IBM Security AppScan Standard
Version 9.0.3.11

Getting Started Guide

Contents

Chapter 1. Installing

System requirements

A summary of the minimum hardware and software required to run AppScan® Standard.

Important: A more complete list, which may include updates added after the product was released, can be found online at: http://www.ibm.com/support/docview.wss?uid=swg27024155

Hardware requirements

Hardware	Minimum Requirement
Processor	Core 2 Duo 2 GHz (or equivalent)
Memory	4 GB RAM
Disk Space	30 GB
Network	1 NIC 100 Mbps for network communication with configured TCP/IP

Operating system and software requirements

Software	Details
Operating System	Supported operating systems: • Microsoft Windows Server 2016: Standard and Datacenter • Microsoft Windows Server 2012: Essentials, Standard and Datacenter • Microsoft Windows Server 2012 R2: Essentials, Standard and Datacenter • Microsoft Windows Server 2008 R2: Standard and Enterprise, with or without SP1 • Microsoft Windows 10: Pro and Enterprise • Microsoft Windows 8.1: Pro and Enterprise • Microsoft Windows 8: Standard, Pro and Enterprise • Microsoft Windows 7: Enterprise, Professional and Ultimate, with or without SP1 **Note:** Both 32-bit and 64-bit editions are supported, but 64-bit is preferred.
Browser	Microsoft Internet Explorer 11 Recommended: Internet Explorer Version 11.0.9600.18537, Update Versions 11.0.38 KB3203621
Other	Microsoft .NET Framework 4.6.2 If using floating or token licenses: Rational® License Key Server 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5 (Optional) Adobe Flash Player for Internet Explorer is required for Flash execution (and for viewing instructional videos in some of the advisories). Versions 9.0.124.0 up to 14.0.0.125 are supported. Earlier versions are not supported, and some versions may require configuration. (Optional) Microsoft Word 2007, 2010, 2013 for custom report templates.

Important: Customers without a local license on their machine require a network connection to their licensing server when using AppScan.

Important: A personal firewall running on the same computer as AppScan can block communication and result in inaccurate findings and reduced performance. For best results do not run a personal firewall on the computer that runs AppScan.

Glass box server requirements

The glass box scanning feature requires a glass box agent to be installed on the application server. For more details, refer to the Online Help, or the Glass Box User Guides found in the main glass box folder that is located by default at:

```
C:\Program Files (x86)\IBM\AppScan Standard\Glass box
```

Java platforms: On Java platforms the following server platforms and technologies are supported.

Software	Details
Operating System	Supported Microsoft Windows systems (both 32-bit and 64-bit editions): • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 SP2 • Microsoft Windows Server 2008 R2 Supported Linux systems: • Linux RHEL 5, 6, 6.1, 6.2, 6.3, 6.4 • Linux SLES 10 SP4, 11 SP2 Supported UNIX systems: • UNIX AIX® 6.1, 7.1 • UNIX Solaris (SPARC) 10, 11
Java™ EE container	JBoss AS 6, 7; JBoss EAP 6.1; Tomcat 6.0, 7.0; WebLogic 10, 11, 12; WebSphere 7.0, 8.0, 8.5, 8.5.5

.NET platforms: On .NET platforms the following systems and technologies are supported:

Item	Details
Operating System	Supported operating systems (both 32-bit and 64-bit editions): • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 SP2 • Microsoft Windows Server 2008 R2
Other	Microsoft IIS 7.0 or later Microsoft .NET Framework 4.0 or 4.5 must be installed, and IIS must be configured at the root level to work with this version of ASP.net

Note: User must have administrator privileges when running the application on the server.

Note: The agent should be installed *after* the application you want to test is successfully installed on the server.

Install

The installation wizard guides you through the fast and simple process.

Procedure

1. Close any Microsoft Office applications that are open.
2. Start IBM Security AppScan Standard setup.

   The InstallShield Wizard starts, and checks that your workstation meets the minimum installation requirements. Then the AppScan installation wizard welcome screen appears.
3. Follow the wizard instructions to complete AppScan installation.

   Note: You will be asked if you want to install or download GSC (Generic Service Client). This is needed for exploring Web Services in order to configure a Web Services scan, but not if you are not scanning web services.

Silent install

Instructions for unattended, installation, using the command line.

You can install AppScan "silently", using the command line and the following parameters:

```
AppScan_Setup.exe /l"LanguageCode" /s /v"/qn INSTALLDIR=\"InstallPath\""
```

Important: If you wish to install Generic Service Client (required for scanning Web services, but not for scanning only web applications) at the same time as you install Rational AppScan, you must run the command line from the folder that contains both the setup (.exe) files.

Parameter	Function
/l	Language code. Options are: • English: **1033** • Chinese (Traditional): **1028** • Chinese (Simplified): **2052** • French: **1036** • German: **1031** • Italian: **1040** • Japanese: **1041** • Korean: **1042** • Portuguese: **1033** • Spanish: **1034**
/s	Activates "Silent Mode" (otherwise the regular installation will be launched). **Note:** Must be used in conjunction with /v"/qn" (see next row)
/v	Sets additional MSI properties such as UI mode and the path where AppScan will be installed. **UI Mode:** For "Silent Mode", include `/qn` as a parameter (enclosed in quotes). **Path:** To define a different install path, add `INSTALLDIR=\"InstallPath\"` as a parameter (enclosed in quotes). The path may include spaces. Example: `/v"/qn INSTALLDIR=\"D:\Program Files\AppScan\""`

Examples:

- To silently install an English version of AppScan in the default directory enter:
  `AppScan_Setup.exe /s /v"/qn"`
- To silently install Japanese versions of AppScan in the default directory enter:
  `AppScan_Setup.exe /l"1041" /s /v"/qn"`
- To silently install a Korean version of AppScan in D:\Program Files\AppScan\ enter:
  `AppScan_Setup.exe /l"1042" /s /v"/qn INSTALLDIR=\"D:\Program Files\AppScan\""`

License

A description of license types, installation and management.

The AppScan Standard installation includes a default license that allows you to scan IBM's custom designed AppScan testing website (demo.testfire.net), but no other sites. In order to scan your own site you must install a valid license supplied by IBM®. Until this is done AppScan will load and save scans and scan templates, but it will not run new scans on your site.

AppScan licenses

There are three types of license:

"Node-locked" licenses
These are installed locally onto the machine on which AppScan runs. Each license is assigned to a single machine.

"Floating" licenses
These are installed onto the IBM Rational License Key Server (which can be the same as the machine on which AppScan runs). Any server on which AppScan is used must have a network connection with the license key server. Each time a user opens AppScan a licence is checked out, and when AppScan is closed the license is checked back in.

"Token" licenses
These are installed onto the IBM Rational License Key Server (which can be the same as the machine on which AppScan runs). Any server on which AppScan is used must have a network connection with the license key server. Each time a user opens AppScan the required number of tokens are checked out, and when AppScan is closed they are checked back in.

License status

To view license status:

- Click **Help > License**. The License dialog box opens, showing license status and the following options:

Open AppScan Standard License Manager	Opens the list of currently loaded licenses, and lets you: • Add or remove node-locked licenses • Set the license key server(s) for floating or token licenses
Add AppScan Enterprise License	If your organization has an AppScan Enterprise license that allows scanning additional sites to those allowed by your local AppScan Standard license, you can import these permissions to use on your local machine in addition to your existing license. **Note:** This option is available only when a full AppScan Standard license (not a demo license) is loaded.
View License Agreement	Click here to see the license agreement.

Note: You can refresh the license information displayed in the dialog box by clicking 

Note: If a floating or token license has been verified, but the license key server later becomes unavailable, AppScan can run in "Disconnected Mode" for up to three days. During this time you can scan your application as usual.

Test-run

You can "test-run" AppScan Standard by scanning the "AltoroMutual Bank" website, which has been created for demonstration purposes. Use the following URL and login credentials:

URL	https://demo.testfire.net/
Username	jsmith
Password	demo1234

Note: If you are using an evaluation copy of AppScan, the AltoroMutual Bank website is the *only* site you can scan.

See also “Sample scans” on page 10.

Chapter 2. Basic principles

Scan stages and scan phases

An AppScan Full Scan consists of two (main) stages: Explore and Test. It is useful to understand the principal behind this, even though most of the scan process is in fact seamless to the user, and little user input is required until the scan is complete.

- **Explore stage:** During the first stage, the site is explored and an application tree is constructed. This is the Explore stage. AppScan analyzes the responses to each request it sends, looking for any indication of a potential vulnerability. When AppScan receives responses that may indicate security vulnerability, it automatically creates tests, as well as noting the validation rules needed to determine which results constitute vulnerability, and the level of security risk involved.
- **Test stage:** During the Test stage, AppScan sends thousands of custom test requests that it created during the Explore stage. It records and analyzes the application's response to identify security problems and rank their level of security risk.
- **Scan phases:** In practice, the Test stage frequently reveals new links within a site, and more potential security risks. Therefore, after completing the first "phase" of Explore and Test, AppScan automatically begins a new "phase" to deal with the new information. (The default number of phases is four.)

Web applications vs. web services

A site is scanned by first exploring it, and then, based on the Explore stage responses, testing it. There are different ways of gathering this "Explore data". In all cases, once the data is gathered AppScan is used to send tests to the site.

Exploring web applications (sites with a user interface)

- In the case of applications (sites) without web services it is often sufficient to supply AppScan with the start URL and login authentication credentials for it to be able to test the site.
- If necessary you can manually explore the site *through AppScan*, in order to get access to areas that can only be reached through specific user input.
- For pages that can be reached only by accessing pages in a specific order, you can record a multi-step operation for AppScan to use.
- While the Configuration Wizard lets you configure and start your scan in a few steps, for complex sites the Configuration Dialog Box lets you fine-tune and customize many more settings.

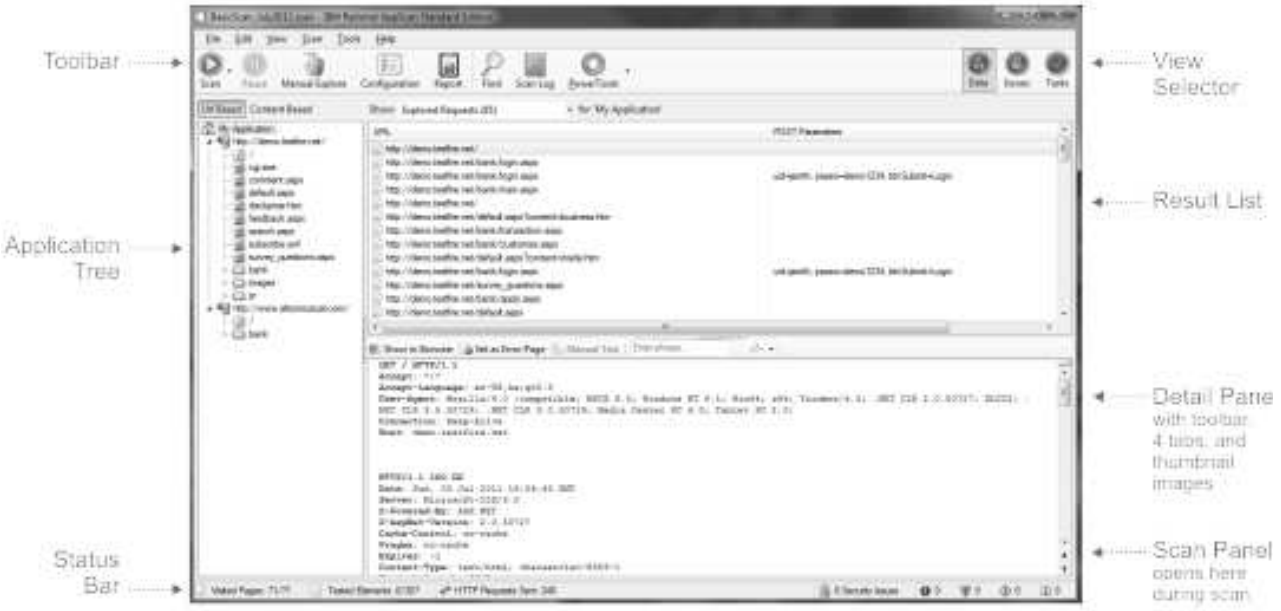
Exploring web services

- You can set up AppScan as a recording proxy for the device (such as a mobile phone or simulator) you use to explore the service. That way AppScan can analyze the Explore data collected, and send appropriate tests. You can also use AppScan to record traffic using external tool, such as a web services functional tester.
- If you have Open API description files (JSON or YAML) for your web service, you can use the Web Services Wizard extension to configure a scan, and the multi-step sequences needed to use the service. AppScan will then automatically scan the service.

- If you cannot use the first two methods, and have a WSDL file for your web service (such as a SOAP web service), the AppScan installation optionally includes a separate tool that lets users view the various methods incorporated in the web service, manipulate input data, and examine feedback from the service. You first need to give AppScan the URL of the service. The integrated "Generic Service Client" (GSC) uses the WSDL file to display the individual methods available in a tree format, and create a user-friendly GUI for sending requests to the service. You can use this interface to enter parameters and view the results. The process is "recorded" by AppScan and used to create tests for the service when AppScan scans the site. GSC can also be used as client for REST requests, without parsing a WSDL file, as a simple HTTP client.

Main window

The main screen contains a menu bar, toolbar, view selector, and three data panes: **Application tree**, **Result list** and **Detail pane**. The figure following shows the main screen populated with data following a scan.



View selector	Click one of the three buttons to select the type of data displayed in the three main panes.
Application tree	As the scan progresses the application tree is populated. By the end of the scan the tree shows all the folders, URLs and files that were found in your application.
Result list	Shows relevant results for the selected node in the application tree.
Detail pane	Shows relevant details for the selected node in the result list, in three tabs: Advisory, Fix Recommendation, and full Request/Response.

Workflow

This section describes a simple workflow using the Scan Configuration Wizard, most suited to new users, or users with a pre-configured scan template. More advanced users may prefer to configure their scan using the Scan Configuration dialog box, Explore some of the site manually (to show AppScan some typical user behavior), and then start the scan.

To scan using the wizard:

1. Select a scan template. (You can later adjust the configuration as required.)
2. Open the Scan Configuration wizard and select scan type:

Explore option	Description
AppScan (automatically or manually)	Select this option for most web application scans. The application is explored manually and/or automatically with requests sent from AppScan to the application.
External device/client (with AppScan as recording proxy)	Select this option to use AppScan as a recording proxy, and manually explore web services using a mobile phone, simulator, or emulator. AppScan displays the domains and requests in its External Traffic Recorder, and sends appropriate tests based on the input.
Generic Service Client (WSDL)	Select this option for web services with a WSDL file. Generic Service Client (GSC) uses your web service's WSDL file to display a simple interface showing the services available, and lets you input parameters and view the results. Use the GSC interface to explore your web service manually, so that AppScan can use your input to create appropriate tests. **Note:** If you did not install GSC when you installed AppScan, you will be prompted to do so when you select this option.

3. Follow the wizard steps to explore the application:

   AppScan:

   a. Type in the starting URL.
   b. (Recommended) Record the login procedure.
   c. (Optional) Review the Test Policy.

   External device:

   a. Configure AppScan as recording proxy.
   b. (If server uses HTTPS:) Install AppScan SSL certificate locally and on the device.
   c. Record the login procedure.
   d. (Optional) Review and edit the Test Policy.
   e. Send requests to the service from your device with AppScan as recording proxy.
   f. Edit the list of domains and requests to use for the Test stage.

   GSC:

   a. Type in the WSDL file location.
   b. (Optional) Review the Test Policy.
   c. Use Generic Service Client (which opens automatically) to send requests to the service while AppScan records your input and the responses received.

      Note: You must send at least one request to the service for AppScan to be able to test it.

4. (Optional, applications only) Run **Scan Expert**:

   a. Run Scan Expert to review the effectiveness of your configuration for the application being scanned.
   b. Review suggested configuration changes and apply selectively.

   Note: You can configure Scan Expert to perform its analysis and apply some of its recommendations *automatically*, when you start the scan.

5. Start Automatic Scan:
   - (Applications:) Full Automatic Scan (Explore and Test)
   - (Services:) Test only
6. Review Results to evaluate the security status of the site, and
   - Explore additional links manually
   - Print Reports
   - Review remediation tasks
   - Log defects to your defect tracking system

Sample scans

The sample scans can help give you a feel for using AppScan and what scan results look like.

Three sample scans are saved to your machine when AppScan is installed. You can open them to see how they are configured, and how the results are displayed in AppScan. They can be found in your main AppScan Standard folder, whose default location is:

```
C:\Program Files (x86)\IBM\AppScan Standard
```

The scans are:

demo.testfire.net.scan
This is a scan of the AppScan demonstration test site. You can review the configuration and results. You can also send additional requests to the site and continue the scan with the new data.

Glass_Box_DotNet_Demo.scan and Glass_Box_Java_Demo.scan
These two scans are examples of glass box scans using a .NET application server and a Java server respectively. You can review the configuration and drill down to individual issues to see what glass box results look like.

Note: Glass box scanning requires access to an agent located on the server of the application being scanned, and you do not have access to the agent that was used for this scan, you cannot continue the scan.

GSC_demo.testfire.scan
This is a web services scan of the AppScan demonstration test site. You can review the configuration and results. If you have installed GSC (Generic Service Client) you can use it to send additional requests to the site and continue the scan with the new data.

Chapter 3. Configuring

About this task

This section describes standard application scan configuration using the wizard. For advanced configuration methods, and details of web service scan configuration, refer to the main user guide and online help.

Procedure

1. Launch AppScan.
2. In the Welcome Screen, click **Create new Scan**.
3. In the New Scan dialog box, verify that the Launch wizard check box is selected.
4. In the Predefined Templates area, click **Regular Scan** to use the default template. (If you are using AppScan to scan one of the test sites for which there is a specialized pre-defined template, select that template: Demo.Testfire, Foundstone, or WebGoat.)
5. Select **Web Application Scan**, and click **Next**.
6. Type in the **URL** where the scan will start.

   Note: Click Advanced if you need to add additional servers or domains.
7. Click **Next**.
8. Select **Recorded Login**, then click **New**. A message appears describing the procedure for recording a login.
9. Click **OK**. The embedded browser opens with the Record button pressed (grayed out).
10. Browse to the login page, record a valid login sequence, and then close the browser.
11. In the Session Information dialog box, review the login sequence and click **OK**, then click **Next**. At this stage you can review the Test Policy that will be used for the scan (i.e. which categories are used for the scan.

    Note: By default all except invasive tests are used.

    Note: The **Advanced** button lets you control additional test options including privilege escalation (testing the extent to which privileged resources are accessible to users with insufficient access privileges) and multiphase scanning.
12. The **In-Session Detection** check box is selected by default, and text indicating that the response is "in-session" is highlighted. During the scan AppScan sends heartbeat requests, checking the responses for this text to verify that it is still logged in (and logs in again as necessary). Verify that the highlighted text is indeed proof of a valid session, then click **Next**.
13. In **Test Optimization**, if you need faster results, and don't mind a less thorough scan, select the **Optimize** radio button, otherwise leave the default setting (Normal). Then click **Next**.
14. Select the appropriate radio button to start **Automatic Scan**, start with **Manual Explore** or **Later** (to start the scan later by clicking the Start icon on the toolbar).
15. (Optional) By default the Scan Expert check box is selected so that Scan Expert will run when you complete the wizard. You can clear this to proceed directly to the scan stage.
16. Click **Finish** to exit the wizard.

Scan Expert

One of the options in the Scan configuration wizard is for Scan Expert to run a short scan to evaluate the efficiency of the new configuration for your particular site.

When Scan Expert runs, the Scan Expert panel opens in the upper part of the screen and the application tree starts to appear in the left-hand pane, as Scan Expert explores the site.

At the end of the short evaluation Scan Expert suggests configuration changes that you can accept or reject. (You can review the suggestions individually or elect to apply suggestions automatically.)

Note: There are some changes that Scan Expert can only apply with human intervention, so when you select the automatic option some changes may not be applied.

- To run Scan Expert manually, preceded by a short Explore stage (when there are no Explore results yet), click **Scan > Run Scan Expert Evaluation**.
- To run Scan Expert manually, on existing Explore stage results, click **Scan > Run Scan Expert Analysis Only**.
- To configure Scan Expert to run automatically before scans, click **Tools > Options > Preferences**, and select **Run Scan Expert before scan**.
- To configure which Scan Expert modules run, click **Configuration > Scan Expert**.

Manual exploring

About this task

Manual Explore lets you browse the application yourself, clicking on links and inputting data. AppScan records your actions, and uses the data to create tests. There are three reasons you might want to explore manually:

- To pass anti-automation mechanisms (such as the requirement to type in a random word, displayed as an image)
- To explore a specific user process (the URLs, files and parameters that a user would access given a certain scenario)
- Because interactive links were discovered during a scan, and you want to fill in the required data to enable a more thorough scan

Note: After creating a Manual Explore, you may want to continue with an automatic Explore stage, so that the scan covers your entire application.

Procedure

1. Click **Scan > Manual Explore**

   The embedded browser opens.
2. Browse the site, clicking on links and filling in fields as required.
3. When finished close the browser.

   Note: You can create a manual explore that contains multiple processes by clicking **Pause**, browsing to a different location, and then clicking **Record** to resume recording.

   The **Explored URLs** dialog box appears, displaying the URLs that you visited.
4. Click **OK**.
5. AppScan checks if any of your input is suitable for adding to the Automatic Form Filler, presents a list, and asks if so asks whether you want to add **All**, **None** or **Selected Parameters**.
   - If you want some of your input to be added to the Automatic Form Filler, click **Add Selected**. Then select items in the Temporary Form Parameters list, and click **Move** (to move them to the Existing Form Parameters list). Then click **OK**.
6. Click **OK**. AppScan analyzes the URLs that you crawled and creates tests based on this analysis.
7. To run the new tests, click **Scan > Continue Scan**.

Chapter 4. Scanning

When the scan begins, the Progress Panel appears in the upper part of the screen, and together with the status bar (along the bottom of the screen), shows details of scan progress. The panes are populated with real-time results as they are processed.

Progress panel

The progress panel shows the current phase of the scan, as well as the URL and parameter being tested.

If new links are discovered during the scan (and multiphase scanning is enabled), and additional scan phase starts automatically upon completion of the previous phase. The new phase may be significantly shorter than the previous phase, since only *new* links are scanned. Alerts such as "Server down" may also be displayed on the progress panel.

Status bar

The status bar at the bottom of the screen shows the following information for the scan:

- **Visited Pages:** Number of pages visited / Total number of pages to be visited

  The second number may increase and then decrease during the scan, as pages are discovered and some then some rejected as not requiring scanning. By the end of the scan the two numbers should be equal.
- **Tested Elements:** Number of elements tested / Total number of elements to be tested

  The second number will increase during the Explore stage, as elements for testing are discovered. During the Test stage the first number will increase. By the end of the scan the two numbers should be equal.
- **HTTP Requests Sent**

  This number represents all requests sent, including in-session detection requests, server-down detection requests, login requests, multi-step operations and test requests. During the scan it is therefore an indicator that AppScan is working, but the actual number is not of any particular significance either during or after the scan.
- **Security Issues**

  Total number of security issues found, followed by the number in each category: High, Medium, Low, and Informational.

Scheduling scans

You can schedule scans to start automatically once or at regular intervals.

Procedure

1. Click **Tools > Scan Scheduler**, then click **New**.
2. Type in a name for the schedule, and fill-in the options you require:
   - Select **Current Scan** or a **Saved** scan (if Saved, browse to the required .scan file)
   - Select **Daily**, **Weekly**, **Monthly**, or **Once Only**.
   - Select **Date** and **Time** for the scan
   - Type in **Domain Name** and **Password**
3. Click **OK**.

   The schedule name appears in the **Scan Scheduler** dialog box.

Chapter 5. Working with Results

Result views

Results can be displayed in three views: Security Issues, Remediation Tasks, and Application Data. The view is selected by clicking a button in the view selector. The data displayed in all three panes varies with the view selected.

	**Data view**	Shows script parameters, interactive URLs, visited URLs, broken links, filtered URLs, comments, JavaScripts and cookies from the Explore stage. **Application Tree:** Complete application tree. **Result List:** Select a filter from the pop-up list at the top of the Result List, to determine which information is displayed. **Detail Pane:** Details of the item selected in the Result List Unlike the other two views, Application data view is available even if AppScan has only completed the Explore stage. Use the pop-up list at the top of the Result list to filter the data.
	**Issues view**	Shows the actual issues discovered, from overview level down to individual requests/responses. This is the default view. **Application Tree:** Complete application tree. Counters next to each item show the number of issues found for the item. **Result List:** Lists issues for the selected note in the application tree, and the severity of each issue. **Detail Pane:** Shows advisory, fix recommendations and request/response (including all variants used) for the issue selected in the Result List
	**Tasks view**	Provides a To Do list of specific remediation tasks to fix the issues found by the scan. **Application Tree:** Complete application tree. Counters next to each item show the number of fix recommendations for that item. **Result List:** Lists remediation tasks for the selected node in the application tree, and the priority of each task. **Detail Pane:** Shows details of the remediation task selected in the Result List, and all the issues that this remediation will solve.

Severity levels

The Result List displays the issues for whatever item is selected in the application tree. These can be for:

- Root level: All site issues are displayed
- Page level: All issues for the page
- Parameter level: All issues for a particular request to a particular page

Each issue is assigned one of four security levels:

	High security issue
	Medium security issue
	Low security issue
	Informational security issue **Note:** This category applies to Issues View only. In Remediation View all issues less than Medium are classified as Low.

Note: The severity level assigned to any issue can be changed manually by right-clicking on the node.

Security issues tabs

In Security Issues view the vulnerability details for the selected issue appear in the Detail pane in four tabs:

Issue Information	A summary of the information available on the other Detail pane tabs, plus additional information, including CVSS Metric scorings for the issue, and relevant screen shots, that can be saved with the results and included in reports.
Advisory	Technical details on the selected issue and links for more information. What has to be fixed and why.
Fix Recommendations	The exact tasks that should be done to make your web application secure against the specific selected issue.
Request/Response	Shows the speciic tests that were sent to the application, and its response (can be viewed as HTML or in a Web browser). **Variants:** If there are variants (different parameters that were sent to the same URL), they can be viewed by clicking the < and > buttons at the top of the tab. Two tabs at the right of this tab let you view **Variant Details** and add a **Screenshot** that will be saved with the results.

Exporting results

About this task

You can export the complete scan results as an XML file, or as a relational database. (The database option exports the results into a Firebird database structure. This is open source, and follows ODBC and JDBC standards.)

Procedure

1. Click **File > Export** and select **XML** or **DB**.
2. Browse to the location you want, and type in a name for the file.
3. Click **Save**.

Chapter 6. Reports

After AppScan has assessed your site's vulnerability, you can generate customized reports configured for the various personnel in your organization.

You can open and view the reports from within AppScan, and you can save a report as a file to be opened with a third-party application, such as Acrobat Reader.

Icon	Name	Short Description
	**Security Report**	Report of security issues found during the scan. Security information may be very extensive, and can be filtered depending on your requirements. Six standard templates are included, but each can easily be tailored to include or exclude categories of information, as necessary.
	**Industry Standard Report**	Report of the compliance (or non-compliance) of your application with a selected industry committee, or your own custom standards checklist.
	**Regulatory Compliance Report**	Report of the compliance (or non-compliance) of your application with a large choice of regulations or legal standards, or with your own custom Regulatory Compliance template).
	**Delta Analysis Report**	The Delta Analysis report compares two sets of scan results and shows the difference in URLs and/or security issues discovered.
	**Template Based Report**	Custom report containing user-defined data and user-defined document formatting, in Microsoft Word .doc format.

Note: Industry Standard and Regulatory Compliance reports are not available in AppScan Developer Edition.

Chapter 7. Main toolbar

The icons on the toolbar offer quick access to frequently used features (that are also available from the menus).

Icon	Name	Click to:
	Scan >	(Available only if a scan is loaded and configured.) Opens a short Scan menu, with the following options:  Full Scan: Start a full scan (Explore and Test stages) or continue a paused scan.  Explore Only: Run an Explore stage only (or continue an Explore that was paused), without following it with the Test stage.  Test Only: Run a Test stage only (or continue a Test that was paused), without first running an Explore stage. Active only if there are already some Explore results.
	Pause Scan	(Active only when a scan is running.) Pause current scan (whether Full Scan, Explore Only or Test Only). You can resume the scan later. You can also save a paused scan to continue at another time.
	Manual Explore	Open the browser to the application's URL and manually browse the site, completing required parameters as you go. AppScan will then add this Explore data to its own, automatically collected Explore data, when creating tests for the site.
	Configure	Open the Scan Configuration dialog box to configure the scan.
	Report	Create a report with the current scan data.
	Scan on Cloud	Uploads an AppScan Standard configuration file (SCAN or SCANT) to IBM Application Security on Cloud. You can use the configuration to run a full scan, or use existing Explore stage results saved in the file and run Test Only.
	Find	Find an issue. (Enabled only when the Issues view is selected.)
	Scan Log	Display the Scan Log during or after a scan. (Lists all actions performed by AppScan during the scan, as they occur.)
	PowerTools	Open one of the PowerTools, applications supplied with AppScan to help you with various tasks.

View Selector

The three icons on the right of the toolbar toggle between the three views: Application Data, Security Issues, and Remediation Tasks.

Icon	Name	Click to display:
	Data view	Application Data view.
	Issues view	Security Issues view.
	Tasks view	Remediation Tasks view.

Notices

This information was developed for products and services offered in the US.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.