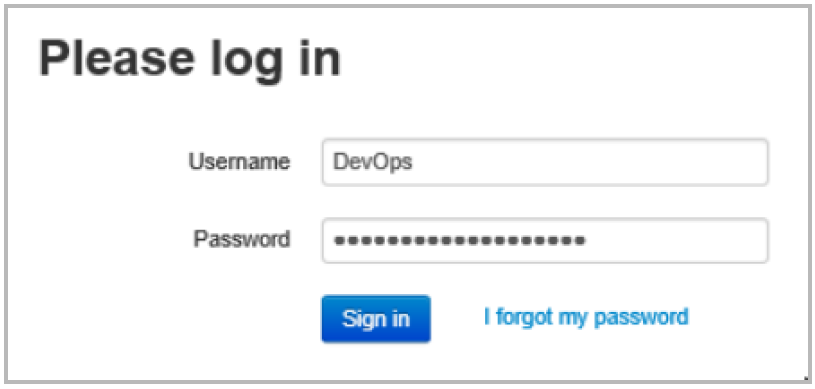
   Tip: Client administrators can create several accounts. Repeat these steps to add additional user accounts to the client.

Getting Started (Individual User)

AppSpider Enterprise individual users have the ability to perform tasks based on the permissions given to them by administration.

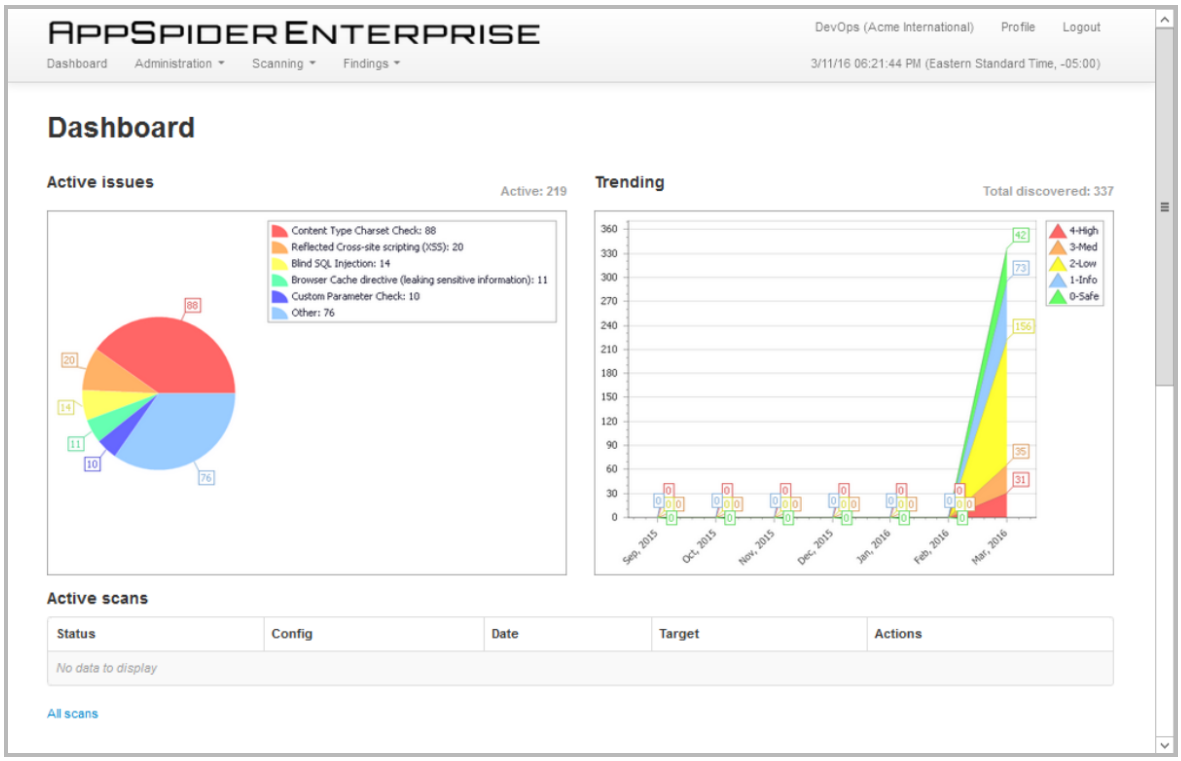
Login

To access the *Login* page, open a web browser and enter the IP address of the AppSpider installation in the navigation bar. The default path is localhost/AppSpiderEnterprise/



1. Provide your **Username** and **Password** then click the **Sign in** button.

Once logged in, you will be taken to the Dashboard where you can view **Active issues**, **Trending** vulnerabilities, and **Active scans** within the client.



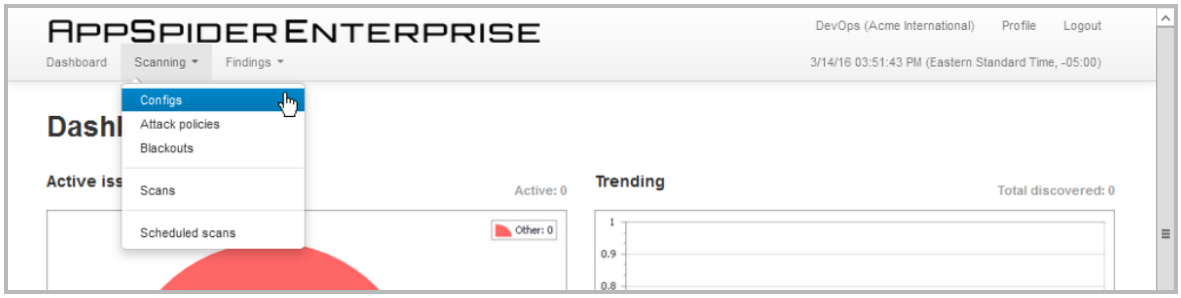
Configure

In addition to crawling traditional applications, AppSpider's Universal Translator technology, is capable of interpreting the new technologies being used in today's web and mobile applications.

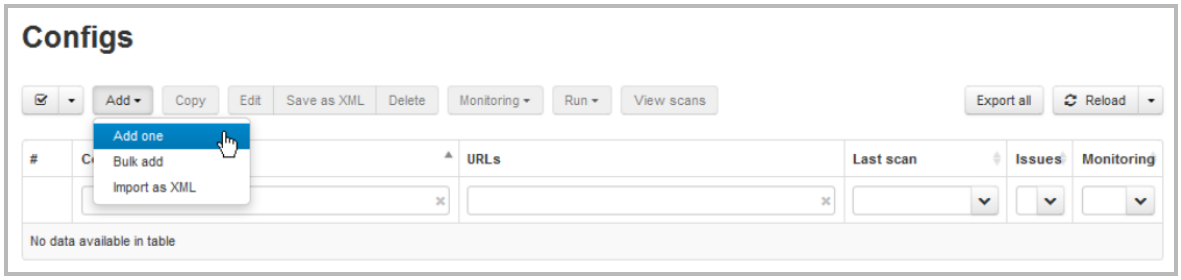
AppSpider gives you the ability to configure many aspects of the scan and gives you more visibility into what exactly is happening behind the scenes.

To add a scan configuration:

1. Select the **Scanning** drop down menu.
2. Select **Configs**



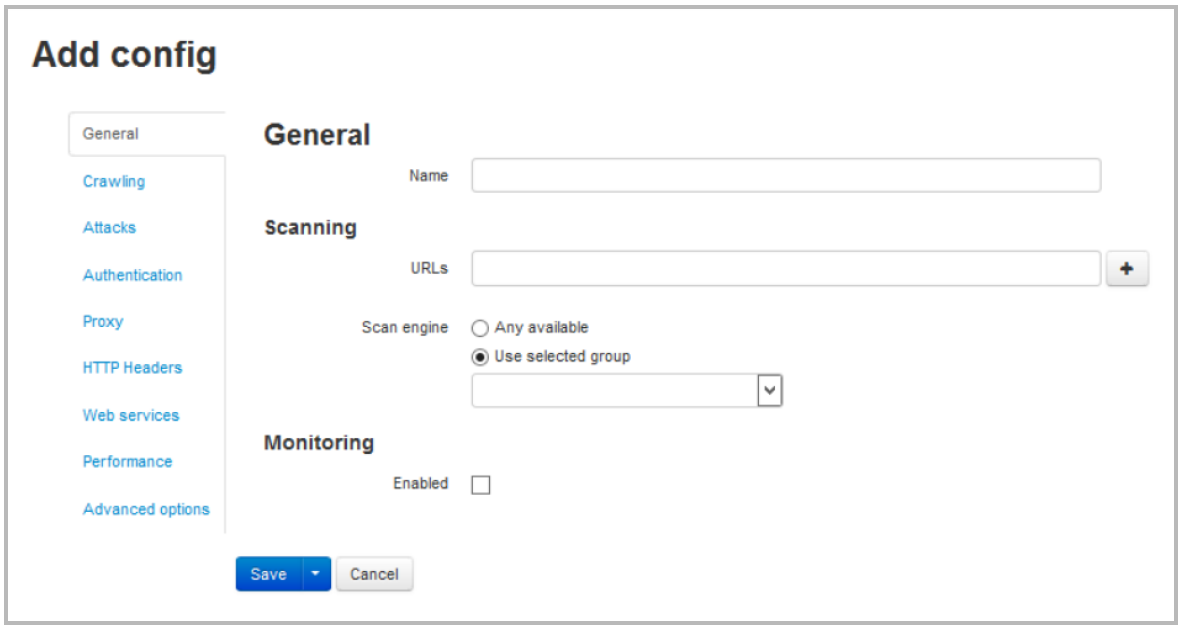
3. Select the **Add** drop down menu on the *Configs* page.
4. Click **Add one** to create a scan configuration.



Add config

A scan configuration is a collection of settings for a scan. These settings include:

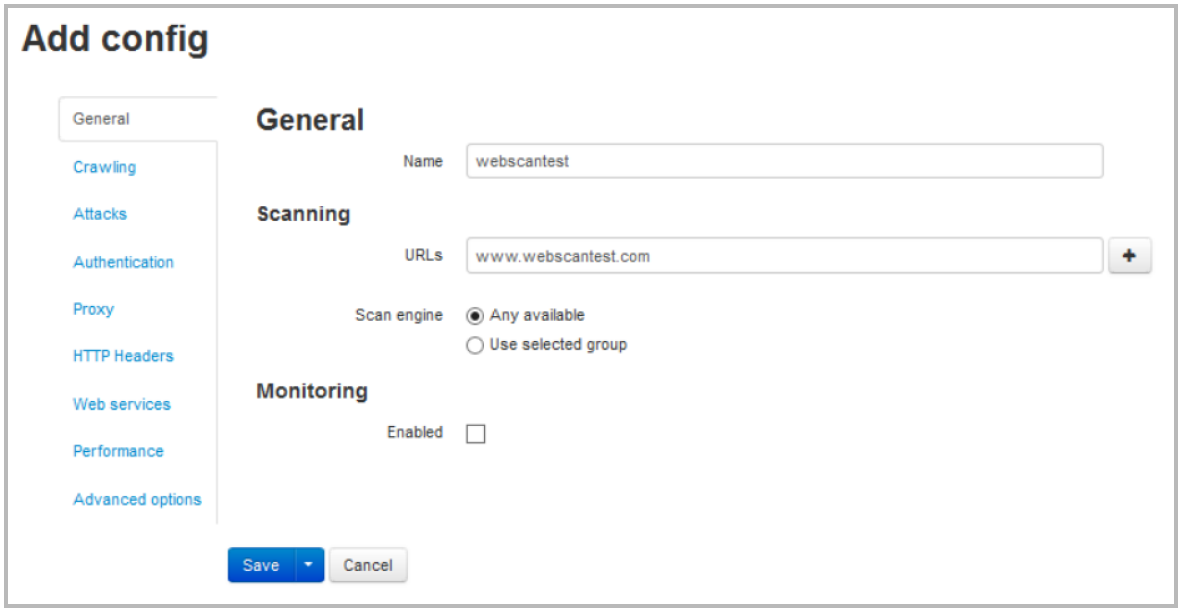
- **General Information:** Provide name and target location of the scan.
- **Crawl Restrictions:** Create a whitelist and/or blacklist for crawling.
- **Attack Policy:** Select which modules AppSpider will use for crawling and/or attacking.
- **Authentication:** Select and configure the authentication method used during the scan.
- **Proxy Settings:** Edit the proxy settings used for the scan.
- **HTTP Headers:** Edit the settings for the HTTP headers used during the scan.
- **Web Service:** Import WSDL files for SOAP-based services.
- **Performance Settings:** Edit the performance settings and logging options.



General Settings

To help you learn how to set up a scan, you can use www.webscantest.com as your target. Webscantest.com is our test web application that is loaded with vulnerabilities. Once you are familiar with the interface, you can move on to scanning your organization's own applications.

1. Select **General** from the *Edit config* page.
2. Provide a **Name** for the config.



Scanning

Eligible URLs include targets created, approved and assigned to your client, by the system admin.

1. Provide the URL of the web application that you intend to scan and click the **[+]** button.

   Tip: By default, AppSpider will crawl both the http and https protocols for a specified url. If you see a URL that you don't want to scan, click on the **[X]** next to the URL in the list to restrict the scan.

2. Select the **Any available** option for *Scan engine*. If selected, AppSpider Enterprise will access the scan engine(s) added during the installation process.

Monitoring

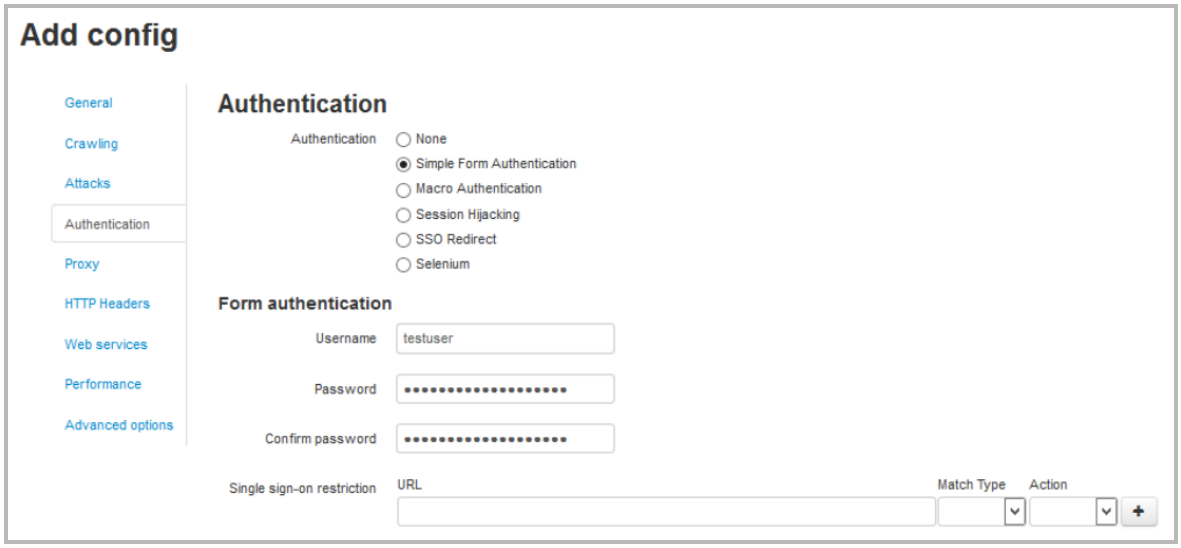
If enabled, this continuous scanning feature will check your web applications periodically to see if they have changed and rescans them if they have.

Authentication

Many applications require authentication and use various authentication schemes. AppSpider Enterprise supports the following authentication approaches for logging into websites and maintaining the session for the duration of scan.

- **Simple Form:** Form authentication looks simple, but developers can implement it in various ways. AppSpider enables users to logon to forms by entering credentials which it then uses to authenticate.
- **Macro:** Macro authentication is convenient when you have a multiple page authentication sequence. AppSpider has a built in macro, to record a login sequence, which can then be used for successful authentication.
- **Session Hijacking:** This authentication mechanism requires manual interaction to acquire a session cookie in order to properly authenticate and perform a scan on your web application.
- **SSO Redirect:** Allows initial redirect for single sign on.
- **Selenium:** AppSpider can leverage a Selenium script of a login sequence to automate authentication.
- **HTTP:** This server based access control supports application servers that use Basic and NTLM authentication to control access to the web apps they serve.

AppSpider will crawl and perform attacks on the application(s) specified in the *General* settings with a predefined set of rules. However, if your application requires **Simple Form Authentication**, access the **Authentication** page and provide the required credentials. Or, if you have a sophisticated login sequence, select **Macro Authentication** and provide a macro recording so AppSpider can properly access your application during the crawl.



Scanning

AppSpider Enterprise allows organizations to perform an unlimited number of simultaneous scans. Scans in AppSpider Enterprise can be started manually or set to a scan schedule that meets your needs.

Notifications

Before initiating a scan, be sure to consider notifications. AppSpider will perform input validation attacks on submission forms. Thus, if a form submission triggers a notification to be sent to an individual or a team within your organization, they should expect to see similar activity when AppSpider performs a scan.

Tip: Be sure to turn notifications off or notify people to ignore the alerts.

Large applications

If the target application is too large, the scan may not complete. What constitutes a large site depends on the interplay of several factors, including the number of functional links, links that accept or process user input, the number of user input parameters, and site complexity.

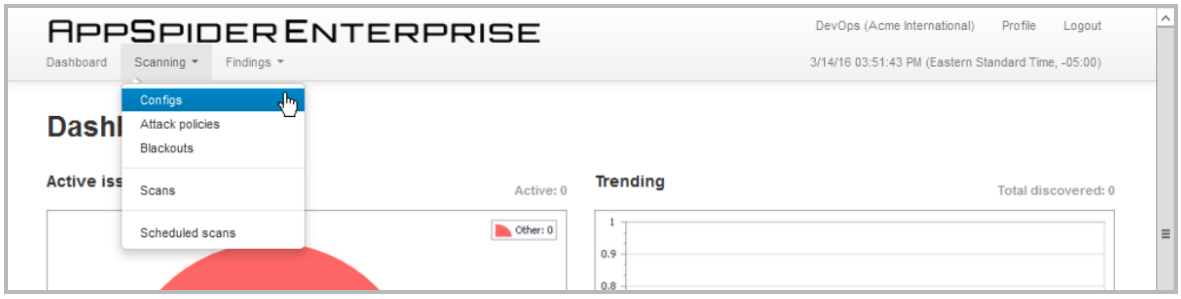
Tip: The best practice for scanning larger targets is to segment the assessment into separate scan configurations for subdomains or subdirectories.

Run A Scan

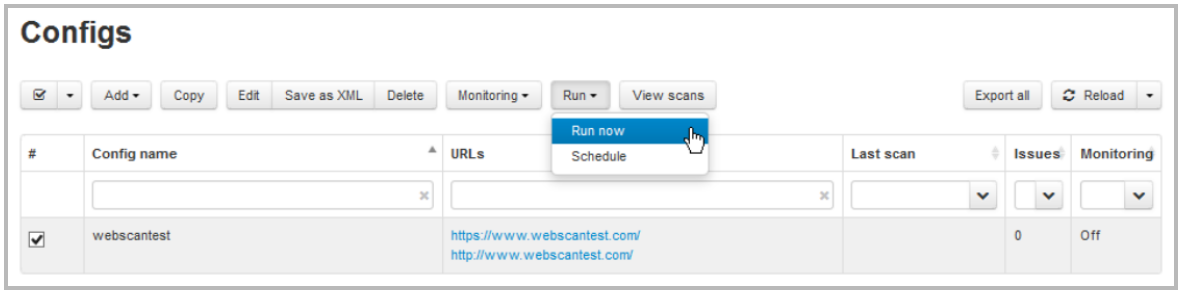
If an immediate scan is necessary, you can launch a scan at any time with AppSpider Enterprise.

To run a scan:

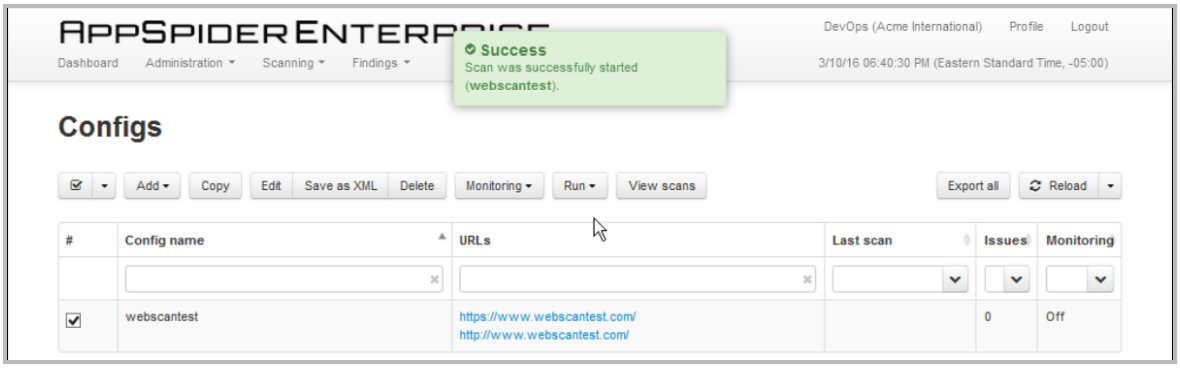
1. Select the **Scanning** drop down menu.
2. Select **Configs**.



3. Select the checkbox for the config(s) you intend to scan.
4. Select the **Run** drop down menu on the *Configs* page.
5. Click **Run now** to continue.



You will be notified as soon as your scan starts.

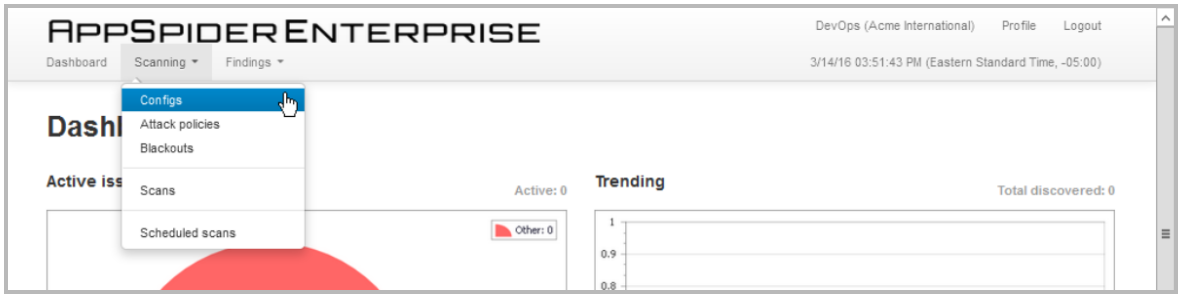


Scan Scheduling

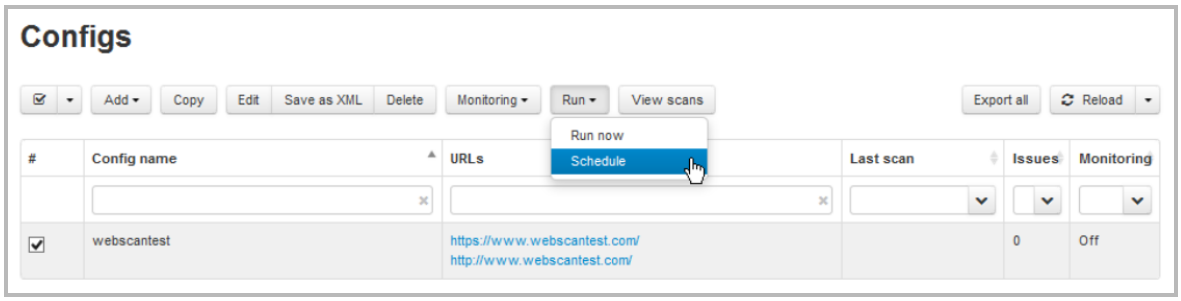
With AppSpider Enterprise you have the flexibility to schedule the start time and frequency of scans.

To schedule a scan:

1. Select the **Scanning** drop down menu.
2. Select **Configs**.



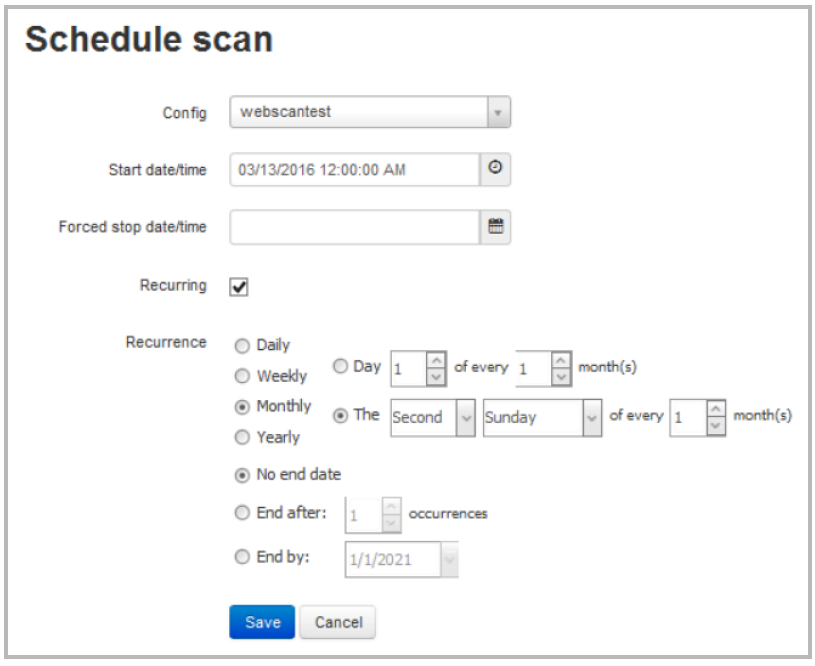
3. Select the checkbox for the config(s) you intend to scan.
4. Select the **Run** drop down menu on the *Configs* page.
5. Click **Schedule** to continue.



Schedule scan

1. Provide the name of the **Config** that you want to schedule.
2. Select the **Start date/time**.
3. Select **Forced stop date/time**.

   Tip: You can discontinue a scan schedule after any number of occurrences or on a specific date.
4. Select **Recurring** to have the scan reoccur on a daily, weekly, monthly, or yearly basis.
5. When you are finished, click the **Save** button.



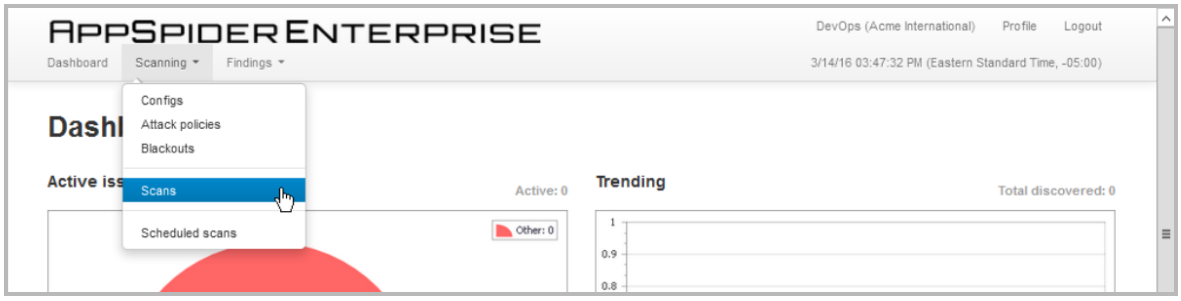
Once your schedule is saved, your scan(s) will be performed as you defined.

Scan Status

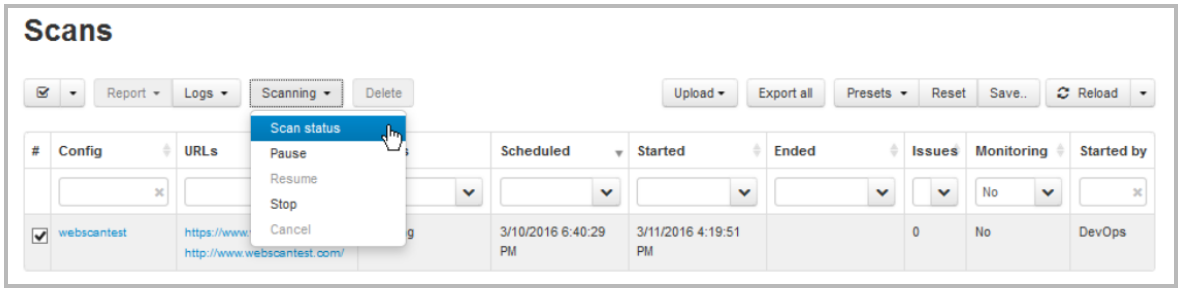
You can view the progress of your scans as soon as they are started.

To view the status of a scan:

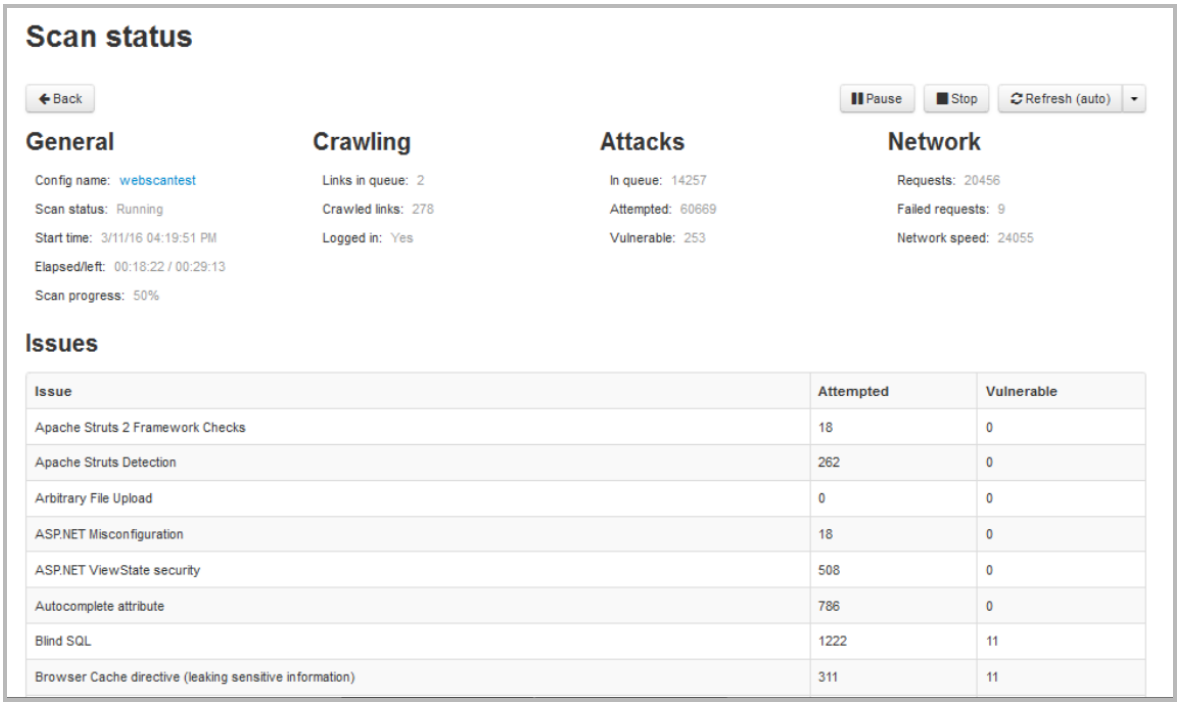
1. Select the **Scanning** drop down menu.
2. Select **Scans**.



3. Select the checkbox for the scan configuration that you want to check the status of.
4. Select the **Scanning** drop down menu on the *Scans* page.
5. Click **Scan status** to continue.



Once the *Scan status* page is loaded, you can view **General** information for the current scan. Active **Crawling**, **Attack**, and **Network** statistics are presented as well. *Attempted* attacks and the number of *Vulnerabilities* found using an attack module are also displayed in the **Issues** section of the *Scan status* page.



Reporting

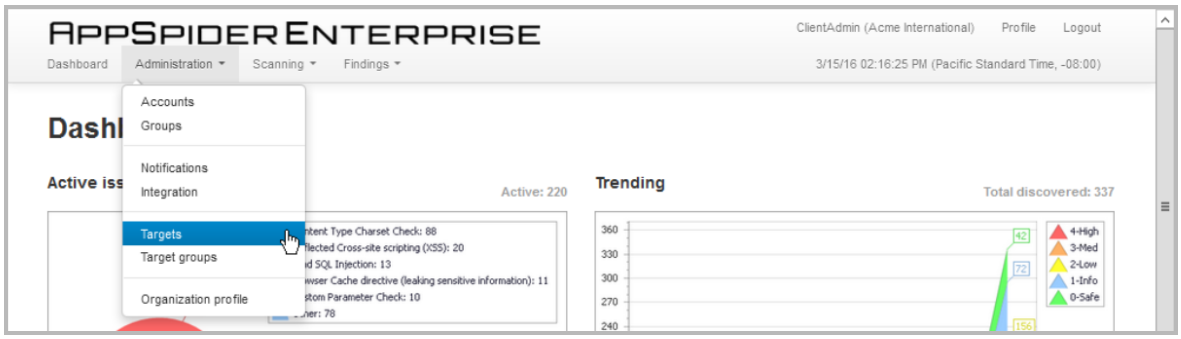
AppSpider provides interactive, actionable reports that behave like web pages with structure and links for deeper analysis. System and client administrators have full access to reports for all clients. Approved individual users, can view the reports for their client as well.

Approve Accounts

Due to target restrictions, individual user accounts cannot access the scan information of a target until they are approved by a client administrator.

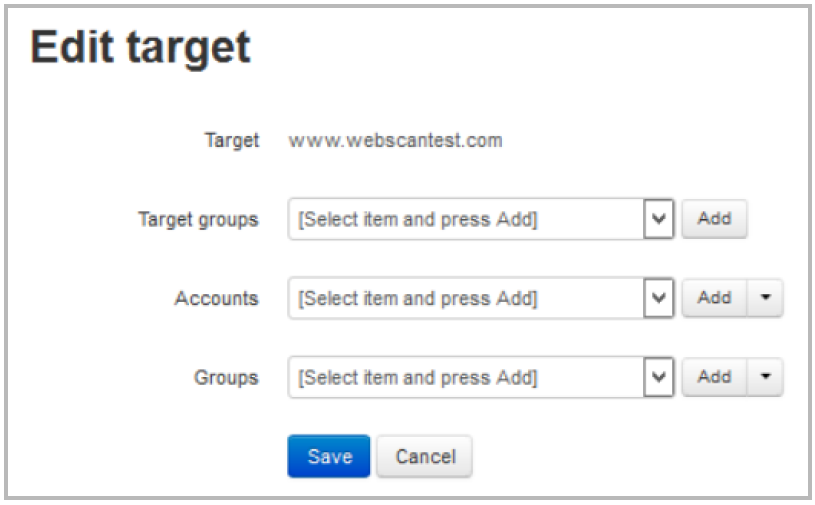
To approve an account for a target:

1. Login as client administrator.
2. Select the **Administrator** drop down menu.
3. Select **Targets**.

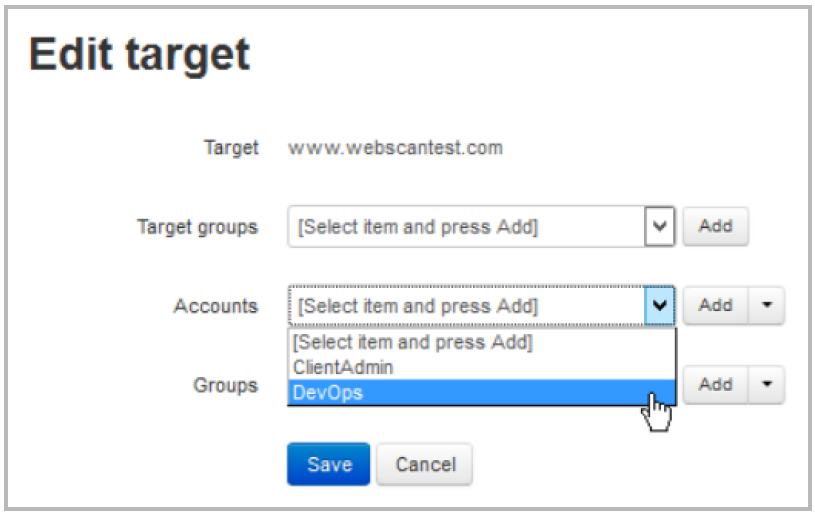


4. Select the checkbox for the target that you want to make changes to.
5. Click the **Edit** button to continue.

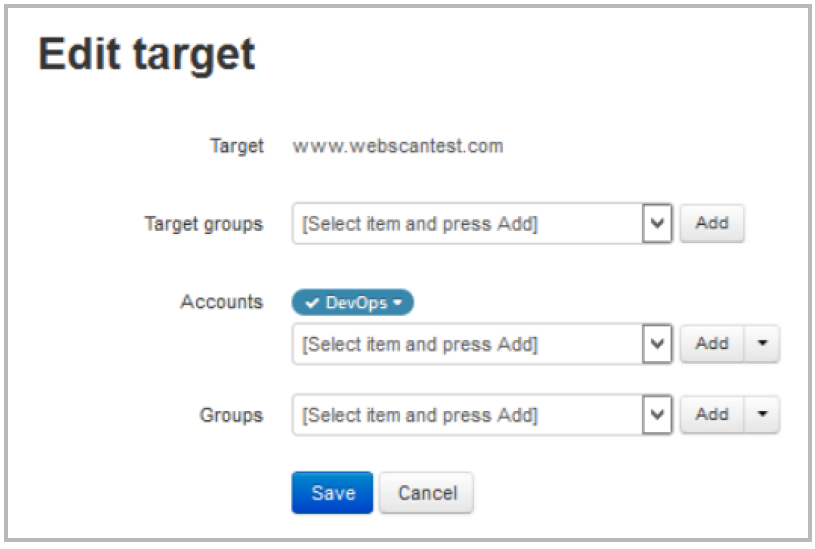
The *Edit target* page will allow you to add **Target groups**, **Accounts**, and **Groups** to the specified **Target**.



6. Locate and select the approved account from the *Accounts* drop down menu and click on the **Add** button. Repeat this step to approve additional accounts for the target.



7. When you are finished, click the **Save** button.

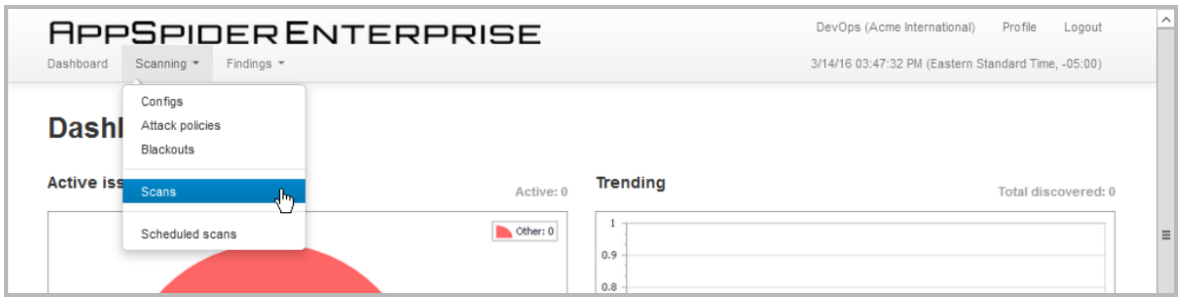


Upon saving, approved accounts can login and access scan information from the reports.

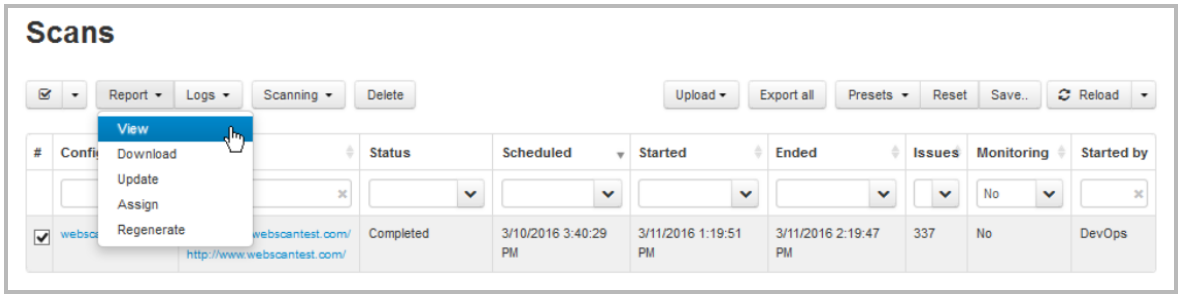
View Report

To view a report:

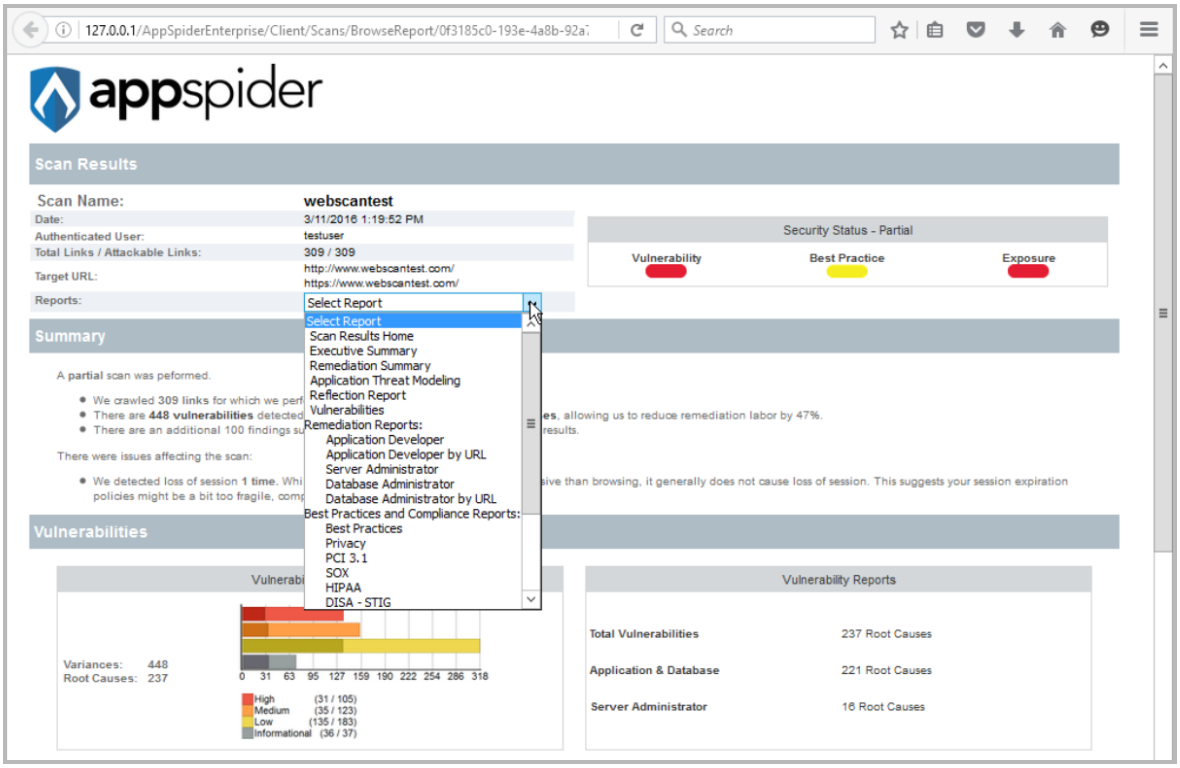
1. Select the **Scanning** drop down menu.
2. Select **Scans**.



3. Select the checkbox for the scan report that you want to view.
4. Select the **Report** drop down menu on the *View* page.
5. Click **View** to continue.



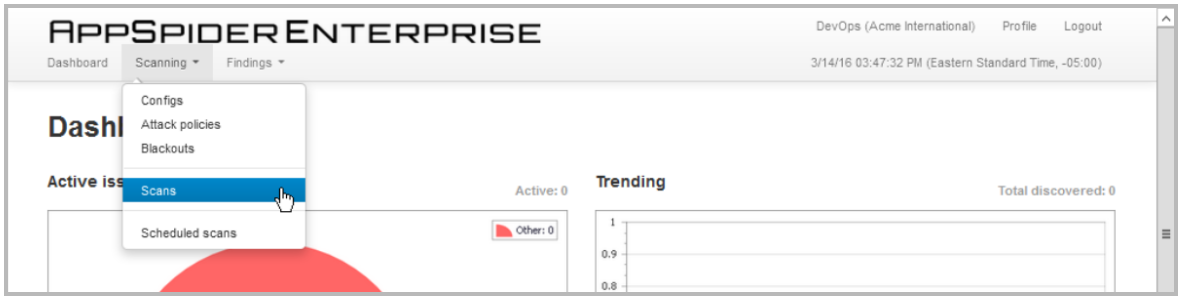
An HTML report will open in your browser.



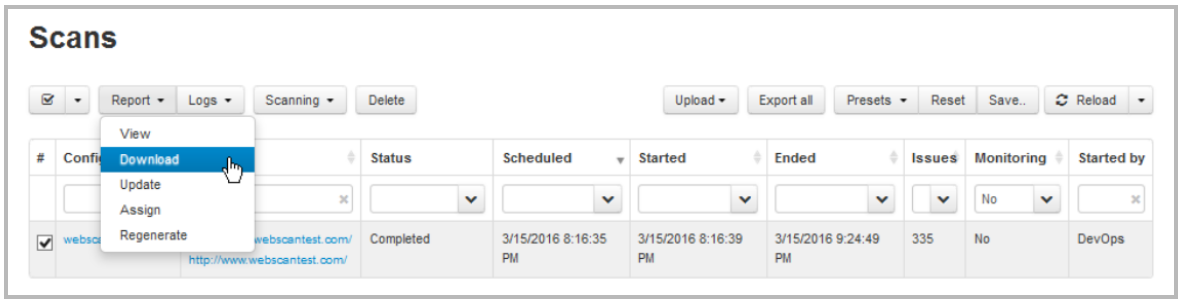
Download Report

To download a report:

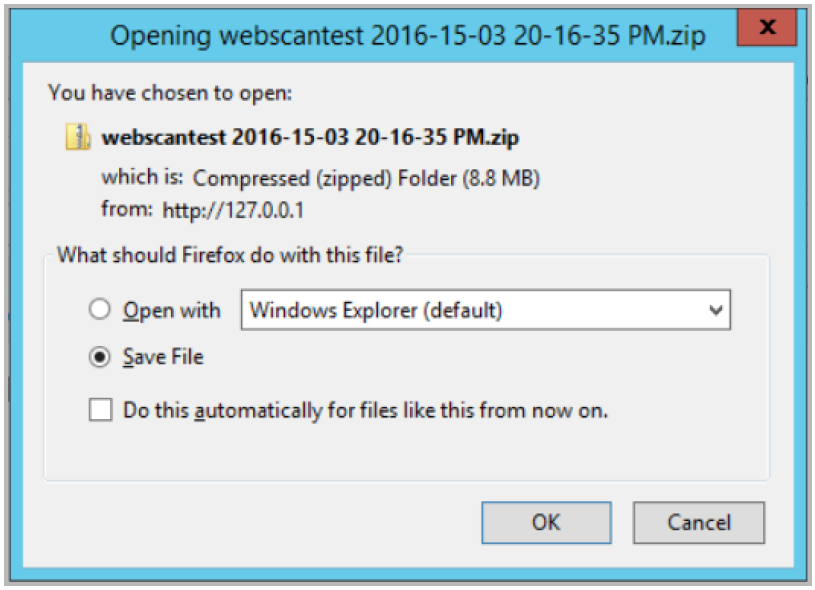
1. Select the **Scanning** drop down menu.
2. Select **Scans**.



3. Select the checkbox for the scan report that you want to download.
4. Select the **Report** drop down menu on the *View* page.
5. Click **Download** to continue.



6. Download the zip file, with your report, to your local hard drive



Getting started scanning your own web applications

Now that you have practiced using AppSpider Enterprise on Webscantest, you can prepare to scan your own applications. The following four items are essential to many deployments:

1. Target URL: You will need the exact location for the application to be scanned.
2. Credentials: For a more thorough scan, it is recommended to scan your web applications both logged in and out.
3. A proxy (if one exists in your environment): AppSpider will automatically note whether scanning your application requires a proxy. It is a good idea to note which one it is using and make sure the scan results accurately reflect your organization's infrastructure.
4. A decision on scan policies: Decide which types of vulnerabilities to scan for and whether to change any from the default settings. Each application is unique. Therefore, the settings might vary from web application to web application within your organization.

As you proceed with your scans, review the AppSpider Enterprise User's Guide for more details on the available options.