

What new in AppScan 9.0.3.9

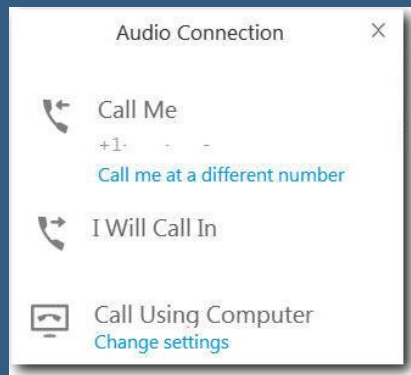
IBM SECURITY SUPPORT OPEN MIC

To hear the WebEx audio, **select an option** in the Audio Connection dialog or by access the Communicate > Audio Connection menu option. To ask a question by voice, you must either Call In or have a microphone on your device.

You will not hear sound until the host opens the audio line.

For more information, visit:

http://ibm.biz/WebExOverview_SupportOpenMic



Florin Coadă – Offering manager, Application Security

July 18, 2018

NOTICE: BY PARTICIPATING IN THIS CALL, YOU GIVE YOUR IRREVOCABLE CONSENT TO IBM TO RECORD ANY STATEMENTS THAT YOU MAY MAKE DURING THE CALL, AS WELL AS TO IBM'S USE OF SUCH RECORDING IN ANY AND ALL MEDIA, INCLUDING FOR VIDEO POSTINGS

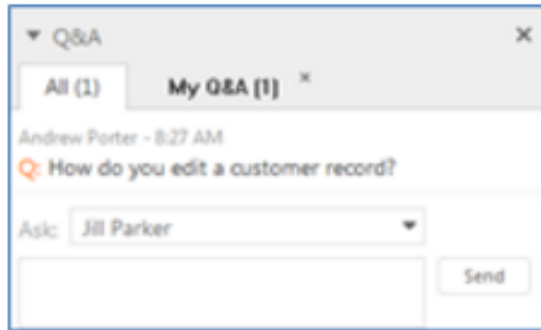
Questions for the panel

To ask the panel a question during the presentation:

Type a question in the box below the *Ask* drop-down menu in the Q&A panel.

Select *All Panelists* from the *Ask* drop-down-menu.

Click **Send**. Your message is sent and appears in the Q&A panel.



The screenshot shows a Q&A panel interface. At the top, there is a header bar with a dropdown menu labeled 'Q&A' and a close button 'X'. Below the header, there are two tabs: 'All (1)' and 'My Q&A (1)'. The 'All (1)' tab is selected. Below the tabs, there is a question displayed: 'Andrew Porter - 8:27 AM' followed by 'Q: How do you edit a customer record?'. Below the question, there is an 'Ask:' label followed by a dropdown menu showing 'Jill Parker'. Below the dropdown menu, there is a text input box and a 'Send' button.

Agenda

- **What's new in AppScan Source 9.0.3.9**
- **What's new in AppScan Standard 9.0.3.9**
- **What's new in AppScan Enterprise 9.0.3.9**

What's new in AppScan Source 9.0.3.9

What's new in AppScan Source for Analysis version 9.0.3.9

- Support for .NET framework v4.7 under VS2017
- Support for .NET Core 2.0 under VS2017
- Support for VS2017 plugin

Support for .NET framework v4.7 under VS2017

- Projects using .NET Framework v4.7 can now be scanned under AppScan Source for Analysis.
- All supported .NET languages are included. (C#, ASP.NET, VB.NET)
- Solution file for .NET Framework v4.7 projects can be dropped into AppScan Source to import or imported via CLI.
- Will require Visual Studio 2017
- Also .NET Framework v4.7 under Visual Studio 2017, which is listed under “Individual components”.

Support for .NET Core 2.0 under VS2017

- **Projects using .NET Core v2.0 can now be imported and scanned under AppScan Source for Analysis.**
 - Solution file for .NET Core v2.0 projects can be dropped into AppScan Source to import or imported via CLI.
 - Project Type will be labeled as “.NET Core” under AppScan Source.
- **Will require Visual Studio 2017**
 - Projects will be published before being scanned

Project Type: .NET Core

Filtering

☐ Filter findings contained in external sources

Caching

☐ Enable Vulnerability Analysis cache

Remove cached Vulnerability Analysis and Custom Rules signature data

String Analysis

☐ Enable String Analysis to find validator/sanitizer functions

☐ Apply imported rules to Global Scope

File Encoding

Select the file encoding for this project: ISO-8859-1

Overview | Filters | Rules and Rule Sets | File Extensions | Additional Assemblies | Project Dependencies

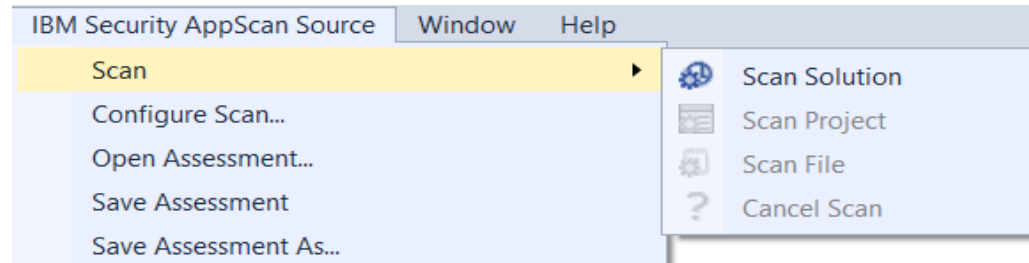
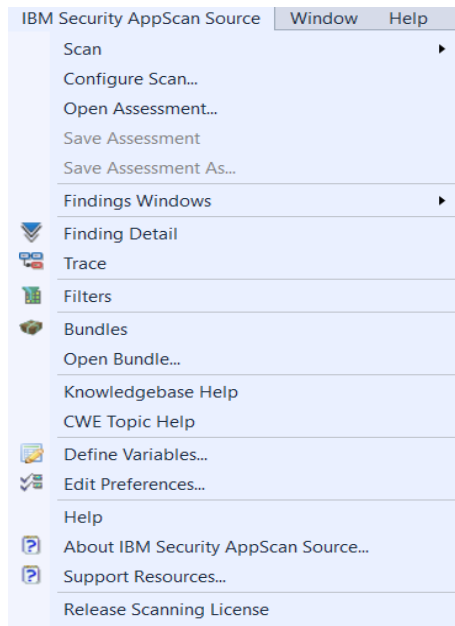
Console Findings

Assessment Output - 6/14/18 9:10 AM

```
06/14/18 09:10:41 - New scan started
06/14/18 09:10:41 - Scanning with Scan Configuration: Normal scan
06/14/18 09:10:41 - Scanning with cross-project analysis disabled
06/14/18 09:10:41
06/14/18 09:10:41 - Scanning Project Infrastructure ( 1 of 1 )
06/14/18 09:10:41 - Preparing project for scan...
06/14/18 09:10:41 - Publishing .NET Core project Infrastructure ...
06/14/18 09:10:52 - Microsoft (R) Build Engine version 15.7.179.6572 for .NET Framework
Copyright (C) Microsoft Corporation. All rights reserved.
```

Support for VS2017 plugin

- **AppScan Source** is available as a plugin for Visual Studio 2017.
 - New menu “IBM Security AppScan Source”.
 - Menu options include executing scans, configuring scans, viewing traces and filters, etc...



Support for VS2017 plugin

- Scan results and traces can be viewed under Visual Studio 2017.

The screenshot displays the IBM Security AppScan Source for Development web interface. The browser tab is labeled 'dotnetsamples.ozasmt'. The page header shows 'IBM Security AppScan Source for Development' and the IBM logo. The main content area is titled 'dotnetsamples' and indicates it was scanned on 6/14/2018 at 9:25 AM. Below this, a 'Results' section provides a summary of findings:

Results			
Viewable Findings	18	Fixed/Missing Findings	0
Filtered Findings	0	Modified Findings	0
Excluded Findings	0	Custom Findings	0

Below the results summary, there is a 'Links' section with links to 'Filters' and 'Bundles'.

The bottom portion of the screenshot shows the 'Viewable Findings' table within the Visual Studio 2017 plugin. The table has columns for Trace, Severity, Classification, API, Context, File, Calling Method, and Line. The findings listed are all of 'Low' severity and 'Definitive' classification, related to 'System.Con' and 'ConsoleMo'.

Trace	Severity	Classification	API	Context	File	Calling Method	Line
	Low	Definitive	System.Con	System.Con	ConsoleMo	ConsoleMo	57
	Low	Definitive	System.Con	System.Con	ConsoleMo	ConsoleMo	53
	Low	Definitive	System.Con	System.Con	ConsoleMo	ConsoleMo	33
	Low	Definitive	System.Con	System.Con	ConsoleMo	CyrillicToRo	46
	Low	Definitive	System.Con	System.Con	ConsoleMo	CyrillicToRo	27
	Low	Definitive	System.Con	System.Con	ConsoleMo	CyrillicToRo	43

Known limitations:

- If 9.0.3.6 VS 2015 plugin that was delivered as an ifix is installed, it needs to be removed manually before upgrading to 9.0.3.9
- Visual Studio 2017 .NET Assembly projects are not supported with .NET Core.
- Visual Studio 2017 C++ projects are not supported.
- Windows 10 requires compatibility mode (Windows 8) for installer and uninstaller.

Resolved Defect:

- PI69539 Unable to sort custom AppScan Source report by Severity



Questions?

Now is your opportunity to ask live questions.

To ask a question now:

Raise your hand by clicking Raise Hand. The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.



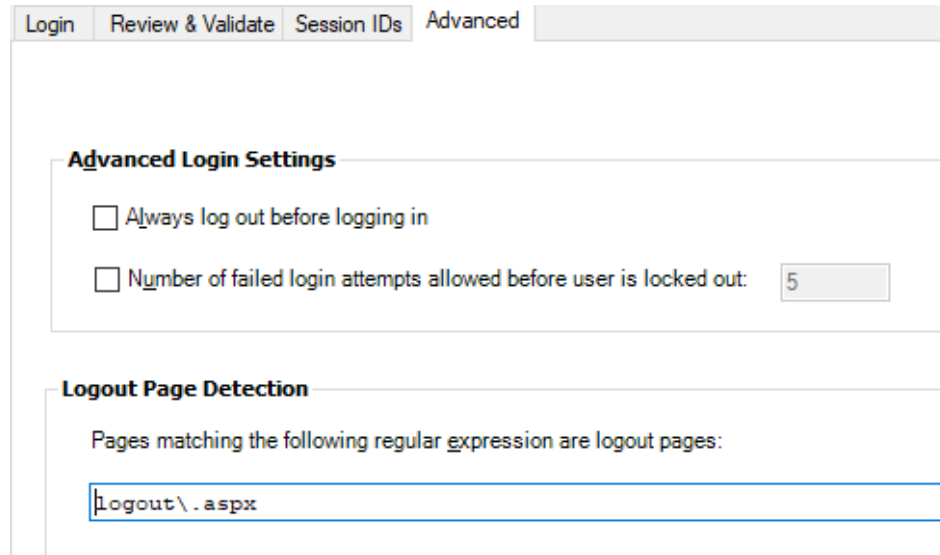
What's new in AppScan Standard 9.0.3.9

What's new in AppScan Standard 9.0.3.9

- Greatly Improved Login Management Configuration
- New Action-Based Explore Options
- Improved Action-Based Scanning
- RFEs & APARs
- Known issues

Login Management: Main tab

- **Export** and **Import** were moved from the recorded login to the bottom of the dialog, and are available in all login modes. This was done because they are not just for Recorded Login, but for all login configurations.
- Advanced Configuration items in this view were moved the new “Advanced” Tab:



The screenshot shows a web interface with a tabbed navigation bar at the top containing five tabs: 'Login', 'Review & Validate', 'Session IDs', 'Advanced', and an unlabeled tab. The 'Advanced' tab is currently selected. Below the tabs, the content area is divided into two sections. The first section, titled 'Advanced Login Settings', contains two checkboxes. The first checkbox is labeled 'Always log out before logging in'. The second checkbox is labeled 'Number of failed login attempts allowed before user is locked out:' and is followed by a text input field containing the number '5'. The second section, titled 'Logout Page Detection', contains a text label 'Pages matching the following regular expression are logout pages:' followed by a text input field containing the regular expression 'logout\\.aspx'.

Login Review & Validate Session IDs **Advanced**

Advanced Login Settings

☐ Always log out before logging in

☐ Number of failed login attempts allowed before user is locked out: 5

Logout Page Detection

Pages matching the following regular expression are logout pages:

logout\\.aspx

Login Management: “Review & Validate” tab

- The Login Management Details tab (now Review & Validate) was changed in order to emphasize the configuration items (login playback, in-session request, Detection pattern) and improve the tools we use to configure and debug login configuration. The more complex actions have their own dialog.

The screenshot shows the 'Review & Validate' tab of the Login Management interface. At the top, there are four tabs: 'Login', 'Review & Validate' (which is selected and highlighted with a dotted border), 'Session IDs', and 'Advanced'. Below the tabs, the interface is divided into two main sections: 'Login Playback' and 'Session Detection'. In the 'Login Playback' section, there is a 'Login Playback Method' dropdown menu set to 'Action-based', a green 'Replay' button with a play icon, and an 'Edit' button with a pencil icon. The 'Session Detection' section contains an 'In-Session Detection Request' dropdown menu with the value 'https://demo.testfire.net/bank/main.aspx' and an 'Advanced request selection' button. Below this is an 'In-Session Detection Pattern' dropdown menu with the value '>Sign Off<' and an 'Advanced pattern selection' button. There are two radio buttons for 'In-Session' (selected) and 'Out of-Session', and a checkbox for 'RegExp' which is unchecked. A green checkmark and the text 'Selected pattern is valid.' are displayed below the pattern selection. At the bottom center, there is a blue 'Validate' button. Below the button, there is a green key icon with a checkmark, followed by the text 'Login successfully configured' in green, and 'Using action-based login' in a smaller font.

Login | **Review & Validate** | Session IDs | Advanced

Login Playback

Login Playback Method: Action-based ▼ ▶ Replay ✎ Edit

Session Detection


In-Session Detection Request: https://demo.testfire.net/bank/main.aspx ▼ Advanced request selection

In-Session Detection Pattern: >Sign Off< ▼ Advanced pattern selection

☒ In-Session ☐ Out of-Session ☐ RegExp

✓ Selected pattern is valid.

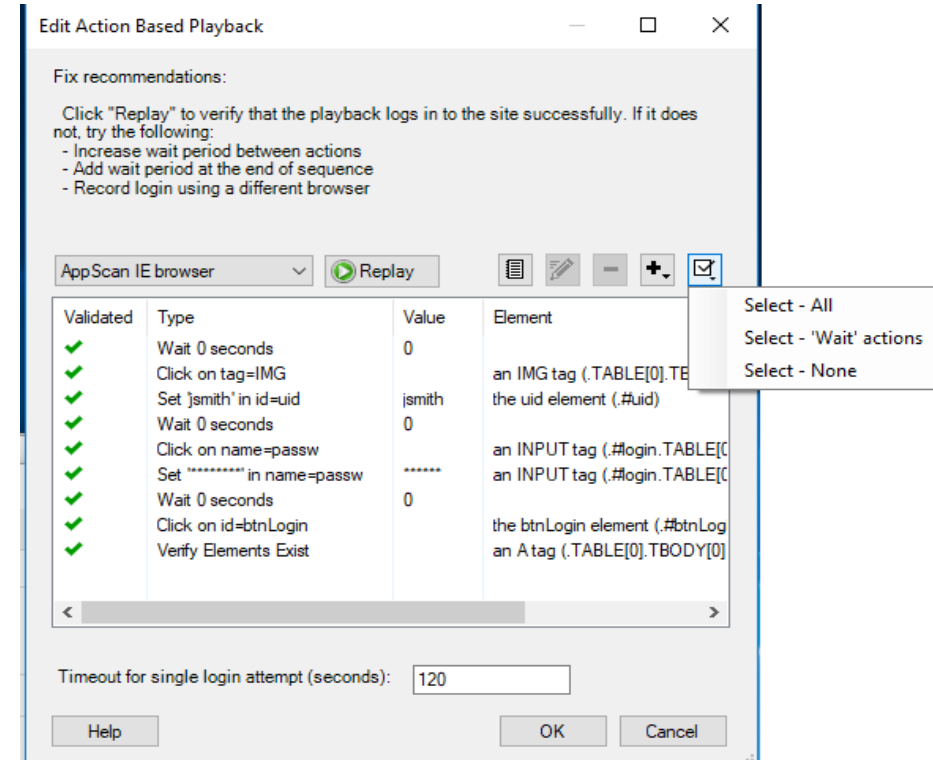
Validate

 **Login successfully configured**
Using action-based login

Login Management: Edit Action-Based playback

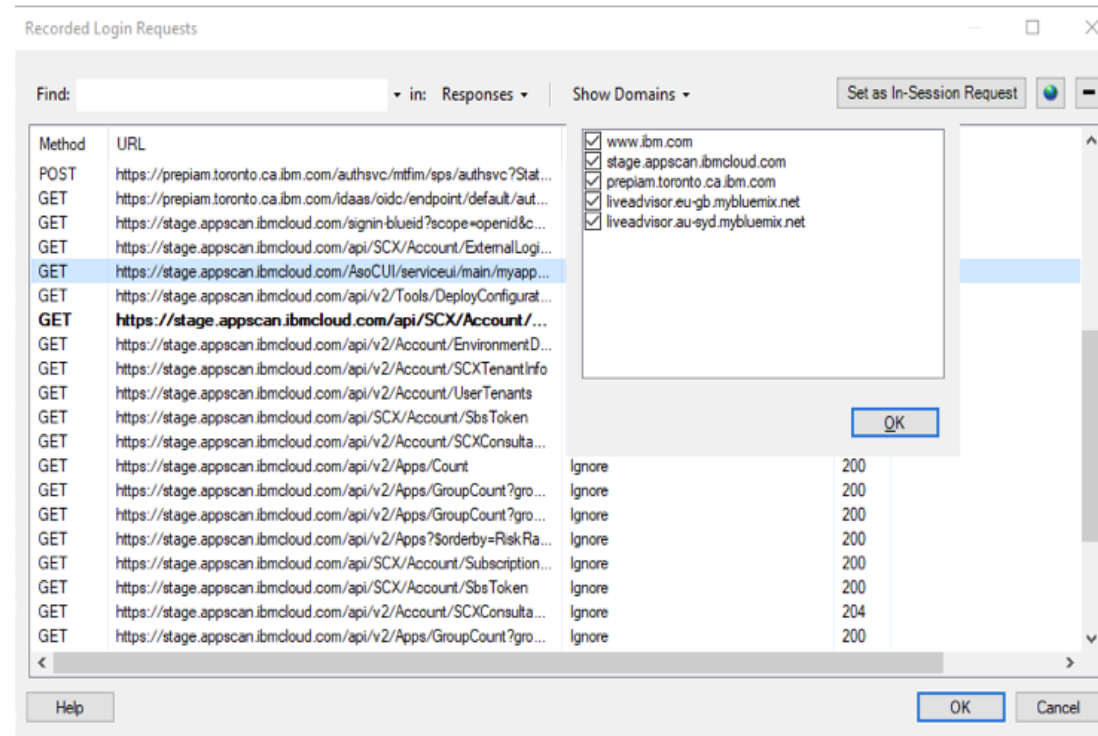
Troubleshoot Action-Based sequence operations in this dialog:

- Add/edit individual “wait” actions.
-OR-
- Select all wait actions using the select menu, and click on edit and increase their delay time (useful when you are not sure where to add a delay).
-OR-
- Change playback browser (e.g. to Chromium)
-OR-
- Increase/reduce total login timeout (max time)



Login Management: Edit Request-Based playback

- To open the request-based edit, click on the edit button when login playback method in “request based”.
- The new view has a search field and a filter viewed domain. This will enable you to easily select and delete unwanted requests.
- You can also select in-session request here, but the preferred dialog to do that is “Advanced request selection”



Login Management: Selecting In-Session Request

- If the “In-Session Detection Request” section indicates an error:



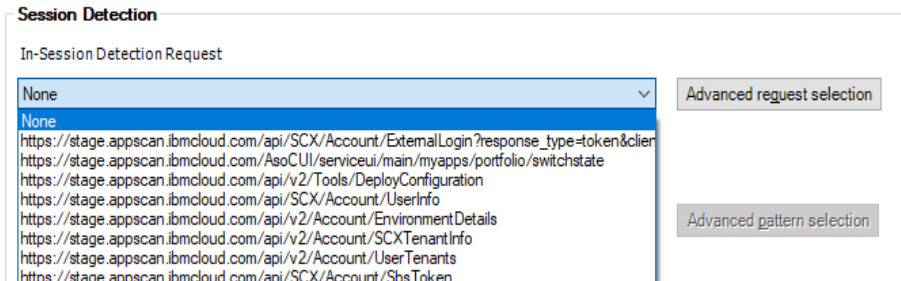
The screenshot shows the 'Session Detection' section. Under 'In-Session Detection Request', there is a dropdown menu currently set to 'None'. To the right of the dropdown is a button labeled 'Advanced request selection'. Below the dropdown, a red error message with an 'x' icon reads: 'Select an in-session request.'

you can now:

- 1) select a new request from the combo-box:

-OR-

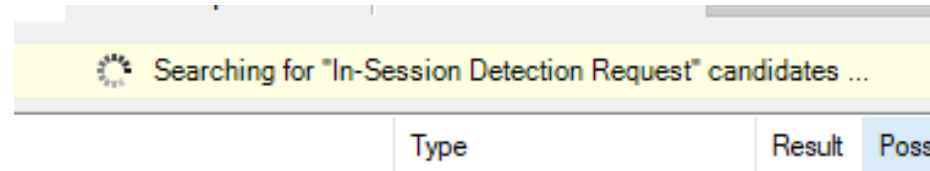
- 2) Click on “Advanced request selection” to get a dialog with more info that will help select a good request, if there is one.



This screenshot shows the 'Session Detection' section with the 'In-Session Detection Request' dropdown menu open. The menu lists several URLs as options, including 'None' at the top. To the right of the dropdown, there are two buttons: 'Advanced request selection' and 'Advanced pattern selection'.

Login Management: Advanced Request Selection dialog

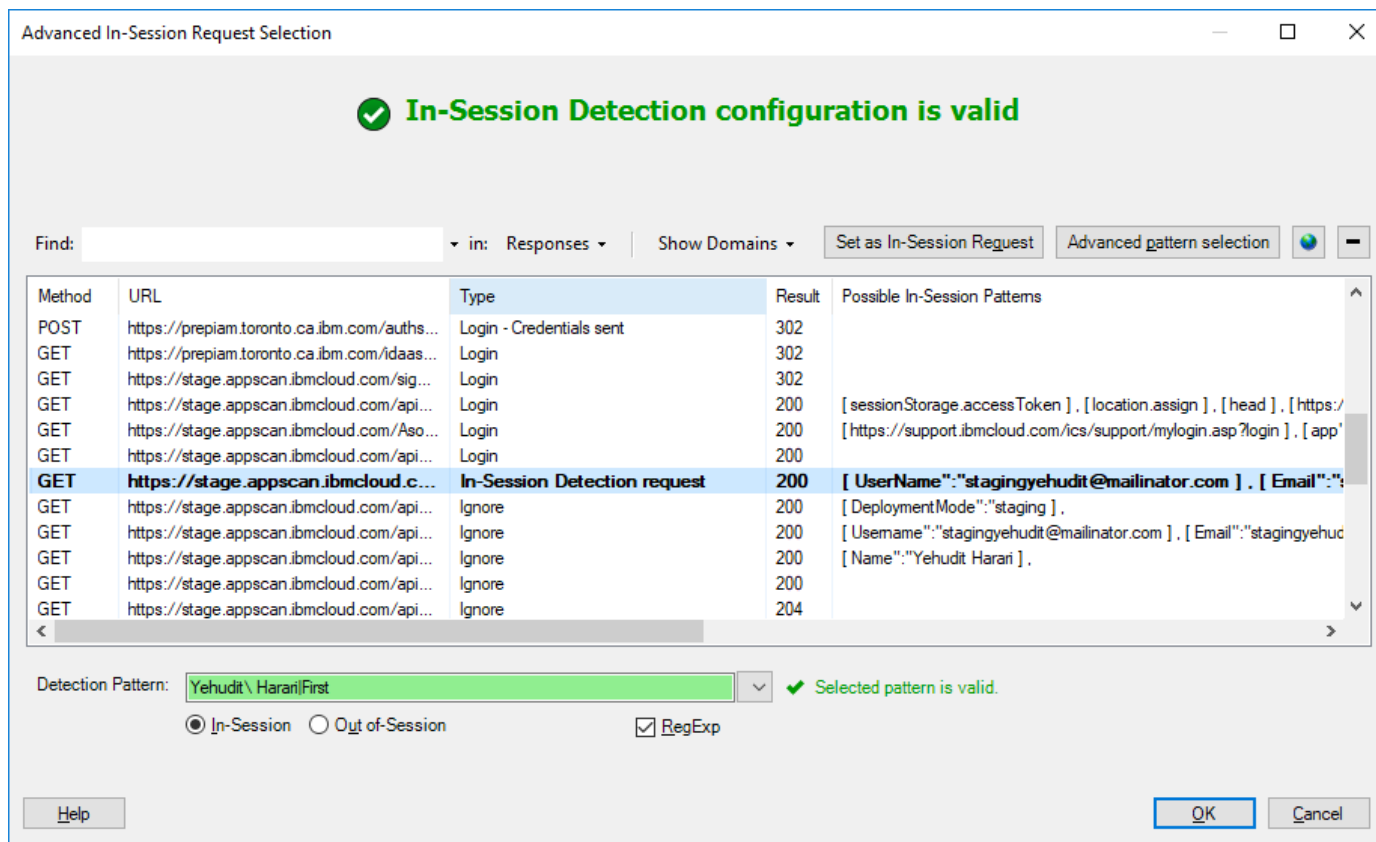
- “Advanced request selection” dialog shows you more info to help you select, at-a-glance, a request with a good pattern. In the image in the next slide, a candidate for the in-session detection request is marked in purple.
- In the right column, we show for each request (after the login request) a few of the possible in-session pattern candidates.
- If a request doesn't have any candidates, and the right column is empty (it might takes a few seconds to fill the column, we have a notice for that:



that means that sending the request with and without the cookies gets the same response, so the request is not suitable to be the “In-Session detection request”.

Login Management: Advanced Request Selection dialog (1)

This image shows the dialog with a “good” working configuration:



Login Management: Advanced Request Selection dialog (2)

This image shows the dialog when no “In-session detection request” is selected:

Marked in green: a request candidate with a nice pattern for the in-session detection request.

Session detection disabled

Select a request that occurs after the login request ('Credentials sent') and that has values in column 'Possible In-Session Patterns'.

Find: in: Responses Show Domains Set as In-Session Request Advanced pattern selection

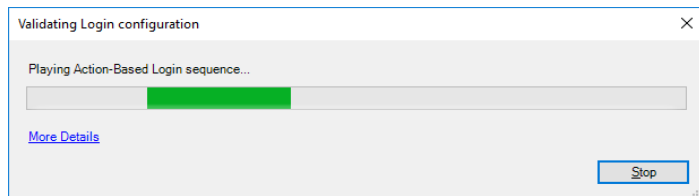
	Type	Result	Possible In-Session Patterns
ibm.com/idaas/mtfim/sps/authsvc?PolicyId=ur...	Login	200	
ount/us-en/	Login	200	
ibm.com/v1/mgmt/idaas/user/identitysources	Login - Credentials sent	200	
ibm.com/authsvc/mtfim/sps/authsvc?StateId=...	Login - Credentials sent	302	
ibm.com/idaas/oidc/endpoint/default/authoriz...	Login	302	
cloud.com/signin-blueid?scope=openid&code=...	Login	302	
cloud.com/api/SCX/Account/ExternalLogin?re...	Login	200	[sessionStorage.accessToken], [location.assign], [head], [https://stage.appscan.ibm...
cloud.com/AsoCUI/serviceui/main/myapps/po...	Login	200	[https://support.ibmcloud.com/ics/support/mylogin.asp?login], [app " ng-strict-di lang],
cloud.com/api/v2/Tools/DeployConfiguration	Login	200	
cloud.com/api/SCX/Account/UserInfo	Ignore	200	[Username:"stagingyehudit@mailinator.com"], [Email:"stagingyehudit@mailinator.com"],
cloud.com/api/v2/Account/EnvironmentDetails	Ignore	200	[DeploymentMode:"staging"],
cloud.com/api/v2/Account/SCXTenantInfo	Ignore	200	[Username:"stagingyehudit@mailinator.com"], [Email:"stagingyehudit@mailinator.com"],
cloud.com/api/v2/Account/UserTenants	Ignore	200	[Name:"Yehudit Harani"],
cloud.com/api/SCX/Account/SbsToken	Ignore	200	
cloud.com/api/v2/Account/SCXConsultantInfo	Ignore	204	

Detection Pattern: **No In-session request selected. Select an in-session request.**

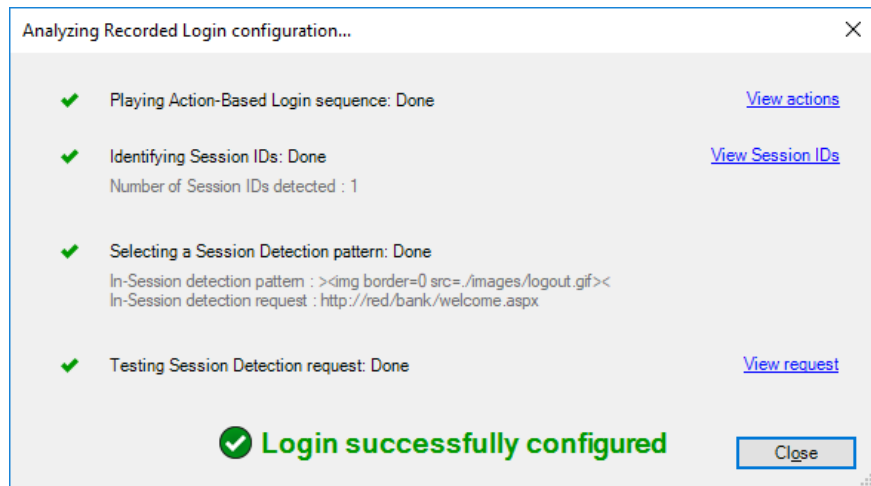
☒ In-Session ☐ Out of-Session ☒ RegExp

Login Validation: Progress dialog “More Details”

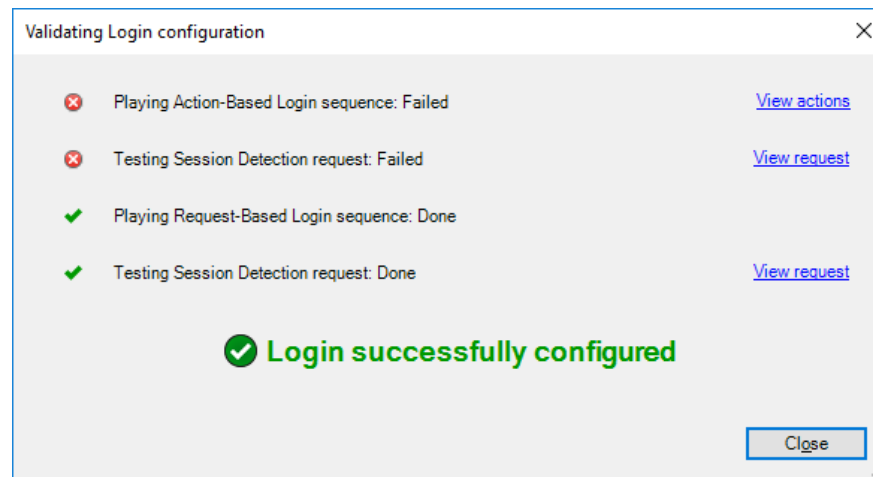
- We have added a “More Details” link to the progress dialog that the user sees after recording login or clicking Validate. Clicking the link will display the steps as they occur.



Details After recording login:



Details after validation, only request base succeeds:



Login Validation Progress dialog: Info on step: “Testing Session Detection”

For the step “Testing Session Detection”, you get a dialog that shows:

Right panel: **actual** request sent

Left panel: the request recorded during login. This lets you determine whether Session IDs were sent correctly.

In the example on the right, I deleted a custom header from configuration, to simulate a problematic scenario. Both requests are sent with the SAME authorization header!! They should have different values.

In previous versions we would have needed to turn on the traffic log, rerun the scan, open Traffic viewer and figure out which requests we need to compare.

In-Session Detection responses

The screenshot displays the 'In-Session Detection failed' dialog. At the top, a red error icon and text state 'In-Session Detection failed'. Below this, a message explains the failure: 'In-Session Detection failed because the configured pattern wasn't found in the response: Yehudit HarariFirst'. The dialog is divided into two main panels: 'From Login Configuration' on the left and 'From In-Session Detection test' on the right. Each panel shows a 'Request' and a 'Response' section. A red circle highlights the 'Authorization' header in both requests, which is 'Bearer G1TcHg3A2X_G3d7o9016C70Swimin9kkoX'. A red arrow points from this circle to the error message, indicating that the same authorization header was used in both requests, which caused the detection to fail.

From Login Configuration

Request

```
GET /api/SCX/Account/UserInfo HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/
Accept: application/json, text/plain, */*
Host: stage.appscan.ibmcloud.com
Connection: Keep-Alive
Referer: https://stage.appscan.ibmcloud.com/AsocUI/servi
Accept-Language: en-US,en;q=0.7,he;q=0.3
Authorization: Bearer G1TcHg3A2X_G3d7o9016C70Swimin9kkoX
```

Response

```
HTTP/1.1 200 OK
X-XSS-Protection: 1; mode=block
Server: Microsoft-IIS/7.5
Content-Length: 1236
X-Content-Type-Options: nosniff
Cache-Control: no-store, no-cache
Strict-Transport-Security: max-age=63072000; includeSubD
Date: Wed, 11 Apr 2018 09:12:28 GMT
```

From In-Session Detection test

Request

```
GET /api/SCX/Account/UserInfo HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/
Accept: application/json, text/plain, */*
Host: stage.appscan.ibmcloud.com
Connection: Keep-Alive
Referer: https://stage.appscan.ibmcloud.com/AsocUI/servi
Accept-Language: en-US,en;q=0.7,he;q=0.3
Authorization: Bearer G1TcHg3A2X_G3d7o9016C70Swimin9kkoX
```

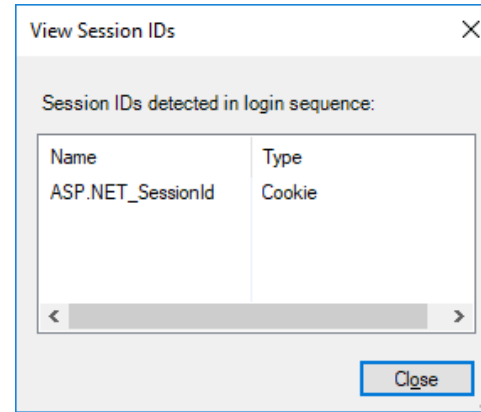
Response

```
HTTP/1.1 401 Unauthorized
X-XSS-Protection: 1; mode=block
Server: HCL-AppC/1.1
Content-Length: 80
WWW-Authenticate: Bearer
WWW-Authenticate: Bearer
X-Content-Type-Options: nosniff
Cache-Control: private
```

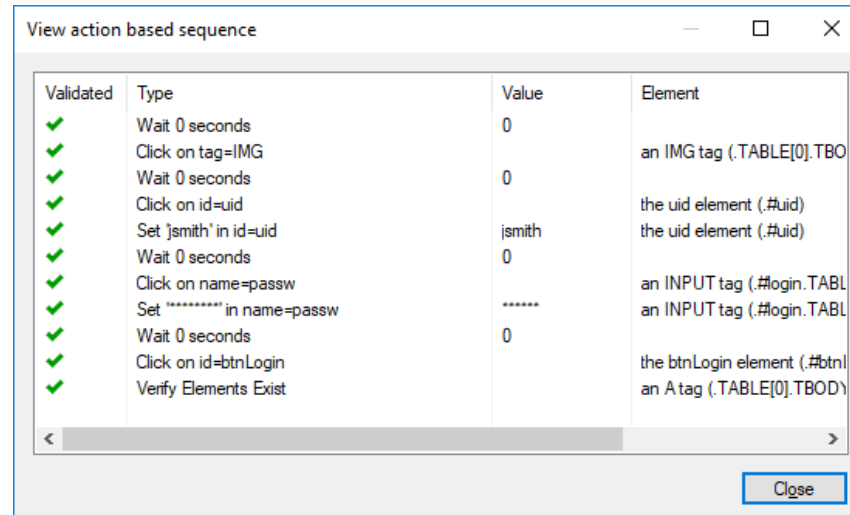
Same value for Authorization header

Login Validation progress dialog: Info on steps (2)

Info dialog for Session IDs step:



Info dialog for Action-Based playback:



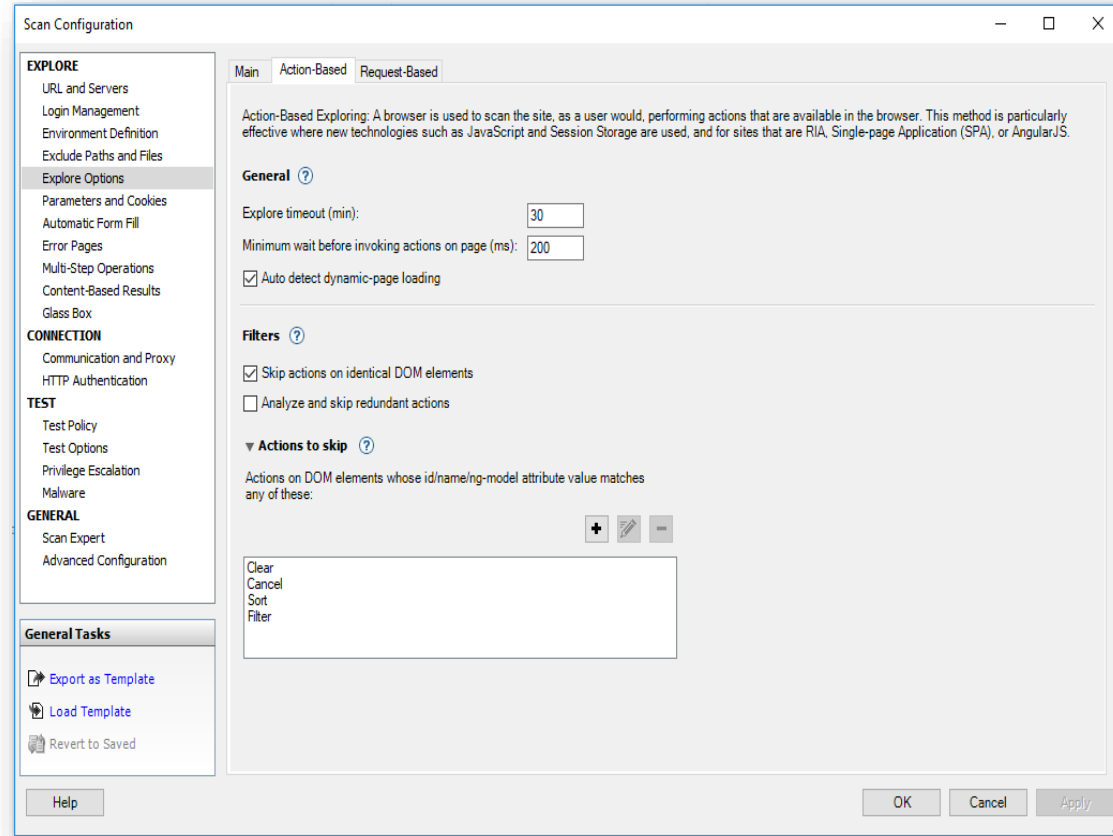
New Action-Based Explore Options

- AppScan Standard 9.0.3.9 supports new scan configuration in Action-Based Explore.
- In previous versions the support team configured some of the scan configuration manually from the template.
- Explore options configuration was redesigned and now contains new tabs for Action-Based and Request-Based configuration.

New Action-Based Explore Options (1)

Added value:

- Action-Based Explore is now more configurable.
- User has more control on Action-Based Explore.
- Configuration can be changed more easily from the AppScan UI rather than using a template.



New Action-Based Explore Options (2)

Configuration options now available in AppScan:

- Explore timeout: Limit the Action-Based Explore duration to certain amount of time.
- Minimum wait before invoking actions: Ensure that the page is Explored only after it has loaded successfully.
- Auto-detect dynamic-page loading: Helps determine dynamic page loading progress.

General ?

Explore timeout (min):

Minimum wait before invoking actions on page (ms):

☒ Auto detect dynamic-page loading

Filters ?

☒ Skip actions on identical DOM elements

☐ Analyze and skip redundant actions

▼ Actions to skip ?

Actions on DOM elements whose id/name/ng-model attribute value matches any of these:

+

-

Clear

Cancel

Sort

Filter

New Action-Based Explore Options (3)

- Skip actions on identical DOM elements: Reduce Explore time.
- Analyse and skip redundant actions: Skip similar actions that will most probably lead to similar results.
- Actions to skip: User can now define DOM elements to exclude from exploring.

General ?

Explore timeout (min):

Minimum wait before invoking actions on page (ms):

☒ Auto detect dynamic-page loading

Filters ?

☒ Skip actions on identical DOM elements

☐ Analyze and skip redundant actions

▼ **Actions to skip** ?

Actions on DOM elements whose id/name/ng-model attribute value matches any of these:

+ [icon] -

Clear
Cancel
Sort
Filter

New Action-Based Explore Options (4)

Notes:

- Request-Based configuration capabilities remains same as before.
- AppScan Extended Support Mode now contains Action-Based Explore logs in addition to the logs that were packed before such as:
 - Graph.dot
 - Crawler log
 - Crawler Click Filtering log.
 - dom-states

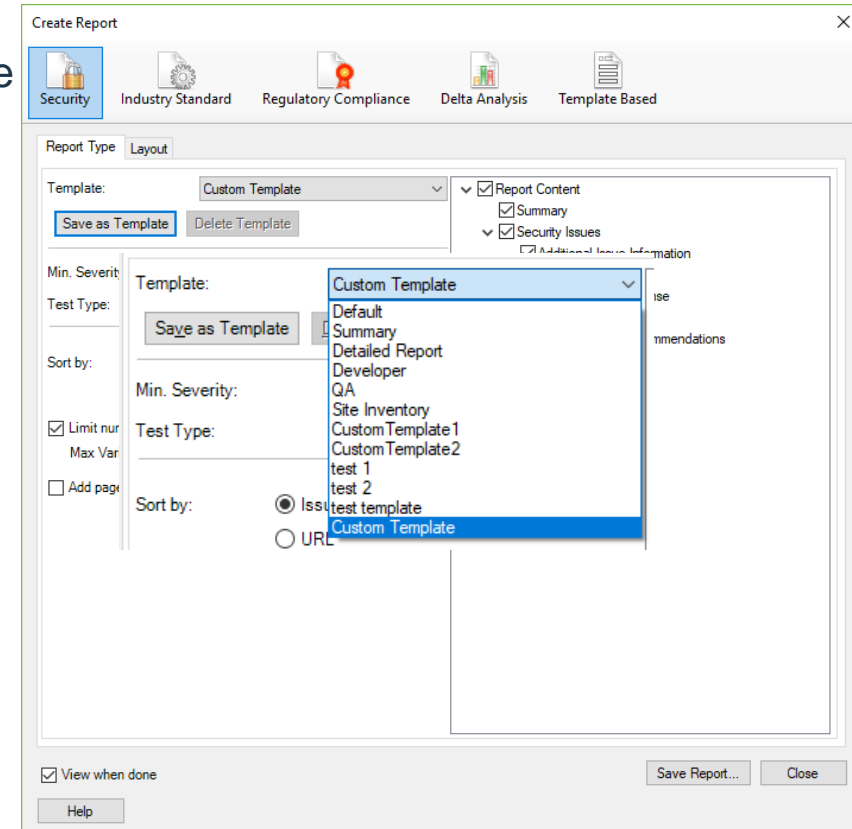
Improved Action-Base Scanning

- The Chromium component (“embedded browser”) has been upgraded under the hood
 - Upgraded from v57 to v65 (includes number of fixes and improvements)
 - Improved several product capabilities: Action-Based Explore, Manual Explore, Login, Multi-Step Operations
- Greater compatibility with newer web apps, and improved coverage to reveal additional vulnerabilities.

AppScan: Custom Report Template

- You can now save your customized report as a template
- You can use the saved report templates in the GUI in future scans
- You can also use them in the CMD with the parameter “/report_template”

```
[ /report_template/rtemplate/rtm <CliDefault,GuiDefault,Summary,DetailedReport,Developer,QA,SiteInventory,CustomTemplate1,CustomTemplate2,test 1,test 2,test template> {CliDefault} ]
```



RFEs

- [222860] Add Test Type filtering and sorting to Custom Word Reports
- [210824] Customized Security Report (as template) from both CLI & UI
- [211222] Include CVSS Scores in Industry Standard and Regulatory Compliance Reports
- [230988] When creating a job in ASE from ASD, add ability to skip Automatic Explore and continue directly with Test stage
- [176376] Support Windows 8.1 and Windows 10 (AppScan License): Solved due to new License Manager that replaced LKAD
- For more information <https://www.ibm.com/support/docview.wss?uid=swg27047066>

APARs

APAR	Security Update	Abstract
PI91784		Files with extensions EPS, AI and LZH are not excluded from scans by default
PI97418	Update	"Temporary Directory Found": Fixed validation issue information
PI98479		No Issue Information for "Body Parameters Accepted in Query" Issue
	New	"Spring Server Endpoints Exposed"

Known Issues

- **Important: Version 9.0.3.9 is not fully localized**
- Some of the changes in this version have not been fully translated into the supported non-English languages, both in the user interface, and in the Online Help documentation. User Interface In a few cases the localized interface contains either outdated localized text, or English text
- Online Help: Two important new features in this version are found in **Login Management** and **Explore Options** views of the configuration dialog box. The translated documentation is not updated with these features, and describes only the features from version 9.0.3.7. The English documentation is up-to-date. To access the English documentation for these features: In Windows Explorer, open ...\\AppScan Standard\\Docs
- Locate and open **AppScanOnlineHelp.chm** (the English Online Help file)
- Go to **Introduction > What's New**, where the first two items describe the new features and contain links to the full documentation

Known Issues

- When you record a login sequence in **Config > Login Management**, and then move to the **Review & Validate** tab, if **Request-Based** is the selected **Login Playback Method**, you may be unable to change it to **Action-Based**.

Workaround: Close the Scan Configuration dialog box and reopen it.



Questions?

Now is your opportunity to ask live questions.

To ask a question now:


Raise your hand by clicking Raise Hand. The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.



What's new in AppScan Enterprise 9.0.3.9

New Features in AppScan Enterprise 9.0.3.9

- Windows 2016 Server support
- Import HTTP Archive (HAR) traffic files for content scan jobs
- Users and Groups search capability in the Administration tab
- OWASP Top 10 2017 Report
- REST APIs for DevOps
- SQL Script to delete old and unused issues from database.
- Compute CVSS for issues imported/published from AppScan Standard
- TLS1.2 Support - defect fixes
- New ADAC capabilities - Proxy settings

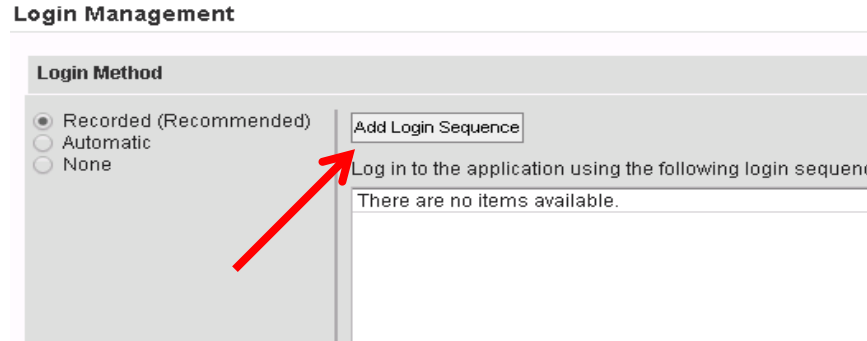


Windows 2016 Server support

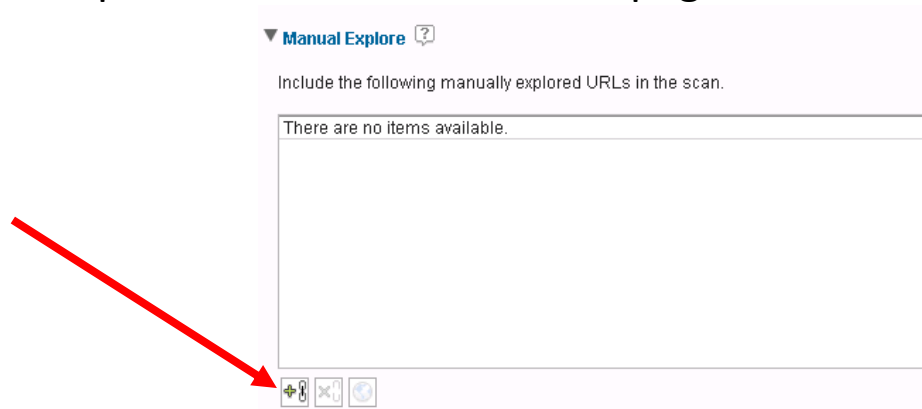
- Machine that hosts the SQL Server Database
- Machine that hosts the AppScan Enterprise Server
- Machine that hosts the Dynamic Analysis Scanner

Import HTTP Archive (HAR) traffic files for content scan jobs.

- To be used as login sequence data in **Login Management** page.

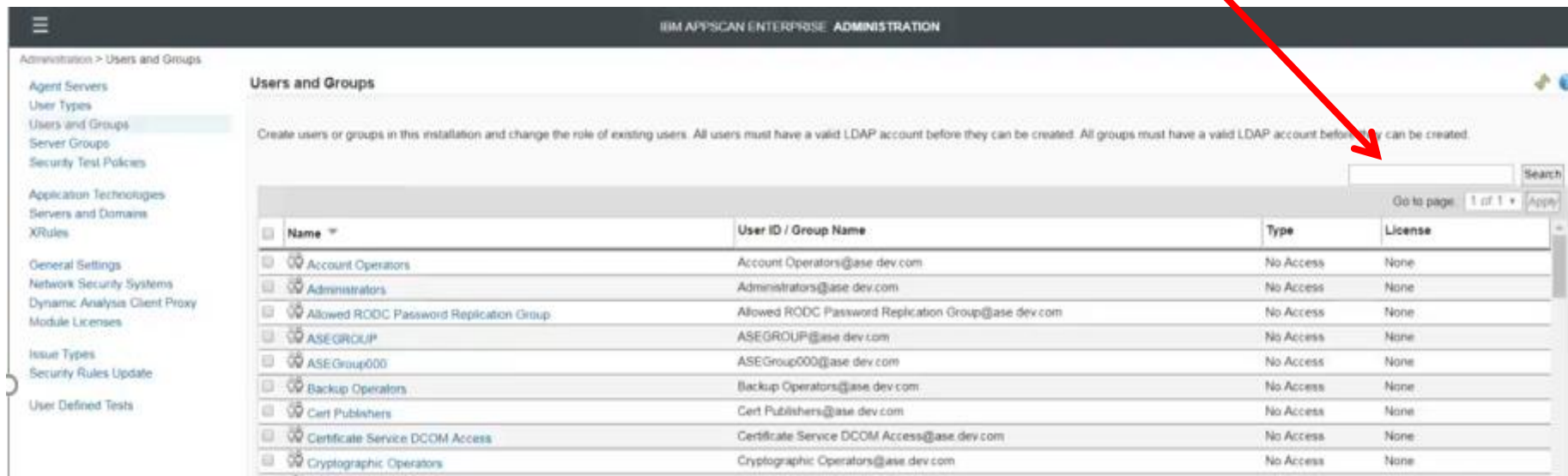


- To be used as explore data in **What to Scan** page.



Users and Groups search capability in the Administration tab

- Users having administrator role can search users and groups by 'Name' field.
- In “Administration > Users and Groups”
- Wildcard character '*' is supported.



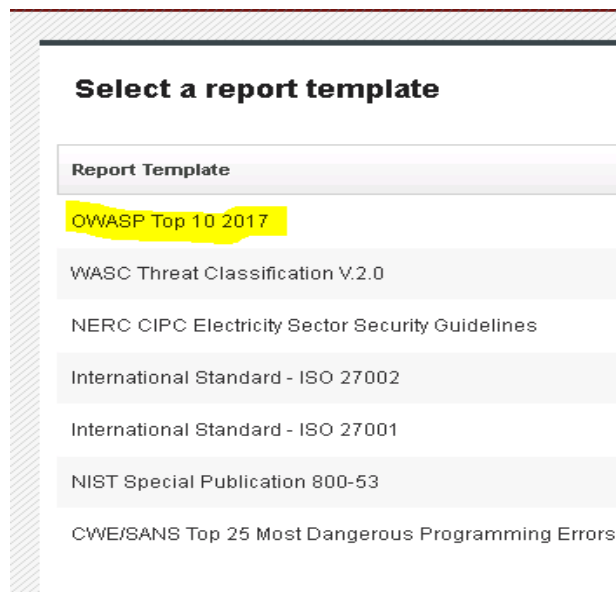
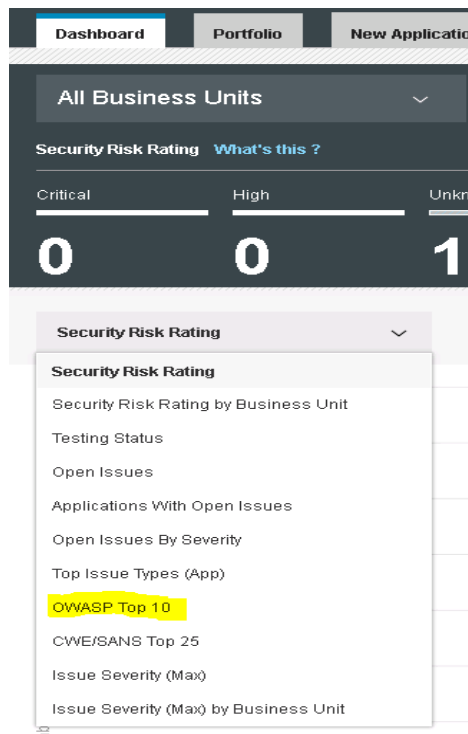
The screenshot displays the IBM AppScan Enterprise Administration interface. The left sidebar shows the navigation menu with 'Users and Groups' selected. The main content area is titled 'Users and Groups' and includes a search bar at the top right. A red arrow points to this search bar. Below the search bar is a table listing various system groups.

Name	User ID / Group Name	Type	License
Account Operators	Account Operators@ase.dev.com	No Access	None
Administrators	Administrators@ase.dev.com	No Access	None
Allowed RODC Password Replication Group	Allowed RODC Password Replication Group@ase.dev.com	No Access	None
ASEGROUP	ASEGROUP@ase.dev.com	No Access	None
ASEGroup000	ASEGroup000@ase.dev.com	No Access	None
Backup Operators	Backup Operators@ase.dev.com	No Access	None
Cert Publishers	Cert Publishers@ase.dev.com	No Access	None
Certificate Service DCOM Access	Certificate Service DCOM Access@ase.dev.com	No Access	None
Cryptographic Operators	Cryptographic Operators@ase.dev.com	No Access	None

OWASP Top 10 2017 Report

Monitor View

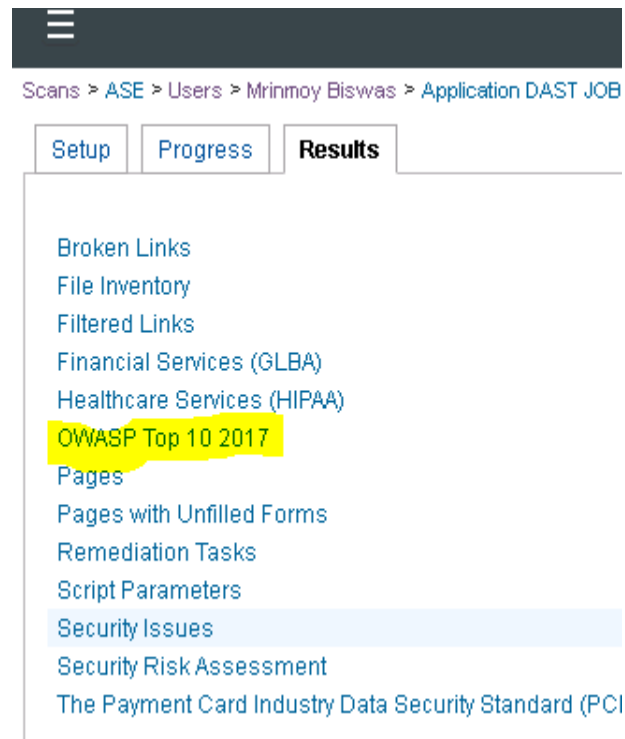
- “OWASP Top 10” report in Dashboard uses 2017 report.
- Report template “OWASP Top 10 2013” is replaced by “OWASP Top 10 2017” in export functionality.



OWASP Top 10 2017 Report

Scan View

- “OWASP Top 10 2013” report is replaced by “OWASP Top 10 2017” in report packs.



REST APIs for DevOps

Scan Management REST APIs

- Enhanced WebHook capability to post job status to endpoint URL.

`/services/folders/<folderId>/folderitems?templateid=<id>`

- Enhanced REST API to support exclusions with exceptions for content scan jobs.

`/services/folderitems/<fiid>/options/<option>`

REST APIs for DevOps

Application Management REST APIs

- New REST API to upload a template file.

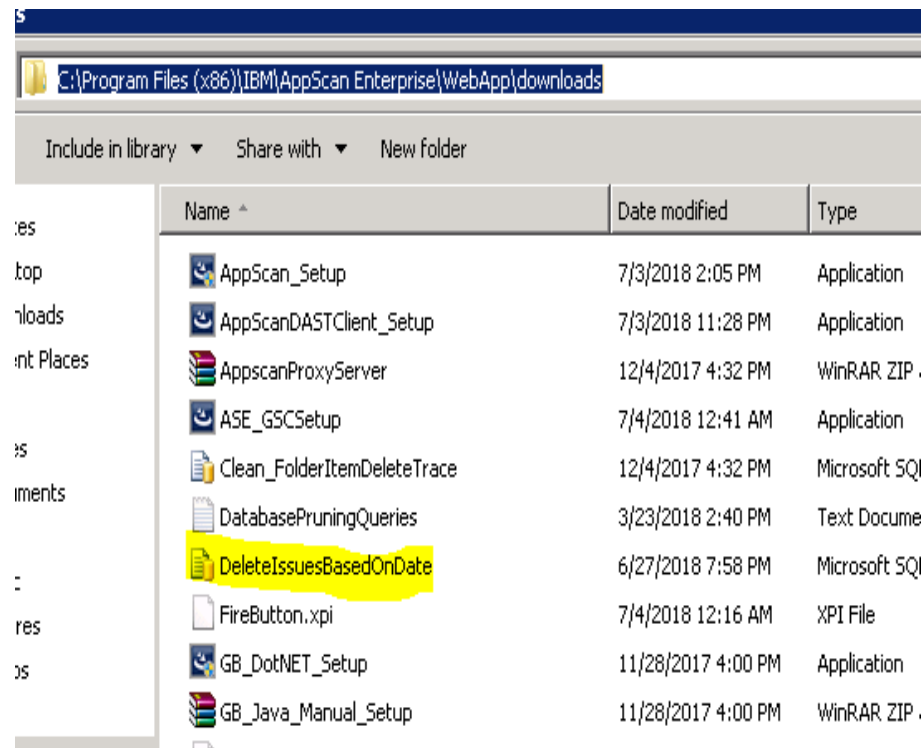
`POST /templates`

- New REST API to create a job using a template file.

`POST /jobs/createjobBasedOnTemplateFile`

SQL Script to delete old and unused issues from database.

- The SQL script 'DeleteIssuesBasedOnDate' accepts issues creation 'from' and 'to' data as input arguments to delete issues from database.



Compute CVSS for issues imported/published from AppScan Standard

- “AppScan Standard” scanner is enhanced so that CVSS is computed for issues imported/published from AppScan Standard.

CVSS_STD_2 x CVSS_SRC_0 Android-1 IBM_OZASMT webhook1 New Application New Application1									
Severity 202 items							Create Scan	Import Issues	...
Issue	Status	CVSS	Issue Type	Location	Scan Name	Severity Value	Last Updated	Date	
High (31)									
250	New	7.5	DOM Based Cross-Site Scripting	https://demo.testfire.net/disclaimer.htm	AppScan Standard	High	06/06/18 14:35		
256	New	7.5	Cross-Site Scripting	https://demo.testfire.net/search.aspx	AppScan Standard	High	06/06/18 14:35		
259	New	7.5	Cross-Site Scripting	https://demo.testfire.net/comment.aspx	AppScan Standard	High	06/06/18 14:35		
262	New	9.7	SQL Injection	https://demo.testfire.net/bank/account.aspx	AppScan Standard	High	06/06/18 14:35		

TLS1.2 Support - defects fixes

- SQL server patch need to be installed.
- SQL Server Native Client need to be installed.
- Enable TLS 1.2 on server boxes.
- Refer this technote for more information.

<http://www.ibm.com/support/docview.wss?uid=swg22015121>

New ADAC capabilities : Proxy settings

- Local Proxy Settings: Proxy for recordings in ADAC (login, manual explore, etc.) on the tested site
- A new option added: Use ASE Agent Proxy settings (Local Proxy settings will be identical to ASE Agent Proxy Settings)
- ASE Agent Proxy Settings: Proxy for the agent connections to the tested site

The screenshot displays the 'Proxy' settings window, which is divided into two main sections: 'Local' and 'ASE Agent'. The 'Local' section is currently active, showing options for proxy settings for AppScan Dynamic Analysis Client connections. The 'ASE Agent' section is also visible, showing options for proxy settings for AppScan Enterprise agent connections. Both sections include radio buttons for selecting the proxy type and input fields for custom proxy settings and authentication credentials.

Proxy ?

Local **ASE Agent**

Use these proxy settings for AppScan Dynamic Analysis Client connections to the tested site.

☒ Use ASE Agent proxy settings

☐ Use this machine's Internet Explorer proxy settings

☐ Don't use proxy

☐ Use custom proxy settings: **Proxy** ?

Local **ASE Agent**

Use these proxy settings for AppScan Enterprise agent connections to the tested site.

☒ Use AppScan Enterprise agent Internet Explorer proxy settings

☐ Don't use proxy

☐ Use custom proxy settings:

Address:

Port:

Use these credentials when Basic, NTLM or Kerberos authentication is required by the proxy:

User Name:

Password:

Confirm Password:

Domain:

Resolved Defects

- PI79408 "Link to unclassified site" issue is unable to export to Detailed Security Issues PDF
- 33790707 Upgraded Jackson data bind libraries bundled in AppScan Enterprise
- PI94897 CVSS values in Monitor tab is zero for issues imported/published to monitor tab from AppScan Standard
- PI85553 2013 OWASP removal and 2017 inclusion
- PI84292 Documentation to create a user account to run stored procedures is no longer valid
- PI95800 Excel report export not displaying properly from the monitor view
- PI83739 Non-admin user has access to Dynamic Analysis Client proxy link



Questions?

Now is your opportunity to ask live questions.

To ask a question now:

Raise your hand by clicking Raise Hand. The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.



IBM Security Learning Academy

www.SecurityLearningAcademy.com

New content
published daily!



Learning at
no cost!

Learning Videos • Hands-on Labs • Live Events

Where do you get more information?

Questions on this or other topics can be directed to the dW Answers forum:
<https://developer.ibm.com/answers/topics/appscan-enterprise/>

More information you can review:

- [AppScan Enterprise fixpack 9.0.3.9 available at FixCentral](#)
- [AppScan Standard 9.0.3 Fix Pack 9 at Fix Central](#)
- [AppScan Source 9.0.3.9 available at Fix Central](#)

- [AppScan Enterprise versions available](#)
- [AppScan Standard versions available](#)
- [AppScan Source versions available](#)

- Security Learning Academy: www.SecurityLearningAcademy.com

Useful links:

[Get started with IBM Security Support](#)

[IBM My Support](#) | [Sign up for "My Notifications"](#)

[FREE learning resources on the Security Learning Academy](#)

Follow us:





THANK YOU

FOLLOW US ON:



facebook.com/IBMSecuritySupport



youtube/user/IBMSecuritySupport



[@askibmsecurity](https://twitter.com/askibmsecurity)



SecurityLearningAcademy.com



securityintelligence.com



xforce.ibmcloud.com

© Copyright IBM Corporation 2018. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.