



AppSpider Enterprise

Getting Started Guide

Contents

Contents	2
About AppSpider Enterprise	4
Getting Started (System Administrator)	5
Login	5
Client	6
Add Client	7
Cloud Engines	8
Scanner Groups	8
Account	8
Add account	9
Permissions	10
Target	10
Add Target	11
Getting Started (Client Administrator)	12
Login	12
Account	13
Add account	14
Permissions	15
Getting Started (Individual User)	16
Login	16
Configure	17
Add config	18
General Settings	19
Scanning	20

Monitoring	20
Authentication	20
Scanning	21
Notifications	21
Large applications	21
Run A Scan	22
Scan Scheduling	23
Schedule scan	24
Scan Status	24
Reporting	26
Approve Accounts	26
View Report	28
Download Report	30
Getting started scanning your own web applications	31

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

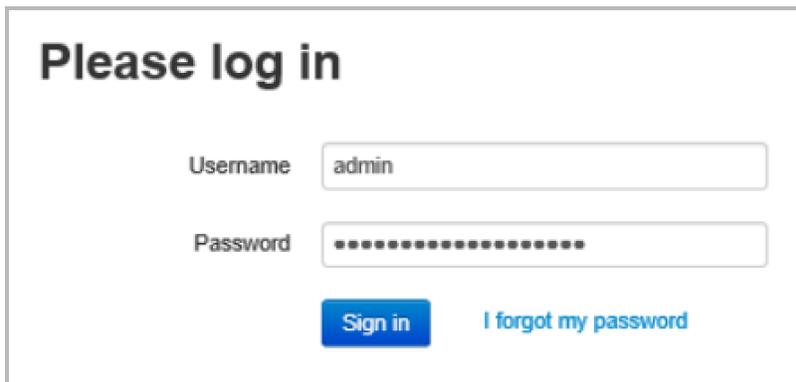
Tip: In order to run AppSpider Enterprise, a SQL Server Database as well as an AppSpider Pro scan engine must be configured. For installation and setup information, see the [AppSpider Enterprise Installation Guide](#).

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/



Please log in

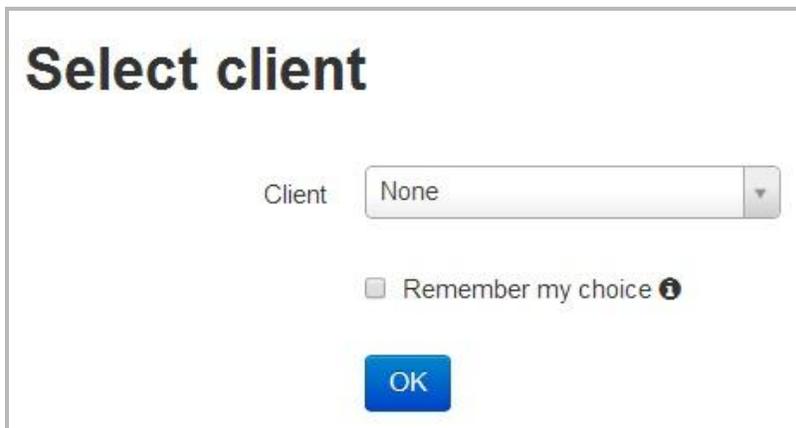
Username

Password

[Sign in](#) [I forgot my password](#)

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**.



Select client

Client

Remember my choice ⓘ

[OK](#)

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**.

The screenshot shows the AppSpider Enterprise Dashboard. At the top, there is a navigation bar with the user name 'admin', 'Change client', 'Profile', and 'Logout'. Below this is a secondary navigation bar with 'Dashboard', 'System', 'Administration', 'Scanning', and 'Findings'. The main content area is titled 'Dashboard' and contains four summary cards: 'Last events' (with a link to 'All events'), 'Last scans' (with a link to 'All scans'), 'Clients' (Total: 0), 'Users' (Accounts: 0, Accounts disabled: 0, Groups: 0, Sysadmins: 1), 'Engines' (Static engines: 1, Engine groups: 0), and 'Targets' (Pending targets: 0, Total targets: 0).

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**.

The screenshot shows the AppSpider Enterprise Dashboard with the 'System' dropdown menu open. The menu items are: 'Clients', 'System admins (SA)', 'Engines (SA)', 'Engine groups (SA)', 'System events (SA)', and 'Attack modules (SA)'. A mouse cursor is pointing at the 'Clients' option. The dashboard content behind the menu is partially visible, showing 'Dashl' and 'Last ever'.

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

Clients						
<input type="checkbox"/> Add		See targets	Edit	Delete	<input type="button" value="Reload"/>	
#	Client name	Contact email	Engine groups	CloudEngines	All engines	
	<input type="text"/>					
<input type="checkbox"/>				No	Yes	

Add Client

Add client

Account details

Client name

Max. scans per IP

Notes

Time zone

Cloud Engines

Enabled

Customer ID

Passcode

Scanner groups

Allow using any available scanner

Allowed scanner groups +

Contacts

Email

Address

Phone

Mobile

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**.

The screenshot shows the AppSpider Enterprise dashboard. At the top, there is a navigation bar with the following items: Dashboard, System, Administration, Scanning, Findings, admin, Change client, Profile, Logout. The date and time are 3/11/16 08:52:23 PM (UTC). The main content area is titled 'Dashboard' and contains sections for 'Last events' and 'Last scans'. A dropdown menu is open under 'Administration', showing 'All accounts', 'All groups (SA)', and 'All targets (SA)'. A mouse cursor is pointing at 'All accounts'.

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

The screenshot shows the 'All accounts' page. At the top, there is a toolbar with buttons: Add, Edit, See targets, Reset password, Enabled status, Unlock, Delete, Presets, Reset, Save.., Reload. Below the toolbar is a table with the following columns: #, Username, Email, Client, Effective roles, Enabled, Locked. The table is empty, and a message at the bottom says 'No data available in table'.

Add account

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

The screenshot shows the 'Add account' form. The form is titled 'Add account' and has a section for 'Account details'. The fields are as follows:

- Client: Acme International (dropdown)
- Login: ClientAdmin
- Email: admin@acme.com
- Password: [Redacted] (password field) with a 'Random' button
- First name: Client
- Last name: Admin
- Enabled:
- Time zone: (UTC-08:00) Pacific Time (US & Canada) (dropdown)
- Change password at logon:

Permissions

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

Permissions

Groups No groups in the client.

Roles		
All	Blackout manager	<input checked="" type="checkbox"/> grant
None	Blackout viewer	<input checked="" type="checkbox"/> grant
	Client admin	<input checked="" type="checkbox"/> grant
	Config manager	<input checked="" type="checkbox"/> grant
	Report assigner	<input checked="" type="checkbox"/> grant
	Report manager	<input checked="" type="checkbox"/> grant
	Report reviewer	<input checked="" type="checkbox"/> grant
	Report viewer	<input checked="" type="checkbox"/> grant
	Scan runner	<input checked="" type="checkbox"/> grant
	Issues manager	<input checked="" type="checkbox"/> grant
	Issues viewer	<input checked="" type="checkbox"/> grant
	WAF manager	<input checked="" type="checkbox"/> grant

Target

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

To add a target:

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



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

All targets			
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	No

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.

Add target

Target

Clients

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.

Add target

Target

Clients

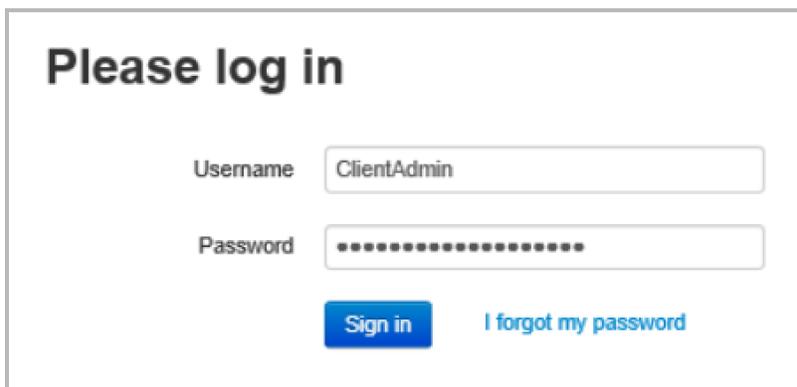
3. When you are finished, click the **Save** button.

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/>



Please log in

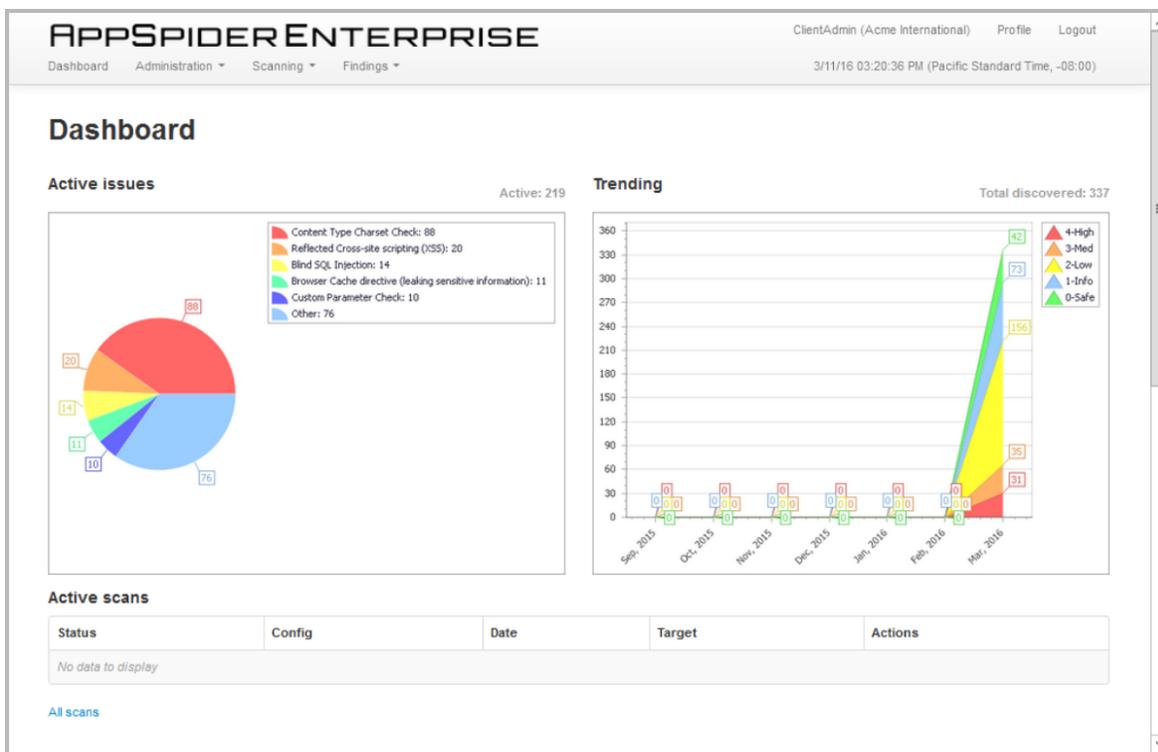
Username

Password

[Sign in](#) [I forgot my password](#)

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.

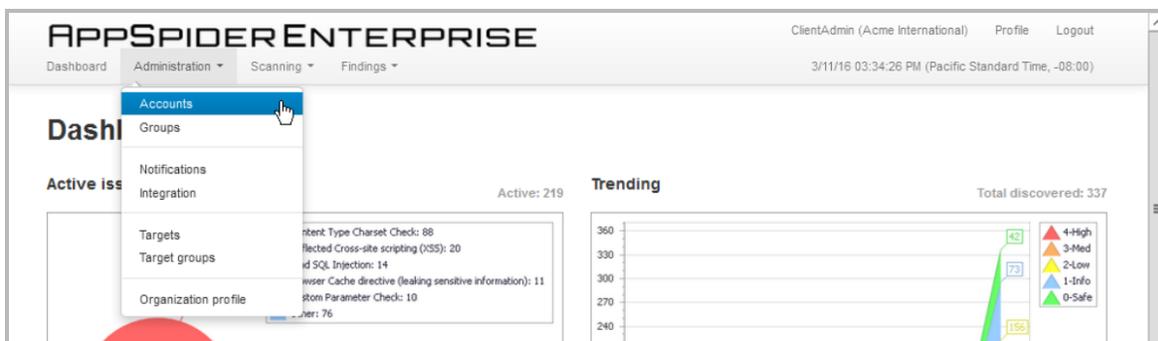


Account

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.

Accounts

#	Username	Email	Groups	Effective roles	Enabled	Locked
<input type="checkbox"/>	ClientAdmin	admin@acme.com		Blackout manager, Blackout viewer, Client admin, Config manager, Report assigner, Report manager, Report reviewer, Report viewer, Scan runner, Issues manager, Issues viewer, WAF manager	Yes	No

Add account

Add account

Account details

Login
 Email
 Password
 First name
 Last name
 Enabled
 Time zone
 Change password at logon

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

Permissions

Permissions

Groups No groups in the client.

Roles

- All
- None

Blackout manager	<input checked="" type="checkbox"/> grant
Blackout viewer	<input checked="" type="checkbox"/> grant
Client admin	<input type="checkbox"/> grant
Config manager	<input checked="" type="checkbox"/> grant
Report assigner	<input checked="" type="checkbox"/> grant
Report manager	<input checked="" type="checkbox"/> grant
Report reviewer	<input checked="" type="checkbox"/> grant
Report viewer	<input checked="" type="checkbox"/> grant
Scan runner	<input checked="" type="checkbox"/> grant
Issues manager	<input checked="" type="checkbox"/> grant
Issues viewer	<input checked="" type="checkbox"/> grant
WAF manager	<input checked="" type="checkbox"/> grant

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

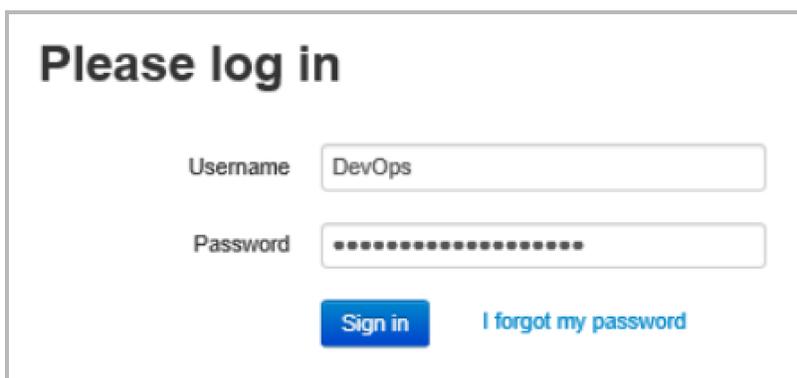
Tip: Client administrators can create several accounts. Repeat these steps to add additional user accounts to the client.

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/



Please log in

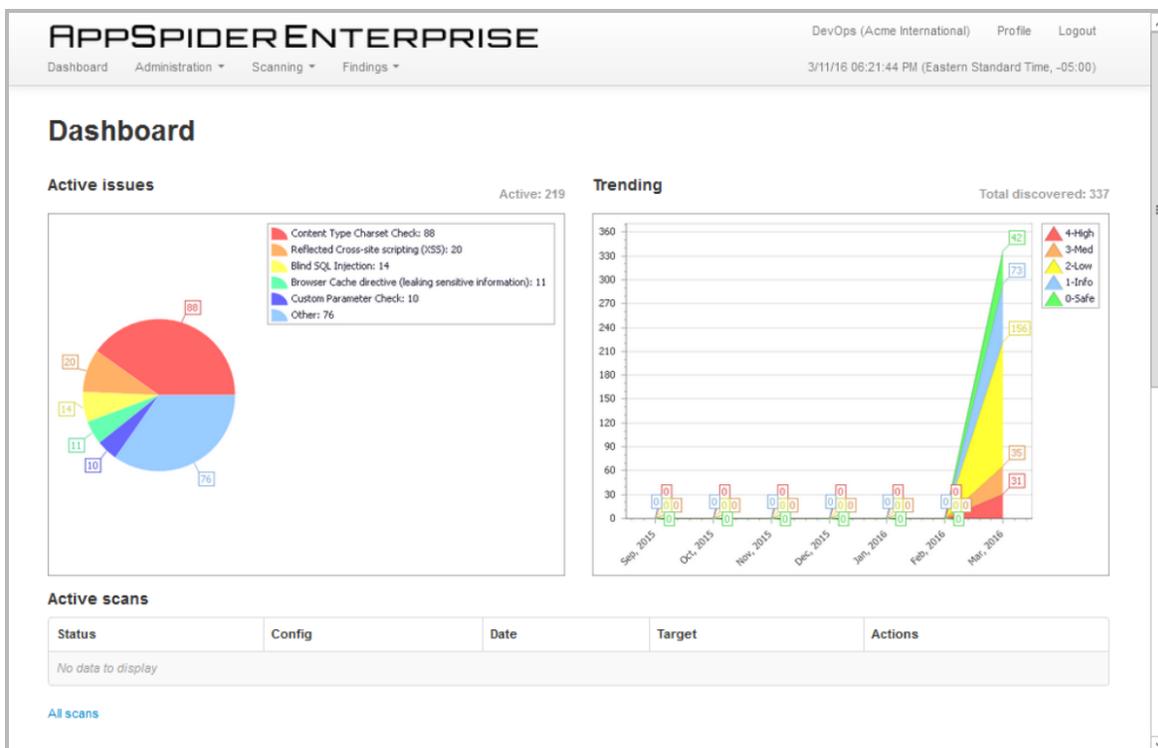
Username

Password

[Sign in](#) [I forgot my password](#)

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.



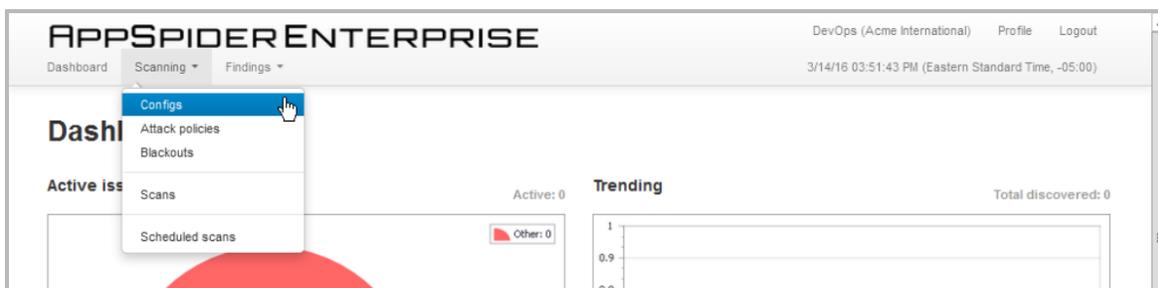
Configure

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.

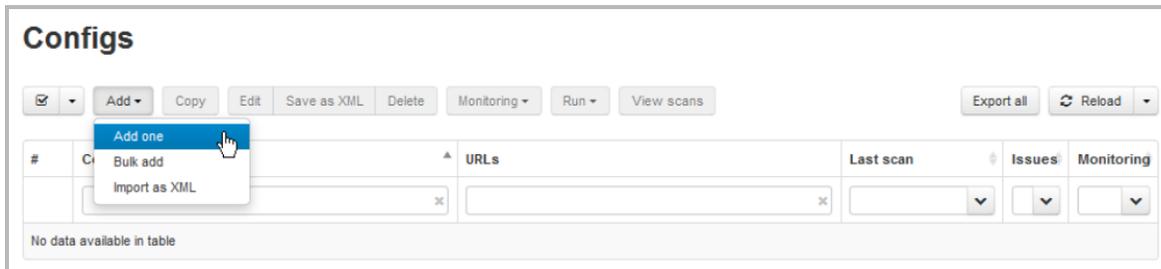
AppSpider gives you the ability to configure many aspects of the scan and gives you more visibility into what exactly is happening behind the scenes.

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.

Add config

General

Crawling

Attacks

Authentication

Proxy

HTTP Headers

Web services

Performance

Advanced options

General

Name

Scanning

URLs +

Scan engine Any available
 Use selected group

▾

Monitoring

Enabled

Save Cancel

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.

Add config

General

Crawling

Attacks

Authentication

Proxy

HTTP Headers

Web services

Performance

Advanced options

General

Name

Scanning

URLs +

Scan engine Any available
 Use selected group

Monitoring

Enabled

Save Cancel

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.

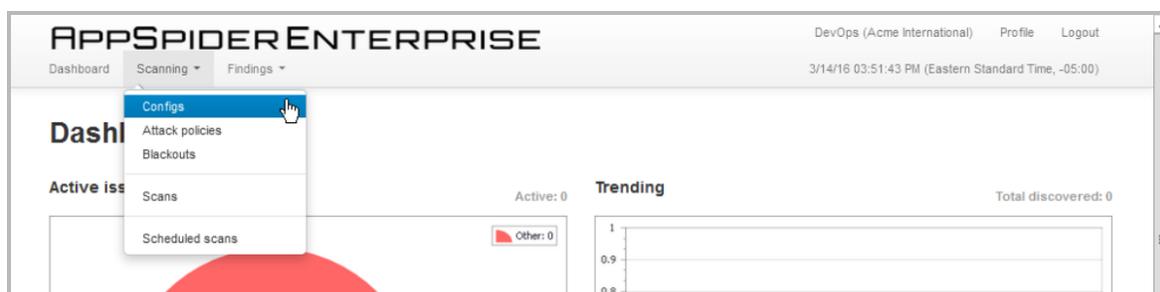
Tip: The best practice for scanning larger targets is to segment the assessment into separate scan configurations for subdomains or subdirectories.

Run A Scan

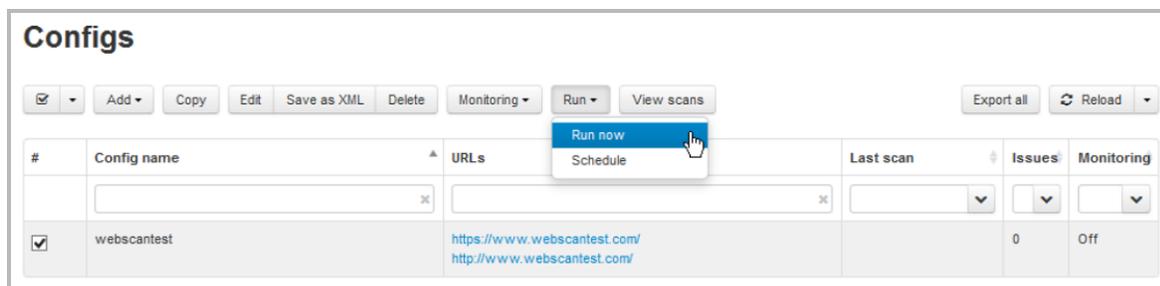
If an immediate scan is necessary, you can launch a scan at any time with AppSpider Enterprise.

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.

APPSPIDER ENTERPRISE

DevOps (Acme International) Profile Logout

Dashboard Administration Scanning Findings

3/10/16 06:40:30 PM (Eastern Standard Time, -05:00)

Success
Scan was successfully started (webscantest).

Configs

Add Copy Edit Save as XML Delete Monitoring Run View scans
 Export all Reload

#	Config name	URLs	Last scan	Issues	Monitoring
<input checked="" type="checkbox"/>	webscantest	https://www.webscantest.com/ http://www.webscantest.com/		0	Off

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**.

APPSPIDER ENTERPRISE

DevOps (Acme International) Profile Logout

Dashboard Scanning Findings

3/14/16 03:51:43 PM (Eastern Standard Time, -05:00)

Configs
 Attack policies
 Blackouts
 Scans
 Scheduled scans

Active issues: 0

Trending

Total discovered: 0

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.

The screenshot shows the 'Configs' management interface. At the top, there are buttons for 'Add', 'Copy', 'Edit', 'Save as XML', 'Delete', 'Monitoring', 'Run', and 'View scans'. A dropdown menu is open under 'Run', with 'Schedule' highlighted. Below this is a table with columns: '#', 'Config name', 'URLs', 'Last scan', 'Issues', and 'Monitoring'. One config is listed: 'webscantest' with two URLs: 'https://www.webscantest.com/' and 'http://www.webscantest.com/'.

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.

The 'Schedule scan' form contains the following fields and options:

- Config:** A dropdown menu showing 'webscantest'.
- Start date/time:** A date and time picker set to '03/13/2016 12:00:00 AM'.
- Forced stop date/time:** An empty date and time picker.
- Recurring:** A checked checkbox.
- Recurrence:**
 - Daily
 - Weekly: Day 1 of every 1 month(s)
 - Monthly: The Second Sunday of every 1 month(s)
 - Yearly
 - No end date
 - End after: 1 occurrences
 - End by: 1/1/2021
- Buttons:** 'Save' and 'Cancel'.

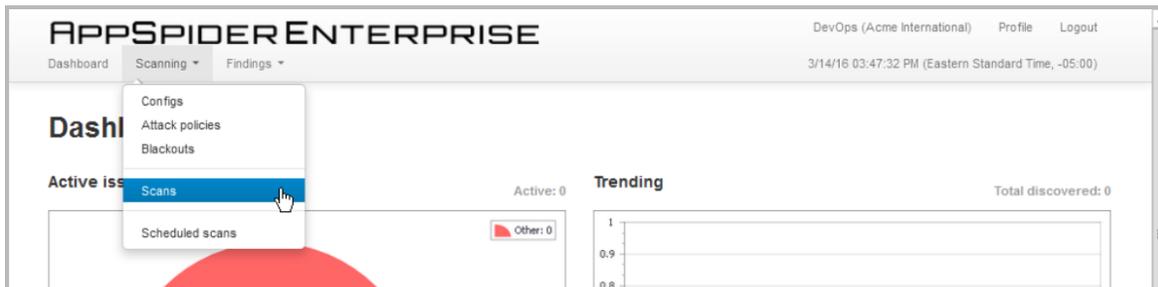
Once your schedule is saved, your scan(s) will be performed as you defined.

Scan Status

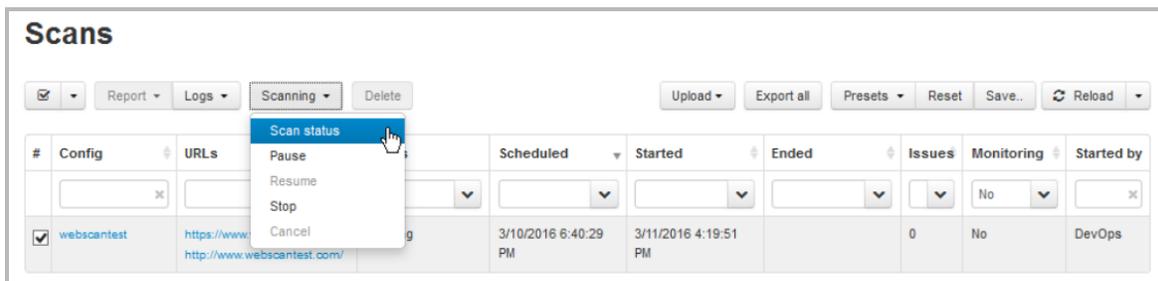
You can view the progress of your scans as soon as they are started.

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.

Scan status

← Back || Pause ■ Stop ↻ Refresh (auto) ▾

General	Crawling	Attacks	Network
Config name: webscantest	Links in queue: 2	In queue: 14257	Requests: 20456
Scan status: Running	Crawled links: 278	Attempted: 60669	Failed requests: 9
Start time: 3/11/16 04:19:51 PM	Logged in: Yes	Vulnerable: 253	Network speed: 24055
Elapsed/left: 00:18:22 / 00:29:13			
Scan progress: 50%			

Issues

Issue	Attempted	Vulnerable
Apache Struts 2 Framework Checks	18	0
Apache Struts Detection	262	0
Arbitrary File Upload	0	0
ASP.NET Misconfiguration	18	0
ASP.NET ViewState security	508	0
Autocomplete attribute	786	0
Blind SQL	1222	11
Browser Cache directive (leaking sensitive information)	311	11

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**.

APPSPIDER ENTERPRISE

ClientAdmin (Acme International) Profile Logout

Dashboard Administration Scanning Findings

3/15/16 02:16:25 PM (Pacific Standard Time, -08:00)

Active issues: 220

Trending

Total discovered: 337

Accounts
Groups
Notifications
Integration
Targets
Target groups
Organization profile

Content Type Charset Check: 88
Reflected Cross-site scripting (XSS): 20
Blind SQL Injection: 13
Browser Cache directive (leaking sensitive information): 11
HTTP Response Splitting: 10
Remote Parameter Check: 10
Server Side Request Forgery: 78

4-High
3-Med
2-Low
1-Info
0-Safe

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

Targets

✉ Edit Accounts Groups Reload

#	Target	Accounts	Groups	Pending
<input checked="" type="checkbox"/>	www.webscantest.com			No

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

Edit target

Target www.webscantest.com

Target groups [Select item and press Add] Add

Accounts [Select item and press Add] Add

Groups [Select item and press Add] Add

Save Cancel

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.

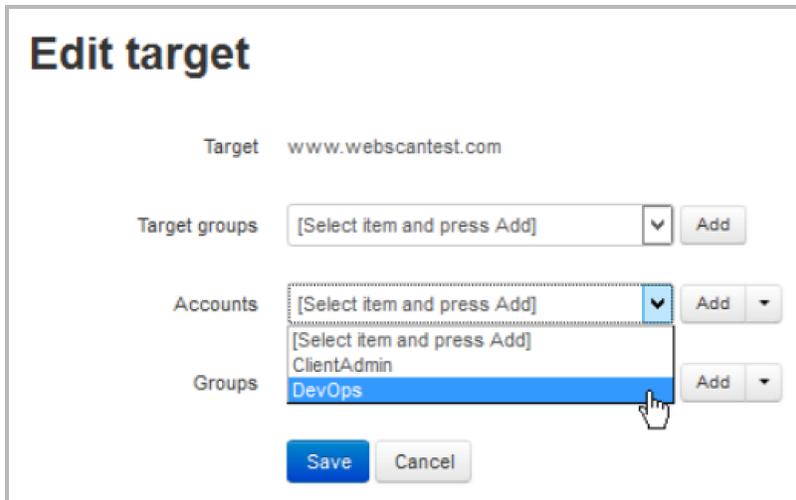
Edit target

Target `www.webscantest.com`

Target groups

Accounts

Groups



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

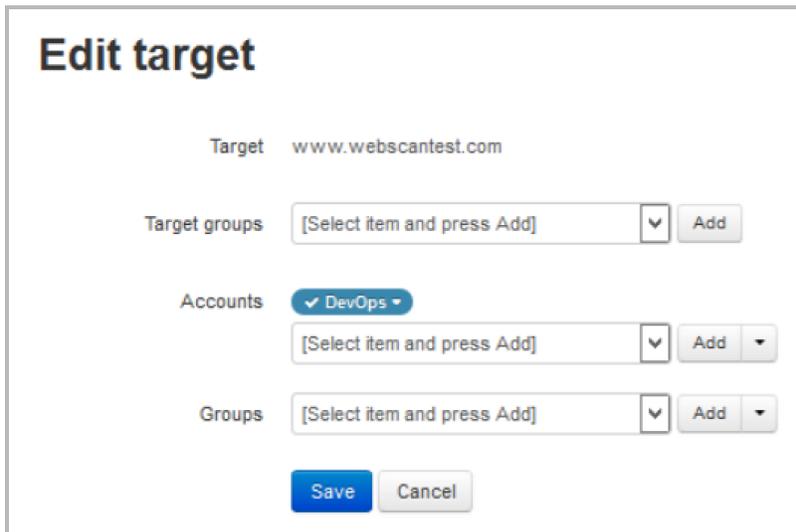
Edit target

Target `www.webscantest.com`

Target groups

Accounts

Groups

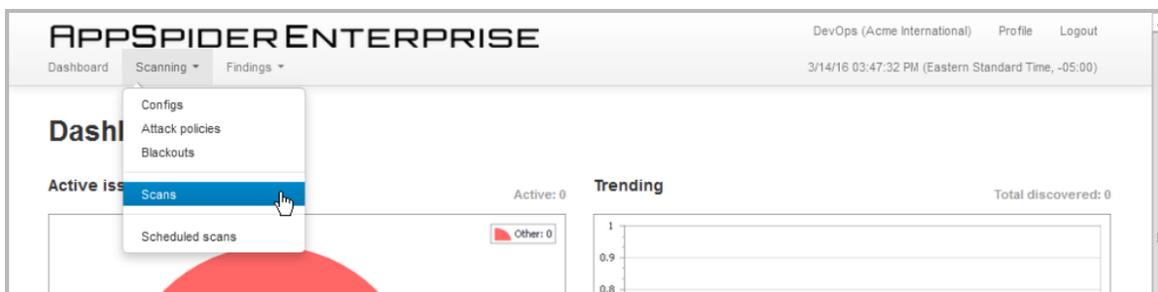


Upon saving, approved accounts can login and access scan information from the reports.

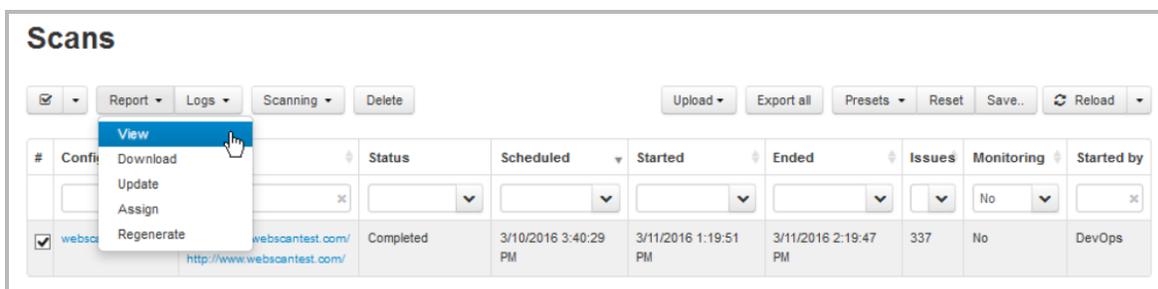
View Report

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.

Scan Results

Scan Name: webscantest

Date: 3/11/2016 1:19:52 PM

Authenticated User: testuser

Total Links / Attackable Links: 309 / 309

Target URL: http://www.webscantest.com/
https://www.webscantest.com/

Reports: Select Report

Summary

A partial scan was performed.

- We crawled 309 links for which we performed a scan.
- There are **448 vulnerabilities** detected.
- There are an additional 100 findings such as session expiration.

There were issues affecting the scan:

- We detected loss of session 1 time. While this is not a critical issue, it suggests your session expiration policies might be a bit too fragile, compared to other applications.

Vulnerabilities

Vulnerability Bar Chart

Variations: 448
Root Causes: 237

Severity	Count	Total
High	31	105
Medium	35	123
Low	135	183
Informational	36	37

Security Status - Partial

Vulnerability: ■ Best Practice: ■ Exposure: ■

Vulnerability Reports

Total Vulnerabilities	237 Root Causes
Application & Database	221 Root Causes
Server Administrator	16 Root Causes

Download Report

To download a report:

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

APPSPIDER ENTERPRISE

DevOps (Acme International) Profile Logout

3/14/16 03:47:32 PM (Eastern Standard Time, -05:00)

Dashboard Scanning Findings

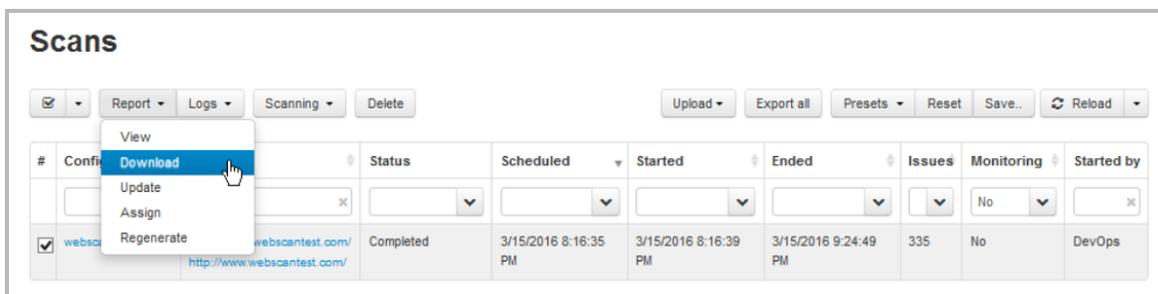
Scans (highlighted)

Active issues: 0

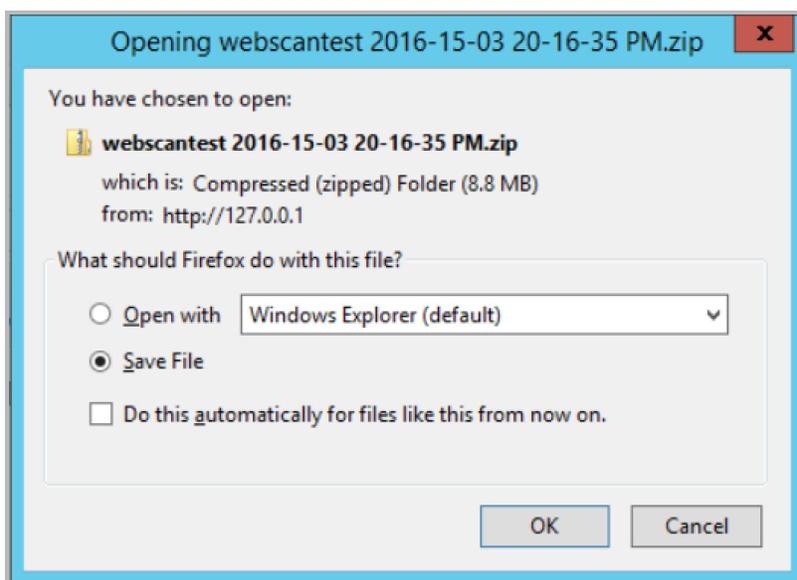
Trending

Total discovered: 0

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.